UNTERSUCHUNGEN ÜBER INTUITIONISTISCHE ALGEBRA

VON

Dr A. HEYTING

VERHANDELINGEN DER NEDERLANDSCHE AKADEMIE VAN WETENSCHAPPEN, AFDEELING NATUURKUNDE

EERSTE SECTIE, DEEL XVIII, Nº. 2

1941

N.V. NOORD-HOLLANDSCHE UITGEVERS MAATSCHAPPIJ

AMSTERDAM

Nederl. Akad. Wet., Verh. (Eerste Sectie), Dl. XVIII, No. 2, p. 1—36, 1941

K 244

1941

Printed in Holland

Einleitung.

Bei intuitionistischer Behandlung zerfällt die Algebra in zwei Gebiete, welche ganz verschiedene Methoden erfordern. Das erste umfaßt die Theorie der endlichen Erweiterungskörper von Primkörpern, und diejenigen Teile der Algebra, welche mit dieser Theorie die folgenden Merkmale gemeinsam haben. Alle auftretenden Spezies sind *diskret*, d.h. von je zweien ihrer Elemente läßt sich entscheiden, ob sie gleich sind oder nicht; für alle Probleme wird eine Lösung angestrebt, welche in endlichvielen Schritten zu einem positiven Ergebnis führt. Entscheidende Resultate auf diesem Gebiet erreichte schon KRONECKER [1]), indem er eine Methode angab, nach der jedes Polynom über einem der genannten Körper in Primfaktoren zerlegt werden kann; auch in neuerer Zeit beschäftigt dieses und verwandte Probleme das Interesse mehrerer Algebraiker [2]).

Von VAN DER WAERDEN [3]) stammt ein Beispiel eines diskreten Körpers, in dem nicht entscheidbar ist, ob das Polynom $x^2 + 1$ prim ist. Hieraus folgt schon, daß die allgemeine intuitionistische Körpertheorie ganz anders aussehen muß als die soeben umschriebene spezielle Theorie. Ihre einfacheren Teile (lineare Gleichungen; Elimination) spalten sich, ähnlich wie z.B. die Reihenlehre [4]), in eine positive und eine negative Theorie; die positive geht im wesentlichen die klassischen Wege und erreicht die klassischen Ziele. Da aber fast jeder Beweis verschärft werden muß und an vielen Stellen ziemlich unerwartet Schwierigkeiten auftauchen (z.B. in 1.7.2 wenn $p + q > n$; in 2.3.5; bei der Eulerschen Eliminationsmethode) und überdies diese Theorien die Grundlage aller weiteren algebraischen Untersuchungen bilden, ist eine ausführliche Darstellung auch für sie notwendig. Für schwierigere Gebiete bleibt nur die negative Theorie bestehen.

---

[1]) L. KRONECKER, Grundzüge einer arithmetischen Theorie der algebraischen Größen [J. reine angew. Math. **92** (1882) = Werke II, 237—388, § 4].

[2]) H. S. VANDIVER, On the foundations of a constructive theory of discrete commutative algebra [Proc. Nat. Acad. Sci. U.S.A. **20** (1937), 579—584; **21** (1935), 162—165]; Constructive derivation of the decomposition-field of a polynomial [Ann. of Math. (2) **37** (1936), 1—6]; On the ordering of real algebraic numbers by constructive methods [ibid., 7—16].

B. L. VAN DER WAERDEN, Moderne Algebra I, 2. Auflage, § 42.

[3]) B. L. VAN DER WAERDEN, Eine Bemerkung über die Unzerlegbarkeit von Polynomen [Math. Ann. **102** (1930), 738—739].

[4]) L. E. J. BROUWER, Über die Bedeutung des Satzes vom ausgeschlossenen Dritten in der Mathematik, insbesondere in der Funktionentheorie [J. reine angew. Math. **154** (1924), 1—7].

M. J. BELINFANTE, Zur intuitionistischen Theorie der unendlichen Reihen [S.—B. preuss. Akad. Wiss. **1929**, 639—660]; Absolute Konvergenz in der intuitionistischen Mathematik [Proc. Kon. Akad. v. Wetensch., Amsterdam, **33**, 1180—1184 (1930)].

So läßt sich nicht jedes Polynom über einem Körper in Primfaktoren zerlegen, da wir ja nicht einmal für jedes Polynom entscheiden können ob es prim ist. Wohl gilt der entsprechende negative Satz: Es ist unmöglich, ein Polynom anzugeben, das nicht in Primfaktoren zerlegt werden kann.

§ 1. Grundbegriffe.

1.1. Alles Folgende bezieht sich auf eine mathematische Spezies S, in welcher eine mit $=$ zu bezeichnende *Gleichheitsrelation* definiert ist, die als reflexiv, transitiv und symmetrisch vorausgesetzt wird. Die Relation $a = b$ zwischen Elementen von S kann mit der Identität von a und b als Elementen von S gleichbedeutend sein; das braucht aber nicht der Fall zu sein. Wir behalten uns also vor, gewisse Elemente von S für unsere Zwecke zu „identifizieren". Statt „$a = b$ ist ungereimt" sagen wir auch: „a ist (*numerisch*) *verschieden* von b" oder „$a \neq b$". Wir setzen nicht voraus, daß, wenn $a \neq b$ ungereimt ist, $a = b$ gilt; diese Eigenschaft gilt nicht für jede Spezies, wenn die Identität als Gleichheit betrachtet wird, und würde also den Bereich der in der Algebra zugelassenen Spezies einschränken. Sie gilt aber für solche Spezies, in welchen eine Entfernungsrelation definiert ist (1.3.3).

1.2.1. Die Definitionen der *Gruppe* und des *Ringes* sind von denjenigen der klassischen Mathematik nicht verschieden. Wegen der soeben beschriebenen allgemeinen Auffassung der Gleichheit muß die Eindeutigkeit der Verknüpfungen besonders festgelegt werden:

Aus $a = b$ und $c = d$ folgt $a + c = b + d$ und $ac = bd$.

Auch die elementaren Eigenschaften, die man z.B. bei V. D. WAERDEN [5]) findet, führen nicht zu Schwierigkeiten. Diese treten erst auf, wenn die Negation oder der Begriff „verschieden" auftritt, namentlich bei dem Begriff des Nullteilers. Wir wollen hierauf etwas näher eingehen.

1.2.2. SATZ. In einer (additiv geschriebenen) Gruppe S folgt aus $x \neq y$, daß für jedes Element a von S gilt $a + x \neq a + y$ und $x + a \neq y + a$.

Beweis. Aus $a + x = a + y$ würde nach 1.2.1 folgen $-a + a + x = -a + a + y$, also $x = y$, gegen die Voraussetzung.

1.2.3. SATZ. In einem Ring folgt aus $ab \neq 0$, daß $a \neq 0$ und $b \neq 0$.

Beweis. Wäre z.B. $a = 0$, so hätte man nach 1.2.1, $ab = 0b = 0$.

Bekanntlich kann es in einem Ring Elemente a und b geben, so daß $a \neq 0$, $b \neq 0$, $ab = 0$; a und b heißen dann *Nullteiler*. In einem *Ring ohne Nullteiler* folgt aus $a \neq 0$ und $b \neq 0$ immer $ab \neq 0$; man darf hieraus nicht folgern, daß, wenn $ab = 0$, immer entweder $a = 0$ oder $b = 0$. Es kann nämlich vorkommen, daß man trotz $ab = 0$ nicht entscheiden kann, welche der Zahlen a und b gleich 0 ist [6]).

---

[5]) Moderne Algebra I, 2. Auflage, § 6 und § 11 bis S. 40.

[6]) A. HEYTING, Mathematische Grundlagenforschung, S. 21.

1.3.1. Eine neue Schwierigkeit tritt auf bei der Definition des Körpers. Es kann nicht einfach vorausgesetzt werden, daß jedes von 0 verschiedene Element eines Körpers ein inverses besitzt; dieses trifft z.B. für den Körper der reellen Zahlen nicht zu. Damit man die inverse a^{-1} einer reellen Zahl a berechnen kann, ist notwendig, daß eine rationale Zahl r zwischen 0 und a bekannt ist; in diesen Fall sagen wir, dass a von 0 *entfernt* ist. Wir definieren nun allgemein eine *Entfernungsrelation* in einer Spezies S als eine symmetrische Relation $\#$, welche die folgenden Eigenschaften besitzt:

I. Die Beziehungen $a = b$, $a \# b$ zwischen Elementen von S schließen sich gegenseitig aus.

II. Wenn $a \# b$ ungereimt ist, so gilt $a = b$.

III. Wenn $a \# b$, so gilt für jedes Element c von S entweder $a \# c$ oder $b \# c$ (d.h. es gilt wenigstens eine dieser Beziehungen und es läßt sich entscheiden, welche gilt, während es für die andere vielleicht unentschieden bleibt, ob sie gilt).

1.3.2. SATZ. In einer Spezies mit Entfernungsrelation folgt aus $a = b$ und $b \# c$, daß $a \# c$.

Beweis. Nach 1.3.1, III ist entweder $a \# b$ oder $a \# c$; das erste steht in Widerspruch zu $a = b$, also $a \# c$.

1.3.3. SATZ. In einer Spezies mit Entfernungsrelation folgt aus der Ungereimtheit der Ungereimtheit von $a = b$ (also aus der Ungereimtheit von $a \neq b$), daß $a = b$.

Beweis. Nach 1.3.1, I folgt aus $a \# b$, daß $a \neq b$, also aus der Ungereimtheit von $a \neq b$ die Ungereimtheit von $a \# b$; aus der letzteren folgt nach 1.3.1, II, daß $a = b$.

1.4.1. DEFINITION. Eine *Gruppe mit Entfernungsrelation* ist eine Spezies S mit Entfernungsrelation, welche eine Gruppe ist, und welche außerdem die folgende Eigenschaft besitzt:

Aus $x \# y$ folgt für jedes Element a von S $a + x \# a + y$ und $x + a \# y + a$. (Verschärfte Eindeutigkeit der Substraktion).

1.4.2. SATZ. In einer Gruppe mit Entfernungsrelation folgt aus $a + b \# 0$, daß entweder $a \# 0$ oder $b \# 0$.

Beweis. Aus der Voraussetzung folgt nach 1.4.1 zunächst $-a + a + b \# -a$, also $b \# -a$. Nach 1.3.1, III hat man nun entweder $b \# 0$ oder $-a \# 0$; aus letzterem folgt durch beiderseitige Addition von a nach 1.4.1, daß $a \# 0$.

1.5.1. DEFINITION. Ein *Ring mit Entfernungsrelation* ist ein Ring, dessen additive Gruppe eine Gruppe mit Entfernungsrelation ist, und in welchem noch gilt:

Aus $ab \# 0$ folgt $a \# 0$ und $b \# 0$.

1.5.2. Ein *regulärer* Ring ist ein Ring mit Entfernungsrelation, in dem auch umgekehrt gilt:

Aus $a \# 0$ und $b \# 0$ folgt $ab \# 0$.

Ein kommutativer regulärer Ring heißt auch *Integritätsbereich.*

1.5.3. SATZ. In einem regulären Ring folgt aus $ab = 0$ und $a \neq 0$, daß $b = 0$.

Beweis. (a) Aus $ab = 0$ und $b \# 0$ folgt $a = 0$, denn wäre $a \# 0$, so wäre $ab \# 0$; Anwendung von 1.3.1, II.

(b) Aus $ab = 0$ und $a \neq 0$ folgt $b = 0$, denn wäre $b \# 0$, so wäre $a = 0$ nach (a).

Bemerkung. In einem Ring ohne Nullteiler gilt dieser Satz nicht notwendig, denn aus $ab = 0$ und $a \neq 0$ kann man folgern, daß $b \neq 0$ unmöglich ist; hieraus folgt aber noch nicht, daß $b = 0$ (1.1).

1.5.4. SATZ. Ein regulärer Ring ist zugleich Ring ohne Nullteiler. (1.2.3).

Beweis. Aus $a \neq 0$ und $b \neq 0$ folgt $ab \neq 0$, denn wäre $ab = 0$, so würde aus $a \neq 0$ nach 1.5.3 folgen $b = 0$.

1.5.5. SATZ. In einem regulären Ring folgt aus $x \# y$ und $a \# 0$, daß $ax \# ay$ und $xa \# ya$. (Verschärfte Eindeutigkeit der Division).

Beweis. Aus $x \# y$ folgt nach 1.4.1 $x - y \# 0$; ist nun $a \# 0$, so hat man nach 1.5.2 $a(x - y) \# 0$, also $ax \# ay$, wiederum nach 1.4.1.

1.5.6. SATZ. Ist $f(x_1, \ldots, x_n)$ ein Polynom mit Koeffizienten aus dem Integritätsgebiet I und sind $\xi_1, \ldots, \xi_n, \eta_1, \ldots, \eta_n$ solche Elemente von I, daß $f(\xi_1, \ldots, \xi_n) \# f(\eta_1, \ldots, \eta_n)$, so ist für wenigstens einen Index i $\xi_i \# \eta_i$.

Beweis. Nach 1.4.2 genügt es, den Satz für eingliedrige Polynome zu beweisen. Nun ist zunächst

$$a\xi_1\xi_2 - a\eta_1\eta_2 = a\xi_1(\xi_2 - \eta_2) + a\eta_2(\xi_1 - \eta_1),$$

woraus nach 1.4.2 und 1.5.1 der Satz für Produkte aus zwei Faktoren folgt. Der allgemeine Fall wird durch Induktion nach der Anzahl der Faktoren erledigt.

1.6.1. DEFINITION. Ein Integritätsgebiet mit einem von 0 entfernten Einselement 1 heißt ein (kommutativer) *Körper*, wenn es zu jedem von 0 entfernten Element a ein *inverses* a^{-1} enthält so daß $aa^{-1} = 1$. (Da ich mich durchweg auf den kommutativen Fall beschränke, lasse ich dieses Adjektiv im folgenden weg.)

1.6.2. Der Übersichtlichkeit halber stelle ich die Definition des Körpers hier zusammen. Eine mathematische Spezies K heißt ein Körper, wenn sie folgenden acht Eigenschaften besitzt:

1. In K ist eine reflexive, symmetrische, transitive Gleichheitsrelation $=$ definiert (1.1);
2. In K ist eine „Entfernungsrelation" $\#$ definiert mit den folgenden drei Eigenschaften (1.2.1):
   - I. Die Relationen $a \# b$ und $a = b$ sind miteinander unverträglich;
   - II. Ist $a \# b$ ungereimt, so gilt $a = b$;
   - III. Aus $a \# b$ folgt für beliebiges c entweder $a \# c$ oder $b \# c$;
3. In K ist eine Abelsche Gruppe als additive Gruppe definiert;
4. Aus $x \# y$ folgt für beliebiges a, $a + x \# a + y$ (1.4.1);
5. In K ist eine eindeutige, assoziative und gegenüber der Addition distributive Multiplikation definiert;

6. Die Multiplikation besitzt den Modulus 1; $1 \neq 0$;
7. Die Division ist möglich durch jedes von 0 entfernte Element (1.6.1);
8. Aus $x \neq y$ und $a \neq 0$ folgt $ax \neq ay$ und $xa \neq ya$ (1.5.2).

Bemerkung. Aus 2 III folgt, indem man c durch a ersetzt, daß die Entfernungsrelation symmetrisch ist. Der Satz (1.5.1), daß aus $ab \neq 0$ sowohl $a \neq 0$ als $b \neq 0$ folgt, kann aus den obigen 8 Axiomen hergeleitet werden. Da das Vorhergehende hauptsächlich die Festlegung einer Terminologie bezweckt, gehe ich auf die axiomatischen Zusammenhänge hier nicht ein.

