Zum wissenschaftlichen Werk von Helmut Hasse

Von Heinrich Wolfgang Leopoldt in Karlsruhe

Aus: Crelles Journal 262/263, 1973

Leicht überarbeitete Fassung eines Vortrags im Rahmen eines Festkolloquiums am 8. Dezember 1972 in Marburg, das zur Feier des Goldenen Doktorjubiläums von H. Hasse vom Mathematischen Institut der Philipps-Universität Marburg veranstaltet wurde. Insbesondere wurde der letzte Teil des Vortrags leicht ergänzt.

Sie, Herr Hasse, haben das Bild der Mathematik Ihrer Zeit ganz wesentlich mitgestaltet! Es war eine Zeit des Übergangs. Und damit meine ich vor allem die Ablösung der klassischen Algebra durch die abstrakte Algebra von heute. Sie haben sich sehr wesentlich für diese Entwicklung eingesetzt, in Vorträgen, in Lehrbüchern, und nicht zuletzt mit einer ansehnlichen Reihe außerordentlicher Erfolge dieser "algebraischen Methode" bei der Lösung konkreter zahlentheoretischer Probleme! Sie haben diese algebraische Methode und mit ihr die Zahlentheorie um einige, ganz spezifische Elemente bereichert, von denen noch die Rede sein wird. Ein am Umfang wie an Bedeutung so gewichtiges Werk wie das Ihre läßt sich in einem einzigen kurzen Vortrag nicht angemessen behandeln! Mir bleibt daher nichts anderes übrig, als diese Aufgabe neu zu definieren, und, da ich Ihnen, Herr Hasse, über Ihr Werk nichts erzählen kann, sehe ich meine Aufgabe nur darin, insbesondere den jüngeren Mathematikern dieses Werk ein wenig näher zu bringen. Lassen Sie mich also dem vorgegebenen Thema: "Das wissenschaftliche Werk von Helmut Hasse" einen Untertitel beigeben, der die Proportionen etwas zurechtrückt, etwa so: "Eine kleine Einführung für Fernerstehende". Genauer gesagt habe ich vor, anstatt von vielem wenig oder nichts zu sagen, von wenigem ein bißchen mehr zu sagen. Konkret: Von den vielen Dingen, die Hasse in weit über 200 Veröffentlichungen behandelt hat, habe ich mir vier herausgesucht, die ich – eingebettet in ihren historischen Bezug – dem der Sache weniger Kundigen etwas deutlicher sichtbar machen möchte. Im einzelnen habe ich mir dafür ausgewählt:

(1) die **Entstehung des Lokal-Global-Prinzips** in den ersten Marburger Arbeiten (1921) und als den wohl schönsten Erfolg dieses Prinzips,

(2) die **Bestimmung der Brauergruppe** $\mathrm{Br}(K)$ eines Zahlkörpers K (1933).

Allein zwischen diesen ersten beiden Themenkreisen liegen in 10 bis 12 Jahren rund 50 bis 70 Arbeiten zur Theorie des Normenrestsymbols, zum allgemeinen Reziprozitätsgesetz, zur organischen Begründung der ersteren, wie über explizite Formeln für das letztere, zur Normenresttheorie und ihrem Zusammenhang mit der Führer- und Diskriminantentheorie, Arbeiten, auf die ich nicht einzeln eingehen werde, deren Vorhandensein hier aber doch wenigstens erwähnt werden soll. Zwischen diesen ersten beiden Themenkreisen liegen so gewichtige, eine ganze Entwicklung beeinflussende Veröffentlichungen wie die drei Teile des sogenannten Klassenkörperberichts. Zwischen diesen beiden Themenkreisen liegt beispielsweise aber auch eine Gruppe von Arbeiten, die hier fortzulassen mir besonders schmerzlich ist; ich meine die Arbeiten zur Neubegründung der klassischen Theorie der komplexen Multiplikation. Und zwischen diesen beiden Themenkreisen liegt noch mehr, was hier nur deshalb nicht genannt wird, weil es sich so schwer unter diese Sammelüberschriften einordnen läßt, was dem speziell Interessierten jedoch noch manche Überraschung bescheren dürfte.

Der zeitliche Abstand zum nächsten ausgesuchten Thema ist kurz; es handelt sich um etwa 3 Jahre und um nur etwas mehr als 20 Arbeiten. Dieses Thema ist

(3) der **Beweis des Analogons der Riemannschen Vermutung für elliptische Kongruenzfunktionenkörper** (1935/36). Es ist *ein* – vielleicht *das* – Musterbeispiel für die Kraft der algebraischen Methode und darf deshalb hier nicht fehlen!

Die Arbeiten der dann folgenden Jahre sind vor allem der Theorie der algebraischen Funktionenkörper und der Theorie der abelschen Funktionen gewidmet. Aber auch ganz andere Dinge finden sich hier, wie Arbeiten zur Struktur der bewerteten Körper oder wie der Vorläufer der späteren Bergströmschen Produktformel, um nur zwei von vielen Themen zu nennen. Etwa 6 Jahre und rund 20 Arbeiten später setzt der Krieg dieser ersten Schaffensperiode ein plötzliches Ende.

Die Wiederaufnahme der Arbeit nach dem Kriege beginnt mit Rückbesinnung auf die Wurzeln der algebraischen Zahlentheorie bei Kummer: Über die Klassenzahl abelscher Zahlkörper. Das ist sowohl der Titel der ersten, nach dem Ende des Krieges, veröffentlichten Arbeit von Hasse, als auch der einige Jahre später im Akademie-Verlag Berlin erscheinenden Monographie. Hinter diesem Titel steckt ein Programm, gerichtet auf

(4) *Abelsche Zahlkörper*. Hierüber und über das, was aus ihm geworden ist, zu berichten, habe ich mir als letzten Punkt ausgewählt.

Natürlich kommt damit wiederum nur ein Bruchteil der mathematischen Arbeit Hasses nach dem Kriege ins Blickfeld. Denn der Themenkatalog fächert sich nun bald weiter als zuvor und die Zahl der Arbeiten aus dieser zweiten Schaffensperiode hat das erste Hundert inzwischen längst überschritten. Weniger spektakuläre, gleichwohl nicht minder bedeutsame Konstruktions- und Einbettungsprobleme stehen von nun an meist im Mittelpunkt, sei es, daß es sich um die Entwicklung des darstellungstheoretischen Apparates und seiner körpertheoretischen Realisierung handelt, oder etwa um Probleme der konstruktiven Beherrschung konkreter Körpertypen oder Zahlklassen, wie zum Beispiel die der Gaußschen Summen.

Doch ich habe versprochen, über die vier ausgewählten Punkte ein wenig mehr zu sagen, und muß mich deshalb für alles übrige auf diese sehr grobe Übersicht beschränken. Ein vorläufiges Verzeichnis der Veröffentlichungen von Herrn Hasse ist enthalten in J. C. Poggendorff, Biographisch-Literarisches Handwörterbuch VII a, 2 (Berlin 1958), 389–391, ferner in Author Index of Mathematical Reviews 1940–1959 (Providence 1961), 796–797, und ebendort 1960–1964 (Providence 1966), 486.

Beginnen wir also mit dem Anfang in Marburg, mit der

Entstehung des Lokal-Global-Prinzips

Versetzen wir uns einmal um gut 50 Jahre zurück! In das Frühjahr 1920! In Göttingen studiert ein vielversprechender junger Mann namens Helmut Hasse. Göttingen! Wirkungsstätte David Hilberts und damit in dieser Zeit unbestritten das Zentrum der Mathematik in Deutschland! Dennoch – ungeachtet der Möglichkeiten, die Göttingen damit bietet – Hasse entschließt sich, von Göttingen weg und hierher in das vergleichsweise weltabgeschiedene kleine Marburg zu ziehen. Warum?

Wie Hasse selbst einmal berichtet hat, war es ein Buch, das ihn zu diesem Schritt veranlaßte: die Henselsche Zahlentheorie, die ihm in einem Göttinger Antiquariat in die Hände fiel. Hier baut Hensel die Zahlentheorie auf mit Hilfe einer neuen und sehr merkwürdigen Konstruktion, den p-adischen Zahlen. Um mehr über diese schwer verständliche, aber doch irgendwie faszinierende Konstruktion zu erfahren, geht Hasse nach Marburg, denn dort lehrt Kurt Hensel, der sie erdachte.

