Zur Zahlentheorie in Körpern von der Charakteristik p.

(Vorläufige Mitteilung.)

Von Friedrich Karl Schmidt in Erlangen.

1. Die Frage nach systematischer Begründung der Zahlentheorie gibt Anlaß, zahlentheoretische Probleme in gewissen, von den Zahlen verschiedenen Bereichen zu verfolgen. Indem durch solche Betrachtungen zahlentheoretische Sätze auf andersartige Elementegebiete übertragen werden, werden zugleich diejenigen abstrakten Eigenschaften der Zahlen bloßgelegt, auf denen die Gültigkeit der Zahlentheorie eigentlich beruht. So hat unlängst Herr A. Speiser[1]) die Idealtheorie eines algebraischen Zahlkörpers auf hyperkomplexe Größen mit nicht-kommutativer Multiplikation ausgedehnt und damit die Unabhängigkeit dieser Theorie vom kommutativen Gesetz der Multiplikation nachgewiesen. Die zahlentheoretischen Untersuchungen in Körpern von der Charakteristik p, die an Dedekind[2]) anknüpfen, lassen sich einem ähnlichen axiomatischen Gedankenkreis einordnen.

Dabei handelt es sich um folgendes: Es sei k ein Körper mit endlich vielen Elementen; dann gibt es bekantlich stets eine Primzahl p von der Art, daß das p-fache des Einheitselements in k gleich 0 ist. Im Anschluß an Herrn E. Steinitz[3]) schreiben wir daher dem Körper k und jeder beliebigen Er-

1) A. Speiser, Allgemeine Zahlentheorie. Vierteljahrschrift d. Naturf. Ges. in Zürich LXXI (1926).

2) R. Dedekind, Abriß einer Theorie der höheren Kongruenzen in bezug auf einen reellen Primzahl-Modulus. Journ. f. d. r. u. a. Math. 54 (1867).

3) E. Steinitz, Algebraische Theorie der Körper. Journ. f. d. r. u. a. Math. 137 (1910). Im folgenden mit „St." zitiert.

weiterung von k die *Charakteristik* p zu [1]). Ist $K = k(t)$ der Körper aller rationalen Funktionen in einer Unbestimmten t mit Koeffizienten aus k, $\mathfrak{K}$ ein Körper, der aus K durch Adjunktion endlich vieler algebraischer Elemente entsteht, so greift man aus K den Integritätsbereich J aller ganzen rationalen Funktionen in t heraus und bezeichnet mit $\mathfrak{J}$ den Integritätsbereich aller Elemente γ aus $\mathfrak{K}$, die einer Gleichung der Form

$$x^m + G_1 x^{m-1} + \ldots + G_m = 0$$

mit Koeffizienten G_i aus J genügen. Der Integritätsbereich $\mathfrak{J}$, dessen Elemente *in* t *ganz* heißen, soll zahlentheoretisch studiert werden.

Nachdem durch Herrn E. Artin [2]) der Spezialfall desjenigen Körpers $\mathfrak{K}$ erledigt war, der aus K durch Adjunktion einer Quadratwurzel $\sqrt{D}$ (D Element aus J) hervorgeht [3]), haben Herr P. Sengenhorst [4]) und der Verfasser [5]) unabhängig voneinander für einen allgemeinen Körper $\mathfrak{K}$ vom m^{ten} Grad die Idealtheorie und die Theorie der Einheiten des Integritätsbereiches $\mathfrak{J}$ entwickelt. Beide Arbeiten ergaben weitgehende Übereinstimmung mit bekannten zahlentheoretischen Tatsachen [6]).

---

1) St. S. 181.

2) E. Artin, Quadratische Körper im Gebiet der höheren Kongruenzen I u. II. Math. Zeitschr. 19 (1924).

3) Nicht jeder quadratische Körper $\mathfrak{K}$ läßt sich aus K durch Adjunktion einer Quadratwurzel erzeugen; dies ist vielmehr nur dann stets der Fall, wenn $p \neq 2$ ist, wie Herr E. Artin voraussetzt. Ist dagegen $p = 2$ und wird $\mathfrak{K}$ durch eine irreduzible quadratische Gleichung mit zwei verschiedenen Wurzeln bestimmt (etwa durch $x^2 + x + t = 0$), so enthält $\mathfrak{K}$ nach einem allgemeinen Satz des Herrn E. Steinitz (St. S. 235) kein Element, das einer in K irreduziblen Gleichung der Form $x^2 + a = 0$ genügt, weil eine solche Gleichung stets nur eine, doppelt zu zählende Wurzel hat.

