Theodor Schneider

Rationale Punkte über eine algebraische Kurve (points rationnels sur une courbe algébrique)

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 15, nº 1 (1973-1974), exp. nº 20, p. 1-7

<http://www.numdam.org/item?id=SDPP_1973-1974__15_1_A16_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
15e année, 1973/74, n° 20, 7 p.

29 avril 1974

RATIONALE PUNKTE ÜBER EINE ALGEBRAISCHE KURVE
[POINTS RATIONNELS SUR UNE COURBE ALGÉBRIQUE]

von Theodor SCHNEIDER
[Freiburg i. Br.]

Ich beginne mit einem Resultat von C. L. SIEGEL [2]. Er hat dort mit der Methode, die die schönen Transzendenzresultate der Werte der Besselfunktionen lieferte, angewandt auf G-Funktionen, gezeigt : Sei y eine algebraische Funktion von x, in deren Gleichung die Koeffizienten algebraische Zahlen sind. Es sei $x = 0$ ein regulärer Punkt der Funktion. Das Abelsche Integral $\int_0^x y\,dt$ sei keine algebraische Funktion.

Es genüge $\xi \neq 0$ einer algebraischen Gleichung ℓ-ten Grades, deren Koeffizienten ganz rational und absolut $\leq M$ sind. Es sei ε irgendeine positive Zahl, und

$$|\xi| < c \exp(-(\log M)^{\frac{1}{2}+\varepsilon} ,$$

wo c nur von ℓ und ε abhängt. Dann genügt die Zahl $\int_0^\xi y\,dt$ keiner algebraischen Gleichung ℓ-ten Grades mit rationalen Koeffizienten. Die Siegelsche Methode gestattet aber nicht, algebraische Funktionen zu behandeln.

Wenn auch das Resultat, das ich nun für algebraische Funktionen angebe, mit dem Siegelschen eine gewisse Ähnlichkeit aufweist, so ist zum Beweis doch ein neuer Weg erforderlich. Ich zeige den folgenden Satz.

SATZ. - Sei $f(z)$ algebraisch in z vom Grade q über dem Körper der rationalen Zahlen. Sei $f(z)$ um $z = 0$ regulär. Es sei ferner r/s der gekürzte Bruch mit ganzrationalen r, s und $s > 0$. Die Werte von $f(z)$ bei $z = 0$ und bei $z = r/s$ seien ebenfalls rationale Zahlen. Für irgendein $\varepsilon > 0$ existiert ein s_0, das nur von ε und f abhängt, so dass für $s > s_0$ die Abschätzung

$$(1) \qquad \left|\frac{r}{s}\right| > s^{-((1/q)+\varepsilon)}$$

gilt.

Bemerkungen :

1° Es ist leicht zu sehen, dass das Resultat bezüglich des Exponenten scharf ist. Dies zeigt das folgende Beispiel :

Sei $f(z) = (1 - z)^{1/q} = y$; so ist $z = 1 - y^q$ und $y = (S - 1)/S$ liefert $z = 1 - (1 - (1/S))^q$ und diese Zahlen sind rational für $S \in N$. Andererseits ist $|x| = 0\ (S^{-1})$ und mit der Bezeichnung $x = r/s$ folgt

$$s = S^q \text{ und } |x| = 0\ (s^{-(1/q)}) .$$

2° Sei α algebraisch vom Grade k, und $f(\alpha) = 0$, $f(r/s) = u/v$ rational, so folgt

$$|\alpha - \frac{r}{s}| > s^{-((k/q)+\varepsilon)}$$

und wenn $f(r/s) = \beta$ algebraisch vom Grade ℓ, zeigt man

$$|\alpha - \frac{r}{s}| > s^{-((k\ell/q)+\varepsilon)} .$$

3° Einer p-adischen Übertragung des Satzes im Ridoutschen Sinne steht die Schwierigkeit entgegen, dass die p-adische Funktion $f(x)$ p-adisch für rationales $x = r/s$ im allgemeinen nicht mehr einen rationalen Zahlenwert annimmt, wenn die Funktion $f(z)$ bei gewöhnlicher Bewertung für $z = r/s$ rational ist.

