ÜBER DIE RIEMANNSCHE VERMUTUNG IN FUNKTIONENKÖRPERN

Von H. HASSE, Göttingen.

Einleitung.

Eine Reihe neuerer zahlentheoretischer Untersuchungen beschäftigt sich mit Fragestellungen, die an eine irreduzible algebraische Gleichung

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

in zwei Unbestimmten mit rationalen Koeffizienten anknüpfen.

Vom Standpunkte des Zahlentheoretikers kann als letztes Ziel dieser Untersuchungen die Frage nach den ganzzahligen Lösungspaaren (a, b) einer solchen Diophantischen Gleichung angesehen werden. Anders ausgedrückt also die Frage nach den Gitterpunkten (a, b) auf einer algebraischen Kurve $f(x, y)=0$.

Darüber hat vor einigen Jahren Siegel einen tiefliegenden Satz bewiesen. Er hat nämlich gezeigt, daß es im allgemeinen nur endlich viele solche ganzzahligen Lösungen gibt. Nur wenn die Gleichung das Geschlecht 0 hat, kann es sein, daß es unendlich viele ganzzahlige Lösungen gibt; die beiden wesentlichen Typen dafür sind die linearen Gleichungen (Geraden) und die indefiniten quadratischen Gleichungen (Hyperbeln).

Dieser Siegelsche Satz stellt aber doch nur eine erste Annäherung an das dar, was man als Zahlentheoretiker wissen möchte. Ziehen wir zu unserer Orientierung den Spezialfall der quadratischen Gleichungen

$$Q(x, y) - m = 0$$

heran, wo $Q(x, y)$ eine quadratische Form mit ganzen rationalen Koeffizienten und m eine ganze rationale Zahl ist. Über die bloße — hier leicht entscheidbare — Frage hinaus, ob es nur endlich oder unendlich viele ganzzahlige Lösungen gibt (Darstellungen von m durch Q), liegt hier eine umfangreiche arithmetische Theorie vor, die über die Lösbarkeit zu entscheiden gestattet und auch die Lösungsanzahl, wenn sie endlich ist, arithmetisch auszudrücken gestattet. Darüber — und über die Verallgemeinerung auf quadratische Formen einer beliebigen Anzahl von Unbestimmten — hat ja der gestrige Vortrag von Siegel berichtet. Analoge genauere arithmetische Einsichten möchte man auch bei der allgemeinen binären Diophantischen Gleichung $f(x, y)=0$ haben. Siegels Endlichkeitssatz kann als ein analytisches Resultat bezeichnet werden, wie auch sein Beweis hervortreten läßt, der tiefliegende Hilfsmittel aus der Analysis heranzieht. Der Zahlentheoretiker möchte gerne genauere und nach Möglichkeit reinarithmetisch begründete arithmetische Einsichten haben.

Betrachtet man den Spezialfall der quadratischen Formen etwas genauer, so ist allerdings zu sagen, daß hier die genannten genaueren arithmetischen Einsichten über die Lösbarkeit und die Lösungsanzahl sich nicht direkt auf die eigentlich erstrebte ganzzahlige Lösbarkeit beziehen, sondern auf einen Zwischenbegriff zwischen „ganzzahliger Lösbarkeit" and „rationalzahliger Lösbarkeit", den man nach Artin „quasiganzzahlige Lösbarkeit" nennt, und der bedeutet, daß bei den rationalzahligen Lösungen beliebig vorgegebene endlich viele Primzahlen im Nenner vermeidbar sind. Das liegt an folgendem: Jedem der genannten drei Lösbarkeitsbegriffe entspricht eine adäquate Klasseneinteilung der quadratischen Formen: ganzzahlige Klassen, quasiganzzahlige Klassen, rationalzahlige Klassen. Für die rationalzahligen Klassen gibt es ein vollständiges arithmetisches Invariantensystem, das im Wesentlichen aus quadratischen Restcharakteren in Form von Hilbertschen Normenrestsymbolen besteht; darüber handeln meine Anfängerarbeiten. Auch für die feineren quasiganzzahligen Klassen gibt es noch ein solches vollständiges arithmetisches Invariantensystem, das im Wesentlichen aus quadratischen Restcharakteren in Form von Legendreschen Restsymbolen besteht; es sind das die von H. J. St. Smith und Minkowski allgemein eingeführten Geschlechtscharaktere, und es ist das Verdienst dieser beiden Forscher, erkannt zu haben, daß sich die Geschlechter quadratischer Formen auch durch die einfache Deutung als quasiganzzahlige Klassen in ein dem Erlanger Programm ähnliches gruppentheoretisches Schema einbauen lassen. Dagegen gibt es für die noch feineren ganzzahligen Klassen kein solches vollständiges arithmetisches Invariantensystem mehr; die quasiganzzahligen Klassen sind vielmehr die engsten, die noch rein-arithmetisch beschreibbar sind. Zur Hervorhebung einer ganzzahligen Klasse aus ihrem Geschlecht bedarf es der wesentlich analytischen Reduktionstheorie.

Merkwürdigerweise ist die historische Entwicklung bei den quadratischen Formen genau umgekehrt gegangen, wie es methodisch dem Fortschritt von einfacherem zu komplizierterem entspricht:

Historisch: ganzzahlig, quasiganzzahlig, rationalzahlig.
Methodisch: rationalzahlig, quasiganzzahlig, ganzzahlig.

Und ebenso ist jetzt auch Siegels Resultat über die Endlichkeit der ganzzahligen Lösungsanzahl von $f(x,y)=0$ einer noch ausstehenden genauen arithmetischen Theorie zunächst einmal der rationalzahligen Lösbarkeit von $f(x,y)=0$ vorangegangen. Allerdings stützt sich Siegel doch auf einen ganz entsprechenden Endlichkeitssatz über die rationalzahligen Lösungen von $f(x,y)=0$, der im Spezialfall des Geschlechtes 1 bereits von Mordell gefunden war, für beliebiges Geschlecht $g \geqq 1$ dann von A. Weil bewiesen wurde, und zwar wieder mit tiefliegenden analytischen Hilfsmitteln:

Man betrachte die Systeme von je g konjugierten algebraischen Lösungen

$$(a_i, b_i) \qquad (i=1, \cdots, g)$$

deren symmetrische Funktionen also rational sind. Diese Systeme bilden im Sinne des zur Gleichung $f(x,y)=0$ gehörigen Abelschen Additionstheorems der g-gliedrigen Lösungssysteme einen endlichen Modul; bildet man also die g-gliedrigen Systeme (a_i, b_i) durch ein System von g Integralen erster Gattung $\int du_j$ in das Periodenparallelotop ab:

$$\sum_i \int_{(a_{i0}, b_{i0})}^{(a_i, b_i)} du_j \equiv u_j \text{ mod. Per., } (a_{i0}, b_{i0}) \text{ festes Lösungssystem,}$$

so bilden die entsprechenden Punkte (u_j) dort einen endlichen Modul. Natürlich sind unter den konjugierten algebraischen Lösungen speziell auch die rationalen Lösungen enthalten, sodaß der Satz von A. Weil insbesondere auch eine Endlichkeitsaussage über diese liefert.