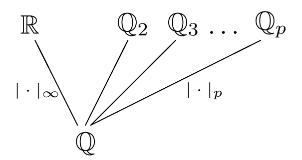
Was die Henselschen p-adischen Zahlen für die Zahlentheorie selbst bedeuten, davon wird heute noch mehrfach die Rede sein, denn dies ist mit dem Namen Helmut Hasse für immer untrennbar verbunden. Doch die historische Rolle dieser Henselschen Schöpfung reicht über die Zahlentheorie weit hinaus: Sie ist vielleicht nicht der einzige, aber doch sicher einer der entscheidenden Anstöße für jenen Prozeß, der die klassische Algebra ersetzt hat durch das, was programmatisch bis vor kurzem noch Moderne Algebra genannt wurde, uns heutigen aber längst die Algebra schlechthin geworden ist. Ein Prozeß, der 1910 mit der großen Arbeit von Steinitz über die "Algebraische Theorie der Körper" beginnt. Ich zitiere eine Fußnote zu ihrer Einleitung:

> Zu diesen allgemeinen Untersuchungen wurde ich besonders durch Hensels Theorie der algebraischen Zahlen (Leipzig, 1908) angeregt, in welcher der Körper der p-adischen Zahlen den Ausgangspunkt bildet, ein Körper, der weder den Funktionen- noch den Zahlkörpern im gewöhnlichen Sinn lies Wortes beizuzählen ist.

Ebenfalls im Bemühen, die p-adischen Zahlen besser zu verstehen, führt Kürschak 1912 den Begriff der Bewertung ein und das, was wir heute als die vollständige Hülle eines Körpers in bezug auf eine Bewertung verstehen. Die p-adischen Zahlen, welche bei Hensel noch als scheinbar divergente Reihen auftreten, lassen sich hiernach als die Elemente der vollständigen Hülle $\mathbb{Q}_p$ des rationalen Körpers $\mathbb{Q}$ in bezug auf den p-Betrag

$$|\cdot|_p = p^{-\operatorname{ord}_p(\cdot)}$$

verstehen und treten damit grundsätzlich den in gleicher Weise gebildeten reellen Zahlen ebenbürtig zur Seite:



Etwas später, 1918, weist Ostrowski nach, daß damit bereits alle Beträge von $\mathbb{Q}$ erschöpft sind.

Ebenbürtig, aber noch nicht gleichberechtigt! Das ist die Situation 1920. In Göttingen mag man vielleicht in der Existenz der p-adischen Zahlen eine spielerische Laune der Natur gesehen haben. Dem entsprechen jedenfalls die Kommentare, die Hasses Wechsel nach Marburg begleiten. Doch schon ein Jahr später, 1921, sieht das alles ganz anders aus: Bereits mit seiner ersten Arbeit, seiner Dissertation, erbringt Hasse in unübersehbarer Weise den Nachweis, daß diese p-adischen Zahlen den reellen Zahlen wenigstens im Bereich der Zahlentheorie an Bedeutung in nichts nachstehen: das Hassesche *Lokal-Global-Prinzip* wird geboren!

Es handelt sich zunächst um die Frage der Darstellbarkeit einer rationalen Zahl r durch eine gegebene quadratische Form $A(x) = \sum a_{ik} x_i x_k$ mit rationalen Koeffizienten a_{ik}. Die Antwort, genauer ihr erster Teil, lautet: *Es gibt genau dann eine* *rationale Lösung* $x = (\dots x_i \dots)$ *mit* $x_i \in \mathbb{Q}$ *der Gleichung* $A(x) = r$*, wenn es für jede Primstelle* p *von* $\mathbb{Q}$ *eine Lösung* $x^{(p)} = (\dots x_i^{(p)} \dots)$ *im zugehörigen lokalen Körper* $\mathbb{Q}_p$ *gibt*, wenn es also einerseits (für $p = \infty$) eine reelle Lösung $x^{(\infty)}$ von $A(x^{(\infty)}) = r$ und andererseits für jede Primzahl p eine p-adische Lösung $x^{(p)}$ von $A(x^{(p)}) = r$ gibt. Auf eine noch kürzere Formel gebracht besagt diese Aussage: Es gibt global eine Lösung genau dann, wenn überall lokal eine Lösung existiert. Dies ist das **Lokal-Global-Prinzip**! Scheinbar wird damit die Aufgabe erschwert; anstatt nach der Lösbarkeit in einem einzigen Körper – hier $\mathbb{Q}$ – zu fragen, wird die entsprechende Frage gleich für unendlich viele Körper, nämlich für alle den Primstellen p von $\mathbb{Q}$ zugeordneten lokalen Körper $\mathbb{Q}_p$ gestellt. In Wahrheit wird aber gerade dadurch die Frage entscheidend vereinfacht: während für den strukturreichen Körper $\mathbb{Q}$ der rationalen Zahlen eine Antwort direkt nur schwer zu erhalten wäre, ist dies für jeden der im Vergleich mit $\mathbb{Q}$ viel gröber strukturierten lokalen Körper $\mathbb{Q}_p$ ganz anders. Genau wie im Falle $p = \infty$ für $\mathbb{Q}_\infty = \mathbb{R}$ die Untergruppe der Quadrate den Index $(\mathbb{R} : \mathbb{R}^2) = 2$ hat und die Lösbarkeit bzw. Unlösbarkeit sich einfach aus dem Trägheitsindex der quadratischen Form ergibt, genau so ist auch für jede Primzahl p die Quadratklassengruppe $\mathbb{Q}_p/\mathbb{Q}_p^2$ endlich und läßt sich die Lösbarkeit in relativ einfacher Weise entscheiden; die notwendigen und hinreichenden Bedingungen – sie lassen sich mit Hilfe von Hilbertschen Normenrestsymbolen beschreiben – gibt Hasse im zweiten Teil der Antwort an. Wenn diese Bedingungen auch nicht so ganz vom Himmel fallen (ähnliche Bedingungen finden sich schon in den Minkowskischen Untersuchungen zu dieser Frage), so läßt sich doch sagen: das Problem wird erstmals abschließend behandelt, und es wird erstmals mit den dafür naturgemäßen, angemessenen Methoden behandelt; denn genau das leistet das Lokal-Global-Prinzip. Seither haben die p-adischen Zahlen das volle uneingeschränkte Bürgerrecht in der Zahlentheorie!

Die zweite Arbeit, zugleich die Habilitationsschrift, behandelt in derselben Weise, abschließend und naturgemäß mit Hilfe des Lokal-Global-Prinzips die Frage nach der rationalzahligen Äquivalenz rationaler quadratischer Formen. So angemessen ist diese neue Methode derartigen Fragen, daß sie sich ohne wesentliche Änderungen auf beliebige algebraische Zahlkörper k übertragen laßt. Die Situation ist hier im Grunde genau dieselbe wie für $\mathbb{Q}$, nur daß man hier im allgemeinen auch mehrere verschiedene unendliche Primstellen $\mathfrak{p}_\infty$ hat, die den Klassen äquivalenter Einbettungen von k in $\mathbb{C}$ entsprechen. Die dritte und vierte Arbeit behandeln so, abschließend und naturgemäß, das Darstellungs- und das Äquivalenzproblem über beliebigen Zahlkörpern, die fünfte Arbeit ebenso eine noch etwas allgemeinere Fragestellung.

Mit diesem – ich möchte sagen – Sturmlauf beginnt das wissenschaftliche Werk des Mannes, dem zu Ehren wir uns heute hier versammelt haben. Die Erfolge bleiben nicht aus: 1922, Dozent in Kiel, wo Steinitz lehrt; 1925, Ordinarius in Halle; 1930, Rückkehr nach Marburg als Nachfolger von Hensel. Doch ich greife vor!

Die kraftvolle, im Lokal-Global-Prinzip liegende Methode ist uns heutigen Mathematikern ebenso unentbehrlich wie selbstverständlich geworden. Hasse selbst hat in der Folgezeit noch manche Kostproben ihrer Wirksamkeit gegeben. Einigen der schönsten Beispiele werden wir später noch begegnen. Und selbst dort, wo dieses Prinzip zunächst unwirksam, weil als Aussage ungültig wird, bleibt es doch ein Wegweiser: wie man seit Kummer durch die Klassengruppe mißt, wie weit die Primzahlzerlegung von der Eindeutigkeit abweicht, ebenso beschreibt man heute die Abweichung vom Lokal-Global-Prinzip durch eine Gruppe, wie etwa in der Zahlentheorie der rationalen Punkte auf elliptischen Kurven.

In der folgenden Zeit macht Hasse das Hilbertsche Normenrestsymbol, mit dem er die Bedingungen für die Darstellbarkeit durch und die Äquivalenz von quadratischen Formen beschrieb, nun selbst zum Gegenstand der nächsten Arbeiten. In ihnen bemüht er sich, es durch lokale und globale Eigenschaften, durch p-Stetigkeit und Produktformel, zu charakterisieren, seine Theorie organisch zu begründen. Parallel damit gehen Untersuchungen über explizite Formeln zum Reziprozitätsgesetz und seinen Ergänzungssätzen. Bald weitet sich das Feld ...