4) P. Sengenhorst, Körper von der Charakteristik p. Math. Zeitschrift 24 (1925). Im folgenden mit „S." zitiert.

5) F. K. Schmidt, Allgemeine Körper im Gebiet der höheren Kongruenzen, Diss. Freiburg i. B. 1925. Im folgenden mit „D" zitiert.

6) Zu vollständigem Parallelismus mit zahlentheoretischen Ergebnissen führt auch die von Herrn H. Hasse angeregte Abhandlung: H. Rauter, Über d. Darstellbarkeit durch quadr. Formen im Körper d. rat. Funkt. einer Unbestimmten über d. Restklassenkörper mod. p. Diss. Halle 1926.

In den nachstehenden Zeilen soll nunmehr auch die allgemeine Übertragung der analytischen Theorie in Angriff genommen werden, die Herr E. Artin in seinem Spezialfall ebenfalls gegeben hat. Ich werde mich dabei in dieser vorläufigen Mitteilung mit der Angabe einiger fundamentaler Eigenschaften der Zetafunktion für den Körper $\mathfrak{K}$ und einer kurzen Skizzierung der Methode begnügen; auf eine ausführliche Darstellung der Beweise werde ich an anderer Stelle zurückkommen. Die hier angeführten Ergebnisse eröffnen u. a. die Möglichkeit, die Takagische[1]) Theorie der Klassenkörper und der höheren Reziprozitätsgesetze auf den Körper $\mathfrak{K}$ zu übertragen, worauf ich ebenfalls demnächst einzugehen gedenke. In Nr. **3** dieser Note zeige ich nur noch kurz, daß sich für den Grundkörper K das Reziprozitätsgesetz zwischen den m^{ten} Potenzresten (m bel. natürl. Zahl) mit wenigen Worten begründen läßt, wobei ich bloß die einfachsten algebraischen Eigenschaften endlicher Körper heranziehe.

2. Ein beliebiger Körper $\boldsymbol{K}$ heißt nach Herrn Kürschák[2]) *bewertet*, wenn jedem Element a aus $\boldsymbol{K}$ eine reelle Zahl $\|a\|$, der *Betrag von* a, in der Weise zugeordnet ist, daß für zwei beliebige Elemente a und b aus $\boldsymbol{K}$ stets

$$\|a \cdot b\| = \|a\| \cdot \|b\| \quad \text{und} \quad \|a + b\| \leqq \|a\| + \|b\|$$

ist. Für bewertete Körper können die Begriffe der Konvergenz und des Grenzwertes einer Folge wie in der Cantorschen Theorie der irrationalen Zahlen erklärt werden. Besitzt jede konvergente Folge von Elementen $a_1, a_2, \ldots$ in einem bewerteten Körper $\boldsymbol{K}$ einen Grenzwert, so wird $\boldsymbol{K}$ *perfekt* genannt.

Der Körper K möge dadurch bewertet werden, daß für jedes Element G aus J $\|G\| = q^g$ gesetzt wird, wo g den Grad von G in t und q die Elementenzahl von k bedeutet. Für die so definierte Bewertung ist insbesondere stets $\|G + H\| \leqq \|G\|$,

1) T. Takagi, Über eine Theorie des relativ Abelschen Zahlkörpers. Journ. Coll. Science, Tokyo, Vol. XLI, Art. 9 (1920).

Ders., Über das Reziprozitätsgesetz in einem beliebigen algebraischen Zahlkörper. Journ. Coll. Science, Tokyo, Vol. XLIV, Art. 5 (1922).

2) Kürschák, Limesbildung und allgemeine Körpertheorie. Journ. f. d. r. u. a. Math. 142.

wenn $\| G \| \geqq \| H \|$ ist, sodaß wir es also in der Ausdrucksweise des Herrn A. Ostrowski[1]) mit einer *nicht-archimedischen* Bewertung zu tun haben. Die kleinste perfekte Erweiterung $\overline{K}$ von K hinsichtlich der angegebenen Bewertung ist isomorph der Gesamtheit aller Potenzreihen der Form

$$A = E_a t^a + E_{a-1} t^{a-1} + \ldots \quad \text{(a ganze rat. Zahl)}$$

mit Koeffizienten E_i aus k, und es ist $\| A \| = q^a$. Die Zahl a bezeichnen wir als *Grad* von A; Gr. (A) = a. In der Zahlentheorie des Körpers K spielt $\overline{K}$ die gleiche Rolle wie die Gesamtheit aller reellen Zahlen gegenüber den rationalen Zahlen.