1.6.3. Die rationalen Zahlen, die reellen Zahlen und die gewöhnlichen komplexen Zahlen bilden Körper.

1.7.1. Alle Polynome in einer Veränderlichen x über ein Integritätsgebiet I bilden ein neues Integritätsgebiet $I[x]$, wenn die Entfernungsrelation zwischen Polynomen wie folgt definiert wird:

Zwei Polynome in x heißen *voneinander entfernt*, wenn die Koeffizienten von wenigstens einer Potenz von x in beiden Polynomen voneinander entfernt sind. Insbesondere ist ein Polynom von 0 entfernt, wenn wenigstens ein Koeffizient von 0 entfernt ist.

Für das Polynom $a_n x^n + \ldots + a_0$ ist die Zahl n (und jede größere natürliche Zahl) ein *Maximalgrad*; ist $a_n = 0$, so ist auch $n-1$ ein Maximalgrad, usw. Ist $a_r \neq 0$ $(r \leq n)$, so ist r ein *Minimalgrad* des Polynoms. Ist $a_r \neq 0$ und $a_{r+1} = \ldots = a_n = 0$ so heiße das Polynom *regulär* und r sein *genauer Grad*.

1.7.2. Wir müssen beweisen, daß $I[x]$ die Eigenschaften I, II, III aus 1.3.1, und ferner die Eigenschaften aus 1.4.1, 1.5.1 und 1.5.2 besitzt. Für die ersten vier ist das sehr leicht; um die Gültigkeit von 1.5.1 nachzuweisen, setzen wir

$$(b_p x^p + \ldots + b_0)(c_q x^q + \ldots + c_0) = a_n x^n + \ldots + a_0; \quad . \quad (1)$$

$p + q \geq n$; wegen der Bemerkung in 1.2.3 braucht nicht $p + q = n$ zu sein.

$$a_{r+s} = b_p c_{r+s-p} + \ldots + b_r c_s + \ldots + b_{r+s-q} c_q. \quad . \quad . \quad . \quad (2)$$

Ist nun $a_{r+s} \neq 0$, so ist nach 1.4.2 wenigstens ein Glied der rechten Seite von 0 entfernt, also ist nach 1.5.1 sowohl ein b wie ein c von 0 entfernt. Hierdurch ist die Eigenschaft 1.5.1 für Polynome bewiesen.

Ist umgekehrt $b_r \neq 0$ und $c_s \neq 0$, so folgt aus (2) nach 1.3.1, daß entweder $a_{r+s} \neq 0$, oder ein zweites Glied rechts von 0 entfernt ist; in diesem Fall gibt es entweder ein $t > r$, so daß $b_t \neq 0$, oder ein $u > s$, so daß $c_u \neq 0$. Wir betrachten nun die (2) entsprechende Gleichung für a_{t+s}, bzw. a_{r+u}; tritt wieder der zweite Fall ein, so wiederholen wir den Prozeß, bis der erste Fall eintritt und wir ein $a_m \neq 0$ finden. Dies ist nach einer endlichen Anzahl von Schritten der Fall, weil der Index von a nicht über n wachsen kann. Hierdurch ist auch die Eigenschaft 1.5.2 bewiesen.

1.7.3. Es ist nützlich, die Relation (1), speziell für den Fall $p + q > n$, etwas näher zu untersuchen. Die letzte Betrachtung zeigt, daß für $r + s > n$

jedes einzelne Produkt $b_r c_s$ verschwindet; denn wäre $b_r c_s \neq 0$, so könnte man in der angegebenen Weise ein $a_m \neq 0$ bestimmen mit $m \geqq r + s > n$, was natürlich ungereimt ist. Der folgende Satz zeigt nun, daß, sobald ein $a \neq 0$, $p + q$ nach oben begrenzt ist:

1.7.4. SATZ. Ist in (1) $a_{n-t} \neq 0$ und $p + q > n + t$, so ist entweder $b_p = 0$ oder $c_q = 0$.

Beweis. Man kann r und s so finden, daß $r + s = n - t$ und $b_r c_s \neq 0$; nun ist $p + q + r + s > n + t + n - t = 2n$, also entweder $r + q > n$ oder $s + p > n$. Im ersten Fall ist $b_r c_q = 0$, also, wegen $b_r \neq 0$, $c_q = 0$; im zweiten Fall ergibt sich ebenso $b_p = 0$.

Durch wiederholte Anwendung dieses Satzes kann man jede Relation wie (1) so schreiben, daß $p + q \leqq n + t$, wo $n - t$ der Index des ersten von 0 entfernten Koeffizienten rechts ist.

1.7.5. Für $t = 0$ erhalten wir:

SATZ. Ist ein reguläres Polynom in Faktoren zerlegt, so sind auch diese regulär und der genaue Grad des Produktes ist gleich der Summe der genauen Grade der Faktoren.

1.7.6. Man kann nacheinander mehrere Veränderliche zu I adjungieren, wodurch immer wieder ein Integritätsgebiet entsteht. Die Definition der Entfernungsrelation zwischen zwei Polynomen aus $I(x_1, x_2, \ldots, x_n)$ ist zunächst abhängig von der Reihenfolge, in welcher die Veränderlichen adjungiert worden sind; man sieht aber sofort, daß zwei Polynome dann und nur dann voneinander entfernt sind, wenn wenigstens ein Potenzprodukt der Veränderlichen in den beiden Polynomen voneinander entfernte Koeffizienten besitzt.

1.8. Aus einem Integritätsgebiet I können wir in bekannter Weise den *Quotientenkörper* K bilden, dessen Elemente Paare (a, b) von Elementen aus I mit $b \neq 0$ sind. Dabei heißen die Elemente (a, b) und (c, d) von K voneinander entfernt, wenn $ad \neq bc$ in I gilt; $(a, b) = (c, d)$, wenn $ad = bc$. Nullelement ist $(0, 1)$, Einselement $(1, 1)$. Es ist zu zeigen, daß 1.3.1, 1.4.1, 1.5.1, 1.5.2 und 1.6.1 gelten.

Beweis für 1.3.1, III. Es sei $(a, b) \neq (c, d)$ und (e, f) ein beliebiges Element von K. $ad \neq bc$, also, wegen $f \neq 0$, $adf \neq bcf$ (1.5.6). Hieraus folgt, daß entweder $adf \neq bde$ oder $bcf \neq bde$; aus dem ersten folgt $d(af - be) \neq 0$, also $af \neq be$, d.h. $(a, b) \neq (e, f)$; aus dem zweiten ebenso $(c, d) \neq (e, f)$.

Beweis für 1.4.1. Es sei $(a, b) \neq (c, d)$ und (e, f) ein beliebiges Element von K. Aus $ad \neq bc$ erhält man leicht $df(af + be) \neq bf(cf + de)$, also $(af + be, bf) \neq (cf + de, df)$, d.h. $(a, b) + (e, f) \neq (c, d) + (e, f)$. Die Eigenschaften 1.5.1, 1.5.2 sind klar.

Ist $(a, b) \neq 0$, also $a \neq 0$, so ist $(a, b)^{-1} = (b, a)$; also gilt 1.6.1.

§ 2. Lineare Gleichungen.

Ich behandle diese Theorie zunächst, was ein gewisses prinzipielles

Interesse bietet, determinantenfrei, sodann (2.3) unter Heranziehung der Determinanten.

2.1. *Lineare Abhängigkeit von Vektoren.*

2.1.1. Die Einführung der Entfernungsrelation bringt ähnliche Verschärfungen in der Theorie der linearen Abhängigkeit mit sich. Ich gebe die Definitionen für Vektoren über einem Körper K. Ein n-dimensionaler *Vektor* $\mathfrak{x}$ ist eine Folge von n Körperelementen $(x_1, \ldots, x_n)$. Gleichheit von Vektoren, Addition von Vektoren, Multiplikation eines Vektors mit einem Körperelement und das innere Produkt von zwei Vektoren werden in bekannter Weise erklärt. Zwei Vektoren $\mathfrak{x}$ und $\mathfrak{y}$ heißen *voneinander entfernt*, wenn für wenigstens einen Index i gilt $x_i \neq y_i$. Der Vektor $\mathfrak{y}$ heißt von den Vektoren $\mathfrak{x}_1, \ldots, \mathfrak{x}_m$ linear *abhängig*, wenn es Elemente von K, $c_1, \ldots, c_m$, gibt, so daß

$$\mathfrak{y} = c_1 \mathfrak{x}_1 + \ldots + c_m \mathfrak{x}_m. \quad \ldots\ldots\ldots \quad (A)$$

$\mathfrak{y}$ heißt *unabhängig* von $\mathfrak{x}_1, \ldots, \mathfrak{x}_m$, wenn für jede Wahl von $c_1, \ldots, c_m$ in (A) das Zeichen $\neq$ stehen muß. $\mathfrak{y}$ heist (linear) *frei* von $\mathfrak{x}_1, \ldots, \mathfrak{x}_m$, wenn für jede Wahl von $c_1, \ldots, c_m$ in A das Zeichen $\neq$ stehen muss.

2.1.2. Die Vektoren $\mathfrak{x}_1, \ldots, \mathfrak{x}_m$ sind *schwach* linear *abhängig*, wenn es Elemente von K, $c_1, \ldots, c_m$, gibt, die nicht alle 0 sein können, so daß

$$c_1 \mathfrak{x}_1 + \ldots + c_m \mathfrak{x}_m = 0. \quad \ldots\ldots\ldots \quad (B)$$

Sie sind (stark) linear *abhängig*, wenn (B) gilt mit wenigstens einem $c_i \neq 0$.

SATZ. Sind $\mathfrak{x}_1, \ldots, \mathfrak{x}_m$ nicht stark voneinander abhängig, so sind sie auch nicht schwach voneinander abhängig.

Beweis. Aus $\Sigma c_i \mathfrak{x}_i = 0$ folgt nach Voraussetzung, daß kein $c_i \neq 0$ sein kann, so daß alle $c_i = 0$; folglich ist $\Sigma c_i \mathfrak{x}_i = 0$ unmöglich, wenn nicht alle $c_i = 0$ sind.

Wir nennen in diesem Fall die m Vektoren voneinander *unabhängig*. Auch hier stellt sich dem negativen ein positiver Begriff an die Seite: Die m Vektoren heißen (linear) voneinander *frei*, wenn

$$c_1 \mathfrak{x}_1 + \ldots + c_m \mathfrak{x}_m \neq 0,$$

sobald wenigstens ein $c_i \neq 0$.

2.1.3. SATZ. Sind die Vektoren $\mathfrak{x}_1, \ldots, \mathfrak{x}_n$ voneinander frei und ist $\mathfrak{y}$ frei von den $\mathfrak{x}$, so sind $\mathfrak{x}_1, \ldots, \mathfrak{x}_n, \mathfrak{y}$ voneinander frei.

Beweis. Ist in $\mathfrak{z} = \Sigma a_i \mathfrak{x}_i + b\mathfrak{y}$ ein $a_i \neq 0$, so ist $\Sigma a_i \mathfrak{x}_i \neq 0$, also entweder $\mathfrak{z} \neq 0$ oder $b \neq 0$. Ist aber $b \neq 0$, so ist $\mathfrak{z} = b\left(\mathfrak{y} + \Sigma \frac{a_i}{b} \mathfrak{x}_i\right) \neq 0$.

2.1.4. Die Vektorspezies $\mathfrak{X}$ heißt von der anderen $\mathfrak{P}$ abhängig, bzw. unabhängig oder frei, wenn jeder Vektor aus $\mathfrak{X}$ abhängig von einer end-

lichen Teilspezies von $\mathfrak{P}$, bzw. unabhängig oder frei von jeder endlichen Teilspezies von $\mathfrak{P}$ ist.

Ist $\mathfrak{X}$ abhängig von $\mathfrak{P}$, so ist jeder von $\mathfrak{X}$ abhängiger Vektor von $\mathfrak{P}$ abhängig und jeder von $\mathfrak{P}$ freier Vektor von $\mathfrak{X}$ frei.

2.1.5. $\mathfrak{X}$ und $\mathfrak{P}$ heißen *äquivalent*, wenn sowohl $\mathfrak{X}$ von $\mathfrak{P}$ als $\mathfrak{P}$ von $\mathfrak{X}$ abhängig ist.

2.1.6. AUSTAUSCHSATZ [7]). Sind $\xi_1, \ldots, \xi_p$ voneinander frei und alle linear abhängig von $\eta_1, \ldots, \eta_m$, so kann man in $\eta_1, \ldots, \eta_m$ ein Teilsystem $\eta_{i_1}, \ldots, \eta_{i_p}$ bestimmen, welches man gegen $\xi_1, \ldots, \xi_p$ austauschen kann, so daß das durch diesen Austausch entstehende System dem ursprünglichen System $\eta_1, \ldots, \eta_m$ äquivalent ist.

Beweis. Wir brauchen nur in dem Beweis bei V. D. WAERDEN überall „unabhängig" durch „frei" zu ersetzen; hier möge die folgende kurze Andeutung genügen. Es seien $\xi_1, \ldots, \xi_{p-1}$ voneinander frei und gegen $\eta_{i_1}, \ldots, \eta_{i_{p-1}}$ austauschbar; dann gilt

$$\xi_p = a_1 \xi_1 + \ldots + a_{p-1} \xi_{p-1} + b_1 \eta_{k_1} + \ldots + b_{m-p+1} \eta_{k_{m-p+1}},$$

wo nur die nicht ausgetauschten η auftreten. Da die ξ voneinander frei sind, ist wenigstens ein $b_l \not\equiv 0$, usw.

2.1.7. ZUSATZ. Ist im Austauschsatz $p = m$, so sind auch die η voneinander frei.

Beweis. In diesem Fall sind die Systeme der ξ und der η äquivalent. Wir können nun $x_1, \ldots, \xi_{p-1}$ tauschen gegen $p-1$ der η, welche wir mit $\eta_1, \ldots, \eta_{p-1}$ bezeichnen, so daß

$$\xi_1, \ldots, \xi_{p-1}, \eta_p \text{ äq. } \eta_1, \ldots, \eta_p \text{ äq. } \xi_1, \ldots, \xi_p,$$

also insbesondere

$$\eta_p = a_1 \xi_1 + \ldots + a_p \xi_p \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (1)$$

und

$$\xi_p = b_1 \xi_1 + \ldots + b_{p-1} \xi_{p-1} + b_p \eta_p . \quad . \quad . \quad . \quad . \quad . \quad (2)$$

Durch Einsetzen von (1) in (2) erhält man, da die ξ voneinander frei sind, $a_p b_p = 1$, also $a_p \not\equiv 0$. Ist nun in

$$\delta = c_1 \xi_1 + \ldots + c_{p-1} \xi_{p-1} + c_p \eta_p . \quad . \quad . \quad . \quad . \quad . \quad (3)$$

eine der Zahlen $c_1, \ldots, c_{p-1}$ von 0 entfernt, so ist entweder $\delta \not\equiv 0$ oder $c_p \not\equiv 0$. Ist $c_p \not\equiv 0$, so folgt durch Einsetzen von (1) in (3) wegen $a_p c_p \not\equiv 0$, daß $\delta \not\equiv 0$. $\xi_1, \ldots, \xi_{p-1}, \eta_p$ sind also voneinander frei.

Nun tauschen wir $\xi_1, \ldots, \xi_{p-2}, \eta_p$ gegen $p-1$ der η; es muß dann wieder ein System aus voneinander freien Vektoren $\xi_1, \ldots, \xi_{p-2}, \eta_p, \eta_q$ entstehen,

[7]) B. L. VAN DER WAERDEN, Moderne Algebra I, 2. Auflage, 106.

so daß $p \neq q$. So fortfahrend ersetzen wir nacheinander alle $\mathfrak{x}$ durch $\mathfrak{y}$, wobei die Vektoren des Systems voneinander frei bleiben.

Bemerkung. Für den Fall $p \neq m$ ist noch nicht bewiesen, daß es unter den $\mathfrak{y}$ p voneinander freie Vektoren gibt; das wird in 2.2.6 nachgeholt.