Die Bemühungen um einen organischen Aufbau der Theorie des Normenrestsymbols und des allgemeinen Reziprozitätsgesetzes finden ihren Höhepunkt und Abschluß aber erst, als es Hasse gelingt, ein ganz anderes, hiervon scheinbar weit entferntes Problem abschließend zu lösen, als es ihm nämlich gelingt, die

Struktur der Brauergruppe $\mathrm{Br}(k)$

eines Zahlkörpers k zu bestimmen. Da es sich hierbei um den meiner Ansicht nach wohl schönsten Erfolg der auf dem Lokal-Global-Prinzip beruhenden Methode handelt, möchte ich hierauf etwas näher eingehen.

Wir schreiben das Jahr 1927. In den Jahresberichten der DMV referiert Hasse über ein soeben übersetztes und von Speiser in Zürich mit einem Anhang versehenes Buch, das in Deutschland eine Lawine auszulösen scheint: es ist Dicksons Buch "Algebras and their Arithmetics". Dasselbe Jahr bringt die Artinsche Arbeit "Zur Arithmetik der hyperkomplexen Systeme", und in einem Zeitraum von nur wenigen Jahren erscheint nun eine Fülle schöner Arbeiten zur Theorie der Algebren. Der gegen Ende dieser stürmischen Entwicklung erscheinende Deuringsche Ergebnisbericht legt davon ein eindrucksvolles Zeugnis ab. Ich muß es mir versagen, dem im einzelnen nachzugehen, und möchte mich auf einen einzigen Aspekt beschränken, der Frage nach den zentralen Divisionsalgebren D/k von endlichem Rang $(D/k) = m^2$.

Für mehr als ein halbes Jahrhundert waren die Hamiltonschen Quaternionen H über $k = \mathbb{R}$ im wesentlichen das einzige Beispiel einer zentralen Divisionsalgebra endlichen Ranges gewesen, hatte Frobenius doch sogar zeigen können, daß über $k = \mathbb{R}$ außer H keine weiteren echten Divisionsalgebren dieser Art vorhanden sind. Das Dicksonsche Buch dürfte hier in zweifacher Hinsicht auslösend gewirkt haben: Einerseits scheint es das Vehikel gewesen zu sein, welches die Wedderburnschen Struktursätze in Deutschland weithin bekannt gemacht hat in einer Form, die hier wohl geradezu als Aufforderung verstanden werden mußte, diese schönen Resultate noch einmal gründlich zu durchleuchten. Andererseits und vor allem aber machte es die eben erwähnte Frage ganz einfach wieder interessant. Dadurch nämlich, daß Dickson hier zeigt, daß über jedem nicht allzu speziellen Grundkörper k zentrale Divisionsalgebren D beliebig großen Ranges $(D/k) = m^2$ wirklich existieren. Dickson zeigt genauer folgendes: Wenn k eine zyklische Erweiterung K/k vom Grade $(K/k) = m$ besitzt und es weiter in k ein Element $\alpha \neq 0$ gibt, welches in der Normenklassengruppe $k^\times / N_{K/k} K^\times$ die höchstmögliche Ordnung $m = (K/k)$ besitzt, so erhält man eine über k zentrale Divisionsalgebra D vom Rang $(D/k) = m^2$ in der Form

$$D = \sum_{\mu=0}^{m-1} u^\mu K \quad \text{mit} \quad u^m = \alpha \quad \text{und} \quad au = ua^S \quad \text{für } a \in K,$$

wo S einen festen erzeugenden Automorphismus von K/k bezeichnet. Für die so erklärte Divisionsalgebra schreiben wir kurz

$$D = (\alpha, K, S).$$

Läßt man die Voraussetzung über die Ordnung der Normenklasse von α fallen, so entsteht auf diese Weise doch wenigstens stets eine einfache zentrale Algebra über k; man nennt die so erhaltenen Algebren auch *zyklische Algebren* über k.

Wie gesagt, das Buch löst so etwas wie eine Lawine aus: zuerst sind es die Vertreter der abstrakten Algebra, allen voran Emmy Noether und Richard Brauer, welche die Wedderburnsche Strukturtheorie mit darstellungstheoretischen Methoden neu durchleuchten. Dabei findet Brauer 1929, daß diese über k endlichen zentralen Schiefkörper D/k eine Gruppe bilden; eben die *Brauergruppe* $\mathrm{Br}(k)$ von k. Für ihre Definition ist es einfacher, gleich beliebige über k endliche und zentrale Algebren A zu betrachten. Jede solche Algebra ist nämlich volle Matrixalgebra über einem über k endlichen und zentralen Schiefkörper,

$$A = \mathcal{M}_r(D),$$

der durch A als Typ eindeutig bestimmt wird als der Automorphismen-Schiefkörper eines einfachen Linksideals. Nennen wir zwei solche Algebren *ähnlich*, $A' \sim A$, wenn sie in diesem Sinne zu demselben Schiefkörper gehören, so können und werden wir, anstatt von über k endlichen, zentralen Schiefkörpern zu reden, auch ebensogut von den Ähnlichkeitsklassen über k endlicher, zentraler einfacher Algebren, kurz: den *Algebrenklassen* über k, sprechen. Nun ist mit A und B auch das direkte Produkt $A \otimes B$ wiederum eine solche, über k endliche zentrale einfache Algebra und hängt die Klasse $(A \otimes B)$ des Produkts nur ab von den Klassen der Faktoren, so daß wir durch

$$\mathcal{C}(A) \cdot \mathcal{C}(B) = \mathcal{C}(A \otimes B)$$

eine offenbar assoziative und kommutative Multiplikation für die Menge $\mathrm{Br}(k)$ dieser Klassen erhalten. Die Klasse $\mathcal{E} = \mathcal{C}(k)$ von k selbst ist das Einselement und die Klasse der zu A jeweils invers-isomorphen Algebra A^* das zu $\mathcal{C}(A)$ inverse Element von $\mathrm{Br}(k)$,

$$\mathcal{C}(A^*) = (\mathcal{C}(A))^{-1}.$$

$\mathrm{Br}(k)$ wird damit zu einer abelschen Gruppe, genauer zu einer Torsionsgruppe; denn ist m der Index von A, also $m^2 = (D/k)$ der Rang des in A steckenden Schiefkörpers, so ist

$$\mathcal{C}(A)^m = \mathcal{E}.$$

Um diese Gruppe $\mathrm{Br}(k)$, seither die Brauergruppe genannt, geht es hier.

Benutzt man das Lokal-Global-Prinzip als systematischen Leitfaden, so hat man die Brauergruppe zunächst für einen lokalen Körper zu bestimmen. Für den archimedischen Fall, also für $k = \mathbb{R}$ bzw. $k = \mathbb{C}$, ist die Lösung dieser Aufgabe implizit enthalten in dem schon erwähnten Resultat von Frobenius. Für den viel interessanteren Fall eines p-adischen Grundkörpers löst Hasse diese Aufgabe in einer großen Arbeit "Über $\wp$-adische Schiefkörper …". Hasse zeigt dort, daß die Arithmetik dieser $\wp$-adischen Schiefkörper in mancherlei Hinsicht bedeutend einfacher ist als im globalen Fall, ja, daß sogar auch gegenüber dem kommutativen Fall wichtige Vereinfachungen auftreten:

(1) $\wp$-adische Schiefkörper D haben nur eine einzige Maximalordnung; sie besteht aus allen ganzen Elementen von D. (2) Die Bewertung des Grundkörpers läßt sich eindeutig und gewissermaßen kommutativ auf D fortsetzen. (3) Restklassengrad und Verzweigungsordnung sind im zentralen Fall stets gleich, $e = f = m$ bei $(D/k) = m^2$. (4) Das Phänomen der irregulären Verzweigung tritt nicht auf; es gilt also hier stets die einfache Differentenformel

$$\mathfrak{D}(D/k) = \wp^{m-1}.$$

Darüberhinaus enthält D stets in der unverzweigten Erweiterung $k^{(m)}/k$ vom Grade m einen maximalen Teilkörper, welcher zyklisch ist und in dem Frobeniusautomorphismus F_m eine ausgezeichnete Erzeugende seiner Galoisgruppe $\mathfrak{G} = \mathrm{Gal}(k^{(m)}/k) = \langle F_m \rangle$ besitzt. Hieraus ergibt sich dann leicht, daß D – und damit allgemeiner jede über k endliche zentrale einfache Algebra A vom Rang $(A/k) = n^2$ – zyklisch darstellbar ist in der Form $A = (\alpha, k^{(n)}, F_n)$ mit passendem $\alpha \in k^\times$. Nach den allgemeinen Regeln

$$(\alpha, K, S) \otimes (\beta, K, S) \sim (\alpha\beta, K, S)$$

und

$$(\alpha, K, S) \sim (\beta, K, S) \iff \beta\alpha^{-1} \in N_{K/k}(K^\times)$$

für zyklische Algebren folgt nun sofort, daß es in jener Darstellung $A = (\alpha, k^{(n)}, F_n)$ nur auf $\mathrm{ord}_\mathfrak{p}(\alpha) \bmod n$ ankommt. Aus diesen und weiteren einfachen Eigenschaften zyklischer Algebren ergibt sich dann als Hauptresultat: *Die Restklasse*

$$\mathrm{inv}\,\mathcal{A} \equiv \frac{\mathrm{ord}_\mathfrak{p}(\alpha)}{n} \mod^+ 1$$

hängt nur von der Klasse $\mathcal{A} = \mathcal{C}(A)$ ab, und die Zuordnung

$$\mathrm{Br}(k) \longrightarrow \mathbb{Q}/\mathbb{Z}, \quad \mathcal{A} \longmapsto \mathrm{inv}\,\mathcal{A} \mod^+ 1$$

liefert einen Isomorphismus der Brauergruppe von k mit der additiven Gruppe der rationalen Zahlen modulo Eins.

