Irreduzibilitätsproblem bei ganzzahligen Potenzreihen

Von Friedrich Zehlein

Inhaltsverzeichnis

Seite

Einleitung 2

Kapitel I: Vorbereitungen. Irreduzibitätsentscheidung bei Polynomen mit p-adischen Koeffizienten 5

§ 1. Das Polygon eines Polynoms 5

§ 2. Zwei Polygonsätze von M. G. Dumas 6

§ 3. Das geradlinige Polygon 7

§ 4. Bestimmung der Ordnung der Resultante zweier Polynome aus ihrem Polygon 11

Kapitel II: Reduktion der Potenzreihenirreduzibilität auf Irreduzibilität des Normalformenpolynoms . . 12

§ 1. Leitidealzerlegung einer Potenzreihe 12

§ 2. Die Sätze von W. Krull 14

Kapitel III: Das Polygon einer Potenzreihe. 15

§ 1. Vorbereitungen 15

§ 2. Der Hauptsatz 16

Kapitel IV: Die Normalform einer Potenzreihe 17

§ 1. Berechnung des Normalformenpolynoms 17

§ 2. Praktische Handhabe der Methode 19

§ 3. Über die einzelnen Schritte 21

§ 4. Bedingung dafür, daß ein Abschnitt von a_v gleichzeitig Abschnitt von c_{n-v} ist 22

Kapitel V: Irreduzibilitätsentscheidung 23

A. Direkte Irreduzibilitätsentscheidung 23

§ 1. Der Satz von Schoenemann-Eisenstein 24

§ 2. Ein weiterer Satz 24

B. Irreduzibilitätsentscheidung aus dem Hensel'schen Polynom der Reihe 25

C. Singuläre Reihen 25
§ 1. Der Hauptsatz 26
§ 2. Ein Polygonsatz 30
Kapitel VI: Das Zerlegungsproblem 30
§ 1. Zerlegung des Normalformenpolynoms in irrezudible Faktoren 31
§ 2. Überführung der Normalformenteiler in Potenzreihenteiler . . 34

Einleitung.

I. Das Problem ist das folgende: Es sei O die Gesamtheit der formalen oder auch konvergenten Potenzreihen in einer Veränderlichen: $\mathfrak{P}(x) = \sum_{\nu=0}^{\infty} a_\nu x^\nu$, deren Koeffizienten a_ν ganze Zahlen eines endlichen algebraischen Zahlenkörpers K sind. o sei der Koeffizientenbereich. Die Bereiche O und o sind Ordnungen (Integritätsbereiche). Gefragt wird nach den innerhalb O geltenden Teilbarkeitsgesetzen.

In einer in der Mathematischen Zeitschrift erschienenen Arbeit: Zur Arithmetik der Potenzreihen mit ganzzahligen Koeffizienten[1]), hat J. Schur gezeigt, daß in O jedes Hauptideal eindeutig als Produkt von Primidealen darstellbar ist. Eine genaue Charakterisierung der Primidealfaktoren der Hauptideale gibt erst W. Krull[2]). W. Krull beweist, daß die Frage nach dem Primidealcharakter eines Quasihauptideals, d. i. die Klasse derjenigen Ideale, die Faktoren von Hauptidealen sind, auf die Irreduzibilität eines Polynoms zurückgeführt werden kann. Eine kurze, zusammenfassende Darstellung der grundlegenden Gedankengänge und Sätze geben wir, soweit sie für unsere Betrachtung notwendig ist, in Kap. II dieser Arbeit.

II. Es sind noch drei Fragen offen: erstens, wie das einer Reihe $\mathfrak{P}(x)$ zugehörige („Normalformen"-) Polynon P(x) durch ein systematisches Verfahren möglichst einfach berechnet werden kann (Normalformenproblem), zweitens, wann und wie für eine Reihe an Hand dieser Normalform eine Irreduzibilitätsentscheidung mit endlichvielen Schritten getroffen werden kann (Entscheidungsproblem) und drittens, wie bei einer reduziblen Reihe

1) J. Schur: Zur Arithmetik der ganzzahligen Potenzreihen. Math. Zeitschr. Bd. 12. 1922. S. 95.

2) W. Krull: Zur Arithmetik der ganzzahligen Potenzreihen. Journ. f. Math. Bd. 164. 1931.

die irreduziblen Teiler systematisch ermittelt werden können (Zerlegungsproblem).

III. 1. Zur Erledigung des Normalformenproblems dient folgender Ansatz[1]): Zunächst ist bekannt[2]), daß für jede Reihe $\mathfrak{P}(x)$, deren Anfangsglied a_o Produkt zweier verschiedener Primzahlpotenzen $p_1^{\nu_1}$ und $p_2^{\nu_2}$, $(p_1, p_2) = 1$, ist, eine (bis auf eine Einheit) eindeutige Produktzerlegung $\mathfrak{P}(x) = \mathfrak{P}_1(x)\,\mathfrak{P}_2(x)$ existiert, wo $\mathfrak{P}_1(x)$ das Anfangsglied $p_1^{\nu_1}$ und $\mathfrak{P}_2(x)$ das Anfangsglied $p_2^{\nu_2}$ besitzt. Für unsere Untersuchungen bedeutet es daher keine Beschränkung der Allgemeinheit, wenn wir grundsätzlich das Anfangsglied jeder Reihe als Primzahlpotenz voraussetzen.

Um die Normalform einer solchen Reihe zu finden (deren erster durch p nicht teilbarer Koeffizient a_n sei) multiplizieren wir sie mit einer Einheitsreihe $\mathfrak{E}(x) = 1 + \Sigma e_{\nu\tau} p^\nu x^\tau$, deren unbestimmte Koeffizienten $e_{\nu\tau}$ wir so bestimmen, daß die Reihe $\mathfrak{P}(x).\,\mathfrak{E}(x) = P(x)$ in x nur bis zum Grade n ansteigt. (Weierstraßscher Vorbereitungssatz). Wir formulieren den Ansatz gleich so, daß er unmittelbar eine praktisch brauchbare Berechnungsmethode der $e_{\nu\tau}$ liefert, die das Rechnen mit Kongruenzen vollständig umgeht. (Tabellenmethode.) Anschließend können sofort die Reihenglieder a_0, $a_1 x$, ... , $a_l x^l$ abgezählt werden, die notwendig und hinreichend dafür sind, daß alle Normalformenkoeffizienten c_ν bis zu einer angegebenen Potenz p^k vollständig bestimmt sind.

2. a) Bei der Erledigung des Entscheidungsproblems liegt es nahe, die aus der Theorie der p-adischen Polynome bekannten Irreduzibilitätssätze auf P(x) anzuwenden. Die weitgehendsten und vor allem einfachsten Ergebnisse lassen sich hier aus Polygonsätzen von M. G. Dumas[3]) herleiten. Wir können nämlich zeigen, daß erstens das Polygon jeder Reihe stets mit endlichvielen Schritten konstruierbar, und weitergehend zweitens, daß das Polygon jeder Reihe sogar direkt aus der Reihe ablesbar ist. (Hauptsatz.) Damit ist die Irreduzibilitätsentscheidung bei allen Reihen mit gebrochenem Polygon, oder einem solchen

1) Hier Beschränkung auf den Fall rationaler Koeffizienten.

2) J. Schur, § 8, S. 108; W. Krull, § 4, S. 19, Hilfssatz 5.

3) M. G. Dumas: Sur quelques cas d'irréductibilités des polynomes à coefficients rationnels. (Journal de Math. VI, 2. 1906.)

gradlinigen Polygon, bei welchem die Achsenabschnitte ϱ (y-Achse) und n (x-Achse) der Polygongeraden zueinander teilerfremd sind (unter Umgehung des Normalformenpolynoms) direkt an der vorgelegten Reihe möglich.

b) Schwieriger gestaltet sich die Irreduzibilitätsentscheidung bei jenen Reihen, bei welchen die Dumasschen Sätze unmittelbar keine volle Entscheidungsmöglichkeit geben. Es sind das diejenigen Reihen mit einem solchen gradlinigen Polygon, bei denen ϱ zu n nicht teilerfremd ist. Hier nehmen wir den bekannten Henselschen Diskriminantensatz [1]) zu Hilfe. Das Normalformenpolynom muß dann allerdings mod $p^{\delta+1}$ (δ Ordnung der Diskriminante von P(x)) explizit bekannt sein. Es liegen die Verhältnisse dann bei denjenigen Reihen am günstigsten, bei welchen δ direkt aus dem Polygon genau abgelesen (Kap. I, § 4), d. h. bei der Bestimmung von δ jegliche Rechnung vermieden werden kann, ferner bei solchen Reihen, bei welchen der Näherungswert $P^{(\delta)}(x)$ von P(x) direkt aus der Reihe (ohne Rechnung) ablesbar ist und weitergehend vielleicht sogar bezüglich der Irreduzibilitätsentscheidung von $P^{(\delta)}(x)$ unmittelbar eine bestimmte Aussage gemacht werden kann (Kap. V, § 3). $P^{(\delta)}(x)$ nennen wir kurz das „Henselsche Polynom der Reihe".

c) Die bisherigen Betrachtungen lehren: Bei jeder Reihe mit nichtverschwindender Diskriminante kann stets aus einem endlichen Abschnitt der Reihe Aufschluß über den Irreduzibilitätscharakter erhalten werden. Wir fragen jetzt weiter nach der Struktur derjenigen „singulären" Reihen, bei welchen aus keinem einzigen ihrer Abschnitte auf Irreduzibilität bezw. Reduzibilität geschlossen werden kann. Es ergibt sich als Antwort der wichtige Satz: Eine Reihe ist dann und nur dann singulär, wenn sie Potenz einer irreduziblen Reihe ist. (Kap. V, C, § 1.) Weiterhin zeigen wir, daß jede Reihe mit einfachem Polygon und einem nicht durch p-teilbaren Polynomgrad n nichtsingulär ist. (Kap. V, C, § 2.)

3. Bei der Erledigung des Zerlegungsproblems (Kap. VI) geben wir zunächt eine Methode an, welche P(x) schrittweise in teilerfremde Faktoren zerlegen läßt (§ 1) und zeigen dann

---

1) Hensel: Theorie der algebraischen Zahlen, Leipzig und Berlin 1908. S. 68.

(§ 2) wie jeder der so gefundenen Normalformenteiler eindeutig in einen Potenzreihenteiler (Potenzreihe in x mit ganzen Zahlkoeffizienten) übergeführt werden kann.

Kapitel I: Vorbereitungen, Irreduzibilitätsentscheidung bei Polynomen mit p-adischen Koeffizienten.

Vorgegeben sei das Polynom $P(x) = c_0x^n + c_1x^{n-1} + \ldots + c_n$ mit p-adischen Koeffizienten $c_i(p)$. Es sei $c_0 = o(p^{\varrho_0})$, $\not\equiv 0(p^{\varrho_0+1})$ und $c_n = 0\,(p^{\varrho}) \not\equiv 0\,(p^{\varrho+1})$ [1]). Gefragt wird ob P(x) irreduzibel ist.

Im Prinzip ist jederzeit eine bestimmte Entscheidung möglich. Denn bedeutet δ die Ordnung der Diskriminante von P(x), so sagt ein Satz von K. Hensel aus, daß P(x) dann und nur dann in zwei Faktoren $P_1(x)$ und $P_2(x)$ niedrigeren Grades zerfällt, wenn die δ-te Näherung $P^{(\delta)}(x)$ modulo $p^{\delta+1}$ reduzibel ist [2]). Praktisch gestaltet sich bei Zugrundelegung dieses Satzes eine Entscheidung meist recht mühevoll. Denn einerseits muß zunächst die Ordnung δ irgendwie berechnet werden, anderseits ist die Zerlegung von $P^{(\delta)}(x)$ mod. $p^{\delta+1}$ nicht immer leicht durchzuführen, besonders bei großem δ. Es ist so von Wichtigkeit zunächst Methoden nachzugehen, die eventuell δ ohne Rechnung genau bestimmen lassen, und dann weitergehend zweitens auch eine Irreduzibilitätsentscheidung ohne Rechnung (wenigstens bei einer Reihe von Fällen) gestatten. Da unsere späteren Betrachtungen zum Teil wesentlich auf den hier in Betracht kommenden Sätzen fußen, so soll gleich etwas genauer auf sie eingegangen werden.

§ 1. Das Polygon eines Polynoms.

$A^{(\nu,\tau)}x^\nu p^\tau$ $(A^{(\nu,\tau)} \not\equiv 0(p))$ sei irgendein Glied von P(x). In einem rechtwinkligen Koordinatensystem ordnen wir jedem solchen Gliede einen Punkt (ν, τ) zu. Die Gesamtheit dieser Punkte soll das „Diagramm des Polynoms" heißen.

Aus dem Diagramm gewinnen wir einen gradlinigen Streckenzug, das „Polygon des Polynoms" durch folgende Konstruktion:

1) Aus drucktechnischen Gründen müssen wir für: „a kongruent b modulo p" stets schreiben: $a \equiv b(p)$. Entsprechendes für $a \not\equiv b(p)$!

2) K. Hensel: Theorie der algebraischen Zahlen. Teubner, Leipzig und Berlin. 1908. S. 68.