2.1.8. Gibt es in einer Vektorspezies $\mathfrak{X}$ r voneinander freie Vektoren, von denen alle übrigen Elemente von $\mathfrak{X}$ linear abhängen, zo heißt r der *Rang* von $\mathfrak{X}$. Sind mehrere solche Basen aus voneinander freien Vektoren bekannt, so folgt aus dem Austauschsatz, daß sie alle aus gleichviel Elementen bestehen.

2.2. *Lineare Gleichungen ohne Determinanten.*

2.2.1. Wir betrachten m lineare Gleichungen in n Veränderlichen:

$$\mathfrak{a}_i \mathfrak{x} = b_i \qquad (i = 1, \ldots, m) \ldots\ldots\ldots (1)$$

oder

$$\sum_{\nu=1}^{n} a_{i\nu} x_\nu = b_i \qquad (i = 1, \ldots, m) \ldots\ldots\ldots (2)$$

Der Rang des Systems $(\mathfrak{a}_1, \ldots, \mathfrak{a}_m)$ sei bekannt und gleich r. Dann sind die Gleichungen lösbar mit Hilfe des Austauschsatzes, wie bei V. D. WAERDEN l.c., 2. Aufl. 109. Ich wiederhole diese Betrachtung, weil ich die darin vorkommenden Formeln weiterhin brauche. Zunächst wählen wir die Bezeichnung so, daß $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ voneinander frei sind und

$$\mathfrak{a}_i = \sum_{k=1}^{r} c_{ik} \mathfrak{a}_k \qquad (i = r+1, \ldots, m) \ldots\ldots\ldots (3)$$

Bedeuten $\mathfrak{e}_1, \ldots, \mathfrak{e}_n$ die n-dimensionalen Einheitsvektoren, so können wir wieder die Bezeichnung so wählen, daß nach dem Austauschsatz

$$\mathfrak{e}_1, \ldots, \mathfrak{e}_n \text{ äq. } \mathfrak{a}_1, \ldots, \mathfrak{a}_r, \mathfrak{e}_{r+1}, \ldots, \mathfrak{e}_n;$$

da die Einheitsvektoren offenbar voneinander frei sind, besteht auch das letzte System nach 2.1.7 aus voneinander freien Vektoren. Es sei

$$\mathfrak{e}_i = \sum_{k=1}^{r} d_{ik} \mathfrak{a}_k + \sum_{k=r+1}^{n} f_{ik} \mathfrak{e}_k \qquad (i = 1, \ldots, r) \ldots\ldots (4)$$

Durch Einsetzen von (3) und (4) in die Formeln $\Sigma a_{i\nu} \mathfrak{e}_\nu = \mathfrak{a}_i$ entsteht eine Identität in $\mathfrak{a}_1, \ldots, \mathfrak{a}_r, \mathfrak{e}_{r+1}, \ldots, \mathfrak{e}_n$, in welcher also alle Koeffizienten verschwinden. Hieraus folgt, daß durch Einsetzen von

$$b_i = \sum_{k=1}^{r} c_{ik} b_k \qquad (i = r+1, \ldots, m) \ldots\ldots\ldots (5)$$

und

$$x_i = \sum_{k=1}^{r} d_{ik} b_k + \sum_{k=r+1}^{n} f_{ik} x_k \qquad (i = 1, \ldots, r) \ldots\ldots (6)$$

in (2) eine Identität in $b_1, \ldots, b_r, x_{r+1}, \ldots, x_n$ entsteht, anders gesagt, wenn $b_1, \ldots, b_m$ den Relationen (5) genügen, so ist (6) für beliebige $x_{r+1}, \ldots, x_n$ eine Lösung von (1).

2.2.2. Bedeutet $\mathbf{a}_\nu$ den m-dimensionalen Vektor $(a_{1\nu}, \ldots, a_{m\nu})$, so sagen die Lösbarkeitsbedingungen (5) aus, daß der Vektor $\mathbf{b}$ von dem System

$$\mathbf{G}\begin{cases}(1, 0, \ldots, 0, c_{r+1,1}, \ldots, c_{m1})\\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\\ (0, \ldots, 0, 1, c_{r+1,r}, \ldots, c_{mr})\end{cases}$$

abhängig ist. $\mathbf{G}$ ist also äquivalent mit $(\mathbf{a}_1, \ldots, \mathbf{a}_n)$. Nennen wir ein System, das durch Indizesvertauschung die Gestalt von $\mathbf{G}$ erhalten kann, *kanonisch*, so haben wir den

SATZ. Hat das Vektorsystem $(\mathfrak{a}_1, \ldots, \mathfrak{a}_m)$ den Rang r, so ist das *transponierte* System $(\mathbf{a}_1, \ldots, \mathbf{a}_n)$ einem kanonischen System aus r Vektoren äquivalent.

2.2.3. Nach 2.1.4 ist jeder von $\mathbf{G}$ freier Vektor $\mathbf{h}$ auch von $(\mathbf{a}_1, \ldots, \mathbf{a}_n)$ frei, d.h. für jedes $\mathfrak{x}$ ist wenigstens ein $\mathfrak{a}_i \mathfrak{x} \not\equiv h_i$. In diesem Sinn sind die Lösbarkeitsbedingungen *verschärft notwendig*.

2.2.4. Die Lösung (6) ist in dem folgenden verschärften Sinn vollständig: Ist ein Vektor $\mathfrak{y}$ von jedem in (6) enthaltenen Lösungsvektor entfernt, so ist für wenigstens einen Index i $\Sigma a_{ik} y_k \not\equiv b_i$.[8])

Beweis. Wir halten $y_{r+1}, \ldots, y_n$ fest und bestimmen nach (6) die zugehörige Lösung $z_1, \ldots, z_r, y_{r+1}, \ldots, y_n$. Nach Voraussetzung ist wenigstens ein $y_i \not\equiv z_i$. Nach (4) ist

$$y_i = \sum_{k=1}^{r} d_{ik}\, \mathfrak{a}_k\, \mathfrak{y} + \sum_{k=r+1}^{n} f_{ik}\, y_k;$$

$$z_i = \sum_{k=1}^{r} d_{ik}\, b_k + \sum_{k=r+1}^{n} f_{ik}\, y_k \qquad \text{(nach Definition)};$$

also folgt aus $y_i \not\equiv z_i$, daß für wenigstens einen Index k gilt $\mathfrak{a}_k \mathfrak{y} \not\equiv b_k$.

Homogene Gleichungen.

2.2.5. Das (1) entsprechende homogene System ($\mathbf{b} = 0$) sei (1*). Das System aller Lösungen von (1*) ist nach (6) äquivalent dem kanonischen System

$$\mathfrak{F}\begin{cases}(f_{1,r+1}, \ldots, f_{r,r+1}, 1, 0, \ldots, 0)\\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\\ (f_{1n}, \quad \ldots, f_{rn}, \quad 0, \ldots, 0, 1).\end{cases}$$

---

[8]) Daß aus dieser verschärften Vollständigkeit die Vollständigkeit im gewöhnlichen Sinn folgt, beweisen wir erst (mit einer Einschränkung) in 2.2.9.

Diese Lösungen zeigen uns $\mathfrak{a}_{r+1}, \ldots, \mathfrak{a}_n$ als abhängig von $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$. Jeder von 0 entfernte Vektor $\mathfrak{y}$ mit $y_\nu = 0$ für $\nu = r+1, \ldots, n$ ist von $\mathfrak{F}$ frei und macht also nach 2.2.4 wenigstens ein $\mathfrak{a}_k\,\mathfrak{y} \neq 0$; d.h., $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ sind voneinander frei. Es folgt:

SATZ. Hat ein endliches Vektorsystem den Rang r, so hat auch das transponierte System den Rang r.

Über den Rang von Vektorsystemen.

2.2.6. Mit Hilfe von 2.2.2 leiten wir hieraus ab, daß jedes Vektorsystem vom Rang r einem kanonischen System aus r Vektoren äquivalent ist. Umgekehrt gilt:

SATZ. Ist das kanonische System $(\mathfrak{y}_1, \ldots, \mathfrak{y}_r)$ abhängig von $(\mathfrak{x}_1, \ldots, \mathfrak{x}_n)$, so gibt es in diesem System r voneinander freie Vektoren.

Beweis. Wir wählen die Bezeichnung so, daß das kanonische System folgende Gestalt hat:

$$\begin{aligned}
\mathfrak{y}_1 &= (1, 0, \ldots, 0, y_{1,r+1}, \ldots, y_{1n}) \\
&\cdots\cdots\cdots\cdots \\
\mathfrak{y}_r &= (0, \ldots, 0, 1, y_{r,r+1}, \ldots, y_{rn}).
\end{aligned}$$

$$\mathfrak{y}_l = \sum_{k=1}^{n} a_{lk}\,\mathfrak{x}_k.$$

Durch einen Strich bezeichnen wir den Vektor, der aus den ersten r Komponenten eines gegebenen Vektors besteht; das transponierte System von $(\mathfrak{x}_1', \ldots, \mathfrak{x}_n')$ sei $(\mathfrak{x}_1', \ldots, \mathfrak{x}_r')$. Die $\mathfrak{y}_l'$ sind r-dimensionale Einheitsvektoren; $y_{ll} = 1$; $y_{lk} = 0$ für $i \neq k$. Nun betrachten wir den n-dimensionalen Vektor

$$\mathfrak{z} = \sum_{l=1}^{r} c_l\,\mathfrak{x}_l', \text{ also } z_\mu = \sum_{l=1}^{r} c_l\,x_{\mu l};$$

Dann ist $\sum_{k=1}^{r} c_k\,y_{lk} = \sum_{k=1}^{r} \sum_{\nu=1}^{n} c_k\,a_{l\nu}\,x_{\nu k}$;

$$c_l = \sum_{\nu=1}^{r} a_{l\nu}\,z_\nu.$$

Ist nun wenigstens ein c_l von 0 entfernt, so ist wenigstens ein z_ν von 0 entfernt; also sind $\mathfrak{x}_1', \ldots, \mathfrak{x}_r'$ voneinander frei. Dann hat auch das transponierte System $\mathfrak{x}_1', \ldots, \mathfrak{x}_n'$ den Rang r; sind z.B. $\mathfrak{x}_1', \ldots, \mathfrak{x}_r'$ voneinander frei, so gilt das Gleiche von $\mathfrak{x}_1, \ldots, \mathfrak{x}_r$.

2.2.7. SATZ. Sind die Vektoren $\mathfrak{x}_1, \ldots, \mathfrak{x}_n$ voneinander frei und kann $\mathfrak{y}$ nicht von ihnen frei sein, so ist $\mathfrak{y}$ von ihnen abhängig.

Beweis. Nach 2.2.6 ist das System der $\mathfrak{x}$ einem kanonischen System äquivalent, das wir so schreiben:

$$\begin{aligned}
\mathfrak{z}_1 &= (1, 0, \ldots, 0, \ldots) \\
&\cdots\cdots\cdots \\
\mathfrak{z}_n &= (0, 0, \ldots, 1, \ldots).
\end{aligned}$$

Nun beweisen wir zunächst: Ist $\mathfrak{y} \not\equiv \sum_{l=1}^{n} y_l \mathfrak{z}_l$, so ist $\mathfrak{y}$ von den $\mathfrak{z}$ frei. Gilt nämlich diese Relation, so hat man für beliebige c_l entweder $\mathfrak{y} \not\equiv \sum_{l=1}^{n} c_l \mathfrak{z}_l$, oder für wenigstens einen Index i ist $c_l \not\equiv y_l$. In diesem Fall ist wegen $1 \leqq i \leqq n$, $c_l = \sum_{k=1}^{n} c_k z_{kl}$, also $y_l \not\equiv \sum_{k=1}^{n} c_k z_{kl}$, d.h. wieder $\mathfrak{y} \not\equiv \Sigma c_k \mathfrak{z}_k$.

Da nun $\mathfrak{y}$ nicht von den $\mathfrak{z}$ frei sein kann, ist $\mathfrak{y} \not\equiv \Sigma y_l \mathfrak{z}_l$ unmöglich, also $\mathfrak{y} = \Sigma y_l \mathfrak{z}_l$.

2.2.8. SATZ. Sind die Vektorsysteme $\mathfrak{A}$ und $\mathfrak{B}$ äquivalent und hat $\mathfrak{A}$ den Rang r, so hat $\mathfrak{B}$ den Rang r.

Beweis. Nach 2.2.6 ist $\mathfrak{A}$ einem kanonischen System aus r Vektoren äquivalent; dann enthält $\mathfrak{B}$ r voneinander freie Vektoren, die ein System $\mathfrak{B}'$ bilden. Wäre nun ein Vektor $\mathfrak{b}$ aus $\mathfrak{B}$ von $\mathfrak{B}'$ frei, so würde $\mathfrak{B}'$ mit $\mathfrak{b}$ ein System von $n+1$ voneinander freien Vektoren bilden (2.1.3); dann müßte auch $\mathfrak{A}$ $n+1$ voneinander freie Vektoren enthalten, was nicht geht. Folglich kann $\mathfrak{b}$ nicht frei von $\mathfrak{B}'$ sein und ist $\mathfrak{b}$ von $\mathfrak{B}'$ abhängig.

2.2.9. Diese Resultate über Vektorsysteme gestatten viele Anwendungen auf die Theorie der Gleichungen.

SATZ 1. Besitzt ein System von m homogenen linearen Gleichungen in n Veränderlichen ein scharf-vollständiges Lösungssystem vom Rang s, so hat das Gleichungssystem den Rang $r = n - s$.

Beweis. Das Lösungssystem ist einem kanonischen System aus s Vektoren äquivalent; wie unter 2.2.5 folgt hieraus, daß das Vektorsystem $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ den Rang r hat, also auch das System $\alpha_1, \ldots, \alpha_m$.

SATZ 2. Ein scharf-vollständiges Lösungssystem von (1), dessen Rang bekannt ist, ist auch vollständig in dem gewöhnlichen Sinn, nämlich, daß es jede vorgelegte Lösung enthält.

Beweis. Unmittelbar aus 2.2.7.

SATZ 3. Diejenigen m-dimensionalen Vektoren, die als rechte Seiten von (1) die Gleichungen lösbar machen, bilden eine Spezies **B**. Hat **B** den Rang r, so hat auch das System $(\alpha_1, \ldots, \alpha_m)$ den Rang r.

Beweis. **B** ist dem transponierten System $(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ äquivalent, so daß dieses den Rang r hat; dann hat auch das erste System den Rang r.

2.3. *Anwendung der Determinantentheorie.*

2.3.1. Ist in der Matrix M jede $(r+1)$-reihige Unterdeterminante gleich 0, aber die r-reihige Unterdeterminante D von 0 entfernt, so ist r der *Rang* und D eine *Hauptdeterminante* von M.

Hauptzweck der folgenden Betrachtungen ist, zu zeigen, daß dieser „Matrixrang" gleich dem früher definierten Vektorrang ist.

2.3.2. Ist die Koeffizientendeterminante A der Gleichungen

$$\sum_{k=1}^{n} a_{ik} x_k = b_k \qquad (i = 1, \ldots, n) \quad . \quad . \quad . \quad . \quad . \quad . \quad (7)$$

von 0 entfernt, so lassen die Gleichungen sich eindeutig lösen nach der Cramerschen Regel.

$$x_k = \frac{A^{(k)}}{A}, \quad \ldots\ldots\ldots\ldots \quad (8)$$

wo die $A^{(k)}$ die bekannte Bedeutung haben. Fügt man zu (7) weitere Gleichungen hinzu, doch so, daß die durch die Spalte der b ergänzte Koeffizientenmatrix den Rang n hat, so genügt (8) auch dem erweiterten System.

