den weitesten Spielraum lassen, ohne dafs es deshalb nötig wird, den Boden strenger arithmetischer Beweisführung jemals unter den Füfsen zu verlieren.

Damit bin ich nun aber am Ziele meines Vortrages angelangt. Weit entfernt von der Prätension, darin irgend etwas wesentlich Neues gesagt zu haben, beabsichtigte ich nur, aus dem, was andere vor mir erdacht, dasjenige auszuwählen und übersichtlich zu gruppiren, was mir für den angedeuteten Zweck passend erschien, ohne etwa zugleich den von mir skizzirten Weg als den einzig möglichen und zweckmäfsigen hinstellen zu wollen.*) Immerhin werden vielleicht jüngere Docenten aus dem Gesagten diese oder jene brauchbare Andeutung entnehmen können. Im übrigen, wie dem auch sei: wesentlich lag mir zunächst nur daran, soweit als thunlich, nachzuweisen, dafs eine Umgestaltung der fraglichen Elementar-Vorlesungen in dem näher erörterten Sinne sowohl wünschenswert, als durchführbar erscheint.

„Das Wesen der Triumphe der Wissenschaft und ihres Fortschrittes“, sagt der englische Philosoph Whewell,**) „besteht darin, dafs wir veranlafst werden, Ansichten, welche unsere Vorfahren für unbegreiflich hielten und unfähig waren zu begreifen, für evident und notwendig zu halten.“ Nach meiner Überzeugung ist die Zeit nicht mehr fern, wo die arithmetischen Theorien der Irrationalzahlen für so „evident und notwendig“ gelten werden, dafs man eine Einführung in die Analysis ohne dieses Hülfsmittel für schlechthin unmöglich ansehen wird.

Über eine neue Begründung der Theorie der algebraischen Zahlen.

Von **K. Hensel** in Berlin.

Die Analogie zwischen den Resultaten der Theorie der algebraischen Functionen einer Variabeln und der der algebraischen Zahlen hat mir schon seit mehreren Jahren den Gedanken nahe ge-

*) Einen von dem meinigen durchaus abweichenden Weg, der sich an die Dedekind'sche Irrationalzahl-Theorie und im übrigen von vornherein mehr an die geometrische Anschauung anschliefst, hat bekanntlich Herr Pasch vorgezeichnet: Einleitung in die Diff.- und Int.-Rechnung, Leipzig 1882.

**) Ich entnehme dieses Citat dem Hankel'schen Buche „Theorie der complexen Zahlensysteme“ (Leipzig 1867), S. 60.

legt, die Zerlegung der algebraischen Zahlen mit Hülfe der idealen Primfactoren durch eine einfachere Behandlungsweise zu ersetzen, welche der Entwickelung der algebraischen Functionen in Potenzreihen für die Umgebung einer beliebigen Stelle völlig entspricht. Die Grundlagen dieser neuen Theorie liegen in den folgenden Sätzen:

Ist

$$f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n = \alpha_0 (x - x_1) \cdots (x - x_n) = 0$$

eine beliebige ganzzahlige Gleichung n^{ten} Grades, so genügt jede rationale ganzzahlige Function $X = \varphi(x)$ von x ebenfalls einer ganzzahligen Gleichung $F(X) = 0$ desselben Grades. Betrachtet man nun irgend eine solche Gleichung als Congruenz für eine beliebig hohe Potenz p^M einer reellen Primzahl als Modul (etwa für $M = 10000$), so besteht der Satz:

Die Congruenz:

$$F(X) \equiv 0 \pmod{p^M}$$

besitzt genau so viele Wurzeln, als ihr Grad angiebt, wie grofs auch der Exponent M angenommen werde, und jene n Congruenzwurzeln $X_1, X_2, \cdots, X_n$ können stets in Potenzreihen entwickelt werden, welche nach steigenden Potenzen von p fortschreiten und höchstens eine endliche Anzahl von Anfangsgliedern mit negativen Exponenten besitzen.

Im allgemeinen schreiten alle diese Entwickelungen nach Potenzen von p mit g a n z z a h l i g e n Exponenten fort, d. h. sie können folgendermafsen geschrieben werden:

$$X = \frac{A_{-h}}{p^h} + \cdots + \frac{A_{-1}}{p} + A_0 + A_1 p + \cdots; \tag{1}$$

für diese Zahlen erhält man also genau dieselben Entwickelungen wie für eine algebraische Function in der Umgebung einer regulären Stelle.