In Analogie mit dem bekannten Dedekindschen[2]) Ansatz definieren wir eine Funktion $Z(s)$ der komplexen Variablen s durch die Gleichung

$$Z(s) = \sum_{\mathfrak{a}} \frac{1}{\| N\mathfrak{a} \|^s} \qquad \text{(N Abkürzung für „Norm"),}$$

wo die Summe sich über alle ganzen Ideale $\mathfrak{a}$ aus $\mathfrak{J}$ erstreckt. Die rechter Hand stehende, unendliche Reihe ist für alle s, deren Realteil $\Re(s) > 1$ ist, eine reguläre analytische Funktion, und es handelt sich wie bei den Zahlen darum, das Verhalten von $Z(s)$ auf und jenseits der Graden $\Re(s) = 1$ festzustellen. Der Kürze halber beschränken wir uns dabei hier auf einen Spezialfall, der bereits alles wesentliche erkennen läßt: Wir nehmen nämlich an, daß $\mathfrak{K}$ und alle zu $\mathfrak{K}$ über K konjugierten Körper als Unterkörper in $\overline{K}$ enthalten sind[3]); wir setzen also voraus, daß $\mathfrak{K}$ *total reell* ist. Der Übergang zum allgemeinsten Körper $\mathfrak{K}$ führt dann auf keine neuen prinzipiellen Schwierigkeiten.

---

1) A. Ostrowski, Acta math. 41.

2) Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, 4. Aufl. (1894), S. 610.

3) Mit dieser Annahme ist die Tatsache äquivalent, daß $\frac{1}{t}$ im Integritätsbereich aller in $\frac{1}{t}$ ganzen Elemente aus $\mathfrak{K}$ gleich einem Produkt von lauter verschiedenen linearen Primidealen ist (vgl. D., Kap. III, § 3).

Unter den für $\mathfrak{K}$ getroffenen Festsetzungen besitzt $\mathfrak{Z}$ ein Fundamentalsystem von $m-1$ Fundamentaleinheiten[1]) $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{m-1}$, d. h. jede Einheit ε aus $\mathfrak{Z}$ ist in der Form

$$\varepsilon = E\,\varepsilon_1^{n_1}\varepsilon_2^{n_2}\ldots\varepsilon_{m-1}^{n_{m-1}}$$

darstellbar, wo E ein Element aus k[2]), n_i ganze rationale Zahlen sind und m den Grad von $\mathfrak{K}$ über K bedeutet. Aus diesen Fundamentaleinheiten und ihren Konjugierten bildet man den *Regulator* r von $\mathfrak{Z}$ ganz entsprechend wie bei den Zahlen, nur hat man die Logarithmen der Einheiten durch die Gradzahlen Gr. (ε) zu ersetzen; r ist also eine positive ganze Zahl. Erwähnen wir noch, daß sich die *Diskriminante*[3]) D von $\mathfrak{Z}$ stets ebenso wie bei den Zahlen definieren läßt und daß sich die Ideale aus $\mathfrak{Z}$ auf endlich viele *Idealklassen*[4]) im Sinne der gewöhnlichen Zahlentheorie verteilen, so können wir folgenden Satz aussprechen, durch den der funktionentheoretische Charakter von $Z(s)$ vollkommen aufgeklärt wird:

Satz: Die Funktion $Z(s)$ ist über die ganze komplexe Zahlenebene fortsetzbar. Sie ist periodisch mit der Periode $\frac{2\pi i}{\log q}$ und überall regulär bis auf die Stellen $1 + \frac{2l\pi i}{\log q}$. Dort besitzt sie jeweils einen Pol von erster Ordnung mit dem Residuum $\frac{(q-1)^{m-1}r}{\sqrt{\|D\|}\log q}h$, wo h die Anzahl der Idealklassen von $\mathfrak{Z}$ bedeutet.

Zum Beweis dieses Satzes betrachten wir wie bei den Zahlen die Funktion

$$Z(s;\,\mathfrak{C}) = \sum_{c \text{ in } \mathfrak{C}} \frac{1}{\|Nc\|^s},$$

1) „S.“, S. 38; D., S. 37.

2) Es wird vorausgesetzt, daß jedes Element aus $\mathfrak{K}$, welches einer algebraischen Gleichung mit Koeffizienten aus k genügt, selbst zu k gehört. Hierin liegt keine Einschränkung.

3) „S.“, S. 23; D., S. 19.

