ALGEBRAISCH-ZAHLENTHEORETISCHE BETRACHTUNGEN ÜBER RINGE. I.

VON

L. RÉDEI und T. SZELE
in SZEGED (Ungarn).[1]

§ 1. Einleitung.

Die Polynome in einem Ring erzeugen dort zugleich eine Funktion[2], auf diesem Wege entstehen aber im allgemeinen nicht alle Funktionen, die sich im Ringe erklären lassen. Wir werfen das Problem auf, dass man einen weiteren Ring angibt, in dem sich die Funktionen des ersten Ringes durch Polynome darstellen lassen. Selbstverständlich verlangen wir eine einfache, gut brauchbare „Darstellung". Wir werden ein Prinzip angeben, das unter Umständen ermöglicht unser Problem auf eine gewisse Art zu lösen, die an Einfachheit nichts zu wünschen übriglässt. Als Anwendung werden wir dann die Frage in einem einfachen, für die Algebra und Zahlentheorie gleich wichtigen Fall ausführlich untersuchen, teilweise — und zwar den Restklassenring mod p^e (s. unten) — mit vollem Erfolg. Zu unseren Untersuchungen haben einige früheren Arbeiten von mehreren Autoren eine Anleitung gegeben, worauf wir später unten zu sprechen kommen.

Immer bezeichnen R, S, T, U einen Ring, insbesondere K den Körper der rationalen Zahlen, G den Ring der ganzen rationalen Zahlen, $K^{(n)}$ einen algebraischen Zahlkörper n-ten Grades über K, $G^{(n)}$ den Ring der ganzen Zahlen von

[1] An dieser ersten und der späteren zweiten Mitteilung hat der erste (RÉDEI) bzw. zweite (SZELE) von uns den vorwiegenden Anteil.

[2] Bekanntlich sind die Ringe die allgemeinsten Mengen (Strukturen), in denen man Polynome zu erklären pflegt. Meistens schreibt man dabei die Existenz des Einselementes vor, von dieser Einschränkung kann man sich frei machen, so dass man einen Oberring mit Einselement zu Hilfe nimmt und nur die Polynome in diesem betrachtet, deren Koeffizienten im gegebenen Ring liegen. Dagegen beschränken wir uns auf kommutative Ringe, da sonst zwischen den Polynomen und den durch sie erzeugten Funktionen kein einfacher Zusammenhang (keine homomorphe Beziehung) besteht (s. unten).

$K^{(n)}$, p eine Primzahl, $m (\geqq 2)$, e natürliche Zahlen, (m) das durch m erzeugte Hauptideal in G, K_m den Ring von den rationalen Zahlen, deren Nenner nur Primfaktoren von m enthält (hierbei kommt es nur auf die verschiedenen Primfaktoren von m an), $\mathfrak{p}$ ein Primideal und $\mathfrak{r} (\neq 0)$ ein Ideal in $K^{(n)}$, $\Re^{(n)}(\mathfrak{r}) = G^{(n)}/\mathfrak{r}$ den Restklassenring von $G^{(n)}$ mod $\mathfrak{r}$, insbesondere $(\Re^{(1)}(m) =) \Re(m)$ den Restklassenring von G mod m — dieser wird uns am meisten beschäftigen, den wir deshalb kurz den Restklassenring mod m nennen — und $\mathfrak{K}(p^e)$ den endlichen Körper mit p^e Elementen, der bekanntlich auch ein Spezialfall von $\Re^{(n)}(\mathfrak{r})$ ist, und zwar ist jeder $\Re^{(n)}(\mathfrak{p})$ ein $\mathfrak{K}(p^e)$.[3]

Wir wollen über $\Re^{(n)}(\mathfrak{r})$ einiges bemerken. Dieser ist bekanntlich die direkte Summe aller $\Re^{(n)}(\mathfrak{p}^e)(\mathfrak{p}^e \| \mathfrak{r})$, insbesondere ist $\Re(m)$ die der $\Re(p^e)(p^e \| m)$. Selbst $\Re^{(n)}(\mathfrak{p}^e)$ ist für $e \geqq 2$ im allgemeinen von verwickelter Struktur, die unseres Wissens noch nicht völlig bekannt ist.[4] Wir lassen den allgemeinen Fall ausser Acht und betrachten nur die erwähnten Spezialfälle $\mathfrak{K}(p^e)$, $\Re(m)$. Diese sind von allereinfachster Struktur unter allen Ringen, wenn man von den sogenannten Zero-Ringen mit lauter verschwindenden Produkten absieht.[5] Über $\Re(m)$ bemerken wir noch, dass die in [5] gesagten Eigenschaften charakteristisch sind, und so gilt neben der obigen, etwas komplizierten, „zahlentheoretischen" Definition auch die viel einfachere, (abstrakt-)„algebraische" Definition: $\Re(m)$ ist ein endlicher Ring mit Einselement und zyklischer additiver Gruppe.[6] Trotzdem werden wir hiervon keinen Gebrauch machen können, sondern wir werden eine Lösung unseres Pro-

[3] $R \approx S$ bezeichnet die Isomorphie zwischen R und S. In allen unseren Fragen sind isomorphe Ringe gleichberechtigt. $R \sim S$ bezeichnet: S ist homomorph zu R, wir sagen hierfür auch: R ist homomorphinvers zu S. Mit $R \sim S$ denken wir immer auch schon eine feste homomorphe Abbildung von R auf S mit angegeben. Insbesondere ist dann auch das Ideal I (der Homomorphiekern) derjenigen Elemente von R mitbestimmt, die auf 0 abgebildet werden. Bekanntlich gilt für den entsprechenden Restklassenring $R/I \approx S$, und umgekehrt besteht für jedes Ideal I von R eine Homomorphie $R \sim R/I$. — Mit R^+ bezeichnen wir die additive Gruppe (der Elemente) von R. „$a^x \| b$" bezeichnet „$a^x \mid b$, $a^{x+1} \nmid b$".

[4] Es ist sogar schon $\Re^{(n)}(\mathfrak{p}^e)^+$ nicht ganz leicht zu überblicken.

[5] Zwischen diesen bekannten Ringen besteht folgende merkwürdige „Dualität": $\mathfrak{K}(p^e)$, $\Re(m)$ sind endliche Ringe mit Einselement, die multiplikative Gruppe der von 0 verschiedenen Elemente des ersten, bzw. die additive Gruppe aller Elemente des zweiten ist zyklisch. Zwischen den unzerlegbaren Bestandteilen $\mathfrak{K}(p^e)$, $\Re(p^e)$ ist auch noch gemeinsam, dass die Elementenzahl beidesmahl eine (beliebige) Primzahlpotenz ist. Trotzdem werden sich diese Ringe in Betracht unseres Problems stark abweichend verhalten. Eine Ausnahme macht $e = 1$, da $\mathfrak{K}(p) \approx \Re(p)$ ist.

[6] Bezeichne nämlich R einen solchen Ring mit m Elementen und dem Einselement ε, weiter sei α ein erzeugendes Element von R. Dann sind die $i\alpha$ $(i = 0, \ldots, m-1)$ alle Elemente von R, und es gilt allgemein $i\alpha = j\alpha$ $(i \equiv j \pmod m)$. Insbesondere sei $\varepsilon = r\alpha$. Wegen $\alpha = \alpha\varepsilon = r\alpha^2$ muss $(r, m) = 1$ gelten, und so ist selbst ε ein erzeugendes Element. Da $i\varepsilon \cdot j\varepsilon = ij\varepsilon$ ist, so sieht man schon $R \approx \Re(m)$ ein.

blems für $\mathfrak{R}(m)$ auf einem Weg suchen (bzw. für $\mathfrak{R}(p^e)$ finden), der sich unmittelbar an die ursprüngliche, kompliziertere Definition anlehnt (s. unten).

Im allgemeinen Fall werden für uns die folgenden zwei Operationen (und ihre Inversen) von Wichtigkeit sein: Das Übergehen von R zu einem Unterring R^1, bzw. zu einem homomorphen Ring R^2. Beide Operationen haben das gemeinsame, dass sie eine „Zusammenschrumpfung" bewirken, weshalb wir sie für den Augenblick eine 1-Ableitung bzw. 2-Ableitung nennen. Werden sie (in dieser Reihenfolge) hintereinander ausgeführt, so schreiben wir hierfür R^{12}. Explizit lautet das

$$R \geqq R^1 \sim R^{12}, \tag{1}$$

d. h. R^{12} ist ein zu einem Unterring von R homomorpher Ring. Werden an R die 1- und 2-Ableitung in beliebiger Reihenfolge endlich vielmal hintereinander ausgeführt, so entsteht immer nur ein R^{12},[7] und deshalb nennen wir R^{12} kurz eine Ableitung (oder einen abgeleiteten Ring) von Q. Da in (1) auch $R = R^1$ oder $R^1 = R^{12}$ sein kann, so kommen unter allen R^{12} auch die R^1 und R^2 vor. Ist umgekehrt R eine Ableitung von S (d. h. $R = S^{12}$), so nennen wir S einen *primitiven* Ring von R. Dieser ist also ein Oberring eines zu R homomorphinversen Ringes. Wieder kommen unter diesen alle Oberringe und homomorphinversen Ringe vor, und aus obigem folgt, dass die (endliche) Iteration immer nur zu einem primitiven Ring führen kann. Bei uns werden die primitiven Ringe die Hauptrolle spielen.

Ein Polynom[8] $f(x)$ oder eine Funktion[9] $f(x)$ in R nennen wir auch ein R-Polynom bzw. eine R-Funktion. Den aus ihnen bestehenden Polynomring bzw. Funktionenring bezeichnen wir mit $R[x]$ und $R(x)$. Die durch ein R-Polynom $f(x)$ erzeugte R-Funktion wird üblicherweise ebenfalls mit $f(x)$ bezeichnet, wir schreiben aber nötigenfalls „Polynom" (statt Polynom), wobei die Anführungszeichen andeuten, dass von der durch ein Polynom erzeugte Funktion die Rede ist. Meistens wird das aus den Zusammenhängen ohnehin klar, und dann lassen wir diese Anführungszeichen weg. Alle R-„Polynome" bilden einen zu $R[x]$ homomorphen Unterring $R([x])$ von $R(x)$:

---

[7] Denn gilt $R \sim S \geqq T$, so gibt es ein U mit $R \geqq U \sim T$. Wegen der Transitivität beider Zeichen $\geqq$, $\sim$ folgt hieraus die Behauptung durch vollständige Induktion.

[8] Wir lassen für gewöhnlich nur Polynome von einer Unbestimmten zu, nur als Hilfsmittel werden später auch Polynome von mehreren Unbestimmten vorkommen.

[9] Wird nichts anderes gesagt, so sprechen wir nur über eindeutige Funktionen.

$$R(x) \geqq R([x]), \tag{2}$$

$$R[x] \sim R([x]).^{10} \tag{3}$$

Sind in R alle Funktionen durch Polynome erzeugt, so ist in R die „Funktionentheorie" bloss ein Kapitel der Theorie der Polynome. Wir fragen vor allem, für welche Ringe dieser günstigste Fall eintritt. Hierüber werden wir folgenden Satz beweisen:

Satz 1. *Unter allen Ringen R sind die endlichen Körper $\mathfrak{R}(p^e)$ dadurch ausgezeichnet, dass für sie und nur für sie in (2) das Zeichen $=$ gilt. In $\mathfrak{R}(p^e)$ werden alle verschiedenen Funktionen durch die Polynome vom Grade $\leqq p^e - 1$ erzeugt.*[11]

Unser Problem besteht kürzer gefasst aus der Aufgabe, dass man alle R-Funktionen (auf eine einfache Art) durch S-Polynome darstellt, wobei S ein geeigneter Ring ist. Nach Satz 1 liegt für $R = \mathfrak{R}(p^e)$ die triviale Lösung $S = R$ vor. Für die übrigen R fassen wir das Problem allgemeiner (weniger scharf), indem wir nur verlangen, dass sich durch die S-Polynome alle R-„Polynome", ausserdem auch noch weitere R-Funktionen darstellen lassen. Jede Lösung dieses verallgemeinerten Problems können wir als eine Partiallösung des ursprünglichen Problems ansehen.

