ÜBER DIE DIOPHANTISCHEN GLEICHUNGEN VOM GESCHLECHT NULL

VON

D. HILBERT UND A. HURWITZ

in KÖNIGSBERG i. Pr.

Die vorliegende Mittheilung behandelt die Aufgabe, alle ganzzahligen Lösungen der Gleichung

$$f(x_1, x_2, x_3) = 0 \tag{1}$$

zu finden, unter der Voraussetzung, dass $f(x_1, x_2, x_3)$ eine ganze ganzzahlige homogene Function vom n^{ten} Grade in den Variabeln x_1, x_2, x_3 bedeutet, und die durch jene Gleichung definirte ebene Curve das Geschlecht Null besitzt. Die Frage nach allen denjenigen Punkten der Curve (1), deren Coordinaten rationale Zahlen sind, bezeichnet offenbar im wesentlichen die gleiche Aufgabe.

Zur Lösung der Aufgabe stützen wir uns auf die Abhandlung von M. NÖTHER: *Rationale Ausführung der Operationen in der Theorie der algebraischen Functionen.*[1] Den dort entwickelten Resultaten zufolge können wir zunächst, falls die Gleichung (1) vorgelegt ist, durch eine endliche Zahl von rationalen Operationen entscheiden, ob die Voraussetzung, dass das Geschlecht der Gleichung Null ist, zutrifft. Sodann ist es ebenfalls durch rationale Operationen möglich, $n - 1$ linear unabhängige ternäre ganzzahlige Formen $\varphi_1, \varphi_2, \ldots, \varphi_{n-1}$ von der $(n-2)^{\text{ten}}$ Ordnung an-

[1] Mathematische Annalen, Bd. 23, S. 311 ff.

zugeben derart, dass für beliebige Parameter $\lambda_1, \lambda_2, \ldots, \lambda_{n-1}$ die Curve (1) von der Curve

$$\lambda_1\varphi_1 + \lambda_2\varphi_2 + \ldots + \lambda_{n-1}\varphi_{n-1} = 0 \tag{2}$$

in $n-2$ mit den Parametern $\lambda_1, \lambda_2, \ldots, \lambda_{n-1}$ veränderlichen Punkten geschnitten wird. Die Gleichung (2) stellt die zu der Curve (1) adjungirten Curven $(n-2)^{\text{ter}}$ Ordnung dar.

Es sei nun zur Abkürzung

$$\left\{\begin{aligned} \Phi_1 &= \lambda_{11}\varphi_1 + \lambda_{12}\varphi_2 + \ldots + \lambda_{1,n-1}\varphi_{n-1}, \\ \Phi_2 &= \lambda_{21}\varphi_1 + \lambda_{22}\varphi_2 + \ldots + \lambda_{2,n-1}\varphi_{n-1}, \\ \Phi_3 &= \lambda_{31}\varphi_1 + \lambda_{32}\varphi_2 + \ldots + \lambda_{3,n-1}\varphi_{n-1}, \end{aligned}\right. \tag{3}$$

wobei $\lambda_{11}, \lambda_{12}, \ldots, \lambda_{3,n-1}$ unbestimmte Parameter bedeuten. Transformiren wir sodann die Gleichung (1) vermöge der Formeln

$$y_1 : y_2 : y_3 = \Phi_1 : \Phi_2 : \Phi_3, \tag{4}$$

so erhalten wir eine Gleichung

$$g(y_1, y_2, y_3) = 0, \tag{5}$$

deren linke Seite eine ganzzahlige Form von y_1, y_2, y_3 und den Parametern $\lambda_{11}, \lambda_{12}, \ldots, \lambda_{3,n-1}$ ist. Ferner ergiebt die Ausführung der Transformation Formeln der Gestalt

$$x_1 : x_2 : x_3 = \Psi_1 : \Psi_2 : \Psi_3, \tag{6}$$

wo Ψ_1, Ψ_2, Ψ_3 ebenfalls ganzzahlige Formen von y_1, y_2, y_3 und den Parametern $\lambda_{11}, \lambda_{12}, \ldots, \lambda_{3,n-1}$ sind. Wir setzen diese Formen ohne einen allen gemeinsamen Theiler voraus. Die Form $g(y_1, y_2, y_3)$ ist nothwendig irreducibel und homogen von der $(n-2)^{\text{ten}}$ Ordnung in den Variabeln y_1, y_2, y_3, eine Thatsache, welche unmittelbar aus den bekannten Sätzen über die rationalen eindeutig umkehrbaren Transformationen der algebraischen Curven folgt. Wir ertheilen jetzt den Parametern $\lambda_{11}, \lambda_{12}, \ldots, \lambda_{3,n-1}$ solche ganzzahligen Werthe, dass die Form $g(y_1, y_2, y_3)$ irreducibel bleibt. Dies ist stets möglich, da diejenigen Werthe von $\lambda_{11}, \lambda_{12}, \ldots, \lambda_{3,n-1}$, für