Nach dem oben über quadratische Formen Gesagten wird man zunächst einmal eine genauere arithmetische Einsicht in diesen die rationalen Lösungen betreffenden Sachverhalt anstreben. Auch hinsichtlich der Methodik dafür gibt die Theorie der quadratischen Formen einen Anhalt. Dort zeigt sich nämlich, daß man das vollständige Invariantensystem für die rationalen Klassen einfach erhält, wenn man die vollständigen Invariantensysteme für die p-adischen Klassen für alle Primzahlen p (inkl. p_∞) zusammenfaßt. Ferner bedeutet die Untersuchung der fraglichen Gleichung in einem p-adischen Körper nicht anders als ihre Untersuchung als Kongruenz nach beliebig hohen Potenzen von p als Modul, und diese wiederum führt sich elementar zurück auf die Untersuchung als Kongruenz nach einer festen kleinen Potenz von p als Modul, die für fast alle p schon als p^1 genommen werden kann. Man kommt so wesentlich auf die Aufgabe zurück, die fragliche Gleichung statt im Körper R der rationalen Zahlen vielmehr im endlichen Körper P der Restklassen nach einer Primzahl p zu untersuchen. Im Falle der quadratischen Formen liefert gerade diese Untersuchung die auf p bezügliche wesentlich einzige Invariante, das Hilbertsche Normenrestsymbol.

So wird man auch für die rationalzahlige Theorie der allgemeinen binären Diophantischen Gleichung $f(x,y)=0$ als Grundlage eines späteren nach Möglichkeit ganz analogen Aufbaus zunächst einmal die Gleichung als Kongruenz nach einer Primzahl p, d. h. im endlichen Körper P der Restklassen mod. p untersuchen. Losgelöst von dem Zusammenhang, den ich vorstehend zur Motivierung dieser Fragestellung entwickelt habe, hat man dann also die folgende Frage:

Gegeben ein Polynom $f(x,y)$ über P, dessen Koeffizienten also Restklassen nach einer festen Primzahl p sind, und das über P irreduzibel ist. Man untersuche arithmetisch die Anzahl N der Lösungen (a, b) in P von

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

Dieser Frage sind meine letzten Arbeiten gewidmet. Die Frage hat auch an sich ein zahlentheoretisches Interesse. Sie wurde in Spezialfällen vor einigen Jahren von Mordell und Davenport aufgegriffen, und teilweise beantwortet. Davenport z. B. bewies, daß für

$$y^2 - f_3(x) \equiv 0 \text{ mod. } p \qquad (f_3(x) \text{ Polynom dritten Grades})$$

die Lösungsanzahl N durch

$$|N-p| \leqq cp^{\frac{3}{4}}, \quad c \text{ von } p \text{ unabhängig,}$$

abschätzbar ist, und Mordell verbesserte den Exponenten $\frac{3}{4}$ zu $\frac{2}{3}$. p ist der mittlere Wert von N; es liegt die Auffassung zugrunde, daß $f_3(x)$ ganzrationale Koeffizienten hat und alle möglichen Primzahlen p zugelassen sind. Beide Forscher vermuteten, daß der Exponent zu $\frac{1}{2}$ verbessert werden könnte, was wie man leicht sieht, der bestmögliche Wert ist. Sie konnten dies aber mit ihren der elementaren Zahlentheorie entnommenen Hilfsmittel nicht beweisen. Etwas ungläubig an der Kraft der modernen zahlentheoretischen Methoden mit ihrer starken begrifflichen Durchsetzung für elementarzahlentheoretische Fragestellungen, forderte Davenport mich heraus, damit doch wenigstens ein greifbares zahlentheoretisches Resultat zu beweisen, etwa die eben genannte Vermutung.

Das ist mir dann auch gelungen, zu meiner eigenen Freude und Genugtuung, und zur vollen Zufriedenheit meines Freundes Davenport. Es ergab sich dabei mehr, als eine bloße genaueste Abschätzung der obigen Anzahl N, nämlich eine genaue Einsicht in die algebraische Struktur der Lösungsmannigfaltigkeit.

Vom Standpunkte der obigen Fragestellung kann der Davenport-Mordellsche Spezialfall als der Fall des Geschlechts 1 charakterisiert werden, also der einfachste nicht-triviale Fall; denn den Fall des Geschlechts 0 beherrscht man mittels rationaler Uniformisierung in ganz trivialer Weise. Die von mir entwickelte Methode ist aber so allgemein, daß sie auch den Fall beliebigen Geschlechtes $g > 1$ anzugreifen gestattet. Zwar sind die Untersuchungen darüber noch nicht ganz abgeschlossen, aber ganz kürzlich hat Deuring die wesentliche Schwierigkeit, die der Verallgemeinerung von $g=1$ auf $g>1$ entgegenstand, aus dem Wege geräumt, sodaß wohl in kurzer Zeit die oben genannte Fragestellung vollständig gelöst sein wird.

Ich will im folgenden einen kurzen Überblick über die Methoden und Resultate im Falle $g=1$ geben, und dann zum Schluß auch noch kurz den zur Verallgemeinerung auf $g>1$ führenden Gedanken Deurings schildern.

Ich möchte noch bemerken, daß in einer eben erschienenen vorläufigen Mitteilung Frl. Lütz, eine Schülerin von A. Weil, die Aufgabe behandelt hat, von meinem Resultat für den Fall $g=1$ im Restklassenkörper P nach p zu der Lösungstheorie im p-adischen Zahlkörper überzugehen; doch kann ich darauf hier nicht eingehen.

Hauptteil.

1. *Der algebraische Funktionenkörper.*

Der erste Schritt für meinen Ansatz besteht darin, die ganze Fragestellung in eine algebraisch-invariante und den modernen Methoden zugängliche Form zu setzen. Er hat noch nichts mit der Beschränkung auf $g=1$ zu tun.