Nunmehr erwähnen wir vor allem eine Arbeit von NAGELL[12] über zahlentheoretische Polynome — so nennt er ein K-Polynom $f(x)$ mit der Eigenschaft $f(x) \in G\,(x \in G)$ — in der es sich für den Ring G um eine Partiallösung unseres Problems handelt. Ein klassisches Beispiel ist

$$\binom{x}{k} = \frac{x(x-1)\ldots(x-k+1)}{k!} \qquad (k = 0, 1, \ldots). \tag{4}$$

Nach Nagells Satz sind die

[10] Und zwar kommt diese Homomorphie so zustande, dass man jedem R-Polynom $f(x)$ das R-„Polynom" $f(x)$ zuordnet. Nach dem sogenannten Einsetzungsprinzip entsprechen dann in der Tat der Summe und dem Produkt zweier R-Polynome $f(x)$, $g(x)$ eben die Summe und das Produkt der R-„Polynome" $f(x)$, $g(x)$. Für nichtkommutative Ringe gilt das bezüglich des Produkts nicht mehr, und dann hören die Polynome auf, ein gut brauchbares Mittel zur Darstellung der Funktionen zu sein, wie wir das in [2] schon bemerkt haben. Hier bemerken wir auch, dass wir unser Problem so lösen wollen, dass dabei (3) nicht verlorengeht (s. unten).

[11] Ist ω die Mächtigkeit von $\mathfrak{R}$, so ist ω^ω die von $R(x)$. Ist ω unendlich, so ist nach dem Wohlordnungssatz die Mächtigkeit von $R[x]$ ebenfalls nur ω, und so ist Satz 1 für diesen Fall wegen $\omega < \omega^\omega$ richtig. Andererseits ist die letzte Behauptung des Satzes bekanntlich auch richtig, und so haben wir Satz 1 nur noch für endliche $R\,(= \mathfrak{R}(p^e))$ zu beweisen.

[12] T. NAGELL, Einige Sätze über die ganzen rationalen Funktionen, Nyt Tidsskrift for Matematik 29. Jahrg., B. (1918), 53—62.

$$a_0 + a_1\binom{x}{1} + \cdots + a_n\binom{x}{n} \qquad (a_i \in G) \tag{5}$$

alle zahlentheoretischen Polynome. PÓLYA[13] und OSTROWSKI[14] haben allgemeiner die $K^{(n)}$-Polynome mit der entsprechenden Eigenschaft $f(x) \in G^{(n)}\,(x \in G^{(n)})$ untersucht, teilweise mit ähnlich einfachen Resultaten. Ein solches Polynom nennen sie ganzwertig. NAGELL[15] und OSTROWSKI[14] haben ihre Untersuchungen auch auf Polynome von mehreren Unbestimmten ausgedehnt. SKOLEM[16] hat gewisse Diophantische Fragen über ganzwertige Polynome behandelt. Die zahlentheoretischen Polynome von einer Unbestimmten haben in einer anderen Fassung (s. unten) auch NIELSEN[17], KEMPNER[18] und DICKSON[19] betrachtet. Ausser Nagells Satz und gewissen Beispielen (s. unten) bei Dickson werden wir mit diesen Untersuchungen nur in wenig Berührung treten. Gleich hier bemerken wir, dass Nagells Satz uns nicht nur ein Beispiel zu einer Partiallösung unseres Problems für $R = G$ liefert, sondern — was uns hier viel wichtiger ist — wir werden unsere ausführlichen Betrachtungen über $R = \mathfrak{R}(m)$ auf diesem Satz aufbauen. (Wir werden diesen Satz vollständigkeitshalber kurz beweisen.)

Wir verallgemeinern den Begriff der (zahlentheoretischen bzw.) ganzwertigen Polynome für beliebige Ringe (führen aber sinngemäss eine andere Benennung ein) und lassen dabei nicht nur Polynome, sondern auch sonstige Funktionen zu.

Definition 1. *Es gelte $S \geq R$. Eine S-Funktion $f(x)$ mit der Eigenschaft*

$$f(x) \in R \qquad (x \in R) \tag{6}$$

nennen wir R-haltend. Offenbar ist diese Eigenschaft notwendig und hinreichend, damit $f(x)$ auch in R eine Funktion erzeugt, die nämlich aus allen Zuordnungen $x \to f(x)\,(x \in R)$ besteht. Diese dürfen wir dann einfach die R-Funktion $f(x)$ nennen.[20]

[13] G. PÓLYA, Über ganzwertige Polynome in algebraischen Zahlkörpern, Journ. f. Math., 149 (1919), 97—116.

[14] A. OSTROWSKI, ebenda, 117—124.

[15] T. NAGELL, Über zahlentheoretische Polynome, Norsk Matematisk Tidsskriftl. Jahrg. (1919), 14—23.

[16] TH. SKOLEM, Sätze über ganzwertige Polynome, Det Kong. Norske Videnskabers Selskab, Forh. X. Nr. 4.

[17] N. NIELSEN, Nieuw Archiv voor Wiskunde (ser. 2), 10 (1913), 100—106.

[18] A. J. KEMPNER, Polynomials and their residue systems, Trans. Amer. Math. Soc., 22 (1921), 240—288.

[19] L. E. DICKSON-E. BODEWIG, Einführung in die Zahlentheorie, Leipzig u. Berlin 1931, 1—175.

[20] Das führt zu keinem Missverständnis, denn man wird immer wissen, ob diese R-Funktion unmittelbar in R definiert wurde oder ein „Teil" einer S-Funktion ist.

Insbesondere erzeugen die R-haltenden S-Polynome zugleich auch R-Funktionen. Nagells Satz lehrt, dass dabei auch solche R-Funktionen erzeugt werden können, die keine R-„Polynome" sind. Wir fragen, ob man zu einem R einen Oberring S finden kann, so dass die R-haltenden S-Polynome alle R-Funktionen erzeugen. Nach Satz 1 geht das für $R = \Re(p^r)$ sogar schon mit $S = R$. In einem scharfen Gegensatz hierzu lautet aber die Antwort für den „Zwillingsbruder" $R = \Re(m)$ völlig verneinend, und zwar gilt der folgende:

Satz 2. *Was immer für ein Oberring S von $\Re(m)$ gegeben wird, so erzeugen doch die $\Re(m)$-haltenden S-Polynome keine $\Re(m)$-Funktionen ausser den $\Re(m)$-„Polynomen".*

Trotzdem werden wir den Begriff der R-haltenden Polynome auf einem „Umweg" mit Erfolg zu unserem Problem insbesondere eben auch bezüglich $\Re(m)$ verwenden können. Statt gleich mit etwas fertigem zu kommen, wollen wir zuerst ein einfaches Beispiel konstruieren, das für unser allgemeines Verfahren in grossem Masse charakteristisch sein wird.

Wir gehen aus dem K_p-Polynom

$$\Phi(x) = \frac{x^p - x}{p} \tag{7}$$

aus, das nach Fermat G-haltend, d. h. zugleich eine G-Funktion ist. Aus

$$(a + p^e t)^p \equiv a^p \pmod{p^{e+1}} \qquad (a,\ t \in G)$$

folgt nach (7)

$$\Phi(a + p^e t) \equiv \Phi(a) - p^{e-1} t \pmod{p^e}. \tag{8}$$

Das „störende" zweite Glied auf der rechten Seite lassen wir jetzt (für $e \geqq 2$) herausfallen, so dass wir die Kongruenz zur p-ten Potenz erheben:

$$\Phi^p(a + p^e t) \equiv \Phi^p(a) \pmod{p^e},$$

mit anderen Worten:

$$\Phi^p(x) \equiv \Phi^p(y) \pmod{p^e} \qquad (e \geqq 2;\ x, y \in G;\ x \equiv y \pmod{p^e}). \tag{9}$$

Diese Kongruenz spricht aus, dass die Restklasse $\Phi^p(x) \pmod{p^e}$ durch die Restklasse $x \pmod{p^e}$ eindeutig bestimmt ist, also dass das K_p-Polynom

$$\psi(x) = \Phi^p(x) \qquad (e \geqq 2) \tag{10}$$

eine $\mathfrak{R}(p^e)$-Funktion darstellt.[21] Dabei wird aus den späteren Resultaten leicht folgen, dass diese Funktion kein $\mathfrak{R}(p^e)$-„Polynom" ist. Es scheint uns, dass dieses interessante Beispiel in der elementaren Zahlentheorie völlig neuartig ist. Bei unseren Untersuchungen war eben dieses Beispiel der Ausgangspunkt, alles übrige ist bloss ein konsequenter Ausbau dieser kleinen Erscheinung.

Das wesentlich neue in diesem Beispiel ist folgendes, wobei wir obige Konstruktion rückwärts überblicken. Um eine $\mathfrak{R}(p^e)$-Funktion durch ein Polynom zu definieren, haben wir zuerst nach einem homomorphinversen Ring G gegriffen (diesen Schritt haben wir oben einen Umweg genannt), erst von hier sind wir dann zu einem Oberring K_p aufgestiegen, in dem wir ein gewünschtes Polynom gefunden haben. Deshalb definieren wir allgemein zunächst folgendes:

Definition 2. *Es gelte $S \sim R$, und bezeichne $\bar{x}$ das homomorphe Bild von $x\,(\in S)$. Unterwirft man in irgendeiner S-Funktion $f(x)$, die also aus allen Zuordnungen $x \to f(x)$ $(x \in S)$ besteht, beide Variablen unserem Homomorphismus, so entsteht eine (im allgemeinen mehrdeutige) R-Funktion als Inbegriff aller Zuordnungen $\bar{x} \to \overline{f(x)}$ $(x \in S)$, die wir das homomorphe Bild von $f(x)$ nennen und mit $\tilde{f}(x)$ bezeichnen. Eindeutig ist diese R-Funktion $\tilde{f}(x)$ offenbar dann und nur dann, wenn*

$$\overline{f(x)} = \overline{f(y)} \qquad (x, y \in S;\ \bar{x} = \bar{y}) \tag{11}$$

gilt, und dann nennen wir selbst $f(x)$ eine (für die Homomorphie $S \sim R$) zulässige S-Funktion.[22]

Bevor wir weitergehen, bemerken wir vor allem die aus der Definition der Homomorphie folgende, oft verwendete, wichtige Tatsache, dass insbesondere alle S-Polynome $f(x) = a_0 x^n + \cdots + a_n$ für jede Homomorphie $S \sim R$ zulässig sind[23], und dabei gilt einfach $\tilde{f}(x) = \bar{a}_0 x^n + \cdots + \bar{a}_n$. Dies spricht zugleich aus, dass auf diesem Wege aus S-Polynomen nur R-„Polynome" abzuleiten sind, und so wird

[21] Das ist ebenso zu verstehen, wie man auch sagen kann, dass jedes G-Polynom zugleich auch eine $\mathfrak{R}(m)$-Funktion (und zwar für jedes m) darstellt, worauf man sich in der Zahlentheorie oft beruft, ohne es ausdrücklich zu sagen. Als grundsätzlicher Unterschied tritt dabei auf, dass das über $\psi(x)$ gesagte für $e = 1$ nicht mehr gilt (darüber später näheres). Die Restklasse mod I, die das Element x enthält, nennen wir manchmal wie auch schon oben kurz die Restklasse x (mod I).

[22] Die Ähnlichkeit beider Definitionen 1, 2 ist augenscheinlich, beidesmal kommt es nämlich darauf an, dass man eine S-Funktion unter Umständen in einem Unterring bzw. homomorphen Ring auffassen kann. Hier bemerken wir auch, dass wir die Definition 1 nur auf den Fall anwenden werden, in dem $f(x)$ ein S-Polynom ist, dagegen wird für uns in der Definition 2 eben der andere Fall von Wichtigkeit sein, in dem nämlich die S-Funktion $f(x)$ kein S-Polynom ist.

