Anwendungen der Theorie der algebraischen Funktionen in der Zahlentheorie.

Von

H. Hasse.

Die Theorie der algebraischen Funktionen beschäftigt sich mit der Untersuchung der durch algebraische Gleichungen

$$f(x,y) \equiv a_{00} + a_{10}\,x + a_{01}\,y + \cdots + a_{mn}x^m y^n = 0$$

in zwei Unbestimmten x, y gegebenen Gebilde. Faßt man die Unbestimmten x, y als die Koordinaten eines Punktes der Ebene auf, so stellt sich ein solches Gebilde als eine ebene algebraische Kurve dar. Die algebraischen Kurven zeichnen sich unter allen Kurven überhaupt durch eine Fülle von eigenartigen Gesetzlichkeiten aus, die sich auf ihre Gestaltsverhältnisse im Großen, auf das Vorkommen besonderer Punkte wie Doppelpunkte, Wendepunkte, Spitzen, sowie auf ihre Schnittpunkte mit anderen algebraischen Kurven beziehen. Diese Gesetzlichkeiten haben von jeher das Interesse der Geometer auf sich gezogen. Man hat zwei große Theorien entwickelt, die algebraische Geometrie und die Theorie der algebraischen Funktionen, in denen Fragen der genannten Art von allgemeinen Gesichtspunkten aus erschöpfend behandelt werden. In der ersteren Theorie steht die Auffassung des Gebildes als algebraische Kurve im Vordergrund, in der letzteren die Auffassung von etwa y als unentwickelte algebraische Funktion der Veränderlichen x. Der Natur der Fragestellungen entsprechend werden in beiden Theorien die Unbestimmten x, y als reelle oder besser gleich komplexe Zahlveränderliche angesehen, und es werden die in der Funktionenlehre entwickelten Methoden, die auf dem Begriff der stetigen Veränderlichkeit fußen, wie z. B. die Methoden der Differential- und Integralrechnung, weitgehend herangezogen.

Es gibt aber auch eine ganz andere Art von Fragestellungen über die algebraischen Gleichungen in zwei Unbestimmten, nämlich solche von zahlentheoretischer Natur. Man setzt dabei die Koeffizienten a_{ij} der gegebenen Gleichung $f(x,y) = 0$ nicht als beliebige reelle oder komplexe Zahlen sondern als rationale und ohne Einschränkung sogar ganze Zahlen voraus und betrachtet unter allen reellen oder komplexen Wertepaaren x, y mit $f(x, y) = 0$ nur die rationalzahligen. Anstelle also z. B. die volle Kreislinie

$$x^2 + y^2 = 1$$

zu betrachten, greift man nur die rationalzahligen Wertepaare

$$x = \frac{p}{r}, \qquad y = \frac{q}{r} \quad (p, q, r \text{ ganze Zahlen})$$

mit $x^2 + y^2 = 1$ heraus. Das läuft dann auf die Betrachtung der Tripel ganzer Zahlen p, q, r mit

$$p^2 + q^2 = r^2,$$

der sog. pythagoräischen Tripel hinaus. Die ihnen entsprechenden Punkte $x = \frac{p}{r}$, $y = \frac{q}{r}$ liegen auf der vollen Kreislinie $x^2 + y^2 = 1$ überall dicht, ohne doch stetig untereinander zusammenzuhängen. Allgemein ergibt sich entsprechend die Frage nach den rationalen Punkten x, y auf einer algebraischen Kurve $f(x, y) = 0$ mit rationalen Koeffizienten a_{ij}.

Man kann den Übergang zu dieser Art der Fragestellung etwa mit der modernen Entwicklung der theoretischen Physik vergleichen. In der klassischen theoretischen Physik beschreibt man das Naturgeschehen durch Beziehungen zwischen kontinuierlichen Veränderlichen. In der modernen theoretischen Physik hat man mit Hinblick auf die atomistische Struktur der Materie und der Energie diese Beschreibungsart zu ersetzen durch eine andere, in der es sich um Beziehungen zwischen diskontinuierlichen Veränderlichen handelt. Die Beschränkung auf rationale Wertepaare x, y kann als Analogon zu der Betrachtung diskontinuierlicher Veränderlicher in der Physik angesehen werden.