2.3.3. Die Eindeutigkeit gilt auch in verschärftem Sinn: Ist $\mathfrak{y}$ ein von dem Vektor (8) freier Vektor, so ist wenigstens ein $\mathfrak{a}_l\,\mathfrak{y} \neq b_l$.

Beweis. Ist z.B. $y_h \neq \frac{A^{(h)}}{A}$, und sind A_{lk} die Minoren von A, so folgt aus $\sum_{l=1}^{n} A_{lh}\,\mathfrak{a}_l\,\mathfrak{y} = Ay_h \neq A^{(h)} = \sum_{l=1}^{n} A_{lh}\,b_l$ nach 1.4.2 und 1.5.1 die Behauptung.

2.3.4. Hat die Koeffizientenmatrix des Systems (1) den Rang r auch nach Ergänzung mit der Spalte der b, und ist z.B. die aus den ersten r Zeilen und Spalten gebildete Unterdeterminante eine Hauptdeterminante, so bringen wir die Glieder mit $x_{r+1}, \ldots, x_n$ nach rechts hinüber; das Verfahren, das auch zu der Cramerschen Regel führt, ergibt hier die Lösung in der Form

$$x_l = \sum_{k=1}^{r} D_{lk}\,b_k + \sum_{k=r+1}^{n} E_{lk}\,x_k \qquad (i = 1, \ldots, r), \quad \ldots \quad (9)$$

und ähnlich wie unter 2.2.4 erweist sich diese Lösung als scharfvollständig.

Nach 2.2.9 folgt hieraus ferner (bei Betrachtung des homogenen Systems (1*): Hat die Koeffizientenmatrix von (1*) den Rang r, so hat auch das System selber den Rang r.

2.3.5. Die Umkehrung muß besonders bewiesen werden, denn hat das System (1*) den Rang r, so ist nicht selbstverständlich, daß man in der Koeffizientenmatrix eine Hauptdeterminante nachweisen kann. Wir betrachten zunächst einen Sonderfall:

SATZ. Hat das System (1*) den Rang n, so hat auch die Koeffizientenmatrix M den Rang n.

Beweis. Nach 2.2.4 folgt aus der Voraussetzung, daß es für jeden von 0 entfernten Vektor $\mathfrak{y}$ einen Index i gibt, so daß $\mathfrak{a}_l\,\mathfrak{y} \neq 0$. Nun wenden wir vollständige Induktion nach n an. Der Satz ist nämlich trivial für m Gleichungen in einer Unbekannten, denn aus $a_{l1}\,x_1 \neq 0$ folgt sofort $a_{l1} \neq 0$. Wir nehmen an, daß er für m Gleichungen mit $n-1$ Unbekannten bewiesen ist, und zeigen, daß er dann auch für (1*) gilt. Betrachten wir speziell diejenigen von 0 entfernten Vektoren $\mathfrak{x}$, in welchen $x_n = 0$, so sehen wir, daß das Gleichungssystem, welches aus (1*) hervorgeht, indem wir $x_n = 0$ setzen, die Eigenschaft besitzt, daß für jeden von 0 entfernten $(n-1)$-dimensionalen Vektor wenigstens ein linkes Glied von 0 entfernt

ist; nach der soeben gemachten Voraussetzung folgt hieraus, daß eine $(n-1)$-reihige Determinante aus den ersten $n-1$ Spalten von M von 0 entfernt ist. Wir permutieren die Gleichungen so, daß die Zeilen dieser Determinante zu den ersten $n-1$ Gleichungen gehören, und bezeichnen mit A_i die $(n-1)$-reihige Determinante, die aus der Koeffizientenmatrix dieser $n-1$ Gleichungen durch Streichen der $i$ten Kolonne entsteht; dann ist $A_n \neq 0$. Für den Vektor $\mathfrak{y}$ mit $y_i = (-1)^i A_i$ ist $\mathfrak{a}_1 \mathfrak{y} = \ldots = \mathfrak{a}_{n-1} \mathfrak{y} = 0$, also ist $\mathfrak{a}_k \mathfrak{y} \neq 0$ für ein $k \geq n$; dieses $\mathfrak{a}_k \mathfrak{y}$ ist aber gleich einer n-reihigen Determinante aus M.

2.3.6. *Bemerkung.* Aus dem Beweis geht hervor, daß der Satz in folgender Fassung auch gilt, wenn statt eines Körpers ein *Integritätsbereich* zugrunde gelegt wird: [9])

SATZ. Gibt es zu jedem von 0 entfernten Vektor $\mathfrak{y}$ einen Index i, so daß $\mathfrak{a}_i \mathfrak{y} \neq 0$, so ist wenigstens eine n-reihige Determinante aus M von 0 entfernt.

2.3.7. Aus 2.3.4 und 2.3.5 folgt: Die notwendige und hinreichende Bedingung, dafür daß r Vektoren voneinander frei sind, lautet, daß ihre Komponentenmatrix den Rang r hat.

2.3.8. Die allgemeine Umkehrung von 2.3.4 ist in den beiden folgenden Sätzen enthalten.

SATZ. Hat das System (1*) $n-r$ voneinander freie Lösungen, so ist jede $(r+1)$-reihige Determinante aus ihrer Koeffizientenmatrix gleich 0.

Beweis. Der Satz ist trivial für $r = n$. Er sei bewiesen für $r > s$; hat nun (1*) $n-s$ voneinander freie Lösungen, so hat es auch $n-(s+1)$ solche; folglich ist dann jede $(s+2)$-reihige Koeffizientendeterminante gleich 0. Wäre nun eine $(s+1)$-reihige Determinante von 0 entfernt, so wäre der Rang der Matrix gleich $s+1$, und (1*) hätte ein scharf-vollständiges System von $n-s-1$ voneinander freien Lösungen, was nach 2.2.6 der Annahme von $n-s$ voneinander freien Lösungen widerspricht.

SATZ. Ist das System von $n-r$ voneinander freien Lösungen von (1*) scharf-vollständig, so ist der Rang der Koeffizientenmatrix gleich r.

Beweis. Die gegebene Lösungsgesamtheit ist nach 2.2.6 äquivalent einem kanonischen System aus r Vektoren, so daß z.B. $x_1, \ldots, x_r$ homogen und linear durch die übrigen ausgedrückt sind. Jeder von 0 entfernte Vektor, für welchen $x_{r+1} = \ldots = x_n = 0$, ist also von den gegebenen Lösungen frei. Hierdurch ist der Satz auf 2.3.5 zurückgeführt.

2.3.9. Aus 2.2.5 und 2.3.8 folgt nun: Ist der Vektorrang von (1*) gleich r, so ist auch der Matrixrang gleich r.

2.4. *Bemerkungen und Zusätze.*

2.4.1. Der Wert der Determinantentheorie muß vom intuitionistischen Standpunkt höher eingeschätzt werden als sonst. Um nämlich die Ab-

---

[9]) Die ganze Theorie der homogenen linearen Gleichungen ließe sich über einem Integritätsbereich entwickeln.

hängigkeit von m Vektoren nach der Definition 2.1.2 zu prüfen, müßte man grundsätzlich alle Systeme $c_1, \ldots, c_m$ durchlaufen; die Determinantentheorie führt nun diese Entscheidung auf die Berechnung von endlich vielen Zahlen, den Unterdeterminanten der Komponentenmatrix, zurück.

Als Beispiel diene die folgende Betrachtung.

SATZ. Ist in der Determinante $A = |a_{ik}|$ ein r-reihiger Minor $A^{(r)}$ und ein $(r+1)$-reihiger Minor $A^{(r+1)}$ von 0 entfernt, so ist auch wenigstens ein $(r+1)$-reihiger Minor, der A enthält, von 0 entfernt. (Verschärfung eines bekannten Determinantensatzes.)

Beweis. $A^{(r)}$ sei aus den ersten r Zeilen und den ersten r Spalten von A gebildet. In der Matrix der ersten r Spalten von A sind nach 2.3.2 die letzten $n-r$ Zeilen homogene lineare Kombinationen der ersten r Reihen:

$$a_{ik} = \sum_{m=1}^{r} c_{im}\, a_{mk} \qquad (i = r+1, \ldots, n;\ k = 1, \ldots, r).$$

Setzen wir nun für $k = r+1, \ldots, n$

$$\Sigma\, c_{im}\, a_{mk} = a'_{ik},$$

und ersetzen wir in $A^{(r+1)}$ die a durch die a', so ist die entstandene Determinante gleich 0. Nach 1.5.5 gibt es nun Indices μ, ν, so daß $a'_{\mu\nu} \# a_{\mu\nu}$. Die Determinante, welche aus $A^{(r)}$ durch Hinzufügung der μ-ten Reihe und der ν-ten Kolonne entsteht, ist von 0 entfernt.

Hieraus folgt nun sofort: Sind die Vektoren $\mathfrak{x}^{(1)}, \ldots, \mathfrak{x}^{(r)}$ von einander frei und die Vektoren $\mathfrak{y}^{(1)}, \ldots, \mathfrak{y}^{(r+1)}$ voneinander frei, so ist wenigstens ein $\mathfrak{y}^{(i)}$ frei von den $\mathfrak{x}^{(k)}$.

Die Bedingung, daß $\mathfrak{x}^{(1)}, \ldots, \mathfrak{x}^{(r)}$ voneinander frei sind, ist wesentlich. Ist z.B. $n = 3$, $r = 2$, $\mathfrak{x}^{(1)} = (0,0,1)$, $\mathfrak{x}^{(2)} = (a, b, 1)$, wo a und b reelle Zahlen bedeuten, von denen nicht bekannt ist, ob sie gleich 0 sind oder nicht, während auch über ihr Verhältnis nichts bekannt ist, so muß für jeden Vektor $\mathfrak{y}$ die Möglichkeit offengelassen werden, daß er von $\mathfrak{x}^{(1)}$ und $\mathfrak{x}^{(2)}$ abhängig ist.

2.4.2. Neben der oben entwickelten positiven Theorie ließe sich eine negative, auf dem Begriff der Unabhängigkeit gegründete, Theorie der linearen Gleichungen entwickeln. Auf die Darstellung dieser Theorie wird hier verzichtet.

2.4.3. Als Sonderfall von 2.3.8 haben wir: Besitzt das System (1*) eine von 0 entfernte Lösung, so ist jede n-reihige Koeffizientendeterminante gleich 0. Die Umkehrung gilt nicht allgemein. Als Gegenbeispiel genügt schon die zweimal gezählte Gleichung $ax + by = 0$, wo die reellen Zahlen a und b wie folgt definiert werden: a ist der Limes der Folge a_i; $a_i = 2^{-i}$, wenn unter den ersten i Dezimalen in der Entwicklung von π keine drei aufeinanderfolgenden 7 vorkommen, aber $a_i = 2^{-k}$, wenn dieses wohl der Fall ist, und k ($\leq i$) die Rangnummer der letzten 7 aus der ersten Folge von drei 7 ist; b wird in analoger Weise definiert mit 8 statt 7. Weder von a noch von b wissen wir ob es gleich null ist oder nicht. Ist eines von beiden

von 0 entfernt, so genügt $x = pb$, $y = -pa$ ($p \neq 0$) der Gleichung und diese Lösung bildet ein scharf-vollständiges Lösungssystem; ist aber $a = b = 0$, so ist diese Lösung trivial, es genügt nun jeder beliebige von 0 entfernte Vektor. Da wir nicht wissen, welcher Fall vorliegt, sind wir nicht imstande, auch nur eine von 0 entfernte Lösung wirklich zu bestimmen.

2.4.4. Wir können das Resultat aus 2.2.5 so formulieren: Das System (1*) besitzt eine von 0 entfernte Lösung, wenn der Rang bekannt und kleiner als n ist. In besonderen Fällen kann es aber zuweilen gelingen, eine von 0 entfernte Lösung zu bestimmen, auch wenn der Rang unbekannt ist. So hat die Gleichung $ax + ay = 0$, wo a wie in 2.4.3 definiert ist, immer die von 0 entfernte Lösung $(1, -1)$, während der Rang 0 oder 1 sein kann, je nachdem $a = 0$ oder $a \neq 0$.

2.4.5. Das folgende Resultat ist etwas schwächer als 2.2.5, aber oft nützlich.

SATZ. Ist jede n-reihige Determinante aus der Koeffizientenmatrix M von (1*) gleich 0, so ist es ausgeschlossen, daß es keine von 0 entfernte Lösung von (1*) gibt.

Beweis. Angenommen, es sei $M = 0$ und es könne keine von 0 entfernte Lösung von (1*) geben. Dann kann der Rang von M nicht $n-1$ sein, weil es sonst nach 2.2.5 eine von 0 entfernte Lösung gäbe; also sind alle $(n-1)$-reihigen Unterdeterminanten von M gleich 0. Nun ergibt sich ebenso, daß alle $(n-2)$-reihigen Unterdeterminanten gleich 0 sind, usw. Schließlich müßten alle Koeffizienten gleich 0 sein; dann hat das System aber gewiß eine von 0 entfernte Lösung. Das ist der erwünschte Widerspruch.

§ 3. Polynome.

3.1.1. *Definitionen.* Es seien f, g, h Polynome in einer Veränderlichen x über ein einem Körper K. Wir sagen, daß $f \equiv g\ (h)$, wenn ein Polynom k bestimmt werden kann, so daß $f - g = kh$.

$f \not\equiv g\ (h)$, wenn für jedes Polynom k gilt $f - g \neq kh$.

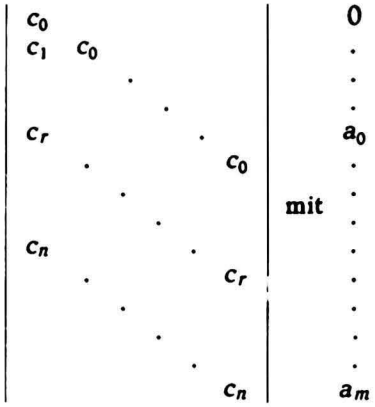
3.1.2. Für die Teilbarkeit von f durch h ($f \equiv 0\ (h)$) ergibt die gewöhnliche Division ein algebraisches Kriterium, falls h regulär ist (1.7.1): Ist $f = qh + r$, wo r von niedrigerem Grad als h ist, so ist $f \equiv 0\ (h)$ gleichbedeutend mit $r = 0$ und $f \not\equiv 0\ (h)$ gleichbedeutend mit $r \neq 0$. Er läßt sich auch für jedes vorgegebene von 0 entfernte, aber nicht notwendig reguläre h die Entscheidung über die Teilbarkeit von f durch h auf die Berechnung von endlich vielen Körperelementen zurückführen. Es sei

$$f = a_0 x^m + a_1 x^{m-1} \ldots + a_m;$$

$$h = c_0 x^n + c_1 x^{n-1} \ldots + c_n; \qquad c_r \neq 0.$$

Die Gleichung $f = kh$, wo k ein Polynom $(m - n + r)$-ten Grades (1.7.3) mit unbestimmten Koeffizienten p_i ist, führt zu einem System von

linearen Gleichungen in den p_i, deren Koeffizientenmatrix die Form hat:



Nun ist entweder die Unterdeterminante D_r, deren Hauptdiagonale aus c_r besteht, von 0 entfernt, oder wenigstens ein Element in dieser Determinante oberhalb der Hauptdiagonale ist von 0 entfernt. Schließlich geraten wir immer zu einer von 0 entfernten Unterdeterminante; ich nehme an, daß $D_r \not\equiv 0$. Notwendig und hinreichend, damit $f \equiv 0\ (h)$, ist nun, daß aus der mit der Spalte der a erweiterten Matrix alle $(m-n+r+2)$-reihigen Determinanten E_s gleich 0 sind; notwendig und hinreichend, damit $f \not\equiv 0\ (h)$ ist, daß wenigstens eine dieser Determinanten von 0 entfernt ist.

