ALGEBRAISCH-ZAHLENTHEORETISCHE BETRACHTUNGEN ÜBER RINGE. II.

Von

L. RÉDEI und T. SZELE

in SZEGED (UNGARN).[1]

§ 1. Einleitung.

Bezeichne R einen kommutativen Ring.[2] Ein Polynom $f(x)$ in R nennen wir kurz ein R-Polynom, ähnlich nennen wir eine in R definierte Funktion $f(x)$ d. h. eine eindeutige Abbildung von R in sich eine R-Funktion. Jedes R-Polynom erzeugt zugleich eine R-Funktion so, dass man in ihm die Unbestimmte als eine Variable auffasst, diese sind die »durch R-Polynome darstellbaren R-Funktionen«. Die R-Polynome, die R-Funktionen, die durch ein R-Polynom darstellbaren R-Funktionen bilden je einen Ring, den wir bzw. mit $R[x]$, $R(x)$, $R([x])$ bezeichnen. Offenbar gilt

$$R[x] \sim R([x]) \subseteq R(x)\,; \tag{1}$$

die hier bezeichnete Homomorphie kommt so zustande, dass man jedem R-Polynom die durch es dargestellte R-Funktion zuordnet.

Bezeichne p eine Primzahl, $e(\geqq 1)$, $m(\geqq 2)$ natürliche Zahlen, $\mathfrak{R}(p^e)$ den endlichen Körper mit p^e Elementen, G den Ring der ganzen Zahlen, K den Körper der

---

[1] Die erste Mitteilung ist ebenfalls in diesen Acta (Bd. 79, 291—320) erschienen und wird mit I zitiert. Die vorliegende Arbeit steht mit I in engem Zusammenhang, ist trotzdem auch selbständig zu lesen. Hier arbeiten wir mit anderen Mitteln als in I, beide Methoden scheinen einander glücklich zu ergänzen, denn keine scheint allein fähig zu sein zu allen unseren Resultaten (in I—II) zu verhelfen, auch lassen sich beide gewiss noch weiter ausbeuten. Mehrere Resultate von I gewinnen wir hier einfacher wieder, teils verallgemeinert oder verschärft; auch die in I offen gebliebene Fragen werden wir hier grösstenteils beantworten.

Die letzte Formel in I, S. 320 enthält einen Druckfehler, die Berichtigung s. hier im Satz 9.

In I haben wir das Zeitwort »darstellen« falsch konjugiert (man lese »stellt dar« statt »darstellt« usw.).

Es entglitt unserer Aufmerksamkeit, dass den in I, S. 294 zitierten Satz ausser Nagell auch schon Pólya hatte: G. PÓLYA, Rend. Circ. Mat. Palermo 40 (1915), 1—16.

[2] Ein Ring soll stets mindestens zwei Elemente enthalten, nur wenn nötig wird stillschweigend auch der Ring mit dem einzigen Element 0 zugelassen.

14. *Acta mathematica*, 82. Imprimé le 8 mars 1950.

rationalen Zahlen, $\mathfrak{R}(m)$ den Restklassenring mod m (gebildet in G) d. h. G/mG, wobei (allgemein) ein Produkt αR die Menge aller αx ($x \in R$) bedeutet. Später werden wir mit R^+ die additive Gruppe (der Elemente) von R und mit »$\approx$« die Isomorphie bezeichnen.

In I haben wir uns das Problem gestellt, die R-Funktionen auf eine einfache Art durch Polynome »darzustellen«, die keine R-Polynome zu sein brauchen. Nach I (S. 294, Satz 1) lassen sich sämtliche R-Funktionen nur im Fall $R = \mathfrak{R}(p^e)$ durch R-Polynome darstellen, wodurch diese Problemstellung reichlich begründet ist. Durch das wichtige Beispiel $R = \mathfrak{R}(m)$ geleitet haben wir in I (S. 298, Grundsatz und Zusatz) ein »Prinzip« aufgestellt, das uns einen Weg eröffnet hat, auf dem man die Lösung suchen kann. Dies gelang uns im Fall $R = \mathfrak{R}(p^e)$ vollkommen (I S. 299, Satz 3). Dieser Erfolg hat uns aufrichtig eingestanden zu übereilten Hoffnungen ermuntert, dass nämlich viele andere Fälle sich mit der Zeit ähnlich erledigen lassen werden. Inzwischen zeigte sich uns aber, dass das gar nicht so ist, sondern nur verhältnismässig wenige Ringe auf diese Art eine Lösung des Problems zulassen können.

Man könnte auch hoffen, dass man unser altes Verfahren passend verändern kann, so dass weitere lösbare Fälle hinzutreten, eine nachträgliche Kritik hat uns aber gezeigt, dass ein solches Bestreben scheitern muss, und so hat man als eine Tatsache hinzunehmen, dass nicht alle Ringe fähig sind, um alle R-Funktionen durch (R-Polynome oder sonstige) Polynome beherrschen zu können.

Genauer gesprochen, im § 2 werden wir auseinandersetzen, was wir für Eigenschaften von einer sinnvollen und begrifflich einfachen »Polynomdarstellung von R-Funktionen« zu verlangen haben. Einen Teil dieser Eigenschaften sprechen wir dann in »Postulaten« aus (von denen aber auch die übrigen Eigenschaften eine Folgerung sind), die wir als Definition betrachten werden. Diese stimmt mit der früheren (in I) zusammen, und so bekräftigt sich die Einzigkeit unseres (in I mehr intuitiv ausgearbeiteten) Verfahrens.[3]

§ 2. Axiomatische Definition der Polynomdarstellung von R-Funktionen.

Wir wollen uns vereinbaren, was wir darunter verstehen, dass gewisse Polynome $f(x)$ (die nicht notwendig R-Polynome zu sein brauchen) R-Funktionen »darstellen«. Das soll vor allem so verstanden werden, dass jedem solchen $f(x)$ eine R-Funktion $\tilde{f}$

[3] Obige Einleitung setzen wir im § 3 fort.

eindeutig zugeordnet wird. Bezeichne $g(x)$ ein weiteres der vorgelegten Polynome, dem dann die R-Funktion $\tilde{g}$ zugeordnet wird. Damit unsere Polynomdarstellung gut brauchbar ist, verlangen wir, dass mit $\tilde{f}$, $\tilde{g}$ zusammen auch $\tilde{f}\pm\tilde{g}$, $\tilde{f}\tilde{g}$ unter den dargestellten R-Funktionen vorkommen und diese eben bzw. durch die Polynome $f(x)\pm g(x), f(x)g(x)$ dargestellt werden, d. h. die Zuordnung von $\tilde{f}$ zu $f(x)$ ein Homomorphismus ist. Eine Vorbedingung hierzu ist, dass die Koeffizienten der betrachteten Polynome $f(x)$ sämtlich in einem und demselben Ring T (der vorläufig nicht notwendig kommutativ zu sein braucht) liegen, und sowohl die $f(x)$ als auch die $\tilde{f}$ einen Unterring vom Polynomring $T[x]$ bzw. vom Funktionenring $R(x)$ ausmachen. Wegen der Kommutativität von R gilt aber unbeschränkt $\tilde{f}\tilde{g}=\tilde{g}\tilde{f}$; dies bedeutet nach obigem, dass die Polynome $f(x)g(x)$, $g(x)f(x)$ dieselbe R-Funktionen darstellen müssen, welcher Forderung man nur so auf eine einfache Weise nachkommen kann, dass man (den Polynomring $T[x]$ d. h.) selbst T kommutativ annimmt. Wir machen diese Annahme und sprechen deshalb in dieser Arbeit weiter nur noch über kommutative Ringe.

Andererseits soll die Zuordnung von $\tilde{f}$ zu $f(x)$ nicht etwa darin bestehen, dass sich $\tilde{f}$ unmittelbar aus den Koeffizienten von $f(x)$ bestimmen lässt, denn dann hätte man es eigentlich nicht mit diesen Polynomen selbst, bloss mit ihren Koeffizienten zu tun, und so würde man nicht mit Recht über eine Polynomdarstellung von $\tilde{f}$ sprechen können. Vielmehr sollen auch diejenigen Funktionen mit in Betracht gezogen werden, die so entstehen, dass man in den $f(x)$ (ihre Polynomeigenschaft ausnutzend) Werte für x (aus dem Ring T) einsetzt.

Wohl haben die $f(x)$ für jedes $x\in T$ einen Sinn, wir wollen aber — das ist das wichtigste Moment in unserer Begriffsbildung — eine grössere Freiheit bewahren dadurch, dass wir x im allgemeinen nur in einer Untermenge S von T variieren lassen. Die Notwendigkeit dieser »Verengung des Definitionsbereiches« erklärt sich nämlich dadurch, dass — wie wir bald sehen werden — sich die Menge der durch T-Polynome darstellbaren R-Funktionen über $R([x])$ hinaus nur dann erweitern lassen kann, wenn S eine echte Untermenge von T ist (Vgl.[5]). Das gesagte bedeutet, dass man aus jedem unserer T-Polynome $f(x)$ die durch die »Funktionentafel«

$$x\to f(x) \qquad (x\in S)$$

gegebene Funktion konstruiert und sich bestrebt, diese Funktionen zur Darstellung der Funktionen $\tilde{f}$ zu verwenden.

Selbstverständlich verlangt man auch, dass die $f(x)$ sich iterieren lassen, d. h. unter unseren Polynomen mit jedem Paar $f(x), g(x)$ zusammen auch $g(f(x))$ vorkommt. Man möchte dabei auch darauf nicht verzichten, dass die entsprechende Funktionentafel

$$x \to g(f(x)) \qquad (x \in S)$$

sich unmittelbar aus den beiden Funktionentafeln

$$x \to f(x)\,, \quad x \to g(x) \qquad (x \in S)$$

berechnen lässt, und das kommt auf die Forderung

$$f(x) \in S \qquad (x \in S) \tag{2}$$

hinaus.[4] Mit dem üblichen Ausdruck bedeutet (2), dass dann $f(x)$ (nicht nur in T sondern auch) in S eine Funktion definiert, die wir deshalb die durch $f(x)$ erzeugte S-Funktion nennen dürfen.

Selbst die Konstruktion der $f(x)$ zugeordneten Funktion $\tilde{f}$ mit Zuhilfenahme dieser S-Funktion kann man sich auf eine einfache Art nur so vorstellen, dass man den gemeinsamen Erklärungsbereich S von diesen Funktionen (der nach (2) auch den Wertevorrat dieser Funktionen umfasst) einer eindeutigen Abbildung $x \to \bar{x}$ $(x \in S, \bar{x} \in R)$ von S auf R unterwirft, diese auf beide Variabeln $x, f(x)$ ausübt und die R-Funktion $\tilde{f}$ als die Gesamtheit der so entstandenen Zuordnungen $\bar{x} \to \overline{f(x)}$ definiert. Damit aber diese Funktion auch eindeutig ist, muss offenbar

$$\overline{f(x)} = \overline{f(y)} \qquad (\bar{x} = \bar{y};\ x, y \in S) \tag{3}$$

gelten.

Nunmehr gilt auch umgekehrt: Ist eine eindeutige Abbildung $x \to \bar{x}$ von S auf R gegeben, so stellt jedes R-Polynom $f(x)$ mit den Eigenschaften (2), (3) eine eindeutige R-Funktion $\tilde{f}$ dar (als Inbegriff der eben genannten Zuordnungen), und so dürfen und wollen wir alle diese Polynome zu unseren Zwecken auch schon behalten.

Insbesondere gelten (2), (3) für die konstanten Polynome $f(x) = c (\in S)$, die offenbar die ebenfalls konstanten R-Funktionen $\tilde{f} = \bar{c}$ darstellen, und so folgt aus der oben geforderten Homomorphie der Zuordnung von $\tilde{f}$ zu $f(x)$, dass selbst die Abbildung $x \to \bar{x}$ von S auf R homomorph sein muss. Eine Vorbedingung hierzu ist, dass S (einen Ring also) einen Unterring von T bildet.

Als Resultat dieser Überlegungen definieren wir in den folgenden Postulaten I,

[4] Trivial kann man (2) so befriedigen, dass man für S einen Unterring von T nimmt, der alle Koeffizienten von den $f(x)$ enthält.

II endgültig, was wir darunter verstehen, dass durch gewisse Polynome $f(x)$ R-Funktionen *dargestellt* werden:

Postulat I. *Die $f(x)$ bilden einen Unterring von einem Polynomring $T[x]$, wobei T ein (kommutativer) Ring ist.*

Postulat II. *Nach Angabe eines Unterringes S von T und einer homomorphen Abbildung $x \to \bar{x}$ von S auf R besteht die durch das Polynom $f(x)$ dargestellte (eindeutige) R-Funktion $\tilde{f}$ aus allen Zuordnungen*

$$\bar{x} \to \overline{f(x)} \qquad (x \in S). \tag{4}$$

Nach Postulat II ist R ein zum Unterring S von T homomorpher Ring:

$$T \supseteq S \sim R\,. \tag{5}$$

In diesem Fall nennen wir T einen *primitiven Ring* von R und umgekehrt R einen *abgeleiteten Ring* von T, ferner nennen wir S einen *Vermittlerring* (dieser hängt von R und T ab ohne im allgemeinen eindeutig bestimmt zu sein). Die Fälle $T \supseteq R$ (mit $S = R$) und $T \sim R$ (mit $S = T$), insbesondere auch $T = S = R$ sind mit einbegriffen.