Damit ist der lokale Fall erledigt. Als Frucht ergibt sich u. a. eine völlig organische Theorie des Normsymbols im lokalen Fall:

Ist K/k eine zyklische Erweiterung vom Grade n und ist S eine Erzeugende ihrer Galoisgruppe $\mathfrak{G}$, so bilde man die *Invariante*

$$\mathrm{inv}\,\mathcal{A} \equiv \frac{\nu}{n} \mod^+ 1$$

der Klasse $\mathcal{A} = \mathcal{C}(A)$ der zyklischen Algebra $A = (\alpha, K, S)$ und erkläre das *Normsymbol* durch

$$(\alpha, K/k) = S^{-\nu}.$$

Dieselben einfachen Regeln über zyklische Algebren zeigen dann, daß die Zuordnung

$$k^\times \longrightarrow \mathfrak{G}, \quad \alpha \longmapsto (\alpha, K/k)$$

ein kanonischer, d.h. von der Wahl von S ganz unabhängiger Homomorphismus von $k^\times$ auf die volle Galoisgruppe $\mathfrak{G}$ von K/k mit der Normengruppe $N_{K/k}(K^\times)$ als Kern ist, der sich speziell im unverzweigten Fall durch die einfache Formel

$$(\alpha, k^{(n)}/k) = F_n^{-\,\mathrm{ord}_\mathfrak{p}(\alpha)}$$

berechnet.

Nun sei k ein Zahlkörper und bezeichne für jede Primstelle $\mathfrak{p}$ von k jeweils $k_\mathfrak{p}$ den zugehörigen lokalen Körper. Aus jeder Algebra A/k entsteht dann durch Grundkörpererweiterung jeweils auf $k_\mathfrak{p}$ das System der zugehörigen lokalen Algebren $A_\mathfrak{p}/k_\mathfrak{p}$. Die Klasse $\mathcal{A}_\mathfrak{p} = \mathcal{C}(A_\mathfrak{p})$ hängt dabei nur von der Klasse $\mathcal{A} = \mathcal{C}(A)$ ab, und wir erhalten so einen Homomorphismus

$$\mathrm{Br}(k) \longrightarrow \prod_{\mathfrak{p}} \mathrm{Br}(k_\mathfrak{p}), \quad \mathcal{A} \longmapsto (\ldots, \mathcal{A}_\mathfrak{p}, \ldots) \tag{1}$$

der Brauergruppe des globalen Körpers k in das Produkt der Brauergruppen der lokalen Körper $k_\mathfrak{p}$ zu k. Die für die Bestimmung der Brauergruppe entscheidende Tatsache entspricht nun vollständig derjenigen Form des Lokal-Global-Prinzips, welche uns schon in der Theorie der quadratischen Formen entgegengetreten ist; es handelt sich um den

Hauptsatz von Brauer-Hasse-Noether. *Eine Algebrenklasse $\mathcal{A}$ über k zerfällt global, d. h. es gilt $\mathcal{A} = \mathcal{E}$ in $\mathrm{Br}(k)$, genau dann, wenn sie überall lokal zerfällt, wenn also für alle Primstellen $\mathfrak{p}$ von k jeweils $\mathcal{A}_\mathfrak{p} = \mathcal{E}_\mathfrak{p}$ in $\mathrm{Br}(k_\mathfrak{p})$ gilt.*

Anders ausgedrückt: der Homomorphismus (1) ist injektiv!

Der wichtigste Beweisschritt betrifft den Spezialfall einer zyklisch darstellbaren Algebrenklasse $\mathcal{A} = \mathcal{C}(A)$, mit $A = (\alpha, K, S)$, und die entsprechende Teilaussage ist äquivalent mit dem

Hasseschen Normensatz. *Ist K/k zyklisch, so ist ein $\alpha \neq 0$ aus k genau dann Norm eines Elements $A \neq 0$ aus K, wenn α überall lokal eine Norm ist.*

In diesem Zusammenhang ist die Bemerkung interessant, daß man – nach Zorn – den Hauptsatz auch ablesen kann aus dem Polverhalten der einer einfachen Algebra über k zugeordneten Zetafunktion. Auf diese Weise ergibt sich also zugleich ein Beweis des Normensatzes!

Für die vollständige Bestimmung von $\mathrm{Br}(k)$ brauchen wir noch die Angabe des Bildes des Homomorphismus (1)! Unmittelbar aus dem Hauptsatz ergibt sich nun zunächst die Möglichkeit, die sogenannten Zerfällungskörper einer Klasse allein durch eine Bedingung für die lokalen Grade zu charakterisieren: *eine normale Erweiterung K/k ist Zerfällungskörper von $\mathcal{A}$ genau dann, wenn für alle Primstellen $\mathfrak{p}$ von k der lokale Grad $n_\mathfrak{p} = (K_\mathfrak{p}/k_\mathfrak{p})$ durch den Index $m_\mathfrak{p}$ von $\mathcal{A}_\mathfrak{p}$ teilbar ist.*

Es ist nun nicht schwer einzusehen, daß sich diese Bedingungen durch relative Kreiskörper über k realisieren lassen! Damit ergibt sich auch im globalen Fall: *Jede über k endliche zentrale einfache Algebra A ist zyklisch darstellbar: $A = (\alpha, K, S)$. Für K/k kann man dabei eine Kreiskörpererweiterung nehmen.*

Damit ist es nun möglich, das Bild von (1) zu bestimmen! Wir beschreiben es mit Hilfe der Invarianten, also der Restklassen

$$\left(\frac{\mathcal{A}}{\mathfrak{p}}\right) \equiv \operatorname{inv} \mathcal{A}_\mathfrak{p} \mod^+ 1.$$

Für sie gilt notwendig jedenfalls die Endlichkeitsbedingung

$$\left(\frac{\mathcal{A}}{\mathfrak{p}}\right) \equiv 0 \mod^+ 1 \quad \text{für fast alle } \mathfrak{p},$$

denn die übrigen Primstellen sind als die Verzweigungsstellen der zu $\mathcal{A}$ gehörenden Divisionsalgebra nur in endlicher Zahl vorhanden. Weiter gilt ersichtlich die folgende

Zusatzbedingung für die unendlichen Primstellen

$$\left(\frac{\mathcal{A}}{\mathfrak{p}}\right) \equiv 0 \begin{cases} \bmod^+ \frac{1}{2} & \text{für } \mathfrak{p} \text{ reell,} \\ \bmod^+ 1 & \text{für } \mathfrak{p} \text{ komplex,} \end{cases}$$

da im ersten Fall nach Frobenius nur die Klasse der Quaternionenalgebra, im übrigen aber überhaupt keine von $\mathcal{E}_\mathfrak{p}$ verschiedene Algebrenklasse über k vorhanden ist. Benutzt man nun einen geeigneten relativen Kreiskörper K/k für die zyklische Darstellung $A = (\alpha, K, S)$ und beachtet man das für diesen Spezialfall sehr einfach zu beweisende Reziprozitätsgesetz, so erhält man als weitere entscheidende Einschränkung den

Summensatz *für die Invarianten*

$$\sum_\mathfrak{p} \left(\frac{\mathcal{A}}{\mathfrak{p}}\right) \equiv 0 \bmod^+ 1.$$

Es zeigt sich nun, daß diese Bedingungen auch hinreichend sind: zu jedem System von Restklassen $\rho_\mathfrak{p} \bmod^+ 1$, das ihnen genügt, gibt es eine Klasse

$$\mathcal{A} \quad \text{mit} \quad \left(\frac{\mathcal{A}}{\mathfrak{p}}\right) \equiv \rho_\mathfrak{p} \bmod^+ 1 \quad \text{für alle } \mathfrak{p}.$$

Dazu zeigt man, daß $\mathcal{A} = \mathcal{C}(A)$ mit $A = (\alpha, K, S)$ für einen geeigneten relativen Kreiskörper K/k bei passender Wahl von $\alpha \in k^\times$ diese vorgegebenen Invarianten hat. Damit ist dann $\mathrm{Br}(k)$ auch im globalen Fall vollständig bestimmt.