3.1.3. Als Anwendung beweisen wir den

SATZ. Ist $h \not\equiv 0$ und $f \not\equiv 0\ (h)$, so ist für jedes Polynom k entweder $f \not\equiv 0\ (k)$ oder $h \not\equiv k$.

Beweis. Machen wir über h die obigen Voraussetzungen, so ist entweder in k der Koeffizient von x^{n-r} von 0 entfernt oder $h \not\equiv k$. Im ersten Fall bleibt $D_r \not\equiv 0$, wenn die Koeffizienten von h durch diejenigen von k ersetzt werden, oder $h \not\equiv k$. Bleibt $D_r \not\equiv 0$, so bleibt ein $E_s \not\equiv 0$, oder $h \not\equiv k$.

3.1.4. SATZ. Ist $h \not\equiv 0$, und $f \not\equiv 0\ (h)$ ungereimt, so ist $f \equiv 0\ (h)$.

Beweis. Man bilde nach 3.1.2 die Determinanten $E_s(f)$; es ist ungereimt, daß ein $E_s(f) \not\equiv 0$, also ist jedes $E_s(f) = 0$.

3.1.5. SATZ. Ist $h \not\equiv 0$ und $f + g \not\equiv 0\ (h)$, so ist entweder $f \not\equiv 0\ (h)$ oder $g \not\equiv 0\ (h)$.

Beweis. Da die E_s linear sind in den Koeffizienten des Dividenden, ist $E_s(f+g) = E_s(f) + E_s(g)$; hieraus folgt der Satz sofort.

3.1.6. Den *Restklassenring* nach einem beliebigen Polynom h kann man in der gebräuchlichen Weise definieren. Ist $h \not\equiv 0$, so erhalten wir wie folgt eine *Entfernungsrelation* in dem Restklassenring:

Definition. Die Restklassen von f und g heißen *voneinander entfernt*, wenn $f \not\equiv g\ (h)$.

Es ist zu beweisen, daß bei dieser Definition 1.3.1, 1.4.1 und 1.5.1 gelten. 1.3.1, I ist klar. II und III folgen unmittelbar aus 3.1.4 und 3.1.5, denn ist $f-g \not\equiv 0\ (h)$ ungereimt, so gilt $f-g \equiv 0\ (h)$, und aus $f-g \not\equiv 0\ (h)$

folgt wegen $f-g=(f-k)+(k-g)$ entweder $f-k \not\equiv 0\ (h)$ oder $k-g \not\equiv 0\ (h)$.

1.4.1 ist klar. 1.5.1 sehen wir so ein: Es sei $fg \not\equiv 0\ (h)$; k sei ein beliebiges Polynom. Dann ist $fg \not\equiv kgh$. also nach 1.7.2 $f \not\equiv kh$. Ebenso ist $g \not\equiv 0\ (h)$.

3.2. *Teilbarkeit von Polynomen.*

3.2.1. Im folgenden bedeute f_i den Koeffizienten von x^i in dem Polynom f aus $K[x]$. f heißt *nichtkonstant*, wenn $f \neq f_0$; dann ist nicht jeder Koeffizient f_i aus f mit $i>0$ gleich Null; f ist von jeder Konstanten verschieden. f heißt *von Konstanten entfernt*, wenn $f \not\equiv f_0$; dann ist $f_i \not\equiv 0$ für wenigstens ein $i>0$.

3.2.2. *Definitionen.* f heißt *schwach teilbar*, wenn es nichtkonstante Polynome g und h gibt, so daß $f=gh$. f heißt (*stark*) *teilbar*, wenn es von Konstanten entfernte Polynome g und h gibt, so daß $f=gh$.

3.2.3. SATZ. Ist f nicht stark teilbar, so ist f nicht schwach teilbar.

Beweis: Ist f nicht stark teilbar, so gilt:

$$\text{Aus } g \not\equiv g_0 \text{ und } h \not\equiv h_0 \text{ folgt } f \neq gh.$$

Auf beide Seiten dieses Satzes wenden wir die doppelte Negation an; wir bedenken, daß die doppelte Negation einer Konjunktion äquivalent der Konjunktion der doppelten Negationen der Glieder ist und ersetzen rechts die driefache Negation durch eine einfache. So finden wir:

$$\text{Aus } g \neq g_0 \text{ und } h \neq h_0 \text{ folgt } f \neq gh,$$

das heißt, f ist nicht schwach teilbar.

Wir nennen in diesem Fall f *unteilbar*.

3.2.4. *Definition.* f heißt *prim*, wenn f entfernt ist von 0 und von jedem Produkt aus zwei Polynomen, die von Konstanten entfernt sind.

3.2.5. Die Definitionen und Sätze aus 3.2.1 bis 3.2.4 lassen sich ohne weiteres auf Polynome in mehreren Veränderlichen ausdehnen.

3.3.1. *Definition.* Die Polynome f und g heißen *relativ prim*, wenn für jedes von 0 entfernte Polynom h, dessen Minimalgrad größer als 0 ist, wenigstens eine der Relationen $f \not\equiv 0\ (h)$, $g \not\equiv 0\ (h)$ gilt.

3.3.2. SATZ. Sind die Polynome f und g relativ prim, ist ein Minimalgrad von f gleich $n>0$, und genügen die Polynome h und k den Bedingungen, daß entweder $h \not\equiv 0$ oder $k \not\equiv 0$ und daß der Maximalgrad von k kleiner als n ist, so ist $hf+kg \not\equiv 0$.

Beweis. Zunächst nehmen wir für k eine von 0 entfernte Konstante; dann ist $hf+kg \not\equiv 0$, denn aus $g \not\equiv 0\ (f)$ folgt $g \not\equiv -\frac{h}{k} f$. Nun sei der Satz schon bewiesen für jedes reguläre k, dessen Grad nicht größer als $p(<n)$ ist; dann gilt er auch für jedes k, dessen Maximalgrad gleich p ist. Denn schreiben wir $k=k_1+k_2$, wo k_2 entweder gleich 0 oder regulär

von geringerem Grad als p ist, so ist für beliebiges h $hf + k_2 g \not\equiv 0$, also entweder $hf + kg \not\equiv 0$ oder $k_1 \not\equiv 0$; in dem letzten Fall kann man die von 0 entfernten Glieder aus k_1 in k_2 hinüberbringen, und durch Wiederholung dieses Verfahrens gelangt man schließlich immer zu $hf + kg \not\equiv 0$.

Ist so der Satz bewiesen für jedes k, dessen Maximalgrad kleiner als q ist, und ist $q < n$, so zeigt die folgende Ableitung, daß er auch für jedes reguläre k mit dem Grad q gilt. Es sei h beliebig, $hf + kg = l$. Da k regulär ist, können wir f durch k dividieren: $f = ks + r$; der Maximalgrad von r ist kleiner als q. Nun folgt:

$$fg = ksg + rg = s(l - hf) + rg.$$
$$f(g + hs) - rg = sl.$$

Da f und g relativ prim sind und s (wegen $q < n$) von Konstanten entfernt, gilt entweder $f \not\equiv 0$ (s) oder $g \not\equiv 0$ (s), also entweder $r \not\equiv 0$ oder $g + hs \not\equiv 0$. Wir können also den Satz auf diesen Fall anwenden, so daß $sl \not\equiv 0$, also $l \not\equiv 0$.

Die angegebenen Schritte genügen, um durch Wiederholung den Induktionsbeweis zu vollenden.

3.3.3. SATZ. Ist f prim und $g \not\equiv 0$ (f), so sind f und g relativ prim.

Beweis. $g \not\equiv 0$ (cf) für jedes von 0 entfernte konstante c. Hieraus folgt, daß für ein von 0 entferntes Polynom h entweder gilt $g \not\equiv 0$ (h) oder $h \not\equiv cf$ für jedes konstante c. [Nämlich: a sei ein von 0 entfernter Koeffizient aus h, b der entsprechende Koeffizient aus f. $b \not\equiv 0$ oder $h \not\equiv cf$ für jedes c. Ist $b \not\equiv 0$, so ist $g \not\equiv 0$ $\left(\frac{b}{a} f\right)$, also $g \not\equiv 0$ (h) oder $h \not\equiv \frac{b}{a} f$; im letzten Fall gilt für konstantes c entweder $h \not\equiv cf$ oder $\frac{b}{a} \not\equiv c$, in diesem Fall ist wieder $h \not\equiv cf$.] Ist $h \not\equiv cf$ für jedes konstante c, so ist $f \not\equiv dh$ für jedes von 0 entfernte konstante d. Ist nun l ein zweites Polynom, so ist $f \not\equiv hl$, oder l ist von Konstanten entfernt; in diesem Fall gilt, da f prim ist, wieder $f \not\equiv hl$. Wir haben also gezeigt, daß entweder $g \not\equiv 0$ (h) oder $f \not\equiv 0$ (h).

3.3.4. SATZ. Ist f prim, so ist der Restklassenring nach f ein Integritätsgebiet.

Beweis. Es sei $g \not\equiv 0$ (f) und $h \not\equiv 0$ (f); es ist zu beweisen, daß $gh \not\equiv 0$ (f).

Da f nicht regulär zu sein braucht, setzen wir $f = f_1 + f_2$, wo f_2 regulär ist. Für beliebiges k sei $gh - kf = l$. Gewöhnliche Division ergibt $g = qf_2 + r$; nach 3.1.3 ist entweder $r \not\equiv 0$ oder $f_1 \not\equiv 0$. Im ersten Fall schließen wir auf

$$f(qh - k) + rh = l + qhf_1.$$

Nach 3.3.3, 3.3.2 ist das linke Glied von 0 entfernt, also $l \not\equiv 0$ oder $f_1 \not\equiv 0$. In diesem Fall kann man die von 0 entfernten Glieder aus f_1 nach f_2 hinüberbringen und dieses, wenn notwendig, wiederholen bis f_1 erschöpft ist. (Diese Methode, nicht notwendig reguläre Polynome zu behandeln, deuten wir im folgenden mit dem Schlagwort „Spaltung" an.)

3.3.5. SATZ. Ist f prim und regulär mit einem Grad > 0, so ist der Restklassenring nach f ein Körper.

Beweis. Es sei n der Grad von f, g ein von 0 entferntes Polynom von dem Maximalgrad m, so daß $g \not\equiv 0 \ (f)$. In $hf + kg = 0$ setzen wir für h, k bzw. Polynome von den Graden $m - 1$, $n - 1$ an; es ergeben sich für die Koeffizienten von h und k homogene lineare Gleichungen, deren Koeffizientendeterminante nach 3.3.2 und 2.2.5, 2.3.5 von 0 entfernt ist. Nach 2.3.2 ist dann $hf + kg = 1$ lösbar; d.h. g hat in dem Restklassenring das inverse Element k. — Nach 1.7.2 ist $1 \not\equiv 0 \ (f)$.

3.3.6. Einem Körper kann also eine Wurzel eines regulären Primpolynoms formal adjungiert werden. Leider gelingt es nicht immer, auch eine zweite Wurzel zu adjungieren.

Als Beispiel diene $f(x) = x^3 + ax + y$; a bedeutet eine reelle Zahl, von der nicht bekannt ist, ob sie gleich Null ist oder nicht. Ist K der Körper der komplexen Zahlen, so ist f prim über $K(y)$. Sei w eine Wurzel von f, also $f = (x - w)(x^2 + wx + w^2 + a)$. Ist $a = 0$, so zerfällt f vollständig in $K(y, w) = K(w)$; ist $a \not\equiv 0$, so ist der zweite Faktor prim über $K(w)$.

3.3.7. SATZ. (Umkehrung von 3.3.4) Ist der Restklassenring nach f ein Integritätsgebiet, so ist f prim.

Beweis. Es sei $f = f_1 + f_2$; f_2 regulär mit dem Grad n; g und h seien regulär und von Konstanten entfernt. Hat g oder h einen höheren Grad als n, so ist $gh \not\equiv f_2$, also $gh \not\equiv f$ oder $f_1 \not\equiv 0$; in diesem Fall bringen wir die von 0 entfernten Glieder aus f_1 nach f_2 hinüber und wiederholen den Prozeß, bis sich entweder ergibt daß $gh \not\equiv f$ oder daß ein Minimalgrad von f größer ist als die Grade von g und h. In diesem Fall ist $g \not\equiv 0 \ (f)$ und $h \not\equiv 0 \ (f)$, also nach der Definition des Integritätsgebiets $gh \not\equiv 0 \ (f)$, also sicher $gh \not\equiv f$. Von der Voraussetzung, daß g und h regulär sind, befreit man sich in einfacher Weise durch Spaltung.

3.4. *Transzendente Erweiterung des Grundkörpers.*

3.4.1. SATZ. Sind die Polynome $f(x)$ und $g(x)$ aus $K[x]$ relativ prim über K und ist t eine Unbestimmte, so sind f und g relativ prim über $K(t)$.

Beweis. Es ist zu beweisen, daß

$$h(t) \cdot f(x) \not\equiv k(x, t) \cdot l(x, t), \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (1)$$

oder die entsprechende Relation für g, wenn $h \not\equiv 0$ und der Minimalgrad von k und von l in x größer als 0 ist. Wir denken uns k und l nach Potenzen von t entwickelt; der Koeffizient von t^p in k sei k_p; entsprechend für l und h.

Erster Fall. k_0 hat einen Minimalgrad > 0 in x.

Es ist $f \not\equiv 0 \ (k_0)$ oder $g \not\equiv 0 \ (k_0)$; wir nehmen das erste an. Ferner sei $h_p \not\equiv 0$. Wir vergleichen

$$h_p f \text{ mit } k_0 l_p + \ldots + k_p l_0 . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (2)$$

Steht in (2) das Zeichen $\not\equiv$, so gilt (1). Nun ist $h_p f \not\equiv k_0 l_p$, also entweder (1) oder ein $l_q \not\equiv 0$ mit $q < p$. In diesem Fall betrachten wir (2) mit q statt p, nennen es (3) und finden, daß entweder (1) oder $h_q \not\equiv 0$ oder ein $l_r \not\equiv 0$ mit $r < q$. Ist aber $h_q \not\equiv 0$, so finden wir wie bei (2), daß ein solches $l_r \not\equiv 0$. Wir können dieses Verfahren fortsetzen, bis sich (1) herausstellt.

Zweiter Fall. k_p hat einen Minimalgrad > 0 $(p > 0)$. Es sei $f \not\equiv 0 \ (k_p)$.

Sei $h = h' t^p + h''$; h'' habe den Maximalgrad $p-1$; ebenso $k = k' t^p + k''$. Nach dem ersten Fall ist $h' f \not\equiv k' l$, also $(h' t^p + h'') f \not\equiv k' t^p l$, also (1) oder $k'' \not\equiv 0$. Wir nehmen letzteres an. Ist noch $k'' = k'''(t) + x k^{IV}(t)$, so können wir im Fall $k^{IV} \not\equiv 0$ p durch eine kleinere Zahl ersetzen, so daß wir annehmen dürfen $k''' \not\equiv 0$, z.B. $k'''_q \not\equiv 0$.

Hat l den Grad 0 in t, so ist $h_p f \not\equiv k_p l$, also (1). Wir wenden Induktion nach dem Grad von l in t an. r sei der Maximalgrad von l und der Satz sei für jedes l von niedrigerem Grad bewiesen, so daß insbesondere

$$(h - h_0) f \not\equiv k(l - l_0),$$

also entweder (1) oder $h_0 \not\equiv 0$ oder $l_0 \not\equiv 0$; aus $h_0 \not\equiv 0$ folgt aber entweder $h_0 f \not\equiv k_0 l_0$, also (1), oder $l_0 \not\equiv 0$; nur dieser Fall braucht noch untersucht zu werden. Wir vergleichen

$$h_q f \text{ mit } k_q l_0 + \ldots + k_0 l_q . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (4)$$

und finden, daß vier Fälle möglich sind: a) (1), b) $h_q \not\equiv 0$, c) $k'''_s \not\equiv 0$ mit $s < q$, d) $k^{IV} \not\equiv 0$, von denen nur b) weiter betrachtet werden muß. Es sei n ein Minimalgrad von f; betrachten wir in (4) die Glieder vom Grad n, so sehen wir, daß entweder (1) oder $k^{IV} \not\equiv 0$ oder l den Minimalgrad n in x hat. Im letzten Fall ist ein Minimalgrad von kl nach x größer als n, also entweder (1) oder f hat einen Minimalgrad größer als n.

