# 120 JAHRE HILBERTS ZAHLBERICHT

FRANZ LEMMERMEYER

Nach der Gründung der DMV im Jahre 1890 gab diese eine Reihe von Berichten über Teilgebiete der Mathematik in Auftrag, die im Laufe der Jahre in den Jahresberichten und später als Sonderbände erschienen. Beim Treffen der DMV 1893 in München wurden Hermann Minkowski und David Hilbert gebeten, einen solchen Bericht über die Zahlentheorie zu schreiben. Daraufhin einigten sie sich dahingehend, dass Hilbert über die Theorie der algebraischen Zahlkörper berichten, Minkowski dagegen die elementare Zahlentheorie (einschließlich der Theorie quadratischer Formen und der Elemente der analytischen Zahlentheorie) übernehmen solle. Minkowski empfand die Arbeit an seinem Teil des Berichts bald als Last, die ihn von der Ausarbeitung seiner Geometrie der Zahlen abhielt, und so konnte 1897 nur Hilberts Bericht erscheinen.

Die in den Jahresberichten veröffentlichten Berichte waren von sehr unterschiedlicher Qualität. Dass der Bericht Hilberts im eigentlichen Sinne des Wortes herausragend ist zeigt sich auch daran, dass dieser Bericht als einziger einen eigenen Namen bekommen hat: Vermutlich war es Rudolf Fueter, der in seiner Dissertation [26] unter Hilbert im Jahre 1903 den Namen *Zahlbericht* erstmals benutzt hat. Ein weiterer Hinweis auf die Ausnahmestellung von Hilberts *Zahlbericht* ist die Tatsache, dass die DMV diesem Bericht einen Artikel zum nur im babylonischen Sexagesimalsystem ganz runden 120ten Geburtstag widmet.

## 1. Von Gauss zu Hilbert

Wie viele andere Zweige der Zahlentheorie kann man auch die Theorie der Zahlkörper mit den Gaußschen *Disquisitiones* beginnen lassen, selbst wenn erste Versuche des Rechnens mit algebraischen Zahlen schon in Eulers Lösung der diophantischen Gleichung $x^3 = y^2+2$ durch die Zerlegung $y^2+2 = (y+\sqrt{-2}\,)(y-\sqrt{-2}\,)$ und in Lagrange's Untersuchungen seiner „fonctions semblables“ zu finden sind. Eine ebenso detaillierte wie beeindruckende Beschreibung der Entwicklung der Zahlentheorie von Gauß bis Hilbert, vor allem vor dem Hintergrund des dominierenden Einflusses der Gaußschen *Disquisitiones*, haben C. Goldstein und N. Schappacher in den beiden Artikeln [30, 31] gegeben, auf die wir ausdrücklich verweisen wollen.

Wir konzentrieren uns hier auf die Entwicklung der Reziprozitätsgesetze und beginnen mit dem quadratischen Reziprozitätsgesetz. In Legendres Version geht es dort um quadratische Restsymbole $(\frac{a}{p})$ für ungerade Primzahlen $p$ und zu $p$ teilerfremden Zahlen $a$, deren Werte $\pm 1$ durch die Eulersche Kongruenz $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \bmod p$ festgelegt sind. Zum eigentlichen Reziprozitätsgesetz

$$\Big(\frac{p}{q}\Big)\Big(\frac{q}{p}\Big) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

für zwei ungerade Primzahlen $p$ und $q$ gesellen sich die beiden Ergänzungssätze

$$\Big(\frac{-1}{p}\Big) = (-1)^{\frac{p-1}{2}} \quad \text{und} \quad \Big(\frac{2}{p}\Big) = (-1)^{\frac{p^2-1}{8}}.$$

Schon als Gauß einen Beweis dieses Reziprozitätsgesetzes nach dem andern suchte (vgl. [9]), hatte er die Verallgemeinerung auf höhere Potenzreste im Blick. Seine Untersuchungen [29] darüber veröffentlichte er erst gegen Ende der 1820er Jahre. Die wesentliche Erkenntnis war die, dass es zur Formulierung eines Reziprozitätsgesetzes für 4. Potenzreste der Erweiterung des Zahlenbereichs auf den Ring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ bedurfte, wo $i$ eine primitive 4. Einheitswurzel bezeichnet. In diesem Ring definierte Gauß Teilbarkeit, Einheiten und Primelemente und zeigte mit Hilfe der Theorie quadratischer Formen, dass dieser Ring eine eindeutige Zerlegung in Primelemente besitzt. Das biquadratische Restsymbol $[\frac{\alpha}{\pi}]$ für Primelemente $\pi \in \mathbb{Z}[i]$ mit ungerader Norm und zu $\pi$ teilerfremden $\alpha \in \mathbb{Z}[i]$ nimmt Werte in $\{\pm i, \pm 1\}$ an und ist durch die Kongruenz $[\frac{\alpha}{\pi}] \equiv \alpha^{\frac{N\pi-1}{4}} \bmod \pi$ festgelegt. Hierbei ist $N(a+bi) = (a+bi)(a-bi) = a^2+b^2$ die Norm der Zahl $a+bi$; offenbar ist die Norm $\equiv 1 \bmod 4$, sobald sie ungerade ist. Die Norm ist das Analogon des Absolutbetrags in $\mathbb{Z}$ und gibt die Ordnung der Restklassengruppe $\mathbb{Z}[i]/(a+bi)$ an.

Das biquadratische Reziprozitätsgesetz nimmt seine einfachste Form an, wenn die Primzahlen $\pi \equiv \lambda \equiv 1 \bmod (2+2i)$ sind, denn dann gilt

$$\Big[\frac{\pi}{\lambda}\Big]\Big[\frac{\lambda}{\pi}\Big]^{-1} = (-1)^{\frac{N\pi-1}{4}\cdot\frac{N\lambda-1}{4}}.$$

Die Beweise dafür gaben erst Jacobi in seinen Vorlesungen [50] und Eisenstein in verschiedenen Abhandlungen.

Damit war klar, dass das Fernziel ein Reziprozitätsgesetz der $n$-ten Potenzreste im Körper der $n$-ten Einheitswurzeln sein würde. Dieser Aufgabe gingen zuerst Dirichlet, vor allem aber Jacobi und Eisenstein nach. Ihnen war ebenso wie Gauß bewusst, dass die eindeutige Zerlegung in Primfaktoren im Allgemeinen nicht gilt, und deswegen versuchten sie, die Arithmetik in solchen Zahlbereichen mit Hilfe der Theorie von Formen höheren Grades aufzubauen. Eisenstein [21] behandelte auf diesem Weg die Theorie der zyklischen kubischen Zahlkörper, Dirichlet selbst gelangte bis zu den Klassenzahlformeln derjenigen Formen, die zu den Körpern der $p$-ten Einheitswurzeln gehören, überließ die Veröffentlichung dieser Resultate aber Kummer, dessen Theorie der idealen Zahlen Dirichlet für die angemessenere Sprache gehalten haben mag. Für die weiteren Arbeiten über das Reziprozitätsgesetz der $p$-ten Potenzreste im Körper $\mathbb{Q}(\zeta_p)$ der $p$-ten Einheitswurzeln waren diese idealen Zahlen unerlässlich, und sie wurden auch von Eisenstein für dessen Beweis eines Spezialfalls verwendet, nämlich den des Eisensteinschen Reziprozitätsgesetzes.

Die Definition des $n$-ten Potenzrestsymbols $(\frac{\alpha}{\mathfrak{p}})$ für Elemente $\alpha \in \mathbb{Z}[\zeta]$ ist dabei kein Problem: dieses Symbol nimmt $n$-te Einheitswurzeln als Werte an und ist durch die Kongruenz

$$\Big(\frac{\alpha}{\mathfrak{p}}\Big) \equiv \alpha^{\frac{N\mathfrak{p}-1}{n}} \bmod \mathfrak{p}$$

festgelegt. Allein mit Methoden der Kreisteilung, also Gauß- und Jacobisummen, gelingt Eisenstein dann der Beweis seines Reziprozitätsgesetzes:

**Satz 1.1** (Eisensteins Reziprozitätsgesetz)**.** *Sei $p$ eine ungerade Primzahl und $\mathbb{Z}[\zeta]$ der Ring der ganzen Zahlen im Körper der $p$-ten Einheitswurzeln. Für semiprimäre $\alpha \in \mathbb{Z}[\zeta]$ (das sind solche, die modulo $\lambda^2 = (1-\zeta)^2$ einer ganzen rationalen Zahl* *kongruent sind) und ganze Zahlen $a \in \mathbb{Z}$ gilt für das $p$-te Potenzrestsymbol bei ungeraden Primzahlen $p$ das Reziprozitätsgesetz*

$$\left(\frac{a}{\alpha}\right) = \left(\frac{\alpha}{a}\right).$$

Weitere Fortschritte erforderten Kummers Theorie der idealen Zahlen. In einer Reihe von Arbeiten bewies Kummer [54] mit Dirichlets analytischen Methoden die Klassenzahlformel und die Existenz gewisser Hilfsprimzahlen, die er zum Beweis der Reziprozitätsgesetze benötigte. Solche Reziprozitätsgesetze konnte er nur für *reguläre* Primzahlen beweisen, also solche, für die die Klassenzahl von $\mathbb{Q}(\zeta_p)$ nicht durch $p$ teilbar ist. Kronecker hat vermutet, dass sich diese Lücke schließen lässt mit Hilfe von unverzweigten abelschen Erweiterungen, auf die er in seinen Arbeiten über die komplexe Multiplikation gestoßen war. Dies wurde viel später durch Hilbert präzisiert und durch Furtwängler bestätigt.

Da Kummer den Begriff einer ganzalgebraischen Zahl nicht zur Verfügung hatte, enthielt nicht nur seine Theorie der idealen Zahlen in Kreisteilungskörpern und ihren Teilkörpern eine Lücke; vielmehr verhinderte dieser Mangel auch den Aufbau einer vollständigen Theorie der idealen Zahlen in Kummererweiterungen $K(\sqrt[p]{\mu}\,)$ von $K = \mathbb{Q}(\zeta_p)$, in denen die „natürliche“ Basis der Zahlen $\zeta^j \sqrt[p]{\mu}^k$ in der Regel keine Ganzheitsbasis bildet. Kummer selbst schreibt[1] in [54, S. 677]:

> *Eine Definition der idealen Primfaktoren der in $\lambda D(\alpha)$ enthaltenen complexen Primzahlen von der Form $f(\zeta)$ wird nicht gegeben und zwar nicht allein darum weil sie für den vorliegenden Zweck entbehrlich ist, sondern hauptsächlich auch darum, weil diese complexen Primzahlen von der Form $f(\zeta)$ in der höheren Theorie der complexen Zahlen in $w$ oder $z$ im allgemeinen in wahre ideale Primfaktoren sich gar nicht zerlegen lassen, welche im vollen Sinne diesen Namen verdienen.*

Eben dieser Mangel erschwerte auch den Nachweis der Behauptung, die Theorie idealer Zahlen in quadratischen Körpern sei äquivalent zur Gaußschen Theorie der binären quadratischen Formen. Erst Dedekinds methodisches Vorgehen und die Einführung der Ideale erlaubten einen Aufbau der Arithmetik in allgemeinen Zahlkörpern.

Dedekind schuf in den Supplementen zu den von ihm herausgegebenen Vorlesungen Dirichlets über Zahlentheorie [14] eine solide Grundlage der Kummerschen Theorie, fand aber nur wenige Leser. Bereits die Kummerschen Arbeiten über Reziprozitätsgesetze waren eher wohlwollend zur Kenntnis genommen als wirklich studiert worden. Das Hauptinteresse der mit Zahlentheorie vertrauten Mathematiker galt im ausgehenden 19. Jhdt. eher der Entwicklung der algebraischen Geometrie und der komplexen Multiplikation, also der Aufdeckung der Zusammenhänge zwischen Zahlentheorie einerseits und elliptischen und Abelschen Funktionen andererseits: Eine intensive Auseinandersetzung mit den Arbeiten Kummers und Dedekinds fand kaum statt. Dies änderte sich grundlegend mit dem Erscheinen des Zahlberichts. Nebenbei bemerkt waren die von Hilbert eingeführten Begriffe und Methoden auch der Schlüssel zu einer abgerundeten Theorie der komplexen Multiplikation.