Genau wie im lokalen Fall läßt sich die Strukturtheorie der Brauergruppe für eine organische Begründung der **Theorie des Normenrestsymbols** heranziehen: Sei dazu wieder K/k eine zyklische Erweiterung vom Grad n mit S als erzeugendem Automorphismus. Man bilde $\mathcal{A} = \mathcal{C}(A)$ für $A = (\alpha, K, S)$, definiere $\nu_\mathfrak{p} \bmod n$ durch

$$\left(\frac{\mathcal{A}}{\mathfrak{p}}\right) \equiv \frac{\nu_\mathfrak{p}}{n} \bmod^+ 1$$

und setze

$$\left(\frac{\alpha, K/k}{\mathfrak{p}}\right) = S^{-\nu_\mathfrak{p}}.$$

Aus den Eigenschaften und Rechenregeln für zyklische Algebren ergibt sich dann genau wie im lokalen Fall, daß die Abbildung

$$k^\times \longrightarrow \mathfrak{G}, \quad \alpha \longmapsto \left(\frac{\alpha, K/k}{\mathfrak{p}}\right)$$

von k in die Galoisgruppe $\mathfrak{G}$ von K/k ein von der Wahl von S unabhängiger, also kanonischer Homomorphismus auf die Zerlegungsgruppe $\mathfrak{G}_\mathfrak{p}$ mit der Gruppe der Normenreste mod $\mathfrak{f}_\mathfrak{p}$ (also der Gruppe der lokalen Normen) als Kern ist, der sich für in K/k unverzweigte Primstellen aus der Formel

$$\left(\frac{\alpha, K/k}{\mathfrak{p}}\right) = F_\mathfrak{p}^{-\operatorname{ord}_\mathfrak{p}(\alpha)}$$

in einfacher Weise durch den zugehörigen Frobeniusautomorphismus berechnen läßt und damit insbesondere der Endlichkeitsbedingung

$$\left(\frac{\alpha, K/k}{\mathfrak{p}}\right) = 1 \text{ für fast alle } \mathfrak{p}$$

genügt. Fügt man noch den Normensatz und die sich aus dem Summensatz für die Invariante ergebende **Produktformel für das Normenrestsymbol**

$$\prod_{\mathfrak{p}} \left(\frac{\alpha, K/k}{\mathfrak{p}}\right) = 1$$

hinzu, so ist die Theorie des Normenrestsymbols in allen wesentlichen Punkten vollständig. In dieser Weise wird die Bestimmung der Struktur der Brauergruppe $\mathrm{Br}(k)$ von k zum Instrument, um aus dem elementar zugänglichen Reziprozitätsgesetz für relative Kreiskörper über k den wesentlichen Teil des allgemeinen Artinschen Reziprozitätsgesetzes herzuleiten, denn darum handelt es sich ja bei der Produktformel für das Normenrestsymbol!

Die so diffizile Frage nach organischer Begründung des allgemeinen Reziprozitätsgesetzes in k verschmilzt mit der ganz konkreten Frage nach den endlichen zentralen Divisionsalgebren über k. Nicht ohne Wehmut werden wir Jüngeren daran denken, was daraus geworden ist, wie die Brauergruppe als zweite Kohomologiegruppe sich zwar einfügt in einen ebenso effektiven wie umfassenden Kalkül, dem man die Antwort auf die erste Frage heute zu entnehmen pflegt, wie sie dabei aber auch um so blasser wird, je mehr sich ihr in der zweiten Frage angesprochener konkreter Inhalt dabei als entbehrliche Zugabe verflüchtigt.

Gehen wir über zum nächsten Punkt, den ich hier herausgreifen möchte, zum

Beweis des Analogons der Riemannschen Vermutung für elliptische Kongruenzfunktionenkörper

Noch im selben Jahr 1932, das mit der großen Arbeit über die "Struktur der Richard Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper" den Höhepunkt und damit im wesentlichen auch den Abschluß der Arbeiten zur Arithmetik der Algebren einerseits, zur Begründung der Theorie des Normenrestsymbols und des allgemeinen Reziprozitätsgesetzes andererseits bringt, erscheint auch schon die Vorankündigung kommender Ereignisse in einer vorläufigen Mitteilung in den Nachrichten der Akademie in Göttingen mit dem Titel: "Beweis des Analogons der Riemannschen Vermutung für die Artinsche und F. K. Schmidtsche Kongruenz-Zetafunktion in gewissen elliptischen Fällen". Es handelt sich dabei um das folgende allgemeine Problem: Gegeben sei ein absolut irreduzibles Polynom $f(x, y)$ mit Koeffizienten aus dem endlichen Körper $k = \mathbb{F}_q$ von q Elementen. Gesucht ist die Anzahl N der Lösungen (ξ, η) in $\mathbb{F}_q$ der Gleichung

$$f(\xi, \eta) = 0.$$

Der "elliptische Fall" ist hier im wesentlichen der Spezialfall

$$f(x, y) = y^2 - f_3(x)$$

mit einem kubischen Polynom $f_3(x)$ ohne mehrfache Faktoren. Zur Vorgeschichte möchte ich zunächst Hasse selbst zitieren. Er sagt an anderer Stelle, nachdem er von den für diesen Spezialfall kurz vorher von Davenport bzw. Mordell erzielten Abschätzungen

$$|N - p| \leq \text{const.}\, p^{\theta} \quad \text{mit} \quad \theta = \frac{3}{4} \text{ bzw. } = \frac{2}{3}$$

im Fall $q = p$ Primzahl berichtet:

> 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 Hilfsmitteln 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.

Wenn ein Mathematiker etwas von einem Analogon zur Riemannschen Vermutung hört, so denkt er an eine Aussage über die Lage von Nullstellen einer Zetafunktion. Davon ist hier zunächst nicht die Rede. Verfolgen wir also die Vorgeschichte ein Stückchen weiter zurück, um den Zusammenhang deutlich zu machen!

Es handelt sich hier um quadratische Erweiterungen K/P des rationalen Funktionenkörpers $P = \mathbb{F}_p(t)$. Solche Körper wurden in einer anderen gewichtigen Dissertation des Jahres 1921 erstmalig untersucht, in der Artinschen Arbeit "Über quadratische Körper im Gebiet der höheren Kongruenzen". Artin nimmt einen nichtinvarianten Standpunkt ein, indem er die Variable t oder also den Ring $\Gamma = \mathbb{F}_p[t]$ auszeichnet. Davon abgesehen entwickelt er die Theorie in weitestgehender Analogie zur Theorie der quadratischen Zahlkörper, wobei er sich meist idealtheoretischer Methoden bedient. Im analytischen Teil führt er die zugehörige Kongruenz-Zetafunktion ein und wirft die Frage auf, ob das Analogon der Riemannschen Vermutung für diese Kongruenz-Zetafunktionen richtig ist. In allen von ihm explizit behandelten Spezialfällen, etwa 40 an der Zahl, kann er das bestätigen. 8 Jahre später, 1929, entwickelt F. K. Schmidt in seiner grundlegenden Arbeit "Analytische Zahlentheorie in Körpern der Charakteristik p" die Theorie der Kongruenzfunktionenkörper, d. h. der endlich erzeugbaren Erweiterungen K/k vom Transzendenzgrad 1 eines endlichen Körpers $k = \mathbb{F}_q$, von dem wir ohne Einschränkung annehmen können, daß er in K algebraisch abgeschlossen ist, und der ihnen zugeordneten Kongruenz-Zetafunktion

$$\zeta_{K/k}(s) = \sum_{\mathfrak{g}} N(\mathfrak{g})^{-s} = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}$$

allgemein und körperinvariant in der hierfür besser geeigneten Sprechweise der Divisorentheorie. In ihr entsprechen die Primdivisoren $\mathfrak{p}$ umkehrbar eindeutig den diskreten normierten Exponentenbewertungen $\mathrm{ord}_{\mathfrak{p}}(\cdot)$ von K/k, sind die ganzen Divisoren $\mathfrak{g}$ deren Potenzprodukte und ist die Norm $N(\mathfrak{g})$ multiplikativ derart erklärt, daß jeweils $N(\mathfrak{p}) = |K\mathfrak{p}| = q^{d(\mathfrak{p})}$ die Elementanzahl des Restklassenkörpers $K\mathfrak{p}$ von K mod $\mathfrak{p}$ ist. Schreiben wir beliebige Divisoren $\mathfrak{a}$ von K/k in der Form