Damit (4) überhaupt einen Sinn hat, muss vor allem (2) gelten. Ein Polynom von dieser Eigenschaft nennen wir *S-haltend*.

Damit dann durch (4) eine eindeutige Funktion definiert wird, muss ausserdem (3) gelten. Ein Polynom mit beiden Eigenschaften (2), (3) nennen wir (für die gegebene Homomorphie) *zulässig*. Man darf R dem Restklassenring S/I gleichsetzen, wobei I das Ideal derjenigen Elemente von S bezeichnet, die bei der Homomorphie $S \sim R$ auf 0 abgebildet werden. Dann bedeutet $\bar{x}$ einfach die durch x representierte Restklasse mod I, und (3) nimmt die äquivalente Form

$$f(x) \equiv f(y) \pmod{I} \qquad (x \equiv y \pmod{I};\ x, y \in S) \tag{6}$$

an, entsprechend darf $f(x)$ auch *mod I zulässig* genannt werden.

Die zulässigen T-Polynome $f(x)$ bilden offenbar einen Ring. Aus der Homomorphieeigenschaft der Abbildung $x \to \bar{x}$ von S auf R folgt für die Polynome $f(x)$, $g(x)$ dieses Ringes:

$$\overline{f(x) \pm g(x)} = \overline{f(x)} \pm \overline{g(x)},\ \overline{f(x)g(x)} = \overline{f(x)}\ \overline{g(x)}\,.$$

Dies bedeutet nach (4), dass die Zuordnung von $\tilde{f}$ zu $f(x)$ wirklich homomorph ist und der Ring der zulässigen T-Polynome durch diese Homomorphie auf einen

Unterring von $R(x)$, nämlich auf den Ring der durch T-Polynome darstellbaren R-Funktionen abgebildet wird.

Wir bemerken, dass dieser Ring stets $R([x])$ umfasst, d. h. die Darstellung der R-Funktionen durch T-Polynome mindestens so viel leistet wie die durch R-Polynome. Das folgt nämlich daraus, dass insbesondere die S-Polynome sämtlich zulässig sind und die durch sie dargestellten R-Funktionen eben den Ring $R([x])$ ausmachen. [5]

Das Resultat fassen wir kurz zusammen im folgenden:

Grundsatz. *Ist ein primitiver Ring T von R mit dem Vermittlerring S nebst einer homomorphen Abbildung von S auf R gegeben, so stellt jedes zulässige T-Polynom $f(x)$ vermöge dieser Homomorphie eine R-Funktion $\tilde{f}$ dar; dabei bilden die $f(x)$ und die $\tilde{f}$ je einen Ring, die bei Zuordnung von $\tilde{f}$ zu $f(x)$ ebenfalls homomorph aufeinander bezogen sind. Werden alle R-Funktionen auf diese Weise durch T-Polynome dargestellt, so nennen wir T kurz einen Darstellungsring für R (mit dem Vermittlerring S).*

Ein Vergleich mit I (S. 298, Grundsatz und Zusatz) zeigt, dass unser jetziges axiomatisches Verfahren (gemeint sind die Postulate I, II nebst den vorangeschickten Überlegungen) in der Tat zu unserem alten »Darstellungsprinzip« zurückgeführt hat.

Die Angabe eines Darstellungsringes ist als eine vollkommene Lösung unseres Problems anzusehen, dieser günstigste Fall tritt aber, wie schon oben bemerkt, nur für wenige Ringe R ein, worüber wir unten auch näheres erfahren werden. Deswegen wollen wir unsere Untersuchungen in allgemeinen Rahmen halten, indem wir für ein beliebiges Tripel (5) nach den durch die T-Polynome darstellbaren R-Funktionen fragen, in dieser Allgemeinheit haben wir ja auch schon den Grundsatz formuliert. Jeder Wahl von S, T in (5) entspricht dann (mit einem der Analysis entlehnten Ausdruck) eine »Funktionenklasse« in $R(x)$.

Da ein Darstellungsring nur für wenige R vorhanden ist, so fragt man im allgemeinen nach einem *optimalen primitiven Ring* von R; so nennen wir einen primitiven Ring T von R, wenn irgendein primitiver Ring von R eine Polynomdarstellung nur von solchen R-Funktionen ermöglicht, die auch schon durch T-Polynome (bei Annahme eines passenden Vermittlerringes) darstellbar sind. Die Angabe

[5] Nennen wir einen Ring S mit $S \sim R$ einen homomorphinversen Ring von R. Obige Bemerkung lässt sich auch so aussprechen, dass durch die Polynome mit Koeffizienten in einem homomorphinversen Ringe von R nur solche R-Funktionen dargestellt werden, die auch schon durch die R-Polynome geliefert sind. Eben deshalb wird für uns der Fall $T \supset S \sim R$ von Wichtigkeit, dann ist nämlich die Möglichkeit für solche T-Polynome vorhanden, die S-haltend aber keine S-Polynome sind, und somit eventuell R-Funktionen ausserhalb $R([x])$ darstellen.

eines optimalen primitiven Ringes ist jedesmal als eine bestmögliche Lösung unseres Darstellungsproblems anzusehen. Insbesondere ist ein Darstellungsring stets ein optimaler primitiver Ring.

Wir werden sehen, dass es auch solche R gibt, die ihre eigenen optimalen primitiven Ringe sind. Dies bedeutet dann, dass keine R-Funktionen ausserhalb $R([x])$ eine Polynomdarstellung zulassen. Diese Fälle sind für uns im allgemeinen als die »ungünstigsten« anzusehen, eine Ausnahme bilden nur die schon erwähnten $R = \mathfrak{R}(p^e)$, die nämlich auch schon Darstellungsringe für sich selbst sind.

§ 3. Fortsetzung der Einleitung.

Nachdem wir unser altes Darstellungsprinzip (in I) im vorigen § auf mehr feste Grundlagen gestellt haben, wollen wir hier unsere weiteren Resultate zusammenstellen. Vor allem nennen wir den folgenden Satz, den wir leicht aus den Definitionen gewinnen werden:

Satz 1. *Ist T ein Darstellungsring für R mit dem Vermittlerring S und R' ein Unterring von R, so ist T zugleich Darstellungsring für R' mit demjenigen Unterring S' von S als Vermittlerring, der in der Homomorphie $S \sim R\ R'$ entspricht.*

Betrachten wir eine in zwei Richtungen unendliche Folge α_i $(i = \ldots, -1, 0, 1, \ldots)$ mit Elementen α_i aus einem Modul. Dann bilden die Elemente $\alpha_{i+1} - \alpha_i$ die Differenzenfolge (der α_i). Durch n-malige Wiederholung entsteht die n-te Differenzenfolge. Die gegebene Folge α_i nennen wir *arithmetisch*, wenn eine der Differenzenfolgen konstant ist, d. h. aus lauter gleichen Elementen besteht. Gilt das zuerst für die n-te Differenzenfolge, so sagen wir genauer, dass unsere Folge arithmetisch von n-ter Ordnung ist.

Bekanntlich entsteht aus einem Polynom $f(x)$ vom Grade n stets eine arithmetische Folge von höchstens n-ter Ordnung, wenn man für x die Werte $i\alpha (i = \ldots, -1, 0, 1, \ldots)$ einsetzt, wobei α ein Element des Koeffizienten-Ringes ist. Diese Eigenschaft überträgt sich auch auf die R-Funktionen, die irgendeiner Polynomdarstellung fähig sind, wie wir das später unten genauer auseinandersetzen, und so kommen wir zum folgenden:

Satz 2. *Damit eine R-Funktion $\tilde{f}$ einer Polynomdarstellung fähig ist, ist notwendig, dass*

$$f(i\alpha) \qquad (i = \ldots, -1, 0, 1, \ldots) \tag{7}$$

für jedes $x \in R$ eine arithmetische Folge ist, auch müssen die Ordnungszahlen dieser Folgen ein Maximum haben. Der Grad eines darstellenden Polynoms ist mindestens so gross wie dieses Maximum.

Dieser Satz wird in unseren Untersuchungen die Rolle eines wichtigen Hilfssatzes einfüllen, und es wird sich in der Hauptsache darum handeln, wie weit sich die in diesem Satz formulierte notwendige Bedingung umkehren lässt. Dieses »Umkehrproblem« ist im allgemeinen keine leichte Aufgabe, das wir nur in wenigen (allerdings wichtigen) Fällen restlos erledigen konnten. Das gelang in der Hauptsache mit Hilfe gewisser elementar-zahlentheoretischen, auch an sich interessanten Untersuchungen, worüber wir gleich hier berichten.

Eine ganzzahlige Folge $a_i (i = \ldots, -1, 0, 1, \ldots)$ nennen wir *arithmetisch von n-ter Ordnung mod m,* wenn die Elemente der n-ten Differenzenfolge miteinander kongruent mod m sind und dabei n minimal ist. Andererseits betrachten wir eine endliche Folge von m Elementen

$$a_1, \ldots, a_m . \tag{8}$$

Wir nennen $\ldots, a_m, a_1, \ldots, a_m, a_1, \ldots$ die zugeordnete *zyklische Folge* (weil es dabei auf eine zyklische Permutation von (8) nicht ankommt). Ist diese arithmetisch von n-ter Ordnung, so nennen wir selbst (8) eine (m-gliedrige) *zyklisch-arithmetische Folge* n-ter Ordnung. Es erklärt sich dann von selbst, was wir unter einer (ganzzahligen) zyklisch-arithmetischen Folge (n-ter Ordnung) mod m zu verstehen haben. Wir beweisen die folgenden an sich interessanten zwei vorbereitenden Sätze:

Satz 3. *Die p^e-gliedrige Folge* $1, 0, \ldots, 0$ *ist zyklisch-arithmetisch von*

$$rp^e - (r-1)p^{e-1} - 1 \tag{9}$$

-ter Ordnung mod p^r ($r \geqq 1$). Folglich ist jede p^e-gliedrige ganzzahlige Folge zyklisch-arithmetisch mod jeder Potenz von p.

Satz 4. *Ist m keine Primzahlpotenz, so ist eine m-gliedrige ganzzahlige Folge $a_1, \ldots, a_m$ dann und nur dann zyklisch-arithmetisch* mod m, *wenn für jeden maximalen Primzahlpotenzfaktor*[6] *P von m*

$$a_i \equiv a_j \pmod{P} \qquad (i \equiv j \pmod{P};\ 1 \leqq i, j \leqq m) \tag{10}$$

gilt. Insbesondere ist die m-gliedrige Folge $1, 0, \ldots, 0$ *nicht zyklisch-arithmetisch* mod d *($d|m$, $d > 1$).*

---

[6] Wir nennen p^e einen maximalen Primzahlpotenzfaktor von m, wenn $p^e | m$, $p^{e+1} \nmid m$ gilt, wofür wir auch $p^e || m$ schreiben.

Bemerkung. Nach diesen Sätzen verhalten sich die aus einer m-gliedrigen Folge gebildeten zyklischen Folgen sehr verschieden, je nachdem m eine Primzahlpotenz oder keine solche ist. In dieser Arbeit wird uns der Beweis der ersten Behauptung von Satz 3 die grössten Schwierigkeiten machen,[7] dagegen wird sich Satz 4 ziemlich leicht gewinnen lassen.

Unser wichtigstes Resultat wird der folgende Satz, den wir aus den Sätzen 2, 4 gewinnen werden:[8]

Satz 5. *Nur für Ringe von einer Charakteristik p^e kann ein Darstellungsring existieren.*

Für den ersten, oberflächlichen Anblick macht dieser Satz einen niederschlagenden Eindruck. Man bedenke sich aber, wie wichtig insbesondere die endlichen p-Ringe vor allem in der Zahlentheorie sind, unter denen z. B. auch alle Restklassenringe mod einer Primidealpotenz vorkommen, die sich im Ring der ganzen Elemente eines absolut algebraischen Zahlkörpers endlichen Grades bilden lassen, und so bedeutet Satz 5 keineswegs, dass die Idee der Darstellung von R-Funktionen durch Polynome von »weniger« Frucht sei. Den hier genannten Fall hoffen wir in einer anderen Arbeit erledigen zu können, nachdem wir dies für die beiden Spezialfälle $\mathfrak{K}(p^e)$, $\mathfrak{R}(p^e)$, wie erwähnt, schon in I getan haben.

