I. SCHUR

Arithmetische Eigenschaften der Potenzsummen einer algebraischen Gleichung

Compositio Mathematica, tome 4 (1937), p. 432-444

<http://www.numdam.org/item?id=CM_1937__4__432_0>

Arithmetische Eigenschaften der Potenzsummen einer algebraischen Gleichung

von

I. Schur

Berlin

(Meinem Freunde Edmund Landau zu seinem 60. Geburtstag am 14. Februar 1937.)

§ 1. *Übersicht über die Hauptresultate.*

Zu jedem Polynom

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_{n-1}x + a_n = \prod_{\nu=1}^{n} (x - x_\nu)$$

gehört die Folge der Potenzsummen

$$s_m = x_1^m + x_2^m + \dots + x_n^m \quad (m = 1, 2, 3, \dots),$$

die sich mit Hilfe der Rekursionsformeln

$$(1) \qquad s_m + a_1 s_{m-1} + \dots + a_{m-1}s_1 + m a_m = 0 \quad (a_{n+1} = a_{n+2} = \dots = 0)$$

als ganze rationale Funktionen von $a_1, a_2, \dots, a_n$ mit ganzen rationalen Koeffizienten darstellen lassen. Dagegen wird für $m \leqq n$ erst

$$(2) \qquad m!\, a_m = A_m(s_1, s_2, \dots, s_m)$$

eine Funktion derselben Art.

Wählt man $a_1, a_2, \dots, a_n$ als Größen eines beliebigen Körpers K der Charakteristik 0, so bestimmen die n ersten Potenzsummen

$$(3) \qquad s_1, s_2, \dots, s_n$$

das Polynom $f(x)$ in eindeutiger Weise.[1]) Geht man aber von einem festgewählten Teilring (Integritätsbereich) R des Körpers K aus, so entsteht folgende Frage:

A. Kann man, wenn n Größen (3) aus R vorgegeben sind, ohne Benutzung der Rekursionsformeln (1) oder der expliziten

---

[1]) Dies gilt auch, wenn die Charakteristik von K größer als n ist. Im folgenden beschränke ich mich der Einfachheit wegen auf den Fall der Charakteristik 0.

Ausdrücke (2) entscheiden, ob die Größen (3) sich als die n ersten Potenzsummen eines Polynoms $f(x)$ auffassen lassen, dessen Koeffizienten $a_1, a_2, \ldots, a_n$ sämtlich in R enthalten sind?

Genügen die n Größen (3) aus R dieser Forderung, so will ich kurz sagen, *daß sie die Eigenschaft* (R) *besitzen.*

Für den Fall des Ringes R_0 der ganzen rationalen Zahlen verdankt man Herrn W. Jänichen [2]) eine sehr interessante Lösung der Aufgabe A:

I. *Dann und nur dann besitzen n ganze rationale Zahlen* (3) *die Eigenschaft* (R_0), *wenn für $m \leqq n$ die Kongruenzen*

$$\sum_{d \mid m} \mu(d)\, s_{\frac{m}{d}} \equiv 0 \pmod{m}$$

gelten.

Man kann diesen Satz noch etwas anders formulieren:

II. 1. *Ist $m > 1$ ein beliebiger Index, p eine in m aufgehende Primzahl und $m = kp^\mu$, so gelten für jedes Polynom $f(x)$ mit ganzen rationalen Koeffizienten die Kongruenzen*

$$s_m \equiv s_{\frac{m}{p}} \pmod{p^\mu}. \tag{4}$$

2. *Dann und nur dann besitzen n ganze rationale Zahlen* (3) *die Eigenschaft* (R_0), *wenn die Kongruenzen* (4) *für alle Indices* $m = 2, 3, \ldots, n$ *und jede in m aufgehende Primzahl p bestehen.*

Man hat hierbei zu beachten, daß in dem speziellen Falle

$$f(x) = x^n - ax^{n-1}$$

die m-te Potenzsumme s_m gleich a^m wird. In diesem Falle liefern die Kongruenzen (4) nur den kleinen Fermatschen Satz der elementaren Zahlentheorie. Man kann auch sagen, daß jedes ganzzahlige Polynom $f(x)$ sich in bezug auf die Kongruenzen (4) so verhält, als wären alle Nullstellen von $f(x)$ ganze rationale Zahlen.

Der erste Teil des Satzes II bleibt (in Analogie zum Fermatschen Satz der Idealtheorie) noch erhalten, wenn man von einem beliebigen algebraischen Zahlkörper K_1 und dem Ring R_1 aller ganzen Zahlen von K_1 ausgeht.