[23] Somit sind die zulässigen Funktionen eine Verallgemeinerung der Polynome.

dadurch für unser Problem kein Fortschritt gemacht. Ganz anders steht es, wenn man (wie auch im obigen Beispiel) aus einem S-haltenden T-Polynom $f(x)$ ausgeht ($T \geqq S$), denn dann kann $\tilde{f}(x)$ von den R-„Polynomen" verschieden sein. Wegen $T \geqq S \sim R$ ist dabei T ein primitiver Ring von R. Genauer sprechen wir das so aus:

Grundsatz. (Prinzip der Darstellung der R-Funktionen durch Polynome.) *Man nehme zu einem gegebenen Ring R zwei weitere Ringe S, T mit $T \geqq S \sim R$, wobei also T ein primitiver Ring von R ist. Bezeichne $\bar{x}$ das Bild von $x (\in S)$ in der angegebenen Homomorphie $S \sim R$. Ist dann $f(x)$ ein T-Polynom mit den Eigenschaften*

$$f(x) \in S \qquad (x \in S) \tag{12}$$

$$\overline{f(x)} = \overline{f(y)} \qquad (x, y \in S;\ \bar{x} = \bar{y}), \tag{13}$$

d. h. (S-haltend und) für die Homomorphie $S \sim R$ zulässig, so ist das homomorphe Bild $\tilde{f}(x)$ von $f(x)$ eine (eindeutige) R-Funktion, die nämlich aus allen Zuordnungen $\bar{x} \to \overline{f(x)}\,(x \in S)$ besteht. Wir nennen $\tilde{f}(x)$ die durch $f(x)$ darstellte R-Funktion. Erschöpfen die $\tilde{f}(x)$ alle R-Funktionen, so nennen wir T einen Darstellungsring für $R(x)$.[24]

Zusatz. *Sind $f(x)$, $g(x)$ (S-haltende) zulässige T-Polynome, so sind es auch $f(x) \pm g(x)$, $f(x)\,g(x)$, und diese darstellen eben die R-Funktionen $\tilde{f}(x) \pm \tilde{g}(x)$ bzw. $\tilde{f}(x)\,\tilde{g}(x)$. Folglich ist die Zuordnung $f(x) \to \tilde{f}(x)$ ein Homomorphismus zwischen einem Unterring von $T[x]$ bestehend aus den zulässigen T-Polynomen, und einem Unterring von $R(x)$ bestehend aus den durch T-Polynome darstellbaren R-Funktionen.*

Die Richtigkeit dieser Sätze ist unmittelbar einzusehen. Die hier beschriebene Darstellung der R-Funktionen durch Polynome ist wirklich sehr einfach, aber die Brauchbarkeit ist davon abhängig, ob man zu einem gegebenen R einen Darstellungsring T finden kann. Als weitere Fragen treten dann noch auf, wie man T zu konstruieren und die zulässigen T-Polynome zu bestimmen hat. Wir sind

---

[24] Da sich R durch einen isomorphen Ring ersetzen lässt, so darf immer $S/I = R$ angenommen werden, wobei I ein Ideal in S ist, und dann bedeutet $\bar{x}$ die Restklasse $x \pmod I$, zugleich nimmt (13) die Form der Kongruenz

$$f(x) \equiv f(y) \pmod I \qquad (x, y \in S;\ x \equiv y \pmod I)$$

an. Entsprechend dürfen wir dann $f(x) \bmod I$ (statt „für die Homomorphie $S \sim R$") zulässig nennen. Später werden wir den Grundsatz in dieser zweiten Form anwenden.

weit entfernt, dass wir diese Fragen im allgemeinen beantworten könnten, sondern begnügen uns damit, dass wir — wie oben schon gesagt — den wichtigen Spezialfall $R = \mathfrak{R}(m)$ ausführlich untersuchen.

Nach dem vorangeschickten Beispiel liegt es an der Hand, dass wir versuchen, den Grundsatz mit $R = \mathfrak{R}(m)$, $S = G$, $T = K_m$ anzuwenden, was wir auch tun werden.[25] Unser wichtigstes Resultat wird folgender:

Satz 3. (Hauptsatz für $\mathfrak{R}(p^m)$.) *K_p ist ein Darstellungsring für den Funktionenring* $\mathfrak{R}(p^e)(x)$.[26]

Hierzu bemerken wir gleich, dass nach Satz 1 $\mathfrak{R}(p^e)$ sein eigener Darstellungsring ist. (Das entspricht nämlich dem Sonderfall $R = S = T$ des Grundsatzes.) Merkwürdig ist dieses abweichende Verhalten von $\mathfrak{R}(p^e)$, $\mathfrak{R}(p^e)$, obwohl beide Spezialfälle von $\mathfrak{R}^{(n)}(\mathfrak{r})$ sind. (Vgl. [5].)

Betreffend den allgemeinen Fall haben wir schon erwähnt, dass $\mathfrak{R}(m)$ sich in die direkte Summe der $\mathfrak{R}(p^e)(p^e \| m)$ zerlegen lässt. Aus diesem Grunde werden wir alle Fragen bezüglich $\mathfrak{R}(m)$ auf den Fall $\mathfrak{R}(p^e)$ zurückführen können. So würde man erwarten, dass sich Satz 3 unmittelbar verallgemeinern lässt, überraschenderweise werden wir dagegen bekommen, dass sich durch K_m-Polynome nur ein Teil aller $\mathfrak{R}(m)$-Funktionen darstellen lassen, und so wird K_m nur eine Partiallösung unseres Problems für $\mathfrak{R}(m)(m \neq p^e)$ liefern.

Zusammenfassend haben wir eine vollständige Lösung unseres Problems nur für die zwei (endlichen) Ringe $\mathfrak{R}(p^e)$, $\mathfrak{R}(p^e)$ gefunden. Als nächstes, ungelöstes Problem bleibt übrig, ob sich zu $\mathfrak{R}(m)$ im allgemeinen ein Darstellungsring finden lässt.[27]

---

[25] Man könnte K statt K_m nehmen, aber das würde nicht mehr leisten.

[26] Dann ist K ein gemeinsamer Darstellungsring für alle $\mathfrak{R}(p^e)(x)$. — Nach Satz 3 können wir wieder sagen, dass die Funktionentheorie in $\mathfrak{R}(p^e)$ ein Kapitel der Theorie der Polynome in K_p ist.

[27] Selbstverständlich schliesst Satz 3 die Möglichkeit nicht aus, dass es zu $\mathfrak{R}(p^e)$ auch solche Darstellungsringe gibt, die keinen zu K_p isomorphen Unterring haben. Es könnte sogar sein, dass es (allgemeiner) zu $\mathfrak{R}(m)$ einen endlichen Darstellungsring gibt, diese Frage haben wir nicht geprüft. Wir sagen nochmals ausdrücklich, dass wir hier bezüglich $\mathfrak{R}(m)$ in der Hauptsache nur die Frage untersuchen, inwieweit sich die $\mathfrak{R}(m)$-Funktionen durch K-Polynome darstellen lassen. Das bedeutet, dass wir die einfachere „algebraische" Definition von $\mathfrak{R}(m)$ ausser Acht lassend unmittelbar an die „zahlentheoretische" Definition angeknüpft haben, und so sind wir zugleich auch den zahlentheoretischen Interessen nachgekommen. — Hier bemerken wir noch, dass sich auch diese ursprüngliche Definition (von $\mathfrak{R}(m)$ und sogar) von $\mathfrak{R}^{(n)}(\mathfrak{r})$ rein algebraisch formulieren lässt, so dass man aus dem Primkörper von der Charakteristik 0 statt K ausgeht und alles sinngemäss verändert, „zahlentheoretisch" wird diese Definition erst dadurch, dass man wieder K einsetzt.

Kurz schicken wir noch folgendes voran. Es werden die aus $\Phi(x)(=\Phi_1(x))$ durch Iteration entstehenden K_p-Polynome

$$\Phi_0(x)=x,\ \Phi_{k+1}(x)=\frac{1}{p}(\Phi_k^p(x)-\Phi_k(x)) \qquad (k=0,1,\ldots) \tag{14}$$

und ihre Potenzen

$$\psi_k(x)=\Phi_k^{p^k}(x) \qquad (k=0,1,\ldots), \tag{15}$$

weiter auch die zu (14) assoziierten G-Hauptpolynome[28]

$$F_k(x)=p^{\frac{p^k-1}{p-1}}\Phi_k(x) \qquad (k=0,1,\ldots) \tag{16}$$

eine wichtige Rolle spielen. Letztere lassen sich auch durch die Rekursion

$$F_0(x)=x,\ \ F_{k+1}(x)=F_k^p(x)-p^{p^k-1}F_k(x) \tag{17}$$

definieren.[29] Insbesondere werden wir dem Satz von Nagell mit Hilfe der $\Phi_k(x)$ eine andere Form geben, die zu unseren Zwecken mehr geeignet ist. Über Satz 3 hinaus, der nur über die Möglichkeit der Darstellung der $\mathfrak{R}(p^e)$-Funktionen spricht, werden wir ein System $\mathfrak{S}$ von K_p-Polynomen angeben, die alle verschiedenen $\mathfrak{R}(p^e)$-Funktionen darstellen (erst hierdurch wird der Beweis von Satz 3 erbracht). Und zwar wird $\mathfrak{S}$ äusserst einfach durch die $\psi_k(x)$ ausgedrückt. Aus $\mathfrak{S}$ leiten wir ein zweites, gleichberechtigtes System $\mathfrak{S}_0$ ab, das sich aus den einfacheren Polynomen $\Phi_k(x)$ zusammensetzt. $\mathfrak{S}_0$ ist nicht mehr von so einfacher Struktur wie $\mathfrak{S}$, hat aber die Eigenschaft, dass seine Glieder von möglichst kleinem Nenner und zugleich auch von möglichst kleinem Grad sind. Wir nennen $\mathfrak{S}$ und $\mathfrak{S}_0$ das normale bzw. minimale Representantensystem von $\mathfrak{R}(p^e)(x)$. Hier erwähnen wir die zwei interessanten Probleme, was die kleinsten Zahlen $\nu=\nu(p^e)$, $g=g(p^e)$ sind, so dass sich alle $\mathfrak{R}(p^e)$-Funktionen durch K_p-Polynome vom Nenner $\leqq p^\nu$, bzw. vom Grad $\leqq g$ darstellen lassen. Wohl sind ν und g das Maximum der in

---

[28] Wir nennen ein Polynom von der Form $x^n+cx^{n-1}+\cdots$ ein Hauptpolynom. A. ALBERT schlug in seiner „Modern higher algebra, 1937" die Benennung (englisch: monique) monisch vor. Der ältere Ausdruck „normiert" ist nicht trefflich, da sich die Polynome in einem Ringe im allgemeinen nicht „normieren" lassen.

[29] Das sieht man am leichtesten so ein, dass man (16) in (17) einsetzt, wodurch eben (14) entsteht. Von (17) liest man unmittelbar ab, dass die $F_k(x)$ Hauptpolynome sind. Insbesondere ist $F_1(x)=x^p-x$ das Polynom von Fermat, und so können wir die $F_k(x)$ als eine Verallgemeinerung von diesem ansehen. Die Fälle $k=2,3$ kommen auch bei DICKSON [19] (SS. 20, 25) vor. Diese Dicksonschen Beispiele haben uns zur allgemeinen Bildung der Polynome $F_k(x)$ die Anleitung gegeben, die in unseren Betrachtungen eine kurze, aber wichtige Rolle spielen werden.