Im folgenden werden wir es wiederholt mit den abgeleiteten Ringen von K zu tun haben. Um diese anzugeben, nehmen wir eine beliebige (leere, endliche oder unendliche) Menge Π von verschiedenen Primzahlen. Mit K_Π bezeichnen wir den Unterring von K bestehend aus denjenigen rationalen Zahlen, deren Nenner ein Potenzprodukt von Primfaktoren aus Π ist. Die sämtlichen abgeleiteten Ringe von K sind, wie wir das später zeigen werden, vor allem die Unterringe von K d. h. die

$$R = rK_\Pi \qquad ((r, \Pi) = 1), \tag{11}$$

ausserdem nur noch die endlichen *zyklischen Ringe*[8], d. h. die

---

[7] Übrigens wird aus dieser ersten Behauptung des Satzes 3 in dieser Arbeit nur beim Beweis vom Satz 9 Gebrauch gemacht. Der Leser also, der sich für den Beweis des Satzes 9 nicht interessiert, mag den schwierigsten § 7 dieser Arbeit (der den Beweis der ersten Behauptung vom Satz 3 enthält) ruhig übergehen und statt dessen nur die Bemerkung [14] (den einfachen Beweis der zweiten Behauptung im Satz 3) lesen.

[8] Sind alle Elemente eines Ringes R von endlicher Ordnung in R^+, und haben diese Ordnungszahlen ein (endliches) Maximum m, so nennen wir m die Charakteristik von R. Gleich hier vereinbaren wir uns, dass wir R einen »p-Ring« nennen, wenn R^+ eine p-Gruppe ist, d. h. wenn jedes Element in R^+ eine Potenz einer und derselben Primzahl p zur Ordnung hat. Unter einem »zyklischen Ring« verstehen wir einen R mit zyklischer additiver Gruppe R^+.

(12) $$R = dG/mG \qquad (d^2|m),$$

wobei r, d natürliche Zahlen sind und $(r, \Pi) = 1$ bezeichnet, dass r zu allen Primzahlen aus Π prim ist. Unter allen diesen Ringen (11), (12) gibt es auch keine isomorphen. Man bemerke: Ist Π die Menge aller Primzahlen, so muss $r = 1$ sein, und dann geht (11) in K über, für jedes sonstige Π ist r unendlich vieler Werte fähig. Es ist klar, dass (12) ein Unterring von $G/mG = \mathfrak{R}(m)$ ist, und so handelt sich in (12) um alle nicht-isomorphen Unterringe sämtlicher $\mathfrak{R}(m)$.

Jetzt kommen wir auf den Spezialfall der *zyklischen p-Ringe*[8] von Satz 5 zurück. Für diese werden wir folgende Umkehrung von Satz 5 beweisen:

Satz 6. *K ist ein Darstellungsring für alle zyklischen p-Ringe. Nimmt man diese nach* (12) *in der Form dG/p^eG $(d^2|p^e)$ an, so kann man dG jedesmal für einen Vermittlerring wählen.*

Dieser Satz enthält den Satz 3 von I (I, S. 299) über $\mathfrak{R}(p^e)$ als spezialfall.

In I haben wir auch die Frage untersucht, welche $\mathfrak{R}(m)$-Funktionen sich durch K-Polynome darstellen lassen (s. unten). Wegen Satz 5 können diese im Falle $m \neq p^e$ nicht alle $\mathfrak{R}(m)$-Funktionen sein. Man könnte fragen, ob man mit einem anderen Ring statt K zu besserem Erfolg kommt. Wir werden das interessante Resultat gewinnen, dass das unmöglich ist und sogar folgendes gilt:

Satz 7. *K ist ein optimaler primitiver Ring von allen seinen abgeleiteten Ringen R. Je nachdem es sich um einen Ring* (11) *oder* (12) *handelt, kann man selbst* (11) *bzw. dG für einen Vermittlerring nehmen. In beiden Fällen lassen sich alle R-Funktionen durch K-Polynome darstellen, die der notwendigen Bedingung von Satz 2 genügen.*

Unter allen hier genannten Ringen R bildet $\mathfrak{R}(m)$ den wichtigsten Spezialfall, mit dem wir uns (wie auch schon in I) ausführlicher beschäftigen. Stets bezeichne ε das Einselement von $\mathfrak{R}(m)$, so dass dann die $i\varepsilon$ $(i = 0, \ldots, m-1)$ alle verschiedenen Elemente sind. Eine beliebige $\mathfrak{R}(m)$-Funktion können wir in der Form

(13) $$\tilde{f}(i\varepsilon) = a_i\varepsilon \qquad (i = 0, \ldots, m-1)$$

annehmen, wobei die a_i ganze Zahlen bezeichnen, die nur mod m in Betracht kommen. Für diesen Fall können wir Satz 7 durch folgenden, mehr expliziten Satz ersetzen:[9]

Satz 8. *Die $\mathfrak{R}(m)$-Funktion* (13) *lässt sich dann und nur dann durch ein (G-hal-*

[9] Vgl. Satz 14, § 11.

tendes, mod *m zulässiges) K-Polynom darstellen, wenn* (10) *gilt. Die anzahl dieser Funktionen ist*

$$P_1^{P_1} \dots P_k^{P_k}, \tag{14}$$

wobei die $P_1, \dots, P_k$ *die maximalen Primzahlpotenzfaktoren von m sind.*

In einer anderen Form haben wir Satz 8 auch schon in I (S. 313, Satz 11) gewonnen, hier wird auch der Beweis anders und einfacher.

Wieder kommen wir auf den weit wichtigsten Spezialfall $\mathfrak{R}(p^e)$ zurück. In I (§§ 6, 7) haben wir solche K-Polynome in sehr durchsichtiger Form angegeben, die alle verschiedenen $\mathfrak{R}(p^e)$-Funktionen darstellen, trotzdem konnten wir die im folgenden Satz erledigte interessante Frage nicht beantworten, was uns jetzt mit voller Ausnutzung des Satzes 3 gelang:

Satz 9. *Mit* $g = g(p^e)$, $v = v(p^e)$ *bezeichnen wir die kleinsten Zahlen, so dass sämtliche* $\mathfrak{R}(p^e)$*-Funktionen durch K-Polynome vom Grad g bzw. vom Nenner*[10] p^v *dargestellt werden können. Es gilt:*

$$g = ep^e - (e-1)p^{e-1} - 1\,, \quad p^{v+e-1} \| g! \tag{15}$$

(*Hiernach ist v um* $e-1$ *kleiner als der Exponent von p in g!*).

Neben die vorigen möchten wir noch die folgenden, teils weniger wichtigen Resultate stellen. Wie gesagt, gehört zu einem Tripel (5) je ein Fall unseres Darstellungsproblems. In den obigen war es viel über den Fall $K \supset G \sim \mathfrak{R}(m)$ von (5) die Rede, betrachten wir jetzt die drei Fälle:

$$G = G \sim \mathfrak{R}(m),\ G = G = G,\ K \supset G = G\,.$$

In den ersten zwei Fällen handelt es sich um $\mathfrak{R}(m)([x])$ (vgl.[5]) bzw. $G([x])$. Über diese gelten die folgenden zwei Sätze:[11]

Satz 10. *Die* $\mathfrak{R}(m)$*-Funktion* (13) *gehört in* $\mathfrak{R}(m)[(x])$ *dann und nur dann, wenn*

---

[10] Jedes K-Polynom $f(x)$ lässt sich in der Form $\frac{h(x)}{b}$ schreiben, wobei $h(x)$ ein G-Polynom und b eine ganze Zahl ist, die wir als den »Nenner« von $f(x)$ bezeichnen. (Dieser ist offenbar nicht eindeutig bestimmt). Stellt $f(x)$ eine $\mathfrak{R}(p^e)$-Funktion $\tilde{f}$ dar, dann lässt sich eine ganze Zahl $a \equiv 1 \pmod{p^e}$ so bestimmen, dass das Polynom $af(x)$ (welches offenbar dieselbe $\tilde{f}$ darstellt wie $f(x)$) einen Nenner p^k hat. Daraus folgt, dass der kleinstmögliche Nenner eines $f(x)$, das eine angegebene $\tilde{f}$ darstellt, notwendig eine Potenz von p sein muss.

[11] Eine andere, viel kompliziertere Form von Satz 10 findet sich bei A. J. Kempner, Polynomials and their residue systems, Trans. Amer. Math. Soc., 22 (1921), 240—288 (insbesondere Satz XIII, S. 283, ausserdem Satz V und (5), S. 261).

$$a_i - \binom{i}{1} a_{i-1} + \cdots + (-1)^i a_0 \equiv 0 \pmod{(m, i!)} \quad (i = 0, \ldots, m-1) \tag{16}$$

gilt. Ihre Anzahl ist[12]

$$\frac{m}{(m, 1)} \cdot \frac{m}{(m, 1!)} \cdot \frac{m}{(m, 2!)} \cdots \tag{17}$$

Satz 11. *Die G-Funktion*

$$f(i) = a_i \qquad (a_i \in G;\ i = 0, \pm 1, \ldots) \tag{18}$$

gehört dann und nur dann in $G([x])$, wenn die Folge $\ldots, a_{-1}, a_0, a_1, \ldots$ arithmetisch von einer Ordnung n ist und

$$a_i - \binom{i}{1} a_{i-1} + \cdots + (-1)^i a_0 \equiv 0 \pmod{i!} \qquad (i = 0, \ldots, n) \tag{19}$$

gilt.

Im dritten der obigen Fälle handelt es sich um die durch G-haltende K-Polynome darstellbaren G-Funktionen. Diese sind nach Satz 7 alle G-Funktionen, die der notwendigen Bedingung von Satz 2 genügen. Die G-haltenden K-Polynome sind nach dem Satz von Pólya-Nagell[1]

$$c_0 + c_1 \binom{x}{1} + \cdots + c_n \binom{x}{n} \qquad (c_0, \ldots, c_n \in G)\,. \tag{20}$$

Wie in I, so wird für uns dieser Satz auch hier ein wichtiges Hilfsmittel sein.

Endlich bemerken wir noch folgendes. Da es insgesamt m^m $\mathfrak{R}(m)$-Funktionen gibt, so ergibt sich hieraus und aus den Anzahlformeln (14), (17) (vgl.[12]) unmittelbar der:

Satz 12. *Bezeichne $\mathfrak{R}(m)(x)_K$ den Ring derjenigen $\mathfrak{R}(m)$-Funktionen, die sich durch K-Polynome (d. h. die sich nach Satz 7 durch Polynome überhaupt) darstellen lassen. In den (stets gültigen) Relationen*

$$\mathfrak{R}(m)(x) \supseteq \mathfrak{R}(m)(x)_K \supseteq \mathfrak{R}(m)([x]) \tag{21}$$

gilt das erste bzw. zweite Gleichheitszeichen dann und nur dann, wenn m eine Primzahlpotenz bzw. eine quadratfreie Zahl ist. (Alle vier Fälle, die man aus (21) so gewinnt, dass man die »$\supseteq$« beliebig durch »$\supset$« oder »=« ersetzt, treten also für passende m wirklich auf).

---

[12] Das Produkt (17) lässt sich mit dem Faktor $\frac{m}{(m, (m_0-1)!)}$ abbrechen, wobei m_0 die kleinste natürliche Zahl mit $m \mid m_0!$ bezeichnet. — Bezeichnen wir (17) mit (m). Dies ist offenbar eine »multiplikative« Funktion, d. h. es gilt $(m) = (P_1) \ldots (P_k)$, wobei die P_i dasselbe bedeuten wie in (14). Ferner gilt nach (17) $(m) \mid m^m$; ($(m) = m^m$ gilt dann und nur dann, wenn $m = p$ ist). Folglich ist (17) stets ein Teiler von (14), beide Zahlen sind gleich dann und nur dann, wenn m eine quadratfreie Zahl ist.

§ 4. Beweis der Sätze 1, 2.

Wir beweisen Satz 1. Wegen $T \supseteq S' \sim R'$ ist T ein primitiver Ring von R' mit dem Vermittlerring S'. Betrachten wir eine beliebige R'-Funktion und ergänzen sie zu einer R-Funktion $\tilde{f}$, so dass man ihr an den Stellen ausserhalb R' beliebige Werte erteilt. Bezeichne dann $f(x)$ ein T-Polynom, das diese Funktion $\tilde{f}$ darstellt. Offenbar genügt $f(x)$ den Bedingungen (2), (3) auch für S', R' statt S, R, und so stellt $f(x)$ mit der Funktion $\tilde{f}$ zusammen auch die gegebene R'-Funktion dar, womit Satz 1 bewiesen ist.

