Über die rationalen Punkte auf Kurven vom Geschlecht Eins

Kurt Mahler

Summary. Let $f(x, y)$ be an irreducible polynomial with rational coefficients and suppose that $f(x, y) = 0$ defines a curve of genus one with infinitely many rational points (x, y) lying on it. In this paper, Mahler shows that given a finite set S of prime numbers, there are only finitely many rational points (x, y) on the curve such that x or y has all its prime factors in S.

Acknowledgement. The article

> K. Mahler. Über die rationalen Punkte auf Kurven vom Geschlecht Eins. *J. Reine Angew. Math.*, 170:168–178, 1934.

is reproduced here with kind permission of de Gruyter.

Über die rationalen Punkte auf Kurven vom Geschlecht Eins.

Von *Kurt Mahler* in Manchester.

In seiner Arbeit (1) bewies C. Siegel vor einigen Jahren einen Satz, von dem eine Teilaussage folgendermaßen lautet:

Besitzt das irreduzible Polynom $f(x, y)$ rationale Koeffizienten und stellt die Gleichung $f(x, y) = 0$ eine algebraische Kurve mindestens vom Geschlecht Eins dar, so liegen auf dieser Kurve höchstens endlichviele Punkte mit ganzen rationalen Koordinaten.

Das Studium des Beweises dieses Satzes hat mich zu der Vermutung geführt, daß auf der Kurve $f(x, y) = 0$ sogar nur endlichviele Punkte (x, y) mit *rationalen* Koordinaten liegen, für die im Hauptnenner der beiden rationalen Zahlen x und y höchstens *endlich viele* feste Primzahlen aufgehen. Ein Beweis dieser Vermutung wird sich wahrscheinlich führen lassen, indem man die Methode der Siegelschen Arbeit verallgemeinert durch Hinzunahme der P-adischen Zahlen und Bewertungen, ähnlich wie in meiner Arbeit (2), wo ich dieses Verfahren zur Verallgemeinerung des Thue-Siegelschen Satzes benutzte.

Auf den folgenden Seiten wird dies im einzelnen ausgeführt für den Fall der Kurven vom Geschlecht Eins. Dabei ergibt das Siegelsche Verfahren durch solche P-adischen Überlegungen folgenden Satz:

Besitzt das irreduzible Polynom $f(x, y)$ rationale Koeffizienten und stellt die Gleichung $f(x, y) = 0$ eine Kurve vom Geschlecht Eins dar, auf der unendlichviele Punkte (x, y) mit rationalen Koordinaten liegen, ist ferner $g(x, y)$ eine rationale Funktion mit rationalen Koeffizienten, die auf der Kurve nicht konstant ist, so wächst die größte Primzahl, die im Nenner der rationalen Zahl $g(x, y)$ aufgeht, über alle Grenzen, wenn (x, y) eine unendliche Folge von Punkten auf der Kurve mit rationalen Koordinaten durchläuft.

Wählt man $g(x, y) = x$ oder y, so ist hierin speziell meine Vermutung für den Fall des Geschlechts Eins enthalten.

Der Beweis ist ganz analog dem Siegelschen. Die ersten Paragraphen sind infolge dessen fast wörtlich der Siegelschen Abhandlung entnommen. Unterschiede treten erst später auf, wenn ausgenutzt wird, daß im Nenner von $g(x, y)$ nur die gegebenen Primzahlen aufgehen. Alsdann muß man alle Schlüsse jeweils gleichzeitig für die Absolutbetragbewertung und die verschiedenen P-adischen Bewertungen durchführen. Auf diese Art läßt sich der Beweis schließlich ableiten aus meiner Verallgemeinerung des Thue-Siegelschen Satzes.

Herrn Prof. Siegel bin ich sehr zu Dank verpflichtet für eine wesentliche Vereinfachung des Beweises im letzten Paragraphen.

Literaturverzeichnis.

(1) C. Siegel, Über einige Anwendungen Diophantischer Approximationen, Abh. d. Preußischen Akademie der Wissenschaften, Phys. Math. Klasse, Jahrgang 1929, Nr. 1.

(2) K. Mahler, Zur Approximation algebraischer Zahlen, I, Math. Annalen **107** (1933).
(3) H. Poincaré, Sur les propriétés arithmétiques des courbes algébriques, Journal de math. pures et appl. (V) **7** (1901).
(4) Tr. Nagell, Sur les propriétés arithmétiques des cubiques planes du premier genre, Acta Math. **52** (1929).
(5) L. J. Mordell, On the rational solutions of the indeterminate equations of the third and fourth degrees, Proc. of the Cambridge Philos. Soc. **21** (1922).
(6) A. Weil, L'arithmétique sur les courbes algébriques, Acta Math. **52** (1929).

1. Eine Kurve C h-ter Ordnung vom Geschlecht Eins besitze die Gleichung

$$f(x, y) = 0,$$

wobei $f(x, y)$ ein irreduzibles Polynom in x und y mit rationalen Koeffizienten ist. Es werde angenommen, daß auf C unendlichviele Punkte (x, y) mit rationalen Koordinaten liegen. Alsdann gibt es eine birationale Transformation

$$x = \Phi(u, t), \quad y = \Psi(u, t)$$

mit der dazu inversen Transformation

$$u = \varphi(x, y), \quad t = \psi(x, y),$$

die die Gleichung von C auf die spezielle Form

$$t^2 = 4u^3 - g_2 u - g_3$$

transformiert. Dabei werden die Invarianten g_2, g_3 und auch die Koeffizienten der rationalen Funktionen Φ, Ψ, φ, ψ rationale Zahlen, wie aus bekannten Sätzen folgt [1]).