Die Frage nach den rationalen Punkten einer algebraischen Kurve und eine Reihe damit verwandter zahlentheoretischer Fragen ist erst in der letzten Zeit systematisch in Angriff genommen worden. Man kennt außer einer großen Reihe von Einzeltatsachen, die sich auf besondere Kurven beziehen, im wesentlichen nur zwei allgemeine Gesetzlichkeiten darüber, nämlich die Endlichkeitssätze von A. Weil und C. Siegel. Jeder algebraischen Kurve $f(x, y) = 0$ kommt eine bestimmte natürliche Zahl g, ihr Geschlecht zu, die angibt um wieviel die tatsächliche Anzahl von Doppelpunkten hinter der den Graden m, n nach größtmöglichen Anzahl

$(m-1)(n-1)$ zurückbleibt. Als die einfachsten algebraischen Kurven sind die vom Geschlecht $g = 0$ anzusehen. Für sie besteht eine allgemeine Auflösung der Form

$$x = g(t), \quad y = h(t)$$

durch rationale Funktionen eines Parameters t, und man kann daraus die rationalen Punkte unmittelbar übersehen. Für die Kurven eines Geschlechts $g > 0$ gibt es keine solche allgemeine Auflösung. Der WEILsche Endlichkeitssatz sagt aus, daß es für sie eine endliche Anzahl r von g-gliedrigen Punktgruppen

$$(x_1, y_1), \ldots, (x_g, y_g)$$

gibt, die zwar nicht notwendig selbst rational sind, aber doch so beschaffen, daß ihre symmetrischen Funktionen rational sind, derart daß man aus ihnen alle ebenso beschaffenen g-gliedrigen Punktgruppen nach einem bestimmten Rechenverfahren herleiten kann. Daraus folgt insbesondere, daß man alle rationalen Punkte der Kurve aus endlich vielen (nicht notwendig rationalen) Punkten der Kurve durch ein bestimmtes Rechenverfahren herleiten kann. Der SIEGELsche Endlichkeitssatz folgert daraus weiter, daß es auf Kurven von einem Geschlecht $g > 0$ höchstens endlich viele Punkte mit sogar ganzzahligen rationalen Koordinaten x, y gibt.

Es erhebt sich dann die weitere sehr tiefliegende Frage, wie groß die Anzahl r des WEILschen Endlichkeitssatzes ist, wie groß also sozusagen das Maß für die im allgemeinen unendliche Mannigfaltigkeit der rationalen Punkte einer algebraischen Kurve von einem Geschlecht $g > 0$ ist. Darüber ist bisher gar nichts bekannt.

Die Beantwortung dieser Frage würde eine Fülle von zahlentheoretischen Ergebnissen mit sich bringen, so z. B. die Entscheidung über die berühmte Fermatsche Vermutung, daß die algebraische Kurve

$$x^n + y^n = 1$$

für $n > 2$ außer den beiden Punkten $(0,1)$, $(1,0)$ und für gerades n auch noch $(0,-1)$, $(-1,0)$ keine weiteren rationalen Punkte enthält.

Meine gegenwärtigen Arbeiten haben die Absicht, das angemessene Werkzeug für die Behandlung der genannten Frage und verwandter Fragen zu schaffen. Man muß dazu weit ausholen. Die geforderte algebraische Gleichung

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

kann ersetzt werden durch die unendlich vielen Forderungen

$$f(x, y) \equiv 0 \bmod. p$$

für alle Primzahlen p, nach dem in der modernen Zahlentheorie überall mit durchschlagendem Erfolg angewandten Prinzip: Eine ganze rationale Zahl m, die durch jede ganze rationale Zahl n oder auch nur durch jede Primzahl p teilbar ist — in Zeichen $m \equiv 0 \bmod. p$ für alle p —, ist notwendig $= 0$. Als einfachere Aufgabe bietet sich so zunächst die Behandlung einer einzelnen der unendlich vielen Kongruenzen

$$f(x, y) \equiv 0 \bmod. p$$

dar, d. h. die Frage nach der Anzahl $N_{f,p}$ derjenigen Paare ganzer Zahlen x, y, für welche $f(x, y)$ durch eine gegebene Primzahl p teilbar wird. Dabei sind Zahlpaare x, y und x', y', die sich nur um Vielfache von p unterscheiden:

$$x \equiv x', \quad y \equiv y' \quad \bmod. p,$$

als nicht wesentlich verschieden zu zählen, es wird also nach der Anzahl $N_{f,p}$ der mod. p inkongruenten Lösungen x, y gefragt.