---

[1] Hier ebenso wie weiter unten ersetzen wir Kummers Schreibweise $\alpha$ kommentarlos durch das heute gebräuchliche $\zeta$.

## 2. Der Zahlbericht als Lehrbuch

Das erste Lehrbuch über Zahlentheorie wollte bereits Euler schreiben; dessen „Tractatus“ [22], den er wohl irgendwann zwischen 1756 und seinem Tod 1783 verfasst hat, blieb aber unvollendet und wurde erst posthum veröffentlicht. Danach hat Legendre in seinem *Essai de Théorie des Nombres* [66] aus dem Jahre VI der Revolution (also 1798) versucht, seinen Lesern den damaligen Stand der Zahlentheorie nahezubringen; Legendres Buch ist sehr reich an Ideen, in der Durchführung aber manchmal weitläufig und, was schlimmer wiegt, wenig präzise. Auch Minkowski hat dies so empfunden, wie er in einem Brief an Hilbert vom März 1895 schreibt:

> *Diese ganze Woche habe ich Legendre und Gauß studiert. [...] Nur übermannt mich bei manchen Stellen von Legendre leicht Schläfrigkeit; welch himmelweiter Unterschied, wie Gauss und Legendre dieselben Dinge ansehen, dieselben Gedanken ordnen.*

Dennoch hat dieses Werk, wenn auch nicht ganz mit demselben Erfolg wie die sehr viel gelesene Geometrie Legendres, enorm zur Popularität der Zahlentheorie beigetragen.

Gauß legte drei Jahre nach Legendre sein Jahrhundertwerk *Disquisitiones Arithmeticae* [28] vor, in dem er zwar dasselbe Feld bebaute wie Legendre (und zwar nicht aus Zufall: Dessen Abhandlung [65] aus dem Jahre 1785 hatte Gauß zu Beginn seines Studiums in Göttingen zu vielen Untersuchungen inspiriert), aber mit ungleich mehr Erfolg: Gauß konnte das quadratische Reziprozitätsgesetz im Gegensatz zu Legendre vollständig beweisen, seine Komposition quadratischer Formen lieferte eine Gruppenstruktur auf den Äquivalenzklassen von Formen gegebener Diskriminante, während Legendres Komposition mehrdeutig war, und der Gaußsche Beweis des Dreiquadratesatzes kam ohne unbewiesene Annahmen aus, während Legendre unter anderem den später von Dirichlet bewiesenen Satz über Primzahlen in arithmetischer Progression benutzen musste. Dass Legendres Buch dennoch weit verbreitet war und auch mehrere Auflagen erlebte, lag an der für die damalige Zeit sehr kompakten Darstellung von Gauß, dessen Verlangen nach Allgemeinheit etwa seine Theorie der quadratischen Formen zu einem unüberwindbaren Hindernis für die meisten Leser machte.

In der ersten Hälfte des 19. Jahrhunderts gelang es nur wenigen, die *Disquisitiones* zu durchdringen: Neben Legendre, Dirichlet, Abel, Jacobi, Eisenstein und Kummer ist hier auch Sophie Germain zu nennen. Dirichlet und Jacobi [50], sowie – in bescheidenerem Umfang – Kummer [62] sorgten in ihren Vorlesungen für eine Verbreitung der Gaußschen Ideen, aber erst mit den von Dedekind herausgegebenen Vorlesungen Dirichlets [14] über Zahlentheorie lag ein Werk vor, welches das Eindringen in die *Disquisitiones* vorbereitete und, insbesondere in Sachen analytischer Hilfsmittel, über diese hinausging.

Dedekind hatte 1879 einen sehr modernen Aufbau als Supplement zu den populären Dirichletschen Vorlesungen über Zahlentheorie gegeben, aber die Reaktionen waren dürftig. Dedekind klärte die Bedeutung der ganzalgebraischen Zahlen auf, führte Ganzheitsbasen und Diskriminanten in beliebigen Zahlkörpern ein, bewies den Fundamentalsatz der Idealtheorie in algebraischen Zahlkörpern, also die eindeutige Primidealzerlegung in jedem solchen Ganzheitsring, und verallgemeinerte die Kummersche Klassenzahlformel von Kreiskörpern auf beliebige Zahlkörper. Die eigentlichen Ergebnisse Kummers, also die tiefer liegenden Teile der Arithmetik der Kreiskörper mit Anwendungen auf die Fermatsche Vermutung und die Reziprozitätsgesetze, blieben von Dedekind unübersetzt.

Offenbar empfand man seitens der DMV das Bedürfnis, den mühsamen Weg an die Spitze der zahlentheoretischen Forschung mit einem Bericht zu ebnen. Für die Zahlentheorie bis Kummer existierte bereits der vorzügliche „Report" [85] von Smith, der bis zu den ersten Arbeiten von Kummer und Kronecker vordringt. Für die elementare Zahlentheorie legte Dickson später drei Bände [17] vor, die allerdings ein ganz anderes Ziel verfolgten als die Berichte, welche die DMV in Auftrag gab. Die Lücke, die Minkowskis fehlender Bericht gelassen hat, wurde durch die Lehrbuchreihe Paul Bachmanns [3, 4, 5, 6, 7, 8] über die ganze Bandbreite der damaligen Zahlentheorie wenn nicht geschlossen, dann doch deutlich verkleinert.

Wie sehr man den Mangel eines guten Überblicks auf dem Gebiet der algebraischen Zahlentheorie gespürt hat, ist eine offene Frage; jedenfalls schrieb Hilbert seinen Bericht wohl für ein Publikum, das es damals gar nicht gab – man kann vielmehr sagen, dass der *Zahlbericht* sich sein Publikum sozusagen selbst geschaffen hat. Die großen Zahlentheoretiker des ausgehenden 19. Jahrhunderts, also Kummer (1810–1893), Kronecker (1823–1891), Dedekind (1831–1916) und H. Weber (1842–1913), waren entweder bereits gestorben oder schon in die Jahre gekommen, und die mathematische Jugend sah sich eher von der algebraischen Geometrie und den Abelschen Funktionen angezogen als von der algebraischen Zahlentheorie. Zu den wenigen Ausnahmen gehören Paul Bachmann, Adolf Hurwitz und Kurt Hensel; der Beweis des Primzahlsatzes durch Jacques Hadamard und Charles-Jean de la Vallée-Poussin im Jahre 1896, aufbauend auf Ideen Bernhard Riemanns, insbesondere den 1895 von Hans von Mangoldt bewiesenen Satz, dass der Primzahlsatz äquivalent zur Nullstellenfreiheit der Riemannschen Zetafunktion auf der Geraden $\mathrm{Re}\, s = 1$ ist, sorgte für Interesse an der analytischen Zahlentheorie, wo insbesondere die Namen Pafnuty Tschebyscheff, Franz Mertens und Edmund Landau zu nennen sind.

Hilbert hat mit seinem *Zahlbericht* die Entwicklung der algebraischen Zahlentheorie in einem Maße gefördert, wie es sich Dedekind nicht hätte träumen lassen. Wie viele Mathematiker Dedekind mit seinen Supplementen für die Zahlentheorie gewonnen hat, ist schwer zu sagen (Bachmann gehört dazu), aber der Aufschwung der Zahlentheorie im 20. Jahrhundert hängt mit der Wirkung des *Zahlberichts* zusammen: So wie Dirichlet, Jacobi, Eisenstein und Kummer die Zahlentheorie aus den *Disquisitiones Arithmeticae* lernten (das ja ebenfalls in erster Linie kein Lehrbuch, sondern eher eine Monographie war), so lernte man algebraische Zahlentheorie im frühen 20. Jahrhundert aus dem *Zahlbericht*: Die Namen Furtwängler, Fueter, Herglotz, Takagi, Hecke, E. Artin, Hasse, Weyl, Siegel, A. Scholz, Chebotarev, Herbrand und Chevalley, um nur einige zu nennen, sprechen für sich.

Auf Anregung Hilberts hin schrieben Sommer [86] und Reid [78] Einführungen in die Theorie vor allem der quadratischen Zahlkörper; auch Bachmann legte mit [8] im Jahre 1905 ein von Hilbert inspiriertes Lehrbuch der algebraischen Zahlentheorie vor. Erst Hecke [33] betonte explizit die abstrakten gruppentheoretischen Strukturen, die Hilbert – wohl im Hinblick auf die Lesbarkeit seines Berichts – eher unterdrückt hatte. Festzuhalten bleibt allerdings, dass die späteren Lehrbücher der algebraischen Zahlentheorie in erster Linie deswegen leichter zu verdauen sind als Hilberts *Zahlbericht*, weil diese die Kummerschen Arbeiten links liegen lassen: Der *Zahlbericht* ist bis heute der einzige Schlüssel zu Kummers Werk geblieben.


Abbildung 1. Hilbert auf einer Photographie aus dem Jahre 1912 (Quelle: MfO, Roquette) und auf einer Briefmarke aus dem Kongo (MacTutor History of Mathematics archive).

## 3. Der Aufbau der Idealtheorie

Dedekind gehörte zu den ersten Mathematikern, die sich mit der neuen Galoistheorie vertraut machten; dabei bemerkte er, dass der wesentliche Begriff, der zu einer glatten Beschreibung der dabei verwendeten Methoden notwendig war, der eines Körpers und seiner Automorphismen ist. Dabei war ein Körper für Dedekind in erster Linie ein algebraischer Zahlkörper, also eine endliche Erweiterung von $\mathbb{Q}$. Im Laufe seiner Untersuchungen begann Dedekind nun systematisch, eine ganze Reihe von für viele seiner Zeitgenossen sehr abstrakten Begriffen einzuführen, etwa Ordnungen, Moduln und Ideale. Es sei ausdrücklich bemerkt, dass sich Dedekind ebenso wie Hilbert dabei auf Strukturen innerhalb von Zahlkörpern beschränkte; die Ausdehnung auf „abstrakte“ Ringe hat erst Emmy Noether vorangetrieben.

Ein Modul ist nach Dedekind ein System von Zahlen, das gegenüber der Subtraktion abgeschlossen ist. Moduln in quadratischen Zahlkörpern und deren Produkte stehen in engem Zusammenhang mit binären quadratischen Formen und deren Komposition.

Es war eine wesentliche Erkenntnis Dedekinds, dass zum Aufbau einer Idealtheorie einschließlich des Fundamentalsatzes die Einführung des Begriffs der ganzen algebraischen Zahl notwendig war. In jedem algebraischen Zahlkörper $K$ konnte er damit den Ring $\mathcal{O}_K$ aller in $K$ enthaltenen ganz algebraischen Zahlen auszeichnen. Der erste fundamentale Satz ist dann die Existenz einer Ganzheitsbasis: Hat $K$ Grad $n$ über $\mathbb{Q}$, dann gibt es Elemente $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ mit $\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$. Das wesentliche Hilfsmittel beim (einfachen) Beweis ist eine aus diesen Elementen gebildete Determinante, die Diskriminante des Zahlkörpers. Kummer hatte sich in den Körpern der $n$-ten Einheitswurzeln mit den Ringen $\mathbb{Z}[\zeta]$ begnügt, und für die

Theorie der idealen Zahlen in Teilkörpern benutzte er als Ganzheitsbasis die Gaußschen Perioden aus dem 7. Abschnitt der *Disquisitiones*; dabei hatte Kummer das Glück, dass diese Ringe mit den Ganzheitsringen übereinstimmen.

