Ein Satz über Iteration von Potenzreihen und seine zahlentheoretische Anwendung.

Von

RUDOLF FUETER.

Als Manuskript eingegangen den 2. Februar 1917.

I.

Schröder hat in den Math. Annalen, Bd. 3 (1871), pag. 310 u. ff. die Iteration einer Potenzreihe:

$$F(z) = z + \alpha_2 z^2 + \alpha_3 z^3 + \cdots + \alpha_a z^a + \cdots,$$

studiert. Bedeutet $F^{(n)}(z)$ die n. Iteration von $F(z)$ mit sich selbst, so ist

$$F^{(n)}(z) = z + \sum_{a=2}^{\infty} \left\{ \binom{n}{1} A_{a,1} + \binom{n}{2} A_{a,2} + \cdots + \binom{n}{n} A_{a,n} \right\} z^a,$$

wo die $A_{i,k}$ ganze rationale Funktionen der α sind mit ganzen rationalen Koeffizienten. Für die $A_{i,k}$ gelten Recursionsformeln. Ich beweise im folgenden den Satz:

Satz: Ist l^i die Potenz einer Primzahl l, so ist der Koeffizient von z^a in $F^{(l^i)}(z)$ eine ganze rationale Funktion der α mit durch l teilbaren ganzen rationalen Zahlkoeffizienten, wenn

$$2 \leqq a \leqq l^i + l^{i-1} + l^{i-2} + \cdots + l + 1.$$

Zum Beispiel ist für $l^i = 3$:

$$F^{(3)}(z) = z + 3\alpha_1 z^2 + 3(\alpha_2 + 2\alpha_1^2) z^3 + 3(\alpha_1 + 5\alpha_1\alpha_2 + 3\alpha_1^3) z^4 + \cdots,$$

also der Koeffizient von $z^2, z^3, z^4 = z^{3+1}$ durch 3 teilbar.

Beweis: Da $\binom{l^i}{k}$, $0 < k < l^i$, durch l teilbar ist, hat man nur zu beweisen, dass die Koeffizienten in A_{a,l^i} für die angegebenen a durch l teilbar sind.

Ferner ergibt sich $A_{a,l^i} = 0$, wenn $a \leqq l^i$ ist.[1]) Es bleiben nur die Fälle:

$$l^i < a \leqq l^i + l^{i-1} + l^{i-2} + \cdots l + 1$$

übrig. Nach Schröder[2]) ist:

$$A_{a,l^i} = \sum_{(a)} F_a^{(a_1)} F_{a_1}^{(a_2)} \cdots F_{a_{l^i-2}}^{(a_{l^i-1})} F_{a_{l^i-1}}^{(1)},$$

wo die Summation über alle Kombinationen $a_1, a_2, \ldots a_{l^i-1}$ der Elemente $2, 3, \ldots a-1$ zur (l^i-1)-Klasse ohne Wiederholung zu erstrecken ist. Ausserdem ist:

$F_{a_{k-1}}^{(a_k)} = 0$, wenn $a_{k-1} < a_k$,

$F_{a_{k-1}}^{(a_k)}$ der Koeffizient von $z^{a_{k-1}}$ in $(z + \alpha_2 z^2 + \alpha_3 z^3 + \cdots)^{a_k}$, wenn $a_{k-1} > a_k$.

Bei der Summation zur Bildung von A_{a,l^i} darf deshalb

$$a > a_1 > a_2 > \cdots > a_{l^i-1}$$

vorausgesetzt werden.

a) Wenn $a_k \equiv 0 \pmod{l}$, $a_{k-1} \not\equiv 0 \pmod{l}$ ist, so werden alle Koeffizienten in $F_{a_{k-1}}^{(a_k)}$ durch l teilbar oder

$$F_{a_{k-1}}^{(a_k)} \equiv 0 \pmod{l}.$$

Denn die Koeffizienten von $F_{a_{k-1}}^{(a_k)}$ sind Polynomialkoeffizienten:

$$P = \frac{a_k!}{\nu_1!\, \nu_2! \ldots \nu_h!}, \text{ wo } \begin{cases} \nu_1 + \nu_2 + \cdots + \nu_h = a_k \\ \nu_1 + 2\nu_2 + \cdots + h\nu_h = a_{k-1} \end{cases}$$

Da a_k durch l teilbar ist, so sind alle P durch l teilbar, ausser wenn sämtliche $\nu_1, \nu_2, \ldots \nu_h$ durch l teilbar sind[3]). Dies ist unmöglich, da a_{k-1} zu l teilerfremd ist.

b) Ist a eine Zahl, die der Bedingung

$$l^i < a < l^i + l^{i-1} + \cdots l$$

genügt, so ist $a < 2l^i$. Setzt man $a = l^i + a'$, so kann man a' eindeutig nach Potenzen von l entwickeln:

$a' = q_1 l^{i-1} + q_2 l^{i-2} + \cdots + q_{i-1} l + q_i$, wo $0 \leqq q_h < l, h = 1, 2, \ldots i$.