Ist $\wp(s)$ die Weierstraßsche elliptische Funktion mit den Invarianten g_2, g_3, so läßt sich C uniformisieren durch die Gleichungen

$$u = \wp(s), \quad t = \wp'(s).$$

Der *Satz von Mordell und Weil* besagt nun, daß die Argumente s, die zu den rationalen Punkten (x, y) auf C gehören, einen endlichen Modul bilden, d. h. sich alle in der Form

$$n_1 s_1 + n_2 s_2 + \cdots + n_q s_q$$

darstellen lassen, wo $s_1, s_2, \ldots, s_q$ endlichviele komplexe Zahlen sind und wo $n_1, n_2, \ldots, n_q$ einzeln alle ganzen rationalen Zahlen durchlaufen [2]).

2. Sei $g(x, y)$ eine rationale Funktion von x und y mit rationalen Koeffizienten, die auf C nicht identisch konstant ist, also etwa jeden Wert r-mal annimmt. Beim Übergang zu der Veränderlichen s verwandelt sich $g(x, y)$ in eine elliptische Funktion

$$G(s) = g(x, y)$$

von der Ordnung r.

In den rationalen Punkten (x, y) auf C wird $g(x, y)$ selbst eine rationale Zahl; als gekürzter Bruch geschrieben laute diese

$$g(x, y) = \frac{Z(g(xy))}{N(g(xy))},$$

wo also $Z(g(xy))$ und $N(g(xy))$ teilerfremde ganze rationale Zahlen bedeuten; natürlich sind Z und N nur arithmetische Funktionen von (x, y).

Von jetzt ab werde die Annahme gemacht, daß auf C eine unendliche Menge $\mathfrak{M}$ rationaler Punkte (x, y) liegt, in denen der Nenner N von $g(x, y)$ nur teilbar durch endlichviele fest gegebene Primzahlen

$$P_1, P_2, \ldots, P_p$$

wird; hieraus soll ein Widerspruch hergeleitet werden Dazu muß man zeigen, daß es

[1]) Daß sich diese Koeffizienten in der Tat rational wählen lassen, folgt aus Überlegungen von Poincaré. Siehe (3), S. 176—180, und (4), S. 94—95. Ein anderer Beweis wird im Anhang der vorliegenden Arbeit dargestellt.
[2]) Siehe (5) und (6).

neben $g(x, y)$ unendlichviele andere rationale Funktionen mit derselben Eigenschaft und zwar von beliebig hoher Ordnung gibt.

3. Die Argumente s, die zu den Punkten (x, y) der Menge $\mathfrak{M}$ gehören, besitzen nach 1. die Gestalt

$$n_1 s_1 + n_2 s_2 + \cdots + n_q s_q,$$

und zwar durchläuft für sie $(n_1, n_2, \ldots, n_q)$ unendlichviele Systeme von je q ganzen rationalen Zahlen. Sei nun n eine beliebig große natürliche Zahl. Dann läßt sich setzen:

$$n_1 s_1 + n_2 s_2 + \cdots + n_q s_q = n(m_1 s_1 + m_2 s_2 + \cdots + m_q s_q) + (n_1^0 s_1 + n_2^0 s_2 + \cdots + n_q^0 s_q),$$

wobei jede der Zahlen $n_1^0, n_2^0, \ldots, n_q^0$ in der Folge $0, 1, 2, \ldots, n-1$ liegt, die Zahlen $m_1, m_2, \ldots, m_q$ aber wieder ganz rational sind. Für die Summe

$$n_1^0 s_1 + n_2^0 s_2 + \cdots + n_q^0 s_q$$

gibt es hiernach nur endlichviele Möglichkeiten, während das Zahlsystem $(m_1, m_2, \ldots, m_q)$ für die Punkte aus $\mathfrak{M}$ unendlichviele Werte annimmt.

Es ist demnach möglich, eine unendliche Teilmenge $\mathfrak{M}_n^*$ von Punkten (x, y) aus $\mathfrak{M}$ auszuwählen, für die in der Zerlegung

$$n_1 s_1 + n_2 s_2 + \cdots + n_q s_q = n(m_1 s_1 + m_2 s_2 + \cdots + m_q s_q) + (n_1^0 s_1 + n_2^0 s_2 + \cdots + n_q^0 s_q)$$

der Ausdruck

$$s^0 = n_1^0 s_1 + n_2^0 s_2 + \cdots + n_q^0 s_q$$

jedesmal derselbe ist. Der Menge $\mathfrak{M}_n^*$ ist eineindeutig die Menge $\mathfrak{M}_n$ der Punkte (x, y) mit den Argumenten

$$m_1 s_1 + m_2 s_2 + \cdots + m_q s_q$$

zugeordnet; es ist klar, daß die elliptische Funktion

$$G_n(s) = G(ns + s^0)$$

in den Punkten von $\mathfrak{M}_n$ wieder einen rationalen Wert erhält, in dessen Nenner nur die gegebenen Primzahlen $P_1, P_2, \ldots, P_p$ aufgehen. Als elliptische Funktion ist $G_n(s)$ genau von der Ordnung $n^2 r$, und zwar sieht man leicht, daß $G_n(s)$ an jeder Stelle einen Wert höchstens r-fach annimmt. Geht man von dem Argument s wieder zurück zu den Veränderlichen x, y auf der Kurve C, so geht $G_n(s)$ über in eine rationale Funktion

$$G_n(s) = g_n(x, y)$$

in x und y; nach den Annahmen in 1. und auf Grund des Additionstheorems der elliptischen Funktionen besitzt diese lauter rationale Koeffizienten; sie nimmt auf C jeden Wert genau $(n^2 r)$-mal, und zwar an jeder Stelle höchstens r-fach, an.