Ausgenommen ist für jeden Zahlkörper nur eine beschränkte Anzahl von Primzahlen, nämlich die Teiler der Körperdiscriminante, oder, was im wesentlichen dasselbe ist, diejenigen Zahlen p, welche zugleich in den Discriminanten a l l e r Gleichungen $F(X) = 0$ enthalten sind.*)

Für diese Zahlen schreiten nämlich jene Entwickelungen, genau

*) Man hat bei dieser zweiten Charakterisirung jener Ausnahmezahlen nur noch die sog. aufserwesentlichen Discriminantenteiler jenes Körpers fortzulassen, welche ich in meiner Dissertation bestimmt habe.

wie in der Umgebung eines Verzweigungspunktes eines algebraischen Gebildes, nicht nach ganzzahligen, sondern nach Potenzen von p mit rational gebrochenen Exponenten fort. Ist nämlich $\pi_1 = \sqrt[d]{p}$ eine richtig gewählte d^{te} Wurzel aus p, so erhält man für eine jener Wurzeln, etwa für X_1, eine Entwickelung der folgenden Art:

$$(2) \qquad X_1 = \frac{A_{-h}}{\pi_1^h} + \cdots + \frac{A_{-1}}{\pi_1} + A_0 + A_1\pi_1 + \cdots.$$

Sind ferner $\pi_2, \cdots \pi_d$ die zu π_1 conjugirten d^{ten} Wurzeln aus p, so stimmen die d conjugirten Entwickelungen:

$$(2\text{a}) \; X_i = \frac{A_{-h}}{\pi_i^h} + \cdots + \frac{A_{-1}}{\pi_i} + A_0 + A_1\pi_i + \cdots, \; (i = 1, 2, \cdots d)$$

genau mit d von den n conjugirten Wurzeln von $F(X) = 0$ überein; jene d Entwickelungen hängen hier also genau in derselben Weise zusammen, wie die d Zweige einer algebraischen Function in der Umgebung eines Verzweigungspunktes V_d von der $(d-1)^{\text{ten}}$ Ordnung. Es sollen daher diese Primzahlen Verzweigungszahlen genannt werden.

Während diese Resultate wörtlich mit den entsprechenden Sätzen für algebraische Functionen übereinstimmen, müssen nunmehr zwei Bemerkungen hinzugefügt werden, durch welche sich die höhere Arithmetik principiell von jener anderen Theorie unterscheidet.

In den unter (1) und (2) gegebenen Entwickelungen der algebraischen Zahlen können nämlich die Coefficienten A naturgemäſs nicht, wie dies in der Functionentheorie der Fall ist, als beliebige Constanten angenommen werden, vielmehr gehören sie für jede der n conjugirten Entwickelungen ganz bestimmten einfachen algebraischen Körpern an. Für eine bestimmte Wurzel, etwa für X_1, sind nämlich $A_{-h}, \cdots A_0, A_1, \cdots$ sämtlich von der Form:

$$A = a_0 + a_1\alpha_1 + \cdots + a_{k-1}\alpha_1^{k-1},$$

wo α_1 eine der k Wurzeln einer auch modulo p irreduciblen Gleichung:

$$(3) \; \varphi(\alpha) = \alpha^k + b_1\alpha^{k-1} + \cdots + b_k = (\alpha - \alpha_1) \cdots (\alpha - \alpha_k) = 0$$

ist, und wo die Coefficienten $a_0, a_1, \cdots a_{k-1}$ die Werte $0, 1, \cdots, p-1$ annehmen können.

Ersetzt man nun in einer Wurzel X in (1) oder in (2) in allen Coefficienten $A_i(\alpha_1)$ die algebraische Zahl α_1 der Reihe nach durch ihre conjugirten $\alpha_2, \cdots \alpha_k$, so ergeben sich k andere Entwickelungen, welche z. B. für (1) folgendermaſsen lauten:

$$X^{(g)} = \frac{A_{-h}(\alpha_g)}{p^h} + \cdots + \frac{A_{-1}(\alpha_g)}{p} + A_0(\alpha_g) + \cdots, \quad (g = 1, 2, \cdots k),$$

und jede von diesen ist einer der n conjugirten Wurzeln $X_1, \cdots X_n$ congruent. Zu jeder Wurzel (oder, für eine Verzweigungszahl p, zu jedem Wurzelcyklus) gehören also k andere, welche ich verbundene Wurzeln oder Cyklen nennen möchte, von denen jede aus einer von ihnen dadurch hervorgeht, dafs man alle Coefficienten A_i durch ihre conjugirten ersetzt.