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}} \text{ mit } a_{\mathfrak{p}} \in \mathbb{Z} \text{ und } a_{\mathfrak{p}} = 0 \text{ für fast alle } \mathfrak{p},$$

so erweist sich der homomorph erweiterte Divisorgrad

$$d(\mathfrak{a}) = \sum_{\mathfrak{p}} d(\mathfrak{p}) a_{\mathfrak{p}}$$

als Klassenfunktion, d. h. es gilt

$$d(\mathfrak{a}) = d(C) \text{ für } C = \mathfrak{a}H,$$

wo H die Gruppe der den Elementen $x \in K^\times$ zugeordneten Hauptdivisoren

$$\mathfrak{h}_x = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(x)}$$

bezeichnet. Dieselbe Eigenschaft, Klassenfunktion zu sein, also

$$\dim \mathfrak{a} = \dim C \quad \text{für} \quad C = \mathfrak{a}H,$$

hat die Dimension $\dim \mathfrak{a}$ des k-Vektorraums

$$L(\mathfrak{a}) = \{x \in K^\times \,|\, \mathrm{ord}_{\mathfrak{p}}(x) \geq -a_{\mathfrak{p}} \text{ für alle } \mathfrak{p}\}$$

der Vielfachen von $\mathfrak{a}^{-1}$. Der Riemann-Rochsche Satz

$$\dim C = d(C) - (g-1) + \dim \frac{W}{C}$$

gewinnt die ihm zukommende zentrale Rolle. Dabei bezeichnet W die sogenannte *Differentialklasse* und $g = \dim W$ das Geschlecht von K/k. Als einfache Folge ergibt sich die *Funktionalgleichung*

$$q^{(g-1)s}\zeta_{K/k}(s) \text{ ist invariant bei } s \longmapsto 1-s.$$

Das Analogon der Riemannschen Vermutung, also die Frage, ob alle Nullstellen von $\zeta_{K/k}(s)$ den Realteil $\mathrm{Re}(s) = \frac{1}{2}$ besitzen, wird erstmalig allgemein aufgeworfen. Der Beweis der Funktionalgleichung setzt dabei die Tatsache in Evidenz, daß die Kongruenz-Zetafunktion eine rationale Funktion von $U = q^{-s}$ ist. Genauer gilt, was allerdings erst ein wenig später deutlich wird,

$$\zeta_{K/k}(s) = \zeta_{K_0/k}(s)L_{K/k}(s),$$

wobei die Kongruenzzetafunktion des rationalen Körpers $K_0 = k(t)$ durch

$$\zeta_{K_0/k}(s) = \frac{1}{(1-q^{-s})(1-q^{1-s})}$$

gegeben ist und $L_{K/k}(s)$ ein Polynom in $U = q^{-s}$ vom Grade $2g$ mit ganzen rationalen Koeffizienten von der Gestalt

$$L_{K/k}(s) = 1 + \{N_1 - (q+1)\}q^{-s} + \ldots + q^g \cdot q^{-2gs}$$

bezeichnet, das demnach etwa über dem komplexen Zahlkörper in der Form

$$L_{K/k}(s) = \prod_{\nu=1}^{2g} \left(1 - \frac{\omega_\nu}{q^s}\right)$$

zerfällt. Als Analogon der Riemannschen Vermutung kann man somit die Aussage ansehen, daß die in q^s gemessenen Nullstellen $\omega_1, \ldots, \omega_{2g}$ dieses Polynoms sämtlich den Betrag

$$|\omega_\nu| = \sqrt{q} \quad (\nu = 1, \ldots, 2g)$$

haben. Für die Anzahl N_1 der Primdivisoren ersten Grades ergibt sich unter Annahme der Richtigkeit der Riemannschen Vermutung nun sofort die Abschätzung

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

Tatsächlich ist nun diese letzte Ungleichung mit dem Analogon der Riemannschen Vermutung sogar äquivalent, was man unschwer erkennt, wenn man K/k zusammen mit allen endlichen Konstantenerweiterungen $Kk^{(d)}/k^{(d)}$ betrachtet. Soweit ich sehen kann, wird dieser Zusammenhang erstmals in einer (unter Benutzung von Mitteilungen von F. K. Schmidt und E. Artin verfaßten) Note von Hasse "Über Kongruenz-Zetafunktionen" in den Sitzungsberichten der Berliner Akademie aus dem Jahre 1934 entwickelt. Sie enthält auch die "gewöhnliche Deutung" dieser Ungleichung: Ist etwa

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

eine geeignete Erzeugung von K/k, so entsprechen die Primdivisoren $\mathfrak{p}$ vom ersten Grade vermöge

$$\mathfrak{p} \leftrightarrow (\xi, \eta) : x \equiv \xi, y \equiv \eta \pmod{\mathfrak{p}}$$

im wesentlichen umkehrbar eindeutig den Punkten (ξ, η) aus k auf der Kurve

$$f(\xi, \eta) = 0.$$

Dies gilt sogar exakt, wenn keine "singulären Punkte" vorhanden sind und auch die "Punkte im Unendlichen" mit einbezogen werden, indem man also die Kurve projektiv (und nicht affin) betrachtet. Damit ist der Zusammenhang mit dem eingangs formulierten Problem hergestellt und zugleich eine birational invariante Formulierung gefunden.

Im elliptischen Fall nun ist $g = 1$, ist also $L_{K/k}(s) = \mathcal{L}(q^{-s})$ ein quadratisches Polynom in $U = q^{-s}$; das Analogon der Riemannschen Vermutung lautet hier also einfach: Die beiden Nullstellen ω_1, ω_2 sind entweder konjugiert komplex oder reell mit gleichem Betrag.

Hasse beweist diese Aussage, indem er gewissermaßen die begriffliche Bedeutung dieser Nullstellen freilegt. Es ist ein beredtes Zeugnis für die Kraft der algebraischen Methode, daß man sagen kann: Dies geht völlig naturgemäß und fast zwangsläufig vor sich. Zunächst verschafft Hasse sich dazu das Analogon der Torusgruppe der klassischen Theorie der elliptischen Funktionenkörper in der additiven Gruppe $\mathcal{A}$ der algebraischen Punkte. Körpertheoretisch betrachtet (und damit die Sonderstellung von singulären oder unendlich fernen Punkten vermeidend) sind dies die Primdivisoren $\overline{\mathfrak{p}}$ der algebraisch abgeschlossenen Konstantenerweiterung $\mathcal{K} = K\overline{k}$. Nach Wahl eines Bezugsprimdivisors $\mathfrak{o}$ vom Grad eins von K/k – der dann zum Nullpunkt von $\mathcal{A}$ wird – entsprechen die $\overline{\mathfrak{p}}$ umkehrbar eindeutig den Nullklassen C_0 von $\mathcal{K}/k$ vermöge

$$\overline{\mathfrak{p}} \leftrightarrow C_0 = \frac{\overline{\mathfrak{p}}}{\mathfrak{o}} H,$$

die Addition in $\mathcal{A}$ kann nun eindeutig aus der Nullklassengruppe von $\mathcal{K}/k$ bezogen werden,

$$\overline{\mathfrak{p}} = \overline{\mathfrak{p}}' + \overline{\mathfrak{p}}'' \leftrightarrow \frac{\overline{\mathfrak{p}}}{\mathfrak{o}} \sim \frac{\overline{\mathfrak{p}}'}{\mathfrak{o}} \cdot \frac{\overline{\mathfrak{p}}''}{\mathfrak{o}},$$

und die Primdivisoron ersten Grades von K/k bilden die Untergruppe $\mathcal{G}$ der rationalen Punkte, deren Ordnung $|\mathcal{G}| = N_1$ gesucht wird. Wie läßt sich $\mathcal{G}$ innerhalb $\mathcal{A}$ charakterisieren? Geht man über zu den Koordinaten der Punkte auf der Kurve, so ist klar, daß diese genau dann zum Grundkörper $k = \mathbb{F}_q$ gehören, wenn sie bei der Potenzierung mit q invariant sind. Der von der Potenzierung mit q bewirkte *Frobeniusendomorphismus* π von $\mathcal{A}$ gestattet nun in der Tat, die Gruppe $\mathcal{G}$ der rationalen Punkte innerhalb $\mathcal{A}$ zu charakterisieren: erwartungsgemäß ist $\mathfrak{p} \in \mathcal{G}$ genau dann, wenn $\pi\mathfrak{p} = \mathfrak{p}$ ist. Die begriffliche Deutung der Nullstellen ω_1, ω_2 liegt nun darin, daß sich $\mathcal{L}(U)$, d.h. genauer das dazu reziproke Polynom

$$\mathcal{F}_\pi(U) = U^2 \mathcal{L}(U^{-1}),$$

als – wie wir heute sagen würden – das charakteristische Polynom eben dieses Frobeniusendomorphismus π erweist.