Um Satz 2 zu beweisen nehmen wir an, dass eine R-Funktion $\tilde{f}$ durch ein T-Polynom $f(x)$ mit dem Vermittlerring S dargestellt wird. Das Bild eines $\alpha(\in S)$ in der Homomorphie $S \sim R$ bezeichnen wir mit $\bar{\alpha}(\in R)$. Bekanntlich ist

$$f(i\alpha) \qquad (i = \ldots, -1, 0, \ldots)$$

eine arithmetische Folge. Diese Eigenschaft bleibt bei homomorphen Abbildungen erhalten, auch kann dabei die Ordnung der Folge nicht zunehmen. Da nunmehr nach der Annahme $\overline{f(i\alpha)} = \tilde{f}(i\bar{\alpha})$ gilt, so ist Satz 2 richtig.

§ 5. Hilfsmittel aus der Differenzenrechnung.

Zu unseren Untersuchungen werden wir oft die folgenden Definitionen und elementaren Tatsachen der Differenzenrechnung gebrauchen.

Den (Differenz-) Operator Δ_α erklären wir durch

$$\Delta_\alpha f(x) = f(x+\alpha) - f(x) ,$$

wobei α ein Element in einem Ring R und $f(x)$ ein R-Polynom oder eine R-Funktion ist. Für ein $\varrho(\in R)$ soll ebenfalls $\Delta_\alpha f(\varrho) = f(\varrho+\alpha) - f(\varrho)$ gelten, d. h. man hat zuerst $\Delta_\alpha f(x)$ zu bilden und dann $x = \varrho$ einzusetzen. Die i-fache Iteration bezeichnen wir mit Δ^i erklärt durch

$$\Delta_\alpha^0 f(x) = f(x), \; \Delta_\alpha^i f(x) = \Delta_\alpha\left(\Delta_\alpha^{i-1} f(x)\right) \qquad (i = 1, 2, \ldots)$$

und ebenso mit ϱ statt x.

Es ist klar, dass die Anwendung von Δ_α den Grad eines nichtkonstanten Polynoms $f(x)$ mindestens um 1 herabdrückt.

Im Fall $R = K$, $\alpha = 1$ schreiben wir wie üblich Δ statt Δ_1. Offenbar gilt dann

$$\Delta^i f(x) = f(x+i) - \binom{i}{1} f(x+i-1) + \cdots + (-1)^i f(x) \qquad (i = 0, 1, \ldots). \tag{22}$$

Wir setzen

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

Hierfür gilt

$$\Delta\binom{x}{k} = \binom{x}{k-1}, \quad \Delta(x)_k = k(x)_{k-1} \qquad (k = 1, 2, \ldots).$$

Jedes K-Polynom lässt sich offenbar eindeutig in der Form

$$f(x) = b_0 + b_1(x)_1 + \cdots + b_n(x)_n \tag{23}$$

schreiben mit Koeffizienten in K. Ist $f(x)$ insbesondere ein G-Polynom, so liegen auch die b_k in G und umgekehrt. Für die Entwicklung (23) gilt

$$\Delta f(x) = b_1 + 2b_2(x)_1 + \cdots + nb_n(x)_{n-1}. \tag{24}$$

Für die *Newtonsche Entwicklung*

$$f(x) = c_0 + c_1\binom{x}{1} + \cdots + c_n\binom{x}{n} \tag{25}$$

gilt einfach

$$\Delta^i f(x) = c_i + \cdots + c_n\binom{x}{n-i},$$

woraus für die Entwicklungskoeffizienten

$$c_i = \Delta^i f(0)$$

folgt. Nach Einsetzung in (25) hat man allgemein

$$f(x) = f(0) + \binom{x}{1}\Delta f(0) + \binom{x}{2}\Delta^2 f(0) + \cdots, \tag{26}$$

wobei die rechte Seite mit einem Glied von selbst abbricht.

Sind die Werte $f(i) = a_i$ $(i = 0, \ldots, n)$ für ein K-Polynom $f(x)$ vom n-ten Grade vorgeschrieben, so gilt nach (22), (26) die sogenannte *Interpolationsformel von Newton*:

$$f(x) = a_0 + (a_1 - a_0)\binom{x}{1} + \cdots + (a_n - \binom{n}{1}a_{n-1} + \cdots + (-1)^n a_0)\binom{x}{n}. \tag{27}$$

Wir wenden den Operator Δ auch auf eine Folge $\alpha_k (k = \cdots, -1, 0, 1, \ldots)$ von Elementen eines beliebigen Moduls an, wobei dann k die Rolle von x zu übernehmen hat, d. h. es soll $\Delta\alpha_k = \alpha_{k+1} - \alpha_k$ und allgemein

$$\Delta^i\alpha_k = \alpha_{i+k} - \binom{i}{1}\alpha_{i-1+k} + \cdots + (-1)^i\alpha_k \tag{28}$$

gelten. Die Aussage »die Folge α_k ist arithmetisch von der Ordnung n« ist äquivalent damit, dass n die kleinste nichtnegative ganze Zahl ist, wofür $\Delta^n\alpha_k\,(k = \cdots, -1, 0, 1, \ldots)$ eine konstante Folge ist. Dies ist gleichbedeutend damit, dass die $n+1$-ten Differenzen $\Delta^{n+1}\alpha_k$ eine Nullfolge bilden, ausgenommen den Fall, in dem selbst α_k eine Nullfolge ist.

§ 6. Zyklische Differenzen.

Wir betrachten eine m-gliedrige Folge in einem beliebig vorgelegten Modul und verwenden für sie die vektorielle Schreibweise:

$$\mathfrak{a} = (\alpha_0, \ldots, \alpha_{m-1})\,. \tag{29}$$

Mit (29) zusammen sollen stets auch alle $\alpha_k (k = 0, \pm 1, \ldots)$ erklärt werden, wie folgt:

$$\alpha_k = \alpha_l \qquad (k \equiv l \pmod m;\ k, l = 0, \pm 1, \ldots)\,.$$

Dann ist $\ldots, \alpha_{-1}, \alpha_0, \alpha_1, \ldots$ eben die oben erklärte, (29) zugeordnete zyklische Folge.

Den Operator Δ wenden wir auch auf $\mathfrak{a}$ an mit folgender Definition:

$$\Delta\mathfrak{a} = (\Delta\alpha_0, \ldots, \Delta\alpha_{m-1})\,.$$

Explizit lautet dies als

$$\Delta\mathfrak{a} = (\alpha_1 - \alpha_0, \ldots, \alpha_{m-1} - \alpha_{m-2}, \alpha_0 - \alpha_{m-1})\,,$$

weswegen wir $\Delta\mathfrak{a}$ die *zyklische Differenz von* $\mathfrak{a}$ nennen. Selbstverständlich erklären wir die höheren zyklischen Differenzen wieder durch $\Delta^i\mathfrak{a} = \Delta(\Delta^{i-1}\mathfrak{a})$, und dann gilt allgemein

$$\Delta^i\mathfrak{a} = (\Delta^i\alpha_0, \ldots, \Delta^i\alpha_{m-1})\,. \tag{30}$$

Es ist klar, dass die Folge (29) dann und nur dann zyklisch-arithmetisch von der n-ten Ordnung ist, wenn die n-te zyklische Differenzenfolge $\Delta^n\mathfrak{a}$ konstant ist, d. h. aus gleichen Gliedern besteht.

Wir bemerken hier einige Eigenschaften der zyklischen Differenzen, die später zur Anwendung kommen.

In $\Delta\mathfrak{a}$ also auch in $\Delta^i\mathfrak{a} (i > 0)$ ist die Summe der Glieder gleich 0.

Dann und nur dann ist $\Delta^{i+1}\mathfrak{a} = 0$, wenn $\Delta^i\mathfrak{a}$ konstant ist.

Bezeichnet C eine zyklische Permutation der Glieder von $\mathfrak{a}$, so gilt offenbar

$$\Delta^i(C\mathfrak{a}) = C\Delta^i\mathfrak{a}\,. \tag{31}$$

(Auch diese Eigenschaft rechtfertigt die Benennung »zyklische Differenz«).

Man erkläre für die m-gliedrigen Folgen Summe und Produkt mit einem Skalar ähnlich wie für Vektoren. Dann gelten die Regeln:

$$\Delta^i(\mathfrak{a}+\mathfrak{b}) = \Delta^i\mathfrak{a}+\Delta^i\mathfrak{b}\,, \tag{32}$$

$$\Delta^i(\alpha\mathfrak{a}) = \alpha\Delta^i\mathfrak{a}\,. \tag{33}$$

Zerlege man m in ein Produkt von zwei positiven ganzen Zahlen p, q (> 1), wobei jetzt p keine Primzahl zu sein braucht, und bilde aus (29) die q-gliedrige Folge

$$\bar{\mathfrak{a}} = (\alpha_0+\alpha_q+\ldots+\alpha_{(p-1)q}, \ldots, \alpha_{q-1}+\alpha_{2q-1}+\ldots+\alpha_{pq-1}) \qquad (m = pq)\,,$$

die wir (in Erinnerung an die Kreisteilungsperioden von Gauss) die q-gliedrige Periodenfolge von $\mathfrak{a}$ nennen. Offenbar sind die beiden Operationen $\Delta\mathfrak{a}$, $\bar{\mathfrak{a}}$ vertauschbar, und so gilt allgemein

$$\overline{\Delta^i\mathfrak{a}} = \Delta^i\bar{\mathfrak{a}}\,. \tag{34}$$

Insbesondere werden für uns die ganzzahligen Folgen

$$\mathfrak{a} = (a_0, \ldots, a_{m-1}) \qquad (a_0, \ldots, a_{m-1} \in G) \tag{35}$$

von grosser Wichtigkeit (um diese handelt es sich ja auch in den Sätzen 3, 4). Für zwei solche Folgen $\mathfrak{a}$, $\mathfrak{b}$ schreiben wir

$$\mathfrak{a} \equiv \mathfrak{b} \pmod{d}\,,$$

wenn die Glieder von $\mathfrak{a}$ und $\mathfrak{b}$ mit gleichen Indizes paarweise kongruent mod d sind. Sind die Glieder von $\mathfrak{a}$ sämtlich $\equiv c \pmod{d}$, dann schreiben wir: $\mathfrak{a} \equiv c \pmod{d}$. Insbesondere nennen wir d einen Teiler von $\mathfrak{a}$ und schreiben hierfür auch $d|\mathfrak{a}$, wenn $\mathfrak{a} \equiv 0 \pmod{d}$ gilt. Hat dagegen $\mathfrak{a}$ keinen Teiler (> 1) mit d gemeinsam, so nennen wir $\mathfrak{a}$ prim zu d. Nach (30) ist klar, dass aus $\mathfrak{a} \equiv 0 \pmod{d}$ auch $\Delta^i\mathfrak{a} \equiv 0 \pmod{d}$ folgt. Daraus machen wir im folgenden öfters Gebrauch.

Bei stets festgehaltenem m führen wir für die folgenden m-gliedrigen Folgen die Bezeichnungen ein:

$$\mathfrak{e}_1 = (1, 0, \ldots, 0),\ \mathfrak{e}_2 = (0, 1, 0, \ldots, 0), \ldots,\ \mathfrak{e}_m = \mathfrak{e} = (0, \ldots, 0, 1)\,. \tag{36}$$

Dann lässt sich (35) in der Form schreiben:

$$\mathfrak{a} = a_0\mathfrak{e}_1+\cdots+a_{m-1}\mathfrak{e}_m\,, \tag{37}$$

und so gilt nach (32), (33)

$$\Delta^i\mathfrak{a} = a_0\Delta^i\mathfrak{e}_1+\cdots+a_{m-1}\Delta^i\mathfrak{e}_m\,. \tag{38}$$

Da die $\mathfrak{e}_k$ durch zyklische Permutationen der Glieder auseinander hervorgehen, so genügt es die höheren zyklischen Differenzen von einem $\mathfrak{e}_k$ zu bestimmen, um hieraus nach (31), (38) auch alle $\Delta^i\mathfrak{a}$ leicht herzustellen.

Die Berechnung der ersten m zyklischen Differenzen von $\mathfrak{e}_m = \mathfrak{e}$ geht besonders einfach:

$$\mathfrak{e} = (0, \ldots, 0, 1),$$
$$\Delta\mathfrak{e} = (0, \ldots, 0, 1, -1),$$
$$\Delta^2\mathfrak{e} = (0, \ldots, 0, 1, -2, 1),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\Delta^{m-1}\mathfrak{e} = \left(1, -\binom{m-1}{1}, \binom{m-1}{2}, \ldots, (-1)^{m-1}\right), \tag{39}$$

$$\Delta^m\mathfrak{e} = \left(-\binom{m}{1}, \binom{m}{2}, \ldots, (-1)^{m-1}\binom{m}{m-1}, 1+(-1)^m\right). \tag{40}$$

Um den späteren Gang des Beweises nicht zu stören, schreiben wir die bekannte »Kürzungsregel«[13]

$$\binom{lp}{kp} \equiv \binom{l}{k} \pmod{p} \qquad (0 \leqq k \leqq l) \tag{41}$$

hin. Ausserdem gilt bekanntlich

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p} \qquad (0 \leqq k \leqq p-1), \tag{42}$$

und so gilt allgemeiner

$$\binom{p^e-p^{e-1}}{kp^{e-1}} \equiv (-1)^k \pmod{p}. \qquad (0 \leqq k \leqq p-1). \tag{43}$$

§ 7. Beweis von Satz 3.