$\mathfrak{S}_0$ auftretenden Nenner und Grade, trotzdem konnten wir diese Zahlen (wegen der komplizierten Struktur von $\mathfrak{S}_0$) nicht bestimmen, und so mussten wir uns begnügen, einige einfache Beispiele zu berechnen. Endlich nennen wir folgendes Problem, das für die Zahlentheorie von grossem Interesse ist, weshalb wir es auch an die Spitze hätten stellen dürfen: Was ist die Menge der m, für die ein vorgelegtes K-Polynom eine $\mathfrak{R}(m)$-Funktion darstellt? (Sonst ist dies im Rahmen unserer Untersuchungen ein Umkehrproblem zu nennen.) Die Antwort gelingt mit Hilfe des minimalen Systems $\mathfrak{S}_0$ in jedem Falle und wird unerwartet interessant lauten. Es wird sich unter anderem ergeben, dass es ausser den G-Polynomen noch viele weitere K-Polynome gibt, die in jedem $\mathfrak{R}(m)$ eine Funktion darstellen (d. h. nach jedem Modul m zulässig sind).

§ 2. Beweis der Sätze 1, 2.

Beim Beweis von Satz 1 dürfen wir uns wegen[11] auf einen endlichen $R(\neq \mathfrak{R}(p^e))$ beschränken. Dann hat R sicher Nullteiler und braucht kein Einselement zu haben. Bezeichne n die Elementenzahl von R und s_k $(k = 1, \ldots, n-1)$ das k-te elementarsymmetrische Polynom der Elemente $(\neq 0)$ von R. Wir setzen für ein beliebiges Element $c(\neq 0)$ von R:

$$f_c(x) = c\,x^{n-1} - c\,s_1\,x^{n-2} + \cdots \pm c\,s_{n-1},$$
$$g_c(x) = c\,x^n - c\,s_1\,x^{n-1} + \cdots \pm c\,s_{n-1}\,x.$$

(Man darf nicht einfach $g_c(x) = x f_c(x)$ schreiben, da x nur dann ein Polynom in R ist, wenn das Einselement existiert.) Es ist klar, dass $g_c(x)$ in R überall verschwindet. Andererseits ist jedes R-Polynom $f(x)$ nach dem durch die $g_c(x)$ erzeugten Ideal in $R[x]$ kongruent einem R-Polynom $f^*(x)$ vom Grad $\leqq n$. Beide Polynome erzeugen dieselbe R-Funktion, und dabei ist die Anzahl aller $f^*(x)$ eben n^n, die der R-Funktionen. Es genügt also zu zeigen, dass es unter diesen Polynomen ein $f^*(x)(\neq 0)$ gibt, das in R überall verschwindet, denn dann sind die R-„Polynome" $f^*(x)$ nicht alle verschieden. Jedes $f_c(x)$ verschwindet für alle $x(\neq 0)$ in R. Ist c insbesondere ein Nullteiler, so ist das konstante Glied von $f_c(x)$ gleich 0, und dann ist auch $f_c(0) = 0$. Dieses $f_c(x)$ ist ein passendes $f^*(x)$, womit wir Satz 1 bewiesen haben.[30]

---

[30] Wir wissen nicht, ob der Satz auch für nichtkommutative Ringe R richtig bleibt. Ist R unendlich, so gilt der Schluss in [11] unverändert. Ist $\mathfrak{R}$ endlich so ist er nach Wedderburn kein Körper (enthält also Nullteiler), aber obiger Beweis gilt nicht mehr.

Zum Beweis von Satz 2 bezeichnen wir das Einselement von $\mathfrak{R}(m)$ mit ε. Wir zeigen zuerst, dass man sich auf den Fall beschränken darf, wo ε auch für S das Einselement ist und für jedes $x(\in S)$ $mx = 0$ gilt. Bezeichne hierzu $f(x)$ ein $\mathfrak{R}(m)$-haltendes S-Polynom. Dann ist es auch $\varepsilon f(x)$, und beide Polynome erzeugen dieselbe $\mathfrak{R}(m)$-Funktion. Andererseits ist die Menge aller verschiedenen $\varepsilon x (x \in S)$ ein Ring, der wegen $m\varepsilon = 0$ die geforderten Eigenschaften hat. Da alle Koeffizienten von $\varepsilon f(x)$ in diesem Ring liegen, so folgt hieraus die Richtigkeit obiger Behauptung.

Machen wir die genannte Einschränkung und nehmen irgendein S-Polynom $f(x)$ an. Die Koeffizienten von $f(x)$ und ε erzeugen eine additive Untergruppe H von S^+ Da ε von maximaler Ordnung in H ist, nämlich von der Ordnung m, so hat H eine unabhängige Basis $\alpha_1, \ldots, \alpha_k$ mit $\alpha_1 = \varepsilon$. Ersetzen wir die Koeffizienten von $f(x)$ durch ihre Basisdarstellung, so bewirkt das eine Zerlegung

$$f(x) = \sum_{i=1}^{k} g_i(x), \tag{18}$$

wobei $g_i(x)$ ein Polynom von der Form $a_0 \alpha_i x^n + \cdots + a_n \alpha_i$ $(a_0, \ldots, a_n \in G)$ ist. Andererseits sind $0, \varepsilon, \ldots, (m-1)\varepsilon$ alle Elemente von $\mathfrak{R}(m)$, und so folgt aus (18), dass für jedes $x(\in \mathfrak{R}(m))$ eine Gleichung von der Form

$$f(x) = g_1(x) + \sum_{i=2}^{k} b_i \alpha_i \qquad (b_2, \ldots, b_k \in G) \tag{19}$$

gilt. Das erste Glied rechts ist in $\mathfrak{R}(m)$ also ein $b_1 \varepsilon = b_1 \alpha_1$ mit $b_1 \in G$, wenn also ausserdem $f(x) \in \mathfrak{R}(m)$ ist, so müssen wegen der Unabhängigkeit der $\varepsilon, \alpha_2, \ldots, \alpha_k$ alle Summanden $b_i \alpha_i$ in (19) verschwinden, und dann geht (19) in $f(x) = g_1(x)$ über, wobei $g_1(x)$ nach obigem ein $\mathfrak{R}(m)$-Polynom ist. Ist $f(x)$ $\mathfrak{R}(m)$-haltend, so gilt das für jedes $x(\in \mathfrak{R}(m))$, womit wir Satz 2 bewiesen haben.

§ 3. Vorbereitungen zu den Betrachtungen über $\mathfrak{R}(m)$.

Von hier an beschäftigen wir uns nur noch mit der Frage der Darstellung der $\mathfrak{R}(m)$-Funktionen durch K-Polynome, dabei werden wir auch die G-haltenden K-Polynome untersuchen müssen. In diesem § machen wir einige Vorbereitungen von verschiedener Natur.

Wir wiederholen für diesen Fall (vgl. [24]), dass eine K-Funktion $f(x)$ dann und nur dann eine $\mathfrak{R}(m)$-Funktion darstellt, wenn.

$$f(x) \in G \qquad (x \in G), \tag{20}$$

$$f(x) \equiv f(y) \pmod{m} \qquad (x \equiv y \pmod{m}) \tag{21}$$

ist. Dabei drückt (20) und (21) aus, dass $f(x)$ G-haltend bzw. mod m zulässig ist. Da (21) nur dann sinnvoll ist, wenn auch (20) gilt, so dürfen wir mit „mod m zulässig" beide Eigenschaften (20), (21) meinen. Die Bezeichnungen vereinfachen wir so, dass wir statt „$\mathfrak{R}(m)$-Funktion $\tilde{f}(x)$" (wobei nämlich $f(x)$ eine mod m zulässige K-Funktion ist) kurz „$\mathfrak{R}(m)$-Funktion $f(x)$" schreiben, was man nicht missverstehen kann.

Jedes K-Polynom lässt sich in der Form

$$f(x) = \frac{g(x)}{m} \tag{22}$$

annehmen mit einem G-Polynom $g(x)$. Damit dann $f(x)$ G-haltend ist, ist offenbar notwendig und hinreichend, dass $g(x)$ überall verschwindet mod m (d. h. $g(x) \equiv 0 \pmod{m}$ $(x \in G)$ gilt). Hieraus sehen wir, dass die „G-haltenden K-Polynome" und die „mod m überall verschwindenden G-Polynome" zwei äquivalente Probleme bieten.[31]

Ist $g(x)$ in (22) zu m prim[32], so wird hierdurch (22) eine eindeutig bestimmte „Normalform" von $f(x)$ sein, selbst m definieren wir den Nenner von $f(x)$. Bekanntlich lässt sich dann (22) in der Form

$$f(x) = \sum_{p_i | m} \frac{g_i(x)}{p_i^{e_i}} \qquad (p_i^{e_i} \| m) \tag{23}$$

schreiben, wobei p_i die verschiedenen Primfaktoren von m durchläuft und $g_i(x)$ ein zu p_i primes G-Polynom ist. Diese $g_i(x)$ sind mod $p_i^{e_i}$ eindeutig bestimmt. Wir nennen (23) eine Partialbruchzerlegung von $f(x)$. Es ist klar, dass $f(x)$ dann und nur dann G-haltend ist, wenn alle Glieder in (23) es auch sind. Mit anderen Worten heisst das, dass es zur Bestimmung der G-haltenden K-Polynome genügt, die G-haltenden K_p-Polynome zu bestimmen. Das werden wir im nächsten § tun, und so wird die erwähnte Umformung von Nagells Satz entstehen.

Die Frage der mod m zulässigen K-Polynome lässt sich auf die der G-haltenden K-Polynome zurückführen. Wir beweisen folgenden (vorbereitenden):

---

[31] KEMPNER[18] und DICKSON[19] haben sich mit dem Problem in der obigen zweiten Fassung beschäftigt.

[32] Selbstverständlich ist dabei m als ein konstantes G-Polynom aufzufassen.

Satz 4. *Ein K-Polynom $f(x)$ ist eine $\mathfrak{R}(m)$-Funktion dann und nur dann, wenn $f(x)$ und*

$$\frac{1}{m}(f(x+m)-f(x)) \tag{24}$$

G-haltend sind.

Denn (24) ist dann und nur dann G-haltend, wenn der zweite Faktor für jedes $x(\in G)$ eine, durch m teilbare ganze Zahl ist. Letzteres ist äquivalent mit (21), womit wir Satz 4 bewiesen haben.

Eine fast triviale Bemerkung ist die folgende. Lässt sich eine $\mathfrak{R}(m)$-Funktion überhaupt durch ein K-Polynom $f(x)$ darstellen, so gibt es auch ein K_m-Polynom $g(x)$, das dieselbe $\mathfrak{R}(m)$-Funktion darstellt. Offenbar darf man nämlich $f(x)$ durch $cf(x)$ ersetzen, wobei $c \in G$, $\equiv 1 \pmod m$ ist. Mit einem geeigneten c ist $g(x) = cf(x)$ ein passendes Polynom.

Ähnlich sieht man folgendes ein. Ist $f(x)$ ein G-haltendes K-Polynom mit einem zu m primen Nenner, so ist $f(x)$ auch eine $\mathfrak{R}(m)$-Funktion, die sich übrigens auch durch ein G-Polynom darstellen lässt.

Darstellt ein K-Polynom $f(x)$ eine $\mathfrak{R}(m)$-Funktion, so folgt hieraus ähnliches für jedes $d(d \mid m;\ 1 < d < m)$ gar nicht, vielmehr werden wir bei jedem m Beispiele angeben, für die das bei keinem d der Fall ist.