Die über P irreduzible Gleichung

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

definiert einen *algebraischen Funktionenkörper einer Unbestimmten*

$$K_0=P(x, y),$$

der in mannigfacher Weise durch Gleichungen über P erzeugbar ist (birationale Transformation). Ich sehe diesen Körper und nicht die zufällig zu seiner Erzeugung dienende Gleichung als das Wesentliche an. Es kann nun sein, daß $f(x, y)$ zwar über P irreduzibel ist, aber doch bei algebraischer Erweiterung von P zerfällt. Sei k_0 der über P endliche Körper der Koeffizienten eines der algebraisch konjugierten absolut-irreduziblen Faktoren $f_0(x, y)$ von $f(x, y)$. Dann stellt sich K_0 auch so dar:

$$K_0=k_0(x, y) \text{ mit } f_0(x, y)=0.$$

k_0 ist dabei ein endlicher Körper von einer Elementanzahl $q=p^f$; er heißt der *Konstantenkörper* von K_0; invariant ist er definiert als die algebraisch-abgeschlossene Hülle von P in K_0. Die in der Einleitung gestellte Frage nach der Lösungsanzahl N von $f(x, y)=0$ reduziert sich dann elementar auf die Frage nach der Lösungsanzahl N_0 von $f_0(x, y)=0$ in k_0.

Diese Lösungsanzahl N_0 ist nun ihrer Definition nach nicht invariant dem Körper K_0 zugeordnet, sondern auf die spezielle Erzeugung von K_0 durch die Gleichung $f_0(x, y)=0$ bezogen.

Zu einer invarianten Anzahl N_1 kommt man, wenn man statt der Lösungen (a, b) von $f_0(x, y)=0$ in k_0 die Punkte $\mathfrak{p}_1$ von K_0 zählt. Dabei bezeichne ich als *Punkte* die Primdivisoren ersten Grades im Sinne der

arithmetischen Theorie der algebraischen Funktionenkörper. Diese sind das abstrakte Analogon der Punkte der Riemannschen Fläche im klassischen Fall (wo statt des endlichen Körpers k_0 der kontinuierliche Körper aller komplexen Zahlen vorliegt), und man erhält sie nach der von Dedekind-Weber gegebenen rein-arithmetischen Definition als die homomorphen Abbildungen des Körpers K_0 auf seinen Konstantenkörper. Jedem Punkte $\mathfrak{p}_1$ von K_0 (von denjenigen abgesehen, für die eine der beiden Erzeugenden x, y unendlich wird) entspricht eindeutig eine Lösung (a, b) in k_0 der Grundgleichung $f_0(x, y)=0$, auf Grund der Relation

$$(x, y)\equiv(a, b) \text{ mod. } \mathfrak{p}_1 ,$$

für die ich auch einfach

$$(x\mathfrak{p}_1, y\mathfrak{p}_1)=(a, b)$$

schreibe, um die Analogie zur Bildung des Funktionenwertes der algebraischen Funktionen x, y im Punkte $\mathfrak{p}_1$ im klassischen Fall anzudeuten. Von Nullstellen der Diskriminante der Grundgleichung abgesehen ist diese Beziehung auch umkehrbar eindeutig. Die Anzahl N_1 der Punkte von K_0 ist also der invariante Ersatz für die von der Wahl der Grundgleichung abhängige Lösungsanzahl N_0. Auf Grund des besprochenen Zusammenhangs ist es in jedem Einzelfalle leicht, aus einer Aussage über N_1 eine solche über N_0 zu gewinnen. Für N_1 erscheinen die uns interessierenden Aussagen in ihrer formal einfachsten Gestalt, während die Formulierung für N_0 nebensächliche Umständlichkeiten hereinbringen würde.

Als mittlerer Wert für N_1 ist $q+1$ anzusehen, entsprechend den $q+1$ Werten für x in k_0 inkl. ∞.

Unsere Fragestellung ist damit auf folgende invariante Form gebracht:

Gegeben ein endlicher Körper k_0 von $q=p^f$ Elementen, und ein absolut-irreduzibles Polynom $f_0(x, y)$ über k_0. Es soll die Anzahl N_1 der Punkte (Primdivisoren ersten Grades) des algebraischen Funktionenkörpers

$$K_0=k_0(x, y) \text{ mit } f_0(x, y)=0$$

arithmetisch untersucht werden, insbesondere die Größe ihrer Abweichung vom mittleren Werte $q+1$ abgeschätzt werden.

Im Davenport-Mordellschen Fall

$$y^2-f_3(x)=0$$

ist übrigens $k_0=P$ und einfach

$$N_1=N_0+1=N+1 ,$$

sodaß also hier

$$|N_1-(q+1)| = |N_0-q| = |N-p|$$

ist.

2. *Zusammenhang mit der Zetafunktion von K_0. Riemannsche Vermutung.*

Für K_0 läßt sich eine *Zetafunktion* definieren:

$$\zeta(s)=\prod_{\mathfrak{p}_n}\frac{1}{1-\frac{1}{\mathfrak{N}\mathfrak{p}_n^s}}=\prod_{n=1}^{\infty}\left(\frac{1}{1-\frac{1}{q^{ns}}}\right)^{N_n}=1+\frac{N_1}{q^s}+\cdots,$$

wo $\mathfrak{p}_n$ alle Primdivisoren beliebigen Grades n von K_0 durchläuft und N_n deren Anzahlen für die einzelnen Grade n bezeichnet. Diese Zetafunktion zerspaltet sich in ein Produkt:

$$\zeta(s)=\zeta_0(s)\,L(s),$$

wo $\zeta_0(s)$ die Zetafunktion eines rationalen Teilkörpers $k_0(x)$ von K_0 ist (nicht von x abhängig, daher als *Zetafunktion zum Geschlecht* 0 *über* k_0 invariant beschrieben):

$$\zeta_0(s)=\frac{1}{1-\frac{1}{q^s}}\,\frac{1}{1-\frac{q}{q^s}}=1+\frac{q+1}{q^s}+\cdots,$$

und

$$L(s)=1+\frac{N_1-(q+1)}{q^s}+\cdots+\frac{q^g}{q^{2gs}}$$

ein Polynom vom Grade $2g$ in $\frac{1}{q^s}$ ist; dabei ist g das in der arithmetischen Theorie von K_0 (aus der Verzweigungstheorie oder aus dem Riemann-Rochschen Satz) definierte Geschlecht von K_0.