Nachdem so die unendlichvielen Funktionen

$$g_n(x, y) \qquad (n = 1, 2, 3, \ldots)$$

und die zugehörigen unendlichen Mengen

$$\mathfrak{M}_n \qquad (n = 1, 2, 3, \ldots)$$

rationaler Punkte (x, y) auf C konstruiert worden sind, in denen diese Funktionen rationale Zahlen werden, in deren Nenner allein die gegebenen Primzahlen aufgehen, braucht von den elliptischen Funktionen kein Gebrauch mehr gemacht zu werden. Zur Abkürzung werde die Darstellung von $g_n(x, y)$ als gekürzter Bruch in den rationalen Punkten (x, y) auf C in der Form

$$g_n(x, y) = \frac{Z(g_n(xy))}{N(g_n(xy))}$$

geschrieben, wo also Z und N teilerfremde ganze rationale Zahlen sind [3]).

[3]) Die bisherigen Schlüsse sind ganz der Arbeit (1), S. 52—54, entnommen.

4. Es werde jetzt näher auf die arithmetischen Eigenschaften der Funktionswerte $g_n(x, y)$ in den Punkten der Menge $\mathfrak{M}_n$ eingegangen. Die beiden Funktionen $g_n(x, y)$ und $g_n(x, y) - 1$ verschwinden nicht an gleichen Stellen. Also läßt sich eine unendliche Teilfolge $\mathfrak{N}_n$ von Punkten (x, y) aus $\mathfrak{M}_n$ auswählen, die alle außerhalb von endlichen Umgebungen der Nullstellen einer dieser beiden Funktionen bleiben, etwa der Funktion $g_n(x, y) - e$, wo also e eine bestimmte der Zahlen 0 und 1 ist. Der gewöhnliche Absolutbetrag von $g_n(x, y) - e$ bleibt also für alle Punkte von $\mathfrak{N}_n$ oberhalb einer positiven Konstanten, dementsprechend der Absolutbetrag der reziproken Funktion

$$\gamma_n(x, y) = \frac{1}{g_n(x, y) - e}$$

unterhalb einer endlichen positiven Konstanten. In allen rationalen Punkten (x, y) auf C stellt auch $\gamma_n(x, y)$ eine rationale Zahl dar; als gekürzter Bruch läßt sich dieselbe etwa in der Form

$$\gamma_n(x, y) = \frac{Z(\gamma_n(xy))}{N(\gamma_n(xy))}$$

schreiben, wo Z und N auch hier teilerfremden ganzen rationalen Zahlen gleich werden. Es ist natürlich

$$Z(\gamma_n(xy)) = N(g_n(xy)).$$

Für die unendlichvielen Punkte (x, y) aus $\mathfrak{N}_n$ gehen demnach in $Z(\gamma_n(x, y))$ nur die endlichvielen gegebenen Primzahlen $P_1, P_2, \ldots, P_p$ auf; hiernach ist dieser Zähler in jenen Punkten speziell von Null verschieden.

5. Nach C. Siegel läßt sich für den gewöhnlichen Absolutbetrag des Quotienten

$$\frac{\gamma_n(x, y)}{Z(\gamma_n(xy))}$$

eine obere Schranke arithmetischer Art angeben, falls (x, y) nur solche rationalen Punkte auf C durchläuft, in denen $|\gamma_n(x, y)|$ unterhalb einer positiven endlichen Zahl C_0 bleibt, und in denen $\gamma_n(x, y)$ nicht verschwindet; diese beiden Bedingungen sind insbesondere in $\mathfrak{N}_n$ erfüllt.

Sei für einen rationalen Punkt (x, y) auf C der gemeinsame Hauptnenner von x und y gleich ζ und alsdann

$$x = \frac{\xi}{\zeta}, \quad y = \frac{\eta}{\zeta},$$

so daß ξ, η, ζ drei endliche teilerfremde ganze rationale Zahlen werden. Bedeutet noch ε eine positive beliebig kleine Zahl, so lautet die Ungleichung von Siegel [4]):

$$\left|\frac{\gamma_n(x, y)}{Z(\gamma_n(xy))}\right| \leqq c(|\xi| + |\eta| + |\zeta|)^{-\frac{n^2 r}{h} + \varepsilon};$$

dabei bedeutet c eine solche positive Konstante, die allein von ε und der Schranke C_0 abhängt. Der Exponent $n^2 r$ steht hierbei als Ordnung von $\gamma_n(x, y)$.

Diese Ungleichung setzt nicht voraus, daß (x, y) in $\mathfrak{N}_n$ liegt. Beschränkt man sich aber auf die rationalen Punkte *dieser* Menge, so läßt sich die linke Seite auf eine Form bringen, in der $Z(\gamma_n(xy))$ nicht mehr vorkommt. Bedeute dazu wie üblich $|\alpha|_p$ den

[4]) Siehe (1), S. 52.

P-adischen Wert einer P-adischen Zahl. Alsdann wird für die Punkte in $\mathfrak{N}_n$ gerade

$$\frac{1}{|Z(\gamma_n(xy))|} = \prod_{\tau=1}^{p} |\gamma_n(x,y)|_{P_\tau},$$

denn nach Voraussetzung ist in den Punkten von $\mathfrak{N}_n$ der Zähler Z von $\gamma_n(x,y)$ ein Potenzprodukt allein von $P_1, P_2, \ldots, P_p$, während der Nenner N wegen seiner Teilerfremdheit zu Z natürlich auch zu diesen Primzahlen teilerfremd ist [5]).

Damit nimmt die Siegelsche Ungleichung die Form

$$|\gamma_n(x,y)| \prod_{\tau=1}^{p} |\gamma_n(x,y)|_{P_\tau} \leqq c(|\xi| + |\eta| + |\zeta|)^{-\frac{n^2 r}{h} + \varepsilon}$$

an; diese gilt aber selbstverständlich nur noch für die Punkte aus $\mathfrak{N}_n$. Der Bequemlichkeit halber werde im folgenden ε gleich $\frac{n^2 r}{2h}$ gesetzt, so daß die letzte Ungleichung die noch etwas einfachere Form

$$|\gamma_n(x,y)| \prod_{\tau=1}^{p} |\gamma_n(x,y)|_{P_\tau} \leqq c(|\xi| + |\eta| + |\zeta|)^{-\frac{n^2 r}{2h}}$$

bekommt.