Im Lauf der Arbeit werden mehrere Polynomfolgen (bestehend aus K- oder G-Polynomen) auftreten, die wir schon hier kennenlernen wollen. Das sind vor allem die schon bekannten $\binom{x}{k}$, $\Phi_k(x)$, $\psi_k(x)$, $F_k(x)$ $(k = 0, 1, \ldots)$. Eine weitere solche Folge ist

$$(x)_k = k!\binom{x}{k} = x(x-1)\ldots(x-k+1) \qquad (k = 0, 1, \ldots). \tag{25}$$

Immer bezeichnen $k_0, k_1, \ldots$ die p-adischen Ziffern einer nichtnegativen ganzen Zahl k:

$$k = k_0 + k_1 p + k_2 p^2 + \cdots \qquad (0 \leqq k_0, k_1, \ldots \leqq p-1), \tag{26}$$

wobei es also unter den $k_0, k_1, \ldots$ nur endlichviele nichtverschwindende gibt. Für irgendeine Polynomfolge $f_k(x)$ $(k = 0, 1, \ldots)$ werde immer auch die weitere Folge

$$f^{(k)}(x) = f_0^{k_0}(x) f_1^{k_1}(x) \ldots \qquad (k = 0, 1, \ldots) \tag{27}$$

definiert, wobei rechts in der Wahrheit ein endliches Produkt steht. Insbesondere ist jedes $f^{(k)}(x)$ $(0 \leqq k \leqq p^e - 1)$ ein Potenzprodukt der $f_0(x), \ldots, f_{e-1}(x)$. Und

zwar bilden wir nach dieser Regel (10) nur die drei Polynomfolgen $\Phi^{(k)}(x)$, $\psi^{(k)}(x)$, $F^{(k)}(x)$ $(k = 0, 1, \ldots)$. Die erste und dritte hiervon hat die Eigenschaft, dass bei jedem Glied der Stellenzeiger k zugleich auch die Gradzahl ist, was aus (26), (27) und daraus folgt, dass $\Phi_k(x)$, $F_k(x)$ nach (14) und (16) vom Grade p^k sind.

Hat eine K-Polynomfolge $f_k(x)$ $(k = 0, 1, \ldots)$ die hier genannte Eigenschaft, dass nämlich k der Grad von $f_k(x)$ ist, so lässt sich jedes K-Polynom eindeutig in der Form

$$f(x) = a_0 f_0(x) + a_1 f_1(x) + \cdots \qquad (a_0, a_1, \ldots \in K) \tag{28}$$

schreiben. (Die rechte Seite ist eine endliche Summe.) Wir nennen (28) die Entwicklung von $f(x)$ nach $f_k(x)$ $(k = 0, 1, \ldots)$ und selbst die $a_0, a_1, \ldots$ die Entwicklungskoeffizienten. Diese sind in G, wenn $f(x)$ ein G-Polynom ist und die $f_k(x)$ G-Hauptpolynome sind. In allen unseren Entwicklungen (28) wird $f_0(x) = 1$, und so schreiben wir rechts für das konstante Glied einfach a_0.

§ 4. Beweis und Umformung des Satzes von Nagell.

Um den Beweis von Nagells Satz zu erleichtern, setzen wir allgemein

$$f_n(x) = a_0 \binom{x}{n} + a_1 \binom{x}{n-1} + \cdots + a_n, \tag{29}$$

und bemerken gleich, dass hieraus nach $\binom{x+1}{k} - \binom{x}{k} = \binom{x}{k-1}$ $(k = 1, 2, \ldots)$

$$f_n(x+1) - f_n(x) = a_0 \binom{x}{n-1} + \cdots + a_{n-1} \tag{30}$$

folgt. Sind $a_0, \ldots, a_n$ in G, so ist (29) offenbar G-haltend. Es ist nur noch zu beweisen, dass auch die Umkehrung gilt. Nehmen wir hierzu an, dass (29) G-haltend ist. Wegen der Annahme ist auch $f_n(x+1)$ G-haltend, und so gilt dasselbe über (30). Mit wiederholter Anwendung folgt, dass alle Polynome

$$a_0 \binom{x}{i} + \cdots + a_i \qquad (i = 0, \ldots, n)$$

G-haltend sind. Insbesondere für $x = 0$ folgt hieraus, dass jedes a_i in G ist, womit wir den Satz bewiesen haben.

Nagells Satz wollen wir noch in drei weiteren Formen ausdrücken, von denen sich jede aus der vorigen gewinnen lässt. Die letzte (vierte) Form werden wir dann zu unseren weiteren Zwecken verwenden. Diese wird wie auch Nagells

Satz die G-haltenden K-Polynome angeben, aber auf eine wesentlich andere Art. Die mittleren (zweite und dritte) Formen sprechen über die mod m überall verschwindenden G-Polynome. Die zweite Form wird sich aus der ersten einfach nach der Bemerkung bei (22) ergeben, ebenso die vierte aus der dritten, das wesentliche Glied unserer Schlusskette wird der Übergang von der zweiten zur dritten Form des Satzes sein.

Die zweite Form des Satzes ist von KEMPNER[18] und lautet so:

Ein beliebiges G-Polynom

$$f(x) = a_n (x)_n + \cdots + a_0 \tag{31}$$

verschwindet überall mod m dann und nur dann, wenn

$$m \mid k!\, a_k \qquad (k = 0, \ldots, n) \tag{32}$$

ist.

Zum Beweis dividieren wir (31) durch m und setzen (25) ein:

$$\frac{f(x)}{m} = \frac{n!\, a_n}{m} \binom{x}{n} + \cdots + \frac{0!\, a_0}{m}. \tag{33}$$

Damit $f(x)$ mod m überall verschwindet, ist notwendig und hinreichend, dass $\frac{f(x)}{m}$ G-haltend ist. Nach Nagells Satz ist die Bedingung hierfür, dass die Entwicklungskoeffizienten in (33) ganz sind, d. h. (32) gilt.

Die dritte Form des Satzes lautet so:

Satz 5. *Ein beliebiges G-Polynom*

$$f(x) = a_n F^{(n)}(x) + \cdots + a_0 \tag{34}$$

verschwindet überall mod p^e *dann und nur dann, wenn*

$$p^e \mid k!\, a_k \qquad (k = 0, \ldots, n) \tag{35}$$

ist.[33]

Wegen (16) und (27) ist nämlich

$$F^{(k)}(x) = p^{\varkappa_k} \Phi^{(k)}(x) \qquad (k = 0, 1, \ldots) \tag{36}$$

mit

$$\varkappa_k = \sum_{i \geqq 0} \frac{p^i - 1}{p - 1} k_i$$

[33] Kleine Bruchstücke von diesem Satz finden sich in den unter [29] zitierten Beispielen von Dickson. Es ist klar, dass durch Satz 5 die ähnliche Frage allgemein für jeden Modul m beantwortet wird, so dass man den Satz mit jedem $p^e (p^e \| m)$ anwendet.

d. h. nach (26)

$$\varkappa_k = \frac{k - (k_0 + k_1 + \cdots)}{p - 1}. \tag{37}$$

Hierfür gilt bekanntlich

$$p^{\varkappa_k} \| k! \qquad (k = 0, 1, \ldots). \tag{38}$$

Nehmen wir jetzt zuerst (35) an. Wir setzen (37) in (35) ein, so entsteht eine Entwicklung von $f(x)$ nach den $\Phi^{(k)}(x)$ mit Koeffizienten $p^{\varkappa_k} a_k$. Diese sind nach (35), (38) durch p^e teilbar. Andererseits sind nach (14) und dem Satz von Fermat die $\Phi_k(x)$, also auch die $\Phi^{(k)}(x)$ lauter G-Funktionen. Beide ergeben, dass die Glieder auf der rechten Seite von (34) für jedes $x\,(\in G)$ durch p^e teilbare Werte annehmen, und so verschwindet $f(x)$ überall mod p^e.

Nehmen wir umgekehrt letzteres an. Wir müssen zeigen, dass (35) gilt. Im Fall $n = 0$ ist das wegen $f(x) = a_0 F^0(x) = a_0$ klar. Im Fall $n \geqq 1$ setzen wir voraus, dass die Behauptung für die kleineren n richtig ist. Da $(x)_k$ und $F^{(k)}(x)$ Hauptpolynome k-ten Grades sind, so stimmen in (31) und (34) die a_n überein, woraus nach obigem Satz von Kempner

$$p^e \mid n!\, a_n$$

folgt. Dies ist eben der Fall $k = n$ von (35). Nach dem schon bewiesenen Teil des Satzes verschwindet also $a_n F^{(n)}(x)$ überall mod p^e, wegen der Annahme gilt dann dasselbe über

$$f(x) - a_n F^{(n)}(x) = a_{n-1} F^{(n-1)}(x) + \cdots + a_0.$$

Nach der Induktionsvoraussetzung folgt hieraus (35) für die übrigen $k = 0, \ldots, n - 1$, womit Satz 5 bewiesen ist.

Endlich lautet die vierte Form des Satzes so:

Satz 6. *Ein beliebiges K_p-Polynom*

$$f(x) = a_n \Phi^{(n)}(x) + \cdots + a_0 \tag{39}$$

ist dann und nur dann G-haltend, wenn $a_0, \ldots, a_n \in G$ gilt.[34]

Ist nämlich $a_0, \ldots, a_n \in G$, so ist $f(x)$ offenbar G-haltend. Nehmen wir umgekehrt letzteres an und bezeichnen mit p^e den Nenner von $f(x)$. Multiplizieren wir (39) mit p^e, so entsteht ein mod p^e überall verschwindendes G-Polynom.

[34] Offenbar lässt sich Satz 6 auch auf K-Polynome anwenden, so dass man dieses durch eine Partialbruchzerlegung ersetzt.

Setzen wir zugleich (36) ein, so muss nach Satz 5 für die Koeffizienten der $F^{(k)}(x)$

$$p^e \mid k! \frac{p^e a_k}{p^{\varkappa_k}} \qquad (k = 0, \ldots, n)$$

gelten. Wegen (38) ist dies äquivalent mit $a_k \in G$, und so haben wir Satz 6 bewiesen.

§ 5. Die Eigenschaften der Polynome $\Phi_k(x)$ und $\psi_k(x)$.

Wir wollen die an sich interessante und für die späteren Anwendungen wichtige Frage untersuchen, ob die G-haltenden K_p-Polynome $\Phi_k(x)$, $\psi_k(x)$ oder allgemeiner diese Polynome mit einem ganzzahligen Faktor versehen (mod p^e zulässig d. h.) $\mathfrak{R}(p^e)$-Funktionen sind. Ohne Einschränkung der Allgemeinheit ziehen wir nur Faktoren p^l $(l \geqq 0)$ in Betracht. Die Antwort ist enthalten im folgenden:

Satz 7. *Ist* $0 \leqq l < e$, *so darstellt das Polynom* $p^l \Phi_k(x)$ *oder* $p^l \psi_k(x)$ *eine* $\mathfrak{R}(p^e)$-*Funktion dann und nur dann, wenn* $k \leqq l$ *bzw.* $k < e$ *ist. Ist dagegen* $l \geqq e$, *so darstellen beide Polynome trivialerweise die Funktion* 0 *in* $\mathfrak{R}(p^e)$.

Bemerkung. Von diesem Satz wird für uns am wichtigsten, dass $\psi_k(x)$ $(k < e)$ eine $\mathfrak{R}(p^e)$-Funktion ist. Weitere interessante, später anzuwendende Beispiele sind die folgenden:

1) $p^{k-1}\psi_k(x)$ ist dann und nur dann eine $\mathfrak{R}(p^e)$-Funktion, wenn $k \neq e$ ist.

2) $p^{k-1}\Phi_k(x)$ ist dann und nur dann eine $\mathfrak{R}(p^e)$-Funktion, wenn $k > e$ ist.

Zum Beweis des Satzes zeigen wir zuerst, dass für jedes ganze a

$$\Phi_k(a + p^e) = \Phi_k(a) + p^{e-k} t \qquad (0 \leqq k \leqq e;\ p \nmid t) \tag{40}$$

gilt mit einem ganzen, zu p primen t.

Dies ist nämlich richtig für $k = 0$, da dann $\Phi_0(x) = x$ ist. Schreiben wir (14) in der Form

$$p\,\Phi_{k+1}(x) = \Phi_k^p(x) - \Phi_k(x).$$

Wenn wir (40) für ein k mit $0 \leqq k < e$ voraussetzen, so folgt aus letzterem

$$p\,(\Phi_{k+1}(a + p^e) - \Phi_{k+1}(a)) = (\Phi_k(a) + p^{e-k} t)^p - \Phi_k^p(a) - p^{e-k} t.$$

Die rechte Seite ist $\equiv -p^{e-k} t \pmod{p^{e-k+1}}$, und so folgt weiter

$$\Phi_{k+1}(a + p^e) - \Phi_{k+1}(a) \equiv -p^{e-k-1} t \pmod{p^{e-k}}.$$

Dies beweist (40) für $k + 1$ (statt k), und somit gilt (40) allgemein.