Wir denken uns durch den am weitesten rechts gelegenen Diagrammpunkt, (n, ϱ_0) eine zur Ordinatenachse parallele Gerade solange im Uhrzeigersinn gedreht, bis sie einen ersten Diagrammpunkt trifft; in diesem wird dieselbe Operation ausgeführt, usw. usf. . . .

Nach M. G. Dumas heißt das Polygon gebrochen, wenn es aus mindestens zwei Geraden verschiedener Neigung besteht, sonst heißt es geradlinig[1]). Wir sprechen im folgenden kurz von einer „einfachen Geraden", („nicht einfachen Geraden"), wenn ein geradliniges Polygon außer seinen beiden Endpunkten durch keinen (mindestens einen) Diagrammpunkt geht. Ferner nennen wir ein gebrochenes Polygon „einfach gebrochen", wenn es aus nur einfachen Geraden besteht, „nichteinfach gebrochen", wenn mindestens ein Geradenstück nichteinfach ist.

§ 2. Zwei Polygonsätze von M. G. Dumas.

Wir konstruierten bisher nur das Polygon eines einzigen Polynoms. Das Polygon aus einem Produkt mehrerer Polynome können wir nach dem bisherigen erst konstruieren, wenn das Produkt wirklich explizit ausgerechnet ist.

Es sei nun von jedem Faktor $P_i(x)$ von $P = \prod_{i=1}^{s} P_i(x)$ das Polygon $\mathfrak{P}_i$ bekannt. Wir fragen, ob das Polygon $\mathfrak{P}$ von $P(x)$ etwa direkt aus den $\mathfrak{P}_i$ $(i = 1, 2, \ldots, s)$ ermittelt werden kann; ferner ob und wann umgekehrt das Polygon $\mathfrak{P}$ eines beliebig angegebenen Polynoms $P(x) = \sum_{i=0}^{n} c_i x^{n-i}$ aus Teilpolygonen, $\mathfrak{P}_1$, $\mathfrak{P}_2$ . . ., $\mathfrak{P}_s$ zusammengesetzt gedacht werden darf. Für das Polynom bedeutet dies: Wann läßt das Polygon $\mathfrak{P}$ eines Polynoms $P(x)$ einen Schluß auf die Existenz einer Zerlegung $P(x) = P_1(x) P_2(x) \cdot \ldots \cdot P_s(x)$ zu?

Auf diese grundlegenden Fragen hat M. G. Dumas folgende Antworten gegeben[2]):

---

1) M. G. Dumas: Sur quelques cas d'irréductibilités des polynomes à coefficients rationnels. (Journal de Math. VI, 2. 1906.) 1. Teil, § 2—7 incl.

2) S. 217 und S. 223.

Satz 1: Bei der Multiplikation zweier p-adischer Polynome addieren sich die Polygone vektoriell. („Satz von der Addition der Polygone".)

Satz 2: 1. Jedes p-adische Polynom P(x) mit gebrochenem Polygon ist reduzibel.

2. Jeder Polygonseite S_i entspricht ein Teiler $P_i(x)$, dessen Polygon sich auf eine Gerade von derselben Länge und Neigung wie S_i reduziert.

§ 3. Das geradlinige Polygon.

1. Der Satz von der Addition der Polygone besagt folgendes: Es bestehe das Polygon $\mathfrak{P}_1$ des Polynoms $P_1(x) = \sum_{i=o}^{n_1} c_i^{(1)} x^{n_1 - i} \left(c_o^{(1)} = 0(p^{\varrho_o^{(1)}}), \neq 0(p^{\varrho_o^{(1)}+1}) \right)$ aus den m_1 Geradenstücken $s_1, s_2, \ldots\ldots s_{m_1}$ und das Polygon $\mathfrak{P}_2$ des Polynoms $P_2(x) = \sum_{i=o}^{n_2} c_i^{(2)} x^{n_2 - i} \left(c_o^{(2)} = 0(p^{\varrho_o^{(2)}}), \neq 0(p^{\varrho_o^{(2)}+1}) \right)$ aus den m_2 Geradenstücken $s'_1, s'_2, \ldots\ldots s'_{m_2}$. Wir ordnen die s_i und s'_i nach wachsenden Neigungen; die erhaltene Reihe sei $S_1, S_2, \ldots\ldots, S_{m_1+m_2}$.

Dann behauptet der Satz: Um das Polygon $\mathfrak{P}$ des Produktes $P(x) = P_1(x)P_2(x)$ zu erhalten, braucht man, vom Punkte $A = (n_1 + n_2, \varrho_o^{(1)} + \varrho_o^{(2)})$ als dem am weitesten rechts gelegenen Diagrammpunkt von P(x), ausgehend, nur die S_i $(i = 1, 2, \ldots, m_1 + m_2)$ aneinanderzureihen. (Streckenzug A, E_1, E_2 . . . .).

2. Wir betrachten jetzt den Fall, daß die S_i $(i = 1, 2, \ldots, m)$ lauter Geradenstücke gleicher Neigung sind. Der durch Aneinanderreihung der S_i erhaltene Streckenzug ist eine einfache Gerade G von derselben Neigung wie jedes der S_i. Die $m-1$ Punkte E_i, in welchen S_i und S_{i+1} zusammenstoßen, sollen kurz „Nahtpunkte" heißen.

Das Polygon $\mathfrak{P}$ des Polynoms $P(x) = \prod_{i=1}^{m} P_i(x)$ ist nicht notwendig mit G identisch; genauer: $\mathfrak{P}$ ist zwar eine Gerade von derselben Neigung und Länge wie G, aber $\mathfrak{P}$ braucht nicht notwendig die $m-1$ Nahtpunkte E_i zu tragen. Wäre das nämlich z. B. der Fall, so folgte, daß das Polynom eines jeden einfachen Polygons irreduzibel ist; im Falle der Reduzibilität

müßte es ja sonst mindestens einen Nahtpunkt besitzen. Daß einer einfachen Geraden aber wirklich ein reduzibles Polynom entsprechen kann, zeigt schon das Beispiel des Polynoms $P(x) = (x + p)^p$. Hier sind die Polygone S_i der Polynome $P_i = x + p$ alle einfach und von gleicher Neigung, $\mathfrak{P}$ trägt aber keinen der etwa erwarteten Nahtpunkte $(p-1, 1)$, $(p-2,2)$, ..., $(1, p-1)$, sondern ist vielmehr einfach. Das Beispiel $P(x) = (x + p)(x + (p-1)p)$ lehrt, daß der gleiche Sachverhalt

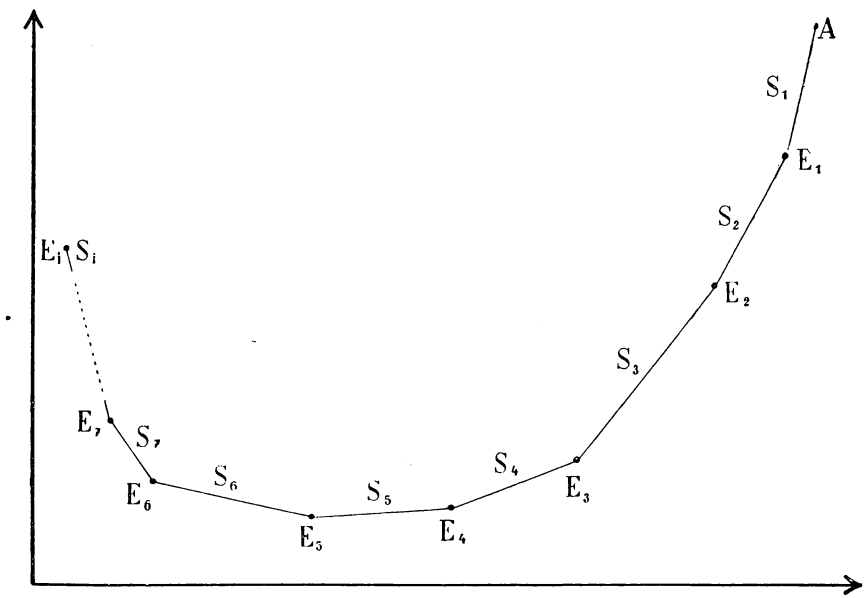

Fig. 1.

auch möglich ist, wenn die $P_i(x)$ voneinander verschieden sind, und schließlich zeigt das einfache Polygon des Polynoms $P(x) = (x+3)(x^2 + 2 \cdot 3x + 1 \cdot 3^2) = x^3 + 3^2x^2 + 3^3x + 3^3$, daß im Produktpolynom $\mathfrak{P}$ sogar ein Nahtpunkt eines Teilpolynoms verschwinden kann.

3. Die Existenz bezw. Nicht-Existenz von Nahtpunkten in einem geradlinigen Polygon läßt also nicht ohne weiteres auf Reduzibilität bezw. Irreduzibilität schließen. Eine unmittelbare Irreduzibilitätsaussage im Falle eines geradlinigen Polygons erlaubt nur folgender

Satz 1: Das Polynom P(x) ist irreduzibel, wenn sein Polygon eine einfache Gerade mit teilerfremden Achsenabschnitten ist.

Beweis: Sei $P(x) = x^n + \sum_{i=1}^{n} c_i x^{n-i}$, $c_n = 0(p^\varrho)$, $\neq 0(p^{\varrho+1})$ und das Polygon $\mathfrak{P}$ von P(x) geradlinig [1]). Anfangspunkt von $\mathfrak{P}$ ist der Punkt $E^{(n)} = (n, o)$, Endpunkt der Punkt $E^{(\varrho)} = (0, \varrho)$.

Es sei P(x) reduzibel, also $P(x) = P_1(x)P_2(x)$,

$$P_1(x) = x^{n_1} + \sum_{i=1}^{n_1} a_i x^{n_1-i},\quad a_{n_1} = 0(p^{\varrho_1}),\ \neq 0(p^{\varrho_1+1}),$$

$$P_2(x) = x^{n_2} + \sum_{i=1}^{n_2} b_i x^{n_2-i},\quad b_{n_2} = 0(p^{\varrho_2}),\ \neq 0(p^{\varrho_2+1}).$$

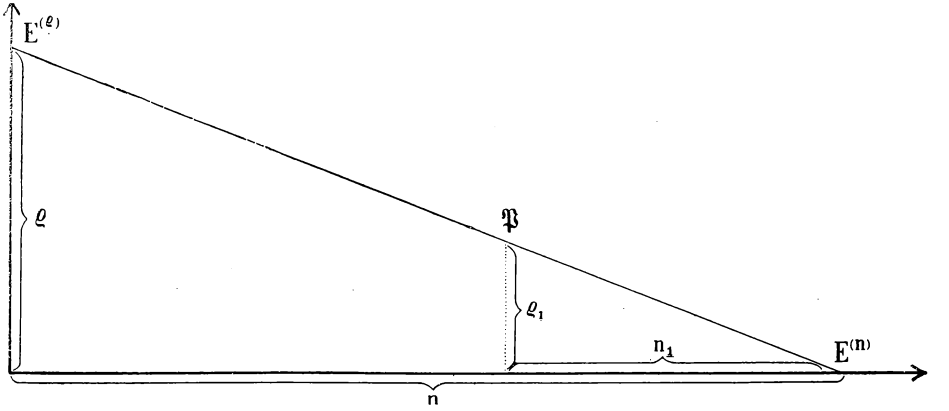

Fig. 2.

Dann muß $n_1 : n_2 = \varrho_1 : \varrho_2$ sein, weil andernfalls $\mathfrak{P}$ ja gebrochen wäre. Nun gibt es aber keine ganzen Zahlen ϱ_1 und n_1, die kleiner ϱ bezw. n sind, sodaß $\varrho : n = \varrho_1 : n_1$ für $(\varrho, n) = 1$. Also kann P(x) nicht reduzibel sein.

In Verallgemeinerung von Satz 1 ergibt sich unmittelbar

Satz 2: Besitzt das Polynom P(x) ein geradliniges Polygon $\mathfrak{P} = \{(0,\varrho); (n,0)\}$ und ist $\varrho = A\varrho_0$, $n = An_0$, $A \neq 1$, $(\varrho_0, n_0) = 1$, so ist (falls P(x) reduzibel ist) jeder Teiler von P(x) vom Grade $i \cdot n_0$, wo i eine Zahl aus der Reihe 1, 2, ..., A − 1 ist.

6. Für später ist von Wichtigkeit

---

1) Von hier ab wird immer $c_0 = 1$ angenommen.

Satz 3: Jedes Polynom P(x), welches r-te Potenz eines Polynoms $P_0(x)$ mit geradlinigem Polygon ist, besitzt ein nicht einfaches Polygon, wenn $r \nmid 0(p)$.

Beweis: Sei $P_0(x) = x^s + c_1 x^{s-1} + \ldots + c_s$, $c_s = 0(p^\varrho)$, $\nmid 0(p^{\varrho+1})$; $c_i = 0(p^{\varrho i})$, $\nmid 0(p^{\varrho i+1})$, $P(x) = x^{r\cdot s} + C_1 x^{rs-1} + \ldots$ $\ldots + C_s$, $\mathfrak{P}_0$ Polygon von $P_0(x)$, $\mathfrak{P}$ das von P(x).

1. $\mathfrak{P}_0$ sei einfach. Wir zeigen: In P(x) ist der Koeffizient $C_{(r-1)s}$ von x^s von der Gestalt: $r \cdot c_s^{r-1} + C$ wo $C = 0(p^{(r-1)\varrho+1})$. Daraus folgt dann: $\mathfrak{P}$ besitzt den Nahtpunkt $(s, (r-1)\varrho)$, wenn $r \nmid 0(p)$.