6. Es gibt nur endlichviele Punkte (x,y) in der Menge $\mathfrak{N}_n$, für die die natürliche Zahl $|\xi| + |\eta| + |\zeta|$ beschränkt ist. Durchläuft also (x,y) alle Punkte von $\mathfrak{N}_n$, so muß $|\xi| + |\eta| + |\zeta|$ über alle Grenzen, die rechte Seite der letzten Ungleichung also gegen Null streben. Das Produkt

$$|\gamma_n(x,y)| \prod_{\tau=1}^{p} |\gamma_n(x,y)|_{P_\tau}$$

strebt also gleichfalls gegen Null, folglich auch einige seiner Faktoren. Der Einfachheit halber soll angenommen werden, daß alle Faktoren

$$|\gamma_n(x,y)|, \quad |\gamma_n(x,y)|_{P_1}, \quad |\gamma_n(x,y)|_{P_2}, \ldots, |\gamma_n(x,y)|_{P_p}$$

gegen Null streben. Falls dies nicht zutrifft, brauchte man für die folgende Untersuchung nur einige dieser Bewertungen von der Betrachtung auszuschließen und eventuell statt $\mathfrak{N}_n$ eine Teilmenge hiervon zu nehmen; im Ganzen würde sich aber nichts Wesentliches an der Beweisführung ändern.

7. Genau so wie die Funktion $g_n(x,y)$ nimmt auch die Funktion $\gamma_n(x,y)$ auf C jeden Wert $(n^2 r)$-mal und zwar an jeder Stelle höchstens r-fach an. Es muß eine lineare Funktion

$$z = a_1 x + a_2 y$$

mit zwei ganzen rationalen Koeffizienten a_1 und a_2 geben, die speziell in allen Nullstellen von $\gamma_n(x,y)$, so weit diese getrennt liegen, auch verschiedene Werte erhält. Durchläuft nun (x,y) alle Punkte aus $\mathfrak{N}_n$, so nimmt z unendlichviele rationale Werte an. Nach den Konvergenzgesetzen der Körper der reellen und P-adischen Zahlen ist es möglich, eine unendliche Teilfolge aus $\mathfrak{N}_n$, welche $\mathfrak{N}_n^*$ heiße, so auszuwählen, daß in ihr die Zahl z gleichzeitig gegen eine reelle Zahl α, eine P_1-adische Zahl α_1, eine P_2-adische Zahl $\alpha_2, \ldots$, eine P_p-adische Zahl α_p konvergiert, wobei einige von diesen Zahlen auch unendlich groß sein können und die Konvergenz jeweils in bezug auf die betreffende Bewertung zu verstehen ist.

Es gibt eine ganze rationale Zahl a_3 unter den Zahlen $0, 1, 2, \ldots, p+1$, die von

[5]) Der letzte Schluß setzt voraus, daß im Zähler $Z(\gamma_n(xy))$ wirklich alle Primzahlen $P_1, P_2, \ldots, P_p$ aufgehen; darin liegt aber keine wesentliche Einschränkung.

den sämtlichen Grenzwerten

$$-\alpha, -\alpha_1, -\alpha_2, \ldots, -\alpha_p$$

verschieden ist; dabei ist zu berücksichtigen, daß a_3 als rationale Zahl mit jedem dieser Grenzwerte in einem gemeinsamen Körper liegt, der Begriff der Ungleichheit also Sinn hat. Mit der so bestimmten Zahl a_3 werde die neue rationale Funktion auf C

$$Z(x, y) = \frac{1}{z + a_3} = \frac{1}{a_1 x_1 + a_2 x_2 + a_3}$$

eingeführt; durchläuft (x, y) alle Punkte aus $\mathfrak{N}_n^*$, so konvergieren die verschiedenen Bewertungen

$$|Z(x, y)|, \quad |Z(x, y)|_{P_1}, \quad |Z(x, y)|_{P_2}, \ldots, |Z(x, y)|_{P_p}$$

der Reihe nach gegen die reelle, die P_1-adische, die P_2-adische, ..., die P_p-adische Zahl

$$\frac{1}{\alpha + a_3}, \quad \frac{1}{\alpha_1 + a_3}, \quad \frac{1}{\alpha_2 + a_3}, \ldots, \frac{1}{\alpha_p + a_3},$$

und diese sind alle endlich, da die Nenner nach Voraussetzung nicht verschwinden. Daraus folgt insbesondere, daß die Werte

$$|Z(x, y)|, \quad |Z(x, y)|_{P_1}, \quad |Z(x, y)|_{P_2}, \ldots, |Z(x, y)|_{P_p}$$

von $Z(x, y)$ beschränkt bleiben, wenn (x, y) die unendlichvielen Punkte aus $\mathfrak{N}_n^*$ durchläuft; die etwaigen endlichvielen Ausnahmepunkte dieser Menge, in denen gerade $z = -a_3$ ist, denken wir dabei bereits aus $\mathfrak{N}_n^*$ fortgelassen.

8. Die neue rationale Funktion $Z(x, y)$ besitzt genau wie die lineare Funktion $z = a_1 x + a_2 y$ die Eigenschaft, in allen Nullstellen von $\gamma_n(x, y)$, soweit diese getrennt liegen, verschiedene Werte anzunehmen. Zwischen

$$Z(x, y) \text{ und } \gamma_n(x, y)$$

besteht eine algebraische Gleichung mit rationalen Koeffizienten, die in $Z(x, y)$ von nicht höherem Grad als $n^2 r$ ist, weil ja $\gamma_n(x, y)$ diese Ordnung hat. Man kann die Gleichung in der Form

$$F(Z(x, y)) + \gamma_n(x, y)\, G(Z(x, y), \gamma_n(x, y)) = 0$$

schreiben, wobei $F(Z)$ ein Polynom in Z, $G(Z, \gamma_n)$ ein Polynom in Z und γ_n ist und beide lauter rationale Koeffizienten haben. Die Nullstellen von $F(Z)$ entsprechen den Stellen auf der Kurve C mit $\gamma_n(x, y) = 0$; sie können also alle höchstens r-fach sein; ferner darf $F(Z)$ in Z von nicht höherem Grad als $n^2 r$ sein.