Insbesondere für $e = k$ folgt aus (40)

$$\Phi_k(a + p^k) \not\equiv \Phi_k(a) \pmod{p} \qquad (k = 0, 1, \ldots). \tag{41}$$

Erhebe man (40) für $k < e$ (k-mal wiederholt zur p-ten d. h.) zur p^k-ten Potenz. Das ergibt

$$\psi_k(a + p^e) \equiv \psi_k(a) \pmod{p^e} \qquad (0 \leqq k < e). \tag{42}$$

Endlich ergibt (41)

$$\psi_k(a + p^k) \not\equiv \psi_k(a) \pmod{p} \qquad (k = 0, 1, \ldots). \tag{43}$$

Aus (40)—(43) folgt die Richtigkeit des Satzes.

§ 6. Das normale System $\mathfrak{S}$. Beweis von Satz 3.

Nach Satz 7 sind die Polynome $\psi_0(x), \ldots, \psi_{e-1}(x)$ lauter $\mathfrak{R}(p^e)$ Funktionen. Dann gilt ähnliches über alle $g(\psi_0(x), \ldots, \psi_{e-1}(x))$, wobei $g(x_0, \ldots, x_{e-1})$ ein beliebiges G-Polynom von $x_0, \ldots, x_{e-1}$ ist. Insbesondere ist jedes $\psi^{(k)}(x)$ $(k = 0, \ldots, p^e - 1)$ als ein Potenzprodukt der $\psi_0(x), \ldots, \psi_{e-1}(x)$ eine $\mathfrak{R}(p^e)$-Funktion. Wir beweisen den folgenden Satz, mit dem zugleich auch Satz 3 bewiesen wird.

Satz 8. *Die K_p-Polynome*

$$f(x) = \sum_{k=0}^{p^e-1} c_k \psi^{(k)}(x) \qquad (c_k = 0, \ldots, p^e - 1) \tag{44}$$

darstellen eben alle verschiedenen $\mathfrak{R}(p^e)$-Funktionen. Dieses (44) nennen wir das normale Representantensystem $\mathfrak{S}$ von $\mathfrak{R}(p^e)(x)$.

Bemerkung. Nach (27) besteht $\mathfrak{S}$ offenbar aus allen Polynomen

$$g(\psi_0(x), \ldots, \psi_{e-1}(x)) \tag{45}$$

mit Exponenten $0, \ldots, p - 1$ und Koeffizienten $0, \ldots, p^e - 1$.

Nach obigem ist jedes $f(x)$ in (44) eine $\mathfrak{R}(p^e)$-Funktion. Andererseits ist die Anzahl $(p^e)^{p^e}$ dieser $f(x)$ eben die Anzahl der $\mathfrak{R}(p^e)$-Funktionen, deshalb genügt es zu zeigen, dass die $f(x)$ lauter verschiedene $\mathfrak{R}(p^e)$-Funktionen darstellen. Da die Differenz zweier $f(x)$ wieder ein $f(x)$ ist — die Koeffizienten c_k kommen nämlich bloss mod p^e in Betracht — so brauchen wir nur zu zeigen, dass (44) nur im Fall $p^e \mid c_k$ $(k = 0, \ldots, p^e - 1)$ die $\mathfrak{R}(p^e)$-Funktion 0 darstellt.

Hierzu nehmen wir an, dass es ein $f(x)$ gibt, das die $\mathfrak{R}(p^e)$-Funktion 0 darstellt, und trotzdem nicht alle c_k verschwinden. Dann gibt es eine ganze Zahl r mit $0 \leqq r < e$, so dass

$$c_k = p^r c_k^* \qquad (k = 0, \ldots, p^e - 1)$$

gilt, wobei die c_k^* ganz und nicht alle durch p teilbar sind. Dividieren wir (44) durch p^r, so folgt aus der Voraussetzung

$$\sum_{k=0}^{p^e-1} c_k^* \psi^{(k)}(x) \equiv 0 \pmod{p} \qquad (x \in G).$$

Nach (15), (27) und dem Satz von Fermat darf in dieser Kongruenz ψ durch Φ ersetzt werden, und das heisst, dass das Polynom

$$\sum_{k=0}^{p^e-1} c_k^* \Phi^{(k)}(x)$$

die $\mathfrak{R}(p)$-Funktion 0 darstellt. Wenn man also dieses durch p dividiert, so entsteht ein G-haltendes K_p-Polynom, wobei aber nicht alle Koeffizienten $\frac{c_k^*}{p}$ ganz sind. Dies widerspricht Satz 6, womit wir Satz 8 bewiesen haben.

§ 7. Das minimale System $\mathfrak{S}_0$.

Satz 9. *Entwickle man die Glieder* (44) *von* $\mathfrak{S}$ *nach* $\Phi^{(k)}(x)$ $(k = 0, 1, \ldots)$[35], *und ersetze die Entwicklungskoeffizienten durch ihren kleinsten nichtnegativen Rest mod* p^e. *Die so entstandenen* K_p*-Polynome* $f_0(x)$ *darstellen wieder alle verschiedenen* $\mathfrak{R}(p^e)$*-Funktionen, und dabei fallen Nenner und Grad dieser Polynome möglichst klein aus. Die Gesamtheit aller* $f_0(x)$ *nennen wir das minimale Representantensystem* $\mathfrak{S}_0$ *von* $\mathfrak{R}(p^e)(x)$.

Bemerkung. Wie einfach auch die Vorschrift ist, mit der man $\mathfrak{S}_0$ berechnen kann, trotzdem ist $\mathfrak{S}_0$ — wie schon erwähnt — von sehr komplizierter Struktur (vgl. den nächsten §). Deshalb können wir sagen, dass die $\psi_k(x)$ ein viel bequemeres Mittel zur Beschreibung der $\mathfrak{R}(p^e)$-Funktionen sind als die $\Phi_k(x)$.

Zum Beweis bemerken wir vor allem, dass eine (endliche) Summe $\Sigma a_k \Phi^{(k)}(x)$ dann und nur dann die $\mathfrak{R}(p^e)$-Funktion 0 darstellt, wenn alle Entwicklungskoeffizienten a_k durch p^e teilbare ganze Zahlen sind. Dies folgt nämlich aus Satz 6 mit ähnlichem Schluss, wie am Ende des vorigen §. Zwei solche Summen, von denen wenigstens die eine eine $\mathfrak{R}(p^e)$-Funktion ist, darstellen also dann und nur dann dieselbe $\mathfrak{R}(p^e)$-Funktion, wenn die Paare entsprechender Entwicklungskoeffizienten mod p^e kongruent sind.

[35] Dies geht wegen (27) und (15) mit wiederholter Anwendung von (14), das man zu diesem Zweck in der Form (49) schreibt. (Vgl. die Beispiele in § 8.)

Es sei

$$f_0(x) = \Sigma a_k \Phi^{(k)}(x) \qquad (a_k = 0, \ldots, p^e - 1) \tag{46}$$

ein beliebiges Glied von $\mathfrak{S}_0$ und

$$f(x) = \Sigma b_k \Phi^{(k)}(x) \qquad (b_k \in G) \tag{47}$$

ein weiteres (G-haltendes) Polynom, von dem wir annehmen, dass es dieselbe $\mathfrak{R}(p^e)$-Funktion wie $f_0(x)$ darstellt, d. h.

$$a_k \equiv b_k \pmod{p^e} \qquad (k = 0, 1, \ldots) \tag{48}$$

ist. Wir haben zu beweisen, dass Nenner und Grad von $f(x)$ mindestens so gross ist wie der von $f_0(x)$, wobei wir $f_0(x), f(x) \neq 0$ annehmen dürfen.

Für den Grad folgt das leicht, denn jedes $\Phi^{(k)}(x)$ ist vom Grad k, und wenn ein $a_k \neq 0$ ist, so ist nach (48) noch mehr $b_k \neq 0$.

Bezeichne p^r das Maximum des Nenners der Glieder in (47), und nehmen wir an, dass k der grösste Index ist, für den $b_k \Phi^{(k)}(x)$ den Nenner p^r hat. Da dieses Polynom zu einem G-Hauptpolynom (nämlich zu $F^{(k)}(x)$) assoziiert ist, so muss p^r zugleich der Nenner von $f(x)$ sein. Ähnlich wie r, k seien r_0, k_0 für $f_0(x)$ definiert, woraus wieder folgt, dass p^{r_0} der Nenner sowohl von $a_{k_0} \Phi^{(k_0)}(x)$ als auch von $f_0(x)$ ist. Wegen (48) hat auch $b_{k_0} \Phi^{(k_0)}(x)$ den Nenner p^{r_0}, und so muss $p^r \geqq p^{r_0}$ sein, woraus die Richtigkeit des Satzes folgt.

§ 8. Beispiele.

Wir berechnen $\mathfrak{S}_0$ für $e = 2, 3$ (der Fall $e = 1$ ist uninteressant), schliessen dabei $p = 2$ aus. Kurz schreiben wir Φ_k, ψ_k für $\Phi_k(x), \psi_k(x)$. Nach (14) und (15) ist

$$\Phi_k^p = \Phi_k + p\,\Phi_{k+1}, \tag{49}$$

$$\psi_k = \Phi_k^{p^k}.$$

Wir bekommen

$$\psi_0 = \Phi_0,\ \psi_1 = \Phi_1 + p\,\Phi_2,$$

$$\psi_2 \equiv \Phi_2 + p\,\Phi_3 + p^2\,\Phi_2^{p-1}\,\Phi_3 \pmod{p^3}.^{36}$$

Mit Berücksichtigung dieser Formeln lässt sich das allgemeine Glied $f_0(x)$ von $\mathfrak{S}_0$ für $e = 2, 3$ berechnen.

---

[36] Es ist nämlich

$$\psi_2 = (\Phi_1 + p\,\Phi_2)^p = \Phi_1^p + p^2\,\Phi_1^{p-1}\,\Phi_2 + \cdots$$

wobei man wieder $\Phi_1^p = \Phi_1 + p\,\Phi_2$ einzusetzen hat. In diesem § beziehen sich die Kongruenzen auf die Koeffizienten der Entwicklungen nach $\Phi^{(k)}(x)$ $(k = 0, 1, \ldots)$

Fall $e = 2$. Es ist

$$f_0(x) \equiv \sum_{r=0}^{p-1} \sum_{s=0}^{p-1} c_{rs} \psi_0^r \psi_1^s \pmod{p^2} \qquad (c_{rs} = 0, \ldots, p^2 - 1).$$

Fall $e = 3$. Es ist

$$f_0(x) \equiv \sum_{r=0}^{p-1} \sum_{s=0}^{p-1} \sum_{t=0}^{p-1} c_{rst} \psi_0^r \psi_1^s \psi_2^t \pmod{p^3} \qquad (c_{rst} = 0, \ldots, p^3 - 1).$$

Nach Ausmultiplizieren sind die Koeffizienten mod p^2 bzw. mod p^3 auf den kleinsten nichtnegativen Rest zu reduzieren, dabei ist beim letzteren (49) wiederholt zu berücksichtigen. So bekommen wir in diesen Fällen für die am Schluss des § 1 erwähnten Zahlen $\nu(p^e)$, $g(p^e)$:

$$\nu(p^2) = 2p - 2, \qquad g(p^2) = 2p^2 - p - 1,$$
$$\nu(p^3) = 3p^2 + p - 4, \qquad g(p^3) = 3p^3 - 2p^2 - 1.$$

Allgemein bekommen wir mit Hilfe von $\mathfrak{S}$ eine, allerdings sehr grobe obere Schranke für ν und g. Nach Satz 8 erreichen nämlich Nenner und Grad von $\mathfrak{S}$ das Maximum gewiss für

$$(\psi_0(x)\psi_1(x) \ldots \psi_{e-1}(x))^{p-1}.$$

Bezeichnen $p^{\nu'}$ und g' den Nenner bzw. Grad dieses Polynoms, so gilt nach (14)—(16):

$$\nu' = (p-1)\left(p + \frac{p^2-1}{p-1} p^2 + \cdots + \frac{p^{e-1}-1}{p-1} p^{e-1}\right),$$
$$g' = (p-1)(1 + p^2 + p^4 + \cdots + p^{2e-2}).$$

Da offenbar $\nu \leqq \nu'$, $g \leqq g'$ ist, so gilt

$$\nu(p^e) \leqq \frac{(p^e - 1)(p^e - p)}{p^2 - 1}, \qquad g(p^e) \leqq \frac{p^{2e} - 1}{p + 1}.$$

Die genaue Berechnung von ν, g scheint auf obigem Wege für den allgemeinen Fall unausführbar zu sein.