Um dieses charakteristische Polynom berechnen und so seine Identität mit dem zu $\mathcal{L}(U)$ reziproken Polynom erkennen zu können, muß man die grundlegenden Tatsachen über die Struktur des Endomorphismenrings von $\mathcal{A}$ herleiten. All dies wird von Hasse mit rein algebraischen Mitteln geleistet. Dabei stellt sich heraus, daß – genau wie im klassischen Fall – neben den ganzrationalen Zahlen als trivialen "Multiplikatoren" von $\mathcal{A}$ höchstens noch solche "komplexen Multiplikatoren" in Betracht kommen, welche ganz imaginär-quadratisch über $\mathbb{Z}$ sind. Der "Multiplikatorenring" ist dann eine Ordnung eines imaginär-quadratischen Zahlkörpers oder einer definiten Quaternionenalgebra. Insbesondere haben die beiden Nullstellen des Hauptpolynoms $\mathcal{F}_\mu(U)$ eines solchen Multiplikators μ stets denselben Betrag, was für $\mu = \pi$ gerade die als Analogon der Riemannschen Vermutung bezeichnete Aussage ist.

Ganz kurz nur einige Bemerkungen darüber, wie sich die dieses schöne Ergebnis begründende Untersuchung des Endomorphismenrings – in klassischem Sinne also der "Multiplikatoren" – von $\mathcal{A}$ entwickelt: Betrachtet man den klassischen Fall mit den Augen eines Algebraikers, so sieht man, diesen Multiplikatoren entsprechen Isomorphismen des zugehörigen Funktionenkörpers in sich (Meromorphismen) und umgekehrt, jeder solche Isomorphismus – läßt er nur den Bezugspunkt $\mathfrak{o}$ fest – liefert einen solchen Multiplikator. Diese Isomorphismen μ aber entsprechen offensichtlich den Lösungen $(x\mu, y\mu)$ in $\mathcal{K}$ einer K/k und damit $\mathcal{K}/\overline{k}$ definierenden Gleichung $f(x, y) = 0$, die sich ihrerseits wie oben durch die Primdivisoren ersten Grades $\mathfrak{P}$ eines durch dieselbe Grundgleichung über $\mathcal{K}$ als Konstantenkörper definierten elliptischen Funktionenkörper $\mathfrak{K}/\mathcal{K}$ beschreiben lassen. Damit hat man das algebraische Hilfsmittel gewonnen, um die gestellte Aufgabe zu lösen, und – in der gröberen Nullklassengruppe von $\mathfrak{K}/\mathcal{K}$ – zugleich die additive Struktur des zu untersuchenden Multiplikatorenbereichs. Die Multiplikation ergibt sich – wie immer bei Endomorphismen – durch Schachtelung. Die als Grad über dem Bildkörper erklärte Norm

$$n(\mu) = (\mathcal{K}/\mathcal{K}\mu)$$

eines Multiplikators μ ist also ersichtlich multiplikativ und für $\mu \neq 0$ nur positiver Werte fähig. Das Herzstück der Theorie liegt nun im Verhalten dieser Norm gegenüber der Addition, liegt in der Normenadditionsformel

$$n(\mu + \nu) + n(\mu - \nu) = 2n(\mu) + 2n(\nu).$$

Aus ihr ergibt sich dann leicht, daß

$$Q_{\mu,\nu}(a, b) = n(a\mu + b\nu)$$

eine positiv semidefinite quadratische Form von $a, b \in \mathbb{Z}$ ist, daß insbesondere

$$\mathcal{F}_\mu(U) = n(U1 - \mu)$$

mit dem identischen Multiplikator 1 von $\mathcal{A}$ das gesuchte Hauptpolynom von μ über $\mathbb{Z}$ ist. Die Normadditionsformel fließt aus dem Additionstheorem für die "große" Konstantenerweiterung $\mathfrak{K}/\mathcal{K}$ und entspricht der 2-Dimensionalität von $\mathcal{A}$ im klassischen Fall, welche Hasse der ganzen Untersuchung in der folgenden rein algebraischen Form voranstellt: Ist die Charakteristik p von k kein Teiler von n, so hat die Untergruppe $\mathcal{A}_n$ der n-Teilungspunkte von $\mathcal{A}$ die Ordnung

$$|\mathcal{A}_n| = n^2.$$

Daß sich die Grundtatsachen der klassischen Theorie der elliptischen Funktionen in so organischer Weise rein algebraisch fassen lassen und in ihrer systematischen Anwendung auf endliche Körper so zu weitreichenden und neuartigen Ergebnissen führen, die sich von der klassischen Theorie her gesehen nicht einmal erahnen lassen, ist sicher ein ganz außerordentlicher Erfolg der "algebraischen Methode" gewesen.

In der Folgezeit wird dieses machtvolle Hilfsmittel, die arithmetische Theorie der algebraischen Funktionen im Verein mit anderen systematisch ausgebaut, wird begonnen, das für $g = 1$ Erreichte auch für den Fall eines Geschlechts $g > 1$ vorzubereiten: eine arithmetische Theorie der abelschen Funktionenkörper beginnt zu entstehen. Doch dieser vielleicht fruchtbarsten Zeit setzt der Krieg ein jähes Ende.

1945!

Im August dieses Jahres schließt Hasse die Arbeit an der ersten Veröffentlichung ab, die der Nachkriegszeit angehört, schreibt er das Vorwort nieder zur Monographie "Über die Klassenzahl der abelschen Zahlkörper". Dieser zweiten Schaffensperiode allein, die damit anhebt, gehören heute schon mehr als 100 Publikationen an, wobei sich der Themenkreis fast noch weiter fächert als zuvor. Doch ich möchte meinen Überblick ausklingen lassen mit diesem Buch, genauer mit seinem auf

Abelsche Zahlkörper

gerichteten Programm und dem, was daraus geworden ist.

Der Titel schon signalisiert, um was es sich handelt: die Wiederaufnahme der Arbeit nach dem Kriege beginnt mit einer Rückbesinnung auf den Ursprung der algebraischen Zahlentheorie bei Kummer. Das Vorwort ist ein Bekenntnis zu den Quellen zahlentheoretischen Tuns. Gerade als solches ist es auch heute noch ein Dokument, das zu lesen sich lohnt und jedem ernsthaft Interessierten sehr empfohlen werden kann! Ich möchte mir erlauben einige Sätze dieses Vorworts zu zitieren!

Nachdem er zunächst geschildert hat, wie sich die algebraische Zahlentheorie unter dem Einfluß Hilberts vom Zahlbericht hin zur Klassenkörpertheorie entfaltet, sagt Hasse:

> Bei dieser ganzen Entwicklung ... ist nun aber das jedem echten Zahlentheoretiker eigene Bedürfnis nach expliziter Beherrschung des behandelten Gegenstandes bis zur Durchführung numerischer Beispiele stark in den Hintergrund getreten. Fragt man heute einen Zahlentheoretiker, für welche Typen algebraischer Zahlkörper er in der Lage ist, die Gesetzlichkeiten der allgemeinen Theorie durch explizite Aufstellung der allgemeinen Strukturinvarianten für den betreffenden Körpertypus zu erläutern oder auch als Vorbereitung dazu nur etwa eine Ganzheitsbasis, die Diskriminante, ein Grundeinheitensystem und die Klassenzahl nach einem systematischen strukturinvarianten Verfahren zu gewinnen, so wird, wenn er ehrlich ist, die Antwort im allgemeinen lauten: nur für die quadratischen Zahlkörper.

Und es erinnert an Kronecker, wenn wir da weiter über die Rollo der Beispiele lesen:

> Mit vollem Recht tritt in der Physik neben die Vorlesung über Experimentalphysik das physikalische Praktikum, in dem das rezeptiv Erlernte in eigener Aktivität befestigt werden soll. Eine ganz

> entsprechende Rolle hat in der Zahlentheorie die Durchführung numerischer Beispiele. Darüber hinaus sind sie in der Hand des forschenden Mathematikers genau das, was für den Physiker das Experiment ist, nämlich eines der Hauptmittel zur Auffindung neuer Gesetzlichkeiten.

Solche Gedanken sind natürlich nicht neu, denn von ihren Wurzeln her ist die Zahlentheorie zu allen Zeiten auch und vor allem eine induktive Wissenschaft gewesen, von dort her bezieht sie ihre Kraft und den ihr eigenen Reiz. Ein Blick etwa auf die Zahlentheorie der elliptischen Kurven – um ein Beispiel aus der jüngsten Zeit zu nehmen – wird bestätigen, daß diese Feststellung auch heute noch unverändert gilt.