III. *Es sei $f(x)$ ein Polynom mit ganzen algebraischen Koeffizienten aus K_1. Ferner sei p eine rationale Primzahl und $\mathfrak{p}$ ein*

---

[2]) Über die Verallgemeinerung einer Gaußschen Formel aus der Theorie der höheren Kongruenzen [Sitzungsberichte der Berliner Mathematischen Gesellschaft **20** (1921), 23—29].

in p aufgehendes Primideal mit der Norm P. Für jeden Index m, der durch $Pp^{\mu-1}$ ($\mu \geqq 1$) *teilbar ist, genügen die Potenzsummen von* $f(x)$ *der Kongruenz*

$$s_m \equiv s_{\frac{m}{P}} \pmod{\mathfrak{p}^\mu}. \tag{5}$$

Daß das Bestehen aller in Betracht kommenden Kongruenzen (5) für alle Indizes $m = 2, 3, \ldots$ nicht für jedes System von n ganzen Zahlen $s_1, s_2, \ldots, s_n$ aus einem beliebigen algebraischen Zahlkörper K_1 ausreicht, um behaupten zu können, daß das System die Eigenschaft (R_1) besitzt, setzt das Beispiel

$$f(x) = x^n - \binom{a}{1}x^{n-1} + \binom{a}{2}x^{n-2} - \ldots + (-1)^n\binom{a}{n}, \tag{6}$$

das auf

$$s_1 = s_2 = \ldots = s_n = a$$

führt, in Evidenz. Denn hier sind die Kongruenzen (5) für jede Zahl a aus R_1 gewiß richtig, dagegen brauchen die Binomialkoeffizienten $\binom{a}{m}$ nicht sämtlich ganze algebraische Zahlen zu sein.

Für jeden beliebigen Körper K (der Charakteristik 0) und jeden Teilring R gelten wesentlich kompliziertere Kriterien, die ich auch im Falle eines algebraischen Zahlkörpers nicht zu vereinfachen imstande bin.

IV. *Dann und nur dann besitzen n Größen* $s_1, s_2, \ldots, s_n$ *aus R die Eigenschaft* (R), *wenn die mit Hilfe der Gleichungen*

$$s_m = \sum_{d|m} d c_d^{\frac{m}{d}} \qquad (m=1, 2, \ldots, n)$$

eindeutig bestimmten Größen $c_1, c_2, \ldots, c_n$ *aus K sämtlich in R enthalten sind.*

Dieses Kriterium ergibt sich sehr einfach mit Hilfe einer kleinen Abänderung der Jänichenschen Überlegungen. Etwas weniger auf der Hand liegend ist folgende Erweiterung von IV:

V. *Für jede (rationale) Primzahl p betrachte man den R enthaltenden Ring* $R^{(p)}$ *aller Größen* $\frac{r}{h}$, *wo r alle Größen aus R durchläuft und h eine beliebige zu p teilerfremde ganze rationale Zahl bedeutet. Dann und nur dann besitzen n Größen* $s_1, s_2, \ldots, s_n$ *aus* $R^{(p)}$ *die Eigenschaft* $(R^{(p)})$, *wenn für jeden Index* $m \leqq n$ *der Form*

$$m = kp^\mu, \quad (k, p) = 1, \quad \mu \geqq 0,$$

die mit Hilfe der n Gleichungen

$$s_m = z_{k,0}^{p^\mu} + p z_{k,1}^{p^{\mu-1}} + p^2 z_{k,2}^{p^{\mu-2}} + \dots + p^\mu z_{k,p^\mu}$$

eindeutig bestimmten Größen $z_{k,\lambda}$ von K sämtlich in $R^{(p)}$ enthalten sind.

Auf Grund dieses Satzes liefert das Beispiel (6) ohne Mühe ein Resultat, das auch für die elementare Zahlentheorie von einem gewissen Interesse ist.

VI. *Ist K ein beliebiger Körper der Charakteristik 0, R ein beliebiger Teilring von K und p eine festgewählte (rationale) Primzahl, so gehören dann und nur dann sämtliche Binomialkoeffizienten $\binom{a}{m}$ $(m=2, 3, \dots)$ für alle Größen a aus R zu $R^{(p)}$, wenn für jede Größe a aus R die Kongruenz*

$$a^p \equiv a \pmod{p}$$

gilt, d.h. $\frac{1}{p}(a^p - a)$ in R enthalten ist[3]).