Zum Beweis von Satz 3 setzen wir manchmal zur Abkürzung $m = p^e$. Als Vorbereitung beweisen wir

$$\Delta^{p^e+r(p^e-p^{e-1})}\mathfrak{e} \equiv 0 \pmod{p^{r+1}} \qquad (r \geqq 0). \tag{44}$$

Für $r = 0$ folgt (44) sofort aus (40) und aus $p \mid \binom{p^e}{k}$ $(k = 1, 2, \ldots, p^e-1)$.

Jetzt beweisen wir (44) zunächst für $e = 1$ $(m = p)$ und beliebiges r. Es genügt nur noch den Fall $r \geqq 1$ zu betrachten, und dabei nehmen wir an, dass (44) (bei $e = 1$) für $r-1$ statt r richtig ist. Hiernach können wir

$$\Delta^{p+(r-1)(p-1)}\mathfrak{e} = (a_0, \ldots, a_{p-1}) \equiv 0 \pmod{p^r} \tag{45}$$

setzen, wobei dann nach einer früheren Bemerkung (am Anfang des vorigen §-en) auch

[13] S. z. B. L. Rédei, Über einige merkwürdige Polynome in endlichen Körpern mit zahlentheoretischen Beziehungen, Acta Sci. Math. (Szeged), 11 (1946), 39—54, insb. S. 50, (64).

(46) $$a_0+\cdots+a_{p-1}=0$$

gelten muss. Setzen wir noch:

(47) $$\Delta^{p+r(p-1)}\mathfrak{e}=(b_0,\ldots,b_{p-1})\,.$$

Da die linken Seiten von (45), (47) durch Anwendung von Δ^{p-1} auseinander hervorgehen, so ergibt (28):

$$b_k=a_{p-1+k}-\binom{p-1}{1}a_{p-2+k}+\cdots+(-1)^{p-1}a_k \qquad (k=0,\ldots,p-1)$$

(wobei kraft obiger Vereinbarung die Indizes von a_k nur mod p in Betracht zu nehmen sind). Nach (42), (45) gilt dann

$$b_k\equiv a_{p-1+k}+\cdots+a_k \pmod{p^{r+1}}\,.$$

Die rechte Seite ist gleich $a_0+\cdots+a_{p-1}$, und so folgt aus (46) $b_k\equiv 0 \pmod{p^{r+1}}$. Dies beweist nach (47) eben die Richtigkeit von (44) für $e=1$.

Im übriggebliebenen Fall $e\geqq 2$ nehmen wir (44) für $e-1$ statt e als bewiesen an:

(48) $$\Delta^{p^{e-1}+r(p^{e-1}-p^{e-2})}\mathfrak{e}'\equiv 0 \pmod{p^{r+1}} \qquad (r=0,1,2,\ldots)\,,$$

wobei $\mathfrak{e}'(=\mathfrak{e}'_{m'})$ die $p^{e-1}=m'$-gliedrige Folge $(0,\ldots,0,1)$ bezeichnet (Vgl. (36)). Wegen $m=pm'$ lässt sich aus $\mathfrak{e}$ die m'-gliedrige Periodenfolge $\bar{\mathfrak{e}}$ bilden, die aber offenbar gleich $\mathfrak{e}'$ ist, und so gilt nach (34) allgemein

(49) $$\overline{\Delta^i\mathfrak{e}}=\Delta^i\mathfrak{e}'\,.$$

Wendet man dies mit

$$i=p^e+(r-1)(p^e-p^{e-1})>p^{e-1}+r(p^{e-1}-p^{e-2})$$

an, so folgt aus (48)

(50) $$\overline{\Delta^{p^e+(r-1)(p^e-p^{e-1})}\mathfrak{e}}\equiv 0 \pmod{p^{r+1}}\,.$$

Hierauf stützend beweisen wir nunmehr (44) für das vorliegende e mit einem zweiten Induktionsschluss nach r, so dass wir (44) für $r-1$ statt r als richtig annehmen und es dann für r beweisen. (Dies genügt auch zum vollen Beweis von (44), denn der Fall $r=0$ ist oben schon erledigt worden). Nach der Annahme können wir setzen:

(51) $$\Delta^{p^e+(r-1)(p^e-p^{e-1})}\mathfrak{e}=(c_0,\ldots,c_{m-1})\equiv 0 \pmod{p^r}\,.$$

Setzen wir noch

(52) $$\Delta^{p^e+r(p^e-p^{e-1})}\mathfrak{e}=(d_0,\ldots,d_{m-1})\,.$$

Die beiden linken Seiten entstehen auseinander durch Ausübung von $\Delta^{p^e-p^{e-1}}$, und so folgt aus (28):

$$d_k = c_{p^e-p^{e-1}+k} - \binom{p^e-p^{e-1}}{1} c_{p^e-p^{e-1}+k-1} + \cdots + c_k \quad (k = 0, \ldots, m-1)\,, \tag{53}$$

(bei der Bestimmung des Vorzeichens des letzten Gliedes wurde $2|(p^e-p^{e-1})$ berücksichtigt ($e \geqq 2$), die Indizes der c_k kommen nur mod m in Betracht). Wir wollen von (53) auf eine Kongruenz mod p^{r+1} übergehen. Nach (51) gilt allgemein $p^r|c_k$, und so folgt aus (53), (43)

$$d_k \equiv c_k + c_{k+p^{e-1}} + \cdots + c_{k+p^e-p^{e-1}} \pmod{p^{r+1}}\,.$$

Die d_k sind die Glieder der m'-gliedrigen Periodenfolge der linken Seite von (51), und so gilt nach (50) $d_k \equiv 0 \pmod{p^{r+1}}$. Dies bedeutet nach (52), dass (44) für r (statt $r-1$) richtig ist, womit wir (44) allgemein bewiesen haben.

Nunmehr wollen wir Satz 3 beweisen. Bei Beibehaltung obiger Bezeichnung $m = p^e$ lässt sich nach (36) die erste Behauptung des Satzes so aussprechen: Die $[p^e+(r-1)(p^e-p^{e-1})-1]$-te zyklische Differenz von $\mathfrak{e}$ ist die erste solche, die aus lauter mod p^r kongruenten Gliedern besteht ($r \geqq 1$). (Die Folge $\mathfrak{e}_1$ im Satz 3 entsteht nämlich aus $\mathfrak{e} = \mathfrak{e}_m$ bloss durch eine zyklische Permutation). Der Beweis wird uns so gelingen, dass wir die Behauptung schärfer fassen, wie folgt: Es gilt

$$\Delta^{p^e+(r-1)(p^e-p^{e-1})-1}\mathfrak{e} \equiv (-p)^{r-1} \pmod{p^r} \qquad (r \geqq 1)\,. \tag{54}$$

Für $r = 1$ folgt die Richtigkeit von (54) so. Nach (44) ($r = 0$) gilt $\Delta^{p^e}\mathfrak{e} \equiv 0 \pmod{p}$, und so gilt $\Delta^{p^{e-1}}\mathfrak{e} \equiv c \pmod{p}$ mit einem ganzen c. Die linke Seite hat nach (39) das erste Glied 1, und so muss $c \equiv 1 \pmod{p}$ sein, weswegen man $c = 1$ setzen darf. Das bedeutet die Richtigkeit von (54) für $r = 1$.

Wir setzen (54) für ein $r(\geqq 1)$ voraus, um hieraus auf die Richtigkeit für $r+1$ zu schliessen. Nach dieser Voraussetzung können wir

$$\Delta^{p^e+(r-1)(p^e-p^{e-1})-1}\mathfrak{e} = (u_0, \ldots, u_{m-1}) \equiv (-p)^{r-1} \pmod{p^r} \tag{55}$$

setzen. Wir setzen noch

$$\Delta^{p^e+r(p^e-p^{e-1})-1}\mathfrak{e} = (v_0, \ldots, v_{m-1})\,, \tag{56}$$

woraus wie oben

$$v_k = u_{p^e-p^{e-1}+k} - \binom{p^e-p^{e-1}}{1} u_{p^e-p^{e-1}+k-1} + \cdots + u_k \qquad (k = 0, \ldots, m-1) \tag{57}$$

folgt (die Indizes der u_k kommen nur mod m in Betracht). Wegen (55) gilt allgemein

$$u_k = p^r x_k + (-p)^{r-1} \qquad (k = 0, \ldots, m-1) \tag{58}$$

mit ganzen x_k. Da die Koeffizientensumme auf der rechten Seite von (57) gleich 0 ist, so folgt nach Einsetzen von (58):

$$v_k = p^r\left(x_{p^e-p^{e-1}+k} - \binom{p^e-p^{e-1}}{1} x_{p^e-p^{e-1}+k-1} + \cdots + x_k\right).$$

Wegen (43) gilt dann

$$v_k \equiv p^r(x_{p^e-p^{e-1}+k} + x_{p^e-2p^{e-1}+k} + \cdots + x_k) \pmod{p^{r+1}}. \tag{59}$$

Wieder greifen wir zu (49). Nach diesem sind die Glieder

$$u_k + u_{k+p^{e-1}} + \cdots + u_{k+p^e-p^{e-1}} \qquad (k = 0, \ldots, m-1) \tag{60}$$

der ($p^{e-1} =$) m'-gliedrigen Periodenfolge der linken Seite von (55) eben die Glieder der Folge

$$\Delta^{p^e+(r-1)(p^e-p^{e-1})-1}\mathfrak{e}'. \tag{61}$$

Wegen

$$p^e + (r-1)(p^e-p^{e-1}) > p^{e-1} + r(p^{e-1}-p^{e-2})$$

folgt aber aus (44) (angewandt für $\mathfrak{e}'$ statt $\mathfrak{e}$, d. h. für p^{e-1} statt p^e), dass (61) durch p^{r+1} teilbar ist. Dasselbe gilt dann über (60), und das ergibt nach (58)

$$p^r(x_k + x_{k+p^{e-1}} + \cdots + x_{k+p^e-p^{e-1}}) + p(-p)^{r-1} \equiv 0 \pmod{p^{r+1}}.$$

Hieraus und aus (59) folgt

$$v_k \equiv -p(-p)^{r-1} \equiv (-p)^r \pmod{p^{r+1}} \qquad (k = 0, \ldots, m-1).$$

Dies bedeutet wegen (56), dass (54) für $r+1$ (statt r) also auch allgemein richtig ist, womit wir die erste Behauptung von Satz 3 bewiesen haben.

Hiernach ist $\Delta^{s+1}\mathfrak{e} \equiv 0 \pmod{p^r}$ ($r \geqq 1$), wenn s die Zahl (9) bezeichnet. Das gilt dann auch für $\mathfrak{e}_1, \ldots, \mathfrak{e}_{m-1}$ statt $\mathfrak{e}_m = \mathfrak{e}$, woraus nach (38) die Richtigkeit der zweiten Behauptung des Satzes 3 folgt.[14]

§ 8. Beweis von Satz 4.

Der Beweis von Satz 4 wird durch Satz 3 ermöglicht. Wir setzen

$$\mathfrak{a} = (a_1, \ldots, a_m). \tag{62}$$

Die erste Hälfte des Satzes lässt sich dann offenbar so aussprechen: Dann und nur dann gibt es ein i mit

---

[14] Die zweite Behauptung des Satzes 3 kann man unmittelbar aus (40) sehr einfach (ohne § 7), wie folgt, gewinnen. Da $p\left|\binom{p^e}{k}\right.$ ($1 \leqq k \leqq p^e-1$) ist, gilt im Fall $m = p^e$ nach (40) $p|\Delta^{p^e}\mathfrak{e}$ d. h. nach (38) $p|\Delta^{p^e}\mathfrak{a}$, wobei $\mathfrak{a}$ eine beliebige p^e-gliedrige ganzzahlige Folge ist. Dann aber folgen aus $\Delta^{p^e}\mathfrak{a} = p\mathfrak{a}'$ durch Wiederhohlung dieses Schlusses: $\Delta^{2p^e}\mathfrak{a} = p\Delta^{p^e}\mathfrak{a}' = p^2\mathfrak{a}'', \ldots, \Delta^{ep^e}\mathfrak{a} = p^e\mathfrak{a}^{(e)}$ mit ganzzahligen $\mathfrak{a}', \ldots, \mathfrak{a}^{(e)}$. Somit gilt $p^e|\Delta^{ep^e}$, w. z. b. w.

$$\Delta^i \mathfrak{a} \equiv 0 \pmod{m}, \tag{63}$$

wenn (10) gilt.