Ein Modul $\mathfrak{a}$ in $\mathcal{O}_K$ nennt Dedekind ein (ganzes) Ideal, wenn dieser $\mathfrak{a}\cdot\mathcal{O}_K$ enthält, also bezüglich der Multiplikation mit Elementen aus $\mathcal{O}_K$ abgeschlossen ist. Die Tatsache, dass Ideale genau die Kerne von Ringhomomorphismen sind (Kummers ideale Primzahlen lassen sich als Ringhomomorphismen des Ganzheitsrings eines algebraischen Zahlkörpers in endliche Körper interpretieren; vgl. [69] und [11]), ist dafür verantwortlich, dass der Idealbegriff für die Algebra zu einem ganz zentralen Begriff geworden ist. Ein Ideal $\mathfrak{p}$ heißt prim, wenn aus $\alpha\beta \in \mathfrak{p}$ immer $\alpha \in \mathfrak{p}$ oder $\beta \in \mathfrak{p}$ folgt; für Hauptideale $\mathfrak{p} = (p)$ läuft dies auf den Euklidischen Satz hinaus, dass die Zahl $p$ genau dann prim ist, wenn aus $p \mid ab$ immer $p \mid a$ oder $p \mid b$ folgt.

In jedem Ganzheitsring $\mathcal{O}_K$ gilt nun der Fundamentalsatz von der eindeutigen Zerlegung in Primideale, wonach sich jedes ganze Ideal $\mathfrak{a} \neq (0)$ eindeutig als Produkt von Primidealen schreiben lässt. Die Crux beim Beweis dieses Satzes ist der Nachweis, dass aus der mengentheoretischen Relation $\mathfrak{a} \supset \mathfrak{c}$ die Existenz eines ganzen Ideals $\mathfrak{b}$ mit $\mathfrak{ab} = \mathfrak{c}$ folgt. Daraus wiederum erhält man sofort, dass es zu jedem Ideal $\mathfrak{a}$ ein Ideal $\mathfrak{b}$ gibt, für das $\mathfrak{ab}$ ein Hauptideal ist, und dieser Satz erlaubt das Zurückspielen von Teilbarkeitseigenschaften von Idealen auf Elemente.

Dedekinds Beweis für den Fundamentalsatz der Idealtheorie konnte Hilbert ebensowenig überzeugen wie derjenige, den Kronecker gegeben hatte. Blumenthal erzählt in Hilberts Gesammelten Abhandlungen [10, S. 397]:

> *Auf den Spaziergängen mit Hurwitz wurden Kroneckers und Dedekinds Arbeiten eingehend besprochen. Hilbert erzählte später drastisch: „Einer nahm den Kroneckerschen Beweis für die eindeutige Zerlegung in Primideale vor, der andere den Dedekindschen, und beide fanden wir scheußlich“.*

Wenig später veröffentlichen Hilbert und Hurwitz ihre eigenen Beweise für den Fundamentalsatz der Idealtheorie. In [47] benutzt Hurwitz den Prager Satz[2], den auch Dedekind bei seinen Untersuchungen der Idealtheorie zu Beginn benutzt hatte; in seiner Kritik des Hurwitzschen Beweises schreibt Dedekind in [15, S. 53]:

> *Aber dieser Weg entspricht durchaus nicht meinen Wünschen, teils weil die Benutzung der Funktionen von Variablen mir immer als ein der Sache fremdes Hilfsmittel erscheint, teils weil die Durchführung aller Beweise einen größeren Raum erfordert als in meiner damaligen Theorie.*

Dieses Desideratum der Methodenreinheit betont er wenig später noch einmal [15, S. 55]:

> *Aus denselben Gründen konnte der oben erwähnte Beweis des Satzes 3, welcher sich auf Satz 5 stützt, mich noch nicht völlig befriedigen, weil durch die Einmischung der Funktionen von Variablen die Reinheit der Theorie nach meiner Ansicht getrübt wird [...].*

Im selben Jahr veröffentlicht Hurwitz einen zweiten Beweis, dessen Grundidee auf Kroneckers Dissertation [53] zurückgeht: Durch ein geometrisches Argument, das dem euklidischen Algorithmus nachgebildet ist, wird gezeigt, dass die Klassenzahl

[2]Der Prager Satz ist eine Verallgemeinerung des Gaußschen Lemmas über die Multiplikativität des Inhalts von Polynomen; vgl. [70].

$h$ eines Zahlkörpers $K$ endlich ist; aus algebraischen Gründen ist dann $\mathfrak{a}^h$ für jedes Ideal $\mathfrak{a}$ ein Hauptideal, und dies genügt wie oben, um den Fundamentalsatz der Idealtheorie zu beweisen. Diesen Beweis haben Ireland & Rosen in ihr Buch [51] aufgenommen. Hurwitz kam in [48] und [49] noch einmal auf seinen Beweis zurück; der Grundgedanke dieser Arbeit wurde von Lenstra [73] benutzt, um euklidische Zahlkörper mit großem Grad zu finden.

Hilbert beweist den Fundamentalsatz in [36] zuerst für Galoissche Erweiterungen, und in einem zweiten Schritt für beliebige Zahlkörper durch Herabsteigen aus dem normalen Abschluss.

In seinem *Zahlbericht* hat Hilbert den Kroneckerschen Beweis vorgestellt, der den Prager Satz als wesentliches Lemma benutzt und welcher der Dedekindschen Forderung nach Methodenreinheit nicht genügt. Ich persönlich erinnere mich daran, dass ich bei meinem ersten Studium des *Zahlberichts* über diesen Beweis gestolpert bin und mit den Kroneckerschen Argumenten wenig anfangen konnte. Heute habe ich für diesen Zugang deutlich mehr übrig und halte ihn, konsequent durchgeführt, für eine gangbare Alternative zum üblichen Aufbau.

Den Schlussakkord im Ringen um den richtigen Aufbau der Dedekindschen Idealtheorie setzte Emmy Noether [76], der es gelang, den Fundamentalsatz der Idealtheorie axiomatisch zu charakterisieren und damit Zahl- und Funktionenkörper gleichberechtigt zu behandeln. Es ist schwer, sich heute einen Eindruck davon zu machen, mit welcher Hochachtung die Algebraiker dieser Noetherschen Leistung damals gegenüber getreten sind.

In seiner Vorlesung [83, I, S. 9] schreibt F.K. Schmidt, der Zeitzeuge dieser Entwicklung gewesen ist:

> *Im ersten Teil der Einleitung haben wir in kurzen Zügen die rein zahlentheoretische Entwicklung der Zahlentheorie kennen gelernt. Sie wird weitgehend der Forderung nach Reinheit der Methode gerecht. Der Sinn dieser Forderung besteht darin, dass man eine mathematische Theorie mit Verfahren behandelt, die dem Gegenstandsbereich entnommen und ihm angemessen sind.*

Die Methodenreinheit führt F.K. Schmidt dann zu einem „einheitlichen Aufbau der Theorie der algebraischen Zahlen und der Theorie der algebraischen Funktionen" mit Hilfe der Theorie der Bewertungen.

Auch Dedekind war sich natürlich der Tatsache bewusst, dass der Methodenreinheit Grenzen gesetzt sind; zum Beweis zentraler Sätze der algebraischen Zahlentheorie sind analytische Eigenschaften der Dedekindschen Zetafunktion unerlässlich. Hecke war ein Meister darin, diese Verbindung von analytischen und algebraischen Techniken auszunutzen, wie man unter anderem an seinen Vorlesungen [33] und [34] sehen kann.

## 4. Die Arbeit am Zahlbericht

Als Minkowski und Hilbert 1893 den Auftrag zur Abfassung eines Berichts über die Zahlentheorie erhielten, war Minkowski bereits ein geachteter Mathematiker, dem zehn Jahre zuvor der Preis der Pariser Akademie für seine Arbeit über die Darstellung von Zahlen als Summen von fünf Quadraten zuerkannt worden war. Auf der 64. Naturforscher- und Ärzteversammlung in Halle hatte Minkowski 1891 über die Geometrie der Zahlen vorgetragen. Hilbert dagegen hatte sich bisher vor allem mit der Invariantentheorie beschäftigt, trug aber auf der DMV-Tagung 1893 in

München über einen Beweis des Fundamentalsatzes der Idealtheorie in Zahlkörpern vor.

In seiner zweiten zahlentheoretischen Arbeit [37] (oder der dritten, wenn man seine Arbeit über die Transzendenz von $e$ und $\pi$ mitzählt) entwickelt Hilbert die „Grundzüge einer Theorie des Galoisschen Zahlkörpers“ und definiert die grundlegenden Begriffe der Zerlegungs-, Trägheits- und Verzweigungsgruppen. Diese Begriffe hat Hilbert dann in seinem Beweis des Satzes von Kronecker und Weber benutzt, wonach jede abelsche Erweiterung des rationalen Zahlkörpers ein Kreiskörper ist, also in einem Körper von $n$-ten Einheitswurzeln enthalten ist. Vermutlich geht man etwas zu weit mit der Behauptung, Hilberts Beweis sei der erste vollständige Beweis dieses Satzes – in jedem Fall war es der erste durchsichtige Beweis. Darüberhinaus führte Hilbert mit der abelschen Durchkreuzung eine Technik ein, die später von Chebotarev für seinen Beweis des Dichtigkeitssatzes ausgebaut wurde; die Grundidee Chebotarevs wurde von Artin dann als der Schlüssel zum Beweis seines Reziprozitätsgesetzes erkannt.

Die große Bedeutung der Galoisschen Erweiterungen tritt bei Hilbert viel deutlicher hervor als bei seinen Vorgängern. Auch im *Zahlbericht* spielt die Operation der Galoisgruppe eine ganz wesentliche Rolle sowohl in der Theorie der ambigen Idealklassen (das sind solche, die unter der Operation der Galoisgruppe fest bleiben), als auch im grundlegenden Satz 90 über Elemente der Norm 1 in zyklischen Erweiterungen. Bei Hilbert ist die Galoistheorie also nicht mehr eine Theorie der Polynome und ihrer Wurzeln, sondern von Anfang an eine Theorie der Körpererweiterungen. Ganz neu war diese Sichtweise nicht: Bereits im wenig beachteten Artikel [2] von Bachmann konnte man eine Darstellung der Galoistheorie finden, bei der nicht mehr die Polynome und ihre Wurzeln, sondern die von diesen Wurzeln erzeugten Körper (und zwar Dedekinds „Zahlenkörper“) im Mittelpunkt standen. Auch H. Webers Algebra war an der Loslösung der Galoistheorie von der Jordanschen Theorie der Substitutionen beteiligt, und in seiner großen Arbeit [87] hat Steinitz die Galoistheorie dann so überzeugend umgeschrieben (und zwar allgemein auch für Körper endlicher Charakteristik), dass danach kaum noch Lehrbücher der Algebra geschrieben wurden, die den ursprünglichen Zugang beibehielten.

Zwischen seinen Arbeiten über die Arithmetik Galoisscher Zahlkörper hat Hilbert 1894 einen weiteren zahlentheoretischen Artikel veröffentlicht, der weithin etwas unterschätzt wird, nämlich [38] „Über den Dirichletschen biquadratischen Zahlkörper“. Dort schreibt er:

> *Die vorliegende Abhandlung hat das Ziel, die Theorie des Dirichletschen biquadratischen Körpers auf rein arithmetischem Wege bis zu demjenigen Standpunkt zu fördern, auf welchem sich die Theorie der quadratischen Körper bereits seit Gauß befindet. Es ist hierzu vor allem die Einführung des Geschlechtsbegriffs sowie eine Untersuchung derjenigen Einteilung aller Idealklassen notwendig, welche sich auf den Geschlechtsbegriff gründet.*

Hilbert gibt hier einen arithmetischen Beweis für die Klassenzahlformel von biquadratischen Erweiterungen $\mathbb{Q}(i, \sqrt{m})$, welche Dirichlet [18] mit analytischen Methoden in der Sprache der quadratischen Formen bewiesen hatte. Der Kern des Hilbertschen Zugangs liegt in seiner Behandlung der Geschlechter, die er mit Hilfe eines neuen Symbols beschreibt, das man als Prototyp des Normenrestsymbols auffassen kann. Mit diesem ist es ihm später gelungen, die Kummerschen Ergebnisse im *Zahlbericht* auf eine klare und strukturierte Art und Weise darzustellen.