Ich hebe ausdrücklich hervor, daß ich hier nur solche Eigenschaften der Potenzsummen eines Polynoms $f(x)$ berücksichtige, die sich ohne Kenntnis des Verhaltens der Nullstellen x_ν von $f(x)$ ergeben. Weiß man z.B. für ein Polynom $f(x)$ mit ganzen rationalen Koeffizienten, daß alle x_ν in einem algebraischen Zahlkörper K_1 liegen, so bestehen neben den Kongruenzen (4) auf Grund des Fermatschen Satzes der Idealtheorie in den früheren Bezeichnungen die (5) umfassenden Kongruenzen

$$s_{m+h} \equiv s_{\frac{m}{P}+h} \pmod{\mathfrak{p}^\mu} \quad (h=0, 1, 2, \dots).$$

Das Studium der schwierigen Frage, was sich umgekehrt aus dem Bestehen der Gesamtheit dieser Kongruenzen über die Beziehungen der x_ν zum Körper K_1 folgern läßt, liegt außerhalb des Rahmens der vorliegenden Untersuchung.

§ 2. *Beweis des Satzes II.*

Betrachtet man neben dem Polynom $f(x)$ das reziproke Polynom

$$g(t) = 1 + a_1 t + \dots + a_n t^n = \prod_{\nu=1}^{n} (1 - x_\nu t)$$

---

[3]) Hieraus folgt insbesondere, daß im Gebiet der ganzen rationalen Zahlen die Ganzzahligkeit der Binomialkoeffizienten aus dem kleinen Fermatschen Satz rein formal zu folgern ist. — Vgl. ferner § 5, Fußnote [5]).

so wird bekanntlich

$$(7)\qquad \varphi(t) = -\frac{tg'(t)}{g(t)} = \sum_{\nu=1}^{n} \frac{x_\nu t}{1-x_\nu t} = s_1 t + s_2 t^2 + \dots$$

Herr Jänichen gelangt zu seinem Satze auf folgendem Wege. Für beliebige Veränderliche $a_1, a_2, \dots, a_n$ darf rein formal

$$(8)\qquad g(t) = \prod_{m=1}^{\infty} (1-t^m)^{b_m}$$

gesetzt werden, wobei unter jedem Faktor die zugehörige binomische Reihe zu verstehen ist. Hierbei wird $b_1 = -a_1$ und allgemein kann jedes b_m rekursiv als der Koeffizient von $-t^m$ in der Potenzreihenentwicklung von

$$g(t)\cdot \prod_{\lambda=1}^{m-1} (1-t^\lambda)^{-b_\lambda}$$

eindeutig gekennzeichnet werden. Auf Grund der Tatsache, daß für eine ganze rationale Zahl z alle Binomialkoeffizienten $\binom{z}{h}$ $(h=2, 3, \dots)$ ganze rationale Zahlen sind, erkennt man leicht, daß für jedes m *die Koeffizienten* $a_1, a_2, \dots, a_m$ *dann und nur dann ganze rationale Zahlen sind, wenn die Exponenten* $b_1, b_2, \dots, b_m$ *diese Eigenschaft besitzen.*

Auf Grund von (7) und (8) folgt ferner

$$\varphi(t) = \sum_{m=1}^{\infty} s_m t^m = \sum_{m=1}^{\infty} m b_m t^m (1-t^m)^{-1} = \sum_{m=1}^{\infty} m b_m (t^m + t^{2m} + \dots).$$

Dies liefert durch Koeffizientenvergleichen

$$s_m = \sum_{d\mid m} d b_d \quad (m=1, 2, \dots),$$

woraus in bekannter Weise umgekehrt

$$(9)\qquad m b_m = \sum_{d\mid m} \mu(d)\, s_{\frac{m}{d}}$$

folgt. Der Jänichensche Satz I ergibt sich hieraus ohne weiteres.

Für eine Primzahlpotenz $m = p^\mu$ wird hierbei

$$p^\mu b_{p^\mu} = s_{p^\mu} - s_{p^{\mu-1}},$$

was für ganze rationale $a_1, a_2, \dots, a_n$ die Kongruenz (4) im Falle $m = p^\mu$ liefert. Für $m = kp^\mu$ mit $k > 1$ ergibt sich aber (4) am einfachsten auf Grund der Tatsache, daß $x_1^k, x_2^k, \dots, x_n^k$ wieder als die n Wurzeln einer Gleichung

$$x^n + a_1^{(k)} x^{n-1} + \ldots + a_n^{(k)} = 0 \tag{10}$$

mit ganzen rationalen Koeffizienten aufzufassen sind. Insbesondere besitzen demnach die Potenzsummen $s_k, s_{2k}, \ldots$ alle Eigenschaften, die den Potenzsummen $s_1, s_2, \ldots$ zukommen.