welche $g(y_1, y_2, y_3)$ reducibel wird, gewissen algebraischen Gleichungen genügen müssen. Vermöge der Formeln (4) und (6) entspricht nunmehr jedem Punkte der Curve (1), dessen Coordinaten rationale Zahlen sind, ein ebensolcher Punkt der Curve (5) und umgekehrt. Daher ist unsere ursprüngliche Aufgabe auf die Behandlung der Gleichung $g(y_1, y_2, y_3) = 0$ zurückgeführt, welche ebenfalls ganzzahlig und vom Geschlechte Null ist, dagegen einen um zwei Einheiten geringeren Grad als $f(x_1, x_2, x_3) = 0$ besitzt.

Da die Fortsetzung dieses Verfahrens so lange möglich ist, als der Grad der Gleichung grösser ist als drei, so gelangen wir schliesslich zu einer Gleichung dritten oder zweiten Grades, je nachdem der Grad n der ursprünglichen Gleichung eine ungerade oder eine gerade Zahl ist. Eine Gleichung dritten Grades können wir aber sofort auf eine Gleichung ersten Grades reduciren. Denn eine solche Gleichung stellt eine Curve dritter Ordnung mit einem Doppel- oder Rückkehr-Punkte vor, dessen Coordinaten nothwendig rationale Zahlen sind, und diese Curve kann stets vermöge einer rationalen eindeutig umkehrbaren Transformation in eine gerade Linie übergeführt werden. Je nachdem also die Ordnung der vorgelegten Gleichung eine ungerade oder eine gerade Zahl ist, erhalten wir schliesslich eine Gleichung ersten oder zweiten Grades. Wir behandeln diese beiden Fälle gesondert.

Im ersteren Falle sei

$$l(u_1, u_2, u_3) = 0 \tag{7}$$

die erhaltene lineare Gleichung. Es lassen sich dann offenbar drei ganzzahlige lineare Formen $\omega_1, \omega_2, \omega_3$ der homogenen Parameter t_1, t_2 von der Art angeben, dass die Proportion

$$u_1 : u_2 : u_3 = \omega_1 : \omega_2 : \omega_3 \tag{8}$$

alle rationalen Lösungen der linearen Gleichung (7) liefert, wenn wir für die Parameter t_1, t_2 alle möglichen ganzen Zahlen einsetzen. Indem wir nun durch successive Anwendung der vorhin ausgeführten Transformationen zu der ursprünglich vorgelegten Gleichung (1) zurückgehen, ergiebt sich eine Proportion von der Gestalt

$$x_1 : x_2 : x_3 = \rho_1 : \rho_2 : \rho_3, \tag{9}$$

wo ρ_1, ρ_2, ρ_3 ganzzahlige Formen n^{ter} Ordnung der homogenen Variabeln t_1, t_2 bedeuten. Nach eventuellem Ausschluss einer endlichen Anzahl von Lösungen, welche wir als singuläre Lösungen bezeichnen und auf welche wir sogleich zurückkommen werden, findet man aus der Proportion (9) alle übrigen, nicht-singulären rationalen Lösungen der Gleichung (1), wenn man den Parametern t_1, t_2 alle möglichen ganzzahligen Werthe ertheilt. Es ist daher offenbar, dass wir alle nicht-singulären ganzzahligen eigentlichen Lösungen x_1, x_2, x_3 unserer Gleichung (1) erhalten, wenn wir in ρ_1, ρ_2, ρ_3 die Parameter t_1, t_2 alle möglichen Paare relativer Primzahlen annehmen lassen, und immer den grössten allen drei Zahlen gemeinsamen Theiler unterdrücken. Um jedoch zu bestimmten Formeln für diese eigentlichen Lösungen zu gelangen, bilden wir die Resultante der beiden Formen

$$\lambda_1\rho_1 + \lambda_2\rho_2 + \lambda_3\rho_3, \quad \mu_1\rho_1 + \mu_2\rho_2 + \mu_3\rho_3,$$

wo $\lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2, \mu_3$ unbestimmte Parameter bedeuten. Diese Resultante ist eine ganze ganzzahlige Function der Parameter $\lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2, \mu_3$, welche nicht identisch verschwinden kann, da die Formen ρ_1, ρ_2, ρ_3 keinen gemeinsamen Theiler besitzen. Es sei R die grösste positive ganze Zahl, welche in sämmtlichen Coefficienten jener Function aufgeht. Bedeutet dann t_1, t_2 irgend ein Paar relativer Primzahlen, so ist leicht einzusehen, dass jede in den drei Zahlen

$$\rho_1(t_1, t_2), \quad \rho_2(t_1, t_2), \quad \rho_3(t_1, t_2)$$

aufgehende Zahl ein Theiler von R sein muss. Lassen wir daher die beiden Parameter t_1 und t_2 unabhängig von einander ein vollständiges Restsystem nach dem Modul R durchlaufen, so gelangen wir durch eine einfache Schlussweise zu folgendem Resultat:

Es lässt sich ein endliches System von Formeln:

$$(10) \quad \begin{cases} x_1 = \alpha_1(\tau_1, \tau_2), & x_2 = \alpha_2(\tau_1, \tau_2), & x_3 = \alpha_3(\tau_1, \tau_2); \\ x_1 = \beta_1(\tau_1, \tau_2), & x_2 = \beta_2(\tau_1, \tau_2), & x_3 = \beta_3(\tau_1, \tau_2); \\ \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot & \cdot\;\cdot\;\cdot \\ x_1 = \varkappa_1(\tau_1, \tau_2), & x_2 = \varkappa_2(\tau_1, \tau_2), & x_3 = \varkappa_3(\tau_1, \tau_2), \end{cases}$$

aufstellen, welches alle nicht-singulären ganzzahligen eigentlichen Lösungen

der Gleichung (1) liefert, wenn man den Parametern τ_1, τ_2 alle möglichen ganzzahligen Werthe beilegt. Dabei bedeuten $\alpha_1, \alpha_2, \alpha_3, \ldots, \varkappa_1, \varkappa_2, \varkappa_3$ ganze, ganzzahlige, nicht homogene Functionen der Parameter τ_1, τ_2.

Die bisherigen Entwicklungen beruhten wesentlich auf dem Umstande, dass die benutzten Transformationen eindeutig umkehrbar sind. Da diese Eindeutigkeit jedoch in den singulären Punkten der Curve (1) eine Ausnahme erfährt, so bedürfen diese Punkte noch einer besonderen Untersuchung. Die singulären Punkte entsprechen den gemeinsamen Lösungen der drei Gleichungen

$$\frac{\partial f}{\partial x_1} = 0, \qquad \frac{\partial f}{\partial x_2} = 0, \qquad \frac{\partial f}{\partial x_3} = 0, \tag{11}$$

und es kann daher stets durch eine endliche Anzahl rationaler Operationen entschieden werden, ob unter ihnen solche vorhanden sind, deren Coordinaten rationale Werthe besitzen. Die so gefundenen »singulären« Lösungen der diophantischen Gleichung (1) werden nicht nothwendig auch durch die Formeln (10) erhalten, wie sich leicht durch Beispiele zeigen lässt.

Wenn zweitens der Grad n der vorgelegten Gleichung eine gerade Zahl ist, so werden wir, wie oben gezeigt worden ist, auf eine quadratische Gleichung

$$q(u_1, u_2, u_3) = 0 \tag{12}$$

geführt. Wir können dann diese Gleichung stets durch eine lineare Transformation mit rationalen Zahlencoefficienten in die Gestalt

$$a_1 u_1^2 + a_2 u_2^2 + a_3 u_3^2 = 0 \tag{13}$$

bringen, wo a_1, a_2, a_3 sämmtlich ohne einen quadratischen Theiler und paarweise relative Primzahlen sind. Bekanntlich besitzt diese Gleichung (13) ganzzahlige Lösungen dann und nur dann, wenn a_1, a_2, a_3 nicht alle dasselbe Vorzeichen haben, und die Zahlen $-a_2a_3$, $-a_3a_1$, $-a_1a_2$ beziehungsweise quadratische Reste der Zahlen a_1, a_2, a_3 sind.[1]

---

[1] LEGENDRE: *Théorie des nombres,* 3me éd. T. I. §§ III, IV. (Deutsch von H. MASER, Leipzig 1886.) Vgl. auch LEJEUNE-DIRICHLET: *Vorlesungen über Zahlentheorie,* herausgegeben von R. DEDEKIND, 3. Aufl. § 157 des X. Supplementes.

Wenn diese Bedingungen erfüllt sind, so giebt es auf dem durch die Gleichung (13) definirten Kegelschnitte Punkte, deren Coordinaten rational sind, und wir können daher durch eine rationale eindeutig umkehrbare Transformation den Kegelschnitt in eine Gerade, oder, was dasselbe ist, die Gleichung (13) in eine lineare Gleichung überführen. An die letztere knüpfen sich sodann dieselben Betrachtungen, welche wir oben im Anschluss an die Gleichung (7) entwickelten. Es wird also auch in dem jetzt betrachteten Falle unsere diophantische Gleichung (1) eine unendliche Zahl von Lösungen besitzen, welche durch ein System von Formeln der Gestalt (10) gefunden werden, und zu welchen sich eventuell eine endliche Zahl von singulären Lösungen gesellt.