4° Man kann die folgende Methode auch auf den von Siegel untersuchten Fall, wo $f(z)$ keine algebraische Funktion, sondern das Integral einer algebraischen Funktion ist, anwenden.

Ich kann aber nicht das Siegelsche Resultat zeigen, sondern nur die schwächere Abschätzung

$$|\xi| < c \exp(-(\log M)^{\frac{2}{3}} + \varepsilon)$$

für die sonst gleiche Aussage erhalten.

Beweis : Wir bilden mit $f(z)$ eine Funktion

$$\Phi(z) = \sum_{i=0,k=0}^{p-1,q-1} c_{ik}\, z^i\, f(x)^k$$

mit einem geeigneten p und nicht sämtlich verschwindenden ganzrationalen c_{ik} und beweisen unter den Voraussetzungen des Satzes und unter Annahme der Negation von (1), d. h.

$$|\frac{r}{s}| \leq s^{-((1/q)+\varepsilon)} ,$$

dass $\Phi(z)$ identisch verschwindet, woraus folgt, dass $f(z)$ eine algebraische Funktion höchstens $(q - 1)$-ten Grades ist im Widerspruch zur Voraussetzung, dass es eine Funktion sei, die vom q-ten Grade algebraisch sein soll. Aus diesem Widerspruch folgt die Richtigkeit von (1) und damit der Satz.

1° Wir wollen uns zunächst über die Koeffizienten c_{ik} die notwendigen Aussagen verschaffen und dann über eine Induktion das identische Verschwinden einer geeigneten Interpolationsreihe von $\Phi(z)$ beweisen.

Die Koeffizienten c_{ik} mögen unter Annahme einer ganzen Zahl p, die später noch geeignet gewählt werden soll, allein durch die Forderung, dass $\Phi(r/s) = 0$ sein soll, bestimmt werden. Bestimmt heisst, dass wir mittels des Schubfachschlusses die Existenz für unsere Zwecke geeigneter, nicht sämtlich verschwindender, ganzrationaler c_{ik} nachweisen. Dabei wird die Negation von (1) noch nicht benutzt. Es sei die rationale Zahl $f(r/s)$ mit u/v bezeichnet. Dabei besteht eine Abhängigkeit der Grössenordnung von v von denjenigen von s, derart, dass mit von s unabhängigem γ gilt

$$(2) \qquad |v| < s^{\gamma}$$

(siehe hierzu die Arbeit [1]). Die Bedingung

$$\Phi(\frac{r}{s}) = \sum_{i=0,k=0}^{p-1,q-1} c_{ik}(\frac{r}{s})^{i} (\frac{u}{v})^{k} = 0$$

liefert demnach eine einzige lineare homogene Gleichung für die c_{ik} mit rationalen Koeffizienten. Durch Multiplikation der Gleichung mit $s^{p-1} \cdot v^{q-1}$ wird daraus eine solche mit ganzrationalen Koeffizienten, die unter Beachtung von (2) dem Betrag nach kleiner als

$$O((\max(1,r,s))^{p-1} \cdot (\max(1,u,v)^{q-1})) = O(s^{p-1}\, v^{q-1}) = O(s^{p-1+\gamma(q-1)})$$

sind. Damit ist die Gleichung, wie mittels des Schubfachschlusses zu sehen ist, lösbar in nicht sämtlichen verschwindenden, ganzrationalen c_{ik}, für die gilt

$$(3) \qquad |c_{ik}| < O(s^{(p-1+\gamma(q-1))1/(pq-1)}) = O(s^{(1/q)+\varepsilon_1})$$

für $\varepsilon_1 > 0$ und $p > p_0(\varepsilon_1)$.