Um auch den zweiten Teil des Satzes II zu beweisen, benutze man wieder die Formel (9). Ist insbesondere $m = m_1 m_2$ mit $(m_1, m_2) = 1$ so läßt (9) die Schreibweise

$$mb_m = \sum_{d_1 | m_1} \mu(d_1) \sum_{d_2 | m_2} \mu(d_2)\, s_{\frac{m_1 m_2}{d_1 d_2}}$$

zu. Für

$$m_1 = k,\ m_2 = p^\mu,\ (k, p) = 1,\ \mu > 0$$

wird hierbei für jeden Teiler d_1 von k die innere Summe gleich

$$s_{k_1 p^\mu} - s_{k_1 p^{\mu-1}},\ \left(k_1 = \frac{k}{d_1}\right). \tag{11}$$

Sind demnach die n ersten Potenzsummen $s_1, s_2, \ldots, s_n$ unseres Polynoms $f(x)$ ganze rationale Zahlen, die für alle $m \leqq n$ und für jede in m aufgehende Primzahl p (bei $m = k p_\mu$, $(k, p) = 1$) den Kongruenzen (4) genügen, so erkennt man, daß alle Differenzen (11) durch p^μ teilbar sind. Folglich ist für $m \leqq n$ die ganze rationale Zahl mb_m durch jede in m aufgehende Primzahlpotenz teilbar, was nur besagt, daß b_m ganz ist. Aus der Ganzzahligkeit von $b_1, b_2, \ldots, b_n$ folgt aber auch, daß alle a_m ganze rationale Zahlen sind.

Man erkennt ohne weiteres, daß die hier durchgeführten Betrachtungen nicht nur für den Ring R_0 der ganzen rationalen Zahlen, sondern auch für jeden Ring R stichhaltig bleiben, der folgender Forderung genügt:

B. Für jede Größe a von R sollen alle Binomialkoeffizienten $\binom{a}{h}$ $(h = 2, 3, \ldots)$ in R enthalten sein.

Dies zeigt, daß für jeden derartigen Ring R auch die Sätze I und II richtig bleiben. Hierbei soll eine Kongruenz der Form

$$r_1 \equiv r_2 \pmod{m}$$

zwischen zwei Elementen r_1, r_2 von R bei ganzem rationalem m nur bedeuten, daß das Element $\frac{1}{m}(r_1 - r_2)$ des Körpers K in R enthalten ist.

Ein Ring R, der der Forderung B. genügt, ist z.B. die Gesamtheit der (in bezug auf R_0) ganzwertigen Polynome in endlich vielen Variabeln.

§ 3. *Die Sätze III und IV.*

Besitzt unser Ring R die Eigenschaft B nicht, so bedarf der Jänichensche Ansatz (8) einer Abänderung.

In jedem Fall darf rein formal

$$g(t) = 1 + a_1 t + \ldots + a_n t^n = \prod_{m=1}^{\infty} (1 - c_m t^m) \tag{12}$$

gesetzt werden, wobei

$$c_1 = -a_1, \ c_2 = -a_2, \ c_3 = a_1 a_2 - a_3$$

zu setzen ist und allgemein rekursiv c_m als Koeffizient von $-t^m$ in der Potenzreihenentwicklung von

$$g(t) \cdot \prod_{\lambda=1}^{m-1} (1 - c_\lambda t^\lambda)^{-1}$$

eindeutig gekennzeichnet werden kann. Hier wird jedes a_m eine ganze rationale Funktion von $c_1, c_2, \ldots, c_m$ mit ganzen rationalen Koeffizienten und umgekehrt jedes c_m eine ebensolche Funktion von $a_1, a_2, \ldots, a_m$. Wir können also sagen: *Für jedes $f(x)$ sind dann und nur dann $a_1, a_2, \ldots, a_n$ in unserem Ring R enthalten, wenn $c_1, c_2, \ldots, c_n$ diese Eigenschaft haben.*

Aus (7) und (8) folgt ferner

$$\varphi(t) = \sum_{m=1}^{\infty} s_m t^m = \sum_{m=1}^{\infty} \frac{m c_m t^m}{1 - c_m t^m} = \sum_{m=1}^{\infty} m(c_m t^m + c_m^2 t^{2m} + \ldots).$$

Dies liefert

$$s_m = \sum_{d \mid m} d c_d^{\frac{m}{d}} \quad (m = 1, 2, 3, \ldots), \tag{13}$$

was insbesondere die Richtigkeit des Satzes IV in Evidenz setzt.