Wir setzen $c_i x^{s-i} = y_i$ $(i = 0, 1, 2, \ldots, s)$, $c_0 = 1$. Dann ist

$$(x^s + \ldots + c_s)^r = \Big(\sum_{i=0}^{s} y_i\Big)^r = \sum \frac{r!}{\tau_0!\,\tau_1!\ldots\tau_s!}\, y_0^{\tau_0}\, y_1^{\tau_1} \ldots y_s^{\tau_s},$$

wobei das Summenzeichen bedeutet, daß über alle r-tupel $\tau_0, \tau_1, \ldots, \tau_s$ von natürlichen Zahlen zu summieren ist, deren Summe r ergibt (polynomischer Satz). $\tau_0 = 1$, $\tau_1 = \tau_2 = \ldots$ $\tau_{s-1} = 0$, $\tau_s = r-1$ führt auf $\dfrac{r!}{(r-1)!}\, x^s\, c_s^{r-1} = r\, c_s^{r-1}\, x^s$. Die Summe C aller übrigen Glieder von $C_{(r-1)s}$ wird folgendermaßen gefunden: Sei i^* beliebig und $1 \leqq i^* < s$. Wir setzen $\tau_{i^*} = 1$ und $\tau_{s-i_\nu} = 1$ $(\nu = 1, 2, \ldots, k)$ für alle i_ν-Kombinationen der Eigenschaft: $\sum_\nu i_\nu = i^*$, schließlich $\tau_s = r - k - 1$ und alle übrigen $\tau_i = 0$. Dann ist $\prod_{i=0}^{s} y_i = x^s [c_{i^*} (\prod_{\nu=1}^{k} c_{s-i_\nu}) c_s^{r-k-1}]$, also

$$C = \sum_{i^*} [c_{i^*}\, c_s^{r-k-1} \prod_{\nu=1}^{k} c_{s-i_\nu}]\ ^1).$$

Um die kleinstmögliche p-Potenz zu finden, die in C aufgeht, beachten wir, daß $\varrho_i = \frac{\varrho \cdot i}{s} + r_i$, wo alle $r_i > 0$. (Vgl. Fig. 3.)

Aus $(\frac{\varrho \cdot i^*}{s} + r_{i^*}) + \varrho\,(r - k - 1) + \sum_{\nu=1}^{k} (\frac{\varrho s - i_\nu)}{s} + r_{s-i_\nu}) =$ $\varrho(r-1) + r_{i^*} + \sum_{\nu=1}^{k} r_{s-i_\nu}$ folgt unmittelbar die Behauptung.

---

1) Der für die Betrachtung belanglose Binomialkoeffizient ist dabei nicht berücksichtigt.

2. $\mathfrak{P}_0$ habe Nahpunkte Zunächst überlegt man, daß der zur Abszisse s gehörige Punkt bei $\mathfrak{P}$ jetzt nicht mehr notwendig Nahtpunkt sein muß. Beispiel: $(x^2 + 3x + 3^2)^2 = x^4 + 2\cdot 3x^3 + 3^3x^2 + 2\cdot 3x + 3^4$.

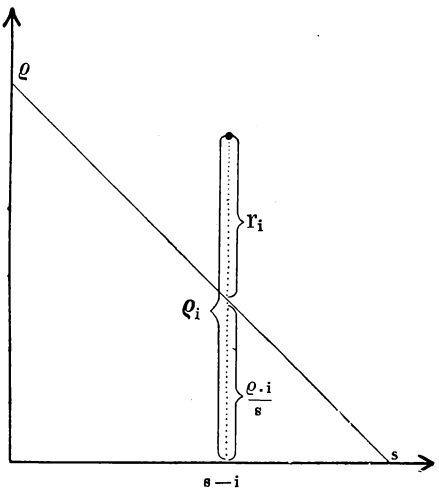

Fig. 3.

Es erzeuge das Glied $c_{s-i_1} x^{i_1}$ den ersten (gerechnet von $(0, \varrho)$ aus) Nahtpunkt von $\mathfrak{P}_0$. ($c_{s-i_1} = 0 (p^{\varrho i_1})$, $\neq (p^{\varrho i_1 + 1})$; $\varrho_{i_1} = \frac{\varrho(s-i_1)}{s}$). Wir zeigen: In $P_0^r(x)$ ist der Koeffizient von x^{i_1} durch $p^{\varrho(r-1)+\varrho_{i_1}}$, aber nicht durch $p^{\varrho(r-1)+\varrho_{i_1}+1}$ teilbar. Das besagt wieder, daß der Punkt $(i_1, \varrho(r-1) + \varrho_{i_1})$ Nahtpunkt von $\mathfrak{P}$ ist.

Für $\tau_{s-i_1} = 1$, $\tau_s = r-1$ und alle übrigen $\tau_i = 0$ wird erhalten $\frac{r!}{(r-1)!} c_{s-i_1} x^{i_1} c_s^{r-1} = r c_s^{r-1} c_{s-i_1} x^{i_1}$.

Die übrigen Glieder des Koeffizienten von x^{i_1} werden für folgende τ-Werte erhalten: i^* beliebig, $\neq i_1$. $\tau_{s-(i_1 - i^*)} = 1$, $\tau_{s-i_\nu} = 1$, für alle i_ν-Kombinationen der Eigenschaft $\sum_\nu i_\nu = i^*$ ($\nu = 0, 2, \ldots, k$), $\tau_s = r - k - 1$ und alle übrigen $\tau_i = 0$. Dann ist

$$C = \sum_{i^*} [c_{s-(i_1 - i^*)} c_s^{r-k-1} \prod_{\nu=0}^{k} c_{s-i_\nu}].$$

Aus $\frac{\varrho(s-i_1+i^*)}{s} + r_{s-(i_1-i^*)} + \varrho(r-k-1) + \sum_\nu (\frac{\varrho(s-i_\nu)}{s} + r_{s-i_\nu})$ $= \frac{\varrho(s-i_1)}{s} + \varrho(r-1) + \Sigma r$ folgt wiederum direkt die Behauptung. ($\Sigma r > 0$.) [1])

§ 4. Bestimmung der Ordnung der Resultante zweier Polynome aus ihrem Polygon. [2])

I. Satz I: Vor. Seien $P(x) = x^n + \sum_{i=1}^{n} c_i x^{n-i}$ und

1) Der Satz läßt sich übrigens auch anschaulich sehr durchsichtig beweisen. — Andere Berechnung der C_ν etwa durch v-fache Differentiation.

2) Dumas, S. 246, § 11.

$Q(x) = x^{n'} + \sum_{i=1}^{n'} c'_i x^{n'-i}$, $c_n = 0(p^{\varrho})$, $\not\equiv 0(p^{\varrho+1})$, $c_{n'} = 0(p^{\varrho'})$, $\not\equiv 0(p^{\varrho'+1})$ zwei Polynome mit geradlinigen Polygonen $\mathfrak{P}$ und $\mathfrak{Q}$. Ferner sei $\varrho = A\varrho_0$, $n = An_0$; $\varrho' = A'\varrho'_0$, $n' = A'n'_0$, $(\varrho_0, n_0) = (\varrho'_0, n'_0) = 1$ und es bedeute $R(P, Q)$ die Resultante der beiden Polynome.

Beh. 1. Es ist $R(P, Q) = 0(p^{\varrho n'})$, $\not\equiv (p^{\varrho n'+1})$ wenn $\frac{\varrho'_0}{n'_0} > \frac{\varrho_0}{n_0}$.

2. Ist $\frac{\varrho_0}{n_0} = \frac{\varrho'_0}{n'_0}$, so ist $R(P, Q)$ mindestens durch $p^{\varrho n'}$ teilbar, jedoch kann die Ordnung r von R auch größer sein.

II. Um in diesem zweiten Falle zu entscheiden ob $r > \varrho n'$ ist, muß man in $P(x)$ und $Q(x)$ die Substitution $x = yp^{\frac{\varrho_0}{n_0}}$ machen. In den so erhaltenen Polynomen $P(y)$ und $Q(y)$ scheide man die größtmögliche p-Potenz aus, die erhaltenen Polynome seien $P_1(y)$ und $Q_1(y)$.

Ist die Resultante $R(P_1, Q_1)$ durch p teilbar, so ist $r > \varrho n'$, und zwar gilt:

$$R(P(x), Q(x)) = p^{\varrho n'} R(P_1(y), Q_1(y)).$$

Um zu entscheiden ob $R(P_1, Q_1) = o(p)$, bildet man aus den von $p^{\frac{1}{n_0}}$ unabhängigen Gliedern von $P_1(y)$ und $Q_1(y)$ zwei ganzzahlige Polynome $\overline{P}_1(y)$ und $\overline{Q}_1(y)$. Wenn $R(\overline{P}_1, \overline{Q}_1) = 0(p)$, dann ist auch $R(P_1, Q_1) = 0(p)$. Die Ordnung r_1 von $R(P_1, Q_1)$ läßt sich durch Ausrechnung bestimmen. Dazu müssen natürlich in $P_1(y)$ und $Q_1(y)$ auch die Glieder der niedrigsten p-Potenzen in Betracht gezogen werden. Dann ist $r = \varrho n' + r_1$ [1]).

Kapitel II. **Reduktion der Potenzreihenirreduzibilität auf Irreduzibilität des Normalformenpolynoms.**

§ 1. Leitidealzerlegung einer Potenzreihe.

1. Sei O der Bereich aller Potenzreihen in x mit Koeffizienten aus der Hauptordnung o eines endlichen algebraischen Zahlkörpers K. Jedes ganze Ideal aus O, welches sich als Produkt

1) Anwendung § 2 Kap. V.

eines ganzen Hauptideals von O mit einem ganzen oder gebrochenen Ideal von o darstellen läßt, nennen wir mit W. Krull[1]) Quasihauptideal.

Sei $\mathfrak{A}$ ein beliebiges Quasihauptideal aus O. Die Gesamtheit der Elemente aus o, die Anfangsglieder der Reihen von $\mathfrak{A}$ sind, bilden ein Ideal $\mathfrak{a}$ aus o. (Leitideal $\mathfrak{a}$ von $\mathfrak{A}$)[2]). Wir zerlegen $\mathfrak{a}$ in Potenzen teilerfremder Primideale; es sei dann $\mathfrak{a} = \mathfrak{p}_1^{r_1}\,\mathfrak{p}_2^{r_2} \ldots\ldots\ldots \mathfrak{p}_s^{r_s}$, $(\mathfrak{p}_i, \mathfrak{p}_k) = 1$, $i \neq k$. Aus dieser Zerlegung von $\mathfrak{a}$ kann sofort eine eindeutig bestimmte Zerlegung von $\mathfrak{A}$ hergeleitet werden. Es gilt:

Satz: Vor. $\mathfrak{A}$ sei ein beliebiges Quasihauptideal aus O, $\mathfrak{a}$ sei das Leitideal von $\mathfrak{A}$, und es sei $\mathfrak{a} = \mathfrak{p}_1^{r_1} \ldots \mathfrak{p}_s^{r_s}$.

Beh. Für $\mathfrak{A}$ existiert eine eindeutig bestimmte Produktzerlegung $\mathfrak{A} = \mathfrak{A}_1\,\mathfrak{A}_2 \ldots \mathfrak{A}_s$, wobei $\mathfrak{A}_i$ Quasihauptideal ist und gerade das Leitideal $\mathfrak{p}_i^{r_i}$ besitzt[3]). (Leitidealsatz.)