$\zeta_0(s)$ ist nullstellenfrei, $L(s)$ besitzt genau $2g$ Nullstellen ω_i in q^s:

$$L(s)=\prod_{i=1}^{2g}\left(1-\frac{\omega_i}{q^s}\right).$$

Für sie gilt:

$$N_1-(q+1)=-\sum_{i=1}^{2g}\omega_i.$$

Damit ist bereits eine arithmetische Darstellung der gesuchten Abweichung $N_1-(q+1)$ gegeben.

Die Riemannsche Vermutung für $L(s)$ besagt:

$$|\omega_i|=q^{\frac{1}{2}},$$

d. h. der Realteil der $2g$ Serien von Nullstellen in s, die periodisch mit der Periode $\frac{2\pi i}{\log q}$ angeordnet sind, ist $\frac{1}{2}$. Sie bedeutet die genaue Abschätzung:

$$|N_1-(q+1)|\leqq 2g\sqrt{q}.$$

Mann kann umgekehrt zeigen, daß aus dieser Abschätzung für N_1 die Riemannsche Vermutung folgt. Man muß dazu nur die fragliche Abschätzung für jeden endlichen Erweiterungskörper von k_0 zugrundelegen:

$k_0^{(r)}$ der endliche Körper von q^r Elementen; Grad r über k_0

$N_1^{(r)}$ die Anzahl der Punkte von $K_0^{(r)}=k_0^{(r)}(x, y)$

$$|N_1^{(r)}-(q^r+1)|\leqq 2g\sqrt{q^r}.$$

Man sieht nämlich leicht, daß einfach

$$L^{(r)}(s)=\prod_{i=1}^{2g}\left(1-\frac{\omega_i^r}{q^{rs}}\right)$$

$$N_1^{(r)}-(q^r+1)=-\sum_{i=1}^{2g}\omega_i^r$$

ist.

Speziell für $g=1$ wird $L(s)$ das quadratische Polynom

$$L(s)=1+\frac{N_1-(q+1)}{q^s}+\frac{q}{q^{2s}}=\left(1-\frac{\omega}{q^s}\right)\left(1-\frac{\bar{\omega}}{q^s}\right),$$

und die Riemannsche Vermutung läuft auf den Nachweis hinaus, daß die beiden Nullstellen ω, $\bar{\omega}$ konjugiert-komplex (oder höchstens im Grenzfall reell und gleich, d. h. rational) sind, aber nicht reell und verschieden (d. h. reell irrational).

3. *Die Struktur der Gesamtheit aller algebraischen Punkte von* K_0.

Wie die Primdivisoren ersten Grades $\mathfrak{p}_1$ von K_0 im wesentlichen den in k_0 rationalen Lösungen (a, b) einer Grundgleichung $f_0(x, y)=0$ entsprechen, so entsprechen die Primdivisoren n-ten Grades $\mathfrak{p}_n$ den Systemen algebraisch-konjugierter Lösungen (a_i, b_i) vom Grade n über k_0. Erweitert man dementsprechend den Grundkörper k_0 auf seine algebraisch-abgeschlossene Hülle k (das sogen. unendliche Galoisfeld mod. p) und bildet demgemäß den algebraischen Funktionenkörper

$$K=k(x, y) \text{ mit } f_0(x, y)=0,$$

so lösen sich die Primdivisoren n-ten Grades $\mathfrak{p}_n$ von K_0 in je n Primdivisoren ersten Grades von K auf. Die Punkte von K können in diesem Sinne als die *algebraischen Punkte von* K_0 aufgefaßt werden. Die Erweiterung von $K_0|k_0$ zu $K|k$ entspricht ungefähr dem, daß man in der klassischen Theorie der algebraischen Funktionen von vornherein den Körper aller komplexen Zahlen als Konstantenkörper zugrundegelegt, auch wenn die Grundgleichung etwa rationale oder algebraische Koeffizienten hat; übrigens bemerken bereits Dedekind-Weber, daß ihr rein-arithmetischer Aufbau dieser klassischen Theorie genau so gut geht, wenn man nur den Körper aller algebraischen Zahlen als Konstantenkörper zugrundelegt, was dann das genaue Analogon zu der obigen Erweiterung darstellt.

Wir werden nun die zu untersuchenden *rationalen Punkte* $\mathfrak{p}_1$ von K_0 dadurch bestimmen, daß wir sie innerhalb der Gesamtheit aller algebraischen Punkte von K_0, d. h. aller Punkte $\mathfrak{p}$ von K, durch einen gruppentheoretischen Mechanismus herausheben.

Dazu muß zunächst die Gesamtheit der algebraischen Punkte $\mathfrak{p}$ auf ihre algebraische Struktur hin untersucht werden. Man kann das nach Analogie mit dem klassischen Fall auch die Bestimmung der Struktur der Riemannschen Fläche von K nennen.

Von jetzt ab sei $g=1$ vorausgesetzt. Dann läßt sich die Gesamtheit der Punkte $\mathfrak{p}$ von K zu einer additiven abelschen Gruppe $\mathfrak{A}$ machen. Wählt man nämlich einen Punkt $\mathfrak{o}$ fest aus — er entspricht dem Unendlichen bei der Weierstraßschen Normierung der Riemannschen Fläche eines elliptischen Funktionenkörpers, also dem Nullpunkt der universellen Überlagerungsfläche (Ebene des Integrals erster Gattung u) —, so lassen sich die Divisorenklassen nullten Grades von K eindeutig durch die Quotienten $\frac{\mathfrak{p}}{\mathfrak{o}}$ repräsentieren, und die Klassenmultiplikation:

$$\frac{\mathfrak{p}}{\mathfrak{o}}\,\frac{\mathfrak{p}'}{\mathfrak{o}} \sim \frac{\mathfrak{p}''}{\mathfrak{o}} \left(\text{d. h. } \frac{\mathfrak{p}\mathfrak{p}'}{\mathfrak{o}\mathfrak{p}''} \cong s = \text{Element in } K\right)$$

liefert eine formale Punktaddition:

$$\mathfrak{p}+\mathfrak{p}'=\mathfrak{p}''$$

und macht damit die Gesamtheit der Punkte $\mathfrak{p}$ von K zu einer additiven abelschen Gruppe $\mathfrak{A}$ mit $\mathfrak{o}$ als Nullelement, die ich *die auf* $\mathfrak{o}$ *bezogene Additionsgruppe der Punkte* $\mathfrak{p}$ *von* K nennen will. Sie ist isomorph zur Gruppe $\mathfrak{D}$ der Divisorenklassen nullten Grades von K.