Um den Satz III zu beweisen, beachte man, daß insbesondere für jede Primzahlpotenz $m = p^\lambda$

$$s_m = c_1^{p^\lambda} + p c_p^{p^{\lambda-1}} + \ldots + p^\lambda c_{p^\lambda} \tag{13'}$$

wird. Ist nun R_1 die Gesamtheit der ganzen Zahlen eines algebraischen Zahlkörpers K_1 und gehören alle Koeffizienten $a_1, a_2, \ldots, a_n$ zu R_1, so gilt dies auch für alle Potenzsummen $s_1, s_2, \ldots$ und für unsere Hilfsgrößen $c_1, c_2, \ldots$ Man betrachte nun eine rationale Primzahl p und ein in p aufgehendes Primideal $\mathfrak{p}$ des Körpers K_1. Bedeutet P die Norm von $\mathfrak{p}$, so wird für jede Zahl c aus R_1

$$c^P \equiv c \pmod{\mathfrak{p}}$$

woraus

$$c^{Pp} \equiv c^{p} \quad (\bmod\ \mathfrak{p}^2),\ c^{Pp^2} \equiv c^{p^2} \quad (\bmod\ \mathfrak{p}^3)\ \text{usw.}$$

folgt. Für $m = Pp^{\mu-1}$ $(\mu \geqq 1)$ ergibt sich hieraus in (13′)

$$c_1^m \equiv c_1^{p^{\mu-1}},\quad pc_p^{\frac{m}{p}} \equiv pc_p^{p^{\mu-2}}, \ldots,\ p^{\mu-1}c_{p^{\mu-1}}^{P} \equiv p^{\mu-1}c_{p^{\mu-1}} \ (\bmod\ \mathfrak{p}^{\mu}).$$

Dies liefert

$$s_m \equiv c_1^{p^{\mu-1}} + pc_p^{p^{\mu-2}} + \ldots + p^{\mu-1}c_{p^{\mu-1}} \quad (\bmod\ \mathfrak{p}^{\mu}).$$

Die rechte Seite ist aber nach (13′) gleich $s_{p^{\mu-1}}$ zu setzen, so daß

$$s_m \equiv s_{\frac{m}{P}} \quad (\bmod\ \mathfrak{p}^{\mu})$$

wird.

Daß diese Kongruenz auch für jedes Multiplum $m = kP_{p^{\mu-1}}$ von $P_{p^{\mu-1}}$ gilt, folgt wieder aus der Tatsache, daß die Zahlen

$$s_{kl} = s_e^{(k)} \quad (l = 1, 2, 3, \ldots)$$

als die Potenzsummen einer Gleichung der Form (10) mit Koeffizienten aus R_1 aufgefaßt werden können.

§ 4. *Eine Hilfsbetrachtung. Der Satz V.*

Man setze, wenn $x_1, x_2, \ldots, x_n$ voneinander unabhängige Veränderliche sind,

$$g(t) = \prod_{\lambda=1}^{n}(1-x_\lambda t) = 1 + a_1 t + \ldots + a_n t^n. \tag{14}$$

Für jede ganze rationale Zahl $k > 0$ bilde man, wenn ε alle k-ten Einheitswurzeln durchläuft,

$$\prod_{\varepsilon} g(\varepsilon t) = \prod_{\lambda=1}^{n}(1-x_\lambda^k t^k) = 1 + a_1^{(k)}t^k + \ldots + a_n^{(k)}t^{kn}. \tag{15}$$

Hierbei wird bekanntlich jeder Koeffizient $a_m^{(k)}$ eine ganze rationale Funktion $H_m^{(k)}$ von $a_1, a_2, \ldots, a_n$ mit ganzen rationalen Koeffizienten.

Setzt man $t^k = u$ und

$$1 + a_1^{(k)}u + \ldots + a_n^{(k)}u^n = g_k(u),$$

so treten wieder an Stelle der früher betrachteten Potenzsummen $s_1, s_2, \ldots$ die Ausdrücke $s_k, s_{2k}, \ldots$