2° Nun soll unter der Annahme $|r/s| \leq s^{-((1/q)+\varepsilon)}$ und der Wahl von ε_1 mit $\varepsilon_1 < \varepsilon$ gezeigt werden, dass $\Phi(z)$ identisch verschwindet. Daraus folgt, dass $f(z)$ eine algebraische Funktion niederer als q-ten Grades ist im Widerspruch zur Voraussetzung, und aus diesem Widerspruch folgt der Satz.

Das identische Verschwinden von $\Phi(z)$ sehen wir aus dem Verschwinden einer Interpolationsreihe für $\Phi(z)$ und zwar aus einer Interpolationsreihe, deren sämtliche Koeffizienten verschwinden.

Wir interpolieren $\Phi(z)$ an den Stellen $\zeta_0, \zeta_1, \zeta_2, \dots, \zeta_n, \dots$. Dabei sei mit einer noch später zu fixierenden natürlichen Zahl m

$$\zeta_0=\zeta_m=\zeta_{2m}=\dots=\frac{r}{s} \text{ und } \zeta_n = 0 \text{ für alle Indizes } n \neq jm, \quad j = 0,1,\dots .$$

Gleiche Werte von ζ_n bedeuten dabei Interpolation von entsprechend höherer Ordnung.

Wir zeigen $\Phi^{(\nu)}(0) = 0$ und $\Phi^{(\nu)}(\frac{r}{s}) = 0$ für alle $\nu = 0, 1, 2, \dots,$ woraus das Verschwinden sämtlicher Koeffizienten der genannten Interpolationsreihe von $\Phi(z)$ folgt. Wir haben $\Phi(z)$ so gewählt, dass $\Phi(\frac{r}{s})$ verschwindet.

Als nächstes zeigen wir $\Phi^{(\mu)}(0) = 0$ für $\mu = 0, 1, \dots, m-2$. Es ist

$$\frac{\Phi^{(\mu)}(0)}{\mu!} = \frac{1}{\mu!} \sum_{i=0,k=0}^{p-1,q-1} c_{ik}\Big(\sum_{\eta=0}^{\mu} \binom{\mu}{\eta} \frac{d^{\eta}(z^{i})}{dz^{\eta}}\Big|_{z=0} \frac{d^{\mu-\eta} f^{k}(z)}{dz^{\mu-\eta}}\Big|_{z=0}\Big)$$

$$= \sum_{i=0,k=0}^{p-1,q-1} c_{ik}\Big(\sum_{\eta=0}^{\mu} \frac{1}{\eta!} \frac{d^{\eta}(z^{i})}{dz^{\eta}}\Big|_{z=0} \frac{1}{(\mu-\eta)!} \frac{d^{\mu-\eta} f^{k}(z)}{dz^{\mu-\eta}}\Big|_{z=0}\Big) .$$

Dabei ist

$$\frac{1}{\eta!} \frac{d^{\eta} z^{i}}{dz^{\eta}}\Big|_{z=0} = \begin{cases} 0 & \text{für } \eta \neq i \\ 1 & \phantom{\text{für }} \eta = i \end{cases}$$

und wegen des Eisensteinschen Satzes für algebraische Funktionen existiert eine ganzrationale Zahl v_0 derart, dass

$$\frac{1}{(\mu-\eta)!}\left.\frac{d^{\mu-\eta} f^k(z)}{dz^{\mu-\eta}}\right|_{z=0} v_0^{\mu-\eta+k}$$

ganzrational ist. (Siehe die zitierte Arbeit [1].) Somit ist

$$\frac{1}{\mu}\,\Phi^{(\mu)}(0)\; v_0^{\mu+q-1}$$

ganzrational, also, falls $\Phi^{(\mu)}(0)$ nicht Null ist,

$$\left|\frac{1}{\mu!}\,\Phi^{(\mu)}\; v_0^{\mu+q-1}\right| \geq 1$$

oder

$$\left|\frac{\Phi^{(\mu)}(0)}{\mu!}\right| \geq v_0^{-(\mu+q-1)} . \tag{4}$$

Zur Abschätzung der linken Seite nach oben wird die Cauchysche Integralformel herangezogen. Es ist wegen $\Phi(r/s) = 0$, integriert über einen Kreis $|z| = \rho > 0$, der r/s umschliesst,