In allen Fällen, die wir haben unterscheiden müssen, gerät man nach einer endlichen Anzahl von Schritten zu (1), womit der Satz bewiesen ist.

3.4.2. HILFSSATZ. Sind $f(x)$ und $g(x)$ relativ prim, ist ein Minimalgrad von f gleich $n > 0$, ist $k(x, y) = k_0 + k_1 y + \ldots + k_p y^p \not\equiv 0$ so beschaffen, daß $k \not\equiv 0$ und die Polynome in x $k_0, \ldots, k_{p-1}$ den Maximalgrad n besitzen, so ist $g^p k\left(x, -\frac{f}{g}\right) \not\equiv 0$.

Beweis. Für $p = 1$ folgt alles aus 3.3.2. Wir wenden vollständige Induktion nach p an. Ist zunächst $k_0 = 0$, also $k = y k'$, so ist $g^p k\left(x, -\frac{f}{g}\right) = f g^{p-1} k'\left(x, -\frac{f}{g}\right) \not\equiv 0$. Hieraus folgt, daß immer ent-

weder $g^p k\left(x, -\frac{f}{g}\right) \not\equiv 0$ oder $k_0 \not\equiv 0$. Nun wenden wir vollständige Induktion nach dem Grad von k_0 an. Es sei also $q < n$ und der Satz sei bewiesen für jedes k, in welchem k_0 einen Maximalgrad kleiner als q hat; wir setzen nun k_0 regulär von dem Grad q an. Es ist

$$g^p k\left(x, -\frac{f}{g}\right) = \begin{vmatrix} f & 0 & . & . & . & 0 & k_0 \\ g & f & & & & & k_1 \\ 0 & g & . & & & & k_2 \\ . & . & . & . & & & . \\ . & . & & . & . & & . \\ . & . & & & . & f & k_{p-1} \\ 0 & . & . & . & . & g & k_p \end{vmatrix}.$$

Division ergibt $f = k_0 s + r$; multiplizieren wir in der Determinante die letzte Kolonne mit s und subtrahieren wir von ihr die erste Kolonne, so erhalten wir $-r,\ k_1 s - g,\ k_2 s, \ldots, k_p s$. Es sei $k_1 s - g = f s_1 + r_1$; wir vermindern die letzte Kolonne um s_1 mal der zweiten, so daß wir $-r,\ r_1,\ k_2 s - s_1 g, \ldots, k_p s$ erhalten. So fortfahrend erreichen wir, daß

$$sg^p k\left(x, -\frac{f}{g}\right) = \begin{vmatrix} f & 0 & . & . & . & -r & \\ g & f & . & . & . & r_1 & \\ 0 & g & . & . & . & r_2 & \\ . & . & . & . & . & . & \\ . & . & . & . & . & . & \\ 0 & . & . & . & . & k_p s - g s_{p-1} & \end{vmatrix}.$$

Entweder $f \not\equiv 0\ (s)$ oder $g \not\equiv 0\ (s)$; $g = -s_1 f + k_1 s - r_1 = -s_1(k_0 s + r) + k_1 s - r_1 = (-k_0 s_1 + k_1)s - r s_1 - r_1$. Es folgt, daß entweder $r \not\equiv 0$ oder $r_1 \not\equiv 0$. Das Polynom in y, dessen Koeffizienten die letzte Kolonne bilden, erfüllt die Voraussetzungen des Satzes für k, überdies ist der Grad von r kleiner als q, so daß nach der Induktionsvoraussetzung die Determinante von 0 entfernt ist; dann ist auch $g^p k\left(x, -\frac{f}{g}\right) \not\equiv 0$.

Der Satz ist nun für alle k, in denen k_0 regulär vom Grad q oder von kleinerem Grad ist, bewiesen; durch Spaltung beweisen wir ihn für alle k, in denen ein Maximalgrad von k_0 gleich q ist. Der Induktionsschritt kann nun wiederholt werden.

Zusatz. Der Satz 3.4.2 gilt auch dann, wenn n ein Minimalgrad von g statt von f ist. Man zeigt das einfach durch die Substitution $y = \frac{1}{z}$.

3.4.3. SATZ. Sind $f(x)$ und $g(x)$ relativ prim über K, so ist $f + gy$, wo y transzendent ist in Bezug auf K, prim über $K(y)$.

Beweis. Es ist zu zeigen, daß

$$h(y)(f + gy) \not\equiv k(x, y)\, l(x, y), \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (1)$$

wenn sowohl in k als in l ein Glied von höherem als dem nullten Grad in x von 0 entfernt ist. Es sei n ein Minimalgrad von f oder von g; wir setzen

$k = k' + K$, $l = l' + L$, wo k' und l' diejenigen Glieder aus k und l enthalten, deren Grad in x kleiner als n ist. Ersetzen wir überall y durch $-\frac{f}{g}$, und schaffen wir die Nenner weg durch Multiplikation mit einer geeigneten Potenz von g, so wird nach 3.4.2 $k'l'$ zu einem von 0 entfernten Polynom in x, während $h.(f + gy)$ zu 0 wird; hieraus folgt, daß $h.(f + gy) \not\equiv k'l'$, also entweder (1) oder $K \not\equiv 0$ oder $L \not\equiv 0$. In den beiden letzten Fällen ist der Grad von kl nach x größer als n, also entweder (1) oder ein Minimalgrad von f oder von g ist $n' > n$. Dann wiederholen wir die Betrachtung für n' statt n, usw.

3.4.4. Für die Eliminationstheorie wäre es wichtig, 3.4.3 auf mehrere Polynome auszudehnen, z.B. wie folgt: Sind $f(x)$, $f_1(x)$, $f_2(x)$, ... relativ prim über K, so ist $f + y_1 f_1 + y_2 f_2 + \ldots$ prim über $K(y_1, y_2, \ldots)$. Der Beweis dieser Behauptung ist mir noch nicht gelungen.

§ 4. Elimination aus binären Gleichungen.

4.1. *Einleitende Bemerkungen.*

4.1.1. Gegeben sind die von 0 entfernten Polynome über einem Körper K

$$\left.\begin{aligned} f^{(m)}(x, y) &= a_0 x^m + a_1 x^{m-1} y + \ldots + a_m y^m; \\ g^{(n)}(x, y) &= b_0 x^n + b_1 x^{n-1} y + \ldots + b_n y^n. \end{aligned}\right\} \quad n \geqq m. \quad \ldots \quad (1)$$

Ein eingeklammerter oberer Index bei dem Namen eines Polynoms gebe immer den maximalen Grad dieses Polynoms an. In der Eliminationstheorie sucht man die Bedingung, dafür daß die Polynome (1) einen gemeinsamen Faktor über K besitzen, dessen Grad $\geqq 1$ ist. Nach der EULERschen Methode führt man diese Frage zurück auf die andere, wann es zwei von 0 entfernte Polynome $h^{(n-1)}$ und $k^{(m-1)}$ gibt, so daß $hf + kg = 0$. Wir können aber aus der Existenz dieser Gleichung nicht allgemein auf das Bestehen eines gemeinsamen Faktors der Polynome (1) schließen, denn dieser Schluß beruht auf der Möglichkeit und Eindeutigkeit der Zerlegung von Polynomen in Primfaktoren. Die Frage der Faktorzerlegung fordert eine ausführliche Untersuchung, aus der wir hier vorweg nehmen, daß man sicher nicht imstande ist, außer bei speziellen Voraussetzungen bezüglich K, jedes Polynom über K in Primfaktoren zu zerlegen. Nehmen wir z.B. für K den Körper $R(t)$, wo R der Körper der reellen Zahlen und t eine Veränderliche ist, und ist $f(x, y) = x^2 + a t y^2$, wo a eine reelle Zahl bedeutet, von der wir nicht wissen, ob sie gleich 0 ist oder nicht, so können wir f nicht in Primfaktoren zerlegen. Ist nämlich $a = 0$, so ist f zerlegbar; ist $a \not\equiv 0$, so ist f prim.

4.1.2. Man könnte noch versuchen, $h^{(n-1)}$ und $k^{(m-1)}$ durch ihren g.g.T. zu dividieren; sind die Quotienten $h^{(n-p)}$ und $k^{(m-p)}$, so muß f durch $k^{(m-p)}$ und g durch $h^{(n-p)}$ teilbar sein und ist der Quotient ein gemeinsamer Faktor vom Grad p. Der g.g.T. kann ohne Faktorzerlegung mit dem Euklidischen

Algorithmus bestimmt werden. Hier stößt man aber auf eine neue Schwierigkeit. Die Division durch ein Polynom kann nur dann ausgeführt werden, wenn der Divisor regulär ist im Sinn von 1.7.1 (Anfangskoeffizient von 0 entfernt). Nichts hindert, die Eliminationstheorie zunächst für reguläre Polynome f und g aufzustellen; auch in diesem Fall können aber im weiteren Verlauf der Rechnung nichtreguläre Polynome als Divisoren auftreten. Der Euklidische Algorithmus ist nur in diskreten Körpern, in denen jedes Polynom regulär ist, allgemein anwendbar.

Es zeigt sich, daß die Verhältnisse ähnlich sind wie in dem Fall der linearen Gleichungen: Wir können den gemeinsamen Faktor der Polynome f und g nur dann bestimmen, wenn der genaue Grad des g.g.T. mitbestimmt werden kann. Das ließe sich erreichen durch Heranziehen der bekannten bei der Erweiterung der EULERschen Eliminationsmethode auftretenden Bedingungen für die Existenz eines gemeinsamen Faktors gegebenen Grades; dieser Weg wäre aber ziemlich umständlich. Wir wählen deshalb den folgenden, der auf einer, in den Hauptzügen ebenfalls bekannten, Erweiterung der Sylvesterschen (dialytischen) Methode beruht.

4.2.1. Wir gehen aus von einer beliebigen Anzahl von nichthomogen geschriebenen Gleichungen:

$$f_1 \equiv a_0 x^{m_1} + \ldots + a_{m_1} = 0;$$
$$f_2 \equiv b_0 x^{m_2} + \ldots + b_{m_2} = 0;$$
$$f_3 \equiv c_0 x^{m_3} + \ldots + c_{m_3} = 0;$$
usw.

Vorausgesetzt wird, daß $m_1 \geq m_2 \geq m_3 \geq \ldots$, daß aus jeder Gleichung wenigstens ein Koeffizient von 0 entfernt ist, und daß aus wenigstens einer Gleichung der Anfangskoeffizient von 0 entfernt ist, also wenigstens ein f_ν regulär ist. Wir setzen $m_1 + m_2 = n$.

4.2.2. Wir bilden in bekannter Weise aus den Gleichungen 4.2.1 die dialytische Matrix M für den Grad $n-1$. (Man multipliziere jedes f nacheinander mit $1, x, \ldots, x^{n-m_l-1}$. M ist die Matrix aus den Koeffizienten aller dieser Polynome.) Der Rang von M sei r.

4.2.3. In dem Ideal $I = (f_1, f_2, f_3, \ldots)$ sei g ein Polynom dessen Grad $\leq n-1$, $g = A_1 f_1 + A_2 f_2 + \ldots + A_\nu f_\nu + \ldots$. Da f_ν regulär ist, kann man jedes A durch f_ν dividieren, und erhält so:

$$A_1 = q_1 f_\nu + r_1;\ A_2 = q_2 f_\nu + r_2, \ldots,$$
$$g = r_1 f_1 + r_2 f_2 + \ldots + (A_\nu + q_1 f_1 + q_2 f_2 + \ldots) f_\nu \ldots.$$

Da der Grad eines jeden $r_l < m_\nu$, haben alle Terme rechts außer dem νten einen Grad $\leq n-1$; da das gleiche für g gilt, hat nach 1.7.3 und 1.5.3 der Faktor von f_ν höchstens den Grad $n-1-m_\nu$. Jedes Polynom aus I, dessen Grad $\leq n-1$, läßt sich in der Form

$$B_1 f_1 + B_2 f_2 + B_3 f_3 + \ldots$$

darstellen, wo der Grad von B_l höchstens $n-1-m_l$ ist.

4.2.4. Hieraus folgt: bezeichnen wir die Elemente von M (4.2.2) mit a_{ik}, so besteht die notwendige und genügende Bedingung, dafür daß

$$g = p_0 x^{n-1} + \ldots + p_{n-1}$$

zu I gehöre, hierin, daß die Gleichungen

$$\Sigma a_{ik} q_k = p_i$$

eine gemeinsame Lösung nach den q_k (den Koeffizienten der B_h) besitzen; ist r der Rang von M, so gibt es nach 2.2.3 r voneinander freie Vektoren $(p_0^{(\nu)}, \ldots, p_{n-1}^{(\nu)})$ $(\nu = 1, \ldots, r)$ für welche das der Fall ist, und ist der Vektor $\mathfrak{s} = (s_0, \ldots, s_{n-1})$ von diesen r Vektoren frei, so gilt für beliebige q und wenigstens ein i $\Sigma a_{ik} q_k \not\equiv s_i$. Anders ausgedrückt: Die Menge der Polynome aus I vom Maximalgrad $n-1$ besitzt eine scharf vollständige lineare Basis aus r linear voneinander freien Polynomen.

4.2.5. Ist g' ein von 0 entferntes Polynom, dessen Maximalgrad kleiner als $n-r$ ist, so sind $g', xg', \ldots, x^r g'$ $r+1$ linear voneinander freie Polynome mit dem Maximalgrad $n-1$; folglich ist wenigstens eines dieser Polynome von I entfernt (2.4.1), z.B. sei $x^t g' \not\equiv 0$ (I). Dann gilt für ein beliebiges Polynom h aus I, $x^t g' \not\equiv x^t h$, also $g' \not\equiv h$. Hieraus folgt, daß jedes von 0 entfernte Polynom aus I den Minimalgrad $n-r$ besitzt. Das heißt, die Vektoren $(p_0^{(\nu)}, \ldots, p_{r-1}^{(\nu)})$ $(\nu = 1, \ldots, r)$ sind voneinander frei. Also ist jeder r-dimensionale Vektor linear aus ihnen kombinierbar, insbesondere $(0, \ldots, 0, 1)$. I enthält also ein Polynom d von dem genauen Grad $n-r$, und dieses Polynom ist eindeutig bestimmt.

4.2.6. Dividiert man $f_1, f_2, f_3, \ldots$ durch d, so sind alle Reste gleich 0, weil man sonst in I ein Polynom von kleinerem Maximalgrad als $n-r$ erhalten würde. d ist also gemeinsamer Teiler von $f_1, f_2, f_3, \ldots$. Es sei $f_i = e_i d$; ist $d = A_1 f_1 + A_2 f_2 + A_3 f_3 + \ldots$, so ist $1 = A_1 e_1 + A_2 e_2 + A_3 e_3 + \ldots$. Hieraus folgern wir, daß die e_ν relativ prim sind. Denn ist erstens h ein reguläres Polynom, dessen Grad > 0, so folgt aus der letzten Identität, daß wenigstens einer der Reste, welche bei Division der e_ν durch h entstehen, von 0 entfernt ist; ist zweitens h ein beliebiges Polynom, dessen Minimalgrad größer als 0 ist, so führt Spaltung zum Ziel.

