also nach Satz 13

$$m < P_{11} h^2 \log^6 |d_0| < P_{23} h^8 \log^6 m,$$

Wegen $m > P_{22}$ ist

$$\log^6 m < \sqrt{m},$$

also

$$m < P_{23} h^8 \sqrt{m},$$

$$m < P_{24} h^{16},$$

$$\log m < P_{25} \log (3h),$$

$$m < P_{26} h^8 \log^6 (3h).$$

Jedenfalls leistet also $P_1 = \text{Max}\ (P_{22}, P_{26})$ das Gewünschte.

Mittel-Schreiberhau, den 19. Juli 1934.

(Eingegangen am 23 Juli 1934.)

Bemerkungen über die Struktur von Ringen, die aus Polynomen in einer Variabel bestehen.

Von

Alexander Ostrowski (Basel).

Einleitung.

Unter einem Polynomring [1]) versteht man eine solche Gesamtheit $\mathfrak{R}$ von Polynomen, dass Summe und Produkt von je zwei Polynomen von $\mathfrak{R}$ wieder zu $\mathfrak{R}$ gehören und ferner das Produkt jedes Polynoms aus $\mathfrak{R}$ mit einer beliebigen Grösse aus dem Koeffizientenkörper K [2]) wieder in $\mathfrak{R}$ liegt. Wir betrachten nun in dieser Mitteilung Ringe $\mathfrak{R}$, die aus Polynomen in einer Variabel x bestehen.

Nach Analogie mit dem, was man von der Theorie der algebraischen Zahlen her kennt [3]), wird man vor allem solche Ringe als besonders einfach ansehen, in denen ein bestimmtes Polynom $\Phi(x)$ niedrigsten Grades — der Führer des Ringes — existiert, mit der Eigenschaft, dass jedes durch $\Phi(x)$ teilbare Polynom mit Koeffizienten aus K in $\mathfrak{R}$ liegt (so dass also $\mathfrak{R}$ aus Restklassen modulo $\Phi(x)$ besteht); solche Ringe wollen wir als Kongruenzringe bezeichnen. Wir

[1]) Vgl. zum Begriff des Ringes van der Waerden, Moderne Algebra, Bd. 1, (1930), Berlin, pp. 36 ff.

[2]) Wir setzen den Körperbegriff in der Allgemeinheit voraus, die ihm durch Steinitz in dessen klassischen Arbeit „Zur algebraischen Theorie der Körper", Crelles Journal, Bd. 137 (1910), pp. 167—309 verliehen wurde. Diese Abhandlung, auf die später nur mit „Steinitz" und Angabe der Seitenzahl Bezug genommen wird, ist auch in der Buchausgabe bei W. de Gruyter, Berlin, 1931, erschienen.

[3]) Vgl. hierzu die Originalabhandlungen von Dedekind in dessen gesammelten Abhandlungen, Bd. 1, Abh. XII, XV, XIX, wo noch die Bezeichnung „Ordnung" statt der von Hilbert später eingeführten „Ring" benutzt wird.

werden nun vor allem die Tatsache herleiten, dass jeder aus Polynomen in einer Variabel bestehende Ring entweder ein Kongruenzring ist, oder aus einem solchen entsteht, indem man in ihm die Variable durch ein Polynom in x ersetzt. Genauer gesagt:

Lässt sich x durch die Polynome von $\mathfrak{R}$ rational ausdrücken (solche Ringe bezeichnen wir als primitiv), so ist $\mathfrak{R}$ ein Kongruenzring (Satz IX). Ist allgemeiner etwa $f(x)$ ein Polynom niedrigsten positiven Grades, das sich durch die Polynome von $\mathfrak{R}$ rational ausdrücken lässt, so ist jedes Polynom $F(x)$ aus $\mathfrak{R}$ ein Polynom $F^*(f(x))$ in $f(x)$, und die Polynome $F^*(x)$ bilden einen Kongruenzring.[4])

Dies wird im § 2 dieser Mitteilung hergeleitet, nachdem im § 1 verschiedene Bemerkungen zum Lüroth'schen Satz entwickelt werden. Wir benutzen im § 1 wesentlich einen einfachen, aber sehr wichtigen und nützlichen Satz von Steinitz über die Grade von rationalen Funktionen (Satz I). Mit Hilfe dieses Satzes lässt sich der von van der Waerden bereits vereinfachte Steinitz'sche Beweis des Lüroth'schen Satzes [5]) noch etwas weiter vereinfachen, und es ergibt sich dann aus ihm eine sehr interessante Tatsache über die Charakterisierung der Lüroth'schen Grössen durch ihre Gradzahlen. Indem wir ferner den Begriff der Ordnung einer rationalen Funktion im Unendlichen einführen (übrigens auf rein algebraischem Wege, also für beliebige Körper), gelangen wir sehr leicht auch zum Satz, dass wenn ein Körper von rationalen Funktionen in x Polynome enthält, seine Lüroth'sche Grösse als Polynom gewählt werden kann (Satz VI) [6]). Endlich zeigen

[4]) Die in einem primitiven Ring nach dem Führer als Modul vorkommenden Restklassen bilden offenbar ein System höherer komplexer Zahlen von besonderer Bauart, und es genügt zur Aufzählung aller primitiven Ringe, alle solche Systeme höherer komplexer Zahlen aufzustellen. Diese Aufgabe bietet keine prinzipiellen Schwierigkeiten, ist übrigens auch im Falle des Körpers aller komplexen Zahlen als Koeffizientenkörper bereits in der bekannten Abhandlung von Weierstrass, „Zur Theorie der aus n Haupteinheiten gebildeten komplexen Grössen" Mathem. Werke, Bd. II, pp. 311—332, weitgehend diskutiert worden. Vgl. hierzu die Angaben in der Encyclopédie des sciences mathématiques, T. 1, Vol. 1, fasc. 3, pp. 409—413.

[5]) Für die verschiedenen Beweise des Lüroth'schen Satzes vergleiche man Lüroth, Math. Ann., Bd. 9 (1876), p. 318; Gordan, Math. Ann., Bd. 29 (1887), p. 318; Netto, Math. Ann., Bd. 46 (1895), p. 310; Steinitz, p. 302 ff. (hier wurde zum erstenmal der Satz für den allgemeinsten Koeffizientenkörper bewiesen); van der Waerden, Moderne Algebra, Bd. 1, p. 126. Vgl. ferner M. Pasch, Math. Ann., Bd. 18 (1881), pp. 91—92.

[6]) Der Satz wurde zum erstenmal von Emmy Noether angegeben im Jahresber. d. D. Math.-Ver., Bd. 22 (1913), p. 318. Der Beweis wurde ausgeführt in der 1915 erschienenen Abhandlung in den Math. Ann. Bd. 76 pp. 161—196. Diese Abhandlungen werden im Folgenden zitiert mit N. I bzw. N. II.

wir, dass dabei die Ganzzahligkeit gewahrt bleibt (Sätze VII, VIII).

Im § 3 bringen wir sodann einige Anwendungen auf das „Endlichkeitsproblem" [7]). Dass jedes System von Polynomen in einer Variabel eine endliche Integritätsbasis besitzt, ist bereits 1913 von Emmy Noether [8]) und einfacher 1918 von mir [9]) bewiesen worden. Wir zeigen nun vor allem, dass, wenn der Führer eines primitiven Ringes $\mathfrak{R}$ vom Grade n ist, man mit n Elementen der Integritätsbasis auskommt, und dass diese Abschätzung bei keiner Wahl des Führers sich verbessern lässt.

Zweitens aber gehen wir auf die Frage nach der *ganzzahligen Integritätsbasis* ein. Ein beliebiges System von ganzzahligen Polynomen in einer Variabel braucht, wie man sehr leicht einsieht, keine endliche ganzzahlige Integritätsbasis zu besitzen. Man kann aber auch die Gesamtheit $\mathfrak{R}^*$ der ganzzahligen Polynome betrachten, die in einem Ring $\mathfrak{R}$ enthalten sind, so dass also dabei auch die Division mit einer ganzen Zahl erlaubt ist, wenn nur ein ganzzahliges Polynom herauskommt. Hier ist die Frage etwas schwieriger zu entscheiden und sie war für mich der Ausgangspunkt der ganzen hier mitgeteilten Untersuchung. Wir diskutieren nun insbesondere die *Z - Ringe*, deren sämtliche Polynome nach dem Führer einer Grösse aus K kongruent sind. In diesem Falle ergeben sich leicht Beispiele von Systemen vom Typus $\mathfrak{R}^*$, die keine endliche ganzzahlige Integritätsbasis haben.

Zum Beweise des Satzes IX ist noch folgendes zu bemerken. Dieser Satz ist eine unmittelbare Folgerung aus dem Satz X, der seinerseits durch Spezialisierung einer in der abstrakten Theorie der Ringe geläufigen Schlussweise zu beweisen ist. Nämlich: Bereits Dedekind beweist den Satz, dass wenn α eine algebraische, aber nicht ganze Zahl ist, dann zu jeder algebraischen Zahl β ein ganzes positives n gehört, so dass $\beta\alpha^n$ nicht ganz ist. Daran knüpft man die folgenden Definitionen an: Ist $\mathfrak{K}$ der Quotientenkörper eines abstrakten Ringes $\mathfrak{R}$, so nennt man ein Element α von $\mathfrak{K}$ „ganz abhängig von $\mathfrak{R}$", wenn α einer algebraischen Gleichung mit dem höchsten Koeffizienten 1 genügt, deren übrige Koeffizienten in $\mathfrak{R}$ liegen. Ferner heist α „fast ganz von $\mathfrak{R}$

[7]) Das Endlichkeitsproblem - das Problem nach der Existenz einer endlichen Integritätsbasis bei Systemen von Polynomen, ist im Anschluss an die invariantentheoretischen Untersuchungen von Gordan und Hilbert entstanden und zuerst allgemein von Hilbert gefasst worden (Hilbert, Ges. Abh., Bd. II, pp. 288—289). Die weitere Literatur: E. Fischer, Crelles Journal, Bd. 140 (1911), pp. 48—81; N., I., II; Emmy Noether, Math. Ann., Bd. 77 (1916), pp. 89 — 92; Gött. Nachr. 1919, pp. 1—17; 1926, pp. 28—35; Ostrowski, Math. Ann., Bd. 78 (1918), pp. 94—119; Bd. 81 (1920), pp. 21—24.