[1]) Schröder, a. a. O. pag. 313, Gleichung (38a).

[2]) Schröder, a. a. O. pag. 314.

[3]) Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, 4. Aufl. 1894, pag. 28 u. ff.

Ist q_r das erste von 1 verschiedene q, so muss $q_r = 0$ sein. Denn für $q_r \geqq 2$ wäre:

$$a = l^i + a' = l^i + l^{i-1} + \cdots + l^{i-r+1} + q_r l^{i-r} + \cdots \geqq l^i + l^{i-1} + \cdots + l^{i-r+1} + 2\,l^{i-r} > l^i + l^{i-1} + \cdots + l^{i-r} + l^{i-r-1} + \cdots + l + 1$$

gegen Annahme. Also hat a die Form:

$$a = l^i + l^{i-1} + \cdots + l^{i-r+1} + q_{r+1} l^{i-r-1} + \cdots + q_i \begin{Bmatrix} 0 < r < i \\ 0 \leqq q < l \end{Bmatrix}.$$

Die Anzahl M der Zahlen $\leqq a$, die durch l teilbar sind, ist daher:

$$M = l^{i-1} + l^{i-2} + \cdots + l^{i-r} + q_{r+1} l^{i-r-2} + \cdots + q_{i-1} \leqq l^{i-1} + l^{i-2} + \cdots + l + 1,$$
$$M < l^i - 1.$$

Die Anzahl N der Zahlen $\leqq a$, die zu l teilerfremd sind, ist:

$$N = (l^i - l^{i-1}) + (l^{i-1} - l^{i-2}) + \cdots + (l^{i-r+1} - l^{i-r}) + q_{r+1}(l^{i-r-1} - l^{i-r-2}) + \cdots + q_{i-1}(l-1) + q_i = l^i - l^{i-r} + q_{r+1}(l^{i-r-1} - l^{i-r-2}) + \cdots + q_{i-1}(l-1) + q_i. \qquad (0 \leqq q < l).$$

Wenn a zu l teilerfremd ist, so ist $q_i > 0$ und

$$N \leqq l^i - l^{i-r} + l^{i-r-1}(l-1) = l^i - l^{i-r-1}.$$
$$N \leqq l^i - 1.$$

Unter den N zu l teilerfremden Zahlen tritt auch a selbst auf. Sieht man von dieser Zahl ab, so bleiben die zu l teilerfremden Zahlen $< a$ übrig; ihre Anzahl ist daher $< l^i - 1$, falls:

$$l^i < a < l^i + l^{i-1} + \cdots + l.$$

Wenn a durch l teilbar ist, so ist $q_i = 0$ und

$$N \leqq l^i - l^{i-r} + (l-1)(l^{i-r-1} - 1) = l^i - l^{i-r-1} - l + 1$$
$$N \leqq l^i - l.$$

Die Anzahl aller zu l teilerfremden Zahlen $< a$, wo a durch l teilbar ist, ist höchstens gleich $l^i - l$, falls

$$l^i < a < l^i + l^{i-1} + \cdots + l.$$

c) Greifen wir aber irgendeinen Summanden aus

$$A_{a,\,l^i} = \sum_{(a)} F_a^{(a_1)} F_{a_1}^{(a_2)} \cdots F_{a_{l^i-1}}^{(1)},\ l^i + \cdots + l > a > a_1 > \cdots > a_{l^i-1} > 1$$

heraus, so sehen wir, dass nicht alle a_k zu l teilerfremd sein können; denn unter den Zahlen $2, 3, \cdots a-1$ gibt es nach dem Resultat unter