Der zweite fundamentale Unterschied zwischen beiden Theorien ergiebt sich aus der folgenden Bemerkung: Für einen Verzweigungspunkt V_d sind die d conjugirten d^{ten} Wurzeln aus p, nach welchen die d Entwickelungen (2a) fortschreiten, im allgemeinen die Wurzeln der reinen Gleichung:

$$\psi(\pi) = \pi^d - p = 0, \tag{4}$$

d. h. sie unterscheiden sich hier, wie in der anderen Theorie, einzig und allein durch die d conjugirten Kreisteilungseinheiten $1, \omega, \omega^2, \cdots \omega^{d-1}$, wenn

$$\omega = \cos\frac{2\pi}{d} + i\sin\frac{2\pi}{d}$$

angenommen wird.*)

Eine Ausnahme macht nur der ganz specielle Fall, wenn die Anzahl d der für einen Verzweigungspunkt conjugirten Wurzeln (2a) durch die betrachtete Primzahl p teilbar ist, ein Fall, der nur für ganz specielle Teiler der Körperdiscriminante, nämlich nur für diejenigen vorkommen kann, welche $\leqq n$ sind. Indessen haben gerade diese Zahlen der Wissenschaft grofse und bisher noch nicht überwundene Schwierigkeiten bereitet, und der Umstand, dafs auch hier die Entwickelungen der Wurzeln im wesentlichen dieselben sind, wie für die gewöhnlichen Verzweigungspunkte, dafs also jene Schwierigkeiten hier überhaupt nicht auftreten, scheint mir ein Beweis für die Berechtigung und Notwendigkeit dieser Theorie zu sein. In diesem Falle können nämlich die Zahlen $\pi_1, \pi_2, \cdots \pi_d$ die conjugirten Wurzeln einer nicht reinen Gleichung d^{ten} Grades:

$$\psi(\pi) = \pi^d + p\varepsilon_{d-1}\pi^{d-1} + p\varepsilon_{d-2}\pi^{d-2} + \cdots + p\varepsilon_0 = 0$$

---

*) In Wahrheit lauten jene reinen Gleichungen:

$$\psi(\pi) = \pi^d - \varepsilon p = 0,$$

wo ε eine bestimmte, durch p nicht teilbare Zahl des Körpers $K(\alpha_1)$ ist. Da dieselbe für alle hier zu ziehenden Folgerungen unwesentlich ist, so wurde für diese kurze Darstellung der Theorie von ihr abgesehen.

sein, deren sämtliche Coefficienten durch p teilbare ganze Zahlen des Körpers $K(\alpha_1)$ sind, und deren constantes Glied $p\varepsilon_0$ diese Primzahl nur einmal enthält. Auch in diesem Falle unterscheiden sich die Zahlen π_i von $\sqrt[d]{p}$ nur durch Einheiten; nur sind dies nicht mehr die Kreisteilungseinheiten.

In der That, setzt man:

$$\pi = \omega \cdot \sqrt[d]{p},$$

so genügt ω der Gleichung:

$$\omega^d + \sqrt[d]{p^{d-1}}\varepsilon_{d-1}\omega^{d-1} + \sqrt[d]{p^{d-2}}\varepsilon_{d-2}\omega^{d-2} + \cdots + \varepsilon_0 = 0,$$

d. h. ω ist eine ganze algebraische Zahl, deren Norm ε_0 p nicht enthält, also eine Einheit für p. Je nachdem die conjugirten Zahlen $\pi_1, \cdots \pi_d$ für einen Verzweigungspunkt V_d einer reinen oder einer gemischten Gleichung d^{ten} Grades genügen, will ich diesen einen Verzweigungspunkt der ersten oder der zweiten Art nennen.

Alle diese Sätze können, wie in einer demnächst in den „Mathematischen Annalen" erscheinenden Abhandlung dargelegt werden soll, mit sehr einfachen Hülfsmitteln und völlig unabhängig von der Theorie der Ideale begründet werden. Es soll jetzt noch der Zusammenhang dieser Theorie mit der der Ideale kurz dargelegt werden.