[8]) N. I, II.

[9]) Ostrowski, in der ersten unter [7]) zitierten Abhandlung, pp. 109—110.

abhängig", wenn für eine geeignete Grösse c von $\mathfrak{R}$ jedes Produkt $c\alpha^n$, $n \geqq 0$, in $\mathfrak{R}$ liegt. Unter sehr allgemeinen Voraussetzungen sind nun die beiden Begriffe äquivalent (vgl. Emmy Noether, Math. Ann., Bd. 96, pp. 32—34; W. Krull, Math. Ann., Bd. 99, pp. 60 ff.; van der Waerden, Mod. Alg., Bd. 2, pp. 90—91; W. Krull, Crelles Journal, Bd. 167, pp. 169—170). Unser Satz X ist nun nichts anderes, als eine Spezialisierung der Tatsache, dass aus der „ganzen Abhängigkeit" die „fast ganze Abhängigkeit" folgt. Wir bringen aber den einfachen Beweis in entsprechender Spezialisierung vollständig.

Die erwähnte allgemeine Tatsache ist bisher unseres Wissens nicht auf Polynomringe angewandt worden; sie liefert aber eine Lösung des Strukturproblems nur für den Fall einer Variabel. Für mehrere Variabeln ergibt sich leicht das folgende Resultat:

Ist $\mathfrak{R}$ ein Ring von Polynomen in n Variabeln $x_1, \ldots, x_n$, dessen Quotientenkörper $x_1, \ldots, x_n$ enthält und in dem n Polynome vorkommen, bei denen die Gliederaggregate höchster Dimension eine von 0 verschiedene Resultante haben, so gibt es ein Polynom $\Phi(x_1, \ldots, x_n)$ derart, dass jedes durch Φ teilbare Polynom mit Koeffizienten aus dem entsprechenden Koeffizientenkörper in $\mathfrak{R}$ liegt.

Um diese an sich sehr interessante Tatsache auf das Strukturproblem anzuwenden, müsste man aber erst kommutative komplexe Zahlensysteme mit abzählbar vielen Einheiten beherrschen. Denn man kann an Beispielen zeigen, dass das Polynomideal der Polynome mit der Eigenschaft von $\Phi(x_1, \ldots, x_n)$ eingliedrig sein kann und zugleich so beschaffen, dass die Reste der Polynome von $\mathfrak{R}$ nach diesem Ideal als Modul keine endliche Basis bilden. Wir diskutieren nun zum Schluss ein solches Beispiel.

§ 1. Bemerkungen zum Lüroth'schen Satz.

1. Es sei K ein beliebiger Körper von der Charakteristik 0 oder p. Es sei x in Bezug auf K transzendent und $K(x)$ die Gesamtheit aller rationalen Funktionen von x mit Koeffizienten aus K. Jede Grösse $f(x)$ aus $K(x)$ lässt sich in der Form schreiben

$$f(x) = \frac{g(x)}{h(x)}, \tag{1}$$

wo $g(x)$ und $h(x)$ teilerfremde Polynome in x mit Koeffizienten aus K sind. Sind dann ν_1, ν_2 die Gradzahlen von $g(x)$, $h(x)$, so bezeichnen wir das Maximum von ν_1, ν_2 als den *Grad von $f(x)$ in Bezug auf x* [10]). Für ein Polynom ist offenbar diese Definition mit der klassischen identisch. Es gilt nun der folgende für manche Anwendungen wichtige Satz von Steinitz:

I. *Sind $F(x), f(x)$ zwei rationale Funktionen von x aus $K(x)$ mit den Gradzahlen M bzw. m, so ist der Grad von $F(f(x))$ genau gleich Mm* [11]).

2. Wir betrachten nun einen beliebigen Zwischenkörper $\overline{K}$ zwischen K und $K(x)$. Die Struktur von $\overline{K}$ wird durch den Lüroth'schen Satz festgelegt:

II. (Der Lüroth'sche Satz). *Jeder Zwischenkörper $\overline{K}$ zwischen einem beliebigen Körper K und seiner einfachen transzendenten Erweiterung $K(x)$ entsteht aus K durch Adjunktion einer geeigneten Grösse $y = f(x)$ aus $K(x)$.*

Jede Grösse $y = f(x)$, für die unter den Voraussetzungen von II $\overline{K} = K(y)$ ist, bezeichnen wir im folgenden als eine *Lüroth'sche Grösse von K* [12]) — genauer gesagt, eine Lüroth'sche Grösse von $\overline{K}$ in Bezug auf K und x.

Den Beweis des Lüroth'schen Satzes kann man folgendermassen führen. Es sei $f(x)$ eine Grösse aus $\overline{K}$, deren Grad m in Bezug auf x positiv und möglichst klein ist. Schreibt man $f(x)$ in der Form (1), so genügt offenbar x der Gleichung m-ten Grades

$$g(t) - y\,h(t) = 0, \tag{2}$$

deren Koeffizienten dem Körper $K(y)$ angehören. Daher ist der Grad μ von $K(x)$ in Bezug auf $K(y)$ höchstens gleich m. Es sei $F(t) = 0$ die in $\overline{K}$ irreduzible Gleichung, der x genügt. Der Grad M von $F(t)$ ist offenbar zugleich der Grad von $K(x)$ in Bezug auf $\overline{K}$, und es gilt sicher $\mu \geqq M$, da $K(y)$ mit y in $\overline{K}$ enthalten ist. Die Koeffizienten der verschiedenen Potenzen von t in $F(t)$ sind dann nach Voraussetzung rationale Funktionen von x, deren Grad in Bezug auf x, wenn er positiv ist, mindestens gleich m sein muss. Multipliziert man daher $F(t)$ mit dem Generalnenner aller Koeffizienten, so ergibt sich ein Polynom $F(t; x)$ in t, dessen Koeffizienten Polynome in x mit dem grössten gemeinschaftlichen Teiler 1 sind, und dann muss der Grad dieses Polynoms in Bezug auf x wenigstens m sein. Da aber auch die Koeffizienten der Gleichung (2) dem Körper $\overline{K}$ angehören, ist die linke

[10]) Steinitz, p. 188.

[11]) Für den einfachen Beweis vgl. man Steinitz, pp. 188—190.

[12]) Die Bezeichnung wurde von Emmy Noether eingeführt, N. I, p. 318; II, p. 191.

Seite von (2) durch $F(t)$ und daher auch das Polynom $h(x)(g(t) - y\,h(t))$ durch $F(t;x)$, *als Polynom in t und x aufgefasst*, teilbar:

$$h(x)\,g(t) - g(x)\,h(t) = F(t;x)\,Q(t;x).$$

Hier ist aber der Grad von Q in Bezug auf x gleich 0, da ja die linke Seite in Bezug auf x höchstens den Grad m und $F(t;x)$ *wenigstens* den Grad m hat. Dann wäre aber die linke Seite von (2) durch ein Polynom $Q(t)$ von t mit von x unabhängigen Koeffizienten teilbar, während $g(t)$ und $h(t)$ als teilerfremd vorausgesetzt wurden [18]). Daher ist $Q(t,x)$ eine Grösse aus K, und der Grad M von F in Bezug auf t gleich m. Aus $\mu \leqq m$, $\mu \geqq M$, $m = M$ folgt $\mu = M$. Also ist der Grad von K in Bezug auf $K(y)$ gleich 1, so dass $\overline{K}$ mit $K(y)$ identisch ist, w. z. b. w.

3. Zugleich hat sich bei diesem Beweis ergeben, dass der Grad von $K(x)$ in Bezug auf $\overline{K}$ gleich dem kleinsten bei den Grössen aus K vorkommenden positiven Grad und dass jede Grösse aus $\overline{K}$ von diesem Minimalgrad in Bezug auf x eine Lüroth'sche Grösse von $\overline{K}$ ist. Ist ferner $R(x)$ eine beliebige Grösse aus $\overline{K}$, so gilt nach Voraussetzung

$$R(x) = F(f(x)), \tag{3}$$

wo $F(x)$ eine rationale Funktion in x mit Koeffizienten aus K und $f(x)$ eine Lüroth'sche Grösse von $\overline{K}$ ist. Daher ist nach I der Grad von $R(x)$ in Bezug auf x durch den Grad von $f(x)$ teilbar. Wir sehen:

III. *Der Grad einer einfachen transzendenten Erweiterung $K(x)$ eines Körpers K in Bezug auf einen beliebigen von K und $K(x)$ verschiedenen Zwischenkörper $\overline{K}$ zwischen K und $K(x)$ ist der grösste gemeinschaftliche Teiler m der Grade aller in $\overline{K}$ liegenden rationalen Funktionen von x. Eine Grösse y aus $\overline{K}$ ist dann und nur dann eine Lüroth'sche Grösse von $\overline{K}$ in Bezug auf K und x, wenn ihr Grad in Bezug auf x gleich m ist. Alle Lüroth'schen Grössen von $\overline{K}$ sind rationale Funktionen voneinander.*

4. Wir werden nun zeigen, dass man als eine Lüroth'sche Grösse von $\overline{K}$ stets ein *Polynom* in x wählen kann, wenn $\overline{K}$ überhaupt Polynome