b) höchstens $l^i - 2$ zu l teilerfremde Zahlen. Ebensowenig können alle durch l teilbar sein, da ja $M < l^i - 1$. Also muss wenigstens einmal auf ein zu l teilerfremdes a_{k-1} ein durch l teilbares a_k treten oder umgekehrt. Im ersten Fall, und dieser tritt immer ein, wenn a zu l teilerfremd ist, ist nach a) $F_{a_{k-1}}^{(a_k)} \equiv 0 \pmod{l}$. Der zugehörige Summand von A_{a,l^i} hat durch l teilbare Koeffizienten. Im zweiten Fall ist $a, a_1, \ldots a_{k-1}$ durch l teilbar, a_k zu l teilerfremd. Dann muss es ein a_{k_1}, $k_1 > k$ geben, das durch l teilbar ist. Denn es gibt höchstens $l^i - l$ zu l teilerfremde Zahlen $< a$, und höchstens $l^i - l - (k-1)(l-1) - 1$ zu l teilerfremde Zahlen, die $< a_k$ sind, und es ist $l^i + 1 - k > (l^i - l) - (k-1)(l-1) - 1$. Damit ist bewiesen, dass in jedem Summand von A_{a,l^i} ein $F_{a_{k-1}}^{(a_k)}$ auftritt, in dem $a_{k-1} \not\equiv 0$, $a_k \equiv 0 \pmod{l}$ ist. Alle Koeffizienten von A_{a,l^i} sind daher durch l teilbar nach a) und der Satz ist bewiesen.

d) Im Fall $a = l^i + l^{i-1} + \cdots + l$ ist $a \equiv 0 \pmod{l}$, $N = l^i - 1$; im Fall $a = l^i + l^{i+1} + \cdots + l + 1$ ist $a \not\equiv 0 \pmod{l}$, $N = l^i$, und es gibt $l^i - 2$ Zahlen zwischen 1 und a mit Ausschluss der Grenzen, die zu l teilerfremd sind. Also muss auch jetzt in A_{a,l^i} ein $F_{a_{k-1}}^{(a_k)}$ auftreten, für das $a_{k-1} \equiv 0 \pmod{l}$, $a \not\equiv 0 \pmod{l}$ ist.

II.

Der unter I. bewiesene Satz leistet gute Dienste bei der Betrachtung der höheren Verzweigungskörper einer Primzahl l, die im Grad und der Discriminante eines Körpers auftritt.[1]) Um dies zu zeigen, seien folgende vereinfachte Annahmen gemacht: Gegeben ein Grundkörper k und in demselben eine zyklische Gleichung $m = l^n$ten Grades:

$$m = l^n : x^m - v_1 x^{m-1} + v_2 x^{m-2} - \cdots + (-1)^l v_m = 0$$

($v_1, v_2, \cdots v_m$ Zahlen von k), deren Wurzeln den Körper K festlegen sollen. Die Wurzeln der Gleichung seien durch

$$\xi, s\xi, s^2\xi, \cdots s^{m-1}\xi$$

gegeben, wo $s^m = e$ die Einheitssubstitution ergebe. Ist $\mathfrak{l}$ ein in (l) enthaltenes Primideal von k, so werde $\mathfrak{l}$ in K die m-Potenz eines Ideals $\mathfrak{L}$

$$\mathfrak{l} = \mathfrak{L}^m.$$

---

[1]) Siehe Hilbert, Die Theorie der alg. Zahlkörper. Berlin 1897, pag. 254 u. ff. Weber, Algebra II. Bd. Braunschweig 1899, pag. 664 u. ff.

Ist λ irgendeine Zahl von K, deren Zähler durch $\mathfrak{L}$, nicht aber durch $\mathfrak{L}^2$ teilbar, deren Nenner aber zu $\mathfrak{L}$ teilerfremd sei, so ist, da s Substitution der Verzweigungsgruppe von $\mathfrak{l}$ ist:

$$s\lambda \equiv \lambda \pmod{\mathfrak{L}^2} \text{ und}$$
$$s\lambda \equiv \lambda + \alpha_2\lambda^2 \pmod{\mathfrak{L}^3},$$

wo α_2 eine Zahl von k ist, deren Nenner zu $\mathfrak{l}$ teilerfremd ist; denn jede Zahl von K ist (mod $\mathfrak{L}$) einer Zahl von k kongruent. Fährt man so fort, so wird

$$s\lambda \equiv \lambda + \alpha_2\lambda^2 + \alpha_3\lambda^3 + \cdots + \alpha_h\lambda^h \pmod{\mathfrak{L}^{h+1}},$$

wo h eine beliebig grosse Zahl ist. Aus dem in I. erhaltenen Satz folgt dann, da $s\mathfrak{L} = \mathfrak{L}$:

$$s^{l^i}\lambda \equiv \lambda + l\left(\beta_2\lambda^2 + \beta_3\lambda^3 + \cdots + \beta_{l^i + l^{i-1} + \cdots + l + 1}\lambda^{l^i + l^{i-1} + \cdots + l + 1}\right) \pmod{\mathfrak{L}^{l^i + \cdots + l + 2}}.$$

i ist hier irgendeine Zahl $< n$. Da

$$l^n > l^{n-1} + l^{n-2} + \cdots + l + 1;\ l \equiv 0 \pmod{\mathfrak{L}^{l^n}},$$

so folgt aus obigem[2]):

$$s^{l^i}\lambda \equiv \lambda \pmod{\mathfrak{L}^{l^i + l^{i-1} + \cdots + l + 2}},\ i = 1, 2, \cdots n-1. \qquad (1).$$

