Sitzungsberichte

der

mathematisch-naturwissenschaftlichen Abteilung

der

Bayerischen Akademie der Wissenschaften

zu München

1930. Heft II
Mai-Julisitzung

München 1930
Verlag der Bayerischen Akademie der Wissenschaften
in Kommission des Verlags R. Oldenbourg München

Über das Kriterium der Rationalität einer algebraischen Kurve.

Von **H. Kapferer** in Freiburg i. Br.

Vorgelegt von O. Perron in der Sitzung am 31. Mai 1930.

Der äußere Anlaß zu der vorstehenden Note ist die Fermatsche Vermutung bezüglich der unendlich vielen Diophantischen Gleichungen

$$x^n + y^n = z^n, \quad n = 2, 3 \ldots \tag{1}$$

und zwar wegen einer merkwürdigen Analogie zwischen dem Inhalt der Fermatschen Aussage einerseits und einem bekannten Satz über algebraische Kurven andererseits. Während nämlich Fermat behauptet, daß die Gleichung

$$x^2 + y^2 = z^2 \tag{2}$$

die einzige sei vom Typus (1), welche in natürlichen von 0 verschiedenen Zahlen x, y, z befriedigt werden kann, ergibt sich aus einem ganz heterogenen Satz, den Clebsch[1]) 1865 aufgestellt hat, daß eben diese Gleichung (2) die einzige ist von denjenigen vom Typus (1), welche eine rationale Parameterdarstellung zuläßt. Eine solche ist z. B. diese:

$$x = u^2 - v^2; \quad y = 2uv; \quad z = u^2 + v^2, \tag{4}$$

wo u und v Parameter bedeuten. Dagegen ist also eine Identität der Art

---

[1]) A. Clebsch, Crelles Journal, Bd. 64 (1865). „Über diejenigen ebenen Kurven, deren Koordinaten rationale Funktionen eines Parameters sind".

(3) Der fragliche Satz lautet: „Diejenigen algebraischen Kurven, welche vom Geschlecht Null sind, und nur diese, lassen eine rationale Parameterdarstellung zu".

Die Kurven vom Geschlecht Null sind also identisch mit den sog. rationalen Kurven oder Unikursalkurven.

$$(5) \qquad \overset{n}{f}(u, v) + \overset{n}{g}(u, v) = \overset{n}{h}(u, v)$$

für $n > 2$ eine Unmöglichkeit, falls man unter f, g, h teilerfremde binäre Formen in u, v versteht.

Die algebraischen Tatsachen (4) und (5) haben aber auch zahlentheoretische Folgen. Zunächst sei daran erinnert, daß die Parameterdarstellung (4) die Gesamtheit der Lösungen der Diophantischen Gleichung (2) zu erfassen gestattet, daß sie also wesentlich mehr bedeutet als nur eine algebraische Angelegenheit. Darauf beruht ja auch der Eulersche[1]) elegante Beweis für die Unmöglichkeit der Diophantischen Gleichung

$$x^4 + y^4 = z^4.$$

Auf ganz derselben Grundlage aufbauend habe ich 1913[2]) die Unmöglichkeit von jeder der beiden folgenden Diophantischen Gleichungen elementar bewiesen:

$$x^6 + y^6 = z^6$$
$$x^{10} + y^{10} = z^{10}.$$

Wenn also schon im Falle $n = 2$ die Parameterdarstellung zahlentheoretisch sich verwerten läßt, so wäre doch wohl etwas Ähnliches zu erwarten im Falle $n > 2$, falls für solche $n > 2$ noch eine Parameterdarstellung existierte. Nach Clebsch ist letztere Voraussetzung unerfüllbar. Das bedeutet ein abschließendes Ergebnis auch für den Zahlentheoretiker; denn wenn die Identität (5) sogar bei beliebig komplexen Koeffizienten unmöglich ist, so ist sie a fortiori unmöglich bei rationalen Koeffizienten.

Die Unmöglichkeit der Identität (5) läßt sich glücklicherweise direkt und elementar beweisen, d. h. ohne Berufung auf den fernliegenden Satz von Clebsch. Das habe ich schon 1914[3])

[1]) Der Beweis findet sich in Eulers Algebra vom Jahre 1767, die ja fast zur Hälfte den Diophantischen Gleichungen gewidmet ist. Neuerdings ist der Beweis wiedergegeben in Landaus Vorlesungen über Zahlentheorie, III. Bd., 1927, S. 204.

[2]) H. Kapferer, „Beweis des Fermatschen Satzes für die Exponenten 6 und 10; Archiv der Mathematik und Physik, 23. Bd., 1913.