Durchläuft (x, y) die Punkte von $\mathfrak{N}_n^*$, so streben die Bewertungen

$$|\gamma_n(x, y)|, \quad |\gamma_n(x, y)|_{P_1}, \quad |\gamma_n(x, y)|_{P_2}, \ldots, |\gamma_n(x, y)|_{P_p}$$

nach Voraussetzung gegen Null, während die Bewertungen

$$|Z(x, y)|, \quad |Z(x, y)|_{P_1}, \quad |Z(x, y)|_{P_2}, \ldots, |Z(x, y)|_{P_p}$$

beschränkt bleiben. Also bleiben auch die Bewertungen

$$|G(Z(x, y), \gamma_n(x, y))|, \quad |G(Z(x, y), \gamma_n(x, y))|_{P_\tau} \qquad (\tau = 1, 2, \ldots, p)$$

alle beschränkt, etwa unterhalb der positiven Konstanten c_1. Dann geht die obige Gleichung gerade in die $p + 1$ Ungleichungen

$$|F(Z(x, y))| \leqq c_1 |\gamma_n(x, y)|, \quad |F(Z(x, y))|_{P_\tau} \leqq c_1 |\gamma_n(x, y)|_{P_\tau} \quad (\tau = 1, 2, \ldots, p)$$

über, und aus der Siegelschen Ungleichung entsteht eine solche für die Funktion $F(Z)$:

$$|F(Z(x, y))| \prod_{\tau=1}^{p} |F(Z(x, y))|_{P_\tau} \leqq c c_1^{p+1} (|\xi| + |\eta| + |\zeta|)^{-\frac{n^2 r}{2h}}.$$

Man kann dieser Ungleichung noch eine einfachere Form geben und damit zu einer Frage

über Diophantische Approximationen im Rationalen gelangen. Sei zu diesem Zweck für beliebige rationale Punkte (x, y) mit

$$x = \frac{\xi}{\zeta}, \quad y = \frac{\eta}{\zeta}, \qquad (\xi, \eta, \zeta) = 1$$

die Darstellung der gleichfalls rationalen Zahl $Z(x, y)$ als gekürzter Bruch gegeben in der Form

$$Z(x, y) = \frac{X}{Y},$$

wo X und Y teilerfremde ganze rationale Zahlen sind. Es ist

$$Z(x, y) = \frac{1}{a_1 x + a_2 y + a_3} = \frac{\zeta}{a_1 \xi + a_2 \eta + a_3 \zeta};$$

die Zahl

$$|X, Y| = \max(|X|, |Y|)$$

bleibt also stets kleiner als

$$c_3(|\xi| + |\eta| + |\zeta|),$$

wobei c_2 eine positive Konstante bedeutet. Durchläuft der Punkt (x, y) die Folge $\mathfrak{N}_n^*$, so nimmt ferner die Funktion $Z(x, y)$ unendlichviele verschiedene Werte an, denn die Kurve C hat mit jeder Geraden nur endlichviele Punkte gemeinsam.

Beachtet man noch, daß

$$c c_1^{p+1}(|\xi| + |\eta| + |\zeta|)^{-\frac{n^2 r}{2h}} \leqq c c_1^{p+1}(c_2^{-1}|X, Y|)^{-\frac{n^2 r}{2h}}$$

ist, und setzt man

$$c_3 = c c_1^{p+1} c_2^{\frac{n^2 r}{2h}},$$

so ist damit gezeigt, daß es eine unendliche Folge gekürzter rationaler Zahlen $Z = X/Y$ gibt, für die das Polynom $F(Z)$ der Ungleichung

$$\left|F\left(\frac{X}{Y}\right)\right| \prod_{\tau=1}^{p} \left|F\left(\frac{X}{Y}\right)\right|_{P_\tau} \leqq c_3 |X, Y|^{-\frac{n^2 r}{2h}}$$

genügt.

9. Um von hier aus zu einem Widerspruch zu kommen, muß man von dem verallgemeinerten Thue-Siegelschen Satz Gebrauch machen. Dieser läßt sich nicht unmittelbar anwenden, weil das Polynom $F(Z)$ im allgemeinen reduzibel ist. Es möge im Körper der rationalen Zahlen etwa in die Faktoren

$$F(Z) = \prod_{\lambda=1}^{l} F_\lambda(Z)^{d_\lambda}$$

zerfallen, wobei

$$F_1(Z), \quad F_2(Z), \ldots, \quad F_l(Z)$$

lauter verschiedene irreduzible Polynome in Z mit rationalen Koeffizienten sind, und die sämtlichen Exponenten

$$d_1, d_2, \ldots, d_l$$

natürliche Zahlen bedeuten, die nicht größer als r sind.