In dieser Gruppe $\mathfrak{A}$ haben nun alle Punkte $\mathfrak{p}$ endliche Ordnung; denn entspricht $\mathfrak{p}$ einem Punkte $\mathfrak{p}_n$ von K_0, so ist $\mathfrak{p}$ bereits ein rationaler Punkt in $K_0^{(n)} = k_0^{(n)}(x, y)$, und diese bilden eine endliche Untergruppe $\mathfrak{U}_n$ von $\mathfrak{A}$.

Insbesondere bilden auch die rationalen Punkte $\mathfrak{p}_1$ von K_0 (die den zugehörigen Punkten von K umkehrbar eindeutig entsprechen) eine endliche Untergruppe $\mathfrak{U}_1$ von $\mathfrak{A}$. Die Hervorhebung dieser Untergruppe $\mathfrak{U}_1$ ist gerade unsere Aufgabe.

Eine eingehende Untersuchung ergibt nun, daß die Gruppe $\mathfrak{A}$ isomorph ist zur Additionsgruppe gewisser rationaler Teilpunkte eines abstrakten Periodenparallelogramms, dessen Relativkoordinaten mit u_1, u_2 bezeichnet seien, nämlich zur Additionsgruppe aller rationalen Zahlpaare (u_1, u_2) mod. 1, wo u_1 beliebigen Nenner hat, u_2 aber nur zu p primen Nenner. Für gewisse ausgeartete Körper K ist auch der Nenner von u_1 noch auf zu p prime Zahlen beschränkt.

Man beweist dies dadurch, daß man zeigt: Die Anzahl der Lösungen von $n\mathfrak{p}=\mathfrak{o}$ in der Gruppe $\mathfrak{A}$ ist gleich

n^2 für $n \not\equiv 0$ mod. p

n oder 1 für $n=p$-Potenz (je nachdem eine gewisse Invariante A von K die Eigenschaft $A \neq 0$ oder $A=0$ hat).

Es ist zu vermuten, daß ein ganz entsprechender Satz auch für beliebiges Geschlecht g gilt, mit n^{2g} statt n^2 im Falle $n \not\equiv 0$ mod. p und n^r $(0 \leqq r \leqq g)$ im Falle $n=p$-Potenz, wo r der Rang einer gewissen g-reihigen Matrixinvariante A von K ist.

Die einzige Abweichung gegenüber dem klassischen Fall besteht also darin, daß hier, der Charakteristik p des Konstantenkörpers k entsprechend, die Anzahl der p-ten Teilpunkte des Periodenparallelogramms nur p oder gar 1 statt p^2 ist, daß also für den p-Bestandteil der Punktgruppe die Struktur der Riemannschen Fläche nicht zweidimensional sondern nur ein- oder gar nulldimensional ist.

4. *Herausheben der rationalen Punkte von K_0.*

Dies geschieht auf Grund der folgenden einfachen algebraischen Charakterisierung der Elemente von k_0 unter allen Elementen a von k:

$$a^q = a\,.$$

Die in k_0 rationalen Lösungen sind also unter allen Lösungen (a, b) durch die Relation

$$(a^q, b^q) = (a, b)$$

charakterisiert.

Geht man von den Lösungen (a, b) in k zu den Punkten $\mathfrak{p}$ von K über, so wird man darauf geführt, jedem Punkte $\mathfrak{p}$ von K einen neuen Punkt $\pi\mathfrak{p}$ von K zuzuordnen auf Grund der Relation:

$$(x, y) \equiv (a^q, b^q) \bmod \pi\mathfrak{p},$$

$$\text{wenn } (x, y) \equiv (a, b) \bmod \mathfrak{p}.$$

Es liegt nun nahe, diese zunächst an die Grundgleichungslösungen geknüpfte Definition der Operation π in der Punktgruppe $\mathfrak{A}$ auf eine invariante begriffliche Art einzuführen.

Denkt man nämlich an die Uniformisierung der bei Geschlecht 1 erreichbaren Weierstraßschen Normalform

$$y^2 = f_3(x) = 4x^3 - g_2 x - g_3$$

durch elliptische Funktionen

$$x = \wp(u), \qquad y = \wp'(u)$$

im klassischen Falle, so weiß man ja aus der komplexen Multiplikation folgendes: Ist das Periodenverhältnis imaginär-quadratisch — Bedingung dafür ist eine gewisse algebraische Gleichung für die absolute Invariante $J = \frac{g_2^3}{\Delta}$, die sich bekanntlich mod. p auf eine Gleichung der Form $J^q = J$ reduziert; hier ist das formal erfüllt, weil J in k_0 liegt —, so gilt für die auf die Dimension 0 normierte $\wp$-Funktion $\tau(u) = \frac{g_2 g_3}{\Delta} \cdot \wp(u)$ eine Kongruenz der Form

$$\tau(\pi u_0) \equiv \tau(u_0)^q \bmod \mathfrak{P},$$

wo π einer der beiden konjugiert-komplexen (oder rationalen und gleichen) Faktoren aus der Zerlegung

$$q = p^f = \pi\bar{\pi}$$

im Körper Ω des Periodenverhältnisses ist und $\mathfrak{P}$ ein Primidealteiler von π im algebraischen Erweiterungskörper $\Omega(J, \wp(u_0))$ (u_0 ein geeigneter rationaler Teilpunkt). Diese Kongruenz ist es gerade, die in der komplexen Multiplikation im Mittelpunkt steht, weil sie das Klassenkörperzerlegungsgesetz für den Teilwertkörper begründet.

Hierdurch wird man darauf geführt, die Operation π in $\mathfrak{A}$ so einzuführen, daß sie ein Analogon zur komplexen Multiplikation mit einem Faktor π von q im klassischen Falle wird. Die komplexe Multiplikation mit π bedeutet doch nun aber algebraisch ausgedrückt eine isomorphe Abbildung des elliptischen Körpers von $\wp(u)$, $\wp'(u)$ auf den Teilkörper von $\wp(\pi u)$, $\wp'(\pi u)$.