$$\frac{1}{2\pi i}\int_{|z|=\rho}\frac{\Phi(z)\,dz}{(z-r/s)z^{\mu+1}} = \frac{1}{\mu!}\left.\left(\frac{\Phi(z)}{z-r/z}\right)^{(\mu)}\right|_{z=0}$$

und unter der Voraussetzung $\Phi(0) = \Phi'(0) = \ldots\ \Phi^{(\mu-1)}(0) = 0$ folgt daraus

$$\frac{1}{2\pi i}\int_{|z|=\rho}\frac{\Phi(z)\,dz}{(z-r/s)z^{\mu+1}} = \frac{1}{\mu!}\,\Phi^{(\mu)}(0)\,\frac{1}{(-r/s)} . \tag{5}$$

Die Annahme, dass $|z| = \rho$ für festes $\rho \neq 0$ die Stelle r/s umschliesst, folgt aus $|r/s| \leq s^{-((1/q)+\varepsilon)}$ für genügend grosses s, also $s > s_1$.

Die Annahme $\Phi(0) = \ldots = \Phi^{(\mu-1)}(0) = 0$ sei als Induktionsannahme aufgefasst. Aus (5) folgt

$$\left|\frac{\Phi^{(\mu)}(0)}{\mu!}\right|\frac{1}{|r/s|} \leq \frac{1}{2\pi}\,2\pi\rho\,\max_{|z|=\rho}\left|\frac{\Phi(z)}{(z-r/s)z^{\mu+1}}\right| .$$

Die Abschätzung von $|\Phi(z)|$ ergibt $s^{(1/q)+\varepsilon_1} c_1^{p+q}$ mit einem von s unabhängigen c_1, so dass wir

$$\left.\left|\frac{\Phi(z)}{(z-r/s)z^{\mu+1}}\right|\right|_{|z|=\rho} < s^{(1/q)+\varepsilon_1} c_2^{p+q+m}$$

und damit

$$\left|\frac{\Phi^{(\mu)}(0)}{\mu!}\right| < |r/s|\; s^{(1/q)+\varepsilon_1} c_2^{p+q+m} \leq s^{-((1/q)+\varepsilon)+((1/q)+\varepsilon_1)} c_2^{p+q+m}$$
$$< v_0^{-(\mu+q-1)}$$

erhalten für $\varepsilon_1 < \varepsilon$ und genügend grosses s bei festem p und m, da auch v_0 von s unabhängig ist. Daraus folgt, zusammen mit (4), dass $\Phi^{(\mu)}(0)$ verschwindet für $\mu \leq (m-1) - 1$. Also verschwindet $\Phi^{(\mu)}(0)$ für alle $\mu = 0, 1, \ldots, m-2$ bei von s unabhängigem m. Nachdem wir so $\Phi(r/s) = \Phi^{(\mu)}(0) = 0$ für $\mu = 0, 1, \ldots, m-2$ erreicht haben, wenden wir für die Untersuchung der höheren Ableitungen von $\Phi(z)$ an den beiden Stellen r/s und 0 Induktion an und zwar müssen wir offenbar folgendermassen vorgehen : Wir haben zwei Induktionsschlüsse durchzuführen, erstens haben wir unter der Voraussetzung des Verschwindens von $\Phi^{(\iota)}(r/s)$ für $\iota = 0 , \ldots , j-1$ und $\Phi^{(\iota)}(0)$ für