Dass das nicht immer einfach war, hat Hilbert in einem Brief an Klein (siehe [23]) beklagt:

> *Die härtesten Nüsse sind die Kummerschen Arbeiten, und es bedarf einer vollständigen Umarbeitung derselben, um dieselben genießbar zu machen. Ich habe nicht geglaubt, daß Kummer ein so verzwickter Rechner sei. Der Hauptübelstand ist der, daß er von vornherein nur ein einziges Ziel nämlich den Beweis der allgemeinen Reciprocitätsgesetze anstrebt, wobei ihm alle Mittel recht sind, und die schönsten daneben liegenden Dinge unbeachtet bleiben.*

Zu den schönsten daneben liegenden Dinge gehörte sicherlich der Satz, der später als Hilberts Satz 90 bekannt wurde, weil er in Hilberts Liste der Sätze im *Zahlbericht* die Nummer 90 trägt. Kummer hat diese Aussage 1855 in [59] en passant bewiesen. Dabei bildete er nach dem Vorbild der Lagrangeschen Resolventen

$$F(\zeta,\xi) = \xi + \zeta\xi^g + \zeta^2\xi^{g^2} + \ldots + \zeta^{p-2}\xi^{g^{p-2}},$$

in welchen $\zeta^{p-1} = \xi^p = 1$ und $g$ eine Primitivwurzel modulo $p$ ist, den Ausdruck

$$P(\varepsilon) = 1 + \varepsilon(\xi) + \varepsilon(\xi)\varepsilon(\xi^g) + \varepsilon(\xi)\varepsilon(\xi^g)\varepsilon(\xi^{g^2}) + \ldots + \varepsilon(\xi)\varepsilon(\xi^g)\varepsilon(\xi^{g^2})\cdots\varepsilon(\xi^{g^{p-3}})$$

wo $\varepsilon \in \mathbb{Q}(\xi)$ ist mit

$$N\varepsilon(\xi) = \varepsilon(\xi)\varepsilon(\xi^g)\varepsilon(\xi^{g^2})\cdots\varepsilon(\xi^{g^{p-2}}) = 1.$$

Als „erste Grund-Eigenschaft dieser Ausdrücke“ hält Kummer die Gleichung

$$\varepsilon(\xi)P(\varepsilon(\xi^g)) = P(\varepsilon(\xi))$$

fest, und dies ist nichts anderes als Hilberts Satz 90, wie man sieht, wenn man die Gleichung in der uns geläufigen Form

$$\varepsilon(\xi) = P(\varepsilon(\xi))^{1-\sigma}$$

schreibt, wo $\sigma$ der durch $\xi \to \xi^g$ definierte Automorphismus der zyklischen Erweiterung $\mathbb{Q}(\xi)/\mathbb{Q}$ ist.

Hilbert hat hier eine Nebenbemerkung Kummers durch die Erhebung zu einem Satz geadelt, und die nachfolgende Entwicklung der Galois-Kohomologie hat ihm recht gegeben.

## 5. Lob und Kritik

Die zahlreichen Lobesreden auf den *Zahlbericht* aufzuführen hieße, Eulen nach Athen zu tragen. Wir belassen es bei der Bemerkung, dass Hilberts Bericht wie die Gaußschen *Disquisitiones Arithmeticae* schnell in französischer Übersetzung [40] veröffentlicht worden sind (inzwischen gibt es sogar eine Übersetzung ins Rumänische [41]), und begnügen uns mit einem Zitat von Hermann Weyl [95]:

> *Nach dem ersten Jahr ging ich mit Hilberts Zahlbericht unter dem Arm nach Hause, und arbeitete ihn während der Sommerferien durch – ohne jede Vorkenntnisse in elementarer Zahlentheorie oder Galoistheorie. Dies waren die glücklichsten Monate meines Lebens,*

> *deren Glanz, über die Jahre hinweg belastet mit den uns allen eigenen Zweifeln und Fehltritten, meine Seele immer noch tröstet.*[3]

Die wenigen Stimmen, die sich kritisch zu Hilberts *Zahlbericht* äußerten, sind durch Olga Taussky bekannt geworden. So schreibt sie[4] in ihren autobiographischen Skizzen [89, S. 20]:

> *Viele Jahre später hat Emmy gegen den Zahlbericht gewettert. [...] Emmy zitierte damals Artin, der gesagt habe, der Zahlbericht habe den wirklichen Fortschritt dieses Gebiets um Jahrzehnte verzögert.*[5]

Es ist wohl so, dass man die Aussagen, die Taussky in ihrer autobiographischen Skizze macht, nicht auf die Goldwaage legen darf. Der ganze Artikel [89] ist durchwebt mit Behauptungen, die bisweilen kaum einen historischen Kern besitzen. Von ihrem Doktoranden Hobby schreibt sie etwa:

> *Ein Student, Hobby, arbeitete über Gruppentheorie, und seine Dissertation führte zur Lösung des Klassenkörperturmproblems durch Golod und Shafarevich.*[6]

Hobby hat in seiner Dissertation [46] gezeigt, dass es unendliche Türme von 2-Gruppen gibt, wie sie in einem Klassenkörperturm auftreten könnten, und dass daher die Möglichkeit unendlicher Klassenkörpertürme nicht aus trivialen gruppentheoretischen Gründen ausgeschlossen ist. Dies ist ein schönes Ergebnis (Serre hat es später verallgemeinert; vgl. [24]), hat aber auf die Lösung des Klassenkörperturmproblems durch Golod und Shafarevich keinen Einfluss gehabt.

In [89, S. 19] schreibt Taussky außerdem, dass Hilberts Bericht „nicht frei von Fehlern jeder Größenordnung“ sei. Auch diesen Vorwurf hat sie des öfteren wiederholt, ohne jedoch konkret zu werden; außer der Hilbertschen Vermutung, wonach der Hilbertsche Klassenkörper eines Zahlkörpers mit Klassenzahl 4 eine ungerade Klassenzahl besitzen soll, sind mir nur zwei kleinere Fehler im *Zahlbericht* bekannt:

(1) Der Beweis von Satz 89 [39, S. 146], wonach die Idealklassengruppe eines Zahlkörpers von Primidealen ersten Grades erzeugt wird (vgl. den Übersichtsartikel [74]; für Kreisteilungskörper geht dieser Satz auf Kummer zurück), enthält eine kleine Lücke, auf die Washington [91] aufmerksam gemacht hat.

(2) Zu Beginn von [39, § 173] schreibt Hilbert, Kummer habe die Unmöglichkeit der Gleichung $\alpha^p + \beta^p + \gamma^p = 0$ mit $\alpha\beta\gamma \neq 0$ im Körper $K = \mathbb{Q}(\zeta_p)$ der $p$-ten Einheitswurzeln auch im Fall bewiesen, wo die Klassenzahl von $K$ durch $p$, aber nicht durch $p^2$ teilbar ist. Hier hat Taussky die Ergänzung angebracht, dass die Einheiten noch gewisse Bedingungen zu erfüllen haben. Tatsächlich hat Kummer die Unmöglichkeit der Fermatgleichung nur im maximalen reellen Teilkörper von $\mathbb{Q}(\zeta_p)$ bewiesen.

---

[3] And after the first year I went home with Hilbert's Zahlbericht under my arm, and during the summer vacation I worked my way through it – without any previous knowledge of elementary number theory or Galois theory. These were the happiest months of my life, whose shine, across years burdened with our common share of doubt and failure, still comforts my soul.

[4] Hier und im Folgenden stammen Übersetzungen von mir.

[5] Many years later, Emmy did lash out about the Zahlbericht. [...] Emmy at that time quoted Artin as having said that the Zahlbericht had delayed the proper advance of the subject by decades.

[6] One student, Hobby, worked on group theory, his thesis leading to the solution, by Golod and Shafarevich, of the class field tower problem.

Ich glaube daher, dass die richtige Frage nicht lautet, *was* Emmy Noether und Emil Artin am *Zahlbericht* kritisieren wollten, sondern ob sie das, zumindest in dieser Form, überhaupt getan haben. Natürlich ist mit dem Erscheinen von van der Waerdens Algebra, die von den Vorlesungen von Noether und Artin geprägt war, deutlich geworden, dass die Hilbertsche Darstellung der algebraischen Zahlentheorie nicht mehr zeitgemäß war, und dass man andere Mittel wählen musste, um die algebraischen Strukturen hinter den Hilbertschen Beweisen (und vor allen Dingen jenen von Furtwängler und Takagi) deutlich sichtbar werden zu lassen. Aber weder Noether noch Artin hätten sich zu der Bemerkung hinreißen lassen, dass Hilbert das 1897 hätte vorhersehen müssen, oder dass es der Entwicklung der algebraischen Zahlentheorie dienlich gewesen wäre, wenn er das getan hätte. Denkbar wäre allenfalls, dass ihre Bemerkungen andeuten sollten, Dedekind wäre mit seinem Zugang seiner Zeit um Jahrzehnte voraus gewesen.

In diese Richtung geht die Äußerung[7] von Hans Zassenhaus, der in [97, S. 19] schreibt:

> *Andererseits wurden die weiterreichenden Ansätze R. Dedekinds auf mehr als zwanzig Jahre in den Hintergrund gedrängt. Sie sind erst unter dem Einfluß E. Noethers sowie E. Artins, R. Brauers, H. Hasses, v.d. Waerdens, A.A. Alberts, Schurs und Frobenius' zur tragenden Basis der neueren Forschung geworden.*

„That's not a bug, that's a feature", könnte man darauf antworten, denn Minkowski schrieb im März 1896 an Hilbert

> *Mir gefällt Dein Referat in seiner knappen und dabei doch vollständigen Form außerordentlich, und es wird sicher allgemein großen Beifall finden und die Kroneckerschen wie Dedekindschen Abhandlungen sehr in den Hintergrund drängen.*

Minkowski erwartete also den Beifall seiner Kollegen dafür, dass Hilbert die anstrengende Lektüre der Arbeiten von Kronecker und Dedekind in weiten Teilen überflüssig machen würde.

Man sollte sich ebenfalls vor Augen halten, dass die von Zassenhaus aufgeführten Autoren die algebraische Zahlentheorie aus dem Hilbertschen *Zahlbericht* gelernt hatten; erst durch diesen Bericht sind ihnen die wesentlichen Ideen Dedekinds verständlich geworden.

Zassenhaus schweigt sich auch darüber aus, was er mit den weiterreichenden Ansätzen Dedekinds meint, aber die Auswahl der von ihm zitierten Namen legt eine Verbindung mit der Theorie der Algebren nahe. Diese Bemerkung scheint ebenfalls auf Olga Taussky zurückzugehen, die in [88, S. 499] vermutet, dass Fueter, Speiser und Schur wohl die Behandlung des Stoffs in Dicksons Buch *Algebras and their arithmetic* bevorzugt hätten. Auch diese Spekulation entbehrt in meinen Augen jeglicher Grundlage, denn wer Dicksons holprigen Stil der Klarheit und Präzision Hilberts vorzieht, kann entweder Dicksons Algebra oder Hilberts *Zahlbericht* nicht gelesen haben. Daneben gibt es kaum stoffliche Überschneidungen: Dicksons Buch befasst sich lediglich mit der Existenz von Ganzheitsbasen in Zahlkörpern, insbesondere in quadratischen.