[18]) Man kann dies folgendermassen weiter ausführen: man dividiere $g(t)$ und $h(t)$ durch $Q(t)$ und bezeichne die Reste mit $g_1(t), h_1(t)$; ihre Grade in t sind kleiner als der Grad von $Q(t)$. Dann müsste aber auch $g_1(t) - y\,h_1(t)$ durch $Q(t)$ noch teilbar sein, während der Grad von $g_1(t) - y\,h_1(t)$ in t kleiner ist als der Grad von $Q(t)$. Daher müssen die Koeffizienten aller Potenzen von t in $g_1(t) - y\,h_1(t)$ identisch in y verschwinden, was nur dann möglich ist, wenn $g_1(t)$ und $h_1(t)$ beide verschwinden. Dann wäre aber $Q(t)$ ein gemeinsamer Teiler von $g(t)$ und $h(t)$, entgegen der Annahme.

in x enthält. Zu dem Zwecke führen wir den Begriff der *Ordnung einer rationalen Funktion $f(x)$ im Unendlichen* ein. Darunter verstehen wir, wenn $f(x)$ als Quotient zweier Polynome dargestellt ist, den (genauen) Grad des Zählers vermindert um den (genauen) Grad des Nenners — offenbar ist es dabei unwesentlich, ob der Zähler und Nenner gemeinschaftliche Faktoren haben oder nicht. Es handelt sich bei dieser Definition natürlich um einen rein algebraischen Sachverhalt, so dass der Koeffizientenkörper K nicht eingeschränkt zu werden braucht. Für jede ganze Zahl n ist offenbar die Ordnung von $f(x)^n$ gleich dem n-fachen der Ordnung von $f(x)$. Die Ordnung eines Polynoms in x im Unendlichen ist gleich seinem Grad, und diese Eigenschaft ist für Polynome unter rationalen Funktionen in x charakteristisch.

Es sei ferner $R(x)$ eine rationale Funktion von x von der Ordnung 0 im Unendlichen, während $f(x)$ im Unendlichen von positiver Ordnung sein möge. Wir behaupten, dass dann $R(f(x))$ von der Ordnung 0 im Unendlichen ist. Denn es sei

$$R(x) = \frac{G(x)}{H(x)}, \qquad f(x) = \frac{g(x)}{h(x)},$$

wo die Gradzahlen von $G(x)$ und $H(x)$ einander gleich und etwa gleich n sind, während die Grade von $g(x)$, $h(x)$ resp. die Werte m_1, m_2 haben. Dann ist

$$R(f(x)) = \frac{h(x)^n\, G\left(\frac{g(x)}{h(x)}\right)}{h(x)^n\, H\left(\frac{g(x)}{h(x)}\right)}.$$

Hier ist aber wegen $m_1 > m_2$ das höchste Glied im Zähler vom Grade $n\,m_1$, da es nur einmal herauskommt und sich daher nicht wegheben kann. Da dasselbe auch für den Nenner gilt, ist unsere Behauptung bewiesen. Daraus folgt aber der Satz.

IV. *Sind $R(x)$, $f(x)$ rationale Funktionen, deren Ordnungen im Unendlichen bzw. gleich r, m sind und ist $m > 0$, so ist die Ordnung von $R(f(x))$ im Unendlichen genau gleich rm.*

In der Tat gilt

$$R(x) = x^r\, R_0(x),$$

wo $R_0(x)$ die Ordnung 0 im Unendlichen hat, und daher gilt auch

$$R(f(x)) = f(x)^r\, R_0(f(x)).$$

Hier ist die Ordnung des ersten Faktors genau gleich rm, während die Ordnung des zweiten Faktors nach dem Obigen verschwindet. Daher ist die Ordnung des Produktes $= r\,m$.

5. Ferner gilt:

V. *Unter den Voraussetzungen des Satzes* II *lässt sich eine Lüroth'sche Grösse von* $\overline{K}$ *so wählen, dass sie im Unendlichen von positiver Ordnung in* x *ist.* — Denn ist $f(x)$ eine Lüroth'sche Grösse von $\overline{K}$, deren Ordnung im Unendlichen von 0 verschieden ist, so ist entweder $f(x)$ oder $\frac{1}{f(x)}$ im Unendlichen von positiver Ordnung. Ist aber in der Darstellung (1) von $f(x)$ der Zähler vom gleichen Grad wie der Nenner und sind a_0, b_0 resp. die höchsten Koeffizienten im Zähler und Nenner, so hat

$$\frac{1}{f(x)-\frac{a_0}{b_0}}$$

im Unendlichen positive Ordnung. — Nunmehr ist es leicht den Satz zu beweisen:

VI. *Enthält unter den Voraussetzungen von* II *der Körper* $\overline{K}$ *Polynome in* x*, so lässt sich als eine Lüroth'sche Grösse von* $\overline{K}$ *stets ein Polynom in* x *wählen, und jedes in* $\overline{K}$ *liegende Polynom lässt sich dann durch diese Lüroth'sche Grösse als ein Polynom in ihr mit Koeffizienten aus* K *ausdrücken*[14].

Beweis: Es sei $P(x)$ ein Polynom aus $\overline{K}$ und es sei y eine Lüroth'sche Grösse von $\overline{K}$ vom Grade m und von der positiven Ordnung μ im Unendlichen. Dann gilt

$$P(x)=F(y),$$

wo $F(x)$ eine rationale Funktion in x mit Koeffizienten aus K ist. Es seien n, ν der Grad von $F(x)$ bzw. ihre Ordnung im Unendlichen. Der Grad von $P(x)$ sei l — dies ist zugleich die Ordnung von $P(x)$ im Unendlichen. Dann folgt aus I und IV

$$l=nm, \quad l=\nu\mu. \tag{4}$$

Da μ nach Voraussetzung positiv ist, ist folglich auch ν positiv. Aus $\mu \leqq m$, $\nu \leqq n$ folgt wegen (4): $\mu=m$, $\nu=n$. Dies bedeutet aber, dass sowohl y als auch $F(x)$ Polynome in x sind, w. z. b. w.

6. Wir beweisen endlich noch die folgende Tatsache, die von Bedeutung ist, wenn es sich um Darstellungen von ganzzahligen Polynomen handelt.

[14] Dieser Satz ist zuerst von Emmy Noether auf anderem Wege bewiesen worden, N. I, p. 318, N. II, p. 191.

VII. *Es sei* $f(x)$ *ein Polynom in* x *mit ganzen rationalen Koeffizienten, für das die Differenz* $f(x)-f(0)$ *primitiv ist, d. h. zum grössten gemeinschaftlichen Teiler aller Koeffizienten* 1 *hat. Es sei* $P(x)$ *ein ganzzahliges Polynom in* x *und es sei*

$$P(x)=F(f(x)), \tag{5}$$

wo auch $F(x)$ *ein Polynom ist. Dann ist* $F(x)$ *durch* (5) *eindeutig bestimmt und ein ganzzahliges Polynom in* x*. Ferner ist* $F(x)$ *dann und nur dann primitiv, wenn dies für* $P(x)$ *der Fall ist.*

Beweis. Setzt man in $F(x)$ für $x: f(0)+y$ ein, so ist das entstehende Polynom in y zugleich mit $F(x)$ ganzzahlig und primitiv. Wir können daher von vornherein annehmen, dass $f(0)=0$ ist. Es sei nun

$$F(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n.$$

Wir setzen

$$F_0(x)=a_0,\ F_1(x)=a_0x+a_1,\ \ldots,\ F_\nu(x)=a_0x^\nu+\ldots+a_\nu,\ \ldots,$$

wo der Symmetrie halber $F(x)=F_n(x)$ zu setzen ist. Offenbar gilt

$$F_{\nu+1}(x)=xF_\nu(x)+a_{\nu+1};\ \nu=0,\ \ldots,\ n-1.$$

Aus der Ganzzahligkeit von $P(x)$ folgt, dass auch

$$P(0)=F_n(f(0))=F_n(0)=a_n$$

eine ganze Zahl ist. Daher ist auch

$$F_n(f(x))-a_n=f(x)F_{n-1}(f(x))$$

ein ganzzahliges Polynom in x. Und da es durch das primitive Polynom $f(x)$ teilbar ist, ist auch:

$$F_{n-1}(f(x))=f(x)F_{n-2}(f(x))+a_{n-1}$$

ganzzahlig. Daher ist auch sein Nullwert a_{n-1} ganz und daraus folgt wiederum, dass auch $F_{n-2}(f(x))$ ein ganzzahliges Polynom in x ist. Indem wir dies Verfahren weiter fortsetzen, zeigen wir sukzessive, dass alle Zahlen $a_{n-1}, \ldots, a_1, a_0$ ganze Zahlen sind. Zugleich ergeben sich offenbar die Werte dieser Koeffizienten von $F(x)$ im Laufe der Betrachtung eindeutig.

Nun folgt aus (5), dass wenn die Koeffizienten von $F(x)$ durch eine ganze Zahl q teilbar sind, dies auch für alle Koeffizienten von $P(x)$ der Fall ist. Daher folgt aus der Primitivität von $P(x)$ die Primitivität von $F(x)$. Es sei umgekehrt $F(x)$ primitiv; wären dann alle Koeffizienten von $P(x)$ durch eine ganze Zahl $q>1$ teilbar, so wäre $\frac{P(x)}{q}$ ganzzahlig und daher analog zu (5) darstellbar. Daher müsste

in (5) das eindeutig bestimmte $F(x)$ durch q teilbar sein und wäre nicht primitiv. Damit ist der Satz VII vollständig bewiesen.