$$\iota = 0 , \ldots , j(m-1)-1$$

das Verschwinden von $\Phi^{(j)}(r/s)$ zu zeigen und zweitens soll unter der Voraussetzung des Verschwindens von $\Phi^{(\iota)}(r/s)$ für $\iota = 0 , \ldots , j$ und des Verschwindens von $\Phi^{(\iota)}(0)$ für $\iota = 0 , \ldots , j(m-1)-1$ das Verschwinden von $\Phi^{(\iota)}(0)$ für $\iota = j(m-1) , \ldots , (j+1)(m-1)-1$ nachgewiesen werden. Ist dies gezeigt, so verschwindet mit den bereits gezeigten Anfangsbedingungen $\Phi(z)$ mittels vollständiger Induktion sowohl an der Stelle $z = 0$ wie bei $z = r/s$ von beliebig hoher Ordnung, und damit sind wir offenbar mit unserem Beweis fertig. Es sind also noch die beiden Induktionsschlüsse auszuführen.

Wir beweisen zuerst das Verschwinden von $\Phi^{(j)}(r/s)$ unter der Annahme des Verschwindens von $\Phi^{(\iota)}(r/s)$ für alle $\iota < j$ und des Verschwindens von $\Phi^{(\iota)}(0)$ für $\iota < j(m-1)$.

Es ist $1/j!\ \Phi^{(j)}(r/s).s^{p-1}.v^{q-1+j}$ ganzrational, also unter der Annahme

$$\Phi^{(j)}(r/s) \neq 0$$

$$\left|\frac{1}{j!}\ \Phi^{(j)}(r/s).s^{p-1}.v^{q-1+j}\right| \geq 1$$

und wegen $|v| < s^{\gamma}$ erst recht

$$\left|\frac{1}{j!}\ \Phi^{(j)}(r/s)\ s^{p-1+\gamma(q-1+j)}\right| \geq 1$$

oder

$$(6) \qquad \left|\frac{1}{j!}\ \Phi^{(j)}(r/s)\right| \geq s^{-(p-1+\gamma(q-1+j))} .$$

Nun ziehen wir die Cauchysche Formel heran und erhalten unter den genannten Annahmen

$$\frac{1}{2\pi i}\int_{|z|=\rho} \frac{\Phi(z)\ dz}{(z-r/s)^{j+1}\ z^{j(m-1)}} = \frac{1}{j!}\ \Phi^{(j)}(r/s).(r/s)^{-j(m-1)}$$

und daraus durch Abschätzung des Integrals

$$\left|\frac{1}{j!}\ \Phi^{(j)}\left(\frac{r}{s}\right)\right| < \left|\frac{r}{s}\right|^{j(m-1)}.\frac{1}{2\pi}.2\pi\rho\ \max_{|z|=\rho}\left|\frac{\Phi(z)}{(z-r/s)^{j+1}\ z^{j(m-1)}}\right|$$

$$< \left|\frac{r}{s}\right|^{j(m-1)}.s^{(1/q)+\varepsilon_1}.c_3^{p+q+jm}$$

mit von s unabhängigem c_3 . Hieraus folgt zusammen mit (6) und mit

$$|r/s| \leq s^{-((1/q)+\varepsilon)}$$

$$s^{-((p-1)+\gamma(q-1+j))} < s^{-((1/q)+\varepsilon)j(m-1)}.s^{(1/q)+\varepsilon_1}\ c_3^{p+q+jm}$$

oder

$$s^{((1/q)+\varepsilon)j(m-1)-((p-1)+\gamma(q-1+j))-((1/q)+\varepsilon_1)} < c_3^{p+q+jm} .$$

Wir erhalten aber für genügend grosses m , gennant $m = m_0$

(7) $$((1/q) + \varepsilon)j(m - 1) > (p - 1) + \gamma(q - 1 + j) + (1/q) + \varepsilon_1$$

für alle $j \geq 1$, und offenbar ist (6) für ein solches m_0 und für alle $m > m_0$ und alle $j \geq 1$ mit genügend grossem s unmöglich, und aus diesem Widerspruch folgt $\Phi^{(j)}(r/s) = 0$. Schliesslich haben wir noch den zweiten Induktionsabschluss zu zeigen, nämlich dass unter der Annahme des Verschwindens von $\Phi^{(\iota)}(r/s)$ für $\iota = 0 , 1 , \ldots , j - 1$ und des Verschwindens von $\Phi^{(\iota)}(0)$ für

$$\iota = (j - 1)(m - 1) , \ldots , j(m - 1) - 1$$

bewiesen wird.