Hat $g(t)$ insbesondere die Gestalt $1 - c_m t^m$ so wird $g_k(u)$ ein Ausdruck der Form

$$(16) \qquad h_m^{(k)}(u) = 1 + b_r u^r + b_{r+1} u^{r+1} + \ldots,$$

wo $rk \geqq m$ ist und $b_r, b_{r+1}, \ldots$ ganzzahlige ganze rationale Funktionen von c_m bedeuten. Ist insbesondere $m = kl$ ein Multiplum von k, so erhält man

$$(16') \qquad h_m^{(k)}(u) = (1 - c_m u^l)^k = 1 - kc_m u^l + \ldots$$

Man stelle nun $g_k(u)$ entsprechend der Formel (12) in der Gestalt

$$g_k(u) = \prod_{m=1}^{\infty} (1 - c_{k,m} u^m)$$

dar, so daß nach (13) für jedes $l = 1, 2, \ldots$

$$(17) \qquad s_{kl} = \sum_{d \mid l} d c_{k,d}^{\frac{l}{d}}$$

und insbesondere für eine Primzahlpotenz $l = p^\mu$ $(\mu \geqq 0)$

$$(17') \qquad s_{kp^\mu} = c_{k,1}^{p^\mu} + p c_{k,p}^{p^{\mu-1}} + \ldots + p^\mu c_{k,p^\mu}$$

wird.

Setzt man $c_{1,m} = c_m$, so gilt

$$g(t) = \prod_{m=1}^{\infty} (1 - c_m t^m),$$

und hieraus folgt in den hier eingeführten Bezeichnungen

$$g_k(u) = \prod_{r=1}^{\infty} (1 - c_{k,r} u^r) = \prod_{m=1}^{\infty} h_m^{(k)}(u).$$

Entwickelt man beide Produkte nach steigenden Potenzen von u und sucht man in beiden Potenzreihen den Koeffizienten einer Potenz u^l, so sind in dem linksstehenden Produkt nur die Indices $r \leqq l$ und rechts nur die Indices $m \leqq kl$ zu berücksichtigen. Die Formeln (16) und (16′) liefern, wie man unmittelbar erkennt, eine Relation der Form

$$(18) \qquad \varphi(c_{k,1}, c_{k,2}, \ldots, c_{k,l-1}) + c_{k,l} = \psi(c_1, c_2, \ldots, c_{kl-1}) + kc_{kl},$$

wo φ und ψ ganze rationale Funktionen ihrer Argumente mit ganzen rationalen Koeffizienten sind.

Diese Relationen sind hier nur für den Fall eines Polynoms der Form (17) abgeleitet worden. Auf Grund einer bekannten

Gaußschen Schlußweise erkennt man, daß sie für beliebige Veränderliche $a_1, a_2, \ldots, a_n$ gelten, wenn man die Potenzsummen s_m etwa mit Hilfe der Newtonschen Rekursionsformel (1) und die $c_{k,r}$ mit Hilfe der Formeln (17) bestimmt.

Es sei nun wieder R ein beliebiger Teilring eines Körpers K der Charakteristik 0. Ist p eine *festgewählte* Primzahl, so bilde man den früher eingeführten Ring $R^{(p)}$. Um den Satz V zu beweisen, genügt es zu zeigen[4]):

Sind für ein Polynom $f(x) = x^n + a_1 x^{n-1} + \ldots$ *alle Koeffizienten* a_m *im Körper* K *enthalten, und weiß man, daß erstens die* n *ersten Potenzsummen* $s_1, s_2, \ldots, s_n$ *Größen aus* $R^{(p)}$ *sind, und daß zweitens auch für jede Zahl*

$$m = kp^\mu \leqq n, \quad \mu \geqq 0, \quad (k, p) = 1 \tag{19}$$

die aus (17′) *zu berechnenden Größen*

$$c_{k,1},\ c_{k,p},\ \ldots,\ c_{k,p^\mu}$$

in $R^{(p)}$ *liegen, so gehören auch* $a_1, a_2, \ldots, a_n$ *zu* $R^{(p)}$.

Nach dem Früheren ist nur zu beweisen, daß alle Größen $c_1, c_2, \ldots, c_n$ in $R^{(p)}$ enthalten sind, demnach auch alle $c_{k,l}$ mit $kl \leqq n$. Für $l = 1$ folgt dies aus $c_{k,l} = s_k$. Es sei nun schon bekannt, daß $c_1, c_2, \ldots, c_{m-1}$ $(m > 1)$ in $R^{(p)}$ enthalten sind. Ist $(m, p) = 1$, so folgt schon aus

$$s_m = \sum_{d|m} d c_d^{\frac{m}{d}},$$

weil hier c_m nur in dem Glied mc_m auftritt, daß auch c_m zu $R^{(p)}$ gehört. Es sei also m von der Form (19) mit $\mu > 0$. Für $l < p^\mu$ geht für dieses k in (19) aus (18) hervor, daß auch $c_{k,1}, c_{k,2}, \ldots, c_{k,p^\mu - 1}$ in $R^{(p)}$ enthalten sind. Ferner gilt dies auf Grund unserer Voraussetzung für c_{k,p^μ}. Setzt man in (18) $l = p^\mu$, so erkennt man, daß auch c_m in $R^{(p)}$ liegt.