§ 9. Die Zurückführung des allgemeinen Falles auf $m = p^e$.

Jetzt kehren wir uns dem allgemeinen Fall $m(\neq 1)$ zu, und wollen untersuchen, inwieweit sich die $\mathfrak{R}(m)$ Funktionen durch K-Polynome darstellen lassen. Wir schicken die Bemerkung voran, dass

(50) $$\mathfrak{R}(m) \sim \mathfrak{R}(d) \qquad (d \mid m)$$

gilt, und zwar lässt sich $\mathfrak{R}(m)$ auf $\mathfrak{R}(d)$ (nur) so homomorph abbilden, dass man jeder Restklasse mod m die sie enthaltende Restklasse mod d zuordnet. Die Beantwortung der gestellten Frage ist enthalten in den folgenden zwei Sätzen:

Satz 10. *Ein K-Polynom darstellt eine $\mathfrak{R}(m)$-Funktion dann und nur dann, wenn es auch in jedem $\mathfrak{R}(p^e)$ $(p^e \| m)$ eine Funktion darstellt. Auch gilt noch folgendes: Es liege irgendeine Partialbruchzerlegung*

$$f(x) = \sum_{p|m} f_p(x) \tag{51}$$

vor, wobei $f(x)$ ein K-Polynom, $f_p(x)$ ein K_p-Polynom ist. Dann und nur dann darstellt $f(x)$ eine $\mathfrak{R}(m)$-Funktion, wenn jedes $f_p(x)$ eine $\mathfrak{R}(p^e)$-Funktion darstellt $(p^e \| m)$.

Satz 11. *Eine $\mathfrak{R}(m)$-Funktion lässt sich dann und nur dann durch ein K-Polynom darstellen, wenn sie für jede Homomorphie $\mathfrak{R}(m) \sim \mathfrak{R}(p^e)$ $(p^e \| m)$ zulässig ist, das bedeutet jetzt, dass durch die Funktion den in einer p^e-Restklasse[37] enthaltenen m-Restklassen lauter solche m-Restklassen zugeordnet werden, die wieder in einer p^e-Restklasse enthalten sind. (Kurz heisst das, dass die entsprechenden homomorphen Bilder der angegebenen Funktion lauter eindeutige $\mathfrak{R}(p^e)$-Funktionen sind.) Die Anzahl der durch K-Polynome darstellbaren $\mathfrak{R}(m)$-Funktionen ist*

$$\prod_{p|m} p^{ep^e}\ ^{38} \qquad (p^e \| m). \tag{52}$$

Bemerkung. Nach diesen Sätzen lassen sich alle unseren Fragen bezüglich $\mathfrak{R}(m)$ auf den vorher erledigten Spezialfall $m = p^e$ zurückführen. Gegen den einfachen Wortlaut von Satz 10 wird der Beweis etwas mühsam. Dabei stützen wir uns auf Satz 4, von dem wir in den vorigen bisher keinen Gebrauch gemacht haben.

Zuerst beweisen wir folgenden:

Hilfssatz. *Ist $f(x)$ ein K-Polynom und c eine ganze Zahl so, dass $cf(x)$ in G liegt, so liegt auch das Polynom*

$$\frac{1}{m}(f(x + cm) - f(x)) \tag{53}$$

in G (m beliebig).

---

[37] Wir sagen „m-Restklasse" statt „Restklasse mod m".

[38] Ersetzt man in (52) den Exponenten ep^e durch em, so bekommt man die Anzahl aller $\mathfrak{R}(m)$-Funktionen, und so sehen wir, dass im allgemeinen nur verhältnismässig wenige von diesen sich durch K-Polynome darstellen lassen.

Setzen wir nämlich $g(x) = cf(x)$, das nach der Annahme ein G-Polynom ist. Da sich (53) nach Newtons Satz in der Form

$$g'(x) + cm\frac{g''(x)}{2!} + c^2m^2\frac{g'''(x)}{3!} + \cdots$$

schreiben lässt, so sehen wir die Richtigkeit des Hilfssatzes ein.

Zum Beweis der ersten Hälfte von Satz 10 dürfen wir uns auf den Fall beschränken, in dem das angegebene Polynom in K_m liegt und G-haltend ist. Bezeichne $f(x)$ ein solches Polynom, von dem wir zuerst annehmen, dass es eine $\mathfrak{N}(m)$-Funktion darstellt. Nach Satz 4 ist dann (24) G-haltend, und dann gilt dasselbe über das Polynom $\frac{1}{m}(f(x + cm) - f(x))$, wobei c eine später zu bestimmende ganze Zahl ist. Noch mehr ist das Polynom

$$\frac{1}{p^e}(f(x + cm) - f(x)) \tag{54}$$

G-haltend. Zerlegen wir $f(x)$ in eine Summe

$$f(x) = g(x) + h(x) \tag{55}$$

so, dass $g(x)$ ein K_p-Polynom ist und $h(x)$ einen zu p primen Nenner hat. Dann sind mit $f(x)$ zusammen auch $g(x)$, $h(x)$ G-haltend, ferner ist $h(x)$ auch zulässig mod p^e. Hieraus folgt, dass

$$\frac{1}{p^e}(h(x + cm) - h(x))$$

G-haltend ist, und so muss wegen (54), (55) auch

$$\frac{1}{p^e}(g(x + cm) - g(x)) \tag{56}$$

G-haltend sein. Wählen wir jetzt c so, dass $\left(c\frac{m}{p^e} - 1\right)g(x)$ in G liegt, was wegen $\left(p^e, \frac{m}{p^e}\right) = 1$ möglich ist. Aus dem Hilfssatz folgt, dass

$$\frac{1}{p^e}(g(x + cm - p^e) - g(x))$$

G-haltend ist. Subtrahiert man dies aus (56) und ersetzt $x + cm - p^e$ durch x, so entsteht, dass auch

$$\frac{1}{p^e}(g(x + p^e) - g(x))$$

G-haltend ist. Da $g(x)$ auch G-haltend ist, so folgt aus Satz 4, dass $g(x)$ eine $\mathfrak{R}(p^e)$-Funktion ist. Dies gilt nach obigem auch über $h(x)$, und so ist $f(x)$ nach (55) ebenfalls eine $\mathfrak{R}(p^e)$-Funktion.

Wenn dies umgekehrt der Fall, d. h. $f(x)$ für jeden mod p^e zulässig ist ($p^e \| m$), so ist $f(x)$ offenbar auch mod m zulässig, d. h. eine $\mathfrak{R}(m)$-Funktion. Hiermit haben wir die erste Hälfte von Satz 10 bewiesen.

Die zweite Hälfte des Satzes folgt leicht aus der jetzt bewiesenen ersten Hälfte. Man kann sich nämlich auf den Fall beschränken, in dem $f(x)$ d. h. auch jeder Summand in (51) G-haltend ist. Für jedes p sind dann die von $f_p(x)$ verschiedenen Glieder auf der rechten Seite von (51) lauter $\mathfrak{R}(p^e)$-Funktionen. Ist nun $f(x)$ eine $\mathfrak{R}(m)$-Funktion, so ist $f(x)$ nach der ersten Hälfte des Satzes zugleich auch eine $\mathfrak{R}(p^e)$-Funktion ($p^e \| m$), und dann muss in der Tat auch das noch übriggebliebene Glied $f_p(x)$ eine $\mathfrak{R}(p^e)$-Funktion sein. Ist das umgekehrt für jedes p der Fall, so folgt, dass $f(x)$ eine $\mathfrak{R}(p^e)$-Funktion ist ($p^e \| m$), und dann ist es auch eine $\mathfrak{R}(m)$-Funktion. So haben wir Satz 10 bewiesen.

Zum Beweis von Satz 11 betrachten wir zuerst eine $R(m)$-Funktion, die durch ein K-Polynom $f(x)$ darstellt wird. Nach Satz 10 gilt dann

$$f(x) \equiv f(y) \pmod{p^e} \qquad (x \equiv y \pmod{p^e};\ p^e \| m). \tag{57}$$

Bestimmen wir das (durch $\mathfrak{R}(m) \sim \mathfrak{R}(p^e)$ vermittelte) homomorphe Bild $\tilde{f}_p(x)$ unserer Funktion. Hierzu betrachten wir eine beliebige Restklasse $x \pmod{p^e}$. Diese enthält alle Restklassen $y \pmod{m}$, wobei $y \equiv x \pmod{p^e}$ ist. Einer solchen Restklasse ordnet unsere Funktion die Restklasse $f(y) \pmod{m}$ zu, die seinerseits in der Restklasse $f(y) \pmod{p^e}$ enthalten ist, und so wird durch $\tilde{f}_p(x)$ einer beliebigen Restklasse $y \pmod{p^e}$ immer nur eine Restklasse $f(y) \pmod{p^e}$ zugeordnet. Wegen (57) ist diese Zuordnung, d. h. auch selbst die $\mathfrak{R}(p^e)$-Funktion $\tilde{f}_p(x)$ eindeutig.

Umgekehrt betrachten wir eine $\mathfrak{R}(m)$-Funktion, von der wir jetzt annehmen, dass die ähnlich wie vorher definierten homomorphen Bilder lauter eindeutige $\mathfrak{R}(p^e)$-Funktionen sind ($p^e \| m$), die dann nach Satz 3 durch gewisse K_p-Polynome $f_p(x)$ darstellt werden. Zu jedem $p\,(p \mid m)$ bestimmen wir eine ganze Zahl c_p mit

$$c_p \equiv 1 \pmod{p^e}, \qquad c_p \equiv 0 \left(\mathrm{mod}\ \frac{m}{p^e}\right) \tag{58}$$

und bilden die Summe

$$f(x) = \sum_{p \mid m} c_p f_p(x). \tag{59}$$

Dann ist $f(x)$ ein G-haltendes K_m-Polynom. Nach der Annahme ist

$$f_p(x) \equiv f_p(y) \pmod{p^e} \qquad (x \equiv y \pmod{p^e}),$$

woraus offenbar

$$f_p(x) \equiv f_p(y) \pmod{m} \qquad (x \equiv y \pmod{m})$$

folgt. Dies ergibt nach (59), dass $f(x)$ eine $\mathfrak{R}(m)$-Funktion darstellt. Die homomorphen Bilder dieser Funktion sind nach (59), (58) eben die $\mathfrak{R}(p^e)$-Funktionen $f_p(x)\,(p|m)$, wie man das leicht einsieht. Wenn aber zu zwei $\mathfrak{R}(m)$-Funktionen dasselbe System homomorpher Bilder gehört, so müssen diese $\mathfrak{R}(m)$-Funktionen gleich sein, was nämlich aus dem chinesischen Restsatz leicht folgt. Das bedeutet, dass die betrachtete $\mathfrak{R}(m)$-Funktion durch das Polynom $f(x)$ darstellt wird.