In unserem Falle liefert die Abbildung

$$k \to k \text{ elementweise}, \quad (x, y) \to (x^q, y^q)$$

ersichtlich eine isomorphe Abbildung π von

$$K = k(x, y) \text{ mit } f_0(x, y) = 0$$

auf einen Teilkörper

$$K\pi = k(x^q,\ y^q) \text{ mit } f_0(x^q,\ y^q) = 0\,,$$

weil aus der gliedweisen Potenzierbarkeit mit $q = p^f$ bei Charakteristik p und der obigen Charakterisierung von k_0 innerhalb k folgt:

$$f_0(x^q,\ y^q) = f_0^q(x^q,\ y^q) = f_0(x,\ y)^q = 0\,.$$

Wir können dann die Operation π in $\mathfrak{A}$, ohne auf die Lösungen $(a,\ b)$ zurückzugreifen, wie folgt definieren:

Zu $\mathfrak{p}$ gehört zunächst ein $\mathfrak{p}$ enthaltender Primdivisor des Teilkörpers $K\pi$, nämlich einfach die Norm $N_\pi p$ für $K \mid K\pi$. Diesen Primdivisor $N_\pi \mathfrak{p}$ bilden wir dann durch den Isomorphismus π^{-1} von $K\pi$ zurück nach K ab und erhalten so einen neuen Primdivisor

$$\pi\mathfrak{p} = (N_\pi \mathfrak{p})\ \pi^{-1}$$

von K. Man stellt leicht fest, daß die so allgemein und invariant eingeführte Operation π in der Punktgruppe $\mathfrak{A}$ gerade die obige Eigenschaft für die den Punkten zugeordneten Lösungen hat. Dies drückt sich in folgender an ein Assoziativgesetz erinnernder Form aus:

$$((x\pi)\mathfrak{p},\ (y\pi)\mathfrak{p}) = (x(\pi\mathfrak{p}),\ y(\pi\mathfrak{p}))\,.$$

Die uns interessierenden rationalen Punkte $\mathfrak{p}_1$ von K_0 sind unter allen algebraischen Punkten $\mathfrak{p}$ von K_0 gerade durch die Eigenschaft

$$\pi\mathfrak{p} = \mathfrak{p}$$

der Invarianz bei der eingeführten Operation π charakterisiert.

5. *Der Meromorphismenring von K.*

Um nun mit der Operation π auch rechnen zu können, werden wir sie, ganz analog zum klassischen Fall der komplexen Multiplikation, in einen Ring einzubetten haben, der der Gesamtheit aller komplexen Multiplikatoren entspricht. Im klassischen Fall ist das eine Ordnung aus dem imaginärquadratischen Körper Ω des Periodenverhältnisses.

Wir betrachten dazu alle *Meromorphismen* von K, d. h. alle isomorphen Abbildungen μ des Körpers K auf Teilkörper $K\mu$. Für jeden solchen läßt sich die Operation

$$\mu\mathfrak{p} = (N_\mu \mathfrak{p})\,\mu^{-1}$$

in der Punktgruppe $\mathfrak{A}$ ganz analog wie oben für den speziellen Meromorphismus π erklären. Sie entspricht einer linearen Funktion $\mu u + \alpha$ mit komplexem Multiplikator μ und beliebigem α im klassischen Fall. Wir

denken uns die μ (durch einen Translationsautomorphismus von K) immer eindeutig so normiert, daß dabei unser Bezugspunkt $\mathfrak{o}$ in sich übergeht:

$$\mu\,\mathfrak{o}=\mathfrak{o}\,.$$

Das entspricht den reinen komplexen Multiplikationen μu im klassischen Fall.

Dann zeigt sich, daß jeder solche normierte Meromorphismus eine homomorphe Abbildung der Punktgruppe $\mathfrak{A}$ *in* sich liefert:

$$\mu(\mathfrak{p}+\mathfrak{p}')=\mu\,\mathfrak{p}+\mu\,\mathfrak{p}',$$

und sogar $\mathfrak{A}$ *auf* sich abbildet, daß sie also die wesentlichen Eigenschaften einer linearen homogenen Funktion hat. Ferner bilden die μ auf Grund der einfachen Nacheinanderausführung ein multiplikativ abgeschlossenes assoziatives System. Jedem μ läßt sich eine *Norm*

$$N(\mu)=[K:K\mu]$$

zuordnen, und es gilt

$$N(\mu\,\mu')=N(\mu)\,N(\mu')\,.$$

Wesentlich ist nun, daß sich dies multiplikativ abgeschlossene System durch formale Hinzunahme einer 0 mit

$$0\,\mathfrak{p}=\mathfrak{o}\text{ für alle }\mathfrak{p}$$

und

$$N(0)=0$$

zu einem Ring M machen läßt, indem man auch eine Addition einführt. Dies geschieht auf Grund des Additionstheorems in rein-algebraischer Gestalt. Die Meromorphismen $\mu\neq 0$ entsprechen nämlich umkehrbar eindeutig den Lösungen $(x\mu,\ y\mu)$ *in* K einer in geeigneter Weise normierten Grundgleichung, und für diese hat man das Additionstheorem. Besser macht man dies, ohne auf eine Grundgleichung Bezug zu nehmen, indem man den Körper

$$\mathfrak{K}=K(\xi,\ \eta)\text{ mit }f_0(\xi,\ \eta)=0$$

vom Geschlechte 1 *über* K als formalem Konstantenkörper einführt. Dann entsprechen die μ gerade den Punkten $\mathfrak{P}$ von $\mathfrak{K}|K$, und die gesuchte Addition der μ ergibt sich einfach als die Klassenmultiplikation in $\mathfrak{K}|K$ oder also als die Addition in der zu $\mathfrak{A}$ analogen Punktgruppe von $\mathfrak{K}|K$, bei der ja die in K rationalen Punkte, wie oben gesagt, für sich eine Untergruppe bilden.

Gerade der letztere Ansatz liegt der nachher zu besprechenden Deuringschen Verallgemeinerung auf beliebiges Geschlecht $g\geqq 1$ zugrunde.

So erhält man dann den *Meromorphismenring* M von K. Er hat folgende Eigenschaften:

Er ist nullteilerfrei (wegen der Normenproduktformel), besitzt ein Einselement 1 (entsprechend dem identischen Automorphismus) und hat die Charakteristik 0, d. h. die natürlichen Vielfachen n von 1 sind in ihm von 0 verschieden (siehe unten); diese natürlichen Vielfachen entsprechen den natürlichen Multiplikationen nu im klassischen Fall.