Bezeichnet $F_\lambda(Z)$ und $F_\mu(Z)$ zwei verschiedene von den letzten Polynomen, so müssen diese wegen ihrer Irreduzibilität zueinander teilerfremd sein. Es gibt also eine nichtverschwindende rationale Zahl d und zwei Polynome $F_\lambda^*(Z)$ und $F_\mu^*(Z)$ mit rationalen Koeffizienten, so daß identisch

$$F_\lambda(Z) F_\lambda^*(Z) + F_\mu(Z) F_\mu^*(Z) = d$$

ist. Gemäß der Konstruktion sind aber die sämtlichen Bewertungen

$$|Z(x, y)|, \quad |Z(x, y)|_{P_1}, \quad |Z(x, y)|_{P_2}, \ldots, |Z(x, y)|_{P_p}$$

von $Z(x, y)$ für die Punkte (x, y) aus $\mathfrak{N}_n^*$ beschränkt; dasselbe gilt folglich auch für die sämtlichen Bewertungen

$$|F_\lambda^*(Z(x, y))|, \quad |F_\lambda^*(Z(x, y))|_{P_\tau} \qquad (\tau = 1, 2, \ldots, p)$$

und

$$|F_\mu^*(Z(x, y))|, \quad |F_\mu^*(Z(x, y))|_{P_\tau} \qquad (\tau = 1, 2, \ldots, p);$$

diese bleiben etwa unterhalb der positiven Konstanten c_4. Ist noch

$$c_5 = \min (|d|, |d|_{P_1}, \ldots, |d|_{P_p}),$$

so folgt aus der obigen Identität durch Übergang zu den verschiedenen Bewertungen, daß

$$\max (|F_\lambda(Z(x, y))|, |F_\mu(Z(x, y))|) \geqq \frac{c_5}{2c_4},$$

$$\max (|F_\lambda(Z(x, y))|_{P_\tau}, |F_\mu(Z(x, y))|_{P_\tau}) \geqq \frac{c_5}{2c_4} \qquad (\tau = 1, 2, \ldots, p)$$

ist. Entsprechende Ungleichungen gelten für irgend zwei andere von den Polynomfaktoren von $F(Z)$. Daraus folgt, daß beim Durchlaufen der Folge $\mathfrak{N}_n^*$ jeweils für höchstens eine der Zahlen

$$F_1(Z(x, y)), \quad F_2(Z(x, y)), \ldots, F_l(Z(x, y))$$

der gewöhnliche Absolutbetrag oder der P_1-adische Wert oder der P_2-adische Wert, usw., oder schließlich der P_p-adische Wert kleiner als eine gewisse positive Konstante sein kann. Daraus ergibt sich, daß beim Durchlaufen der Folge $\mathfrak{N}_n^*$ zu gleicher Zeit höchstens für $p + 1$ Indizes λ der Reihe

$$0, 1, 2, \ldots, l$$

das Produkt

$$|F_\lambda(Z(x, y))| \prod_{\tau=1}^{p} |F_\lambda(Z(x, y))|_{P_\tau}$$

oder, was dasselbe besagt, das Produkt

$$\left|F_\lambda\left(\frac{X}{Y}\right)\right| \prod_{\tau=1}^{p} \left|F_\lambda\left(\frac{X}{Y}\right)\right|_{P_\tau}$$

kleiner als eine feste positive Konstante sein kann. Ist für ein Argument $Z(x, y) = X/Y$ etwa das Produkt mit dem Index λ das kleinste, so wird wegen $\max (d_1, d_2, \ldots, d_l) \leqq r$

$$\left|F\left(\frac{X}{Y}\right)\right| \prod_{\tau=1}^{p} \left|F\left(\frac{X}{Y}\right)\right|_{P_\tau} \geqq c_6 \left\{\left|F_\lambda\left(\frac{X}{Y}\right)\right| \prod_{\tau=1}^{p} \left|F_\lambda\left(\frac{X}{Y}\right)\right|_{P_\tau}\right\}^{(p+1)r},$$

wobei c_6 eine gewisse von λ unabhängige positive Konstante ist [6]).

Für das einzelne Produkt

$$\left|F_\lambda\left(\frac{X}{Y}\right)\right| \prod_{\tau=1}^{p} \left|F_\lambda\left(\frac{X}{Y}\right)\right|_{P_\tau}$$

liefert jetzt der verallgemeinerte Thue-Siegelsche Satz eine untere Schranke, wenn man von den endlichvielen Elementen von $\mathfrak{N}_n^*$ absieht, für die dieses Polynom verschwindet. Es ergibt sich, wenn das irreduzible Polynom $F_\lambda(Z)$ den genauen Grad n_λ hat, daß [7])

$$\left|F_\lambda\left(\frac{X}{Y}\right)\right| \prod_{\tau=1}^{p} \left|F_\lambda\left(\frac{X}{Y}\right)\right|_{P_\tau} \geqq c_7 |X, Y|^{-2\sqrt{n_\lambda}}$$

[6]) Die in 9. gegebene Herleitung dieser Ungleichung verdanke ich Herrn Prof. Siegel; mein eigener Ansatz war umständlicher und machte Gebrauch von Eigenschaften der Teilungsgleichung der elliptischen Funktionen.

[7]) Siehe den Hauptsatz meiner Arbeit (2). Dieser bezieht sich auf Binärformen; der hier benutzte Satz über Polynome ergibt sich aber daraus auf triviale Weise. In meiner Arbeit wird vorausgesetzt, daß der Grad der Form mindestens 3 ist; ist er aber gleich 2 oder 1, so ist das hier benutzte Ergebnis ganz selbstverständlich.

ist, wobei c_7 eine gewisse positive Konstante bedeutet. Nun haben aber natürlich die Faktoren $F_\lambda(Z)$ des Polynoms $F(Z)$ vom Grad $\leqq n^2r$ erst recht einen Grad n_λ, der n^2r nicht übersteigt; also ist

$$\left|F_\lambda\left(\frac{X}{Y}\right)\right| \prod_{\tau=1}^{p} \left|F_\lambda\left(\frac{X}{Y}\right)\right|_{P_\tau} \geqq c_7 |X, Y|^{-2n\sqrt{r}},$$

und damit folgt schließlich die Ungleichung

$$\left|F\left(\frac{X}{Y}\right)\right| \prod_{\tau=1}^{p} \left|F\left(\frac{X}{Y}\right)\right|_{P_\tau} \geqq c_6 c_7^{(p+1)r} |X, Y|^{-2(p+1)r^{3/2}n}$$

für eine unendliche Folge von Brüchen X/Y aus $\mathfrak{N}_n^*$. Andrerseits ist nach früherem

$$\left|F\left(\frac{X}{Y}\right)\right| \prod_{\tau=1}^{p} \left|F\left(\frac{X}{Y}\right)\right|_{P_\tau} \leqq c_2 |X, Y|^{-\frac{n^2r}{2h}}$$

für die Zahlen aus $\mathfrak{N}_n^*$. Ist nun die beliebige natürliche Zahl n größer als

$$4h(p+1)\sqrt{r},$$

so wird

$$\frac{n^2r}{2h} < 2(p+1)r^{3/2}n,$$

und die vorigen beiden Ungleichungen stehen für hinreichend großes $|X, Y|$ miteinander im Widerspruch.