Sind jedoch die genannten Bedingungen nicht erfüllt, so besitzt der Kegelschnitt (13) keinen Punkt, dessen Coordinaten rationale Zahlen sind. Folglich giebt es dann auch auf der Curve (1) keinen solchen Punkt, es sei denn, dass von den singulären Punkten dieser Curve einer oder mehrere rationale Coordinaten besitzen. Unsere Gleichung (1) hat also jetzt entweder eine endliche Zahl von (singulären) Lösungen oder überhaupt keine Lösung, je nachdem die Gleichungen

$$\frac{\partial f}{\partial x_1} = 0, \qquad \frac{\partial f}{\partial x_2} = 0, \qquad \frac{\partial f}{\partial x_3} = 0$$

gemeinsame rationale Lösungen zulassen oder nicht. Dass von diesen beiden Möglichkeiten auch die erstere eintreten kann, dass also ein singulärer Punkt der Curve (1) rationale Coordinaten besitzen kann, ohne dass ein weiterer Punkt mit rationalen Coordinaten auf der Curve liegt, zeigt folgendes Beispiel. Es seien φ, ψ_1, ψ_2, ψ_3 vier ganzzahlige quadratische Formen, ferner l eine ganzzahlige lineare Form der Variabeln u_1, u_2, u_3. Diese Formen mögen so gewählt werden, dass der durch die Gleichung

$$\varphi = 0 \tag{14}$$

definirte Kegelschnitt keinen Punkt mit rationalen Coordinaten besitzt, dass ferner die Kegelschnitte

$$\psi_1 = 0, \qquad \psi_2 = 0 \tag{15}$$

durch die beiden Schnittpunkte von $\varphi = 0$ mit der Geraden $l = 0$ hindurchgehen, ohne mit $\varphi = 0$ zu demselben Büschel zu gehören, und dass endlich der Kegelschnitt

$$\psi_3 = 0 \tag{16}$$

die genannten beiden Schnittpunkte nicht enthält. Offenbar können die Formen auf unendlich viele Weisen diesen Bedingungen gemäss angenommen werden. Transformiren wir nun die Gleichung (14) vermöge der Formeln

$$x_1 : x_2 : x_3 = \psi_1 : \psi_2 : \psi_3, \tag{17}$$

so erhalten wir eine ganzzahlige Gleichung

$$f(x_1, x_2, x_3) = 0, \tag{18}$$

welche eine Curve vierter Ordnung vom Geschlechte Null darstellt. Den Schnittpunkten der Geraden $l = 0$ mit dem Kegelschnitt $\varphi = 0$ entspricht ein Doppelpunkt dieser Curve vierter Ordnung, dessen Coordinaten die rationalen Werte

$$\frac{x_1}{x_3} = 0, \qquad \frac{x_2}{x_3} = 0$$

besitzen. Dagegen kann sich unter den nicht-singulären Punkten der Curve (18) keiner mit rationalen Coordinaten finden, weil einem solchen auf dem Kegelschnitt (14) ein Punkt mit ebenfalls rationalen Coordinaten entsprechen würde. Durch zweckmässige Wahl der Form ψ_3 kann man, wie wir noch bemerken wollen, nach Belieben erreichen, dass entweder nur einer oder dass jeder der singulären Punkte der Curve (18) rationale Coordinaten erhält.

Durch die vorstehende Darlegung findet die diophantische Gleichung

$$f(x_1, x_2, x_3) = 0$$

von beliebigem Grade und vom Geschlechte Null ihre vollkommene Erledigung. Wie sich dabei gezeigt hat, *besitzt eine solche Gleichung entweder keine Lösung, oder sie besitzt eine endliche Zahl von Lösungen, welche dann stets die gemeinsamen ganzzahligen Lösungen der Gleichungen* (11) *sind, oder endlich sie besitzt eine unendliche Zahl von Lösungen, welche abgesehen*

von eventuellen gemeinsamen ganzzahligen Lösungen der Gleichungen (11), *durch ein System von Formeln der Gestalt* (10) *gefunden werden.*

Wenn der Grad der Gleichung eine ungerade Zahl ist, so tritt stets der letzte Fall ein. Eine diophantische Gleichung von ungeradem Grade und vom Geschlechte Null besitzt also stets unendlich viele Lösungen.

Königsberg i. Pr. den 14. März 1889.