4.2.7. *Zusammenfassung.* Wir haben nun folgendes bewiesen: Hat M den Rang r, so besitzen $f_1, f_2, f_3, \ldots$ einen eindeutig bestimmten gemeinsamen Teiler d vom Grad $n-r$. Die Quotienten der f_ν durch d sind relativ prim. I ist Hauptideal und fällt mit (d) zusammen. Gilt für ein Polynom g, daß $d \not\equiv 0$ (g), so gilt für wenigstens ein i $f_i \not\equiv 0$ (g). Als wichtigsten Sonderfall heben wir hervor:

SATZ A. Ist $M \not\equiv 0$, so sind die f_ν relativ prim.

SATZ B. Besitzen die f_ν einen von Konstanten entfernten gemeinsamen Teiler, so ist $M = 0$.

Beweis. Nach Satz A ist $M \not\equiv 0$ ausgeschlossen.

SATZ C. Ist $M = 0$, so ist es unmöglich, daß die f_ν keinen gemeinsamen Teiler mit einem Grad grösser als 0 besitzen.

Beweis. Wie für 2.4.5.

4.2.8. Wir schreiten nun zur Umkehrung des vorigen, zunächst für zwei Polynome.

SATZ D_1. Sind f_1, f_2 relativ prim und ist entweder f_1 oder f_2 regulär, so ist ihre Resultante (d.h. die nach 4.2.2 gebildete dialytische Matrix) von 0 entfernt. Der Beweis ergibt sich aus 3.3.2 und 2.3.5.

4.2.9. Sind f und g Polynome und ist f regulär vom Grad n, so sind die folgenden vier Eigenschaften äquivalent:

I. Die Resultante R von f und g ist von 0 entfernt.

II. Sind h und k Polynome mit $h \neq 0$ oder $k \neq 0$, und ist der Maximalgrad von k kleiner als n, so ist $hf + kg \neq 0$.

III. Das Ideal (f, g) enthält 1.

IV. f und g sind relativ prim.

In 4.2.6 ist nämlich bewiesen, daß aus III folgt IV; in 4.2.8, daß aus IV folgt I. Daß ferner aus I folgt III, und daß I mit II äquivalent ist, lehrt die Theorie der linearen Gleichungen.

4.2.10. SATZ. (Umkehrung von 4.2.7.) f_1 sei regulär vom Grad m_1 in x, f_2 habe den Maximalgrad m_2; $m_1 + m_2 = n$. Besitzen f_1 und f_2 den gemeinsamen Teiler g, der ein reguläres Polynom vom Grad $n - r$ ist und sind die Quotienten $\frac{f_1}{g} = e_1$, $\frac{f_2}{g} = e_2$ relativ prim, so hat die Resultante von f_1, f_2 den Rang r.

Beweis. Nach 4.2.8 ist $(e_1, e_2) = (1)$, also $(f_1, f_2) = (g)$; (g) enthält genau r voneinander freie Polynome vom Maximalgrad $n - 1$, nämlich $g, xg, \ldots, x^{r-1} g$, von denen jedes Polynom aus (g) mit dem Maximalgrad $n - 1$ linear abhängig ist. Dann geht aus 2.2.9, Satz 3, und 2.3.9 hervor, daß die Resultante den Rang r hat.

4.3. Hätten wir die unter 3.4.4 genannte Eigenschaft zur Verfügung, so könnten wir 4.2.8 und 4.2.10 unmittelbar auf mehrere Polynome ausdehnen. Solange der Satz nicht bewiesen ist, müssen wir uns auf den Fall beschränken, daß der Grundkörper algebraisch abgeschlossen ist.

4.3.1. In diesem Fall erhalten die Sätze A, B, C die folgende Form:

SATZ A_2. Ist $M \neq 0$, so ist für jedes ξ wenigstens ein $f_\mu(\xi) \neq 0$.

SATZ B_2. Besitzen die f_ν eine gemeinsame Wurzel, so ist $M = 0$.

SATZ C_2. Ist $M = 0$, so ist es unmöglich, daß die f_ν keine gemeinsame Wurzel besitzen.

Nun läßt sich der zugehörige Satz D_2 beweisen.

4.3.2. Vorher ist die Bemerkung nützlich, daß sich die ganze Eliminationstheorie, mit Einschluß des HILBERTschen Nullstellensatzes, ohne Schwierigkeit entwickeln läßt für den Körper der rationalen Zahlen als Grundkörper: diese Möglichkeit beruht auf der Eigenschaft, daß die

Spezies der algebraischen Zahlen diskret ist (BROUWER, Math. Ann. 83, 201—210, § 4).

4.3.3. Bezeichnungen wie in 4.2.1, 4.2.2. Die Wurzeln des regulären Polynoms f_ν seien $a_1, \ldots, a_{m_\nu}$.

Die Produkte $f_{k_1}(a_1) \ldots f_{k_{m_\nu}}(a_{m_\nu})$ nennen wir in irgendeiner Reihenfolge $P_1, P_2, \ldots$. Ist ein $P_\sigma \neq 0$, so ist für jedes a_l ein $f_{k_l}(a_l) \neq 0$; für eine beliebige Zahl ξ läßt sich nun entweder μ so bestimmen, daß $f_\mu(\xi) \neq 0$ oder $\xi \neq a_l$ für jedes i (1.5.6); in diesem Fall ist aber $f_\nu(\xi) \neq 0$. Nun seien $D_1, \ldots, D_h$ die Determinanten höchsten Grades aus M, geschrieben als Polynome in den a und den *Koeffizienten* der f (f_ν ausgenommen). Sind für spezielle Werte der Koeffizienten und Wurzeln $D_1 = \ldots = D_h = 0$, so führt die Annahme, daß ein $P_\sigma \neq 0$, wegen Satz C_2 zu einem Widerspruch, also sind alle $P_\sigma = 0$. Auf die D und P können wir den Nullstellensatz anwenden; das ergibt: $P_\sigma^{\varrho} \equiv 0\,(D_1, \ldots, D_h)$. (1)

Nun sei für jedes ξ ein $f_\mu(\xi) \neq 0$; dann läßt sich insbesondere zu jedem i ein k_l finden, so daß $f_{k_l}(a_l) \neq 0$;

$P_\sigma = \prod_l f_{k_l}(a_l) \neq 0$. Dann ist nach (1) wenigstens ein $D_l \neq 0$.

SATZ D_2. Ist unter den Voraussetzungen von 4.2.1 für jedes ξ aus dem algebraisch abgeschlossenen Grundkörper wenigstens ein $f(\xi) \neq 0$, so ist $M \neq 0$.

4.3.4. Es ist notwendig, uns von den seit 4.2.1 durchweg gemachten Voraussetzungen α) jedes $f_\mu \neq 0$, β) wenigstens ein f_ν regulär, zu befreien. Das ist sehr leicht für Satz A, weil β) schon aus der Voraussetzung $M \neq 0$ folgt; diejenigen f_μ, deren Koeffizienten in einer von 0 entfernten Determinante aus M auftreten, sind sicher von 0 entfernt und auf diese f_μ kann man die weitere Betrachtung beschränken. — Satz B ist unmittelbar aus Satz A gefolgert. — Für Satz C schließen wir so: Ist $M = 0$, und hätten die f_μ keinen von Konstanten entfernten gemeinsamen Teiler, so könnte nicht α) und β) gelten. Da es ungereimt ist, anzunehmen, ein Polynom, das von 0 entfernt ist, könne nicht regulär sein, könnte α) nicht gelten, d.h. das Produkt aller f_μ wäre gleich 0. Nun nehmen wir an, der erweiterte Satz C sei für k Polynome bewiesen (für $k = 1$ ist er trivial), und zeigen. daß er auch für $k + 1$ Polynome gilt. Wäre eines von diesen gleich 0, so könnten die übrigen nach Voraussetzung keinen von Konstanten entfernten gemeinsamen Teiler haben. Daß keines der f_μ, wohl aber ihr Produkt gleich 0 wäre, wäre ein Widerspruch.

Satz D_2 ist allein aus Satz C gefolgert; bei seinem Beweis ist β) wesentlich gebraucht, so daß wir uns nur von α) befreien können.

4.3.5. Die Sätze A_2, B_2, C_2, D_2 lassen sich ohne weiteres auf homogene Gleichungen anwenden, wobei zunächst für (ξ_1, ξ_2) nur solche Wertepaare, in denen $\xi_2 \neq 0$, zugelassen sind; wegen der Symmetrie kann man in Satz A_2, B_2 und C_2 diese Bedingung ersetzen durch die, daß entweder $\xi_1 \neq 0$ oder $\xi_2 \neq 0$. Bei Satz D_2 erreichen wir in dieser Weise, wie die Substitution von $(1, 0)$ zeigt, daß auch Bedingung β) überflüssig wird.

§ 5. Elimination aus Gleichungen in mehreren Veränderlichen.

5.1. Das geht jetzt leicht mittels der Methode der sukzessiven Elimination (z.B. B. L. VAN DER WAERDEN, Moderne Algebra II, § 76). Durch Elimination von x_1 erhalten wir $D_1, \ldots, D_h$, die jetzt Polynome in $x_2, \ldots, x_m$ sind; das nach Elimination aller Veränderlichen erhaltene Resultantensystem sei $R_1, \ldots, R_s$.

SATZ A_3. Ist ein $R_\tau \not\equiv 0$, so ist für jeden von 0 entfernten Vektor $\xi = (\xi_1, \ldots, \xi_m)$ wenigstens ein $f_\mu(\xi) \not\equiv 0$.

Der Beweis ergibt sich durch wiederholte Anwendung des Hilfssatzes: Ist für jeden Vektor $(\xi_2, \ldots, \xi_m) = \xi' \not\equiv 0$ wenigstens ein $D_\sigma(\xi') \not\equiv 0$, so ist für jedes $\xi \not\equiv 0$ wenigstens ein $f_\mu(\xi) \not\equiv 0$. Ist nämlich ξ so gewählt, daß das zugehörige $\xi' \not\equiv 0$, so folgt es aus Satz A_2. Da ferner das Polynom $D_\tau \not\equiv 0$, ist wenigstens ein f_μ regulär in x_1; für $\xi_1 \not\equiv 0$ ist entweder dieses $f_\mu \not\equiv 0$ oder $\xi' \not\equiv 0$.

SATZ B_3. Besitzen die Gleichungen eine von 0 entfernte Lösung, so sind alle $R_\sigma = 0$.

Beweis. Nach Satz A_3 ist $R_\tau \not\equiv 0$ ausgeschlossen.

SATZ C_3. Sind alle $R_\tau = 0$, so ist es unmöglich, daß die Gleichungen keine von 0 entfernte Lösung besitzen.

Beweis durch wiederholte Anwendung des Hilfssatzes: Ist es unmöglich, daß die Gleichungen $D_\tau = 0$ keine von 0 entfernte Lösung besitzen, so ist es ebenfalls unmöglich, daß die Gleichungen $f_\mu = 0$ keine von 0 entfernte Lösung besitzen. Dies folgt aus Satz C_2 und dem logischen Satz: Folgt eine negative Behauptung aus einer gewissen Prämisse, so folgt sie schon aus der doppelten Negation dieser Prämisse.

SATZ D_3. Ist für jedes ξ wenigstens ein $f_\mu(\xi) \not\equiv 0$, so ist wenigstens ein $R_\sigma \not\equiv 0$.

Beweis. Es sei $\xi' = (\xi_2, \ldots, \xi_m) \not\equiv 0$; dann ist ein $f_\mu(\xi) \not\equiv 0$ für $\xi = (\xi_1, \xi_2, \ldots, \xi_m)$ mit beliebigem ξ_1, also ist nach Satz D_2 wenigstens ein $D_\varrho(\xi') \not\equiv 0$. Wiederholte Anwendung dieses Schlusses ergibt den Satz.

§ 6. Faktorzerlegung.

6.1. Wie schon bemerkt, gilt nicht der Satz, daß jedes Polynom über einem Körper sich eindeutig in Primfaktoren zerlegen läßt. Wir müssen uns auf diesem Gebiet mit negativen Sätzen begnügen.

6.1.1. Die folgende Bemerkung wird bei Beweisen von negativen Sätzen viele Wiederholungen unnötig machen.

SATZ. Ist die Ungereimtheit der Ungereimtheit eines Satzes A bewiesen und folgt B aus A, so gilt die Ungereimtheit der Ungereimtheit von B.

Beweis. Wäre B ungereimt, so wäre auch A ungereimt.

Ist nun B ein negativer Satz, so ist die Ungereimtheit der Ungereimtheit von B mit B gleichwertig; man kann also in dem Beweis von B annehmen, A sei bewiesen.

Wir werden diese Bemerkung benutzen um in den folgenden Beweisen alle von 0 verschiedenen Polynome als regulär vorauszusetzen. Es ist klar, dass ein Polynom, das nicht regulär sein kann, gleich 0 ist, denn sein erster Koeffizient kann nicht von 0 entfernt sein, ist also gleich 0, dann ebenso der zweite Koeffizient usw. Die Anname, daß nicht alle in einem bestimmten Beweis auftretenden von 0 verschiedenen Polynome regulär sind, ist ungereimt. Denn unter diesen gibt es ein letztes Polynom φ in diesem Sinn, daß die Existenz der übrigen Polynome nicht mehr davon abhängt ob φ regulär ist. Wären nun alle übrigen Polynome regulär, so könnte φ nicht regulär sein, was nicht kann, usw. bis alle Polynome erschöpft sind.

Ebenso hat ein von 0 verschiedenes Polynom in mehreren Veränderlichen immer einen bestimmten Grad.

In analoger Weise werden wir nachdem 6.2.1 bewiesen ist, voraussetzen, daß alle auftretenden Polynome in einer Veränderlichen in unteilbare Faktoren zerlegbar sind usw.

6.2.1. SATZ. Es ist unmöglich, ein Polynom über einem Körper anzugeben, das nicht in unteilbare Faktoren [10]) zerlegt werden kann.

Beweis. Wir können das Polynom f vom bestimmten Grad n und in jeder Veränderlichen regulär annehmen. Da jedes reguläre Polynom vom Grad 1 prim ist, gilt der Satz für den Grad 1. Er sei nun bewiesen für alle Polynome von kleinerem Grad als n. Wäre nun f nicht in unteilbare Faktoren zerlegbar, so könnte f nicht teilbar sein, denn sonst wäre für die Faktoren, welche regulär von geringerem Grad wären, eine Zerlegung in unteilbare Faktoren unmöglich, entgegen der Voraussetzung; also wäre f selber unteilbar, ebenfalls entgegen der Voraussetzung.

6.2.2. *Bemerkung.* Der entsprechende Satz für Zerlegung in Primfaktoren wird in 6.3 mit Hilfe der Eliminationstheorie bewiesen. Die obige Methode führt hier nicht zum Ziel, weil die Behauptung, f sei unteilbar und doch nicht prim, noch keinen Widerspruch enthält. Es mag unwahrscheinlich sein, daß man jemals ein f finden wird, das nicht prim sein kann, während man andererseits niemals imstande sein wird, eine bestimmte Zerlegung anzugeben, widerspruchsvoll ist die Annahme eines grundsätzlich unlösbaren Problems dieser Art an sich nicht.

6.2.3. SATZ. Es ist unmöglich, daß ein Polynom über einem Körper auf zwei verschiedene Weisen in unteilbare Faktoren zerlegt werden kann. Genauer: es ist unmöglich, daß

$$f = ap_1 \dots p_r = bq_1 \dots q_s, \text{ wenn } f \neq 0 \quad . \quad . \quad . \quad . \quad . \quad (1)$$

wo a und b Konstante, die p und q unteilbare Polynome sind, p_1 nichtkonstant ist und $p_1 \neq c\,q_i$ für $i = 1, \dots, s$ und jedes Konstante c.

6.2.4. *Beweis für Polynome in einer Veränderlichen* [11]). Der Satz gilt

[10]) Auch Produkte aus einem Faktor sind zugelassen.