7. Offenbar gilt unser Beweis des Satzes VII in allen Fällen, wo im Koeffizientenkörper K der betrachteten Polynome ganze Grössen und Teilbarkeit derart definiert sind, dass ein grösster gemeinschaftlicher Teiler eines beliebigen endlichen Systems von ganzen Grössen existiert und der Gauss'sche Satz über primitive Polynome (das Produkt von zwei primitiven Polynomen ist wieder primitiv) richtig bleibt. Solche Körper nennt man *vollständig* in Bezug auf die entsprechende Definition der „Ganzheit" [15]). Dies trifft insbesondere in den drei folgenden Fällen zu:

A. Der Koeffizientenkörper K ist ein (algebraischer) Zahlkörper mit der Klassenzahl 1.

B. Der Koeffizientenkörper K ist der Körper aller rationalen Funktionen von n Variablen $t_1, t_2, \ldots, t_n$ mit Koeffizienten aus einem beliebigen Körper K_0, in Bezug auf den $t_1, t_2, \ldots, t_n$ transzendent sind. Als eine ganze Grösse aus K ist dann jedes Polynom in $t_1, t_2, \ldots, t_n$ mit Koeffizienten aus K_0 anzusehen.

C. Wenn im Falle B der Körper K_0 insbesondere ein Zahlkörper mit der Klassenzahl 1 ist, kann man als eine ganze Grösse von K jedes Polynom in $t_1, t_2, \ldots, t_n$ mit *ganzen* Koeffizienten aus K_0 ansehen.

Wir sehen:

VIII. *Wird im Satz* VII *die Voraussetzung, dass* $f(x)$ *und* $P(x)$ *ganzzahlig sind und* $f(x) - f(0)$ *primitiv ist, durch die Voraussetzung ersetzt, dass* $f(x)$ *und* $P(x)$ *Polynome aus einem vollständigen Körper* K *sind und der grösste gemeinschaftliche Teiler der Koeffizienten von* $f(x) - f(0)$ *gleich* 1 *ist, so ist das Polynom* $F(x)$ *in* (5) *eindeutig bestimmt und hat als Koeffizienten ganze Grössen aus* K. *Ferner ist* $F(x)$ *dann und nur dann primitiv, wenn* $P(x)$ *primitiv ist.*

§ 2. Darstellung von Polynomringen in einer Variabel durch Kongruenzringe.

8. Es sei K ein beliebiger Körper und x in Bezug auf K transzendent. Es sei $\mathfrak{R}$ eine Gesamtheit von Polynomen in x mit Koeffizienten aus K, die die folgenden Eigenschaften besitzt:

1) *Summe und Produkt von je zwei Grössen aus* $\mathfrak{R}$ *gehören wieder zu* $\mathfrak{R}$.

[15]) Vgl. die interessante Abhandlung von H. Prüfer, Crelles Journal, Bd. 168 (1932), pp. 1—36, wo vollständige Körper eingehender untersucht werden und insbesondere gezeigt wird, dass, wenn stets ein grösster gemeinschaftlicher Teiler existiert, daraus auch die Gültigkeit des Gauss'schen Satzes folgt.

2) *Das Produkt jeder Grösse aus* $\mathfrak{R}$ *mit jeder Grösse aus* K *gehört wieder zu* $\mathfrak{R}$.

Eine solche Gesamtheit bezeichnen wir als einen Ring. Bildet man die Quotienten aller Grössen aus $\mathfrak{R}$, so bilden diese Quotienten einen Körper, den *Quotientenkörper* $\mathfrak{R}/\mathfrak{R}$ von $\mathfrak{R}$. Wir nennen $\mathfrak{R}$ einen *primitiven* Ring, wenn $\mathfrak{R}/\mathfrak{R}$ mit $K(x)$ identisch ist, wenn also x in $\mathfrak{R}/\mathfrak{R}$ liegt.

Ist nun $\mathfrak{R}$ nicht primitiv, so sei $y = f(x)$ eine Lüroth'sche Grösse von $\mathfrak{R}/\mathfrak{R}$. Nach Satz VI kann $y = f(x)$ als ein Polynom in x angenommen werden, und zwar können wir für $f(x)$ jedes Polynom aus $\mathfrak{R}/\mathfrak{R}$ annehmen, dessen Grad in x positiv und minimal ist. Dann ist nach Satz VI jedes Polynom von $\mathfrak{R}$ ein Polynom $F(f(x))$ von $f(x)$, und die Polynome $F(x)$ bilden einen primitiven Ring, der mit $\mathfrak{R}$ „isomorph" ist [16]).

9. Wir nennen nun einen Ring $\mathfrak{R}$, wie er in der letzten Nummer betrachtet wurde, einen *Kongruenzring*, wenn er die Eigenschaft hat, dass es ein Polynom $\Phi(x)$ in $\mathfrak{R}$ gibt, derart, dass jedes durch $\Phi(x)$ teilbare Polynom mit Koeffizienten aus K zu $\mathfrak{R}$ gehört. Es sei $\mathfrak{R}$ ein Kongruenzring, und es mögen zwei Polynome $\Phi_1(x)$ und $\Phi_2(x)$ beide die oben angegebene Eigenschaft besitzen. Es seien $F_1(x)$ und $F_2(x)$ zwei beliebige Polynome in x mit Koeffizienten aus K. Dann besitzt auch das Polynom

$$\Phi_3(x) = F_1(x)\,\Phi_1(x) + F_2(x)\,\Phi_2(x)$$

die Eigenschaft, dass jedes durch $\Phi_3(x)$ teilbare Polynom in x mit Koeffizienten aus K wieder zu $\mathfrak{R}$ gehört. Daher besitzt insbesondere auch der grösste gemeinschaftliche Teiler von $\Phi_1(x)$ und $\Phi_2(x)$ die gleiche Eigenschaft. Folglich gibt es dann ein Polynom $\Phi^*(x)$ in $\mathfrak{R}$ mit den beiden Eigenschaften:

a) jedes durch $\Phi^*(x)$ teilbare Polynom in x mit Koeffizienten aus K gehört zu $\mathfrak{R}$; b) jedes andere Polynom $\Phi(x)$, für das jedes derartige Vielfache von $\Phi(x)$ zu $\mathfrak{R}$ gehört, ist selbst ein Vielfaches von $\Phi^*(x)$. Das Polynom $\Phi^*(x)$ ist dabei offenbar bis auf einen Faktor aus K eindeutig bestimmt. Wir wollen es als den *Führer des Kongruenzringes* $\mathfrak{R}$ bezeichnen.

Wir wollen nun den Satz beweisen:

IX. *Jeder primitive Ring von Polynomen in einer Variabel* x *mit Koeffizienten aus einem beliebigen Körper* K *ist ein Kongruenzring.*

[16]) Aus dem Satz III folgt offenbar, dass $\mathfrak{R}$ dann und nur dann ein primitiver Ring ist, wenn der grösste gemeinschaftliche Teiler der Grade aller in ihm vorkommenden Polynome gleich 1 ist. Ist dieser grösste gemeinschaftliche Teiler gleich m, so ist das Polynom $y = f(x)$, das als Lüroth'sche Grösse von $\mathfrak{R}/\mathfrak{R}$ angenommen werden kann, vom Grade m.

Dieser Satz ergibt sich unmittelbar aus dem folgenden Satz:

X. *Ist unter den Voraussetzungen des Satzes* IX

$$x = \frac{Q(x)}{P(x)}, \tag{6}$$

wo Q und P Polynome aus $\mathfrak{R}$ sind, und hat ein Polynom $T(x)$ aus $\mathfrak{R}$ den Grad $n > 0$, so ist jedes Polynom mit Koeffizienten aus K, das durch P^{n-1} teilbar ist, in $\mathfrak{R}$ enthalten. (Vgl. zu diesem Satz die Fussnote.[4]))

B e w e i s. Man kann $T(x)$ in der Form annehmen:

$$T(x) = x^n + a_1 x^{n-1} + \ldots + a_n, \tag{7}$$

wo $a_1, \ldots, a_n$ Grössen aus K sind. Dann ergibt sich

$$x^n = T(x) - a_1 x^{n-1} - \ldots - a_n. \tag{8}$$

Ich behaupte nun, dass für jedes $q \geqq 0$ eine Formel gilt:

$$x^q = \sum_{p=0}^{n-1} \varphi_{q,p}(T)\, x^p, \tag{9}$$

wo jedes $\varphi_{q,p}(x)$ ein Polynom in x mit Koeffizienten aus K ist. Für $q \leqq n$ ist die Behauptung nach (8) klar. Es sei die Behauptung für ein q wahr. Dann multipliziere man (9) mit x und ersetze rechts x^n durch die rechte Seite von (8). Man erhält:

$$x^{q+1} = \sum_{p=0}^{n-2} \varphi_{q,p}(T) x^{p+1} + \varphi_{q,n-1}(T)(T - a_1 x^{n-1} - a_2 x^{n-2} - \ldots - a_n).$$

Hier kommen aber rechts die Potenzen von x nur bis zur $(n-1)$-ten vor. Damit ist die Formel (9) allgemein bewiesen.

Multipliziert man nun (9) mit P^{n-1} so folgt:

$$x^q P^{n-1} = \sum_{p=0}^{n-1} \varphi_{q,p}(T) P^{n-p-1} P^p x^p = \sum_{p=0}^{n-1} \varphi_{q,p}(T) P^{n-p-1} Q^p, \tag{10}$$

und daher liegt $x^q P^{n-1}$ in $\mathfrak{R}$. Dasselbe gilt daher allgemein für $S(x) P^{n-1}$, wo $S(x)$ ein beliebiges Polynom mit Koeffizienten aus K ist, w. z. b. w.