Nehmen wir zuerst (10) an. Die ersten P Glieder von (62) bilden eine Folge $\mathfrak{b} = (a_1, \ldots, a_P)$. Nach Satz 3 gibt es ein i mit $\Delta^i \mathfrak{b} \equiv 0 \pmod{P}$. Wenn wir $\mathfrak{b}$ $\frac{m}{P}$-mal nebeneinander schreiben, so ensteht eine m-gliedrige Folge

$$\mathfrak{a}' = (a_1, \ldots, a_P, a_1, \ldots, a_P, \ldots), \tag{64}$$

und dann gilt auch hierfür $\Delta^i \mathfrak{a}' \equiv 0 \pmod{P}$ mit demselben i. Andererseits folgt aus (10), (62), (64) $\mathfrak{a} \equiv \mathfrak{a}' \pmod{P}$, und so gilt ebenfalls $\Delta^i \mathfrak{a} \equiv 0 \pmod{P}$. Da dies für jeden maximalen Primzahlpotenzfaktor P von m mit je einem passenden i richtig ist, so gibt es in der Tat ein i mit der Eigenschaft (63).

Dem Beweis der übrigen Teile des Satzes schicken wir folgendes voran. Mit Beibehaltung der Bezeichnungen des Satzes setzen wir $P = p^e$ und geben eine ganzzahlige Folge

$$\mathfrak{z} = (z_0, \ldots, z_{m-1}) \tag{65}$$

an, wofür

$$p | z_0, \ldots, z_{P-1};\ p \nmid \mathfrak{z} \tag{66}$$

gilt. Wir behaupten, dass dann $p \nmid \Delta^i \mathfrak{z}$ $(i = 0, 1, \ldots)$ ist.

Bezeichne nämlich z_{P+k} *das erste Glied* von (65) mit

$$p \nmid z_{P+k} \qquad (0 \leqq k \leqq m-P-1). \tag{67}$$

Ist die Behauptung falsch, so gibt es ein u mit

$$p | \Delta^{p^u} \mathfrak{z} \qquad (u \geqq 0).$$

Nach (28) gilt dann

$$z_{p^u+k} - \binom{p^u}{1} z_{p^u-1+k} + \cdots + (-1)^{p^u} z_k \equiv 0 \pmod{p} \qquad (k = 0, \ldots, m-1)$$

(in den z_k kommen die Indizes nur mod m in Betracht). Hieraus folgt

$$z_{p^u+k} \equiv z_k \pmod{p}. \tag{68}$$

Mit einem u zusammen gilt das für alle grösseren u, und so dürfen wir

$$p^{u-e} \equiv 1 \left(\mathrm{mod}\ \frac{m}{P}\right) \qquad (u \geqq e)$$

annehmen. Dies ergibt $p^u \equiv P \pmod{m}$, $z_{p^u+k} = z_{P+k}$, und so gilt nach (68) $z_{P+k} \equiv z_k \pmod{p}$, ein offenbarer Widerspruch mit der Annahme über (67), womit wir die letzte Behauptung bewiesen haben.

Hiervon ist die Schlussbehauptung von Satz 4 bloss ein Spezialfall.

Um auch die restliche Behauptung des Satzes zu beweisen nehmen wir die Existenz eines i mit (63) an. Wieder nehmen wir $\mathfrak{a}'$ in (64) zu Hilfe, worüber wir schon bemerkt haben, dass es ein j mit $P|\Delta^j\mathfrak{a}'$ gibt. Hieraus und aus (63) folgt die Existenz eines l mit

$$(p^e =)P|\Delta^l(\mathfrak{a}-\mathfrak{a}') . \tag{69}$$

Gilt nun $P|\mathfrak{a}-\mathfrak{a}'$ für alle P, so bedeutet dies wegen (62), (64) das Bestehen von (10), was wir eben zu beweisen haben. Deshalb genügt es die Unmöglichkeit von $P\nmid(\mathfrak{a}-\mathfrak{a}')$ zu zeigen. Bezeichne v die grösste ganze Zahl mit $p^v|(\mathfrak{a}-\mathfrak{a}')$ $(0 \leqq v < e)$. Wird dann $\mathfrak{a}-\mathfrak{a}' = p^v\mathfrak{z}$ gesetzt, so treten (65), (66) wegen (62), (64) in Kraft (es gilt sogar $z_0 = \ldots = z_{P-1} = 0$), woraus $p\nmid\Delta^t\mathfrak{z}$ $(t = 0, 1, \ldots)$ folgt. Andererseits gilt wegen (69) auch $p|\Delta^l\mathfrak{z}$. Dieser Widerspruch beweist Satz 4.

9. Beweis von Satz 5.

Um Satz 5 zu beweisen bezeichnen wir mit R einen Ring, der keine Primzahlpotenz zur Charakteristik hat. Es genügt eine R-Funktion $\tilde{f}$ anzugeben, die sich durch kein Polynom darstellen lässt. Wir wählen diese so, dass $\tilde{f}(0) = \alpha \neq 0$ ist (wobei wir über α später passend verfügen werden), und sonst $\tilde{f}(x)$ überall in R verschwindet.

Zuerst betrachten wir den Fall, in dem R^+ Elemente von unendlicher Ordnung enthält. Wählen wir für α ein beliebiges solches Element. Die Folge (7) hat jetzt die Form $\ldots, 0, \alpha, 0, \ldots$, ist also gewiss nicht arithmetisch, und so folgt aus Satz 2, dass $\tilde{f}$ durch kein Polynom darstellbar ist.

Betrachten wir dann den Fall, in dem es in R^+ ein Element von einer endlichen Ordnung m gibt und dabei m keine Primzahlpotenz ist. Bezeichne α ein solches Element. Wieder zeigen wir, dass (7) keine arithmetische Folge also $\tilde{f}$ durch kein Polynom darstellbar ist. Jetzt ist nämlich (7) die der m-gliedrigen Folge $\alpha, 0, \ldots, 0$ zugeordnete zyklische Folge. Diese ist dann und nur dann arithmetisch, wenn die genannte endliche Folge zyklisch-arithmetisch d. h. die (m-gliedrige) Koeffizientenfolge $1, 0, \ldots, 0$ zyklisch-arithmetisch mod m ist. Dies gilt nach Satz 4 nicht, womit der Beweis auch für diesen Fall beendet ist.

Es ist nur noch der Fall übrig, in dem R^+ eine p-Gruppe ist, die Elemente von beliebig hoher Ordnungen enthält. Wir nehmen an, dass $\tilde{f}$ gegen die Behauptung

durch ein Polynom n-ten Grades dargestellt wird. Wegen der Annahme gibt es in R^+ ein Element α_1 von einer Ordnung $n_1 \geqq n+2$. (n_1 ist eine Potenz von p, worauf es aber nicht ankommen wird). Gewiss ist die n_1-gliedrige Folge $1, 0, \ldots, 0$ nicht zyklisch-arithmetisch von einer Ordnung $\leqq n$ modulo der Ordnung von α in R^+, die nämlich wegen $\alpha \neq 0$ eine ganze Zahl > 1 ist[15]), und so ist die n_1-gliedrige Folge $\alpha, 0, \ldots, 0$ nicht zyklisch-arithmetisch von einer Ordnung $\leqq n$. Dies bedeutet, dass die Folge

$$\tilde{f}(i\alpha_1) \qquad (i = \ldots, -1, 0, 1, \ldots)$$

(die nämlich eben die von $\tilde{f}$ der vorhergenannten Folge $\alpha, 0, \ldots, 0$ zugeordnete zyklische Folge ist) nicht arithmetisch von einer Ordnung $\leqq n$ sein kann. Nach Satz 2 steht dies in einem Widerspruch mit der Annahme, dass $\tilde{f}$ durch ein Polynom n-ten Grades darstellbar ist. Damit ist Satz 5 bewiesen.

§ 10. Die abgeleiteten Ringe von K.

Wir wollen zeigen, dass (11), (12) die sämtlichen abgeleiteten Ringe von K und diese untereinander nicht isomorph sind.

Betrachten wir zunächst nur die Unterringe von K. Vor allem ist klar, dass die K_Π die sämtlichen Ringe zwischen G und K sind. Ist dann R ein beliebiger Unterring von K, so bezeichne r die kleinste natürliche Zahl in R. Offenbar ist dann die Menge $\frac{1}{r}R$ ein Ring zwischen G und K also ein K_Π, woraus $R = rK_\Pi$ folgt. Auch muss $(r, \Pi) = 1$ gelten, denn sonst wäre r nicht die kleinste natürliche Zahl in R. Wir haben gezeigt, dass alle Unterringe von K unter den Ringen (11) vorkommen, und so sind die letzteren offenbar alle verschiedenen Unterringe von K. Wir haben noch zu zeigen, dass aus der Isomorphie $R \approx R'$ zweier Unterringe R, R' ihre Gleichheit folgt. Schon aus der Isomorphie $R^+ \approx R'^+$ folgt nämlich, dass für die entsprechenden Elemente α, α' von R, R' $\alpha = c\alpha'$ gelten muss mit einer Konstanten c. Aus $R \approx R'$ folgt weiter $c^2 = 1$, $c = \pm 1$, $R = R'$ womit die Behauptung bewiesen ist.

Jetzt wollen wir zeigen, dass die (12) die sämtlichen endlichen zyklischen Ringe und auch untereinander nicht isomorph sind. Bezeichne R einen endlichen zyklischen Ring mit n Elementen. Offenbar gibt es in R^+ ein erzeugendes Element α, so dass $\alpha^2 = d\alpha$ $(d|n, d > 0)$ gilt. Neben n ist auch die Ordnung $\frac{n}{d}$ von α^2 eine Invariante von R, und so bestimmen R und n, d einander eindeutig. Wird noch $m = dn$ gesetzt,

[15]) Denn nach (39) kann das Glied 1 zuerst aus der n_1-ten Differenzenfolge fehlen.

wobei dann die Bedingung $d|n$ durch $d^2|m$ zu ersetzen ist, so sieht man, dass R zum Ring (12) isomorph ist, womit wir die letzte Behauptung bewiesen haben.

Endlich haben wir nur noch zu zeigen, dass jeder abgeleitete Ring R von K, der kein Unterring von K ist, notwendig ein Ring (12) sein muss. Bezeichne S einen Vermittlerring, für den dann $K \supseteq S \sim R$ gilt. Wir nehmen S in der Form (11) an. Bezeichne I das Ideal bestehend aus denjenigen Elementen von S, die durch die Homomorphie $S \sim R$ auf 0 abgebildet werden. Es ist $I \neq 0$, denn sonst wäre R isomorph zu $S(\subseteq K)$, was aber ausgeschlossen ist. Da I ein Unterring von K und zugleich ein Ideal von S ist, so gilt nach (11) (mit demselben K_{II}) $I = krK_{II}$, wobei $k(\geqq 2)$ eine ganze Zahl ist. Wir zeigen, dass jede Restklasse von S nach I eine ganze Zahl enthält. Betrachten wir nämlich ein beliebiges Element $\frac{ra}{b}$ von S, wobei a, b ganze Zahlen sind mit $b > 0$, $(ra, b) = 1$. Man bestimme eine ganze Zahl a' mit $ka' \equiv a \pmod{b}$. Dann ist

$$\frac{ra}{b} - \frac{kra'}{b} = r\frac{a-ka'}{b} \quad (\in R)$$

ganz und gehört in dieselbe Restklasse mod I wie $\frac{ra}{b}$, womit wir gezeigt haben, dass alle Restklassen von S nach I auch ganze Zahlen enthalten. Andererseits sind die ganzen Elemente von S die sämtlichen Vielfachen von r und kr ist die kleinste natürliche Zahl in I, woraus folgt, dass $R(\approx S/I)$ zum Restklassenring rG/krG isomorph ist. Hiermit haben wir alle unsere Behauptungen über die abgeleiteten Ringe von K bewiesen.

§ 11. Allgemeines über die Darstellung der $\mathfrak{R}(m)$-Funktionen.

In diesem Paragraphen wollen wir als Vorbereitung die Frage untersuchen, was für $\mathfrak{R}(m)$-Funktionen sich durch ein K-Polynom $f(x)$ darstellen lassen, indem stets G als Vermittlerring angenommen werden soll, und wie man die gewünschten $f(x)$ angeben kann. Nach dem Grundsatz und (6) kommen nur diejenigen $f(x)$ in Frage, die vor allem G-haltend, ausserdem mod m zulässig sind. Wir wiederholen für diesen Fall, dass beide Bedingungen bzw. so lauten:

$$f(x) \in G \qquad (x \in G), \tag{70}$$

$$f(x) \equiv f(y) \pmod{m} \qquad (x \equiv y \pmod{m};\ x, y \in G). \tag{71}$$

Umgekehrt, wenn diese erfüllt sind, so stellt $f(x)$ auch schon eine $\mathfrak{R}(m)$-Funktion $\tilde{f}$ dar, die man einfach in der Form

$$\tilde{f}(x\varepsilon) = \varepsilon f(x) \qquad (x \in G) \tag{72}$$

schreiben kann, wobei ε stets das Einselement von $\mathfrak{R}(m)$ bezeichnen soll.