4) „S.“, S. 38; D., S. 44.

wo jetzt die Summe sich über alle Ideale c aus einer Idealklasse $\mathfrak{C}$ erstreckt. Im Gegensatz zu den Zahlen ist die Funktion $Z(s;\ \mathfrak{C})$ in geschlossener Form summierbar und zwar ist:

$$(1)\quad Z(s;\ \mathfrak{C}) = \frac{(q-1)^{m-1}r}{\sqrt{\|D\|}\,(1-q^{-(s-1)})\,q^{g(s-1)}} + f(s),$$

wo g eine ganze Zahl ist und f(s) eine endliche Summe der Gestalt $\sum_n \frac{c_n}{q^{ns}}$, also sicher eine ganze Funktion von s darstellt. Da

$$Z(s) = \sum_{\mathfrak{C}} Z(s;\ \mathfrak{C})$$

und nach (1) $\lim_{s\to 1}(s-1)Z(s;\ \mathfrak{C}) = \frac{(q-1)^{m-1}r}{\sqrt{\|D\|}\log q}$,

d. h. von der Klasse $\mathfrak{C}$ unabhängig ist, so ergibt (1) die Richtigkeit des Satzes.

Die Herleitung von (1) nimmt ihren Ausgang von folgender Umformung, die ebenso wie bei den Zahlen bewiesen wird[1]):

$$(2)\quad \|Nc\|^{-s} Z(s;\ \mathfrak{C}) = \sum_{c}{}' \sum_{\xi} \frac{1}{\|N\xi\|^s}.$$

Dabei bedeutet c ein Ideal aus der zu $\mathfrak{C}$ reziproken Klasse, und der Strich am Summenzeichen besagt, daß ξ alle nicht assoziierten Elemente von c durchlaufen soll. Die Summierung der Reihe $\sum_{c\,|\,\xi}{}' \frac{1}{\|N\xi\|^s}$ geschieht in der Weise, daß wir abzählen, wieviel nicht-assoziierte Elemente ξ aus c eine Norm von vorgeschriebenem Betrag q^n besitzen und dadurch zu einer unendlichen Reihe der Form $\sum_n \frac{z_n}{q^{ns}}$ gelangen, bei der die Koeffizienten z_n bekannt sind.

1) Vgl. etwa E. Landau, Theorie der algebraischen Zahlen und der Ideale, S. 58. Leipzig 1918.

Um zunächst aus allen mit einem bestimmten ξ assoziierten Elementen $\xi\varepsilon$ gewisse herauszuheben, definieren wir in Anlehnung an die Theorie der Zahlkörper für jedes ξ eindeutig $m-1$ Zahlen $e_i(\xi)$ durch die Gleichungen:

(3)

$$\mathfrak{Gr}.(\xi^{(1)}) = e_1(\xi)\,\mathfrak{Gr}.(\varepsilon_1^{(1)}) + \ldots + e_{m-1}(\xi)\,\mathfrak{Gr}.(\varepsilon_{m-1}^{(1)}) + \frac{1}{m}\mathfrak{Gr}.(N\xi),$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\mathfrak{Gr}.(\xi^{(m-1)}) = e_1(\xi)\,\mathfrak{Gr}.(\varepsilon_1^{(m-1)}) + \ldots + e_{m-1}(\xi)\,\mathfrak{Gr}.(\varepsilon_{m-1}^{(m-1)}) + \frac{1}{m}\mathfrak{Gr}.(N\xi),$$

aus denen wegen $\sum_{j=1}^{m} \mathfrak{Gr}.(\varepsilon^{(j)}) = \mathfrak{Gr}.(N\varepsilon) = 0$ noch die Gleichung

$$\mathfrak{Gr}.(\xi^{(m)}) = e_1(\xi)\,\mathfrak{Gr}.(\varepsilon_1^{(m)}) + \ldots + e_{m-1}(\xi)\,\mathfrak{Gr}.(\varepsilon_{m-1}^{(m)}) + \frac{1}{m}\mathfrak{Gr}.(N\xi)$$

folgt. Unter allen $\xi\varepsilon$ gibt es genau $q-1$, für die $0 \leqq e_i(\xi\varepsilon) < 1$ ist, und diese gehen aus einem unter ihnen durch Multiplikation mit den $q-1$ von 0 verschiedenen Elementen von k hervor. In (3) betrachten wir nun die Größen $\mathfrak{Gr}.(\xi^{(j)})$ als Funktionen der reellen Variablen $e_i(\xi)$, welche wir auf den Bereich $0 \leqq e_i(\xi) < 1$ einschränken, und stellen fest, für wieviel Wertsysteme $e_i(\xi)$ aus diesem Bereich die $\mathfrak{Gr}.(\xi^j)$ bei festem $\mathfrak{Gr}.(N\xi) = n$ gleich ganzen rationalen Zahlen sind. Nachdem dies geschehen ist, wählen wir aus c eine Modulbasis $\gamma_1, \ldots, \gamma_m$ aus und fragen, für wieviel m-tupel von Elementen $x_1, \ldots, x_m$ aus J die m Linearformen