10. Unter Berücksichtigung des in der Nr. 8 Gesagten, können wir daher den folgenden Satz formulieren, der die Struktur allgemeinster Polynomringe in einer Variabel festlegt:

XI. *Ist $\mathfrak{R}$ ein Ring von Polynomen in einer Variabel x mit Koeffizienten aus einem Körper K, und ist $y = f(x)$ ein im Quotientenkörper $\mathfrak{R}/\mathfrak{R}$ liegendes Polynom positiven Grades, für das dieser Grad minimal ist, so entsteht $\mathfrak{R}$ aus einem Kongruenzring $\overline{\mathfrak{R}}$ von Polynomen in einer in Bezug auf K transzendenten Variabel y mit Koeffizienten aus K, indem y in jedem Polynom von $\overline{\mathfrak{R}}$ durch $f(x)$ ersetzt wird.*

11. Was nun den Führer $\Phi^*(x)$ eines primitiven Ringes $\mathfrak{R}$ anbetrifft, so folgt aus dem Satz X, dass, wenn y als ein Quotient zweier Polynome $\frac{Q}{P}$ aus $\mathfrak{R}$ dargestellt werden kann, der Führer von $\mathfrak{R}$ ein Teiler von P^{n-1} ist, wenn n der Grad von P ist. Andererseits hat Φ^* selbst definitionsgemäss die Eigenschaft, dass $x\Phi^*(x)$ in $\mathfrak{R}$ liegt. Wir wollen nun zeigen, dass trotzdem die Aussage des Satzes X im allgemeinen Falle nicht verschärft werden kann. Ist nämlich $P(x)$ ein Polynom in x mit Koeffizienten aus K, so werden wir zwei primitive Polynomringe in x konstruiren, deren erster $P(x)$, deren zweiter aber $P(x)^{n-1}$ zum Führer hat, wenn n der Grad von $P(x)$ ist. Der erste Ring $\mathfrak{R}_1$ wird gebildet von der Gesamtheit aller Polynome in x, die sich in der Form

$$S(x) P(x) + k \tag{11}$$

schreiben lassen, wo k ein beliebiges Element aus K und $S(x)$ ein beliebiges Polynom in x mit Koeffizienten aus K ist. Denn, dass $\mathfrak{R}_1$ ein Ring ist, ist klar, und da andererseits in $\mathfrak{R}_1$ kein von x wirklich abhängiges Polynom von niedrigerem Grade als n vorkommt, ist offenbar P selbst der Führer von $\mathfrak{R}_1$. Ringe von diesem Typus werden wir als Z-Ringe bezeichnen.

12. Zweitens betrachten wir die Gesamtheit $\mathfrak{R}_2$ von Polynomen, die sich aus $P(x)$ und $x P(x)$ durch Multiplikation mit Grössen aus K und wiederholte Addition und Multiplikation ergeben. Man übersieht leicht, dass in $\mathfrak{R}_2$ die Grössen aus K die einzigen durch P nicht teilbaren Polynome sind. Die in $\mathfrak{R}_2$ liegenden, *genau* durch die erste Potenz von P teilbaren Polynome setzen sich linear (mit Koeffizienten aus K) zusammen aus P, $x P$. Die in $\mathfrak{R}_2$ liegenden, genau durch P^2 teilbaren Polynome setzen sich linear zusammen aus P^2, $x P^2$, $x^2 P^2$. Allgemein, für positive $\nu < n-1$ setzen sich die in $\mathfrak{R}_2$ liegenden, genau durch P^ν teilbaren Polynome linear zusammen aus P^ν, xP^ν, $\ldots$, $x^\nu P^\nu$, sodass insbesondere in $\mathfrak{R}_2$ alle Produkte

$$P^{n-2},\ x P^{n-2},\ \ldots,\ x^{n-2} P^{n-2}$$

liegen, während $x^{n-1} P^{n-2}$ in $\mathfrak{R}_2$ nicht enthalten ist; daraus folgt aber, dass in $\mathfrak{R}_2$ kein Polynom von der Form

(12) $$\psi(x)P^{n-2}$$

enthalten sein kann, wo der Grad von $\psi(x)$ genau $n-1$ ist. Dagegen liegen alle Produkte

$$P^{n-1},\ xP^{n-1},\ \ldots,\ x^{n-1}P^{n-1}$$

in $\mathfrak{R}_2$, andererseits lässt sich jedes Polynom $S(x)$ (mit Koeffizienten aus K) in der Form schreiben

$$\sum_{\nu=0}^{k} \varphi_\nu(x)P^\nu,$$

wo alle Koeffizienten $\varphi_\nu(x)$ Polynome in x mit Koeffizienten aus K sind, deren Grade *unterhalb* n liegen. Daher liegt $S(x)P^{n-1}(x)$ stets in $\mathfrak{R}_2$. Daher ist $P^{n-1}(x)$ sicher durch den Führer $\Phi^*(x)$ von $\mathfrak{R}_2$ teilbar. Es sei nun

$$P(x) = P_1^{d_1}P_2^{d_2}\ldots P_k^{d_k}$$

die Darstellung von P als Potenzprodukt von in K irreduziblen, wesentlich verschiedenen Polynomen $P_1(x), P_2(x), \ldots, P_k(x)$ mit Koeffizienten aus K. Wäre $\Phi^*(x)$ ein echter Teiler von P^{n-1}, so müsste in $\Phi^*(x)$ wenigstens eines der Polynome $P_1, P_2, \ldots, P_k$ in niedrigerer Potenz vorkommen als in P^{n-1}. Es sei dies etwa P_1 und es sei der Grad von P_1 gleich m. Dann ist das Polynom $\frac{P^{n-1}}{P_1}$ durch $\Phi^*(x)$ teilbar. Dasselbe gilt daher auch von $x^{m-1}\frac{P^{n-1}}{P_1}$. Dieses Polynom liegt daher in $\mathfrak{R}_2$, während es sich andererseits in der Form (12) schreiben lässt, wo $\psi(x)$ genau den Grad $n-1$ hat. Mit diesem Widerspruch ist bewiesen, dass $\Phi^*(x)$ mit P^{n-1} identisch und daher P^{n-1} der Führer von $\mathfrak{R}_2$ ist.

13. Wenn im Koeffizientenkörper K der Begriff von ganzen Grössen so definiert ist, dass K in Bezug auf diesen Begriff der „Ganzheit" vollständig ist, kann man insbesondere die Gesamtheit aller in $\mathfrak{R}$ liegenden Polynome mit *ganzen* Koeffizienten aus K ins Auge fassen. Diese Gesamtheit bezeichnen wir mit $\mathfrak{R}^*$. Wenn $\mathfrak{R}$ nicht primitiv ist, dann kann als eine Lüroth'sche Grösse von $\mathfrak{R}/\mathfrak{R}$ ein Polynom $f(x)$ angenommen werden, das für $x=0$ verschwindet, ganze Koeffizienten hat und primitiv ist. Dann ist nach dem Satz VIII jedes Polynom aus $\mathfrak{R}^*$ in der Form darstellbar: $F(f(x))$, wo $F(x)$ ein Polynom mit ganzen Koeffizienten ist. Wenn der primitive Ring, der so aus $\mathfrak{R}$ entsteht, mit $\mathfrak{R}_1$ bezeichnet wird, bilden die Polynome $F(x)$ dann genau die Menge $\mathfrak{R}_1^*$.

§ 3. Bemerkungen zum Endlichkeitsproblem. Z-Ringe.

14. Ist uns eine Menge von Polynomen gegeben, so sagt man von dieser Menge, sie besässe eine *endliche Integritätsbasis*, wenn es unter den Polynomen der Menge endlich viele gibt, durch die sich alle übrigen ganz und rational ausdrücken lassen, wobei als Koeffizienten alle Grössen des Koeffizientenkörpers der Polynome zugelassen werden. Es seien nun insbesondere die Polynome unserer Menge Polynome in einer Variabel x mit Koeffizienten aus einem beliebigen Körper K. Und es sei $\mathfrak{R}$ der durch die Polynome unserer Mengen erzeugte Ring, d. h. die Gesamtheit aller Polynome in x, die sich aus je endlich vielen unter den Polynomen der Menge ganz und rational mit Koeffizienten aus K ausdrücken lassen. Es ist klar, dass unsere Menge gleichzeitig mit der Menge aller Polynome des Ringes eine endliche Integritätsbasis besitzen muss. Es ist nun bekannt, dass dies auch immer zutrifft [17]), während im Falle von Polynomen in mehr als einer Variabel eine endliche Basis nicht zu existieren braucht. Aus unserem Satze über die Existenz des Führers bei jedem primitiven Ring lässt sich nun diese Tatsache in einer insofern schärferen Form herleiten, als sich daraus sogar eine Abschätzung für die *Anzahl* der Elemente einer Integritätsbasis eines solchen Ringes herleiten lässt. Ist nämlich der Grad des Führers gleich n, so kommt man mit höchstens n Elementen der Basis aus. Und damit ergibt sich offenbar zugleich eine Abschätzung für die *Anzahl* der Elemente einer Integritätsbasis für den Fall eines nicht primitiven Ringes.

XII. *Es sei K ein beliebiger Körper und x in Bezug auf K transzendent. Es sei $\mathfrak{R}$ ein primitiver Ring von Polynomen in x mit Koeffizienten aus K und es sei $\Phi(x)$ der Führer von $\mathfrak{R}$. Ist n der Grad von $\Phi(x)$, so lassen sich in $\mathfrak{R}$ Polynome $f_1(x), \ldots, f_n(x)$ finden, derart, dass jedes Polynom $f(x)$ aus $\mathfrak{R}$ sich ganz rational durch $f_1(x), \ldots, f_n(x)$ mit Koeffizienten aus K ausdrücken lässt.*

Ist $\Phi(x)$ ein beliebiges Polynom in x vom Grade n mit Koeffizienten aus K, für das $\Phi(0)=0$ ist, so hat der aus allen Polynomen von der Form

(13) $$S(x)\Phi(x)+a,$$

wo a eine beliebige Grösse aus K und $S(x)$ ein beliebiges Polynom in x mit Koeffizienten aus K ist, bestehende Ring keine Basis, die weniger als n Elemente besässe.