[3]) Vgl. die Rezension von Herrn Albert Fleck, Berlin, über die Abhandlung Krohs „Dühring und Fermat"; Archiv der Mathematik und Physik, 23. Bd., 1914. Der fragliche Beweis, der nur eine halbe Seite in Anspruch nimmt, wird dort, als von mir herrührend, mitgeteilt.

gezeigt. Einen andern Beweis hat mir kürzlich Herr Perron[1]) brieflich mitgeteilt. Derselbe ist schon deshalb bemerkenswert, weil er auf der spezifisch zahlentheoretischen Schlußweise der descente infinie beruht.

Jetzt erst kommen wir zum eigentlichen Thema. Wir wollen die für den Zahlentheoretiker heterogene, und auch sonst durchaus nicht einfache Schlußweise von Clebsch zum Beweis seines allgemeinen Satzes (3) ersetzen durch eine ganz einfache Betrachtung, allerdings unter Beschränkung auf singularitätenfreie Kurven. D. h. wir wünschen Beweise für die beiden folgenden Aussagen:

(A) Jede irreduzible algebraische Kurve 2. Ordnung ist rational.

(B) Jede irreduzible Kurve von höherer als 2. Ordnung ist nicht rational, falls sie keine vielfachen Punkte besitzt.

Beweis der positiven Aussage (A).

Hierzu zunächst 2 Tatsachen allgemeiner Art:

(6) Wenn 2 algebraische Kurven — als ternäre Formen geschrieben — durch lineare ternäre Transformationen in einander gegenseitig übergeführt werden können, so sind entweder beide rational oder beide nicht rational.

---

[1]) Perrons Beweis: Zerlegt man die linke Seite der angenommenen Identität

$$f^n(u, v) + g^n(u, v) = h^n(u, v)$$

in ein Produkt von n Faktoren, nämlich in $\prod_{i=1}^{n}(f - \varepsilon_i g)$, so sind je 2 der Faktoren relativ prim (weil sonst f, g, h einen gemeinsamen Teiler hätten), also jeder eine n^{te} Potenz. Da $n \geq 3$ sein soll, so gilt also jedenfalls

$$f - \varepsilon_1 g = \varphi_1^n; \quad f - \varepsilon_2 g = \varphi_2^n; \quad f - \varepsilon_3 g = \varphi_3^n.$$

Daraus folgt $\begin{vmatrix} 1, & \varepsilon_1, & \varphi_1^n \\ 1, & \varepsilon_2, & \varphi_2^n \\ 1, & \varepsilon_3, & \varphi_3^n \end{vmatrix} = 0$. Dies bedeutet aber eine neue Lösung der Identität (5) in wiederum teilerfremden Polynomen, aber von geringerem Grad (> 0).

(7) Die irreduziblen ternären Polynome 2. Ordnung haben die besondere Eigenschaft — die den ternären Polynomen höherer Ordnung fehlt[1]) — daß jede von ihnen in jede andere durch eine lineare ternäre Transformation übergeführt werden kann.

Behauptung (6) bedarf wohl keines weiteren Beweises; sie ist fast unmittelbar mit der Definition der rationalen Kurve gegeben. Zum Beweis der Behauptung (7) genügt es zu zeigen, daß man in jedem Fall auf ein und dieselbe ausgewählte irreduzible Ternärform, etwa auf $x^2 + y^2 - z^2$, gelangen kann. Dies ist aber leicht zu zeigen[2]). Nachdem aber die Kurve $x^2 + y^2 = z^2$ schon als rational bekannt ist (siehe (4)), so folgt aus (6) und (7) die Richtigkeit der Aussage (A).

Nun zum Beweis der negativen Aussage (B), auf die es uns hier hauptsächlich ankommt. Sie ist äquivalent mit folgendem ausführlicherem Satz:

---

[1]) Z. B. kann eine irreduzible C_3 mit Doppelpunkt nicht in eine C_3 ohne Doppelpunkt transformiert werden; die Vielfachheit eines Kurvenpunktes ist bekanntlich eine Invariante der betreffenden Kurve gegenüber linearen umkehrbaren Transformationen. Bei den C_2 dagegen sind Irreduzibilität und „singularitätenfrei" äquivalente Begriffe.

[2]) Die gegebene irreduzible Ternärform sei $K(x, y, z)$. Die gewünschte Transformation läßt sich aus folgenden drei aufeinanderfolgenden Transformationen zusammensetzen, von denen jede umkehrbar ist:

1. Man transformiere so, daß das Glied mit x^2 den Koeffizienten $+1$ erhält, sodaß K die Gestalt

$$x^2 + 2x(a_{12}y + a_{13}z) + b_{22}y^2 + 2b_{23}yz + b_{33}z^2$$

annimmt.

2. Man setze $x = x' - a_{12}y' - a_{13}z'$, $y = y'$, $z = z'$, sodaß also K die Gestalt

$$x'^2 + (k_1 y' + k_2 z')(k_3 y' + k_4 z')$$

annimmt; dabei ist a priori $k_1 k_4 - k_2 k_3 \neq 0$, weil sonst K einen Doppelpunkt haben, also zerfallen würde, nämlich den Doppelpunkt $x' = 0$, $k_1 z' + k_2 z' = 0$.