Wie schon erwähnt, die G-haltenden Polynome sind nach dem Satz von Pólya-Nagell einfach die

$$f(x) = c_0 + c_1\binom{x}{1} + \cdots \qquad (c_i \in G)\,, \tag{73}$$

wobei nur endlich viele $c_i \neq 0$ sind. Die weitere Frage, wie dann die c_i zu wählen sind, damit $f(x)$ mod m zulässig ist, d. h. eine $\mathfrak{R}(m)$-Funktion darstellt, ist nicht mehr so leicht zu beantworten. Hierüber beweisen wir vorläufig nur, dass in gewissem Sinne Eindeutigkeit vorliegt, und zwar es gilt der folgende:

Satz 13. *Wird eine gegebene $\mathfrak{R}(m)$-Funktion durch ein K-Polynom $f(x)$ dargestellt, so sind die Newtonschen Entwicklungskoeffizienten $c_0, c_1, \ldots$ von $f(x)$ in* (73) mod m *eindeutig bestimmt.*

Bemerkung. Schon dieser Satz zeigt, dass die Newtonsche Entwicklung für unsere Zwecke gut geeignet ist, denn für die Koeffizienten der Entwicklung nach *Potenzen* $f(x) = a_0 + a_1 x + \cdots$ ist kein ähnlicher Satz gültig.

Der Beweis entsteht ebenfalls aus dem Satz von Pólya-Nagell. Stellen nämlich zwei K-Polynome $f(x)$, $g(x)$ dieselbe $\mathfrak{R}(m)$-Funktion dar, so ist das Polynom $\frac{1}{m}(f(x)-g(x))$ G-haltend, hat also lauter ganze Newtonsche Entwicklungskoeffizienten, und so ist Satz 13 richtig. Nun beweisen wir den folgenden:

Hilfssatz. *Wird die $\mathfrak{R}(m)$-Funktion $\tilde{f}$ durch das K-Polynom $f(x)$ dargestellt, so stellt $\Delta f(x)$ die Funktion $\Delta_\varepsilon \tilde{f}$ (vgl. § 5) dar. Umgekehrt, wenn für eine $\mathfrak{R}(m)$-Funktion $\tilde{f}$ die Funktion $\Delta_\varepsilon \tilde{f}$ durch das K-Polynom*

$$g(x) = c_1 + c_2\binom{x}{1} + \cdots + c_n\binom{x}{n-1} \tag{74}$$

dargestellt wird, so stellt

$$f(x) = c_0 + c_1\binom{x}{1} + c_2\binom{x}{2} + \cdots + c_n\binom{x}{n} \tag{75}$$

die gegebene Funktion $\tilde{f}$ dar, wobei c_0 eine ganze Zahl ist, für die

$$\tilde{f}(0) = c_0\varepsilon \tag{76}$$

gilt.

Die erste Behauptung des Hilfssatzes folgt sofort daraus, dass nach (72)

$$\Delta_\varepsilon \tilde{f}(x\varepsilon) = \tilde{f}(x\varepsilon+\varepsilon)-\tilde{f}(x\varepsilon) = \varepsilon\big(f(x+1)-f(x)\big) = \varepsilon\Delta f(x) \qquad (x \in G)$$

gilt.

Für die zweite Behauptung gilt wegen der Annahme nach (72)

$$\Delta_\varepsilon \tilde{f}(x\varepsilon) = \varepsilon g(x) \qquad (x \in G),$$

ausserdem gilt nach (74), (75) und § 5

$$g(x) = \Delta f(x) = f(x+1)-f(x).$$

Beide ergeben

$$\tilde{f}\big((x+1)\varepsilon\big)-\varepsilon f(x+1) = \tilde{f}(x\varepsilon)-\varepsilon f(x). \tag{77}$$

Die rechte Seite verschwindet nach (75), (76) für $x = 0$, und so folgt aus (77) durch Induktion, dass sie für $x = 1, 2, \ldots$ und ebenfalls für $x = -1, -2, \ldots$ verschwinden muss. Dann gilt (72) allgemein, womit der Hilfssatz bewiesen ist.

Wir beweisen den folgenden:

Satz 14. *Eine beliebige $\mathfrak{R}(m)$-Funktion*

$$\tilde{f}(i\varepsilon) = a_i\varepsilon \qquad (i = 0, \pm 1, \ldots) \tag{78}$$

lässt sich dann und nur dann durch ein K-Polynom $f(x)$ darstellen, wenn die Folge $\mathfrak{a} = (a_0, \ldots, a_{m-1})$ zyklisch-arithmetisch mod m *ist. Ist das der Fall und fällt dabei die Ordnungszahl der Folge gleich n aus, so ist n zugleich der kleinstmögliche Grad für $f(x)$; ein gewünschtes $f(x)$ von diesem Grad wird durch* (75) *geliefert, indem man dort für $c_0, \ldots, c_n$ die Anfangsglieder der $\mathfrak{a}, \ldots, \Delta^n\mathfrak{a}$ einsetzt.*

Man wende nämlich Satz 2 auf unsere Funktion $\tilde{f}$ mit $\alpha = \varepsilon$ an. Nach (78) ist die Folge (7) dann und nur dann arithmetisch von n-ter Ordnung, wenn $\mathfrak{a}$ zyklisch-arithmetisch von n-ter Ordnung mod m ist. Aus Satz 2 folgt also die »nur dann« Behauptung von Satz 14, auch folgt aus ihm, dass ein die Funktion darstellendes Polynom mindestens vom im Satz 14 genannten Grade sein muss.

Den Beweis der übrigen Behauptungen von Satz 14 dürfen wir nunmehr unter der Annahme führen, dass $\mathfrak{a}$ zyklisch-arithmetisch von n-ter Ordnung mod m ist. Da ferner im Fall $n = 0$ die Glieder von $\mathfrak{a}$ miteinander mod m kongruent sind, d. h. es sich um eine konstante Funktion $\tilde{f}$ handelt, so ist der Satz in diesem Falle richtig. Im übrigen Fall $n > 0$ setzen wir die Richtigkeit des Satzes für die »kleineren« n voraus.

Aus (78) folgt sofort, dass der Funktion $\Delta_\varepsilon \tilde{f}$ die Folge $\Delta\mathfrak{a}$ zugehört. Diese ist zyklisch-arithmetisch von der Ordnung $n-1$ mod m, und so folgt aus der Voraussetzung, dass $\Delta_\varepsilon \tilde{f}$ durch ein K-Polynom $g(x)$ vom Grade $n-1$ darstellbar ist, weshalb man $g(x)$ in der Form (74) annehmen kann. Wegen des Hilfssatzes wird dann $\tilde{f}$ durch das K-Polynom $f(x)$ in (75) vom Grade n dargestellt, wofür auch (76) gilt.

Wegen der Voraussetzung und des Satzes 13 darf auch angenommen werden, dass die $c_1, \ldots, c_n$ in (74) eben die Anfangsglieder von $\Delta\mathfrak{a}, \ldots, \Delta^n\mathfrak{a}$ sind. Hierzu kommt noch, dass für c_0 nach (76), (78) das Anfangsglied a_0 von $\mathfrak{a}$ genommen werden kann, womit Satz 14 in allen Teilen bewiesen ist.

§ 12. Beweis von Satz 6.

Um Satz 6 zu beweisen betrachten wir zuerst den Fall $d = 1$. Dann lautet die Behauptung des Satzes so, dass sich alle $\mathfrak{R}(p^e)$-Funktionen durch K-Polynome mit dem Vermittlerring G darstellen lassen. Das ist in der Tat eine Folgerung von der ersten Hälfte des Satzes 14 und von der zweiten Hälfte des Satzes 3, und so ist der Satz für diesen Fall richtig.

Im allgemeinen Fall handelt es sich um einen Unterring des vorherbetrachteten $\mathfrak{R}(p^e)$, dem in der Homomorphie $G \sim \mathfrak{R}(p^e)$ der Unterring dG von G entspricht. Aus dem eben bewiesenen folgt also nach Satz 1 die Richtigkeit von Satz 6 im allgemeinen.

§ 13. Beweis von Satz 7.

Um Satz 7 zu beweisen bezeichne R einen beliebigen abgeleiteten Ring von K und $\tilde{f}$ eine R-Funktion, die der notwendigen Bedingung von Satz 2 genügt. Wir haben zu beweisen, dass dann $\tilde{f}$ durch ein K-Polynom darstellbar ist (stets mit dem im Satz genannten Vermittlerring). Wir behandeln die im Satz unterschiedenen zwei Fälle getrennt.

Erstens sei R ein Unterring (11) von K. Aus der Annahme folgt nach Satz 2, dass die Folge $\tilde{f}(ir)$ $(i = \ldots, -1, 0, 1, \ldots)$ arithmetisch ist. Bekanntlich gibt es dann ein K-Polynom $f(x)$ mit

$$f(ir) = \tilde{f}(ir) \qquad (i = 0, \pm 1, \pm 2, \ldots). \tag{79}$$

Betrachten wir ein beliebiges Element

(80) $$\alpha = \frac{ra}{b} \qquad (a, b \in G)$$

in R. Wegen der Annahme und Satz 2 ist die Folge $\tilde{f}(i\alpha)$ $(i = \ldots, -1, 0, 1, \ldots)$ arithmetisch, und so gibt es ein K-Polynom $g(x)$ mit

(81) $$g(i) = \tilde{f}(i\alpha) \qquad (i = 0, \pm 1, \pm 2, \ldots).$$

Zunächst sei $\alpha \neq 0$. Wir nehmen auch noch das Polynom $h(x) = g\left(\frac{x}{\alpha}\right)$ zu Hilfe und gewinnen so nach (79)—(81):

$$f(ira) = \tilde{f}(ira) = \tilde{f}(ib\alpha) = g(ib) = h(ib\alpha) = h(ira).$$

Hiernach nehmen die beiden Polynome $f(x)$, $h(x)$ an unendlich vielen Stellen gleiche Werte an, folglich sind sie gleich. Insbesondere für $x = \alpha$ ergibt sich also aus (79), (81):

$$f(\alpha) = h(\alpha) = g(1) = \tilde{f}(\alpha).$$

Dasselbe Resultat $f(\alpha) = \tilde{f}(\alpha)$ folgt aus (79) unmittelbar für $\alpha = 0$, und so ist Satz 7 für den jetzt betrachteten Fall richtig.

Zweitens sei R ein Ring (12).

Wir betrachten zunächst den Fall ($d = 1$ d. h.) $R = \mathfrak{R}(m)$. Jetzt haben wir zu zeigen, dass die $\mathfrak{R}(m)$-Funktion $\tilde{f}$ durch ein K-Polynom mit dem Vermittlerring G darstellbar ist. Aus der Annahme folgt nach Satz 2, dass die Folge $\tilde{f}(i\varepsilon)$ $(i = \ldots, -1, 0, 1, \ldots)$ arithmetisch ist. Wie wir oben schon gesehen haben, bedeutet dies mit den Bezeichnungen von Satz 14, dass die Folge $\mathfrak{a}$ zyklisch-arithmetisch mod m ist. Hieraus folgt nach der ersten Hälfte von Satz 14 die Richtigkeit von Satz 7 für diesen Fall.

Sei R auch weiterhin ein Ring (12). Wir haben noch zu zeigen, dass obige R-Funktion $\tilde{f}$ durch ein K-Polynom mit dem Vermittlerring dG dargestellt werden kann. Für unseren Ring R kann man den Unterring von $\mathfrak{R}(m)$ bestehend aus den Elementen $id\varepsilon$ $\left(i = 0, \ldots, \frac{m}{d} - 1\right)$ nehmen, und dann lässt sich $\tilde{f}$ in der Form

(82) $$\tilde{f}(id\varepsilon) = a_i(d\varepsilon) \qquad \left(i = 0, \ldots, \frac{m}{d} - 1\right)$$

annehmen mit ganzen a_i. Hierdurch wird zugleich auch eine (eindeutige) $\mathfrak{R}\left(\frac{m}{d}\right)$-Funktion

$$\tilde{g}(i\eta) = a_i\eta \qquad \left(i = 0, \ldots, \frac{m}{d} - 1\right)$$

definiert, wobei η das Einselement in $\mathfrak{R}\left(\frac{m}{d}\right)$ bezeichnet. Aus der Annahme folgt nach Satz 2, dass die Folge $a_i\eta$ $(i = \ldots, -1, 0, 1, \ldots)$ arithmetisch d. h. die Folge $a_i \left(i = 0, \ldots, \frac{m}{d} - 1\right)$ zyklisch-arithmetisch mod $\frac{m}{d}$ ist. Dies bedeutet nach Satz 14, dass sich $\tilde{g}$ durch ein K-Polynom $g(x)$ darstellen lässt, wofür dann gilt:

$$g(j) \equiv a_i \left(\mathrm{mod}\ \frac{m}{d}\right) \qquad \left(j \equiv i \left(\mathrm{mod}\ \frac{m}{d}\right)\right).$$

Setzen wir $f(x) = dg\left(\frac{x}{d}\right)$. Da $g(x)$ G-haltend ist, so ist $f(x)$ offenbar dG-haltend. Ausserdem gilt

$$f(j) \equiv a_i d \pmod{m} \qquad (j \equiv id \pmod{m}),$$

und so stellt $f(x)$ wegen (82) die Funktion $\tilde{f}$ (mit dem Vermittlerring dG) dar. Das beendet den Beweis von Satz 7.