[7]Ich danke Peter Ullrich für den Hinweis auf diese Stelle.

Es ist auch kaum glaubhaft, dass Noether oder Artin wegen einiger weniger Seiten, etwa was den Beweis des Fundamentalsatzes der Idealtheorie oder den sparsamen Gebrauch der Gruppentheorie angeht, den Stab über den ganzen *Zahlbericht* gebrochen haben könnten. In Artins Rede [1] zu Hilberts hundertstem Geburtstag im Jahre 1962 ist von einer derartigen Kritik keine Spur zu hören:

> *So wurde denn der im Jahre 1897 im Jahresbericht der Deutschen Mathematikervereinigung erschienene Zahlbericht Hilberts von allen Mathematikern mit großer Freude begrüßt. Hilbert stellt in ihm alle bis zur damaligen Zeit bekannten Ergebnisse zusammenfassend dar und machte durch große Vereinfachungen die Ergebnisse Kummers einem größeren Leserkreis zugänglich. Auch heute noch zieht jeder Zahlentheoretiker neben den neueren Lehrbüchern dieses grundlegende Werk zu Rate.*

Ebenso wie die längst widerlegte Behauptung (siehe [19]), Kummer habe in einer frühen Arbeit einen Beweis der Fermatschen Vermutung gegeben, der auf der fälschlichen Annahme der eindeutigen Primzerlegung in Kreisteilungskörpern beruhte, sich kaum mehr aus der Welt schaffen lassen wird, haben auch die Kommentare Tausskys weite Kreise gezogen. So schreibt Gian-Carlo Rota in seinem Artikel [81] über „Ten lessons I wish I had been taught“:

> *Als die Deutschen planten, Hilberts gesammelte Abhandlungen herauszugeben und sie ihm zu einem seiner späteren Geburtstage zu überreichen, stellten sie fest, dass sie die Arbeiten nicht originalgetreu abdrucken konnten, weil sie voller Fehler waren, darunter sehr ernste. Daraufhin stellten sie die junge arbeitslose Mathematikerin Olga Taussky-Todd ein, welche Hilberts Arbeiten durchgehen und alle Fehler verbessern sollte. Olga quälte sich drei Jahre lang ab; es stellte sich heraus, dass alle Fehler ohne größere Änderungen in den Formulierungen der Sätze korrigiert werden konnten. Eine Ausnahme gab es allerdings: eine Arbeit, die Hilbert in hohem Alter geschrieben hatte, konnte nicht repariert werden. Dort hatte Hilbert behauptet, einen Beweis der Kontinuumshypothese gegeben zu haben; man findet dies in einem Band der Mathematischen Annalen der frühen 1930er Jahre.*[8]

Eine weitere Lektion, die man oft erst zu spät lernt, ist – gerade im Zeitalter der alternativen Fakten – die, dass man derartige Behauptungen nach Möglichkeit zu verifizieren suchen sollte. Taussky wurde auf der Jahrestagung der DMV Mitte September 1931 in Bad Elster gebeten, an der Herausgabe der Hilbertschen Werke mitzuarbeiten, vor allem an Band 1 über Zahlentheorie, und zwar nicht wegen der vielen Fehler, sondern damit diese Hilbert zu seinem 70. Geburtstag am 23. Januar

---

[8] When the Germans were planning to publish Hilbert's collected papers and to present him with a set on the occasion of one of his later birthdays, they realized that they could not publish the papers in their original versions because they were full of errors, some of them quite serious. Thereupon they hired a young unemployed mathematician, Olga Taussky-Todd, to go over Hilbert's papers and correct all the mistakes. Olga labored for three years; it turned out that all the mistakes could be corrected without any major changes in the statement of the theorems. There was one exception: a paper Hilbert wrote in his old age which could not be fixed. It was a purported proof of the continuum hypothesis; you will find it in a volume of the Mathematische Annalen of the early thirties.

1932 übergeben werden konnten. Band I wurde zwar nicht pünktlich zu Hilberts Geburtstag fertig, erschien aber noch 1932, und im Herbst 1932 kehrte Taussky nach Wien zurück. Taussky hat also maximal ein Jahr am Bericht gearbeitet, und die Fehler, die sie gefunden haben will, lassen sich wohl an einer Hand abzählen: Furtwängler und Takagi haben ihre Beweise nach denen von Hilbert modelliert, und wenn es grobe Schnitzer gegeben hätte, hätten die beiden auf diese ebenso hingewiesen wie die Kommentatoren G. Humbert und Th. Got der französischen Übersetzung [40].

Hilberts „Beweis“ der Kontinuumshypothese ist das Programm, das er 1925 (und nicht in den frühen 1930er Jahren) in einem Vortrag [44] skizzierte. Die Darstellung Rotas war auch Grundlage für entsprechende Aussagen auf der Wikipedia-Seite [96]. Es ist wohl an der Zeit, Tausskys „viele Fehler“, die sie in Hilberts Bericht entdeckt haben will, ein für alle Mal zu beerdigen.

Auch eine auf den ersten Blick abfällige Bemerkung Hasses über den *Zahlbericht* in seinem Brief an Kurt Hensel [80] vom April 1923 ist eher eine augenzwinkernde Hommage an seinen Lehrer, den Schöpfer der $p$-adik, als ein Vorwurf in Richtung Hilbert. In diesem Brief geht es um Normenreste in relativ-zyklischen Erweiterungen, an der Hensel und Hasse gemeinsam arbeiteten. Hasse zitiert drei Sätze Takagis und schreibt zum Schluss:

> *Übrigens habe ich Herrn Tornier vorige Woche ein längeres Manuskript über die Theorie der Trägheits- und Verzweigungskörper mit Ihren Methoden entwickelt, gesandt, das Ihnen Herr Tornier wohl gerne mal zur Verfügung stellt. Sie finden darin die genaue Skizzierung der nur angedeuteten Sätze 1.) – 3.) über diese Körper und zwar aus dem „botokudischen“ Hilbertschen Zahlbericht ins „Deutsche“ übersetzt und mit Zusätzen versehen.*

Zu Beginn des 19. Jahrhunderts hatten Johann Baptist von Spix und Carl Friedrich Philipp von Martius zwei Indiokinder von Brasilien nach München gebracht[9] und deren Sprache (das Botokudische, nicht das Bayrische) wurde bald zum Synonym für etwas vollkommen Unverständliches.

In seinem zitierten Brief an Hensel spielt Hasse darauf an, dass Trägheits- und Verzweigungsgruppen lokale Größen sind, sich also bei der Komplettierung eines Zahlkörpers nicht ändern und die folglich, ebenso wie die ohnehin lokale Theorie der Normenreste, mit Hilfe der von Hensel entwickelten Theorie der $p$-adischen Zahlen beschrieben werden können. Hasses Ziel war es, die Normenresttheorie im abelschen (und eventuell im galoisschen) Fall in die einzelnen Verzweigungskörper aufzuspalten. Selbstverständlich wollte Hasse dies nicht als Vorwurf an Hilbert verstanden wissen, da Hensel seine Theorie der $p$-adischen Zahlen erst nach dem Erscheinen des *Zahlberichts* veröffentlichte.

## 6. Der Inhalt

**Hilberts Vorwort.** Der folgende Satz aus Hilberts Vorwort über das Wesen der Theorie der algebraischen Zahlkörper ist oft zitiert worden:

[9] Auch in anderen europäischen Ländern wurden Schwarze und Indianer zum „Völkerschauen“ ausgestellt; die beiden Kinder Juri und Miranha, die Spix und Martius zu diesem Zweck nach München gebracht hatten, starben 1821 und 1822 bereits im Alter von 14 Jahren. Mehr dazu findet man in der von Anne Dreesbach verfassten Dissertation *Gezähmte Wilde: Die Zurschaustellung „exotischer“ Menschen in Deutschland 1870–1940*, Campus-Verlag 2005.

*Die Theorie der Zahlkörper ist wie ein Bauwerk von wunderbarer Schönheit und Harmonie; als der am reichsten ausgestattete Teil dieses Bauwerkes erscheint mir die Theorie der Abelschen und relativ-Abelschen Körper, die uns Kummer durch seine Arbeiten über die höheren Reziprozitätsgesetze und Kronecker durch seine Untersuchungen über die komplexe Multiplikation der elliptischen Funktionen erschlossen haben.*

Zu diesem Bauwerk von wunderbarer Schönheit gehören nach Hilbert auch die von Dirichlet und Riemann eingeführten analytischen Methoden, und zwar auch deswegen, weil zwischen der Theorie der algebraischen Zahlkörper und derjenigen der algebraischen Funktionen einer Veränderlichen zahlreiche und merkwürdige Analogien bestehen. Auf eine dieser Analogien weist er in seinem Artikel über relativquadratische Zahlkörper hin, wo er schreibt, dass das Reziprozitätsgesetz, ausgedrückt durch die Produktformel für Hilbertsymbole, „an den Cauchyschen Integralsatz in der Funktionentheorie“ erinnere.

Noch mehr Aufmerksamkeit hat eine andere Stelle erfahren, in der Hilbert die Rolle der Theorie der Zahlen als die Königin der Mathematik untermauert. Hilbert deutet die Entwicklung der Mathematik im ausgehenden 19. Jahrhundert als Arithmetisierung, also die Zurückführung aller mathematischen Wahrheiten einer Theorie auf Beziehungen natürlicher Zahlen. Dieses Programm sah er durch die Arbeiten von Cauchy, Weierstraß und Cantor in der Analysis bereits verwirklicht, während er, was die Arithmetisierung der Geometrie betrifft, keine andern Mathematiker zitiert. Für eine eingehende Untersuchung dieser Fragen verweisen wir auf Laugwitz [64], sowie Petri & Schappacher [77].

**Der Bericht.** Hilbert unterteilt seinen Bericht in fünf Teile (vgl. Tab. 1). Der erste Teil ist dabei im Wesentlichen eine Zusammenfassung der Dedekindschen Idealtheorie mit Einsprengseln von Kronecker. Das einzig wesentlich neue ist Hilberts Betonung der Relativkörper, also das Studium von Erweiterungen von Zahlkörpern. Dies ist der Rahmen, in welchem Hilbert die Kummersche Theorie der Kummererweiterungen $K(\sqrt[p]{\mu})/K$ des Kreisteilungskörpers $K = \mathbb{Q}(\zeta_p)$ betrachtet. Erst dieser Blickwinkel hat seine Vision der Hilbertschen Klassenkörper, zuerst im Spezialfall der relativquadratischen Erweiterungen, als abelsche Erweiterungen mit Relativdiskriminante (1) ermöglicht. Der zweite Teil des *Zahlberichts* baut ebenfalls darauf auf und bringt die Theorie der Galoiserweiterungen, also eine Darstellung der Hilbertschen Ergebnisse über Zerlegungs-, Trägheits und Verzweigungsgruppen. Hilbert stellt als wesentliches Hilfsmittel für den analytischen Teil der Beweise des Reziprozitätsgesetzes den Kroneckerschen Dichtesatz bereit, wonach die Primideale, die in einer normalen Erweiterung $L/K$ voll zerfallen, die Dichte $1/(L : K)$ besitzen. Einen Hilfssatz, der in einem Spezialfall bereits bei Kummer auftaucht, erhebt Hilbert in den Rang eines Satzes; in ihren Arbeiten über die Klassenkörpertheorie zitieren Furtwängler und Takagi diesen Satz so oft, dass er schließlich als „Hilberts Satz 90“ bekannt wird. Auch die Tatsache, dass die Idealklassengruppe eines Zahlkörpers von Primidealen ersten Grades erzeugt wird, geht im Spezialfall von Kreisteilungskörpern auf Kummer zurück.