15. Beweis des ersten Teils von Satz XII. Ohne Beschränkung der Allgemeinheit darf angenommen werden, dass der höchste Koeffizient von $\Phi(x)$ gleich 1 ist. Für jede ganze Zahl

[17]) Zuerst in N. II, p. 191 bewiesen; sodann einfacher von Ostrowski in der in 7) an erster Stelle zitierten Abhandlung, pp. 109—110.

r, $0<r<n$ definiere man ein Polynom $\varphi_r(x)$ folgendermassen. Kommt in $\mathfrak{R}$ ein Polynom von Grade r vor, so dividiere man es durch seinen höchsten Koeffizienten und nehme das so entstehende Polynom als $\varphi_r(x)$. Kommt aber in $\mathfrak{R}$ ein Polynom vom Grade r nicht vor, so setzen wir $\varphi_r(x)=x^r\Phi(x)$. Endlich bezeichnen wir $\Phi(x)$ mit $\varphi_0(x)$. Ist dann $f(x)$ ein Polynom aus $\mathfrak{R}$, dessen höchstes Glied etwa ax^t ist, so gibt es unter den Polynomen $\varphi_r(x)$ ein solches, dessen Grad n_r höchstens gleich t und für das $\frac{t-n_r}{n}=k$ ganz ist. Dann ist die Differenz

$$f(x)-a\,\varphi_r(x)\,\varphi_0(x)^k$$

ein Polynom aus $\mathfrak{R}$, dessen Grad $<t$ ist. Von diesem Polynom lässt sich ein Potenzprodukt der $\varphi_r(x)$ abziehen, so dass sein Grad weiter erniedriegt wird, und dieses Verfahren lässt sich fortsetzen, bis man auf von x unabhängige Grössen aus K stösst. Daher lässt sich $f(x)$ ganz rational mit Koeffizienten aus K durch n Polynome $\varphi_0(x)$, $\varphi_1(x)$, . . . , $\varphi_{n-1}(x)$ ausdrücken, und wir haben in diesen n Polynomen eine aus n Elementen bestehende Integritätsbasis von $\mathfrak{R}$.

16. Beweis des zweiten Teiles des Satzes XII. Es möge der Ring aller Grössen von der Form (13) eine Basis aus m Elementen besitzen

$$S_\mu(x)\,\Phi(x)+a_\mu,\quad \mu=1,2,\ldots,m.$$

Offenbar kann von jeder Grösse (13) die entsprechende Grösse a_μ abgezogen werden, da ja Addition von und Multiplikation mit Grössen aus K sowieso zugelassen sind. Wir können daher unsere Basis in der folgenden Form annehmen:

$$S_\mu(x)\,\Phi(x),\quad \mu=1,2,\ldots,m. \tag{14}$$

Nun liegt in unserem Ring jedes der Polynome

$$x^r\Phi(x),\quad r=0,1,\ldots,n-1.$$

Wird ein solches Polynom durch die Grössen (14) ganz rational ausgedrückt, so ergibt sich eine Gleichung von der Form

$$x^r\Phi(x)=a+\sum_{q=1}^{m}\alpha_{r,q}\,S_q(x)\,\Phi(x)+F_2\big(S_q(x)\,\Phi(x)\big),$$

wo F_2 ein Polynom in seinen m Variabeln ist, in dem alle Glieder

wenigstens von zweiter Dimension sind. Daraus folgt modulo $\Phi(x)^2$ die Kongruenz

$$x^r\Phi(x)\equiv a+\sum_{q=1}^{m}\alpha_{r,q}\,S_q(x)\,\Phi(x)\quad(\mathrm{mod.}\ \Phi(x)^2).$$

Wegen $\Phi(0)=0$ muss aber hier a verschwinden. Daher ergibt sich nach Division durch $\Phi(x)$ die Kongruenz

$$x^r\equiv\sum_{q=1}^{m}\alpha_{r,q}\,S_q(x)\quad(\mathrm{mod.}\ \Phi(x)),\ r=0,1,\ldots,n-1.$$

Wäre nun die Anzahl m der $S_q(x)$ in diesen Kongruenzen $<n$, so würde sich daraus eine Kongruenz von der Form ergeben

$$\beta_0+\beta_1 x+\ldots+\beta_{n-1}x^{n-1}\equiv 0\quad(\mathrm{mod.}\ \Phi(x)),$$

wo nicht alle β_ν verschwinden. Dies ist aber unmöglich, da der Grad von $\Phi(x)$ genau gleich n ist. Damit ist der Satz XII bewiesen.

17. Eine Verfeinerung der Frage nach der Existenz einer endlichen Integritätsbasis bietet sich dar, wenn es sich um *ganzzahlige* Polynome handelt. Es sei L ein beliebiges System von Polynomen $f(x)$ mit ganzen rationalen Koeffizienten in einer Variabel x. Wir sagen, L besitze eine *endliche ganzzahlige Integritätsbasis*, wenn sich unter den Polynomen von L ein endliches System $f_1(x)$, . . . , $f_m(x)$ so wählen lässt, dass jedes Polynom von L sich durch die Polynome $f_1(x)$, . . . , $f_m(x)$ ganz rational mit ganzen rationalen Koeffizienten darstellen lässt. Dass nicht jedes System L eine ganzzahlige Integritätsbasis besitzt, sieht man sofort am Beispiel des Systems

$$2x,\ 2x^2,\ \ldots,\ 2x^\nu,\ \ldots\ .$$

Indessen liegt hier eine weitere Verfeinerung der Fragestellung nach ganzzahliger Integritätsbasis nahe, indem man zum System L alle ganzzahligen Polynome hinzunimmt, die aus den Polynomen von L durch ganze rationale Operationen, aber auch eventuell mit nicht ganzen Koeffizienten entstehen. Dies läuft darauf hinaus, dass wir den durch die Polynome von L erzeugten Ring $\mathfrak{R}$ betrachten und dann die Gesamtheit $\mathfrak{R}^*$ der in $\mathfrak{R}$ liegenden ganzzahligen Polynome ins Auge fassen. Dass aber auch die Systeme vom Typus $\mathfrak{R}^*$ keine ganzzahlige Integritätsbasis zu haben brauchen, ergibt sich aus den

recht allgemeinen Beispielen, die wir der Theorie der Z-Ringe entnehmen.

18. Ist $\Phi(x)$ ein primitives ganzzahliges Polynom, so bezeichnen wir als den Z-Ring mit dem Führer $\Phi(x)$ die Gesamtheit aller Polynome mit gewöhnlichen rationalen Koeffizienten, die nach $\Phi(x)$ als Modul einer rationalen Zahl kongruent sind, also die Form haben

$$S(x)\,\Phi(x)+a,$$

wo a eine rationale Zahl und $S(x)$ ein Polynom mit rationalen Koeffizienten ist. Wir wollen nun zunächst eine Darstellung für die zu einem solchen Ring $\mathfrak{R}$ gehörende Gesamtheit $\mathfrak{R}^*$ von in ihm liegenden ganzzahligen Polynomen herleiten. Diese Darstellung wird durch den folgendem Satz geliefert:

XIII. *Es sei $\mathfrak{R}$ ein Z-Ring mit dem primitiven ganzzahligen Polynom $\Phi(x)$ als Führer,*

$$\Phi(x)=\pi\,Q(x)-A, \tag{15}$$

wo $Q(0)=0$ ist, $\Phi(0)=-A$, $(\pi, A)=1$ und $Q(x)$ primitiv ist, so dass π der Teiler des Polynoms $\Phi(x)-\Phi(0)=\Phi(x)+A$ ist. Dann ässt sich jedes in $\mathfrak{R}^*$ enthaltene ganzzahlige Polynom in den beiden Formen darstellen:

$$\text{I}\qquad \frac{S(x)\,\Phi(x)+a}{\Delta},$$

wo a und Δ ganze Zahlen sind, $S(x)$ ein ganzzahliges Polynom und Δ durch keine Primzahl teilbar ist, die nicht in π vorkommt;

$$\text{II}\qquad S(x)\,\Phi(x)+\varphi(Q),$$

wo $S(x)$ und $\varphi(x)$ ganzzahlige Polynome sind.

Beweis. Wir zeigen zunächst, dass, wenn ein Polynom von der Form

$$S(x)\,\Phi(x)+a, \tag{16}$$

wo a eine ganze Zahl und $S(x)$ ein ganzzahliges Polynom ist, durch eine zu π teilerfremde Primzahl p teilbar ist, sowohl a als auch $S(x)$ durch p teilbar sind. In der Tat folgt aus der Annahme die Kongruenz

$$S(x)\,\Phi(x)\equiv -a \pmod{p}.$$

Wäre nun a durch p nicht teilbar, so müssten, da auch im Bereich ganzzahliger Polynome modulo p der Satz von der eindeutigen Zerlegung in irreduzible Faktoren gilt, sowohl $S(x)$ als auch $\Phi(x)$ modulo p ganzen Zahlen kongruent sein, was für $\Phi(x)$ sicher nicht

zutrifft, wenn p in π nicht aufgeht. Daher ist a durch p teilbar, und da $\Phi(x)\not\equiv 0 \pmod{p}$ ist, folgt, dass $S(x)$ durch p teilbar ist

Andererseits ist offenbar jedes ganzzahlige Polynom aus $\mathfrak{R}$ in der Gestalt I darstellbar, wenn als Δ eine beliebige ganze Zahl zugelassen wird. Wie aus der eben bewiesenen Tatsache folgt, lassen sich aber dann in dieser Darstellung alle Primteiler von Δ wegkürzen. die nicht in π aufgehen. So gelangen wir zur Darstellung I, in der Δ keine nicht in π aufgehenden Primteiler besitzt.