Damit ist bewiesen, daß es keine auf C nicht identisch konstante rationale Funktion $g(x, y)$ mit rationalen Koeffizienten gibt, deren Wert in einer unendlichen Folge von rationalen Punkten (x, y) auf C einen Nenner besitzt, in dem nur die endlichvielen festgegebenen Primzahlen

$$P_1, P_2, \ldots, P_p$$

aufgehen.

Anhang.

Es soll bewiesen werden, *daß eine Kurve C vom Geschlecht Eins, deren Gleichung*

$$f(x, y) = 0$$

lauter rationale Koeffizienten hat und auf der hinreichend viele Punkte (x, y) mit rationalen Koordinaten liegen, sich durch eine birationale Transformation

$$x = \Phi(u, t), \quad y = \Psi(u, t), \quad u = \varphi(x, y), \quad t = \psi(x, y)$$

derart in eine Kurve $\mathfrak{C}$ der Gleichung

$$t^2 = 4u^3 - g_2 u - g_3$$

überführen läßt, daß sowohl die Koeffizienten der rationalen Funktionen $\Phi, \Psi, \varphi, \psi$ als auch die Zahlen g_2, g_3 rational werden.

Nach bekannten Eigenschaften der Kurven vom Geschlecht Eins ist es jedenfalls immer möglich, die Kurve C durch eine birationale Transformation

$$x = \Phi'(u', t'), \quad y = \Psi'(u', t'), \quad u' = \varphi'(x, y), \quad t' = \psi'(x, y)$$

in eine Kurve $\mathfrak{C}'$ mit der Gleichung

$$t'^2 = 4u'^3 - g_2' u' - g_3'$$

zu überführen, so daß gleichzeitig ein Punkt $\mathfrak{p}_1 = (x_1, y_1)$ auf C mit rationalen Koordinaten in den unendlichfernen Punkt $u' = t' = \infty$ auf $\mathfrak{C}'$ übergeht. Sei weiter $\mathfrak{p}_2 = (x_2, y_2) \neq \mathfrak{p}_1$ ein solcher zweiter Punkt auf C mit rationalen Koordinaten, daß sein Bildpunkt (u_2', t_2') auf $\mathfrak{C}'$ nichtverschwindende Koordinaten u' und t' erhält. Alsdann gibt es eine affine Abbildung

$$t' = \lambda^3 t, \quad u' = \lambda^2 u \qquad (\lambda \neq 0 \text{ und } \neq \infty),$$

die die Kurve $\mathfrak{C}'$ in eine Kurve $\mathfrak{C}$ mit der Gleichung

$$t^2 = 4u^3 - g_2 u - g_3$$

überführt, so daß gleichzeitig der Bildpunkt (u_2, t_2) von (u_2', t_2') auf der Geraden Γ mit der Gleichung

$$u = t$$

zu liegen kommt; dazu braucht man nur λ in eindeutiger Weise gleich

$$\lambda = \frac{t_2'}{u_2'}$$

zu setzen.

Eliminiert man t', u', so entsteht eine birationale Transformation

$$x = \Phi(u, t), \quad y = \Psi(u, t), \quad u = \varphi(x, y), \quad t = \psi(x, y),$$

die die Kurve C direkt in die Kurve $\mathfrak{C}$ überführt, und zwar entspricht dabei dem Punkt $\mathfrak{p}_1$ auf C der Punkt $u = t = \infty$ und dem Punkt $\mathfrak{p}_2$ auf C der Punkt (u_2, t_2) mit $u_2 = t_2$ auf der Geraden Γ. Ohne Einschränkung kann angenommen werden, daß sowohl die Koeffizienten der rationalen Funktionen $\Phi, \Psi, \varphi, \psi$, als auch die Zahlen g_2, g_3 algebraisch sind und also etwa gleichzeitig in dem galoisschen Zahlkörper K liegen; dann müssen offenbar auch u_2 und t_2 Zahlen aus K sein.

Bedeute θ einen der Automorphismen von K. Durch Anwendung von θ auf die Koeffizienten der rationalen Funktionen $\Phi, \Psi, \varphi, \psi$ entstehen neue rationale Funktionen $\Phi^\theta, \Psi^\theta, \varphi^\theta, \psi^\theta$, durch Anwendung auf die Zahlen g_2, g_3, u_2, t_2 neue Zahlen $g_2^\theta, g_3^\theta, u_2^\theta, t_2^\theta$. Dann stellt auch

$$x = \Phi^\theta(u, t), \quad y = \Psi^\theta(u, t), \quad u = \varphi^\theta(x, y), \quad t = \psi^\theta(x, y)$$

eine birationale Transformation dar; durch sie wird C in die Kurve $\mathfrak{C}^\theta$ mit der Gleichung

$$t^2 = 4u^3 - g_2^\theta u - g_3^\theta$$

übergeführt. Dem Punkt $\mathfrak{p}_1$ muß dabei auf $\mathfrak{C}^\theta$ wieder der Punkt $u = t = \infty$ entsprechen, dem Punkt $\mathfrak{p}_2$ aber ein Punkt (u_2^θ, t_2^θ) mit $u_2^\theta = t_2^\theta$. Denn es ist nach Voraussetzung $u_2 = t_2$; diese Beziehung bleibt aber unverändert, wenn man θ anwendet.