3. Man setze

$$k_1 y' + k_2 z' = y'' + z''$$
$$k_3 y' + k_4 z' = y'' - z'',$$

sodaß also K die gewünschte Gestalt $x''^2 + y''^2 - z''^2$ erhält.

Voraussetzungen:

1. $S(x, y, z)$ sei homogen in x, y, z, vom Grade n (nicht identisch Null).
2. $f(u, v)$, $g(u, v)$, $h(u, v)$ seien homogen in u, v, vom Grade $m > 0$, und ohne gemeinsamen Teiler.
3. $S(f, g, h)$ sei identisch Null.
4. Die Polynome S'_x, S'_y, S'_z haben keine gemeinsame nicht triviale Nullstelle (d. h. die Kurve $S = 0$ hat keinen singulären Punkt).

Behauptung: $n < 3$.

Beweis: Aus der Identität in u, v

$$S(f, g, h) = 0$$

folgt durch Differentiation nach u bzw. v

$$(8) \quad \begin{vmatrix} S'_x(f,g,h) \cdot f'_u + S'_y(f,g,h) \cdot g'_u + S'_z(f,g,h) \cdot h'_u = 0 \\ S'_x(f,g,h) \cdot f'_v + S'_y(f,g,h) \cdot g'_v + S'_z(f,g,h) \cdot h'_v = 0 \end{vmatrix}$$

Nicht alle zweireihigen Determinanten der Matrix

$$(9) \quad \begin{Vmatrix} f'_u, & g'_u, & h'_u \\ f'_v, & g'_v, & h'_v \end{Vmatrix}$$

verschwinden identisch. Denn aus $A \equiv f'_u \cdot g'_v - f'_v \cdot g'_u = 0$, würde, in Verbindung mit den Eulerschen Identitäten:

$$m \cdot f = u \cdot f'_u + v \cdot f'_v; \quad m \cdot g = u \cdot g'_u + v \cdot g'_v$$

folgen: $u \cdot A = m \cdot (f \cdot g'_v - g \cdot f'_v)$, also $f g'_v - g f'_v = 0$, und ebenso $f g'_u - g f'_u = 0$. Daher würden sich f und g nur um einen konstanten Faktor unterscheiden. Entsprechend würden sich überhaupt die drei Polynome f, g, h nur um konstante Faktoren unterscheiden.

Letzteres ist aber unmöglich wegen Voraussetzung 2.

Damit ist (9) bewiesen.

Aus (8) und (9) folgt die Proportion:

$$(10) \quad \begin{aligned} &S'_x(f,g,h) : S'_y(f,g,h) : S'_z(f,g,h) \\ &= -\begin{vmatrix} g'_u, h'_u \\ g'_v, h' \end{vmatrix} : +\begin{vmatrix} f'_u, h'_u \\ f'_v, h'_v \end{vmatrix} : -\begin{vmatrix} f'_u, g'_u \\ f'_v, g'_v \end{vmatrix} \end{aligned}$$

(11) Die drei Polynome links in (10) — sogar je zwei von ihnen, bei geeigneter Transformation des Ausgangspolynoms $S(x, y, z)$, wovon wir aber hier keinen Gebrauch machen — haben keinen gemeinsamen Teiler. Denn andernfalls wäre mindestens ein linearer Teiler $u - c \cdot v$ ihnen gemeinsam.

Setzt man dann

$$f(c, 1) = \alpha, \quad g(c, 1) = \beta, \quad h(c, 1) = \gamma,$$

so wäre $(\alpha, \beta, \gamma) \neq (000)$ infolge Voraussetzung 2. Es wäre also (α, β, γ) eine nicht triviale gemeinsame Nullstelle der drei Polynome $S'_x(x, y, z)$, $S'_y(x, y, z)$, $S'_z(x, y, z)$, entgegen der Voraussetzung 4. Somit ist (11) bewiesen. Aus (10) und (11) folgt sodann das simultane System:

$$\begin{aligned} h'_u \cdot g'_v - h'_v \cdot g'_u &= k(u, v) \cdot S'_x(f, g, h) \\ f'_u \cdot h'_v - f'_v \cdot h'_u &= k(u, v) \cdot S'_y(f, g, h) \\ g'_u \cdot f'_v - g'_v \cdot f'_u &= k(u, v) \cdot S'_z(f, g, h), \end{aligned} \tag{12}$$

wobei $k(u, v)$ eine wegen (9) nicht identisch verschwindende Binärform in u, v ist. Die Gradvergleichung in (12) verlangt

$$\begin{aligned} 2m - 2 &\geqq m \cdot (n - 1), \\ -2 &> m \quad (n - 3), \\ \text{also} \quad n &< 3; \qquad \text{w.z.b.w.} \end{aligned}$$