2. Zur Konstruktion der „Leitidealzerlegung" eines beliebigen Quasihauptideals dient ein Ansatz von J. Schur[4]): Wir setzen $\mathfrak{a}_1 = \mathfrak{p}_1^{r_1}$, $\mathfrak{b} = \prod_{\nu=2}^{s} \mathfrak{p}_\nu^{r_\nu}$; wir bestimmen in K zwei ganze Zahlen α und β so, daß α durch $\mathfrak{a}_1$, aber nicht durch $\mathfrak{p}^{r_1+1}$, β durch $\mathfrak{b}$ jedoch nicht durch $\mathfrak{p}_\nu^{r_\nu+1}$ $(\nu = 2,3 \ldots, s)$ teilbar wird. $z_1 = (\mathfrak{p}_1^{r_1})\,\mathfrak{m}$, $z_2 = (\prod_{\nu=2}^{s} \mathfrak{p}_\nu^{r_\nu})\,\mathfrak{n}$ $(\varrho_\nu \geqq r_\nu)$ seien zwei durch $\mathfrak{a}$ teilbare ganze Zahlen von K; dabei soll $\mathfrak{m} = \mathfrak{o}$ $(\mathfrak{b})$, $\mathfrak{n} = \mathfrak{o}$ $(\mathfrak{a}_1)$; $(\mathfrak{n}, \mathfrak{b}) = (\mathfrak{m}, \mathfrak{a}_1) = (1)$ sein. Nun wird α_1 so gewählt, daß $\alpha_1 = \alpha$ $(\mathfrak{a}_1^2)$, $\alpha_1 = 1\,(\mathfrak{m})$; dann wird $\mathfrak{a}_1 = (z_1, \alpha_1)$ und es ist α_1 zu $\mathfrak{b}$ teilerfremd, weil $\mathfrak{b}$ ein Teiler von $\mathfrak{m}$ ist. Daher kann β_1 so bestimmt werden, daß $\beta_1 = \beta\,(\mathfrak{b}^2)$, $\beta_1 = 1$ $(\alpha_1 \cdot \mathfrak{n})$ und es ist $\mathfrak{b} = (z_2, \beta_1)$, wobei α_1 und β_1 keinen Idealteiler gemeinsam haben. z_1, z_2 und $\alpha_1\,\beta_1$ sind in $\mathfrak{a}$ enthalten; daher können in $\mathfrak{A}$ drei Potenzreihen

$$\mathfrak{P}_i = z_i + \sum_{\nu=1}^{\infty} z_\nu^{(i)} x^\nu \;(i = 1, 2), \qquad \mathfrak{P}_3 = \alpha_1\,\beta_1 + \sum_{\nu=1}^{\infty} z_\nu^{(3)} x^\nu$$

---

1) Krull, S. 17, § 3.
2) Schur, S. 37, § 1; Krull, S. 19, § 4.
3) Schur, S. 108, § 8; Krull, S. 19, § 4, Hilfssatz 5.
4) Schur, S. 109.

angegeben werden. Wir setzen nun an:

$$\mathfrak{P}_3^{(1)} = \alpha_1 + \alpha_1^{(1)} x + \ldots; \quad \mathfrak{P}_3^{(2)} = \beta_1 + \beta_1^{(1)} x + \ldots,$$

und bestimmen die $\alpha_\nu^{(1)}$, $\beta_\nu^{(1)}$, $\nu = 1, 2, \ldots\ldots$ in K (ganzzahlig) so, daß $\mathfrak{P}_3 = \mathfrak{P}_3^{(1)} \mathfrak{P}_3^{(2)}$ wird. Dies ist stets möglich, weil wegen $(\alpha_1, \beta_1) = (1)$ sämtliche Gleichungen

$$\alpha_1 \beta_1^{(1)} + \beta_1 \alpha_1^{(1)} = z_1^{(3)}$$
$$\alpha_1 \beta_2^{(1)} + \beta_1 \alpha_2^{(1)} = z_2^{(3)} - \alpha_1^{(1)} \beta_1^{(1)}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

schrittweise erfüllbar sind. Die beiden Ideale $\mathfrak{A}_1 = (\mathfrak{P}_1, \mathfrak{P}_3^{(1)})$, $\mathfrak{B} = (\mathfrak{P}_2, \mathfrak{P}_3^{(2)})$ — $\mathfrak{A} = \mathfrak{A}_1 \cdot \mathfrak{B}$! — haben dann die Leitideale $\mathfrak{a}_1 = \mathfrak{p}_1^{r_1}$ bezw. $\mathfrak{b} = \prod_{\nu=2}^{s} \mathfrak{p}_\nu^{r_\nu}$.

§ 2. Die Sätze von W. Krull.

Auf Grund des Leitidealsatzes brauchen in O nur solche Ideale $\mathfrak{A}^*$ betrachtet werden, deren Leitideal gleich einer bestimmten, etwa der r-ten Potenz eines Primideals $\mathfrak{p}$ ist. Es bedeute $\mathfrak{P}(x)$ jetzt immer eine Reihe aus $\mathfrak{A}^*$, deren Anfangsglied durch $\mathfrak{p}^r$ aber nicht durch $\mathfrak{p}^{r+1}$ teilbar ist.

Für die Irreduzibilitätsentscheidung von $\mathfrak{P}(x)$ ist die naheliegendste Frage die, ob $\mathfrak{P}(x)$ auf eine möglichst einfache Form gebracht werden kann, genauer, ob für $\mathfrak{P}(x)$ eine eindeutig bestimmte „Normalform" existiert. Hier führen folgende Überlegungen zum Ziel.

1. In dem zu o gehörigen Ring von π-adischen Zahlen ist p gleich einer Potenz eines Primelementes π. Durch π-adische Entwicklung sämtlicher Koeffizienten von $\mathfrak{P}(x)$ kommen wir zu den Bereichen o_π und O_π. Entscheidend ist nun zunächst, daß jede Reihe $\mathfrak{P}(x) = \pi^\varrho + \sum_{\nu=1}^{\infty} a_\nu x^\nu$, $(a_\nu = \alpha_{\nu_i} \pi^{\nu_i} + \ldots\ldots; \alpha_{\nu_i} \not\equiv 0 (p)$; alle α_{ν_i} aus einem Restsystem mod π) durch Multiplikation mit einem eindeutig bestimmten Einheitsfaktor $\mathfrak{E}(x)$ so normiert werden kann, daß sie in der Variablen x Polynomform annimmt. Dieses Polynom P(x) („Weierstraßsche Normalform von $\mathfrak{P}(x)$") hat die Eigenschaft, daß der Koeffizient der höchsten x-Potenz gleich Eins ist und daß alle übrigen Koeffizienten c_ν durch π teilbar sind. Existenz und Eindeutigkeit von P(x) ergibt sich auch in dieser Arbeit bei Angabe eines Verfahrens zur Berechnung von P(x). (Kap. IV, § 1.)

2. Grundlegend ist weiterhin folgendes: W. Krull zeigte: Das Irreduzibilitätsproblem der Reihe $\mathfrak{P}(x)$ erledigt sich vollkommen an der Normalform $P(x)$; die irreduziblen Teiler $P_i(x)$ von $P(x)$ und die irreduziblen Teiler $\mathfrak{P}_i(x)$ von $\mathfrak{P}(x)$ entsprechen einander umkehrbar eindeutig. Es gilt nämlich[1]):

Satz 1: Jede durch π unteilbare Potenzreihe aus O_π ist einer einzigen Weierstraßschen Normalform äquivalent (Weierstraßscher Vorbereitungssatz).

Satz 2: 1. In O_π läßt sich jedes Element eindeutig als Produkt von Primelementen darstellen.

2. Eine durch π unteilbare Reihe aus O_π ist dann und nur dann Primelement, wenn ihre zugehörige Weierstraßsche Normalform als Polynom im Koeffizientenring O_π irreduzibel ist.

3. Die Zerlegungen in O_π und O sind einander äquivalent.

Kapitel III: **Das Polygon einer Potenzreihe.**

§ 1. Vorbereitungen.

Ziel der folgenden Betrachtungen ist, in Anwendung der Sätze des Kapitel I, an Hand von $P(x)$ Polygonkriterien für $\mathfrak{P}(x)$ im p-adischen Bereich zu gewinnen.

1. Sei $\mathfrak{P}(x) = p^\varrho + \Sigma a_\nu x^\nu$ eine beliebige Reihe $a_\nu = o(p)$, $\nu = 1, 2, \ldots, n-1$, $a_n \not\equiv o(p)$. In § 1 des nächsten Kapitel zeigen wir: $P(x)$ ist stets vom Grade n. $(P(x) = x^n + \sum_{\nu=1}^{n} c_\nu x^{\nu^{n-\nu}})$. Daraus folgt: Bei jeder Reihe können Diagrammpunkte nur auf den zur Koordinatenachse parallelen Graden im Abstande o, 1, 2, ..., n—1 liegen, ferner besitzen alle Diagrammpunkte nur positive Ordinaten. Der am weitesten rechts gelegene Diagrammpunkt ist der Punkt $E^{(n)} = (n, o)$; er ist nach § 1, Kap. I der Ausgangspunkt für die Konstruktion des Polygons. Endpunkt wird dann der Punkt $E^{(\varrho)} = (o, \varrho)$. Das besagt: Anfangs- und Endpunkt des Polygons können stets direkt aus der Reihe abgelesen werden.

2. Man sieht unmittelbar, daß derselbe Streckenzug erhalten wird, wenn statt vom Punkte $E^{(n)}$ vom Punkte $E^{(\varrho)}$ aus-

1) W. Krull, S. 15, § 2, S. 16, § 2 (Satz 1).

gegangen und um ihn eine in der Ordinatenachse liegende Gerade solange entgegen dem Uhrzeigersinn gedacht wird, bis sie einen ersten Diagrammpunkt trifft; usw. usf. Endpunkt wird dann der Punkt $E^{(n)}$.

Das Polygon auf diese Weise entstanden zu denken ist für die folgenden Betrachtungen zweckmäßig. Denn hierbei durchlaufen wir bei der Konstruktion des Polygons die Reihe vom Anfangsgliede an gliedweise.

3. Die c_ν können aus den a_ν als Potenzreihen in p schrittweise berechnet werden. Zur Konstruktion des Polygons braucht man von dem Diagramm offenbar nur jeweils den tiefsten Punkt auf $x = 1$, $x = 2$, . . ., $x = n - 1$. Diese Punkte werden durch das Anfangsglied der c_ν ($\nu = 1, 2, \ldots, n-1$) geliefert; alle weiteren Glieder von c_ν sind nämlich durch höhere p-Potenzen teilbar (Kap. IV). Das Anfangsglied eines jeden c_ν ist mit endlich vielen Schritten bestimmbar. Daraus folgt: Das Polygon einer jeden Potenzreihe kann mit endlich vielen Schritten konstruiert werden.

§ 2. Der Hauptsatz.

Satz: Das Polygon jeder Reihe kann stets direkt aus den in den Reihenkoeffizienten a_ν ($\nu = 0, 1, \ldots, n$) aufgehenden p-Potenzen abgelesen werden.

Beweis: Wir tragen die durch die Anfangs-p-Potenzen p^{i_ν} der a_ν ($\nu = 0, 1, \ldots, n$) bestimmten Punkte (ν, i_ν) („a-Punkt") ins Koordinatensystem ein und konstruieren daraus das Polygon $\mathfrak{P}^*$ der a_ν. $\mathfrak{P}$ sei das Polygon der c_ν. Wir behaupten: $\mathfrak{P} = \mathfrak{P}^*$.

$\mathfrak{P}(x)$ und $P(x)$ sind in O_p einander äquivalent. Wegen der Symmetrie der Äquivalenz ($\mathfrak{P}(x)\ \mathfrak{E}(x) = P(x)$, $P(x)\ \mathfrak{E}^{-1}(x) = \mathfrak{P}(x)$ ($\mathfrak{E}(x) = \Sigma e_\nu x^\nu$) braucht nur gezeigt zu werden: $\mathfrak{P}$ liegt nicht tiefer als $\mathfrak{P}^*$. Dazu müssen wir zeigen: Jedes c_ν, dessen Anfangs-p-Potenz einen Punkt von $\mathfrak{P}$ liefert, beginnt mit keiner niedrigeren p-Potenz als $a_{n-\nu}$.

Sei $A^*_{n-\nu^*}$ irgendein Punkt auf $\mathfrak{P}^*$ (also entweder Eckpunkt E^* oder Nahtpunkt N^*). $A^*_{n-\nu^*}$ werde durch das Glied $a_{n-\nu^*}\, x^{n-\nu^*}$ von $\mathfrak{P}(x)$ geliefert. ($0 < \nu^* < n$; $a_{n-\nu^*} = o(p^{i_{n-\nu^*}})$, $\neq o\,(p^{i_{n-\nu^*}+1})$).

Gemäß der Konstruktion von $\mathfrak{P}^*$ ist $A^*_{n-\nu^*}$ der erste Punkt mit einer Ordinate $i_{n-\nu^*}$; alle vor ihm (links) gelegenen a-Punkte besitzen eine größere Ordinate.

Angenommen der c-Punkt $A_{n-\nu^*}$ (mit der Abszisse $n-\nu^*$) liege tiefer als $A^*{}_{n-\nu^*}$. Dann müßte die Anfangs-p-Potenz von c_{ν^*} um mindestens Eins kleiner sein als die von $a_{n-\nu^*}$. Damit beim Übergang vom a-Diagramm zum c-Diagramm eine solche Exponentenerniedrigung möglich wäre, müßte $c_{\nu^*} = a_{n-\nu^*} e_o + a_{n-\nu^*-1} e_1 + \ldots\ldots + a_o e_{n-\nu^*}$ mindestens ein Glied haben, das durch keine höhere Potenz als $p^{i_{n-\nu^*}-1}$ teilbar wäre. Dies wiederum wäre aber — geometrisch gesprochen — nur möglich, wenn sich vor (links von) $A^*_{n-\nu^*}$ mindestens ein a-Punkt von geringerer Ordinate als $i_{n-\nu^*}$ fände. Die Existenz eines solchen Punktes widerspräche aber der Voraussetzung, daß $A^*_{n-\nu^*}$ der erste Punkt mit einer Ordinate $i_{n-\nu^*}$ ist, bezw. daß alle vor $A^*_{n-\nu^*}$ gelegenen a-Punkte eine größere Ordinate als $i_{n-\nu^*}$ haben. $(a_k = o\,(p^{i_{n-\nu^*}+1}),\ k = 0, 1, \ldots,\ n-\nu^*-1)$.

Kapitel IV: **Die Normalform einer Potenzreihe.**

§ 1. Berechnung des Normalformenpolynoms.

1. Wir entwickeln in $\mathfrak{P}(x) = p^o + \sum_{\nu=1}^{\infty} a_\nu x^\nu$ jeden Koeffizienten nach Potenzen von p. Demgemäß sei

$a_\nu = \alpha_{i_\nu} p^{i_\nu} + \ldots\ldots + \alpha_{N_\nu} p^{N_\nu} (\alpha_{i_\nu} \neq 0)$.