Hasse sagt dann weiter:

> Wie man sich in der Musik nach der in heroischen und dämonischen Werken und in kühnsten Phantasien schwelgenden romantischen und nachromantischen Epoche heute bei aller Freude an diesem Schaffen doch auch wieder stärker auf den Urquell reiner und schlichter Musikalität der alten Meister besinnt, so scheint mir auch in der Zahlentheorie, die ja wie kaum eine andere mathematische Disziplin von dem Gesetz der Harmonie beherrscht wird, eine Rückbesinnung auf das geboten, was den großen Meistern, die sie begründet haben, als ihr wahres Gesicht vorgeschwebt hat.

Damit ist sicherlich nicht gemeint, daß diese Rückbesinnung auch eine solche in der Wahl des Gegenstandes oder der Form seiner Behandlung sein muß. Die Zahlentheorie ist vielmehr trotz ihres Alters erstaunlich vital. Als erstes Beispiel möchte ich abermals die Arithmetik der elliptischen Kurven erwähnen, die Resultate und Vermutungen von Birch, Cassels, Swinnerton-Dyer, Tate und anderen, in denen dieses Gesetz der Harmonie in unübertrefflicher Weise zum Ausdruck kommt. Diese Vitalität kommt jedoch auch dann zum Durchbruch, wenn man – wie Hasse es hier tut – als Gegenstand denjenigen Ideenkreis wählt, aus dem die algebraische Zahlentheorie rund 100 Jahre zuvor entsprang. Um dies etwas deutlicher machen zu können, erlauben Sie mir, daß ich zu guter letzt noch einige mehr persönliche Worte hinzufüge:

Es war im Sommersemester 1948, als ich mich, gerade mein zweites Studiensemester beginnend, in Berlin in Ihre Vorlesung über Elementare Zahlentheorie setzte, und es war wohl auch Ihre erste Vorlesung in Berlin nach dem Kriege. In der ersten Stunde dieser Vorlesung sprachen Sie, Herr Hasse, mindestens ebensoviel über Musik wie über Zahlentheorie, und beschworen in mir persönlich unvergeßlicher Weise beider innere Verwandtschaft. Ohne daß ich es damals wußte, hatte sich damit für mich entschieden, wohin im Reich der Mathematik mich meine Wünsche ziehen würden.

An diesem Ihrem Programm, als dessen erster Teil die Klassenzahlmonographie gedacht war, habe ich dann mitzuarbeiten versucht. Es handelte sich um die systematische und rechnerische Erschließung der abelschen Zahlkörper, ein – der Zeit entsprechend – durch und durch im besten Sinne konservatives Programm. Dem entsprechen auch meine ersten Beiträge dazu (über Geschlechtertheorie, über Einheitengruppe und Klassenzahl, über die Hauptordnung der ganzen Elemente usw.), alle dafür bestimmt, es realisieren zu helfen, was mir bis zu einem gewissen Grade wohl auch gelungen ist. Spätere Beiträge haben ihre Wurzeln zunehmend auch in der Faszination selbst, die von der analytischen Klassenzahlformel für diese Körper ausgeht. Im Bemühen, sie besser und besser zu verstehen, haben sich am Beispiel dieser Körperklasse Einsichten herausgeschält, deren Bedeutung über die Klasse der absolut abelschen Zahlkörper weit hinausreicht und, welche die Frage nach den Beziehungen zwischen einem Zahlkörper K und seiner Zetafunktion $\zeta_K(s)$, genauer den rationalen Werten dieser Zetafunktion für negativ-ganzzahliges Argument $s = 1 - m$ mit $m \in \mathbb{N}$, völlig neu beleuchten.

Den Ausgangspunkt bildete die Frage, wie sich das klassische Kriterium von Kummer, nach welchem eine Primzahl p genau dann in der Klassenzahl h_K des Körpers $K = \mathbb{Q}^{(p)}$ der p-ten Einheitswurzeln steckt, wenn p im Zähler einer der ersten $\frac{p-3}{2}$ Bernoullischen Zahlen B^{2n} $(n = 1, \ldots, \frac{p-3}{2})$ aufgeht, wie sich dieses rein rationale Kriterium auf beliebige abelsche Zahlkörper übertragen läßt. Die Tatsache, daß es sich bei den B^m entsprechend

$$\zeta_{\mathbb{Q}}(1-m) = -\frac{B^m}{m}$$

um Zetawerte handelt, wenn auch zum "falschen" Körper $K = \mathbb{Q}$ gehörige, wurde allerdings erst dadurch interessant, daß in einer jüngeren Arbeit auch Artin, Ankeny und Chowla bei der Herleitung von Klassenzahlkongruenzen reeller quadratischer Zahlkörper nach Verzweigungsprimzahlen auf Zetawerte gestoßen waren, anscheinend ohne sie als solche zu erkennen, und zwar wiederum zu einem "falschen" Körper gehörend. Die Aufklärung dieses merkwürdigen Tatbestands konnte ich dann in der, ganz analog zur analytischen Klassenzahlformel gebildeten und für beliebige reelle abelsche Zahlkörper einerseits und beliebige ungerade, im Grad nicht aufgehende Primzahlen p andererseits gültigen **Klassenzahlformel mod** p geben

$$\frac{2^{n_K-1} h_K R_{K,(p)}}{\sqrt{|d_K|}} \equiv \left(\frac{d_K}{p}\right)\frac{\zeta_K}{\zeta_{\mathbb{Q}}}(2-p) \bmod p;$$

in ihr ist lediglich der klassische Regulator durch den mit Hilfe der *Fermatquotienten* an Stelle der Logarithmen, im übrigen aber analog gebildeten *Restklassenregulator* mod p zu ersetzen. Es war mir klar, daß dies nur eine erste Approximation des wahren Tatbestands sein konnte. Um ihn im vollen Umfang aufzudecken, habe ich in einer gemeinsamen Arbeit mit Kubota diese rationalen Zetawerte für negatives ganzzahliges Argument benutzt, um die Zetafunktion eines reellen abelschen Zahlkörpers gewissermaßen "ins p-adische" fortzusetzen. Innerhalb ihres Existenzbereichs hat diese *p-adische Zetafunktion* – wie wir heute wissen: nahezu exakt – dieselben Eigenschaften, gelten für sie dieselben Formeln wie im klassischen "komplexen" Fall, soweit sich dies irgendwie erwarten läßt. Insbesondere ist die Klassenzahlformel mod p nur die erste Näherung einer *p-adischen Klassenzahlformel*, die man – grob gesagt – durch p-adische Uminterpretation der in die klassische Formel eingehenden Größen erhält, soweit eine solche Uminterpretation überhaupt notwendig ist. Und dies gilt für jede der beiden Versionen dieser Formel, ob mit oder ob ohne "Summation" der eingehenden $L(1,\chi)$-Werte.

So hat sich das damals von Ihnen, Herr Hasse, begonnene Programm nicht nur im Sinne seiner ursprünglichen Konzeption zu einem guten Teil erfüllen lassen, sondern ist auch die an seinem Anfang stehende Aufgabe, diese Klassenzahlformel besser verstehen zu lernen, zu einem Schlüssel geworden, der neue Türen aufschloß, von deren Vorhandensein damals wohl niemand etwas ahnen konnte. Aber verstehen wir diese faszinierende Formel heute wirklich besser? Denkt man an den großen Bogen, der von der klassischen Formel über deren global-arithmetisch-gruppentheoretische Deutung zu ihrer p-adischen Uminterpretation führt, wohingegen (jedenfalls heute noch) jeder Ansatz fehlt, ihr p-adisches Analogon mit p-adisch analytischen Methoden direkt zu beweisen, so möchte man eher sagen: diese Formel gibt uns mehr Rätsel auf als je zuvor! Um so mehr, als man vermuten muß, daß die hier im abelschen Fall sichtbar gewordenen Zusammenhänge für beliebige totalreelle Zahlkörper gültig sind. Daß es Serre gelungen ist, die Fortsetzbarkeit der Zetafunktion ins p-adische in dieser Allgemeinheit zu beweisen, ist dafür sicherlich wohl mehr als nur ein erster Schritt.

Beginnend mit Ihrer Monographie, Herr Hasse, hat so der wohl älteste Ast am Baum der algebraischen Zahlentheorie einen neuen kräftigen grünen Zweig hervorgebracht. Nehmen wir dies als ein Zeichen für die Vitalität dieses Baumes und wünschen wir dem Jubilar die gleiche (oder doch eine vergleichbare) Lebenskraft, auf daß sein Interesse und seine Schaffenskraft ihm und uns noch lange erhalten bleiben!

Eingegangen am 15. Dezember 1972