Die noch übriggebliebene Behauptung (52) folgt nunmehr aus dem schon bewiesenen Teil von Satz 11 und aus der zweiten Hälfte von Satz 10. Nach diesen werden nämlich alle verschiedenen, durch K-Polynome darstellbaren $\mathfrak{R}(m)$-Funktionen durch die Polynome (51) darstellt, indem man für jeden Summanden $f_p(x)$ voneinander unabhängig die Elemente eines vollen Representantensystems von $\mathfrak{R}(p^e)(x)$ (z. B. die Elemente des normalen Systems $\mathfrak{S} = \mathfrak{S}(p^e)$) einsetzt. Da die Zahl dieser Möglichkeiten eben (52) ist, so haben wir Satz 11 bewiesen.

§ 10. Die Bestimmung aller $\mathfrak{R}(m)$, in denen ein gegebenes K-Polynom eine Funktion darstellt.

Wir wenden uns dem im § 1 schon erwähnten, für die Zahlentheorie wichtigen Problem zu, das darin besteht, dass man im Falle eines gegebenen K_p-Polynoms $f(x)$ diejenigen m bestimmt, für die $f(x)$ eine $\mathfrak{R}(m)$-Funktion, d. h. mod m zulässig ist. Wir sagen (mit einem ähnlichen Ausdruck), dass diese Moduln m für das Polynom $f(x)$ zulässig sind (oder $f(x)$ lässt m zu), und definieren bequemlichkeitshalber die „charakteristische Funktion" $\chi(f(x), m)$ so, dass sie 1 oder 0 ist, je nachdem m für $f(x)$ zulässig oder nicht zulässig ist. Dann kommt es nur auf die Bestimmung von $\chi(f(x), m)$ an. Wir betrachten nur ein G-haltendes $f(x)$, da sonst gewiss $\chi(f(x), m) = 0$ ist.

Liegt $f(x)$ in G, so gilt unbeschränkt $\chi(f(x), m) = 1$. Allgemeiner gilt dies, wenn m zum Nenner von $f(x)$ prim ist. Ferner folgt aus Satz 10 die Produktformel:

$$\chi(f(x), m) = \prod_{p|m} \chi(f(x), p^e) \qquad (p^e \| m). \tag{60}$$

Hiernach genügt es nur $\chi(f(x), p^e)$ zu bestimmen, und dabei darf angenommen werden, dass $f(x)$ ein (G-haltendes) K_p-Polynom ist.

Nachdem wir so das Problem auf diesen Fall reduziert haben, gewinnen wir die Lösung nach Satz 9 mit Hilfe des minimalen Systems $\mathfrak{S}_0$ folgenderweise. Entwickeln wir $f(x)$ nach der Polynomfolge $\Phi^{(k)}(x)$ $(k = 0, 1, \ldots)$. Da $f(x)$ G-haltend ist, müssen die Entwicklungskoeffizienten ganz sein.[39] Ersetzen wir diese mit dem kleinsten nichtnegativen Rest mod p^e, wodurch ein Polynom $f_0(x)$ entsteht. Offenbar ist nach Satz 9 dann und nur dann $\chi(f(x), p^e) = 1$, wenn $f_0(x)$ ein Element von $\mathfrak{S}_0 (= \mathfrak{S}_0(p^e))$ ist, und dann gilt sogar, dass $f(x)$ und $f_0(x)$ dieselbe $\mathfrak{R}(p^e)$-Funktion darstellen.

Wohl können wir das obige Problem mit dieser Antwort für gelöst erklären, aber es tritt noch folgende, sehr interessante Frage auf. Halten wir ein (sonst beliebiges) p fest und fassen alle G-haltenden K_p-Polynome $f(x)$ ins Auge. Kann dann die Folge $\chi(f(x), p^e)$ $(e = 0, 1, \ldots)$ beliebig sein, d. h. in eine beliebig vorgegebene Zahlenfolge $a_1, a_2, \ldots$ $(a_i = 0, 1)$ übergehen? Das ist schon aus dem Grunde unmöglich, dass es über abzählbar viele solche Zahlenfolgen und nur abzählbar viele Polynome $f(x)$ gibt. Dagegen gilt der folgende überraschende:

Satz 12. *Es sei eine Folge* $a_1, a_2, \ldots$ $(a_i = 0, 1)$ *irgendwie vorgegeben so, dass darin entweder nur endlich viele Glieder* 0 *oder nur endlich viele Glieder* 1 *vorkommen. Für jedes* p *gibt es ein* G*-haltendes* K_p*-Polynom* $f(x)$ *mit*

$$\chi(f(x), p^e) = a_e \qquad (e = 1, 2, \ldots). \tag{61}$$

Bemerkung. Für den Fall, in dem alle a_i gleich 1 sind, liefert dieser Satz nichts neues, denn dann wird (61), wie schon öfter erwähnt, durch alle G-Polynome $f(x)$ befriedigt. Unten im Satz 13 werden wir weitere solche Polynome angeben.

Wir beweisen Satz 12 so, dass wir ein $f(x)$ explizit konstruieren das (61 befriedigt. Es seien

$$a, b, \ldots, k, l \qquad (1 \leqq a < b < \cdots < k < l) \tag{62}$$

endlich viele verschiedene positive ganze Zahlen nach der Grösse geordnet. Wir setzen

$$f_1(x) = p^{a-1}\psi_a(x) + p^{b-1}\psi_b(x) + \cdots + p^{k-1}\psi_k(x), \tag{63}$$

$$f_2(x) = f_1(x) + p^{l-1}\Phi_l(x). \tag{64}$$

[39] Man braucht nicht im voraus zu wissen, ob $f(x)$ G-haltend ist, sondern man kann es gleich mit obiger Entwicklung anfangen, denn nach Satz 6 wird eben durch diese Entwicklung entschieden, ob $f(x)$ wirklich G-haltend ist.

Nach dem Beispiel 1) in § 5 ist ein beliebiges Glied $p^{i-1}\psi_i(x)$ von $f_1(x)$ dann und nur dann keine $\Re(p^e)$-Funktion, wenn $i = e$ ist. Folglich ist $\chi(f_1(x), p^e) = 0$ dann und nur dann, wenn e eine der Zahlen $a, b, \ldots, k$ ist.

Nach dem Beispiel 2) in § 5 ist ferner das Glied $p^{l-1}\Phi_l(x)$ von $f_2(x)$ dann und nur dann eine $\Re(p^e)$-Funktion, wenn $e < l$ ist. Dies mit dem vorigen zusammen ergibt offenbar, dass dann und nur dann $\chi(f_2(x), p^e) = 0$ ist, wenn e eine der Zahlen $a, b, \ldots, k, l, l+1, l+2, \ldots$ ist.

Nach passender Wahl von (62) liefert also (63) oder (64) eine Lösung von (61), je nachdem es unter den a_i nur endlich viele 0 bzw. nur endlich viele 1 gibt. Hierdurch haben wir Satz 12 bewiesen.

Satz 13. *Bilde man die K_p-Polynome*

$$p\,\psi_1(x),\ p^2\,\psi_2(x),\ p^3\,\psi_3(x),\ \ldots$$

für alle Primzahlen p. Der durch diese Polynome und durch die G-Polynome gebildete Ring besteht aus lauter solchen Polynomen $f(x)$, für die mit jedem m

$$\chi(f(x), m) = 1 \tag{65}$$

gilt.

Nach dem am Anfang von diesem § gesagten ist dieser Satz eine Folgerung der Teilbehauptung, dass $\chi(p^l\psi_l(x), p^e) = 1$ $(l, e = 1, 2, \ldots)$ ist. Dieses ist ein Spezialfall von Satz 7, womit wir Satz 13 bewiesen haben.

Bemerkung. In mehr expliziter Form bedeutet (65), dass für das K-Polynom $f(x)$ mit jedem m

$$f(x) \equiv f(y) \pmod{m} \qquad (x, y \in G;\ x \equiv y \pmod{m}) \tag{66}$$

gilt. Die Polynome mit dieser Eigenschaft können wir deshalb als eine Verallgemeinerung der G-Polynome ansehen. (Das sind die K-Polynome, die jeden Modul m zulassen.) Wir wissen nicht, ob wir durch Satz 13 alle solche Polynome angegeben haben. Wir bemerken den Spezialfall aus Satz 13:

$$p^{p-1}\psi_1(x) = \frac{(x^p - x)^p}{p}.$$

Dies ist wohl das allereinfachste Beispiel für ein Polynom mit rationalen (nicht ganzen) Koeffizienten und der Eigenschaft (66)

§ 11. Die Verschärfung eines Satzes von Kempner.

Zuletzt wollen wir uns noch mit einem Satz von KEMPNER[40] beschäftigen, der sich auf die mod m überall verschwindenden G-Polynome bezieht, dabei von unserem Hauptthema etwas abseits liegt. Der Satz gibt das Minimum des Grades an unter der Bedingung, dass das betrachtete Polynom ein Hauptpolynom ist. Wir haben das überraschende Resultat bekommen, dass dasselbe Minimum auch dann gilt, wenn alle, zu m primen Polynome zugelassen werden. Wir fassen das in den folgenden:

Sats 14. *Unter allen, zu m primen,* mod m *überall verschwindenden G-Polynomen von minimalem Grad gibt es auch Hauptpolynome. Dieser minimale Grad ist die Faktorialbasis von m, worunter wir die kleinste natürliche Zahl m_0 mit*

$$m \mid m_0! \tag{67}$$

verstehen.[41]

Bezeichne nämlich P einen Primzahlpotenzfaktor von m mit

$$P \nmid (m_0 - 1)!; \tag{68}$$

ein solches P gibt es gewiss, da sonst $m \mid (m_0 - 1)!$ wäre, gegen die Annahme. Wir betrachten ein beliebiges Polynom $f(x)$ aus Satz 14, das wir gleich in der Form (31) schreiben, wobei dann n der Grad von $f(x)$ ist. Da $f(x)$ zu m prim ist, muss es einen Koeffizienten a_k geben, der zu P prim ist, woraus nach (32) $P \mid k!$ folgt. Dies und (68) ergeben $k > m_0 - 1$, $k \geqq m_0$, und dann gilt noch mehr $n \geqq m_0$. Andererseits ist $(x)_{m_0}$ ein G-Hauptpolynom m_0-ten Grades, das nach (25) mod m überall verschwindet. Somit haben wir den Satz bewiesen.

Bemerkung bei der Korrektur. Die vorliegende Mitteilung I wird in der Mitteilung II durch mehrere wichtige Resultate ergänzt, die teils inzwischen entstanden sind. So bekommen wir (vgl. Satz 3 und Fussnote[27]): Für $m \neq p^e$ hat $\mathfrak{R}(m)$ keinen Darstellungsring. Weiter gilt: K liefert die beste »Annäherung» der Lösung unseres Problems für $\mathfrak{R}(m)$, denn ist T irgendein primitiver Ring von $\mathfrak{R}(m)$, so werden doch durch T-Polynome nur solche $\mathfrak{R}(m)$-Funktionen darstellt (im Sinne des Grundsatzes), die schon durch $T = K$ erfasst wurden (vgl. Satz 11). Für einen allgemeinen Ring R bekommen wir: Damit R einen Darstellungsring hat ist not-

[40] Siehe [18] S. 245, auch bei DICKSON [19] S. 22, IV.

[41] Dieser Satz lässt sich auch aus den Resultaten von PÓLYA [13] (S. 103, Satz IV und S. 107) gewinnen.

wendig, dass in der additiven Gruppe R^+ alle Elemente eine endliche Ordnung haben und diese Ordnungen Potenzen einer festen Primzahl sind. Hiernach haben verhältnismässig wenig Ringe einen Darstellungsring. (Die Bedeutung hiervon wird dadurch stark betont dass — wie wir zeigen werden — unter Annahme gewisser Postulate überhaupt keine anderen Darstellungen der R-Funktionen durch Polynome denkbar sind als die im Grundsatz beschriebenen.) Für $\mathfrak{N}(p^e)$ erwähnen wir noch, dass uns gelang $g(p^e)$, $\nu(p^e)$ genan zu berechnen (vgl. das Ende von § 1 und § 8):

$$g(p^e) = e\,p^e - (e-1)\,p^{e-1} - 1,$$

$$p^{\nu(p^e)+e-1} \parallel g\,p^e!$$