Ferner sei $a_n \not\equiv o\,(p)$ und alle $a_\nu = o\,(p)$ für $\nu < n$.

Die Reihe $\mathfrak{P}(x)$ ordnen wir jetzt nach Formen steigender Dimension in x und p. Sie erscheint dann in der Gestalt:

$$\mathfrak{P}(x) = \sum_{\nu=m}^{\infty} \varphi_\nu\,(x, p);$$

$$\varphi_{m+\nu}(x,p) = A_{m+\nu,o}\, x^{m+\nu} + A_{m+\nu-1,1}\, x^{m+\nu-1} p + \ldots + A_{o,\,m+\nu}\, p^{m+\nu}.$$

Dabei bedeutet m die niederste Dimension; alle Koeffizienten $A_{\nu,\tau}$ sind aus dem Restsystem $\{o, 1, \ldots, p-1\}$.

2. Besitzt die Form $\varphi_m\,(x, p)$ ein von p freies Glied $A_{m,o}\, x^m$, $A_{m,o} \not\equiv o\,(p)$, so heißen wir die Reihe regulär. Es bedeutet keine Beschränkung der Allgemeinheit jede Reihe als regulär von der Dimension $m = n$ vorauszusetzen. — Denn Regularität

läßt sich durch die Substitution $p = t^r (r > 1)$ erzwingen. Dabei hat diese Transformation nur die formale Bedeutung, daß man p ein anderes „Gewicht“ erteilt als x, erfordert aber nicht etwa die Adjunktion von $t = \sqrt[r]{p}$. r ist eindeutig festgelegt als kleinster Exponent, der hinreicht alle Reihenglieder formal mit einer Dimension $\geqq n$ zu versehen.

3. Wir dürfen ferner stets $A_{n,o} = 1$, also $a_n = 1 + \alpha_{\nu_1} p^{\nu_1} + \ldots\ldots + \alpha_{\nu_N} p^{\nu_N}$, voraussetzen. Der Fall $A_{n,o} \neq 1$ läßt sich immer auf den Fall $A_{n,o} = 1$ zurückführen. Ist nämlich $A_{n,o} \neq 1, \neq o\,(p)$, so rechnen wir statt mit $\mathfrak{P}(x)$ mit der Reihe

$$\mathfrak{P}^*(x) = A^*_{n,o}\,\mathfrak{P}(x),\ A_{n,o} \cdot A^*_{n,o} = 1\,(p).$$

Der Irreduzibilitätscharakter von $\mathfrak{P}(x)$ wird durch diese Multiplikation nicht geändert, denn $A^*_{n,o}$ ist Einheit. Ferner bleiben die Anfangs-p-Potenzen der a_ν unverändert erhalten. Die Form niederster Dimension ist deshalb stets von der Gestalt:

$$\varphi_n(x, p) = x^n + A_{n-1,1}\, x^{n-1}\, p + \ldots. + A_{o,n}\, p^n.$$

4. Um die Weierstraßsche Normalform P(x) der Reihe $\mathfrak{P}(x)$ zu erhalten, multiplizieren wir $\mathfrak{P}(x)$ mit einer Einheit

$$\mathfrak{E}(x) = 1 + \sum_{\nu=1}^{\infty} \varepsilon_\nu;\ \ \varepsilon_\nu = e_{\nu o} x^\nu + e_{\nu-1,1}\, x^{\nu-1}\, p + \ldots + e_{o\nu}\, p^\nu.$$

Die $e_{\lambda\varrho}$ sind dabei unbestimmte Koeffizienten.

Nach Formen steigender Dimensionen geordnet stellen wir $\mathfrak{P}(x)\,\mathfrak{E}(x) = P(x)$ dar in der Form:

$$P = \sum_{\nu=o}^{\infty} \Phi_{n+\nu};\ \ \Phi_n = \varphi_n;\ \ \Phi_{n+\nu} = \varphi_{n+\nu} + \sum_{k=1}^{\nu} \varphi_{n+\nu-k}\, \varepsilon_k.$$

5. Damit $\mathfrak{P}\mathfrak{E}$ ein Normalformenpolynom P vom Grade n wird, müssen die $e_{\lambda\varrho}$ so bestimmt werden, daß in jedem Φ_i, $i > n$, x^{n-1} die höchste Potenz von x wird. Das bedeutet, daß in Φ_{n+1} der Koeffizient der Potenzen x^{n+1} und x^n, ... , in $\Phi_{n+\nu}$ jeweils der Koeffizient von $x^{n+\nu}$, ..., x^n zum Verschwinden gebracht werden muß.

Diese Forderung führt auf ein lineares Gleichungssystem von 2; . . . .; $\nu + 1$ Gleichungen mit den Unbekannten e_{10}, e_{01}; . . . . . .; $e_{\nu o}$, ..., $e_{o\nu}$. Die eindeutige Auflösbarkeit dieses Systems erkennt man leicht durch vollständige Induktion.

a) Der Ansatz $\varepsilon_1 = e_{10}\,x + e_{01}\,p$ führt formal auf $\Phi_{n+1} = A_{n+1,0}\,x^{n+1} + A_{n,1}\,x^n p + A_{n-1,2}\,x^{n-1}p^2 + \ldots + A_{1,n}\,xp^n + A_{0,n+1}\,p^{n+1} + e_{10}\,x^{n+1} + e_{10}\,A_{n-1,1}\,x^n p + e_{10}\,A_{n-2,2}\,x^{n-1}p^2 + \ldots + e_{10}\,A_{0n}\,xp^n + e_{01}\,x^n p + e_{01}\,A_{n-1,1}\,x^{n-1}\,p^2 + \ldots + e_{01}\,A_{1,n-1}\,xp^n + e_{01}\,A_{0,n}\,p^{n+1}$. Die erwähnten Bedingungen führen auf:

$$e_{10} = -A_{n+1,0};\quad e_{01} = -A_{n,1} + A_{n-1,1}\,A_{n+1,0}.$$

b) Nun seien die Formen $\varepsilon_1, \varepsilon_2, \ldots \varepsilon_{\nu-1}$ bekannt, gesucht werde ε_ν Ausrechnung obiger Bedingung gemäß, führt auf ein inhomogenes Gleichungssystem:

$$\begin{aligned} e_{\nu o} &= \beta_1 \\ \alpha_{20}\,e_{\nu o} + e_{\nu-1,1} &= \beta_2 \\ &\vdots \\ \alpha_{\nu+1,o}\,e_{\nu o} + \ldots\ldots\ldots + e_{o\nu} &= \beta_{\nu+1}, \end{aligned}$$

welches durch schrittweise Elimination trivial eindeutig auslösbar ist.

6. Man sieht sofort: Wegen $A_{n,o} = 1$ besitzen die zu bestimmenden Unbekannten $e_{\nu o}$, bezw. $e_{\nu-1,1}$, ..., bezw. $e_{o,\nu}$ in der sie festlegenden Gleichung 1, bezw. 2, ..., bezw. $\nu+1$ den Koeffizienten 1. Die $e_{\lambda\varrho}$ berechnen sich deshalb lediglich vermittels der Operationen der Addition, Subtraktion und Multiplikation aus den $A_{\nu r}$. Da letztere ganzzahlig sind, sind es damit auch die $e_{\lambda\varrho}$.

Die durch Auflösung obigen Systems gefundenen $e_{\lambda\varrho}$ entwickeln wir sodann nach Potenzen von p. Dadurch erhalten wir die c_ν unmittelbar als Potenzreihen in p, deren sämtliche Koeffizienten dem Restsystem modulo p angehören.

7. Bezeichnungen. Den Grad von P(x) heißen wir den „Polynomgrad der Reihe", ϱ den „Primgrad der Reihe". Der Polynomgrad einer Reihe bestimmt sich nach dem Vorausgehenden als Index des ersten nicht durch p teilbaren Reihenkoeffizienten.

§ 2. Praktische Handhabung der Methode.

Es seien die Entwicklungen $a_\nu = \alpha_{i_\nu}\,p^{i_\nu} + \ldots\ldots (\alpha_{i_\nu} \not\equiv 0)$ berechnet. Für die Ordnung von $\mathfrak{P}(x)$ nach Formen steigender Dimensionen empfiehlt es sich die $\varphi_\nu(x, p)$ für $\nu = n,\ n+1, \ldots$. der Reihe nach in einer Tabelle von oben nach unten aufzu-

schreiben, und ferner gleich rechts daneben eine gleiche Tabelle anzulegen, in welche die jeweils gefundenen Formen $\varepsilon_1, \varepsilon_2, \ldots$ der Weierstraßschen Einheit $\mathfrak{E}$ einzutragen sind. Bei der Berechnung der $\Phi_i = \Sigma \varphi_\nu \varepsilon_\tau$ hat man

i	$\mathfrak{P} = \Sigma \varphi_i$ $\overset{n}{\varrho} \equiv$
n	
n + 1	
n + 2	
.	
.	
.	
.	
.	

i	$\mathfrak{E} = 1 + \Sigma \varepsilon_i$
1	
2	
3	
.	
.	
.	
.	
.	

dann stets alle benötigten Formen übersichtlich beisammen.

Am raschesten geschieht die Berechnung der Φ_i (d. h. die Auflösung des Gleichungssystems für die $e_{\lambda\varrho}$) vielleicht auf folgendem tabellarischen Weg:

Für jedes $\Phi_{n+\nu}$ ($\nu = 1, 2 \ldots$.) legen wir eine Tabelle an, in deren Spalten wir die Koeffizienten von $x^{n+\nu}$, $x^{n+\nu-1}p$, ..., $p^{n+\nu}$ eintragen. Bis zur Spalte $x^n p^\nu$ muß in jeder Spalte die Summe der in ihr aufgezeichneten Zahlen gleich Null sein. So kann deshalb aus der 1. Spalte unmittelbar der Wert $e_{\nu 0}$, aus der 2. Spalte für $e_{\nu-1,1}$, ..., schließlich aus der $(\nu+1)$ten Spalte der Wert von $e_{0\nu}$ durch eine bloße Kopfrechnung abgelesen werden.

Die berechneten Werte werden sodann in die $(\nu+2)^{te}$, ..., bis $(n+\nu+1)^{te}$ Spalte eingetragen, sodann alle Zahlen einer jeden Spalte addiert und diese Summe sofort nach Potenzen p entwickelt.

Daß die Summe aller Zahlen in der 1^{ten} bis $(\nu+1)^{ten}$ Spalte gleich Null sein muß, deuten wir nach der $(\nu+1)^{ten}$ Spalte

immer durch einen dicken Strich an. So brauchen wir am Ende der Rechnung, wenn das Normalformenpolynom explizit angegeben werden soll, nur die in diesen Tabellen rechts unten stehenden Entwicklungen, multipliziert mit der oben aus der Spalte ablesbaren p-Potenz, entsprechend addieren.

	$\Phi_{n+v} = \varphi_{n+v} + \varphi_{n+v-1}\varepsilon_1 + \cdots\cdots + \varphi_n\varepsilon_v$						
x^{n+v}	$x^{n+v-1}p$	$x^{n+v-2}p^2$	. . . . .	$x^n p^v$	$x^{n-1}p^{v+1}$	. . . . .	p^{n+v}
$e_{v0} =$	$e_{v-1,1} =$	$e_{v-2,2} =$	. . . . .	$e_{0v} =$			

Da in den Spalten nur die Koeffizienten der Formen aufzuschreiben sind, so reduziert sich durch Anschreiben dieser Tabellen das Rechnen mit der Reihe auf ein bloßes Rechnen mit den Koeffizienten ihrer Formen. Gleichzeitig ersieht man aus den Tabellen unmittelbar wie die c_v mit jedem Schritt bezüglich der p-Potenzen fortschreiten.

§ 3. Über die einzelnen Schritte.

Unsere Methode gestattet nach jeder beliebigen Anzahl von Schritten jeweils aus der letzten Tabelle anzugeben, bis zu welcher p-Potenz jeder Normalformenkoeffizient vollständig bestimmt ist. Es gilt:

Jeder Schritt liefert eine und nur eine p-Potenz sicher.

Jeder neue Schritt liefert formal nur höhere p-Potenzen als der vorangehende.