Damit ist der Satz V als bewiesen anzusehen.

§ 5. *Eine Ergänzung zum Satz I. Der Satz IV.*

Unser Ring R möge in bezug auf eine *festgewählte* Primzahl p folgender Forderung genügen:

F_p. Für jedes Element a von R sei

$$a^p \equiv a \pmod{p},$$

d.h. $a^p = a + pa_1$, *wo auch* a_1 *in* R *enthalten sein soll.*

[4]) Man hat auf S. [4] 435 nur $z_{k,\nu} = c_{k,p^\nu}$ für $\nu = 0, 1, 2, \ldots$ zu setzen.

Hieraus folgt dann auch

$$a^{p^2} \equiv a^p \pmod{p^2}, \quad a^{p^3} \equiv a^{p^2} \pmod{p^3}, \ldots$$

Ferner erkennt man leicht, daß auch für den Ring $R^{(p)}$ die Forderung F_p erfüllt ist. Denn ist $c = \frac{a}{h}$, wo a ein Element von R ist und h eine zu p teilerfremde ganze rationale Zahl bedeutet, so wird

$$c^p - c = \frac{1}{h^p} \cdot (a^p - h^{p-1}a) = p \cdot \frac{a_1}{h^p} + (1 - h^{p-1}) \cdot \frac{a}{h^p},$$

was wegen $p/(1-h^{p-1})$ die Gestalt pc_1 mit $c_1 \subset R^{(p)}$ hat.

Auf Grund des Satzes V läßt sich hieraus ohne Mühe folgern:

II . *Dann und nur dann liegen alle Koeffizienten* $a_1, a_2, \ldots, a_n$ *unseres Polynoms* $f(x)$ *in* $R^{(p)}$, *wenn erstens die* n *Potenzsummen* $s_1, s_2, \ldots, s_n$ *in* $R^{(p)}$ *enthalten sind, und wenn zweitens für jeden Index*

$$m = kp^\mu \leqq n, \quad \mu > 0, \quad (k, p) = 1$$

in $R^{(p)}$ *die Kongruenz*

$$s_m \equiv s_{\frac{m}{p}} \pmod{p^\mu} \tag{20}$$

besteht.

Um dies zu beweisen, benutze man wieder die durch die Formeln (17) eindeutig bestimmten Größen c_{k,p^ν} $(\nu=0, 1, \ldots)$. Liegen alle $a_1, a_2, \ldots, a_n$ in $R^{(p)}$, so gilt dies auch für alle s_m und alle c_{k,p^ν}. Die Differenz

$$d_m = s_m - s_{\frac{m}{p}}$$

läßt sich in der Form

$$d_m = \left(c_{k,1}^{p^\mu} - c_{k,1}^{p^{\mu-1}}\right) + p\left(c_{k,p}^{p^{\mu-1}} - c_{k,p}^{p^{\mu-2}}\right) + \ldots + \\ + p^{\mu-1}\left(c_{k,p^{\mu-1}}^p - c_{k,p^{\mu-1}}\right) + p^\mu c_{k,p^\mu} \tag{21}$$

schreiben. Ist aber für R, also auch für $R^{(p)}$ die Forderung F_p erfüllt, so wird jeder Summand der in (21) rechts stehenden Summe in $R^{(p)}$ kongruent 0 mod p^μ, folglich gilt dies auch für d_m, was die Kongruenz (20) liefert.

Weiß man umgekehrt, daß $s_1, s_2, \ldots, s_n$ in $R^{(p)}$ liegen und den Kongruenzen (20) genügen, so erhält man für jedes zu p teilerfremde k und für

$$m = k, k_p, k_{p^2}, \ldots, \quad m \leqq n$$

Schritt für Schritt (innerhalb des Ringes $R^{(p)}$)

(22) $s_k = c_{k,1}$

(22′) $d_{kp} = (c_{k,1}^p - c_{k,1}) + pc_{k,p} \equiv 0 \pmod p$

(22″) $d_{kp^2} = (c_{k,1}^{p^2} - c_{k,1}^p) + p(c_{k,p}^p - c_{k,p}) + p^2 c_{k,p} \equiv 0 \pmod{p^2}$

usw. Aus (22) folgt $c_{k,1} \subset R^{(p)}$, aus (21′) ergibt sich daher

$$pc_{k,p} \equiv 0 \pmod{p^2}, \text{ d.h. } c_{k,p} \subset R^{(p)},$$

aus (22″) alsdann

$$p^2 c_{k,p^2} \equiv 0 \pmod{p^2}, \text{ d.h. } c_{k,p^2} \subset R^{(p)}$$

usw. Folglich sind neben den s_m auch alle c_{k,p^ν} in $R^{(p)}$ enthalten, demnach gilt dies auch für $a_1, a_2, \ldots, a_n$.