Seine wichtigste Eigenschaft ist das Analogon der Tatsache, daß das Periodenverhältnis im klassischen Falle imaginär ist, woraus dort leicht folgt, daß es außer den ganzrationalen Multiplikatoren höchstens noch gewisse imaginär-quadratische Multiplikatoren gibt. Diese Eigenschaft ergibt sich aus einer grundlegenden Identität für die Norm in M, nämlich für ihr Verhalten bei der Addition:

$$N(\mu+\nu)+N(\mu-\nu)=2\,N(\mu)+2\,N(\nu),$$

zusammen mit der Tatsache, daß die Norm in M ihrer Definition nach wesentlich positiv ist:

$$N(\mu)\geqq 0\,.$$

Die Normenadditionsformel erhält man, wenn man das aus der klassischen komplexen Multiplikation geläufige Verfahren der Nullstellen- und Polbestimmung der Funktion

$$\wp(\mu u)-\wp(\nu u)$$

algebraisiert, d. h. die Zähler- und Nennerprimdivisoren von

$$x\mu-x\nu$$

bestimmt und ihre Anzahlen gleichsetzt, wo x irgendein Element vom genauen Nenner $\mathfrak{o}^2$ aus K ist.

Die Normenadditionsformel führt rein-algebraisch zu der Formel

$$N(m\mu+n\nu)=m^2\,N(\mu)+mn\,(N(\mu+\nu)-N(\mu)-N(\nu))+n^2\,N(\nu)$$

für beliebige ganzrationale m, n, speziell

$$N(n)=n^2.$$

Die letztere Formel ergibt die oben vorweggenommene Nullteilerfreiheit von M. Aus der ersteren Formel fließt wegen der Positivität der Norm sofort die Ungleichung

$$(N(\mu\pm\nu)-N(\mu)-N(\nu))^2\leqq 4\,N(\mu)\,N(\nu),$$

speziell

$$(N(\mu\pm 1)-N(\mu)-1)^2\leqq 4\,N(\mu).$$

Ferner ergibt sich aus dieser Formel durch ein rein-algebraisches Schlußverfahren, das meine Schüler Behrbohm und Teichmüller ausgearbeitet haben, daß jeder Meromorphismus μ einer quadratischen Gleichung

$$\mu^2 + l\mu + m = 0$$

genügt, sodaß also ein weiterer zu μ konjugierter Meromorphismus $\bar{\mu}$ durch

$$l = N(\mu - 1) - N(\mu) - 1 = \mu + \bar{\mu}$$

definierbar ist, für den dann

$$m = N(\mu) = \mu\bar{\mu} = \bar{\mu}\mu$$

gilt. Dabei ist ferner nach der genannten Ungleichung

$$l^2 \leqq 4m,$$

d. h. die beiden konjugierten Meromorphismen μ, $\bar{\mu}$ sind formal konjugiert-komplex (im Grenzfall rational und gleich).

Aus allem diesem ergibt sich noch leicht, daß der Meromorphismenring M nur von einem der drei folgenden Typen sein kann:

I. Hauptordnung der ganzen Zahlen im Körper P der rationalen Zahlen,

II. Ordnung in einem imaginär-quadratischen Zahlkörper

$$\Omega = P(\delta) \text{ mit } \delta^2 = d < 0,$$

III. Ordnung in einer imaginär-quadratischen Divisionsalgebra

$$A = P(\delta, \delta') \text{ mit } \delta^2 = d < 0,\ \delta'^2 = d' < 0,\ \delta'\delta = -\delta\delta'.$$

Diese drei Typen kommen wirklich vor.

6. *Beweis der Riemannschen Vermutung.*

Die Untergruppe $\mathfrak{U}_1$ der rationalen Punkte $\mathfrak{p}_1$ war in der Gruppe $\mathfrak{A}$ aller Punkte $\mathfrak{p}$ durch die Relation

$$\pi\mathfrak{p} = \mathfrak{p}$$

charakterisiert. Diese Relation kann jetzt in der Form

$$(\pi - 1)\mathfrak{p} = \mathfrak{o}$$

geschrieben werden. Die rationalen Punkte entsprechen also den $(\pi - 1)$-ten Teilpunkten der klassischen Theorie.

Damit ist eine auch an sich bemerkenswerte algebraische Charakterisierung der gesuchten rationalen Punkte $\mathfrak{p}_1$ gewonnen.

Die gesuchte Anzahl N_1 ergibt sich nun ferner, wie aus der genaueren Theorie der Meromorphismennorm folgt, einfach als

$$N_1 = N(\pi - 1).$$

Nun genügt π einer quadratischen Gleichung

$$\pi^2 + l\pi + q = 0 \text{ mit } l^2 \leqq 4q,$$

weil ja

$$N(\pi) = [K : K\pi] = [K : K^q] = q$$

ist, und dabei ist

$$l=N(\pi-1)-N(\pi)-1=N_1-(q+1).$$

Daher ist die quadratische Gleichung für π einfach das der Funktion $L(s)$ zugrundeliegende Polynom in q^s. Die beiden Nullstellen ω, $\bar{\omega}$ von $L(s)$ oder $\zeta(s)$ in q^s sind also formal identisch mit dem Meromorphismus π:

$$K\pi=K^q$$

und seinem konjugierten $\bar{\pi}$:

$$K\bar{\pi}=(Kq)^{q^{-1}},$$

letzteres entsprechend der Relation $\bar{\pi}\pi=q$. Die mit der Riemannschen Vermutung äquivalente Tatsache, daß ω, $\bar{\omega}$ konjugiert-komplex sind, oder also, daß die Abschätzung

$$|N_1-(q+1)|\leqq 2\sqrt{q}$$

besteht, erscheint hiernach als abstraktes Analogon der Tatsache, daß das Periodenverhältnis eines elliptischen Funktionenkörpers im klassischen Falle imaginär ist.

Es sei noch bemerkt, daß die Grenzfälle

$$N_1-(q+1)=0 \text{ oder } \pm 2\sqrt{q}$$

genau den ausgearteten Körpern mit $A=0$, d. h. mit nulldimensionaler Struktur des p-Bestandteils der Punktgruppe $\mathfrak{A}$, entsprechen. Insbesondere kommt der Grenzfall $\pm 2\sqrt{q}$ wirklich vor, d. h. die gewonnene Abschätzung für $N_1-(q+1)$ ist bestmöglich.

7. *Verallgemeinerung auf beliebiges Geschlecht* $g\geqq 1$.