§ 14. Beweis von Satz 8.

Nach der ersten Hälfte von Satz 4 folgt diejenige von Satz 8 aus der ersten Hälfte von Satz 14. Die zweite Hälfte von Satz 8 lässt sich dann mit Rücksicht auf (13) so aussprechen: (14) ist die Anzahl aller mod m verschiedenen Lösungen $a_1, \ldots, a_m$ von (10). Somit folgt die Richtigkeit von (14) aus dem chinesischen Restsatz, womit wir Satz 8 bewiesen haben.

§ 15. Beweis von Satz 9.

Wir wollen Satz 9 d. h. die Formeln (15) beweisen. Im Fall $e = 1$ gilt bekanntlich $g = p-1$, $v = 0$, und so ist (15) für diesen Fall richtig, weshalb wir im folgenden $e \geqq 2$ annehmen.

Nach Satz 14 (angewandt für $m = p^e$) ist g gleich dem Maximum der Ordnungszahlen aller ganzzahligen p^e-gliedrigen zyklisch-arithmetischen Folgen mod p^e. Mit Berücksichtigung von (38) folgt aus der ersten Hälfte von Satz 3, dass dieses Maximum gleich dem Fall $r = e$ von (9) ist, womit wir die erste Formel (15) bewiesen haben.

Es wird bequem die restliche Behauptung von Satz 9 (d. h. die zweite Formel (15))

so zu beweisen, dass wir ν durch (15) definieren, und dann haben wir zu zeigen, dass für dieses ν auch die im Satz 9 formulierte (erste) Definition gilt.

Bezeichne $\tilde{f}$ diejenige $\Re(p^e)$-Funktion, die an der Stelle 0 gleich ε ist und sonst überall in $\Re(p^e)$ verschwindet, wobei ε das Einselement von $\Re(p^e)$ bezeichnet. Weiter betrachten wir die Menge aller K-Polynome $f(x)$, die die Funktion $\tilde{f}$ darstellen. Es ist klar, dass mit einem solchen $f(x)$ durch die Polynome

$$\sum_{i=0}^{p^e-1} a_i f(x-i) \qquad (a_i = 0, \ldots, p^e-1)$$

alle $\Re(p^e)$-Funktionen dargestellt werden. Es genügt also zu zeigen, dass p^ν das Minimum der Nenner[10]) aller $f(x)$ aus der betrachteten Menge ist.

Ein spezielles $f(x)$ lässt sich nach Satz 14 als

$$f_0(x) = c_0 + c_1\binom{x}{1} + \cdots + c_g\binom{x}{g} \qquad (g = ep^e-(e-1)p^{e-1}-1) \tag{83}$$

angeben, wobei c_i das erste Glied von $\Delta^i \mathfrak{e}_1$ für das p^e-gliedrige Folge $\mathfrak{e}_1 = (1, 0, \ldots, 0)$ bezeichnet. (Dabei haben wir berücksichtigt, dass $\mathfrak{e}_1$ nach dem vorigen zyklisch-arithmetisch von der Ordnung g mod p^e ist). Bezeichne μ die Vielfachheit, mit der p im Nenner von $f_0(x)$ aufgeht, und ähnliches sollen $\mu_0, \ldots, \mu_g$ der Reihe nach für die Glieder $\frac{c_i}{i!}(x)_i$ der Summe auf der rechten Seite von (83) bezeichnen.

Wir wollen zeigen, dass $\mu = \nu$ ist. Hierzu zeigen wir zunächst

$$\mu_g \geqq \mu_0, \ldots, \mu_{g-1}\,, \tag{84}$$

woraus offenbar $\mu = \mu_g$ folgt, und dann werden wir nur noch

$$\mu_g = \nu \tag{85}$$

zu beweisen haben. Für einen Augenblick bezeichnen wir die Zahl (9) mit s. Nach Satz 3 gilt

$$p^r \nmid \Delta^s \mathfrak{e}_1\,, \quad p^r | \Delta^{s+1}\mathfrak{e}_1 \qquad (r = 1, \ldots, e)\,. \tag{86}$$

Aus letzterem folgt

$$p^r | c_i \qquad (rp^e-(r-1)p^{e-1} \leqq i \leqq g;\ r = 1, \ldots, e-1)\,. \tag{87}$$

Insbesondere gilt also $p^{e-1}|c_g$. Andererseits folgt aus (85) (nämlich mit $r = e$), dass die Glieder von $\Delta_g \mathfrak{e}_1$ miteinander kongruent aber $\not\equiv 0$ (mod p^e) sind, und so gilt genauer

$$p^{e-1} || c_g\,. \tag{88}$$

Bezeichne i^* die Vielfachheit, mit der p in $i!$ aufgeht. Aus der obigen Definition

von μ_i $\left(= \text{der Vielfachheit von } p \text{ im verkürzten Bruch } \frac{i!}{c_i}\right)$ folgt sofort

$$\mu_i \leqq i^* \qquad (i = 0, \ldots, g), \tag{89}$$

und wegen (87) gilt sogar

$$\mu_i \leqq i^* - r \qquad \left(rp^e - (r-1)p^{e-1} \leqq i \leqq g;\ r = 1, \ldots, e-1\right). \tag{90}$$

Insbesondere gilt nach (88) genauer

$$\mu_g = g^* - (e-1). \tag{91}$$

Zum Beweis von (84) genügt es wegen (89)—(91), wenn wir

$$g^* - (e-1) \geqq i^* - r \qquad \left(rp^e - (r-1)p^{e-1} \leqq i \leqq (r+1)p^e - rp^{e-1} - 1;\ r = 1, \ldots, e-1\right),$$
$$g^* - (e-1) \geqq i^* \qquad (0 \leqq i \leqq p^e - 1)$$

zeigen. Es genügt dies offenbar nur für das grösstmögliche i des jeweiligen Intervalls zu tun, und dann handelt es sich einfach um den Beweis von

$$g^* - (e-1) \geqq \left((r+1)p^e - rp^{e-1} - 1\right)^* - r \qquad (r = 0, \ldots, e-1).$$

Beim Vergrössern von r um 1 vergrössert sich die rechte Seite mindestens um $p^{e-1} - p^{e-2} - 1 (\geqq 0)$, wächst also mit r monoton zu. Für $r = e-1$ sind beide Seiten (nach (15)) gleich, womit wir (84) bewiesen haben. Ausserdem folgt (85) aus (15) und (91), womit die Behauptung $\mu = \nu$ bewiesen ist.

Ist a eine ganze Zahl, die $\equiv 1 \pmod{p^e}$ ist, sogehört $af_0(x)$ unter den (obiges $\tilde{f}$ darstellenden) Polynomen $f(x)$. Man kann a so wählen, dass der Nenner von $af_0(x)$ gleich p^μ ist. Wenn wir also beweisen, dass der Nenner von jedem $f(x)$ (aus der betrachteten Menge) durch p^μ teilbar ist, so werden wir wegen $\mu = \nu$ auch schon Satz 9 bewiesen haben.

Wir schicken folgende Bemerkung voran. Hat

$$a_0 + a_1(x)_1 + \cdots + a_n(x)_n \tag{92}$$

rationale Koeffizienten a_i und ist der Nenner eines Gliedes $a_i(x)_i$ durch eine ganze Zahl k teilbar, so ist der Nenner von (92) ebenfalls durch k teilbar. Die Richtigkeit folgt sofort daraus, dass das Polynom $(x)_i$ ganzzahlig und von der Form $x^i + \cdots$ ist.

Nunmehr setzen wir für das beliebige Polynom $f(x)$ aus der betrachteten Menge

$$f(x) = d_0 + d_1\binom{x}{1} + \cdots + d_n\binom{x}{n}.$$

Wegen der ersten Hälfte von Satz 9 muss $n \geqq g$ sein. Weiter folgt aus Satz 13, dass $d_g \equiv c_g \pmod{p^e}$ gelten muss. Hiernach und nach (88) enthalten d_g, c_g dieselbe

Potenz von p, und so folgt aus dem obigen, dass der Nenner von $d_g\binom{x}{g}$ (wie der von $c_g\binom{x}{g}$) durch p^μ teilbar ist. Da $f(x)$ von der Form (92) ist, so hat dies nach der vorangeschickten Bemerkung zur Folge, dass auch der Nenner von $f(x)$ durch p^μ teilbar ist, womit wir Satz 9 bewiesen haben.

§ 16. Beweis von Satz 10.

Um Satz 10 zu beweisen nehmen wir zuerst (16) an. Da die a_i in (13) nur mod m bestimmt sind, so darf angenommen werden, dass (16) sogar mod $i!$ gilt.[16] Dann liefert die Formel (27) für $n = m-1$ ein G-Polynom $f(x)$ mit $f(i) = a_i$ $(i = 0, \ldots, m-1)$, und so stellt dieses $f(x)$ die Funktion (13) dar. Dies beweist die »dann« Behauptung von Satz 10.

Nehmen wir umgekehrt an, dass die Funktion (13) durch ein G-Polynom $f(x)$ dargestellt werden kann. Dann gilt

$$f(i) \equiv a_i \pmod{m} \qquad (i = 0, \ldots, m-1)\,. \tag{93}$$

Setzen wir

$$f(i) = c_i \qquad (i = 0, 1, \ldots)\,, \tag{94}$$

so gilt (Formel (27))

$$f(x) = \sum_i \left(c_i - \binom{i}{1} c_{i-1} + \cdots + (-1)^i c_0\right)\binom{x}{i}$$

(die rechte Seite bricht mit einem Gliede ab), woraus

$$c_i - \binom{i}{1} c_{i-1} + \cdots + (-1)^i c_0 \equiv 0 \pmod{i!}$$

folgt. Dies gilt mod $(m, i!)$ noch mehr, und da wegen (93), (94) $c_i \equiv a_i \pmod{m}$ $(i = 0, \ldots, m-1)$ gilt, so sind die Kongruenzen (16) erfüllt. Das beweist die »nur dann« Behauptung von Satz 10.

Um auch (17) zu beweisen, haben wir nur zu zeigen, dass (17) der Anzahl aller mod m verschiedenen Lösungen $a_0, \ldots, a_{m-1}$ $(a_i = 0, \ldots, m-1)$ von (16) gleich ist. In der Tat lassen sich $a_0, \ldots, a_{m-1}$ der Reihe nach auf

$$\frac{m}{(m, 0!)}, \ldots, \frac{m}{(m, (m-1)!)}$$

[16] Das sieht man so ein. Die a_i $(i = 0, \ldots, m-1)$ lassen sich nacheinander gegen solche $a_i' = a_i + mx_i$ $(x_i \in G)$ austauschen, für die die entsprechende Kongruenz (16) schon mod $i!$ gilt. Die lineare Kongruenz

$$(mx_i + a_i) - \binom{i}{1} a_{i-1}' + \cdots + (-1)^i a_0' \equiv 0 \pmod{i!}$$

lässt sich nämlich wegen (16) für das Unbekannte x_i auflösen.

Arten (mod m) so wählen, dass (16) erfüllt wird, womit wir (17) und auch Satz 10 bewiesen haben.

§ 17. Beweis von Satz 11.

Im Satz 11 handelt es sich um die Frage, wann durch (18) ein G-Polynom $f(x)$ charakterisiert wird. Vor allem ist hierzu notwendig, dass $\ldots, a_{-1}, a_0, a_1, \ldots$ eine arithmetische Folge von einer Ordnung n ist. Ist dies der Fall, so zeigt (27), dass die gestellte Frage mit der weiteren Bedingung

$$(\Delta^i a_0 =)\, a_i - \binom{i}{1} a_{i-1} + \cdots + (-1)^i a_0 \equiv 0 \pmod{i!} \qquad (i = 0, 1, \ldots)$$

beantwortet ist. Für $i \geqq n+1$ verschwindet die linke Seite, und so muss nur (19) gefordert werden, womit wir Satz 11 bewiesen haben.