Um nunmehr aus der Darstellung I die Darstellung II herzuleiten, zeigen wir zuerst, dass, wenn ein in der Form II dargestelltes ganzzahliges Polynom $f(x)$ durch einen Primteiler p von π teilbar ist, sich dann auch $\frac{f(x)}{p}$ in der Form II darstellen lässt. In der Tat ergibt sich aus unserer Annahme

$$S(x)\,\Phi(x)+\varphi(Q)\equiv 0,\quad \varphi(Q)-A\,S(x)\equiv 0 \pmod{p}.$$

Da A zu π teilerfremd und also durch p nicht teilbar ist, gibt es eine ganze Zahl A' derart, dass $A'A\equiv 1 \pmod{p}$, $A'A-1=tp$ ist. Dann folgt

$$S(x)\equiv A'\varphi(Q) \pmod{p},$$

$$S(x)=A'\varphi(Q)+p\,S_1(x).$$

Trägt man diesen Wert von $S(x)$ in die Darstellung II von $f(x)$ ein, so ergibt sich

$$f(x)=p\,S_1(x)\,\Phi(x)+A'\varphi(Q)\,(\pi Q-A)+\varphi(Q),$$

$$\frac{f(x)}{p}=S_1(x)\,\Phi(x)+\left(A'\frac{\pi}{p}Q-t\right)\varphi(Q),$$

womit die Behauptung bewiesen ist.

Nun ist aber der Zähler $S(x)\,\Phi(x)+A$ in der Darstellung I bereits in der Form II dargestellt ($\varphi(Q)\equiv A$). Durch wiederholte Anwendung der soeben bewiesenen Tatsache erhalten wir sodann die Darstellung II auch für den ganzen Quotienten I, womit der Beweis des Satzes XIII erbracht ist.

19. Wir können nunmehr eine recht allgemeine Klasse von Z-Ringen angeben, für die die zugehörigen $\mathfrak{R}^*$-Systeme keine endliche ganzzahlige Integritätsbasis besitzen:

XIV. *Unter den Voraussetzungen des Satzes* XIII *möge der höchste Koeffizient A_0 von $Q(x)$ durch eine Primzahl p teilbar sein, die nicht in π aufgeht. Dann besitzt die Gesamtheit der in $\mathfrak{R}$ liegenden ganzzahligen Polynome keine endliche ganzzahlige Integritätsbasis.*

Beweis. Es möge $\mathfrak{N}^*$ eine aus m Polynomen $f_1(x), \ldots, f_m(x)$ bestehende ganzzahlige Integritätsbasis besitzen und es möge hier die Darstellung I des Satzes XIII allgemein lauten

$$f_q(x) = \frac{S_q(x)\,\Phi(x) + a_q}{\Delta_q}.$$

Es sei M eine Zahl, die grösser als die Grade der m Polynome $S_1(x), \ldots, S_m(x)$ ist, und es sei das Polynom $f(x) = x^M \Phi(x)$ durch $f_1(x), \ldots, f_m(x)$ ganzzahlig in der Form dargestellt

$$f(x) = F(f_1(x), \ldots, f_m(x)).$$

Dann gibt es ein solches Potenzprodukt Δ der Zahlen $\Delta_1, \ldots, \Delta_m$, dass das Produkt $\Delta f(x)$ sich darstellen lässt als ein ganzzahliges Polynom in

$$\Delta_1 f_1(x),\ \Delta_2 f_2(x),\ \ldots,\ \Delta_m f_m(x).$$

Da aber die Zahlen $a_1, \ldots, a_m$ ganz sind, ergibt sich hieraus eine Darstellung von $\Delta f(x)$ als ein ganzzahliges Polynom in den Ausdrücken

$$\Delta_q f_q(x) - a_q = S_q(x)\,\Phi(x).$$

Diese Darstellung lässt sich nun aber in der Form entwickeln

$$\Delta f(x) = a + \sum_{q=1}^{m} a_q S_q(x)\,\Phi(x) + F_2(S_1(x)\,\Phi(x), \ldots, S_m(x)\,\Phi(x)),$$

wo jedes Glied des ganzzahligen Polynoms $F_2(z_1, \ldots, z_m)$ wenigstens von der zweiten Dimension in Bezug auf die Variabeln $z_1, \ldots, z_m$ ist. Hieraus folgt aber die Kongruenz nach $\Phi(x)^2$ als Modul:

$$\Delta x^M \Phi(x) \equiv a + \Phi(x) \sum_{q=1}^{m} a_q S_q(x) \quad (\mathrm{mod.}\ \Phi(x)^2).$$

Daher muss a durch $\Phi(x)$ teilbar sein, a verschwindet also, und es ergibt sich durch Division mit $\Phi(x)$ die Kongruenz

$$\Delta x^M - \sum_{q=1}^{m} a_q S_q(x) \equiv 0 \quad (\mathrm{mod.}\ \Phi(x)).$$

Da aber Δx^M das höchste Glied des ganzzahligen Polynoms auf der linken Seite ist, müsste Δ durch den höchsten Koeffizienten A_0 von $\Phi(x)$ teilbar sein. Dies ist aber unmöglich, da Δ als Produkt der Δ_q nur Primteiler enthält, die in π vorkommen, während, A_0 nach Voraussetzung durch eine in π nicht vorkommende Primzahl teilbar ist. Damit ist der Satz XIV bewiesen.

20. Wir fügen noch einige Angaben über Ringe hinzu, die von Polynomen in mehreren Veriabeln gebildet werden.

XV. *Es sei $\mathfrak{N}$ ein Ring aus Polynomen in n Variabeln $x_1, \ldots, x_n$, $n>0$, mit Koeffizienten aus einem beliebigen Koeffizientenkörper K. Es mögen sich die n Variabeln $x_1, \ldots, x_n$, $n>0$, rational mit Koeffizienten aus K durch Grössen von $\mathfrak{N}$ ausdrücken lassen. Ferner möge jede dieser n Variabeln einer algebraischen Gleichung mit dem höchsten Koeffizienten 1 genügen, deren übrige Koeffizienten Grössen aus $\mathfrak{N}$ sind. Dann existiert ein solches Polynom $\Phi(x, \ldots, x)$ mit Koeffizienten aus K, dass jedes durch Φ teilbare Polynom in $x_1, \ldots, x_n$ mit Koeffizienten aus K in $\mathfrak{N}$ enthalten ist.*

Bemerkung. Die Voraussetzung der „ganzen Abhängigkeit" der Variabeln $x_1, \ldots, x_n$ von $\mathfrak{N}$ ist sicher erfüllt, wenn es in $\mathfrak{N}$ n Polynome gibt, bei denen die Gliederaggregate höchster Dimension eine von 0 verschiedene Resultante besitzen.

Der Beweis von XV ist ganz analog zu führen, wie derjenige von X. Sind die Grade der in der Voraussetzung des Satzes erwähnten algebraischen Gleichungen, denen $x_1, \ldots, x_n$ genügen resp. $m_1, \ldots, m_n$, so kann man jede Potenz von x_ν, deren Exponent $\geqq m_\nu$ ist, linear mit Koffizienten aus $\mathfrak{N}$ durch $x_\nu^{m_\nu - 1}, \ldots, x_\nu$, 1 ausdrücken. Sind daher $P_1, \ldots, P_N$, $N = m_1 m_2 \ldots m_n$, alle Potenzprodukte von $x_1, \ldots, x_n$, deren Exponenten resp. $m_1, \ldots, m_n$ nicht überschreiten, so lässt sich jedes Polynom in $x_1, \ldots, x_n$ mit Koeffizienten aus K in der Form darstellen

$$F = Q_1 P_1 + \ldots + Q_N P_N,$$

wo $Q_1, \ldots, Q_N$ Grössen aus $\mathfrak{N}$ sind. Nun folgt aber aus der Voraussetzung des Satzes unmittelbar die Existenz eines Polynoms Φ aus $\mathfrak{N}$, für das die N Produkte

$$P_1\Phi,\ P_2\Phi,\ \ldots,\ P_N\Phi$$

zu $\mathfrak{N}$ gehören. Dasselbe gilt daher auch für das Produkt $F\Phi$, w. z. b. w.

21. Wir werden nun das Beispiel des Ringes $\mathfrak{N}$ ausführlicher diskutieren, der durch die drei Polynome

$$f_1 = x_1^2 - x_2,\ f_2 = x_2^2,\ f_3 = x_1 x_2^2$$

erzeugt wird, wenn der Körper aller rationalen Zahlen als Koeffizientenkörper genommen wird. Wir wollen nun zuerst zeigen,

dass x_2^6 dle Eigenschaft hat, dass jedes durch x_2^6 teilbare Polynom in x_1, x_2 mit rationalen Koeffizienten $\mathfrak{R}$ angehört und dass ferner, wenn ein rationalzahliges Polynom Φ_1 in x_1, x_2 die Eigenschaft hat, dass jedes durch Φ_1 teilbare Polynom in x_1, x_2 dem Ring $\mathfrak{R}$ angehört, dieses Polynom Φ_1 selbst durch x_2^6 teilbar sein muss.