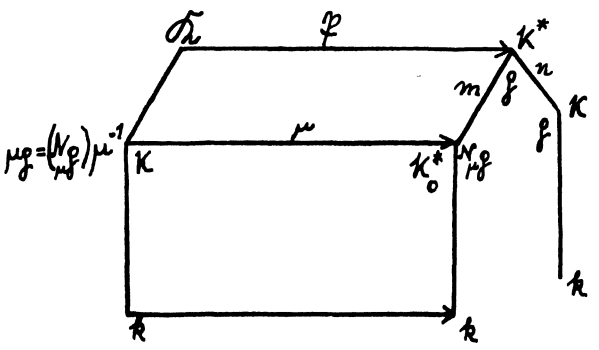
Deuring hat kürzlich erkannt, wie man den Begriff des Meromorphismus verallgemeinern muß, um die ganze entwickelte Theorie auch für beliebiges Geschlecht $g\geqq 1$ durchführen zu können. Man muß dazu das algebraische Äquivalent der von Hurwitz ausgebildeten Theorie der Korrespondenzen algebraischer Funktionenkörper zugrundelegen.

Eine *Korrespondenz* eines algebraischen Funktionenkörpers $K|k$ zu einem algebraischen Funktionenkörper $K|k$ ist nach Hurwitz eine konforme Abbildung einer endlichen Überlagerungsfläche von K auf eine endliche Überlagerungsfläche von K. Rein-algebraisch bedeutet dies, soweit es sich um zusammenhängende Überlagerungsflächen handelt, folgendes:

Es liegt ein Isomorphismus μ von K auf einen Teilkörper K_0^* einer endlichen algebraischen Erweiterung K^* von K vor, die gleich als kleinstmöglich, d. h. als Kompositum

$$K^* = K_0^* K$$

angenommen werden darf; schematisch so:



Sind m, n die Gradzahlen wie eingezeichnet, so ordnet die Korrespondenz μ jedem Punkt $\mathfrak{p}$ von K eine n-gliedrige Punktgruppe $\mu\mathfrak{p}$ von K zu, und dabei ist je m Punkten $\mathfrak{p}$ von K dieselbe n-gliedrige Punktgruppe $\mu\mathfrak{p}$ von K zugeordnet.

Rein-algebraisch vollzieht sich diese Punktkorrespondenz so: Man betrachte den Punkt $\mathfrak{p}$ von K als zusammengesetzten Divisor n-ten Grades (n-gliedrige Punktgruppe) von K^*, bilde seine Norm $N_\mu\mathfrak{p}$ für $K^* | K_0^*$ und bilde diese durch μ^{-1} auf K ab:

$$\mu\mathfrak{p} = (N_\mu\mathfrak{p})\,\mu^{-1}.$$

Das ist formal das gleiche Schema, wie oben bei den Meromorphismen, nur daß hier $\mu\mathfrak{p}$ nicht ein Punkt sondern eine Punktgruppe von K wird, und daß wir zunächst von dem Bildkörper K noch nicht die Isomorphie zu K gefordert haben.

Diese Korrespondenzen entsprechen nun wieder umkehrbar eindeutig den Primdivisoren $\mathfrak{P}$ des Körpers $\mathfrak{K} | K$, der aus $K | k$ durch formale Konstantenerweiterung entsteht. Dabei ist n der Grad von $\mathfrak{P}$. Den anderen Grad m wird man für die Definition der Norm $N(\mu)$ zugrundezulegen haben; soviel ich sehe hat man

$$N(\mu) = m^g$$

zu definieren. Bei dieser Zuordnung der Korrespondenzen μ zu den Primdivisoren $\mathfrak{P}$ muß man allerdings noch gewisse ausgeartete Korrespondenzen mitrechnen, bei denen K nur homomorph auf den Konstantenkörper k abgebildet wird; sie entsprechen den konstanten Primdivisoren von $\mathfrak{K} | K$, d. h. denjenigen, die sich bereits als Primdivisoren von $K | k$ darstellen.

Wenn schon darin ein wesentlicher Unterschied gegenüber dem Spezialfall $g=1$ besteht, daß hier Primdivisoren $\mathfrak{P}$ beliebigen Grades n (nicht nur ersten Grades) auftreten, so liegt ein weiterer wesentlicher Unterschied noch darin, daß die nach dem bisherigen Schema gewonnenen Korrespondenzen μ noch nicht additiv abgeschlossen sind. Das liegt daran, daß jetzt das Additionstheorem als Klassenmultiplikation der $\mathfrak{K}|K$ nicht durch die Primdivisoren $\mathfrak{P}$ allein, sondern erst durch die Divisoren $\mathfrak{D}$ vom Grade g vollständig beschrieben wird. Daher muß man hier auch formale Zusammensetzungen von Primkorrespondenzen in Betracht ziehen; sie sind das abstrakte Analogon zu Hurwitzschen Korrespondenzen, bei denen die Überlagerungsflächen unzusammenhängend sind.

Deuring ist auf diese Weise bisher bis zur Aufstellung des *Korrespondenzenrings* M der Korrespondenzen von K auf sich vorgedrungen. Dieser entspricht dem Ring der ganzen Multiplikatoren der K zugeordneten Riemannschen Matrix in der klassischen Theorie. Es steht dann im wesentlichen noch eine Theorie der Norm in M und insbesondere der Beweis einer Normenadditionsformel aus. Man sieht aber schon, daß die Riemannsche Vermutung für beliebiges Geschlecht $g \geqq 1$ wieder einfach das abstrakte Analogon zu der Tatsache wird, daß die bekannte aus der Riemannschen Matrix von K gebildete Hermitesche Form positiv definit ist.

Auch nach einer anderen Richtung hin lassen sich die vorstehend geschilderten Methoden anwenden, nämlich auf das berühmte Hilbertsche Problem der Klassenkörperkonstruktion für algebraische Zahlkörper durch Teilwerte Abelscher Funktionen. Deuring kann hier bereits den Fall $g=1$, der mit der Klassenkörperkonstruktion zu einem imaginär-quadratischen Zahlkörper verknüpft ist, also den Fall der klassischen komplexen Multiplikation, auf rein-algebraische Weise durchführen. Die weitere Ausbildung seiner Methode wird entsprechend zu einer rein-algebraischen Lösung für beliebige algebraische Zahlkörper führen. Als Haupthilfsmittel dafür wird man die Konstruktion einer Riemannschen Matrix zu einem vorgegebenen Multiplikatorenring brauchen; darüber ist in letzter Zeit viel gearbeitet worden, vor allem von A. A. Albert. Charakteristisch für diesen Zugang zur Lösung des Hilbertschen Problems ist, daß man durch die rein-algebraische Behandlung die Schwierigkeiten vermeidet, die bei den bisherigen Ansätzen von Hecke u. a. in dem Auftreten analytischer Funktionen von mehreren Variablen liegen.