Der dritte Teil über quadratische Zahlkörper ordnet den großen Abschnitt V der Gaußschen *Disquisitiones*, nämlich die Theorie der binären quadratischen Formen, in die algebraische Zahlentheorie ein. Der neue Gesichtspunkt ist die zentrale

| Teil | Nr. | Stichworte |
|---|---|---|
| 1 | | Algebraische Zahlkörper |
| | 1 | Norm, Spur, Differente, Diskriminante, Ganzheitsbasis |
| | 2 | Fundamentalsatz der Idealtheorie; Zerlegbare Formen |
| | 3 | Restklassenringe, kleiner Fermatscher Satz |
| | 4 | Zerlegung der Ideale, Diskriminantenteiler, Verzweigung |
| | 5 | Relativerweiterungen; Transitivität der Differente |
| | 6 | Dirichlets Einheitensatz |
| | 7 | Endlichkeit der Klassenzahl; Dedekindsche $\zeta$-Funktion |
| | 8 | Zerlegbare Formen; Formenklassen |
| | 9 | Ordnungen; Ringklassengruppe; Einheiten in Ordnungen |
| 2 | | Galoiserweiterungen |
| | 10 | Zerlegungs-, Trägheits und Verzweigungsgruppen |
| | 11 | Differente und Diskriminante in Galoiserweiterungen |
| | 12 | Kroneckers Dichtesatz |
| | 13 | Komposita von Zahlkörpern |
| | 14 | Primideale ersten Grades erzeugen Idealklassengruppe |
| | 15 | Relativzyklische Erweiterungen von Primzahlgrad; Satz 90 |
| 3 | | Quadratische Zahlkörper |
| | 16 | Zerlegungsgesetz; Pellsche Gleichung |
| | 17 | Geschlechtertheorie |
| | 18 | Hauptgeschlechtssatz; ambige Klassenzahlformel |
| | 19 | Klassenzahlformel; biquadratische Zahlkörper |
| | 20 | Korrespondenz Moduln und quadratischen Formen |
| 4 | | Kreiskörper |
| | 21 | Zerlegungsgesetz |
| | 22 | Ganzheitsbasen, Diskriminante |
| | 23 | Satz von Kronecker-Weber |
| | 24 | Primidealzerlegung Gaußscher Summen |
| | 25 | Eisensteins Reziprozitätsgesetz |
| | 26 | Klassenzahlformel; Kreiseinheiten |
| | 27 | Anwendung auf das quadratische Reziprozitätsgesetz |
| 5 | | Kummererweiterungen |
| | 28 | Zerlegungsgesetz |
| | 29 | Normenreste |
| | 30 | Primideale mit vorgeschriebenem Restcharakter |
| | 31 | Teilbarkeit der Klassenzahl von $\mathbb{Q}(\zeta_p)$ durch $p$ |
| | 32 | Ambige Klassenzahlformel |
| | 33 | Reziprozitätsgesetz für reguläre Primzahlen |
| | 34 | Geschlechtertheorie |
| | 35 | Zweiter Beweis des Reziprozitätsgesetzes |
| | 36 | Die Fermatgleichung |

TABELLE 1. Der Inhalt von Hilberts Zahlbericht

Stellung der Geschlechtertheorie, zu deren Beschreibung Hilbert hier sein Normenrestsymbol einführt, mit welchem er später den Kummerschen Arbeiten Struktur gibt. In der Tat war es eines von Hilberts Zielen, die Theorie der Kreiskörper in Analogie zu derjenigen der quadratischen Körper aufzubauen. In seinem Bericht schreibt er etwa am Ende von [39, § 34]:

> *Damit ist es dann gelungen, alle diejenigen Eigenschaften auf den regulären Kummerschen Körper zu übertragen, welche für den quadratischen bereits von Gauß aufgestellt und bewiesen worden sind.*

Was beim ersten Lesen klingt wie der erfolgreiche Abschluss einer Theorie war für Hilbert der Beginn eines Programms, das hier mit der Einschränkung auf *reguläre* Kreiskörper angekündigt wird: Die Ausdehnung dieser Resultate auf *beliebige* Kreiskörper besteht in der Entwicklung der Theorie des Hilbertschen Klassenkörpers, die Hilbert im Anschluss an den *Zahlbericht* mit seinen Arbeiten über relativquadratische und relativ-Abelsche Zahlkörper anstößt.

Die letzten beiden Teile des *Zahlberichts* gehen im Wesentlichen komplett auf Kummer zurück. Der Abschnitt über Kreiskörper bringt außerdem Eisensteins Reziprozitätsgesetz als Vorstufe und wesentliches Hilfsmittel zum Beweis des allgemeinen Reziprozitätsgesetzes, sowie die Primidealzerlegung Gaußscher Summen (Hilbert nennt sie nach ihrem Ursprung Lagrangesche Resolventen) und den Satz von Kronecker und Weber, wonach jede abelsche Erweiterung des rationalen Zahlkörpers in einem Kreisteilungskörper enthalten ist.

Während der Inhalt der ersten drei Kapitel bis auf kleinere Ausnahmen der Standardstoff ist, der auch in heutigen Lehrbüchern der Zahlentheorie behandelt wird[10], findet man die Resultate von Kapitel 4 eher in Monographien[11] über abelsche Zahlkörper.

Der größte Teil von Kapitel 5 ist, da sein Inhalt in der Klassenkörpertheorie aufgegangen ist, im Wesentlichen nur noch von historischer Bedeutung. Das ist ein Grund mehr, uns hier etwas ausführlicher damit auseinanderzusetzen.

## 7. Der Zahlbericht als Schlüssel zu Kummer

Von vielen Zahlentheoretikern wurde ein Aspekt des Hilbertschen *Zahlberichts* wiederholt hervorgehoben: Hilbert hat die Kummerschen Ergebnisse durch seine klare Darlegung der Allgemeinheit zugänglich gemacht. André Weil praktiziert einmal mehr seine sehr eigene Sicht der Dinge, und schreibt über Hilberts Übersetzung der Kummerschen Ergebnisse auf der ersten Seite des Vorworts zu Kummers *Collected Papers*:

> *Mehr als die Hälfte seines berühmten Zahlberichts, nämlich die Abschnitte IV und V, besteht in wenig mehr als der Darstellung von*

[10]Es gibt Ausnahmen: Quadratische Formen spielen heute nur noch eine Nebenrolle, und auch die analytischen Methoden, die zu Kroneckers Dichtesatz führen, werden nur selten in den üblichen Lehrbüchern behandelt; am nächsten kommen dem *Zahlbericht* wohl das Meisterwerk Heckes [33] und das jüngere Buch [25] von Fröhlich und Taylor.

[11]Hier sind Hasses Klassiker [32] zu nennen, von welchem demnächst eine englische Übersetzung durch Mikihito Hirabayashi erscheinen wird, sowie die Werke von S. Lang [63] und L. Washington [90].

> *Kummers zahlentheoretischem Werk, mit unwesentlichen Verbesserungen [...].*[12]

Diese Bemerkung sagt, wie schon Schappacher [82, S. 708] andeutet, mehr über Weil als über den Hilbertschen Bericht aus. Was Weil mit seiner Bemerkung wohl meint, erklärt er etwas später: Kummers zweiter Beweis des Reziprozitätsgesetzes läuft, so Weil (S. 11), auf die Berechnung des Normenrestsymbols $(\frac{\mu, D}{(1-\zeta)})$ hinaus:

> *Angesichts dieser Tatsache fehlt nichts mehr zur Formulierung des Hilbertschen Reziprozitätsgesetzes außer der Sprache und einer klaren Wahrnehmung der Beziehung zwischen „lokalen" und „globalen" Fakten.*[13]

Natürlich hat Weil leicht reden, denn wenn Hilbert die Kummerschen Rechnungen nicht in seine Produktformel übersetzt hätte, hätte Weil sie in Kummers Werk wohl kaum wiedererkannt: Erst durch die Hilbertsche Brille betrachtet bekommen Kummers Ergebnisse Struktur.

In der Tat erinnert Weils Aussage an eine andere, die er öfter in der ein oder anderen Form wiederholt hat. In seinem Artikel [93] nennt Weil einige Probleme, in denen unser Unwissen ziemlich vollständig sei, etwa die Frage, wie die Automorphismen der Galoisgruppe auf der Idealklassengruppe operieren (hier kann man den Satz von Weil-Shafarevich als Antwort im Falle abelscher Erweiterungen auffassen; für beliebige Galoiserweiterungen fasst [67] unser Unwissen zusammen), die Theorie der Normenreste in nicht-zyklischen Erweiterungen (hier hatte Arnold Scholz ([84]; siehe auch [71]) bereits tiefe Resultate erzielt, die allerdings vor [52] nicht verstanden worden sind), oder die Theorie der $\mathbb{Z}_p$-Erweiterungen (auf diesem Gebiet wurden in der zweiten Hälfte des 20. Jahrhunderts wesentliche Fortschritte erzielt), und schreibt dann:

> *Dies sind einige der Richtungen, über deren Verfolgung man nachdenken kann und soll, bevor man die Geheimnisse der nichtabelschen Erweiterungen betritt. Es ist durchaus möglich, dass wir dabei zu Prinzipien von außerordentlicher Fruchtbarkeit gelangen, und dass sich uns, wenn der erste entscheidende Schritt auf diesem Weg erst einmal gemacht ist, der Zugang zu weiten Gebieten öffnet, deren Existenz wir kaum erahnen; denn bisher, wie weit unsere Verallgemeinerungen der Gaußschen Resultate auch gehen, kann man nicht sagen, dass wir sie wirklich übertroffen hätten.*[14]

Dieser letzte Satz, schreibt Serre [13, S. 795], habe Serge Lang geschockt, während er selbst ihn berechtigt finde; Tate dagegen widerspricht Serre in seiner Antwort und nennt die Aussage bestenfalls dichterische Freiheit, eine Übertreibung, um einen

[12] More than half of his famous *Zahlbericht* (viz., parts IV and V) is little more than an account of Kummer's number-theoretical work, with inessential improvements [...].

[13] In view of this, nothing is missing for the formulation of Hilbert's reciprocity law, except the language and a clear perception of the relationship between "local" and "global" facts.

[14] Ce sont là quelques-unes des directions qu'on peut et qu'on doit songer à suivre afin de pénétrer dans le mystère des extensions non abéliennes; il n'est pas impossible que nous touchions là à des principes d'une fécondité extraordinaire, et que le premier pas décisif une fois fait dans cette voie doive nous ouvrir l'accès à de vastes domaines dont nous soupçonnons à peine l'existence; car jusqu'ici, pour amples que soient nos généralisations des résultats de Gauss, on ne peut dire que nous les ayons vraiment dépassés.

Punkt deutlich zu machen, und schlimmstenfalls eine Widerspiegelung der unangenehmen Seite von Weils Charakter.

Eine ähnliche Aussage hatte Weil auch in einem Brief [92] an seine Schwester Simone Weil gemacht, den er im März 1940 im Militärgefängnis von Rouen geschrieben hat: Er beschreibt, dass das quadratische Reziprozitätsgesetz nichts anderes sei als das Gesetz hinter den Koeffizienten der Artinschen L-Reihen. Letztere sind im abelschen Fall ganze Funktionen, während man im nichtabelschen Fall darüber nichts wisse:

> *es gibt hier, wie bereits Artin bemerkt hat, einen Angriffspunkt [. . . ]: Weil die bekannten Mittel der Arithmetik anscheinend nicht ausreichen, um zu zeigen, dass die Artinschen L-Reihen ganze Funktionen sind, darf man hoffen, dass der Beweis dieser Aussage eine Bresche schlägt, die es uns erlaubt, dort einzutreten [. . . ].*[15]

Mit „dort" meint Weil die Welt der nichtabelschen Reziprozitätsgesetze. Auch auf seine Idee des „unwesentlichen Fortschritts" wird bereits in diesem Brief angespielt:

> *[. . . ] man kann sagen, dass alles, was in der Arithmetik seit Gauß bis in unsere Zeit gemacht worden ist, aus Variationen über das Reziprozitätsgesetz besteht: Man ist vom Gaußschen ausgegangen und gelangt, als Krönung aller Arbeiten von Kummer, Dedekind und Hilbert, zu demjenigen von Artin, und es ist dasselbe.*[16]

Subtrahiert man die gewollte Provokation von Weils Aussagen, so bleibt ein gewisser Ausdruck der Frustration darüber, dass nicht einmal Artins Reziprozitätsgesetz aus der abelschen Welt herausragt. Vor diesem Hintergrund mag man die „unwesentlichen Verbesserungen" Hilberts durchaus als das größte Lob auffassen, zu dem André Weil fähig war.