Jeder von den n conjugirten Entwickelungen $X_1, \cdots X_n$ einer rationalen Function $X = \varphi(x)$ modulo p^M kann man, genau wie in der Theorie der algebraischen Functionen, je eine Stelle $(p, x_1), \cdots (p, x_n)$ des zugehörigen algebraischen Zahlengebildes eindeutig zuordnen; eine solche Stelle (p, x_i) ist dann regulär oder singulär, je nachdem die zugehörigen Entwickelungen aller Functionen $X_i = \varphi(x_i)$ modulo p^M nach ganzen oder gebrochenen Potenzen von p fortschreiten, und sie ist eine singuläre oder Verzweigungsstelle der ersten oder der zweiten Art, je nachdem die zugehörige Zahl π einer reinen oder einer gemischten Gleichung $\psi(\pi) = 0$ genügt. Eine beliebige Zahl X besitzt an der Stelle (p, x_i) eine ϱfache Nullstelle, wenn die Entwickelung von X_i erst mit der Potenz $A_\varrho p^\varrho$ (bzw. $A_\varrho \pi^\varrho$) beginnt, und sie hat dort einen ϱfachen Pol, wenn sie mit $\frac{A_{-\varrho}}{p^\varrho}$ oder $\frac{A_{-\varrho}}{\pi^\varrho}$ anfängt. Nach diesen Definitionen kann der Zusammenhang zwischen beiden Theorien einfach folgendermafsen ausgesprochen werden:

Ist p eine beliebige Primzahl und P ein idealer Primteiler von p für einen der n conjugirten Körper, etwa für $K(x_1)$, so ist diesem eine Stelle (p, x_i) in der Weise zugeordnet, dafs eine algebraische Zahl X dann und nur dann durch P^ϱ teilbar ist, wenn X an der zugehörigen Stelle eine ϱfache Nullstelle hat, und dafs sie $P^{-\varrho}$ enthält, wenn X dort einen ϱfachen Pol besitzt. Der Primteiler P ist dann vom Grade k (d. h. es ist $Nm(P) = p^k$), wenn zu der Stelle (p, x_i) genau k verbundene Stellen gehören, und p ist genau durch P^d teilbar, wenn die zugehörige Stelle (p, x_i) einem Verzweigungspunkte $(d - 1)^{\text{ter}}$ Ordnung angehört, der von der ersten oder von der zweiten Art sein kann.

In zwei weiteren Arbeiten*) sind die hier auseinandergesetzten Principien auf die Lösung einiger Aufgaben angewendet worden, deren Lösung mit Hülfe der Idealtheorie noch nicht gelungen war.

Über die Theorie der relativquadratischen Zahlkörper.

Von **David Hilbert** in Göttingen.

In der Theorie der relativ Abel'schen Zahlkörper nehmen zunächst die Körper vom zweiten Relativgrade unser Interesse in Anspruch.

Es sei ein beliebiger Zahlkörper k vom Grade n als Rationalitätsbereich zu Grunde gelegt; unsere Aufgabe ist es dann, die Theorie der relativquadratischen Zahlkörper $K(\sqrt{\mu})$, d. h. derjenigen Körper zu begründen, die durch die Quadratwurzel aus einer beliebigen ganzen Zahl μ des Körpers k bestimmt sind. Die „disquisitiones arithmeticae" von Gaufs sind als der einfachste Fall in jenem Problem enthalten. Wir können unseren Gegenstand auch als die Theorie der quadratischen Gleichungen oder Formen bezeichnen, deren Coefficienten Zahlen des vorgelegten Rationalitätsbereiches k sind.

Für unsere Theorie ist vor allem die Erkenntnis notwendig, dafs auch in dem beliebigen Zahlkörper k ein Reciprocitätsgesetz für quadratische Reste besteht. Das quadratische Reciprocitätsgesetz im Bereiche der rationalen Zahlen lautet bekanntlich:

---

*) Über die Bestimmung der Discriminante eines algebraischen Körpers. — Über die Fundamentalgleichung und die aufserwesentlichen Discriminantenteiler eines algebraischen Körpers, Göttinger Nachrichten v. J. 1897, Heft 3.