Der Satz VI ist nur ein Spezialfall von II . Denn setzt man für beliebiges a

$$f(x) = x^n - \binom{a}{1} x^{n-1} + \binom{a}{2} x^{n-2} - \ldots + (-1)^n \binom{a}{n},$$

so wird

$$g(t) = 1 - \binom{a}{1} t + \binom{a}{2} t^2 - \ldots + (-1)^n \binom{a}{n} t^n$$

der n-te Abschnitt der Potenzreihenentwicklung von

$$h(t) = (1-t)^a.$$

Daher stimmt der n-te Abschnitt von

$$-\frac{tg'(t)}{g(t)} = s_1 t + s_2 t^2 + \ldots$$

mit dem n-ten Abschnitt von

$$-\frac{th'(t)}{h(t)} = \frac{at}{1-t} = at + at^2 + \ldots$$

überein, d.h. es wird

$$s_1 = s_2 = \ldots = s_n = a.$$

Ist nun a in einem Ring R gelegen, der der Forderung F_p genügt, so sind in diesem speziellen Fall die Voraussetzungen des Satzes II gewiß erfüllt, folglich sind alle Binomialkoeffizienten $\binom{a}{m}$ für $m = 2, 3, \ldots$ in $R^{(p)}$ enthalten. [5])

[5]) Man beachte, daß der Grad n von $f(x)$ beliebig groß gewählt werden kann. Bei der Berechnung von

$$\binom{a}{m} = \frac{1}{m!} \cdot a(a-1) \cdots (a-m+1)$$

in unserem Körper K hat man unter $a - \nu$ das Element $a - \nu\varepsilon$ zu verstehen, wenn ε das Einheitselement von K bedeutet.

Soll umgekehrt für jedes a aus R jedes $\binom{a}{m}$ in $R^{(p)}$ liegen, so ergibt sich insbesondere, daß

$$(p-1)!\binom{a}{p} = \frac{1}{p} \cdot a(a-1) \cdots (a-p+1)$$

in $R^{(p)}$ enthalten ist. Es ist aber, wie in der elementaren Zahlentheorie bewiesen wird, für beliebiges a

$$a(a-1) \cdots (a-p+1) = a^p - a + p\,\gamma(a)$$

wo $\gamma(a)$ eine ganze rationale Funktion von a mit ganzen rationalen Koeffizienten ist. Es ergibt sich daher, daß in $R^{(p)}$

$$b = a^p - a \equiv 0 \pmod{p}$$

wird. Hieraus folgt in bekannter Weise, daß diese Kongruenz auch in R gilt. Denn ist

$$b = p \cdot \frac{c}{h},\ b, c \subset R,\ h = 1, 2, 3, \ldots, (h, p) = 1,$$

so bestimme man zwei ganze rationale Zahlen u, v, so daß $up + vh = 1$ ist. Es wird dann

$$bhu = pcu = (1-vh)c,$$

also

$$\frac{c}{h} = bu + cv \subset R.$$

Ein Beispiel für einen Ring R, der für eine passend gewählte Primzahl p der Forderung F_p genügt, erhält man, indem man die Gesamtheit R aller ganzen Zahlen eines algebraischen Zahlkörpers K des Grades k betrachtet und für p eine Primzahl

$$p = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_k$$

wählt, wobei $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_k$ voneinander verschiedene Primideale von K sein sollen. Die Normen dieser Primideale müssen dann sämtlich gleich p sein. Für jede ganze Zahl a von K wird also

$$a^p \equiv a \pmod{\mathfrak{p}_\lambda} \quad (\lambda = 1, 2, \ldots, k),$$

was

$$a^p \equiv a \pmod{p}$$

liefert. Für eine solche Primzahl p ergibt sich also, ohne daß weitere Hilfsmittel der Idealtheorie herangezogen zu werden brauchen, daß für jede ganze Zahl a aus K alle Binomialkoeffizienten $\binom{a}{m}$ mod p ganz sind.

(Eingegangen den 18. Februar 1937.)