$$\xi^{(1)} = x_1\gamma_1^{(1)} + \ldots + x_m\gamma_m^{(1)},$$

$$\ldots\ldots\ldots\ldots$$

$$\xi^{(m)} = x_1\gamma_1^{(m)} + \ldots + x_m\gamma_m^{(m)}$$

vorgegebene Grade $\mathfrak{Gr}.(\xi^{(1)}), \ldots, \mathfrak{Gr}.(\xi^{(m)})$ haben. Das Produkt der beiden so erhaltenen Zahlen, dividiert durch $q-1$, ist gleich der Anzahl z_n aller nicht-assoziierten Elemente ξ aus c, für die $\|N\xi\| = q^n$ ist.

Der hier eingeschlagene Weg ist gangbar, weil die Größen $\mathfrak{Gr}.(\xi^j)$ als Gradzahlen notwendig ganze Zahlen sind. Dieser Umstand ermöglicht es, die Anzahl der nicht-assoziierten Ele-

mente ξ mit $\| N\xi \| = q^n$ von einem gewissen n an genau anzugeben, während in Zahlkörpern die bekannte Methode der Volumbestimmung bei der Erledigung einer entsprechenden Aufgabe nur eine asymptotische Formel liefert.

Zur Durchführung der beiden oben erwähnten Abzählungen stützen wir uns auf zwei Hilfssätze, die aus einer gemeinsamen Quelle fließen und von denen der erste wohlbekannt ist. Sie lauten:

Hilfssatz 1: Es sei

$$\begin{aligned} l_1 &= a_{11} y_1 + \ldots + a_{1s} y_s + b_1 \quad \text{(Determ. d. } a_{ik} \\ &\ldots\ldots\ldots\ldots \quad \text{ungleich 0)} \\ l_s &= a_{s1} y_1 + \ldots + a_{ss} y_s + b_s, \end{aligned}$$

wo die a_{ik} ganze rationale, die b_i rationale Zahlen und die y_k reelle Variable sind, und es werde die Determinante der a_{ik} gleich a gesetzt. Dann gibt es genau $|a|$ Wertsysteme y_k mit $0 \leqq y_k < 1$, für die die l_i ganze Zahlen sind.

Hilfssatz 2: Es sei

$$\begin{aligned} L_1 &= A_{11} x_1 + \ldots + A_{1s} x_s \quad \text{(Determ. d. } A_{ik} \\ &\ldots\ldots\ldots\ldots \quad \text{ungleich 0)} \\ L_s &= A_{s1} x_1 + \ldots + A_{ss} x_s, \end{aligned}$$

wo die A_{ik} Elemente aus $\bar{K}$ und die x_k Unbestimmte bedeuten, und es werde die Determinante der A_{ik} gleich A gesetzt. Versteht man dann unter $n_1, \ldots, n_s$ ganze, hinlänglich große Zahlen, so gibt es genau

$$\frac{(q-1)^s q^{n_1 + n_2 + \ldots + n_s}}{\| A \|}$$

Systeme von Elementen $G_1 \ldots G_s$ aus J der Art, daß $\| L \| = q^{n_i}$ ist, falls man für $x_1 \ldots x_s$ die Elemente $G_1, \ldots, G_s$ einsetzt.

Aus diesen Sätzen ergibt sich, daß von einem gewissen n ab $z_n = \frac{(q-1)^{m-1} r \cdot q^n}{\sqrt{\| D \| \, \| Nc \|}}$ ist, und hieraus folgt durch Vermittelung von (2) die Gleichung (1).

Auf Formulierung und Beweis des allgemeinen Satzes, in dem die Hilfssätze 1 und 2 als Spezialfälle enthalten sind, soll hier nicht mehr eingegangen werden. Um diesen Satz aussprechen zu können, führe ich den Begriff des *natürlich bewerteten Integritätsbereichs* ein, und zwar definiere ich:

Ein bewerteter[1]) Integritätsbereich I heißt natürlich bewertet, wenn er den beiden nachstehenden Bedingungen genügt:

1. I enthält ein Elementesystem $\mathfrak{S}$ der Art, daß der Betrag $\|a\|$ jedes Elementes a aus $\mathfrak{S}$ gleich der Anzahl aller Elemente in $\mathfrak{S}$ ist, deren Betrag kleiner ist als $\|a\|$.