Bei Einführung symbolischer Potenzen lässt sich diese Kongruenz so schreiben:

$$\lambda^{1 - s^{l^i}} \equiv 1 \pmod{\mathfrak{L}^{l^i + l^{i-1} + \cdots + l + 1}},$$

woraus durch Potenzieren:

$$\lambda^{h(1 - s^{l^i})} \equiv 1 \pmod{\mathfrak{L}^{l^i + l^{i-1} + \cdots + l + 1}};\ s^{l^i}\lambda^h \equiv \lambda^h \pmod{\mathfrak{L}^{l^i + l^{i-1} + \cdots + l + h + 1}}$$

Ist A eine beliebige Zahl von K, deren Nenner zu $\mathfrak{L}$ teilerfremd ist, so ist auch jetzt:

$$A \equiv \gamma_0 + \gamma_1\lambda + \gamma_2\lambda^2 + \cdots + \gamma_h\lambda^h \pmod{\mathfrak{L}^{h+1}} \quad (\gamma_i \text{ Zahlen von } k)$$
$$s^{l^i}A - A \equiv \gamma_1(s^{l^i}\lambda - \lambda) + \gamma_2(s^{l^i}\lambda^2 - \lambda^2) + \cdots + \gamma_h(s^{l^i}\lambda^h - \lambda^h) \pmod{\mathfrak{L}^{h+1}}$$

oder wegen oben:

$$s^{l^i}A \equiv A \pmod{\mathfrak{L}^{l^i + l^{i-1} + \cdots + l + 2}}. \qquad (2).$$

[2]) Vergl. Math. Annalen, Bd. 75 (1914), pag. 195. II. Hilfsatz.

Hieraus erkennt man, wie der Körper K im allgemeinen n überstrichene Verzweigungskörper bildet, von denen jeder den Relativgrad l zum vorhergehenden hat. Zugleich ergibt sich der Satz:

Satz: Ist K ein relativ-cyklischer Körper zu k vom Relativgrad l^n und wird ein Primideal $\mathfrak{l}$ von (l) in k die $l^{n\text{te}}$ Potenz eines Primideals in K, so ist die Relativdiscriminante von K in bezug auf k teilbar durch:

$$\mathfrak{l}^{nl^n+(l-2)(l^{n-1}+l^{n-2}+\cdots+l+1)}.$$

Denn die Relativdifferente von A lässt sich so schreiben:

$$\delta(A)=\prod_{h=1}^{l^n-1}(A-s^hA)=\prod_{i=0}^{n-1}\prod_{h=1}^{l^n-l^i}{}'(A-s^{hl^i}A),$$

wo das innere Produkt nur über diejenigen h zu erstrecken ist, die zu l teilerfremd sind. Solcher Zahlen gibt es aber $\varphi(l^{n-i})=l^{n-i-1}(l-1)$. Also ist das innere Produkt durch

$$\mathfrak{L}^{l^{n-i-1}(l-1)(l^i+l^{i-1}+\cdots+l+2)}=\mathfrak{L}^{l^n+(l-2)l^{n-i-1}}$$

teilbar, und $\delta(A)$ durch:

$$\mathfrak{L}^{\sum_{i=0}^{n-1}(l^n+(l-2)l^{n-i-1})}=\mathfrak{L}^{nl^n+(l-2)(l^{n-1}+l^{n-2}+\cdots+l+1)}.$$

Die Relativdiscriminante ist aber die Relativnorm der Differente bezüglich k, w. z. b. w.

Wenn $\mathfrak{l}$ zur Discriminante des Körpers k teilerfremd ist, so lässt sich leicht zeigen, dass die Kongruenz (1) für keine höhere Potenz von $\mathfrak{L}$ erfüllt sein kann. Die im Satz enthaltene Potenz ist dann auch die höchste in der Relativdiscriminante enthaltene Potenz von $\mathfrak{l}$. Dies tritt zum Beispiel ein, wenn k der Körper der rationalen Zahlen und K Unterkörper der l^n-Einheitswurzel ist.

Zürich, den 18. Januar 1917.