[11]) Der Grundgedanke dieser Methode stammt von ZERMELO; sie wurde zuerst ver-

für Polynome von dem Grad 0, da eine von 0 verschiedene Konstante keinen nichtkonstanten Faktor haben kann. Der Beweis sei geführt für alle Polynome, deren Maximalgrad kleiner als n ist; f sei regulär mit dem Grad n. Dann ist $a \not\equiv 0$, $b \not\equiv 0$; $p_1, \ldots, p_r, q_1, \ldots, q_s$ sind regulär und wir dürfen sie von höherem Grad als 0 annehmen, da wir eventuelle konstante Faktoren in a und b aufnehmen können. Aus $p_i = cq_k$ würde nun folgen $c \not\equiv 0$ und $g = acp_1 \ldots p_{i-1}\, p_{i+1} \ldots p_r = bq_1 \ldots q_{k-1}\, q_{k+1} \ldots q_s$, was nicht kann, weil der Grad von g kleiner als n ist. Es ist also $p_i \neq cq_k$. Nun nehmen wir noch an, daß der Grad von p_1 nicht kleiner ist als der von q_1. Es sei $p_1 = q_1 u + v$, wo v kleineren Grad als p_1 hat. Wäre $v = 0$, so könnte u weder nichtkonstant (da p_1 unteilbar) noch konstant (wegen $p_1 \neq cq_1$) sein, also $v \not\equiv 0$. Nun ist

$$\varphi = avp_2 \ldots p_r = q_1 (bq_2 \ldots q_s - aup_2 \ldots p_r) = q_1 w.$$

Zerlegen wir v und w in unteilbare Faktoren, so erhalten wir zwei verschiedene Zerlegungen von φ, denn q_1 hat höheren Grad als jeder Faktor von v und ist also von jedem Faktor links verschieden. Da φ einen Maximalgrad kleiner als n hat, ist das unmöglich.

6.2.5. Wir nehmen nun an, der Satz 6.2.4 sei bewiesen für Polynome in k Veränderlichen und ziehen zunächst aus ihm einige Folgerungen.

SATZ. Ist φ unteilbar und nichtkonstant, $fg \equiv 0\ (\varphi)$ und $f \not\equiv 0\ (\varphi)$ (f nicht teilbar durch φ), so ist $g \not\equiv 0\ (\varphi)$ ungereimt.

Beweis. Es sei $fg = h\varphi$; man zerlege f, g und h in unteilbare Faktoren; jeder Faktor von f ist von φ verschieden, so daß nach 6.2.4 nicht jeder Faktor von g von φ verschieden sein kann. Wäre aber $g \not\equiv 0\ (\varphi)$, so wäre doch jeder Faktor von g ungleich φ.

Ist φ von 0 entfernt, so schließt man mit Hilfe von 3.1.2 weiter, dass $g \equiv 0\ (\varphi)$.

6.2.6. *Beweis* von 6.2.4 für Polynome in mehreren Veränderlichen. Es sei (x steht für $x_1, \ldots, x_k$)

$$f(x, y) = a(x)\, p_1(x, y) \ldots p_r(x, y) = b(x)\, q_1(x, y) \ldots q_s(x, y),$$

wo alle Polynome regulär in allen Veränderlichen, die p und q unteilbar von höherem Grad als 0 in y sind und $p_i \neq cq_l$ ($i = 1, \ldots, s$) für jedes konstante c.

Wir erledigen erst den Fall $r = s = 1$, also $ap = bq$. a sei in unteilbare Faktoren zerlegt und π sei ein solcher Faktor. Ist $q = \Sigma q^{(l)} y^l$, so ist jedes $bq^{(l)}$ durch π teilbar; wäre b nicht durch π teilbar, so wäre nach 6.2.5 jedes $q^{(l)}$, also q durch π teilbar; da dieses unmöglich ist, muß b durch π teilbar sein. Man kann links und rechts durch π teilen und ähnlich schließen

---

öffentlicht von H. HASSE (Aufgabensammlung zur höheren Algebra, S. 72); S. auch E. ZERMELO, Elementare Betrachtungen zur Theorie der Primzahlen. Nachr. Ges. Wiss. Göttingen [Math.-Phys. Klasse, Fachgruppe 1, Neue Folge, Bd. 1, Nr. 3].

für einen zweiten Primfaktor von a; so ergibt sich $b \equiv 0$ (a) und ebenso $a \equiv 0$ (b). a und b unterscheiden sich nur durch einen konstanten Faktor.

Nun sei $r > 1$. Wir wenden Induktion nach dem Grad von f in y an und beweisen ebenso wie in 6.2.4, daß $p_i \neq c\,q_k$ $(i = 1, \ldots, r;\ k = 1, \ldots, s)$ für jedes konstante c. Wir teilen q_1 durch p_1 und vertreiben etwaige Nenner:

$$m(x)\ p_1 = q_1 g + h.$$

Wäre $h = 0$, so kämen wir in Streit mit den Induktionsvoraussetzungen, denn g, also jeder unteilbare Faktor von g, hat in y niedrigeren Grad als p_1 und $m(x)p_1$ hat in y niedrigeren Grad als f.

Also $h \neq 0$.

$$f_1(x, y) = ahp_2 \ldots p_r = q_1 (bmq_2 \ldots q_s - agp_2 \ldots p_r).$$

Jeder unteilbare Faktor von h ist von $c\,q_1$ verschieden; da f_1 geringeren Grad in y hat als f, sind wir zu einem Widerspruch gelangt.

6.2.7. SATZ. Es ist unmöglich, daß ein Polynom über einem Körper auf zwei verschiedene Weisen in Primfaktoren zerlegt werden kann. Die genaue Fassung des Satzes entnimmt man aus 6.2.4, wo nur „unteilbare Polynome" durch „Primpolynome" zu ersetzen ist. Der Satz ist bloss eine Abschwächung von 6.2.4.

6.3. Um 6.2.1 auf Primfaktoren auszudehnen, müssen wir uns auf einen algebraisch abgeschlossenen Körper beschränken. Zunächst verschärfen wir das algebraische Irreduzibilitätskriterium [12]).

6.3.1. Es sei $F(x) = F(x_1, \ldots, x_k)$ das allgemeine Polynom in k Veränderlichen von dem Grad n mit unbestimmten Koeffizienten A_λ; $G(x)$ und $H(x)$ ebenso für die Grade p und $n-p$ mit Koeffizienten B_λ und C_λ. Setzt man $F = GH$, so ergeben sich Beziehungen

$$A_\lambda = \varphi_\lambda(B, C).$$

Ist $f(x)$ ein Polynom von dem Grad n mit Koeffizienten a_λ aus dem algebraisch abgeschlossenen Körper K und besitzen die Gleichungen

$$a_\lambda = \varphi_\lambda(B, C) \quad \ldots\ldots\ldots\ldots \quad (1)$$

eine Lösung $B_\tau = b_\tau$, $C_\tau = c_\tau$ in K, so nennen wir f *p-teilbar*.

Aus (1) folgt:

$$a_\lambda \varphi_\mu - a_\mu \varphi_\lambda = 0. \quad \ldots\ldots\ldots\ldots \quad (2)$$

Ist $f(x)$ p-teilbar, so ist (2) lösbar nach den B, C. Besitzt umgekehrt (2)

---

[12]) E. NOETHER, Ein algebraisches Kriterium für absolute Irreduzibilität [Math. Annalen 85 (1922), 26—33]. E. FISCHER, Über absolute Irreduzibilität [Math. Annalen 94 (1925), 163—165]. Für den Hinweis auf diese Litteratur, sowie für eine die intuitionistische Umgestaltung erleichternde Darstellung des FISCHERschen Beweises bin ich Herrn B. L. VAN DER WAERDEN zu Dank verpflichtet.

eine Lösung, in der sowohl ein b_τ als ein c_τ von 0 entfernt ist (kurz: einen *von* 0 *entfernten* lösenden *Doppelvektor*), so kann man die Zahl β so bestimmen, daß $\varphi_\lambda = \beta a_\lambda$ $(\lambda = 1, \ldots, n)$, also $gh = \beta f$, so daß $\beta \neq 0$ und $(\beta^{-1} g)h$ ist eine p-Zerlegung von f.

Ist für jeden von 0 entfernten Doppelvektor b, c für wenigstens ein Indexpaar $\lambda, \mu \neq a_\lambda \varphi_\mu - a_\mu \varphi_\lambda \neq 0$, so ist auch für jeden Doppelvektor b, c wenigstens ein $a_\lambda \neq \varphi_\lambda$, also $f \neq gh$ für alle Polynome g, h von den angegebenen Graden; wir sagen, daß f *p-prim* ist. Ist umgekehrt f p-prim, so gibt es zu jedem von 0 entfernten Doppelvektor b, c und jeder Zahl β wenigstens ein $a_\lambda \neq \beta \varphi_\lambda$. Aus $g \neq 0$ und $h \neq 0$ folgt $gh \neq 0$, also ein $\varphi_\mu \neq 0$. Da $a_n \neq 0$, ist entweder $a_n \varphi_\mu - a_\mu \varphi_n \neq 0$ oder $\varphi_n \neq 0$; im letzten Fall wählen wir $\beta = \frac{a_n}{\varphi_n}$ und finden dazu ein ν, so daß $a_\nu - \beta \varphi_\nu \neq 0$, also $a_\nu \varphi_n - a_n \varphi_\nu \neq 0$.

Zusammenfassung: Notwendig und hinreichend, damit f p-teilbar sei, ist die Existenz einer von 0 entfernten Lösung von (2); notwendig und hinreichend, damit f p-prim sei, ist, daß für jeden Doppelvektor b, c in einer Gleichung (2) $\neq$ stehen muß.

6.3.2. Wir eliminieren aus (2) die C; das Resultat sei

$$D_1(a, B) = 0, \ldots. \qquad D_q(a, B) = 0. \quad . \quad . \quad . \quad . \quad . \quad (3)$$

Nach § 5, Sätze A_3, D_3 ist notwendig und hinreichend, damit f p-prim sei, daß für jeden von 0 entfernten Vektor b in wenigstens einer Gleichung (3) $\neq$ stehen muß; ist f p-teilbar, so ist (3) nach den B lösbar (Satz B_3); besitzt (3) eine von 0 entfernte Lösung, so ist es unmöglich, daß f nicht p-teilbar ist (Satz C_3).

Nun eliminieren wir aus den in den B homogenen Gleichungen (3) die B und erhalten das Eliminationsresultat

$$R_{p1}(a) = 0, \ldots. \qquad R_{p, r_p}(a) = 0. \quad . \quad . \quad . \quad . \quad . \quad (4)$$

Ebenso wie für (3) ergeben sich die analogen Resultate für (4):

Notwendig und hinreichend, damit f p-prim sei, ist, daß wenigstens ein $R_{p\lambda}(a) \neq 0$. Ist f p-teilbar, so ist jedes $R_{p\lambda}(a) = 0$. Ist jedes $R_{p\lambda} = 0$, so ist es unmöglich, daß f nicht p-teilbar ist. Schreiben wir die Gleichungen (4) auf für $p = 1, \ldots, \left[\frac{n}{2}\right]$, so finden wir: Notwendig und hinreichend, damit f prim sei, ist, daß für jedes p wenigstens ein $R_{p\lambda}(a) \neq 0$. Ist f teilbar, so ist für ein bestimmtes p jedes $R_{p\lambda} = 0$; ist umgekehrt für ein bestimmtes p jedes $R_{p\lambda} = 0$, so ist es unmöglich, daß f nicht teilbar ist.

6.3.3. Die Aussage „Für wenigstens ein λ ist $R_{p\lambda} \neq 0$" (für bestimmtes p) bezeichnen wir mit A_p; ferner sei $\left[\frac{n}{2}\right] = s$. Nun leiten wir aus der

Annahme, daß f unteilbar und doch nicht prim sei, wie folgt einen Widerspruch her. Aus dieser Annahme würde folgen:

1. Nicht alle A_p sind richtig (sonst wäre f prim);

2. Es ist unmöglich, daß ein A_p falsch ist (sonst könnte f nicht unteilbar sein).

Daß dies schon ein Widerspruch ist, sehen wir ein mittels vollständiger Induktion nach s (der Anzahl der A_p). Es sei schon gezeigt, daß ein Widerspruch vorliegt, falls 1. und 2. gelten für $s-1$ Aussagen. Wären $A_1, \ldots, A_{s-1}$ richtig, so wäre nach 1. A_s falsch in Widerspruch mit 2.; also können $A_1, \ldots, A_{s-1}$ nicht alle richtig sein, wodurch der Widerspruch erhalten ist.

6.3.4. Die Beweisführung aus 6.2.1 liefert uns jetzt:

SATZ. Es ist unmöglich, ein Polynom über einem algebraisch abgeschlossenen Körper anzugeben, das nicht in Primfaktoren zerlegt werden kann.

6.4. Das folgende Beispiel soll zeigen, wie diese negativen Ergebnisse zu Beweisen von positiven Sätzen zu verwerten sind.

6.4.1. HILFSSATZ. Sind f und g Polynome über einem Körper und $g \neq 0$, so kann man eine Konstante c so bestimmen, daß aus $f \neq cg$ folgt $f \neq dg$ für jedes konstante d. Dann gilt auch folgendes: Ist es unmöglich, daß $f \neq dg$ für jedes konstante d, so ist $f = cg$.

Beweis. Es sei a ein von 0 entfernter Koeffizient aus g, b der entsprechende Koeffizient aus f, $c = \frac{b}{a}$. Ist nun $f \neq cg$, so gilt für beliebiges konstante d entweder $f \neq dg$ oder $d \neq c$; in diesem Fall ist $ad \neq b$, also $f \neq dg$.

6.4.2. SATZ. Es seien f, g, φ Polynome über einem algebraisch abgeschlossenen Körper, φ prim und von Konstanten entfernt, s eine natürliche Zahl und $fg = \varphi^s$. Dann kann man die Konstante c und die nichtnegative ganze Zahl t so bestimmen, daß $f = c\varphi^t$.

Beweis. h sei der Maximalgrad von f. Wir bestimmen die Zahlen a_i $(i = 1, \ldots, h)$ so daß aus $f \neq a_i \varphi^i$ folgt $f \neq c\varphi^i$ für jedes konstante c. Wir setzen $D = \prod_{i=1}^{h} (f - a_i \varphi^i)$ und leiten aus der Annahme $D \neq 0$ einen Widerspruch her. Dazu dürfen wir nach 6.1.1 und 6.3.4 f und g in Primfaktoren zerlegt denken:

$$f = f_1 f_2 \cdots f_\lambda; \quad g = g_1 g_2 \cdots g_\mu,$$

also $f_1 f_2 \cdots f_\lambda g_1 g_2 \cdots g_\mu = \varphi^s$.

Nach 6.2.7 ist es unmöglich, daß $f_i \neq c\varphi$ für jedes konstante c; nach dem Hilfssatz bestimmen wir die Zahlen b_i so, daß $f_i = b_i \varphi$ $(i = 1, \ldots, \lambda)$, so daß $f = b_1 \ldots b_\lambda \varphi^\lambda$. Dann ist aber $b_1 \ldots b_\lambda = a_\lambda$ und ist der Widerspruch mit $D \neq 0$ erhalten. Folglich ist $D = 0$; da die Faktoren von D zu

je zweien voneinander entfernt sind ($f \neq 0$, also entweder $f - a_i \varphi^i \neq 0$ oder $a_i \neq 0$), ist ein bestimmter Faktor gleich 0.

Bekannt ist die Anwendung dieses Satzes in dem Anfang der Invariantentheorie [13]).

---

[13]) Z. B. R. WEITZENBÖCK, Invariantentheorie, S. 12. Die Frage von Herrn G. F. C. GRISS, ob dieser Schluß intuitionistisch zulässig sei, gab den Anstoß zu den obigen Untersuchungen.