2. I entsteht aus $\mathfrak{S}$, indem man zu jedem Element a aus $\mathfrak{S}$ das entgegengesetzte $-a$ adjungiert.

Die ganzen rationalen Zahlen, in gewöhnlicher Weise durch den absoluten Betrag bewertet, bilden offenbar einen natürlich bewerteten Integritätsbereich. Dasselbe gilt von dem Integritätsbereich J, wenn man die in dieser Note benutzte Bewertung zugrunde legt. Umgekehrt läßt sich zeigen, daß die genannten Integritätsbereiche, in der angegebenen Weise bewertet, die einzigen natürlich bewerteten Integritätsbereiche sind.

3. Die in Nr **2** angeführten Tatsachen sind, wie bereits erwähnt, für die Theorie der Klassenkörper und die Begründung der Reziprozitätsgesetze in $\mathfrak{R}$ von besonderer Bedeutung. Im Körper K läßt sich dagegen das Reziprozitätsgesetz für m^{te}-Potenzreste (m bel. nat. Zahl) mit den einfachsten Hilfsmitteln erledigen, was vor allem deswegen von Interesse ist, weil man in Zahlkörpern Reziprozitätsgesetze nur für Primzahlexponenten kennt. In dem Spezialfall $m = 2$ ist das Reziprozitätsgesetz zwischen Elementen aus K bereits von Dedekind ohne ausgeführten Beweis angegeben und von Herrn E. Artin mit Hilfe der Theorie des über K quadratischen Körpers hergeleitet worden. Eine sinngemäße Verallgemeinerung des Gedankens, der den Dedekindschen Andeutungen zugrunde liegt, liefert

---

1) Bei jeder Bewertung wird stillschweigend der triviale Fall ausgeschlossen, daß alle Elemente entweder mit 0 oder 1 bewertet sind.

jedoch bereits das Reziprozitätsgesetz für beliebiges m in elementarer, allerdings ziemlich umständlicher Weise, wie an anderer Stelle gezeigt wurde[1]). Hier soll eine neue, wesentlich kürzere Ableitung Platz finden, die den Grund für die Gültigkeit des allgemeinen Reziprozitätsgesetzes in K klar hervortreten läßt.

Es sei die Elementezahl q von k kongruent 1 modulo m, d. h. die Gleichung $x^m - 1 = 0$ zerfalle in k in Linearfaktoren, die m^{ten} Einheitswurzeln seien also in k enthalten. Ist $R(t)$[2]) eine Primfunktion aus J, so wird das Symbol $\left\{\frac{G(t)}{R(t)}\right\}$ bei beliebigem $G(t) \not\equiv 0 \ (R(t))$ gleich derjenigen m^{ten} Einheitswurzel gesetzt, der $G^{\frac{\|R\|-1}{m}}$ modulo R kongruent ist. Sehen wir von dem Ergänzungssatz ab, so besteht das allgemeine Reziprozitätsgesetz in dem

Satz: Für zwei verschiedene Primfunktionen R(t) und S(t) aus J, bei denen der Koeffizient des Elementes höchster Potenz in t gleich 1 ist, ist:

$$\left\{\frac{R(t)}{S(t)}\right\}\left\{\frac{S(t)}{R(t)}\right\}^{-1} = (-1)^{\frac{rs(q-1)}{m}},$$

wo r und s bezw. die Grade von R(t) und S(t) bedeuten.

Beweis: Für jedes Element E aus k ist nach dem Fermatschen Satz $E^q = E$; daher $[R(t)]^q = R(t^q)$. R(t) besitzt also mit ϱ zugleich ϱ^q zur Nullstelle, und da ϱ^{q^r} die niedrigste Potenz von ϱ ist, die gleich ϱ wird, so hat die Zerlegung von R(t) bezw. S(t) in Linearfaktoren die Gestalt

---

1) D., S. 9—13. Es sei mir bei dieser Gelegenheit gestattet, zwei Berichtigungen zur Autographie meiner Dissertation zu geben: S. 8, Z. 24 lies: „ohne ausgeführten Beweis“ statt „ohne Beweis“; S. 10, Z. 6 füge hinzu: (vgl. [3]).

2) Im Hinblick auf das Folgende soll durch diese Schreibweise zum Ausdruck gebracht werden, daß die Elemente aus K Funktionen der Unbestimmten t sind.