Die beiden kubischen Kurven $\mathfrak{C}$ und $\mathfrak{C}^\theta$ müssen ineinander überführbar sein mittels einer birationalen Transformation. Da die unendlichfernen Punkte beider Kurven einander entsprechen, so kann diese Transformation nur eine Affinität

$$t \to \mu^3 t, \quad u \to \mu^2 u$$

sein. Diese muß aber gleich der Identität sein, denn es entsprechen einander die beiden Punkte (u_2, t_2) und (u_2^θ, t_2^θ) mit $u_2 = t_2$ und $u_2^\theta = t_2^\theta$. Also stimmen die beiden Kurven $\mathfrak{C}$ und $\mathfrak{C}^\theta$ überein.

Daraus folgt erstens, daß die Invarianten g_2 und g_3 von den Automorphismen θ nicht geändert werden; also sind sie rationale Zahlen. Zweitens ergibt sich, daß die birationalen Transformationen

$$x = \Phi^\theta(u, t), \quad y = \Psi^\theta(u, t), \quad u = \varphi^\theta(x, y), \quad t = \psi^\theta(x, y)$$

unabhängig von θ jedem Punkt (x, y) denselben Punkt (u, t) zuordnen. Also sind sie alle identisch und auch identisch mit der Transformation

$$x = \frac{1}{k}\sum_\theta \Phi^\theta(u, t), \quad y = \frac{1}{k}\sum_\theta \Psi^\theta(u, t), \quad u = \frac{1}{k}\sum_\theta \varphi^\theta(x, y), \quad v = \frac{1}{k}\sum_\theta \psi^\theta(x, y),$$

wo die Summen über alle Automorphismen von K erstreckt werden und k die Anzahl dieser Automorphismen bedeutet. Hier steht aber nach den bekannten Sätzen über

symmetrische Funktionen jetzt wirklich eine birationale Transformation, die durch rationale Funktionen mit rationalen Koeffizienten vermittelt wird; der behauptete Satz ist also wahr [8]).

Göttingen 17. 2. 33.

[8]) Dieser Beweis ist einem entsprechenden Beweis für Kurven vom Geschlecht Null in der Siegelschen Arbeit (1), S. 50, nachgebildet.

Eingegangen 26. Februar 1933.

Anmerkung der Redaktion.

Der im Anhang gegebene Beweis läßt sich durch einen einfacheren und weitertragenden auf Grund der arithmetischen Theorie der algebraischen Funktionen ersetzen. Es genügt, die Existenz *mindestens eines* rationalen Punktes vorauszusetzen. Außerdem kann der Koeffizientenkörper k ein beliebiger vollkommener Körper mit von 2 und 3 verschiedener Charakteristik p ($= 0$ oder Primzahl) an Stelle des Körpers der rationalen Zahlen sein.

Sei also K ein Körper algebraischer Funktionen einer Unbestimmten vom Geschlecht $g = 1$ über einem solchen Koeffizientenkörper k, und besitze K mindestens einen „in k rationalen Punkt", d. h. Primdivisor $\mathfrak{P}$ vom Grade 1. Wie F. K. Schmidt [1]) bewiesen hat, gilt für K (sogar bei *beliebigem* Geschlecht g und vollkommenem k *beliebiger* Charakteristik p) der Riemann-Rochesche Satz [1]). Bei $g = 1$ gibt es danach für jeden Divisor $\mathfrak{D}$ positiven Grades n genau n bezgl. k linear unabhängige ganze Multipla von $\frac{1}{\mathfrak{D}}$ in K. Insbesondere existiert also in K ein von 1 linear unabhängiges ganzes Multiplum x_0 von $\frac{1}{\mathfrak{P}^2}$ und ein von 1, x_0 linear unabhängiges ganzes Multiplum y_0 von $\frac{1}{\mathfrak{P}^3}$, und diese Multipla liegen genau bis auf Transformationen

$$x = ax_0 + a', \qquad y = by_0 + b'x_0 + b''$$

mit beliebigen $a \neq 0$, $b \neq 0$, a', b', b'' aus k fest. Ferner sind $1, x, x^2, x^3, y, xy$ dann das volle System der 6 linear unabhängigen ganzen Multipla von $\frac{1}{\mathfrak{P}^6}$. Das ganze Multiplum y^2 von $\frac{1}{\mathfrak{P}^6}$ ist also linear über k aus $1, x, x^2, x^3, y, xy$ komponierbar. Wegen $p \neq 2$ können b' und b'' (eindeutig) so normiert werden, daß y^2 schon aus $1, x, x^2, x^3$ (ohne y, xy) linear komponierbar ist, und wegen $p \neq 3$ kann a' (eindeutig) so normiert werden, daß y^2 schon aus $1, x, x^3$ (ohne x^2) linear komponierbar ist. Schließlich kann wegen $p \neq 2$ die Normierung von a, b so gegeneinander ausgeglichen werden, daß diese Abhängigkeit lautet:

$$y^2 = 4x^3 - g_2 x - g_3$$

mit g_2, g_3 aus k, und man sieht überdies, daß die so gewonnenen x, y, g_2, g_3 bis auf die Homogenitätstransformationen

$$x' = c^2 x, \quad y' = c^3 x, \quad g_2' = c^4 g_2, \quad g_3' = c^6 g_3$$

eindeutig durch $\mathfrak{P}$ bestimmt sind. Das Abelsche Theorem (Additionstheorem) lehrt dann noch, daß sie auch für jeden anderen Primdivisor 1. Grades $\mathfrak{Q}$ von K dieselben sind.

H. Hasse.

[1]) Analytische Zahlentheorie in Körpern der Charakteristik p, Math. Zeitschr. **33** (1931).