Beweis: Wir dürfen uns auf die Betrachtung von c_1 beschränken, weil für alle übrigen c_ν die Untersuchung in ganz der gleichen Weise verläuft. Beim ersten Schritt wird erhalten: $c_1 = A_{n-1,1}\, p + \{A_{n-1,2} - A_{n-2,2}\, A_{n+1,0} - A_{n,1}\, A_{n-1,1} + A_{n-1,1}^2\, A_{n+1,0}\}\, p^2 + \ldots\ldots\ldots$ Durch den zweiten Schritt (Berechnung von Φ_{n+2}) wird dem c_1 ein Ausdruck angefügt, in welchem p^3 die kleinste p-Potenz ist, weil in Φ_{n+2} die $(n-1)$te Potenz von x durch p^3 zur Dimension $n+2$ ergänzt wird. Eine Potenz p^3 kann in c_1 formal schon durch den ersten Schritt entstehen, dann nämlich, wenn der Ausdruck $\{A_{n-1,2} - \ldots\ldots\ldots + A_{n-1,1}^2\, A_{n+1,0}\}$ eine Entwicklung $\gamma_0 + \gamma_1\, p + \ldots$ mit $\gamma_1 \neq 0$ zuläßt. Durch den zweiten Schritt wird jedoch der Koeffizient von p^3 eindeutig festgelegt, weil der Ausdruck, der durch den nächsten Schritt (Φ_{n+3}) entsteht, schon p^4 als kleinste p-Potenz besitzt. Dieser dritte Schritt legt zusammen mit den vorausgehenden Schritten den Koeffizienten von p^4 endgültig fest, weil der nächste Schritt (Φ_{n+4}) schon p^5 als kleinste p-Potenz hat; usw. — Wir können das Ergebnis auch so aussprechen:

Jeder Abschnitt $(a_0, a_1 \ldots\ldots a_i)$ von $\mathfrak{P}(x)$ bestimmt eindeutig einen gewissen Abschnitt $P^{(k)}(x)$. Genauer: Durch $(a_0, a_1 \ldots\ldots, a_{n+\nu})$ ist P(x) mod. $p^{\nu+2}$ vollständig bestimmt, mod. $p^{\nu+3}$ aber erst durch den Abschnitt $(a_0, a_1, \ldots, a_{n+\nu}, a_{n+\nu+1})$.

§ 4. Bedingung dafür, daß ein Abschnitt von a_ν gleichzeitig Abschnitt von $c_{n-\nu}$ ist.

Satz: Sei k eine vorgegebene positive Zahl, $P(x) = x^n + c_1 x^{n-1} + \ldots\ldots\ldots + c_n$ die Normalform von $\mathfrak{P}(x) = p^\varrho + \sum_{\nu=1}^{\infty} a_\nu x^\nu$, und $a_\nu = o\,(p^{\tau_\nu})$.

Es ist $c_\nu = a_{n-\nu}(p^{k+1})$, $\nu = 1, 2, \ldots, n$ wenn $\tau_\nu \geqq n+k-\nu$ für $\nu = n+1, \ldots, n+k-1$ und $a_n - 1 = o(p^k)$.

Beweis: Der Satz besagt, daß die k-te Näherung $P^{(k)}(x)$ von P(x) unter den angegebenen Voraussetzungen direkt aus $\mathfrak{P}(x)$ ablesbar ist.

Wir überlegen: Zur Berechnung von $P^{(k)}(x)$ sind höchstens $(k-1)$ Schritte notwendig und nicht mehr als die $(n+k)$ Reihenglieder $a_0, a_1 x, \ldots\ldots, a_{n+k-1} x^{n+k-1}$.

1. Der erste Schritt liefert nämlich Φ_{n+1}, also formal die Potenzen x^{n+1}, $x^n p$, $x^{n-1}p^2, \ldots\ldots x p^n$, $p^{n+1}; \ldots\ldots$; der (k—1)te Schritt schließlich $x^{n+k-1}, \ldots\ldots, x^{n-1}p^k, \ldots\ldots, x p^{n+k-2}$, p^{n+k-1}. Da jeder weitere Schritt nur höhere p-Potenzen liefert (§ 3), ist durch $\Phi_n + \ldots\ldots + \Phi_{n+k-1}$ jedes c_ν bis zur Potenz p^k einschließlich, exakt bestimmt. (Genauer c_1; für c_2 ist schon ein Schritt weniger nötig, für c_3 wieder ein Schritt weniger, usw. usf.). Die Behauptung ist bewiesen, wenn gezeigt ist, daß unter den angegebenen Voraussetzungen $\Phi_n + \Phi_{n+1} + \ldots\ldots + \Phi_{n+k-1} = \varphi_n + \varphi_{n+1} + \ldots + \varphi_{n+k-1}$ ist.

2. Es ist $\Phi_{n+1} = \varphi_{n+1}$, wenn $\varepsilon_1 = 0$. Dazu genügt aber (wie man aus der Φ_{n+1}-Tabelle sofort sieht):

$$a_{n+1} = 0(p), \quad a_n - 1 = 0(p^2).$$

Es ist dann $\Phi_{n+2} = \varphi_{n+2}$, wenn $\varepsilon_2 = 0$; das ist der Fall, wenn $a_{n+2} = 0(p)$, $a_{n+1} = 0(p^2)$, $a_n - 1 = 0(p^3)$.

Jetzt ist $\Phi_{n+3} = \varphi_{n+3}$, wenn $\varepsilon_3 = 0$. Dazu genügt:

$$a_{n+3} = 0(p), \quad a_{n+2} = 0(p), \quad a_{n+1} = 0(p^2), \quad a_n - 1 = 0(p^3).$$

Schließlich ist, wenn $\varepsilon_1 = \varepsilon_2 = \ldots\ldots \varepsilon_{k-2} = 0$ erreicht ist, $\Phi_{n+k-1} = \varphi_{n+k-1}$, wenn $\varepsilon_{k-1} = 0$. Das wiederum ist der Fall, wenn $a_{n+k-1} = o(p)$, $a_{n+k-2} = 0(p^2), \ldots\ldots\ldots$

$$\ldots, a_{n+1} = (p^{k-1}), a_n - 1 = 0(p^k).$$

Anmerkung: Der Satz charakterisiert eine Klasse besonders einfacher Reihen (vgl. Kap. IV, A, § 2 und B). Nützliche Dienste leistet er vor allem bei der Konstruktion von Reihen mit vorgegebenen Irreduzibilitätseigenschaften. Man konstruiert zweckmäßig zunächst ein Polynom mit den erwünschten Eigenschaften und fügt diesem nur solche Glieder an, die den Bedingungen des obigen Satzes genügen. ($k = \delta$; Kap. V, A § 2 und B.)

Kapitel V. **Irreduzibilitätsentscheidung.**

A. Direkte Irreduzibilitätsentscheidung.

Das Entscheidungsproblem ist durch den Hauptsatz vom Kap. III bereits weitgehend erledigt; mit seiner Hilfe kann in vielen Fällen ohne Kenntnis der Normalform, auf Grund von Satz 2, § 2, Kap. I und Satz 1, § 3, Kap. I direkt an $\mathfrak{P}(x)$

die Reduzibilität bezw. Irreduzibilität von $\mathfrak{P}(x)$ erkannt werden. (Direkte Irreduzibilitätsentscheidung.) Wir bringen hier noch kurz einige einfachen Kriterien.

§ 1. Der Satz von Schoenemann-Eisenstein.

1. Bereits bei J. Schur findet sich

Satz 1: Jede Potenzreihe vom Primgrad Eins ist irreduzibel. (Satz von Schoenemann-Eisenstein.)

2. Zu einer Verallgemeinerung dieses Satzes führt folgende Überlegung: Nach Satz 1, § 3 Kap. I ist P(x) irreduzibel, wenn $(\varrho, n) = 1$ und die Exponenten der in den c_ν aufgehenden p-Potenzen oberhalb der Geraden $(o, \varrho) — (n, o)$ liegen. Zusammen mit dem Hauptsatz folgt so:

Satz 2: Jede Potenzreihe, deren Primgrad zum Polynomgrad teilerfremd ist, ist irreduzibel, wenn $a_\nu = o\,(p^{\left[\frac{\varrho(n-\nu)}{n}\right]})$ für $\nu = 1, 2, \ldots, n-1$.

3. Aus Satz 2 gewinnt man speziell z. B. folgende (auch direkt herleitbare) Kriterien:

Kriterium I: Jede Potenzreihe, deren Primgrad um Eins kleiner ist als ihr Polynomgrad und bei der jeder Koeffizient $a_\nu (1 \leqq \nu \leqq n-1)$ durch $p^{n-\nu}$ teilbar ist, ist irreduzibel.

Kriterium II: Jede Potenzreihe, deren Primgrad um Eins größer ist als ihr Polynomgrad und bei der jeder Koeffizient $a_\nu (1 \leqq \nu \leqq n-1)$ durch $p^{\varrho-\nu}$ teilbar ist, ist irreduzibel.

§ 2. Ein weiterer Satz.

1. Bei dem folgenden Satz brauchen wir erstmalig den Begriff der Diskriminante D einer Potenzreihe $\mathfrak{P}(x)$. Unter D verstehen wir die in der bekannten Weise definierte Diskriminante der Normalform P(x). Die Zahl δ, welche der Bedingung genügt: $D = 0(p^\delta), \not\equiv 0(p^{\delta+1})$ heißt die Ordnung von D.

2. Direkte Irreduzibilitätsentscheidung ist z. B. noch möglich, wenn P(x) (genauer $P^{(\delta)}(x)$) direkt aus P(x) ablesbar (Satz 1, § 4, Kap. IV) und bezüglich des Irreduzibilitätscharakters von $P^{(\delta)}(x)$ unmittelbar eine bestimmte Aussage möglich ist.

Z. B. gilt der

Satz: Der Polynomgrad von $\mathfrak{P}(x)$ sei gleich dem Primgrad und keine Potenz von 2. Es sei $a_\nu = p^{n+1-\nu}$ für $\nu = 1, 2, \ldots, n-1$, $a_\nu = o(p^{\tau_\nu})$, $\tau_\nu \geqq n + n(n-1) - \nu$ für $\nu = n+1, \ldots, n(n-1)$ und $a_n - 1 = 0(p^{n(n-1)-1})$. Beh. $\mathfrak{P}(x)$ ist reduzibel.

Beweis. Es ist $P^{(\delta)}(x) = x^n + p^2x^{n-1} + p^3x^{n-2} + \ldots + p^nx + p^n$. Für ungerades n gilt: $P^{(\delta)}(x) = (x+p)[x^{n-1} + (p-1)px^{n-2} + \ldots\ldots + (p-1)p^{n-2}x + p^{n-1}]$. Eine analoge Zerlegung existiert für jedes gerade n, das nicht Potenz von 2.

B. Irreduzibilitätsentscheidung aus dem Henselschen Polynom der Reihe.

Die Irreduzibilitätsentscheidung wird schwieriger, wenn keines der bisherigen Kriterien eine Aussage gestattet. Wir müssen dann aus $\mathfrak{P}(x)$ zunächst das „Henselsche Polynom" $P^{(\delta)}(x)$ vollständig berechnen. Dazu muß aber zunächst der Wert von δ bekannt sein. Dieser kann in vielen Fällen aus dem Polygon, auf Grund des Hauptsatzes also direkt aus $\mathfrak{P}(x)$ abgelesen werden. (Kap. I, § 4.) Ist das nicht möglich, so ist $P(x)$ zunächst soweit zu berechnen, bis δ aus der Diskriminante berechnet werden kann und dann die bisher gefundene Näherung von $P(x)$ zu $P^{(\delta)}(x)$ zu erweitern.

Zur Entscheidung ob $P^{(\delta)}(x)$ irreduzibel ist, konstruiere man alle Polynome $P_g^{(\delta)}(x)$ von einem Grade $g < n$, bilde alle möglichen Produkte von zwei Polynomen, deren Gradsumme gleich n ist und sehe zu, ob eines dieser Produkte nach dem Modul $p^{\delta+1}$ zu $P^{(\delta)}(x)$ kongruent ist. Ist das der Fall, so ist $P(x)$ reduzibel, im anderen Falle irreduzibel. Im übrigen läßt sich das Verfahren am konkreten Beispiel häufig wesentlich abkürzen. Eine Vereinfachung gestattet vor allem der Satz 2 § 3, von Kap. I, indem er uns über die Grade der möglichen Teiler von $P(x)$ Aufschluß gibt.

C. Singuläre Reihen.

1. Definition: Eine Reihe heißt singulär, wenn aus keinem einzigen ihrer Abschnitte Reduzibilität bezw. Irreduzibilität erschlossen werden kann.

§ 1. Der Hauptsatz.

Satz: Eine Reihe ist dann und nur dann singulär, wenn sie Potenz einer irreduziblen Reihe ist.

Beweis. I. Wir zeigen zunächst das „dann“ der Behauptung.

1. Die Untersuchung der Abschnitte von $P(x)$ ist gleichbedeutend mit der Untersuchung der Abschnitte von $\mathfrak{P}(x)$. (Kap. II, § 2; Kap. IV, § 3). Ist $\mathfrak{P}(x)$ Potenz einer irreduziblen Reihe, so gilt für jedes k: $P(x) = P^{(k-1)}(x) = [g(x)]^r(p^k)$, $g(x)$ irreduzibel; d. h.: Bei der successiven Untersuchung von $P(x)$ besteht nach jedem Schritt die Möglichkeit der Reduzibilität von $\mathfrak{P}(x)$. Das „dann“ der Behauptung zeigen wir nun dadurch, daß wir nachweisen, daß nach jedem Schritt auch die Möglichkeit der Irreduzibilität von $\mathfrak{P}(x)$ besteht. Dazu genügt es offenbar zu zeigen: Aus jedem p-adischen Polynom $P^{(k-1)}(x)$, welches mod. p^k Potenz eines irreduziblen Polynoms $g(x)$ ist, kann durch Anfügen geeigneter v-ter Potenzen ($v \geqq k$), ein irreduzibles Polynom $P^{(k-1,\,v)}(x)$ konstruiert werden.