(4) $\quad R(t) = (t-\varrho)(t-\varrho^q) \ldots (t-\varrho^{q^{r-1}})$

bezw. $\quad S(t) = (t-\sigma)(t-\sigma^q) \ldots (t-\sigma^{q^{s-1}})$.

Es ist

$$\left\{\frac{R(t)}{S(t)}\right\} \equiv [R(t)]^{\frac{q^s-1}{m}} \ (S(t)),$$

also sicher

$$\left\{\frac{R(t)}{S(t)}\right\} \equiv [R(t)]^{\frac{q^s-1}{m}} \ (t-\sigma).$$

Weil $\left\{\frac{R(t)}{S(t)}\right\}$ nach Definition ein Element aus k ist, folgt hieraus die Gleichung:

$$\left\{\frac{R(t)}{S(t)}\right\} = [R(\sigma)]^{\frac{q^s-1}{m}} = [R(\sigma)]^{(1+q+q^2+\ldots+q^{s-1})\frac{q-1}{m}}$$

oder

$$\left\{\frac{R(t)}{S(t)}\right\} = [R(\sigma)\,R(\sigma^q) \ldots R(\sigma^{q^{s-1}})]^{\frac{q-1}{m}}.$$

Ebenso ergibt sich

$$\left\{\frac{S(t)}{R(t)}\right\} = [S(\varrho)\,S(\varrho^q) \ldots S(\varrho^{q^{r-1}})]^{\frac{q-1}{m}},$$

und die aus (4) fließende Relation

$$[R(\sigma)\,R(\sigma^q) \ldots R(\sigma^{q^{s-1}})]\,[S(\varrho)\,S(\varrho^q) \ldots S(\varrho^{q^{r-1}})]^{-1} = (-1)^{rs}$$

liefert nunmehr unmittelbar die Behauptung.

Die hier angewandte Methode, den Koeffizientenkörper k zu erweitern, ermöglicht auch eine sehr einfache Übertragung der bekannten Beziehung zwischen Potenzcharakteren in Unter- und Oberkörper auf $\mathfrak{R}$ [1]).

Erlangen, Mathemat. Seminar, im August 1926.

---

1) Bei den Zahlen ist diese Beziehung zuerst von Herrn Ph. Furtwängler (Math. Ann. 58 (1904), S. 24 ff.) für einen Galoisschen, später von Herrn T. Takagi (Journ. Coll. Science, XLIV, Art. 5, § 2) für einen beliebigen algebraischen Oberkörper bewiesen worden. Eine gegenüber Takagi wesentlich abgekürzte Herleitung findet sich bei H. Hasse, Allgemeines Reziprozitätsgesetz im Kreiskörper und Oberkörpern, Journ. f. d. r. u. a. Math. 154, S. 107 ff.

Zusatz bei der Korrektur. Weitergehende Überlegungen haben mich zu einer Vertiefung der in Nr. 2 enthaltenen Ergebnisse geführt, die ich kurz angeben möchte.

Während bisher der Unbestimmten t unter allen Elementen von $\mathfrak{K}$ eine ausgezeichnete Stellung eingeräumt wurde, sollen nunmehr alle nicht zu k gehörigen Elementen aus $\mathfrak{K}$ durchaus gleichberechtigt behandelt werden. Wir nehmen also jetzt gegenüber $\mathfrak{K}$ den Standpunkt ein, der in der Theorie der algebraischen Funktionen einer Veränderlichen zuerst bei Dedekind und Weber[1]) zu finden ist. Diese beiden Autoren haben bekanntlich für die von ihnen behandelten Körper algebraischer Funktionen eine arithmetische Definition des Punktbegriffs gegeben[2]), der von jeder Bezugnahme auf eine Variable frei ist, und es wurde bereits in D. gezeigt[3]), daß diese Definition sinngemäß auf den Körper $\mathfrak{K}$ übertragen werden kann. Ein Punkt $\mathfrak{P}_\nu$ von $\mathfrak{K}$ ist dabei dadurch charakterisiert, daß den Elementen aus $\mathfrak{K}$ die Elemente eines endlichen algebraischen Erweiterungskörpers k_ν von k in bestimmter Weise zugeordnet werden. Ich setze nun $\| \mathfrak{P}_\nu \| = q^\nu$, wo q^ν die Elementezahl von k_ν bedeutet und betrachte die Funktion

$$Z_{\mathfrak{K}}(s) = \prod_{\mathfrak{P}} \frac{1}{1 - \| \mathfrak{P} \|^{-s}},$$