Für die Beantwortung dieser leichteren Frage erweist es sich als notwendig, das gesamte Lehrgebäude der algebraischen Geometrie oder der Theorie der algebraischen Funktionen auf eine rein-algebraische Grundlage zu stellen, nämlich alle auf dem Begriff der stetigen Veränderlichkeit fußenden Schlußweisen daraus zu entfernen. Die Durchführung dieses Programms erfordert eine Fülle von Einzelarbeit, die zu einem beträchtlichen Teil in den letzten Jahren geleistet worden ist. Es ist klar, daß durch die Entfernung eines so anschaulichen und wirkungsvollen Hilfsmittels, wie es der Begriff der stetigen Veränderlichkeit ist, sowohl für den Geometer als auch für den Funktionentheoretiker wesentliche und geradezu bestimmende Züge der Theorie verloren gehen. Dabei muß man sich aber vor Augen halten, daß die Absicht nicht eine neue Begründung der geometrischen oder funktionentheoretischen Theorie ist, sondern daß es sich in erster Linie um Anwendungen auf zahlentheoretische Fragestellungen handelt.

Bei der weiteren Verfolgung des genannten Zieles stellt sich ein ganz andersartiger merkwürdiger Zusammenhang mit funktionentheoretischen Dingen heraus. Die Größe der Abweichung der Anzahl $N_{f,p}$ von ihrem wahrscheinlichen Wert p, also die Größe des Absolutwertes $|N_{f,p} - p|$ steht in engem Zusammenhang mit der Lage der Nullstellen einer durch f und p bestimmten analytischen Funktion $\zeta_{f,p}(s)$ in der komplexen s-Ebene, und zwar ganz analog, wie nach RIEMANN die Größe der Abweichung der Primzahlanzahl $\pi(x)$ von 2 bis zur Grenze x hin von ihrem wahrscheinlichen Wert $\int\limits_2^x \frac{du}{\log u}$, also der Absolutwert $\left|\pi(x) - \int\limits_2^x \frac{du}{\log u}\right|$ eng mit der Lage der Nullstellen der RIEMANNschen Zetafunktion

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots\cdot$$

in der komplexen s-Ebene zusammenhängt. RIEMANN hat vermutet, daß für seine Zetafunktion alle komplexen Nullstellen den reellen Teil $\frac{1}{2}$ haben. Dies ist gleichwertig damit, daß die Abweichung für die Anzahl der Primzahlen von der Größenordnung $\sqrt{x} \log x$ ist. Die Richtigkeit der entsprechenden Vermutung für die Funktion $\zeta_{f,p}(s)$ ist gleichwertig damit, daß die oben erklärte Abweichung $|N_{f,p} - p|$ von der Größenordnung $\sqrt{p}$ ist.

Während nun aber die berühmte RIEMANNsche Vermutung selbst bisher allen Beweisversuchen getrotzt hat und als mit den heutigen Hilfsmitteln unangreifbar bezeichnet werden muß, erweist sich die entsprechende Vermutung für die Funktionen $\zeta_{f,p}(s)$ als durchaus zugänglich. Für den einfachsten nicht-trivialen Fall des Geschlechtes $g = 1$ ist mir der Beweis bereits vor einigen Jahren gelungen, und zwar gerade durch den oben erwähnten Prozeß der Entfernung aller Stetigkeitsschlüsse aus der Theorie der Kurven vom Geschlecht $g = 1$, oder — in funktionentheoretischer Auffassung — aus der Theorie der elliptischen Funktionen. Dieser Prozeß ist in der letzten Zeit so weit fortgeschritten, daß nun auch der Beweis für $g > 1$ in handgreifliche Nähe gerückt ist.

Damit ist dann allerdings erst ein erster Schritt in Richtung auf das Endziel, die Beherrschung der rationalen Punkte algebraischer Kurven getan. Es bleibt als wesentliche weitere Aufgabe die Zusammenfügung der für die einzelnen Kongruenzen $f(x, y) \equiv 0 \bmod. p$ gewonnenen Erkenntnisse zu solchen für die Gleichung $f(x, y) = 0$. Nicht nur in der weiteren Verfolgung dieses Ziels, sondern auch in mannigfachen anderen zahlentheoretischen Anwendungen der Theorie der algebraischen Funktionen, z. B. solchen auf die Theorie der algebraischen Zahlen, bietet sich ein reiches Feld für weitere Forschung.