2. Es sei K der Körper der p-adischen Zahlen und $g(x) = (x-\alpha_0)(x-\alpha_1)\ldots\ldots(x-\alpha_{s-1})$ ein in K irreduzibles Polynom mit ganzen p-adischen Koeffizienten. K_i bedeute den Körper $K(\alpha_i)$, $i = 0, 1, \ldots, s-1$. r und k seien vorgegebene positive ganze Zahlen.

Zum Beweis steht folgende

Behauptung: In K kann ein Polynom $q(x)$ vom Grade $q \leqq r \cdot s - 1$ mit ganzen Koeffizienten so bestimmt werden, daß das Polynom $[g(x)]^r + p^k q(x)$ in K irreduzibel ist.

3. Wir zeigen zunächst: In K_0 kann ein ganzzahliges Polynom $q_0(x)$ vom Grade $q_0 \leqq r-1$ so bestimmt werden, daß

1. das Polynom $f_0(x) = (x-\alpha_0)^r + p^k q_0(x-\alpha_0)$ in K_0 irreduzibel wird, und daß
2. die Polynome $f_i(x) = (x-\alpha_i)^r + p^k q_i(x-\alpha_i)$, $f_1(x) = (x-\alpha_1)^r + p^k q_1(x-\alpha_1)$ für $i \neq 1$ stets teilerfremd sind.

Ad. 1. In K_0 bezw. dem zugehörigen Ring von π-adischen Zahlen ist p gleich einer Potenz eines Primelementes π. Es seien die Exponenten v_i der in den Koeffizienten a_i eines Polynoms $A(x) = x^r + a_1 x^{r-1} + \ldots\ldots + a_r$ aufgehenden

π-Potenzen sämtlich absolut oberhalb k gelegen. A(x) ist sicher irreduzibel, wenn $v_r = h \cdot r + 1$, h ganz, positiv, $a_r = o(\pi^{v_r})$, $\not\equiv o(\pi^{v_r+1})$, und alle $v_i \geqq h \cdot i + 1$ für $i = 1, 2, \ldots, r-1$. Denn bei der Transformation $x = x'\pi^h$ erweist sich $A(x'\pi^h)$ nach Vorsetzen von $\pi^{h \cdot r}$ als Eisensteinsches Polynom. Wir sehen: Durch Variation von h ist es möglich unendlichviele irreduzible Polynome A(x) zu konstruieren, bei denen die Exponenten der in den Koeffizienten von A(x) aufgehenden π-Potenzen sämtlich über einer angegebenen Schranke k liegen. Da ferner mit $A(x) = x^r + \pi^k(a_1 x^{r-1} + \ldots\ldots + a_r)$ auch $A(x - \alpha_o) = (x - \alpha_o)^r + \pi^k(a_1(x - \alpha_o)^{r-1} + \ldots\ldots + a_r)$ irreduzibel ist, so folgt, daß jeder der Koeffizienten eines ganzzahligen Polynoms $q_o(x)$ vom Grade $q_o \leqq r - 1$ in K auf unendlichviele Weisen so gewählt werden kann, daß das Polynom $f(x) = (x - \alpha_o)^r + p^k q_o(x)$ in K_o irreduzibel ist.

Ad. 2. Wir setzen f(x) an als Polynom $u(x) = x^r + u_1 x^{r-1} + \ldots\ldots + u_r$ mit unbestimmten Koeffizienten u_i. $f_i(x)$ setzen wir so an: $u^{(i)}(x) = (x - \alpha_i)^r + \sum_{v=o}^{r-1}(u_{vo} + u_{v1}\alpha_i + \ldots + u_{v,s-1}\alpha_i^{s-1})(x - \alpha_i)^v$, und zeigen, daß die $u_{v\mu}$ ($v = 0, \ldots, r-1$; $\mu = 0, \ldots, s-1$) in K so wählbar sind, daß neben der Bedingung $u_i = o(p^k)$ und $u^{(o)}(x)$ irreduzibel in K_o, noch Teilerfremdheit zwischen $u^{(i)}(x)$ und $u^{(l)}(x)$, $i \not\equiv l$, gewährleistet ist.

Für die Teilerfremdheit ist notwendig und hinreichend, daß die Resultante $R(u^{(i)}(x), u^{(l)}(x))$ von Null verschieden ist. Man sieht zunächst, daß R nicht identisch verschwindet. Wir betrachten R als ein Polynom $R(u_{v\mu})$ in den $u_{v\mu}$. Nun ist ein Polynom in beliebigvielen Veränderlichen bekanntlich dann und nur dann identisch Null, wenn alle Koeffizienten gleich Null sind. In $R(u_{v\mu})$ ist das aber sicher nicht der Fall. Um das einzusehen, betrachten wir die Wurzeln $\beta_1, \ldots, \beta_r$, von $u^{(o)}(x)$; die β_i sind algebraische Funktionen der Variablen $u_{v\mu}$.

Wir spezialisieren folgendermaßen: Wir setzen $u_{v\mu} = o$ für $\mu > o$ und setzen die Wurzeln von $u^{(i)}(x)$ gleich $\beta_v + \alpha_i$, $v = 1, 2, r$, die von $u^{(l)}(x)$ gleich $\beta_v + \alpha_l$, $v = 1, 2$; . ., r. Es ist dann $R(u^{(i)}(x), u^{(l)}(x)) = \prod_{v=1}^{r}\prod_{\tau=1}^{r}[(\beta_v + \alpha_i) - (\beta_\tau + \alpha_l)]$. Man sieht nun, daß R nicht identisch verschwindet, weil R nicht ver-

schwindet, wenn man für die β_i irgendwelche Variable einsetzt.

Wir sehen: Nach 1) haben wir für jeden einzelnen Koeffizienten unendlich viele Möglichkeiten die $u_{\nu\mu}$ so zu wählen, daß $u_i = o$ (p^k), und $u^{(o)}(x)$ irreduzibel in K_o. Da $R(u_{\nu\mu})$ ein nicht identisch verschwindendes Polynom in den $u_{\nu\mu}$ ist, können wir die $u_{\nu\mu}$ gleichzeitig auf unendlichviele Weisen so auswählen, daß Teilerfremdheit zwischen $u^{(i)}(x)$ und $u^{(l)}(x)$ vorliegt, indem wir nämlich die $u_{\nu\mu}$ so wählen, daß $R(u_{\nu\mu}) \neq o$. Das besagt: Man kann die $u_{\nu\mu}$ in K zahlenmäßig so spezialisieren, daß bei dieser Spezialisierung $u^{(o)}(x)$ in K_o irreduzibel wird, und daß dabei ferner keine der Resultanten $R(u^{(i)}(x), u^{(e)}(x))$ verschwindet.

4. Jetzt ergibt sich sofort die Richtigkeit der Behauptung von Nr. 2. Es habe $f_i(x)$ dieselbe Bedeutung wie in Nr. 3 und es werde $f(x) = \prod_{i=o}^{s-1} f_i(x)$ gesetzt. $f(x)$ gehört sicher zu K. Es ist $f_o(x)\, f_1(x) =$
$\{(x-\alpha_o)(x-\alpha_1)\}^r + p^k\{(x-\alpha_o)^r q_1(x-\alpha_1) + (x-\alpha_1)^r q_o(x-\alpha_o)\}$,
d. h. es ist $\prod_{i=o}^{1} f_i(x)$ von der Form $g_0(x) + p^k g_1(x)$, wo $g_0(x)$ vom Grade $g_0 = 2r$ und $g_1(x)$ vom Grade $g_1 \leqq 2r-1$. Allgemein erhält man: $f(x) = [g(x)]^r + p^k q(x)$, wo $g(x) = \prod_{i=o}^{s-1}(x-\alpha_i)$ und $q(x)$ ein ganzzahliges Polynom vom Grade $q \leqq rs-1$. — Weiterhin muß $f(x)$ die Potenz eines irreduziblen Polynoms aus K sein. Da aber die $f_i(x)$ paarweise teilerfremd sind, so folgt, daß dies nur die erste Potenz sein kann.

II. Wir zeigen jetzt das „nur dann" der Behauptung. Dazu genügt es zu zeigen: Für jedes p-adische Polynom $P(x)$, das Produkt zweier teilerfremder Polynome $P_1(x)$ und $P_2(x)$ ist, kann stets die Produktzerlegung $P(x) = P_1(x)\, P_2(x)$ konstruiert werden.

Sei $P_i^{(k-1)}(x)$ der Näherungswert des Teiles $P_i(x)$ von $P(x)$ mod p^k. Wir konstruieren schrittweise für $k = 1, 2, \ldots$. alle möglichen Teiler $P_i^{(k-1)}(x)$ von $P(x)$. In der Reihe dieser Näherungswerte können nicht fortgesetzt lauter gleiche vorkommen; wegen der teilerfremden Reduzibilität muß man einmal zu einem $k = s$

kommen der Eigenschaft, daß die beiden Näherungswerte $P_i^{(s-1)}(x)$ $(i=1,2)$, — $P(x)=P_1^{(s-1)}(x)\,P_2^{(s-1)}(x)\,(p^s)$ —, bei geeigneter Wahl der Approximation teilerfremd sind.

Sei r die Ordnung der Resultante der Polynome $P_1(x)$ und $P_2(x)$. Wir konstruieren die Zerlegung von $P(x)$ bis $k=s_1$, $s_1>2r$. Von der Zerlegung $P(x)=P_1^{(s_1-1)}(x)\,P_2^{(s_1-1)}(x)\,(p^{s_1})$ führt dann der Ansatz:

$$(1)\quad P(x)=(P_1^{(s_1-1)}(x)+K_1(x))\,(P_2^{(s_1-1}(x)+K_2(x))\,(p^{s_1+1})$$

systematisch zu einer eindeutigen Zerlegung $P(x)=P_1(x)\,P_2(x)$, wo $P_1(x)$ und $P_2(x)$ Polynome in x mit Potenzreihenkoeffizienten in p.

Es sei $P_1^{(s_1-1)}(x)$ vom Grade n_1 und $P_2^{(s_1-1)}(x)$ vom Grade n_2 in x. Wir setzen die „Korrektionsglieder" $K_1(x)$ und $K_2(x)$ an als Polynome in x vom Grade $\leqq n_1-1$ bezw. n_2-1 mit unbestimmten Koeffizienten a_i bezw. b_i. Nach Ausmultiplikation von (1) erhält man:

$$(2)\quad P(x)=P_1^{(s_1-1)}(x)P_2^{(s_1-1)}(x)+(P_1^{(s_1-1)}(x)K_2(x)+P_2^{(s_1-1)}(x)K_1(x))+K_1(x)K_2(x)\,(p^{s_1+1}).$$

Wir setzen $P(x)-P_1^{(s_1-1)}(x)\,P_2^{(s-1)}(x)=P^*(x)$; $P^*(x)$ ist in x vom Grade $\leqq n-1$ und es gilt $P^*(x)=p^{s_1}P_o^*(x)$.

Demgemäß machen wir für $K_1(x)$ und $K_2(x)$ den Ansatz:

$$K_1(x)=p^{s_1-r}K_1^*(x);\quad K_1^*=a_o^*x^{n_1-1}+\ldots+a_{n_1-1}^*$$

$$K_2(x)=p^{s_1-r}K_2^*(x);\quad K_2^*=b_o^*x^{n_2-1}+\ldots+b_{n_2-1}^*.$$

Dann gilt gemäß (2):

$$p^{s_1}P_o^*(x)=p^{s_1-r}[P_1^{(s_1-1)}(x)K_2^*(x)+P_2^{(s_1-1)}(x)K_1^*(x)]+p^{2s_1-2r}K_1^*(x)K_2^*(x)(\mathrm{mod}\,p^{s_1+1}),$$

oder nach Division mit p^{s_1-r}:

$$(3)\quad p^rP_o^*(x)=P_1^{(s_1-1)}(x)K_2^*(x)+P_2^{(s_1-1)}(x)K_1^*(x)\qquad(p^{r+1}).$$

Durch Gleichsetzen der Koeffizienten von x^{n-1}, ..., 1 wird ein System von n linearen Gleichungen in den Unbekannten a_i^*, b_i^* erhalten. Die Determinante dieses Systems ist gerade die Resultante $R(P^{(s_1-1)}(x),\,P_2^{(s_1-1)}(x))$. Und als solche genau durch p^r teilbar. Daraus folgt jetzt sofort die ganzzahlige Bestimmbarkeit der a_i^* und b_i^*.

Damit ist der Satz vollständig bewiesen. —

2. Definition: Eine Reihe heißt singulär, wenn aus keinem einzigen ihrer Abschnitte die genaue Anzahl der irreduziblen Teiler angegeben werden kann.

Bei Zugrundelegung dieser Definition lautet der dem Hauptsatz äquivalente

Satz: Eine Reihe ist dann und nur dann singulär, wenn sie einen mehrfachen Faktor besitzt.

§ 2. Ein Polygonsatz.

Satz: Jede Reihe mit einfachem Polygon und einem nicht durch p teilbaren Polynomgrad, ist nichtsingulär.

Beweis: Sei $\mathfrak{P}(x) = \Sigma a_\nu x^\nu$, $a_\nu = o(p)$, $\nu = 0, 1, \ldots, n-1$; $a_n \not\equiv o(p)$, $P(x) = x^n + \ldots + c_n$. Wäre die Reihe singulär, so würde sie Potenz einer irreduziblen Reihe sein, also wäre $P(x) = (x^s + \ldots + c_s)^r$. Da aber $r \not\equiv o(p)$, so müßte die Reihe nach Satz 3, § 3, Kap. I ein nicheinfaches Polygon besitzen.