Zunächst folgt für x_2^p, $p>6$:

$$p=2q,\ x_2^{2q}=f_2^q;\ p=2q+1,\ x_2^{2q+1}=f_2^{q-2}f_3^2\ldots f_2^q f_1.$$

Ebenso folgt für $x_1 x_2^p$, $p\geqq 6$:

$$p=2q,\ x_1 x_2^{2q}=f_3 f_2^{q-1};\ p=2q+1,\ x_1 x_2^{2q+1}=f_2^{q-3}f_3^3\ldots f_2^{q-1}f_1 f_3.$$

Ist aber $r\geqq 2$, $p\geqq 6$, so folgt aus

$$x_1^r x_2^p = f_1 x_1^{r-2} x_2^p + x_1^{r-2} x_2^{p+1},$$

dass $x_1^r x_2^p$, $p\geqq 6$ für $r\geqq 2$ sicher $\mathfrak{R}$ angehört, wenn dies für das um zwei Einheiten verkleinerte r und alle $p>6$ der Fall ist. Daher ist in der Tat jedes durch x_2^6 teilbare Polynom in x_1, x_2 mit rationalen Koeffizienten in $\mathfrak{R}$ enthalten.

22. Es möge nun ein Polynom Φ_1 aus $\mathfrak{R}$ die Eigenschaft haben, dass das Produkt von Φ_1 mit jedem rationalzahligen Polynom in x_1, x_2 zu $\mathfrak{R}$ gehört. Wir wollen beweisen, dass Φ_1 durch x_2^6 teilbar ist. Es genügt, wenn wir dies für jedes Polynom Φ_2 aus $\mathfrak{R}$ beweisen, für das jedes Produkt $x_1^r \Phi_2$ für hinreichend grosse r zu $\mathfrak{R}$ gehört. Wir können offenbar Φ_2 in der Form annehmen:

$$\sum_{p=0}^{5} c_p x_1^{\alpha_p} x_2^p.$$

Dann gehört nach Voraussetzung

$$x_1^r \Phi_2 = x_1^{r-2} f_1 \Phi_2 + x_2 x_1^{r-2} \Phi_2,$$

daher auch $x_1^{r-2}\Phi_3$ zu $\mathfrak{R}$, wo

$$\Phi_3 = \sum_{p=0}^{4} c_p x_1^{\alpha_p} x_2^{p+1} = x_2 \Phi_2 - c_5 x_1^{\alpha_5} x_2^6$$

ist, sobald r hinreichend gross ist. Daher hat auch Φ_3 die gleiche Eigenschaft wie Φ_2. Indem wir diese Überlegung wiederholen, sehen wir, dass die gleiche Eigenschaft auch

$$\sum_{p=0}^{3} c_p x_1^{\alpha_p} x_2^{p+2},\ \sum_{p=0}^{2} c_p x_1^{\alpha_p} x_2^{p+3},\ \sum_{p=0}^{1} c_p x_1^{\alpha_p} x_2^{p+4},\ c_0 x_1^{\alpha_0} x_2^5$$

zukommt. Daher gibt es sicher ein Potenzprodukt von der Form $x_1^q x_2^p$, $0\leqq p<6$ mit der gleichen Eigenschaft. Wir sehen, dass, wenn Φ_2 nicht durch x_2^6 teilbar ist, es eine Potenz von x_2, x_2^p, $0\leqq p\leqq 5$ geben muss, derart, dass alle Potenzprodukte $x_1^q x_2^p$ zu $\mathfrak{R}$ gehören müssen, sobald q hinreichend gross ist. Da die gleiche Eigenschaft aber dann auch x_2^{p+1}, x_2^{p+2} usw. zukommen muss, müsste dann insbesondere jedes Potenzprodukt $x_1^q x_2^5$ für hinreichend grosse q zu $\mathfrak{R}$ gehören. Gehört aber $x_1^q x_2^5$ für ein ungerades q zu $\mathfrak{R}$, so gilt eine Relation von der Form:

$$x_1^q x_2^5 = F(f_1, f_2, f_3),$$

wo F ein rationalzahliges Polynom in seinen drei Argumenten ist. Ersetzt man aber hier x_1 durch $-x_1$, so ergibt sich

$$x_1^q x_2^5 = -F(f_1, f_2, -f_3) = \frac{1}{2}\big(F(f_1, f_2, f_3) - F(f_1, f_2, -f_3)\big),$$

und hier ist die rechte Seite als Polynom in den drei f-Variabeln durch f_3 teilbar. Dividiert man auf beiden Seiten durch f_3, so ergibt sich eine Relation von der Form:

$$x_1^q x_2^3 = G(f_1, f_2, f_3),$$

wo auch G ein rationalzahliges Polynom in den drei f-Variabeln ist, während für q eine beliebige, hinreichend grosse gerade Zahl angenommen werden kann. Hieraus folgt weiter, wenn man wieder x_1 durch $-x_1$ ersetzt,

$$x_1^q x_2^3 = G(f_1, f_2, f_3) = \frac{1}{2}\big(G(f_1, f_2, f_3) + G(f_1, f_2, -f_3)\big),$$

wo die rechte Seite ein Polynom in f_3^2 ist. Da aber f_2^2, f_3^2 durch x_2^4 teilbar sind, folgt die Kongruenz

$$x_1^q x_2^3 \equiv Q_0(f_1) + Q_1(f_1) f_2 \pmod{x_2^4}.$$

Für $x_2 = 0$ folgt aber hieraus

$$Q_0(x_1^2) = 0,\quad Q_0(f_1) = 0,$$

so dass schliesslich nach dem Taylorschen Satz

$$x_1^q x_2^3 \equiv Q_1(f_1) x_2^2 \equiv Q_1(x_1^2) x_2^2 - Q_1'(x_1^2) x_2^3 \pmod{x_2^4}$$

folgt. Dann muss aber $Q_1(x_1^2) = 0$, $Q_1(f_1) = 0$ sein, so dass nach dem Obigen $x_1^q x_2^3$ durch x_2^4 teilbar wäre.

Wir zeigen nun zweitens, dass es in $\mathfrak{R}$ unendlich viele modulo x_2^6 inkongruente Potenzprodukte gibt, nämlich alle Potenzprodukte von der Form

$$x_1^{2p} x_2^5, \quad p = 0, 1, 2, \ldots$$

Denn, dass alle diese Potenzprodukte dem Ring $\mathfrak{R}$ angehören, folgt aus den Relationen

$$f_3^2 - f_1 f_2^2 = x_2^5,$$

$$x_1^{2p+2} x_2^5 = x_1^{2p} x_2^6 + x_1^{2p} x_2^5 f_1,$$

von denen die zweite den Schluss von p auf $p+1$ rechtfertigt, während die erste den Beweis für $p = 0$ enthält.

23. Im allgemeinen Falle des Satzes XV bilden die Polynome Φ, deren Existenz in ihm behauptet wird, offenbar ein Polynomideal, d. h. eine Gesamtheit von Polynomen mit der Eigenschaft, dass erstens die Summe zweier Polynome aus dieser Gesamtheit wieder zu ihr gehört und zweitens dasselbe für jedes Produkt eines Polynoms dieser Gesamtheit mit einem beliebigen rationalzahligen Polynom in $x_1, \ldots, x_n$ gilt. Dieses Polynomideal wollen wir als das *Führerideal* dieses Ringes bezeichnen.

Das in den Nummern 21 und 22 behandelte Beispiel zeigt nun, dass das Führerideal auch im Falle von mehr als einer Variabel *eingliedrig* sein kann, d. h., dass dieses Ideal aus sämtlichen rationalzahligen Vielfachen eines festen Polynoms-des Führers des Ringes-bestehen kann. Zugleich bildet in unserem Beispiel die Gesamtheit der Restklassen aller Polynome des Ringes nach dem Führer als Modul ein Beispiel eines kommutativen Systems höherer komplexer Zahlen mit abzählbar vielen Einheiten.

Andererseits ist es leicht Beispiele von Ringen des Satzes XV zu konstruiren, für die das Führerideal nicht eingliedrig ist. Das einfachste Beispiel dieser Art wird von derGesamtheit aller rationalzahligen Polynome in x_1, x_2 geliefert, die im Nullpunkt verschwinden. In diesem Falle deckt sich das Führerideal mit dem Ring selbst und seine Basis wird durch x_1, x_2 gebildet.

(Eingegangen am 30. Juli 1934.)

Verschärfung eines Romanoffschen Satzes.

Von

Edmund Landau (Göttingen).

Einleitung.

Lateinische Buchstaben, ausser e, f, o, O, bedeuten ganze Zahlen; die p Primzahlen, die q positive quadratfreie Zahlen, die P positive Weltkonstanten.

In seiner Arbeit *Über einige Sätze der additiven Zahlentheorie* [Mathematische Annalen, Bd. 109 (1934), S. 668—678] bewies Herr Romanoff zwei wichtige Sätze. Ich knüpfe an den zweiten an, der so formuliert werden kann:

Es sei $a > 1$. Dann gibt es ein nur von a abhängiges positives α mit folgender Eigenschaft.

Ist $R(x, a)$ die Anzahl der in der Form $p + a^i$, $i \geqq 0$, darstellbaren Zahlen $\leqq x$ (also 0 für $x < 3$), *so ist*

$$R(x, a) > \alpha x \text{ für } x \geqq 3. \tag{1}$$

Durch genauere Betrachtung der Romanoffschen Methode werde ich α in seiner Abhängigkeit von a mit dem Ergebnis

$$R(x, a) > \frac{x}{P_1 \log a} \text{ für } x \geqq 3 \tag{2}$$

abschätzen.

(2) kommt unerwartet; denn eine bessere Grössenordnung in Bezug auf a gibt es nicht. In der Tat ist $R(x, a)$ für $x \geqq 1$ nicht grösser als die Lösungszahl von

$$p \leqq x, \ a^i \leqq x, \ i \geqq 0,$$

also

$$R(x, a) \leqq \pi(x) \left(\left[\frac{\log x}{\log a} \right] + 1 \right), \tag{3}$$