Nach (4) ist

(8) $$\left|\frac{\Phi^{(\iota)}(0)}{\iota!}\right| \geq v_0^{-(\iota+q-1)} ,$$

falls nur $\Phi^{(\iota)}(0) \neq 0$ angenommen wird. Unter der weiteren Induktionsvoraussetzung

$$\Phi^{(\mu)} = 0 \quad \text{für} \quad \mu = (j - 1)(m - 1) - 1 , \ (j - 1)(m - 1) , \ldots , (\iota - 1)$$

folgt analog (5) dann

$$\frac{1}{2\pi i}\int_{|z|=\rho} \frac{\Phi(z)\ dz}{(z - r/s)^j\ (z)^{\iota+1}} = \frac{1}{\iota!}\ \Phi^{(\iota)}(0)\ \frac{1}{(-r/s)^j}$$

und daraus

$$\left|\frac{\Phi^{(\iota)}(0)}{\iota!}\right| \leq |r/s|^j . \rho \max_{|z|=\rho} \left|\frac{\Phi(z)}{(z - r/s)^j\ z^{\iota+1}}\right| .$$

Mit

$$\left.\left|\frac{\Phi(z)}{(z - r/s)^j\ z^{\iota+1}}\right|\right|_{|z|=\rho} < s^{(1/q)+\varepsilon_1} . c_3^{p+q+\iota}$$

folgt so

$$|\Phi^{(\iota)}(0)| < \left|\frac{r}{s}\right|^j s^{(1/q)+\varepsilon_1}\ c_3^{p+q+\iota} \leq s^{-j((1/q)+\varepsilon)+(1/q)+\varepsilon_1}\ c_3^{p+q+\iota} .$$

und zusammen mit (8) ergibt dies

$$v_0^{-(\iota+q-1)} < s^{-j((1/q)+\varepsilon)+(1/q)+\varepsilon_1}\ c_3^{p+q+\iota} .$$

Bei $j \geq 2$, was nach dem ersten Induktionsschluss angenommen werden darf (es genügte sogar $j \geq 1$) und ι in dem fraglichen Invervall $(j-1)(m-1) \leq \iota \leq j(m-1)-1$ ergibt sich so eine nur von p , c_3 abhängige, von m sogar unabhängige Zahl s_0 , derart dass (9) für $s > s_0$ unmöglich wird, und damit ist auch der zweite Induktionsschluss bewiesen.

Wähle also zu ε ein $\varepsilon_1 > 0$ und $\varepsilon > \varepsilon_1$, z. B. $\varepsilon_1 = \frac{\varepsilon}{2}$, dann p genügend gross, nun m genügend gross, und zu diesen Werten von p und m schliesslich s genügend gross, so folgt der behauptete Satz.

BIBLIOGRAPHIE

[1] SCHNEIDER (Theodor). - Zur Charakterisierung algebraischer Funktionen mit Hilfe des Eisensteinischen Satzes, Math. Z., t. 60, 1954, p. 98-108.

[2] SIEGEL (Carl Ludwig). - Über einige Anwendungen diophantischer Approximationen, Abh. preuss. Akad. Wiss., Berlin, 1929, n° 1, 71 p.

(Texte reçu en juillet 1974)

Theodor SCHNEIDER
Mathematisches Institut
der Albert-Ludwigs-Universität
40 Hebelstrasse
D-7800 FREIBURG i. Br.
(Allemagne fédérale)