Kapitel VI.

Das Zerlegungsproblem.

1. Sei $\mathfrak{P}(x) = p^\varrho + \sum_{\nu=1}^{\infty} a_\nu x^\nu$ reduzibel. Gesucht wird ein Verfahren, das die irreduziblen Teiler $\mathfrak{P}_i(x)$ von $\mathfrak{P}(x)$ systematisch finden läßt; präziser: das von jedem $\mathfrak{P}_i(x) = p^{\varrho_i} + \sum_{\nu=1}^{\infty} a_\nu^{(i)} x^\nu$ $(\sum_i \varrho_i = \varrho)$ jeden beliebigen endlichen Abschnitt $(a_o^{(i)}, \ldots, a_{\nu^*}^{(i)})$ mit einer von vornherein genau angebbaren Maximalzahl von Schritten zu konstruieren gestattet.

2. Wir gehen folgendermaßen vor: Wir berechnen zunächst die irreduziblen Teiler $P_{(i)}(x)$ der Normalform $P(x)$. Diese Aufgabe läßt sich in übersichtlicher Weise an Hand des Polygons erledigen, durch ein Verfahren, das sich im wesentlichen aus dem Beweis des Dumas'schen Reduzibilitätssatzes (Kap. I, § 2, Satz 2) herleiten läßt[1]). Dann führen wir jeden Normalteiler $P_{(i)}(x)$ in eine Potenzreihe in x mit ganzen Zahlkoeffizienten über,

1) Dumas, S. 223—S. 235; § 5, § 7.

durch ein Verfahren (Multiplikation mit einer Einheit $E_{(i)}(x)$), das formal genau so verläuft, wie die Berechnung von $P(x)$ aus $\mathfrak{P}(x)$.

§ 1. Zerlegung des Normalformenpolynoms in irreduzible Faktoren.

A. Konstruktion des zu einer Polygonseite S_v gehörigen Teilers $P^{(v)}(x)$.

I. 1. Es seien $S_1, S_2 \ldots\ldots S_l$ die Seiten des Polygons $\mathfrak{P}$. Wir fassen diejenigen Glieder von $P(x)$, deren Diagrammpunkte auf ein und derselben Seite S_v liegen, zusammen. Es werden dann Ausdrücke folgender Gestalt erhalten:

$$\gamma_{v_1} x^{n_{v_1}} p^{i_{v_1}} + \ldots\ldots + \gamma_{v_s} x^{n_{v_s}} p^{i_{v_s}} =$$
$$x^{n_{v_s}} [\gamma_{v_1} x^{n_{v_1} - n_{v_s}} + \ldots\ldots + \gamma_{v_s} p^{i_{v_s} - i_{v_1}}] p^{i_{v_1}};$$
$$(n_{v_1} > \ldots\ldots > n_{v_s};\ i_{v_1} < \ldots < i_{v_s}).$$

Alle γ_{v_i} gehören dem Restsystem mod p an, die Null ist ausgeschlossen. Man erhält l solche Ausdrücke. Die Polynome in der eckigen Klammer schreiben wir einfacher in der Form: $\gamma_{\varrho_{v,0}} x^{n_v} + \ldots + \gamma_{0,n_v} p^{\varrho_v}$ $(v = l, 2, \ldots, l)$.

2. Wir bestimmen die Zahl $\gamma^*_{\varrho_{v,0}}$, welche der Gleichung: $\gamma^*_{\varrho_{v,0}} \gamma_{\varrho_{v,0}} \equiv 1 (p)$ genügt, sodann die Zahlen $\gamma^*_{\tau,\lambda}$ $(\tau = v-1, \ldots, 0;$ $\lambda = 0, \ldots, n_\tau)$ als die kleinsten positiven Reste der Produkte $\gamma^*_{\varrho_{\tau,0}} \cdot \gamma_{\tau\lambda}$ nach dem Modul p. Ersetzt man $\gamma^*_{\varrho_{v,0}}$ durch 1 und im übrigen $\gamma_{\tau\lambda}$ durch $\gamma^*_{\tau\lambda}$, so gelangt man zu Polynomen $p_v(x)$ der Gestalt: $p_v(x) = x^{n_v} + \ldots + \gamma^*_{0,n_v} p^{\varrho_v}$.

II) Die Bestimmung von $P^{(v)}(x)$ beruht auf folgenden Gedanken: Zunächst gilt (nach Dumas):

$$P(x) \equiv P^{(1)}_1(x)\, P^{(1)}_2(x) \qquad (p)$$
$$(P^{(1)}_1(x) = \Pi p_i(x)_{i=1,2,\ldots,v-1,v+1,\ldots l},\ P^{(1)}_2(x) = p_v(x))$$

Man macht den Ansatz:

$$P_1(x) = P^{(1)}_1(x) + \sum_{i=1}^{\infty} p^i A_i(x)$$
$$P_2(x) = P^{(1)}_2(x) + \sum_{i=1}^{\infty} p^i B_i(x)$$

mit unbestimmten Koeffizienten $A_i(x)$ und $B_i(x)$; alle $A_i(x)$ sind in x von einem Grade, der kleiner als der von $P_1^{(1)}(x)$, entsprechend alle $B_i(x)$ von einem Grade, der kleiner als der von $P_2^{(1)}(x)$ ist. Man zeigt, daß, falls die A_i, B_i für $i = 1, 2, \ldots, k-1$ bekannt sind, von der dann gültigen Gleichung

$$P(x) = P_1^{(k)}(x) P_1^{(k)}(x) \qquad (p^k)$$

$$[P_1^{(k)}(x) = P_1^{(1)}(x) + \sum_{i=1}^{k-1} p^i A_i(x),\ P_2^{(k)}(x) = P_2^{(1)}(x) + \sum_{i=1}^{k-1} p^i B_i(x)]$$

zur Gleichung:

$$P(x) = (P_1^{(k)}(x) + p^k A_k(x))(P_2^{(k)}(x) + p^k B_k(x)) \qquad (p^{k+1})$$

übergegangen werden kann, welche die noch unbekannten Polynome $A_k(x)$ und $B_k(x)$ eindeutig berechnen läßt.

III. 1. Die Durchführbarkeit dieses Ansatzes beruht auf folgendem Hilfssatz[1]): Wenn für die Normalform P(x) zwei ganzzahlige Polynome $P_1^{(1)}(x)$ und $P_2^{(1)}(x)$ existieren, deren Reresultante nicht durch p teilbar ist und welche der Gleichung genügen:

$$P(x) = P_1^{(1)}(x)\, P_2^{(1)}(x) \qquad (p),$$

so ist P(x) notwendig reduzibel.

2. Unsere Polynome $P_1^{(1)}(x)$ und $P_2^{(1)}(x)$ sind nicht von der Eigenschaft eine durch p unteilbare Resultante zu besitzen. Durch Anwendung der Transformation

$x = y\, p^{\frac{\varrho_\nu^*}{n_\nu^*}}$ $(n_\nu = An_\nu^*,\ \varrho_\nu = A\varrho_\nu^*;\ (n_\nu^*, \varrho_\nu^*) = 1)$ gehen aber $P_1^{(1)}(x)$ und $P_2^{(1)}(x)$ in Polynome $P_1^{(1)}(y)$ und $P_2^{(1)}(y)$ über, die eine durch $p^{\frac{1}{n_\nu^*}}$ unteilbare Resultante besitzen[2]).

3. Der obige Ansatz führt jetzt auf

$$P(y) = (P_1^{(k)}(y) + P^{\frac{k}{n_\nu^*}} A_k(y))(P_2^{(k)}(y) + p^{\frac{k}{n_\nu^*}} B_k(y) \qquad (p^{\frac{k+1}{n_\nu^*}}).$$

Da er jetzt mod $p^{\frac{k}{n_\nu^*}}$ bereits gültig ist, gilt:

---

1) K. Hensel: Neue Grundlagen der Arithmetik; Crelles Journ. Bd. 127, 1904, S. 81.
Dumas, § 2, S. 205, Nr. 4.

2) Dumas, S. 224–226, Nr. 4,5.

$P(y) - P_1^{(k)}(y) P_2^{(k)}(y) = p^{\frac{k}{n_\nu^*}} G(y) \qquad (p^{\frac{k+1}{n_\nu^*}})$
und schließlich:

$G(y) = P_1^{(k)}(y) B_k(y) + P_2^{(k)} A_k(y) \qquad (p^{\frac{1}{n_\nu^*}})$.
Koeffizientenvergleich führt hier auf ein lineares, inhomogenes Gleichungssystem von gleichviel Unbekannten wie Gleichungen; gemäß dem Hensel-Dumas'schen Hilfsatz ist stets eindeutige Auflösbarkeit möglich.

4. Die Umkehrtransformation $y = x p^{-\frac{\varrho_\nu^*}{n_\nu^*}}$ liefert zwei Polynome $P_1(x)$ und $P_2(x)$ mit nur ganzen p-Potenzen in den Koeffizienten[1]).

B. Konstruktion der irreduziblen Teiler von $P^{(\nu)}(x)$.

$P^{(\nu)}(x)$ ist irreduzibl, wenn $(\varrho_\nu, n_\nu) = 1$. (Kap. I, § 3, Satz 1). Im Falle $(\varrho_\nu, n_\nu) = A \neq 1$ ist Reduzibilität möglich. $P^{(\nu)}(x)$ muß dann weiter zerlegt werden.

Sei $p_\nu(x) = x^{n_\nu} + \ldots + \gamma_{o,n_\nu} p^{\varrho_\nu}$. Wir machen die Substitution[2]): $x^{n_\nu} = z \cdot p^{\varrho_\nu}$ $(n_\nu = t \cdot n'_\nu,\ \varrho_\nu = t \cdot \varrho'_\nu;\ (n'_\nu,\ \varrho'_\nu) = 1)$ und erhalten nach Division mit p^{ϱ_ν}: $p^*(z) = z^t + \ldots + \gamma_{o,n_\nu}$.

$p^*(z)$ wird mod p in irreduzible Faktoren $p_i^*(z) = z^{n_i} + \ldots + \gamma_i$ zerlegt. Dann können wir schreiben: $p^*(z) = \Pi [p_i^*(z)]^{\nu_i} + p\varphi(z)$. Setzt man nach der Rücktransformation $(z = x^{n'_\nu} p^{-\varrho'_\nu})$

$p^{n_i \cdot \varrho'_\nu} p_i^* \left(\frac{x^{n'_\nu}}{p^{\varrho'_\nu}} \right) = p_i(x)$, so erhält man schließlich: $P(x) = \Pi [p_i(x)]^{\nu_i} + \Sigma \gamma_{\alpha\beta} p^\alpha x^\beta$, wo die Punkte $\gamma_{\alpha\beta} p^\alpha x^\beta$ sämtlich oberhalb der Polygonseite S_ν liegen und $\beta \leqq n - 1$ ist.

Jetzt ermöglicht die Transformation $x = y p^{\frac{\varrho'_\nu}{n'_\nu}}$ die Durchführung des unter A) entwickelten Ansatzes auch für $P^{(\nu)}(x)$[3]).

---

1) Dumas, S. 228, Nr. 7.
2) Dumas, S. 220, § 4, Nr. 2.
3) Dumas, S. 232, Nr. 7.

§ 2. Überführung der Normalformenteiler in Potenzreihenteiler.

Wir bestimmen nach dem in Kap. IV entwickelten Verfahren zu jedem Normalformenteiler von der Form $P_i(x) = x^{n_i} + c_1^{(i)}(p)x^{n_i-1} + \ldots + c_{n_i}^{(i)}(p)$ eindeutig die Einheit $E_i(p,x)$ so, daß $P_i(x) \cdot E_i(x)$ ein Polynom in p vom Grade ϱ_i wird, falls $c_{n_i}^{(i)} = o\,(p^{\varrho_i})$, $\neq o\ (p^{\varrho_i+1})$. Die Koeffizienten dieses Polynoms $\mathfrak{P}_i(x) = p^{\varrho_i} + C_1^{(i)}(x)p^{\varrho_i-1} + \ldots + C_{\varrho_i}^{(i)}(x)$ werden dann Potenzreihen in x. — Zu Beginn der Berechnung ist eventuell Regularitätstransformation nötig, also $x = t^r$ so zu substituieren, daß $P_i(x)$ nach Formen steigender Dimension in p und t geordnet regulär in p von der Dimension ϱ_i ist. Ordnet man $P_i(x) \cdot E_i(x)$ nach Potenzen von x, so wird eine Potenzreihe $\mathfrak{P}_i(x) = p^{\varrho_i} + \sum_{\nu}^{\infty} a_\nu^{(i)} x^\nu$ in x mit ganzen Zahlkoeffizienten erhalten.

ZOBODAT - www.zobodat.at

Zoologisch-Botanische Datenbank/Zoological-Botanical Database

Digitale Literatur/Digital Literature

Zeitschrift/Journal: Sitzungsberichte der Physikalisch-Medizinischen Sozietät zu Erlangen

Jahr/Year: 1933-1934

Band/Volume: 65-66

Autor(en)/Author(s): Zehlein Friedrich

Artikel/Article: Irreduzibilitätsproblem bei ganzzahligen Potenzreihen 1-34