Zurück zu Kummer: Dessen Arbeiten über die höheren Reziprozitätsgesetze wurden vor Hilbert wohl eher bewundert als studiert, und seinen Arbeiten über die Fermatsche Vermutung ging es nicht wesentlich besser, jedenfalls bis Vandiver in den 1920er Jahren begann, diese aufmerksam durchzuarbeiten. Ein kurzer Blick in den ersten Band von Kummers gesammelten Werken macht schnell deutlich, welche Opfer man bringen muss, um sich die Kummerschen Ideen zu eigen zu machen. Der einzige Mathematiker von Weltformat, der in der Kummerschen Welt zu Hause war, war Kummers Schüler Kronecker, der, um es vorsichtig auszudrücken, nicht gerade für eine meisterhafte Darstellung seiner eigenen tiefen Ideen bekannt war.

So schlummern auch heute noch viele Ideen in den Kummerschen Arbeiten, die durch das Hilbertsche Raster gefallen sind. Kummers Arbeit über kubische Gaußsche Summen [54, S. 145–163] und über das Auffinden von Assoziierten mit kleinen Koeffizienten bezüglich einer Ganzheitsbasis [54, S. 895–906] sind nur zwei Beispiele aus Kummers Werk, die meines Wissens (zu Unrecht) überhaupt nicht beachtet worden sind.

[15] il y a donc là, comme le signalait déja Artin, un point où faire porter l'attaque [. . . ]: *puisque* les moyens connus de l'arithmétique ne paraissent pas permettre de démontrer que les fonctions d'Artin sont des fonctions entières, on peut espérer qu'en le démontrant on aura ouvert une brèche qui permette d'entrer dans la place [. . . ].

[16] [. . . ] on peut dire que *tout* ce qui a été fait en arithmétique depuis Gauss jusqu'à ces dernières années consiste en variations sur la loi de réciprocité: on est pareti de celle de Gauss; on aboutit, couronnement de tous les travaux de Kummer, Dedekind, Hilbert, à celle d'Artin, et *c'est la même.*

## 8. Die Geschlechtertheorie

Die Geschlechtertheorie spielt seit Gauß eine ganz wichtige Rolle in der algebraischen Zahlentheorie: Kummer benutzte die Geschlechtertheorie in Kummererweiterungen für seinen Beweis des Reziprozitätsgesetzes, Hilbert formulierte sie mit Hilfe seines Normenrestsymbols, Hecke [33] beschrieb Normenreste mit deutlich mehr Gruppentheorie als Hilbert und machte einen großen Schritt in Richtung einer $p$-adischen Beschreibung der Geschlechter, und die frühe Klassenkörpertheorie von Takagi bis Hasse benutzte die Theorie der Geschlechter als unverzichtbares Hilfsmittel (sh. [68]).

8.1. **Normenreste bei Euler und Gauß.** Die ersten Untersuchungen über Restklassen, in welchen von einer quadratischen Form dargestellte Zahlen liegen, gehen auf Leonhard Euler zurück, wenn man von einigen Spezialfällen bei Bachet und Fermat absieht. Euler ist aufgefallen, dass die Form $x^2 - ay^2$ nur solche zu $4a$ teilerfremden Zahlen repräsentiert, deren Restklassen in einer Untergruppe vom Index 2 in der Gruppe der primen Restklassen modulo $4a$ liegen. Aus solchen Beobachtungen hat Euler dann seine Version des quadratischen Reziprozitätsgesetzes herausdestilliert. Einem Beweis seiner vielen Vermutungen auf diesem Gebiet ist erst Legendre näher gekommen.

Der erste vollständige Beweis des quadratischen Reziprozitätsgesetzes durch Gauß (siehe [28, Art. 125 ff] und [9]) ging von der Definition quadratischer Reste aus: schreibt man die Kongruenz $x^2 \equiv p \bmod q$ als Gleichung $x^2 - kq = p$, so kann man durch Reduktion modulo $p$ versuchen, das Restverhalten von $q$ modulo $p$ zu bestimmen. Mit Hilfe eines Induktionsbeweises und eines Lemmas, dessen Beweis in keinster Weise auf der Hand liegt, gelang Gauß die Durchführung.

Der zweite Gaußsche Beweis [28, Art. 262] benutzte die Theorie der Geschlechter quadratischer Formen. Die Kernidee dabei ist dieselbe wie beim ersten Beweis: Man verwandelt die Kongruenz $x^2 \equiv p \bmod q$ in eine Gleichung, die dann modulo $p$ reduziert wird. Im zweiten Beweis wird dies wie folgt realisiert: sind $p \equiv 1 \bmod 4$ und $q \equiv 3 \bmod 4$ prim, und gibt es nur eine Formenklasse der Diskriminante $4q$, dann folgt aus $(\frac{p}{q}) = 1$, dass $p$ von der Hauptform dargestellt wird, dass also $p = x^2 - qy^2$ gilt. Reduziert man diese Gleichung modulo $p$, so folgt daraus $(\frac{q}{p}) = +1$. Von der Beschränkung auf Klassenzahl 1 kann man sich befreien, indem man zeigt, dass die Klassenzahl in diesem Fall immer ungerade ist: Dies ist eine von vielen Folgerungen aus der Theorie der Geschlechter.

8.2. **Geschlechter bei Gauß.** In Abschnitt V seiner *Disquisitiones* betrachtete Gauß binäre quadratische Formen $Q(x, y) = Ax^2 + Bxy + Cy^2$, bei denen er allerdings $B$ als gerade annahm.

Ist $\Delta$ eine Fundamentaldiskriminante, also die Diskriminante eines quadratischen Zahlkörpers, dann kann man $\Delta$ eindeutig als Produkt von Primdiskriminanten schreiben, also Diskriminanten, die durch keine zwei verschiedene Primzahlen teilbar sind. So ist $\Delta = -20 = -4 \cdot 5$ und $\Delta = 21 = (-3)(-7)$. Jede Form $Q = Ax^2 + Bxy + Cy^2 = (A, B, C)$ mit Diskriminante $\Delta = B^2 - 4AC$ stellt Primzahlen dar, die zu $\Delta$ teilerfremd sind. Ist nun etwa $Q(x, y) = p$, dann hängen die Werte der Legendresymbole $\chi_j(p) = (\Delta_j/p)$ nicht von der Wahl der Primzahl $p$ ab, welche von $Q$ dargestellt wird, sondern nur von (der Klasse von) $Q$, und sind damit Charaktere der Form $Q$ selbst. Ist $\Delta = \Delta_1 \cdots \Delta_t$ die Zerlegung in Primdiskriminanten, dann gibt es also $t$ Charaktere $\chi_1, \ldots, \chi_t$. Der Gaußsche Hauptsatz der Geschlechtertheorie besagt dann, dass ein Vektor $(\pm 1, \cdots, \pm 1)$ genau dann das Charaktersystem einer Form ist, wenn das Produkt der Einträge $+1$ ist, und dass jede Form, deren Charaktersystem $(+1, \ldots, +1)$ ist, eine Klasse erzeugt, die ein Quadrat ist:

**Satz 8.1.** *Ist $\Delta$ eine Fundamentaldiskriminante mit Zerlegung $\Delta = \Delta_1 \cdots \Delta_t$ in Primdiskriminanten, dann definieren $\chi_j(Q) = (\frac{\Delta_j}{p})$, wo $p \nmid \Delta$ von der quadratischen Form $Q$ mit Diskriminante $\Delta$ dargestellt wird, Charaktere auf der Formenklassengruppe. Dabei gilt für jede Form $Q$ mit Diskriminante $\Delta$ die Produktformel*

$$\chi_1(Q) \cdots \chi_t(Q) = 1. \tag{1}$$

*Genau dann gilt $\chi_1(Q) = \cdots = \chi_t(Q) = 1$ für eine Form $Q$, wenn die Formenklasse von $Q$ ein Quadrat ist.*

**Beispiel.** Es gibt genau zwei Klassen von Formen der Diskriminante $\Delta = -15$, und diese werden von der Hauptform $x^2+xy+4y^2$ und von $2x^2+xy+2y^2$ repräsentiert.

Ist $p$ zur Diskriminante $d = -15$ teilerfrende Primzahl, die von der Hauptform dargestellt wird, so gilt

$$\begin{aligned} 4p &= (2x+y)^2 + 15y^2 \equiv (2x+y)^2 \bmod 3 \qquad \text{und} \\ 4p &= (2x+y)^2 + 15y^2 \equiv (2x+y)^2 \bmod 5. \end{aligned}$$

Für alle solchen Primzahlen gilt also $(\frac{-3}{p}) = (\frac{5}{p}) = +1$, wobei die Zähler der Legendresymbole von der Zerlegung der Diskriminante $15 = -3 \cdot 5$ in Primdiskriminanten herrühren.

Wird $p$ dagegen von der Form $(2,1,2)$ dargestellt, ist also etwa $p = 2x^2+xy+2y^2$, dann gilt $8p = (4x+y)^2 + 15y^2$, und diesmal zeigt eine Reduktion modulo 3 und 5, dass wegen $(\frac{2}{3}) = (\frac{2}{5}) = -1$ für alle solchen Primzahlen $(\frac{-3}{p}) = (\frac{5}{p}) = -1$ ist.

Im Falle $m = -15$ gibt es also zwei Charaktere $\chi_1(p) = (\frac{-3}{p})$ und $\chi_2(p) = (\frac{5}{p})$; außerdem gibt es zwei Formenklassen, nämlich $Q_1 = (1,1,4) = x^2 + xy + 4y^2$, sowie $Q_2 = (2,1,2)$. Nun ist $Q_1(1,2) = 19$ und $\chi(Q_1) = (\chi_1(Q_1), \chi_2(Q_1)) = ((\frac{-3}{19}), (\frac{5}{19})) = (+1,+1)$, sowie $Q_2(1,1) = 5$ und $\chi(Q_2) = (-1,-1)$. Wir halten diese Informationen in folgender Tabelle fest:

| $Q$ | $p$ | $\chi(Q)$ |
|---|---|---|
| $(1,1,4)$ | $19 = Q(1,2)$ | $(+1,+1)$ |
| $(2,1,2)$ | $5 = Q(1,1)$ | $(-1,-1)$ |

Die Klassengruppe der Formen mit Diskriminante $\Delta = -15 \cdot 2^2$ hat ebenfalls Ordnung 2; die Formen sind jetzt $Q_1(1,0,15)$ und $Q_2(3,0,5)$. Beide Formen stellen sowohl Primzahlen der Form $p \equiv 1 \bmod 4$ als auch solche der Form $p \equiv 3 \bmod 4$ dar, und wie im Falle $\Delta = -15$ gibt es genau zwei Charaktere:

| $Q$ | $p$ | $\chi(Q)$ |
|---|---|---|
| $(1,0,15)$ | $19 = Q(2,1)$ | $(+1,+1)$ |
| $(3,0,5)$ | $5 = Q(0,1)$ | $(-1,-1)$ |