wo s eine komplexe Variable ist und das Produkt über alle Punkte $\mathfrak{P}$ von $\mathfrak{K}$ erstreckt wird. Diese Funktion, deren Ähnlichkeit mit der Produktdarstellung der Dedekindschen Zetafunktion in die Augen springt, ist mit Hilfe des Körpers $\mathfrak{K}$ allein, ohne Benutzung irgendeines Integritätsbereiches in $\mathfrak{K}$ erklärt. Sie ist ebenso wie die in 2 behandelte Funktion $Z(s)$ über die ganze Ebene fortsetzbar und überall regulär bis auf die Stellen $1 + \frac{2l\pi i}{\log q}$, an denen sie jeweils Pole erster Ordnung hat. Es ist ferner

---

1) Dedekind-Weber, Theorie d. algebraischen Funktionen einer Veränderlichen. Journ. f. d. r. u. a. Math. 92 (1882).

2) a. a. O. § 14.

3) D. Kap. III, § 3.

$$(5) \qquad \lim_{s \to 1} (s-1) Z_{\mathfrak{K}}(s) = \frac{q^{1-g}}{(q-1)\log q} h_{\mathfrak{K}},$$

wo g und $h_{\mathfrak{K}}$ zwei Invarianten des Körpers $\mathfrak{K}$ sind, von denen die erste das Analogon zum Geschlecht eines Körpers algebraischer Funktionen darstellt. Ist nämlich z irgendein nicht zu k gehöriges Element aus $\mathfrak{K}$, $\mathfrak{J}_z$ bezw. $\mathfrak{J}_{\frac{1}{z}}$ der Integritätsbereich aller in z bezw. $\frac{1}{z}$ ganzen Elemente aus $\mathfrak{K}$, w_z der Grad der Diskriminante von $\mathfrak{J}_z$ vermehrt um den Exponenten der höchsten Potenz von $\frac{1}{z}$, die in der Diskriminante von $\mathfrak{J}_{\frac{1}{z}}$ aufgeht, und bedeutet m_z den Grad von $\mathfrak{K}$ über k(z), so ist $g = \frac{1}{2} w_z - m_z + 1$. Andererseits ist $h_{\mathfrak{K}} = \frac{h_z r_z}{u_z}$, wo h_z bezw. r_z die Klassenzahl bezw. den Regulator von $\mathfrak{J}_z$ bezeichnen und u_z den größten gemeinschaftlichen Teiler der Gradzahlen, welche den in $\frac{1}{z}$ aufgehenden Primidealen aus $\mathfrak{J}_{\frac{1}{z}}$ zukommen. Der Ausdruck $\frac{h_z r_z}{u_z}$ steht in enger Beziehung zur Einteilung gewisser Divisoren[1]) von $\mathfrak{K}$ in Klassen, woraus seine Invarianz, d. h. die Unabhängigkeit von der Wahl des Elementes z, unmittelbar erhellt.

Mit Hilfe von (5) bestimmt man leicht das Residuum der Zetafunktion $Z_z(s)$ für irgendeinen Integritätsbereich $\mathfrak{J}_z$, denn es ist für jedes s mit einem Realteil $\Re(s) > 1$

$$Z_{\mathfrak{K}}(s) = \prod_{u} \frac{1}{1 - \| Nu \|^{-s}} Z_z(s).$$

Dabei ist das Produkt über die endlich vielen verschiedenen Primideale u erstreckt, in die $\frac{1}{z}$ in $\mathfrak{J}_{\frac{1}{z}}$ zerfällt. Je nach Anzahl und Grad der Primideale u wird man also verschiedene

1) Zur Definition der Divisoren vgl. K. Hensel, Math. Enc. II, 3, 1; S. 552.

Formeln für das Residuum von $Z_z(s)$ erhalten, wie das im Spezialfall bereits aus der Arbeit des Herrn E. Artin hervorgeht, der jedoch nur die Funktion $Z_z(s)$ betrachtet und die Residuenbildung in den einzelnen Fällen auf verschiedenen Wegen durchführt; alle diese Formeln haben somit in (5) ihren gemeinsamen Ursprung. Die Gleichung (5) scheint aber auch vor allem deswegen von Interesse, weil sie eine Beziehung zwischen den beiden wichtigen Begriffen, dem Geschlecht und der Klassenzahl, vermittelt, auf deren parallele Stellung in der Theorie der algebraischen Funktionen und der algebraischen Zahlen bereits Hilbert in seinem Pariser Vortrag hinwies.

Erlangen, im Oktober 1926.