Für $\Delta = -15 \cdot 4^2$ ist dagegen die Klassenzahl 4, und die Klassengruppe vom Typ $(2,2)$. Die Klassen werden erzeugt von den Formen $Q_1 = (1,0,60)$, welche nur Primzahlen $p \equiv 1 \bmod 4$ darstellt, $Q_2 = (5,0,12)$, die ebenfalls nur $p \equiv 1 \bmod 4$

darstellt, und den beiden Formen $Q_3 = (4, 0, 15)$ und $Q_4 = (3, 0, 20)$, welche beide nur Primzahlen der Form $p \equiv 3 \bmod 4$ darstellen. Zu $\chi_1$ und $\chi_2$ kommt also jetzt der Charakter $\chi_3(p) = (\frac{-1}{p})$ hinzu, und die Verteilung auf die Geschlechter sieht wie folgt aus:

| $Q$ | $p$ | $\chi(Q)$ |
|---|---|---|
| $(1, 0, 60)$ | $61 = Q(1, 1)$ | $(+1, +1, +1)$ |
| $(4, 0, 15)$ | $19 = Q(1, 1)$ | $(+1, +1, -1)$ |
| $(5, 0, 12)$ | $17 = Q(1, 1)$ | $(-1, -1, +1)$ |
| $(3, 0, 20)$ | $23 = Q(1, 1)$ | $(-1, -1, -1)$ |

Auch beim nächsten Schritt erhöht sich der 2-Rang der Klassengruppe, die für $\Delta = -15 \cdot 8^2$ den Typus $(2, 2, 2)$ hat. Die Hauptform $(1, 0, 240)$ stellt jetzt nur noch Primzahlen der Form $p \equiv 1 \bmod 8$ dar, was nahelegt, dass zu den drei bereits vorhandenen Charakteren jetzt der Charakter $\chi_4(p) = (\frac{2}{p}) = 1$ hinzukommt; die Aufstellung der entsprechenden Tabelle überlassen wir den Lesern.

Damit ist die Maximalanzahl der Charaktere erreicht: Für $\Delta = -15 \cdot 4^n$ mit $n \geq 4$ erhöht sich in jedem Schritt, in dem $n$ um 1 erhöht wird, die 2-Klassenzahl, der Rang bleibt aber konstant; die Klassengruppen haben dann Typ $(4, 2, 2)$, $(8, 2, 2, )$ usw.

8.3. **Normenreste bei Hilbert.** Wir wollen die Gaußsche Geschlechtertheorie jetzt von Hilberts Blickwinkel aus betrachten. Die von Euler und Gauß untersuchte Form $x^2 - my^2$ ist die Normform des quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{m}\,)$. Hilbert studiert die Restklassen modulo $p$, in welchen diese Normen liegen, nicht nur für die Teiler von $4m$, sondern für jede beliebige Primzahl.

Dies legt nahe, für Primzahlen $p$ die Abbildung

$$\nu_p : K_p^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \tag{2}$$

der Gruppe aller zu $p$ teilerfremden Elemente von $K^\times$ in die prime Restklassengruppe zu betrachten. Man findet dann leicht:

**Proposition 8.2.** *Für ungerade Primzahlen $p$ ist die durch (2) definierte Normabbildung $\nu_p$ surjektiv, falls $p$ unverzweigt ist, und das Bild hat Index 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$, wenn $p$ verzweigt ist.*

Für die Primzahl $p = 2$ funktioniert diese Idee nicht, weil die Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ trivial ist; stattdessen muss man hier die Restklassen modulo 4 (für Diskriminante $\Delta \equiv 4 \bmod 8$) bzw. modulo 8 (für Diskriminante $\Delta \equiv 0 \bmod 8$) betrachten, um ein analoges Ergebnis zu erhalten.

Hilbert führt nun ein neues Symbol $(\frac{a,b}{p})$ ein, das Normenrestsymbol. Dabei ist $p$ eine Primzahl, und $a$ und $b$ sind beliebige rationale Zahlen $\neq 0$, die modulo $p$ ganz sind. Die Zahl $a$ heißt dann ein Normenrest modulo $p$ im quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{b}\,)$, wenn es eine ganze algebraische Zahl $\alpha \in K^\times$ gibt, sodass $a$ für jedes $m \geq 1$ kongruent einer Norm $N\alpha$ modulo $p^m$ ist (hier darf $\alpha$ von $m$ abhängen). Hilbert setzt dann

$$\Big(\frac{a, b}{p}\Big) = \begin{cases} +1 & \text{falls } a \text{ Normenrest modulo } p \text{ in } \mathbb{Q}(\sqrt{b}\,) \text{ ist,} \\ -1 & \text{sonst.} \end{cases}$$

Hilbert zeigt, dass dieses Symbol bimultiplikativ ist, dass also $(\frac{aa',b}{p}) = (\frac{a,b}{p})(\frac{a',b}{p})$ und $(\frac{a,bb'}{p}) = (\frac{a,b}{p})(\frac{a,b'}{p})$ gilt; weilter gilt $(\frac{a,b}{p}) = (\frac{b,a}{p})$. Daneben hat das Normenrestsymbol zwei tiefliegende Eigenschaften; eine davon ist der folgende

**Satz 8.3.** *Das quadratische Reziprozitätsgesetz ist äquivalent zur Produktformel*

$$\prod_p \left(\frac{a,b}{p}\right) = 1 \tag{3}$$

*für alle positiven Zahlen $a$ und $b$.*

Dieses Produkt ist wohldefiniert, da das Normenrestsymbol für alle $p \nmid 2ab$ den Wert 1 hat. Um die Produktformel (3) auf ganze Zahlen mit beliebigem Vorzeichen zu übertragen führt Hilbert ein zusätzliches Symbol $(\frac{a,b}{-1})$ ein, das sich später als Hilbertsymbol an der unendlichen Primstelle von $\mathbb{Q}$ herausstellen wird.

Diese Formulierung des quadratischen Reziprozitätsgesetzes ist nicht nur äußerst elegant, sondern sie erlaubt, das quadratische Reziprozitätsgesetz in einem beliebigen algebraischen Zahlkörper zumindest hinzuschreiben. Hilbert hat dies in seiner Arbeit über relativquadratische Erweiterungen für den Fall bewiesen, dass die Klassenzahl des Grundkörpers ungerade oder $= 2$ ist.

Die zweite tiefliegende Eigenschaft des Normenrestsymbols ist der folgende Satz 102 von Hilberts Bericht:

**Satz 8.4.** *Sind $a \neq 0$ und $b$ ganze Zahlen und ist $b$ keine Quadratzahl, dann ist $a$ genau dann eine Norm einer Zahl des Körpers $\mathbb{Q}(\sqrt{b}\,)$, wenn $(\frac{a,b}{p}) = 1$ für jede Primzahl $p$ gilt.*

Um zu entscheiden, ob eine Zahl Norm aus einem quadratischen Zahlkörper ist, muss man daher nur nachprüfen, dass $(\frac{a,b}{p}) = 1$ für alle verzweigten Primzahlen $p$ gilt; das geht aber in endlich vielen Schritten.

Der eigentliche Zweck der Einführung des Normenrestsymbols war aber die Beschreibung der Geschlechtercharaktere. Dies gelingt Hilbert wie folgt: ist $\mathfrak{a}$ ein Ideal der Norm $N\mathfrak{a} = a$ im Zahlkörper $K = \mathbb{Q}(\sqrt{b}\,)$, den wir der Einfachkeit halber als imaginärquadratisch annehmen wollen, und sind genau die Primzahlen $p_1, \ldots, p_t$ in $K$ verzweigt, dann setzen wir

$$\chi_j(\mathfrak{a}) = \left(\frac{a,b}{p_j}\right) \quad \text{und nennen} \quad X(\mathfrak{a}) = (\chi_1(\mathfrak{a}), \ldots, \chi_t(\mathfrak{a}))$$

das Charakterensystem von $\mathfrak{a}$. Direkt aus der Definition des Normenrestsymbols und der Äquivalenz von Idealen folgt, dass das Charakterensystem $X(\mathfrak{a})$ eines Ideals $\mathfrak{a}$ nur von seiner Idealklasse abhängt (Satz 99).

Diese Stelle ist ganz typisch für die Hilbertsche Darstellung der Materie im Vergleich zu der, die wir gewohnt sind: während Hilbert mit Charakterensystemen rechnet, die nur von der Idealklasse abhängen, würden es heutige Leser gerne sehen, dass man ihnen sagt, $X$ induziere einen Homomorphismus $X : \mathrm{Cl}(K) \longrightarrow (\mathbb{Z}/2\mathbb{Z})^t$, oder noch besser, dass es eine exakte Sequenz

$$1 \longrightarrow \mathrm{Cl}(K)^2 \longrightarrow \mathrm{Cl}(K) \xrightarrow{X} (\mathbb{Z}/2\mathbb{Z})^t \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1 \tag{4}$$

gibt, aus der man den fundamentalen Isomorphismus $\mathrm{Cl}(K)/\,\mathrm{Cl}(K)^2 \simeq (\mathbb{Z}/2\mathbb{Z})^{t-1}$ ablesen kann (ist $K$ ein reellquadratischer Körper, so ist hier statt $\mathrm{Cl}(K)$ die Idealklassengruppe im engeren Sinne zu betrachten).

Wir wollen uns ansehen, was dies im Falle $K = \mathbb{Q}(\sqrt{-15}\,)$ bedeutet. Die beiden Idealklassen werden repräsentiert von $\mathfrak{o} = (1)$ und von $\mathfrak{z}_1 = (2, \frac{1+\sqrt{-15}}{2})$. Wegen $N(\mathfrak{o}) = 1$ ist $X(\mathfrak{o}) = (+1, +1)$. Um $X(\mathfrak{z}_1)$ zu bestimmen, müssen wir die Hilbertschen Normenrestsymbole $(\frac{2,-15}{p})$ für $p = 3$ und $p = 5$ bestimmen. Nach Definition ist $(\frac{2,-15}{p}) = 1$ genau dann, wenn $2 \equiv x^2 + xy + 4y^2$ modulo allen Potenzen von $p$ lösbar ist. Multiplikation mit 4 verwandelt diese Kongruenz in $8 \equiv (2x + y)^2 + 15y^2 \bmod 3^m$. Weil diese Kongruenz nicht einmal modulo $p = 3$ oder $p = 5$ lösbar ist, folgt $(\frac{2,-15}{3}) = (\frac{2,-15}{5}) = -1$ und damit $X(\mathfrak{z}_1) = (-1, -1)$. Weil die Hauptklasse ein triviales Charakterensystem besitzt, folgt daraus, dass das Ideal $\mathfrak{z}_1$ kein Hauptideal sein kann.

Letztendlich laufen Hilberts Normenrestsymbole also auf die Gaußschen Geschlechtercharaktere hinaus. Der große und wesentliche Unterschied ist, dass sich Hilberts Konstruktion ohne großartige Änderungen auf beliebige Zahlkörper erweitern lässt, welche die für die Normenrestsymbole notwendigen Einheitswurzeln enthalten. Die Beweise werden allerdings wegen der nichttrivialen Einheiten- und Idealklassengruppen deutlich schwieriger.

Im Laufe der späteren Untersuchungen von Hensel und vor allem von Hasse hat sich dann herausgestellt, dass das Hilbertsche Normenrestsymbol $(\frac{a,b}{p})$ ein $p$-adisches Symbol ist, sich also problemlos für $a, b \in \mathbb{Q}_p$ definieren lässt. Die Produktformel (3) ist dann das globale Band, das diese lokalen Symbole verbindet. Die Verallgemeinerung des Normenrestsymbols auf beliebige abelsche Erweiterungen ist dann erst mit Hilfe der neuen Interpretation des abelschen Reziprozitätsgesetzes durch Artin möglich geworden.

## 9. Kummers Reziprozitätsgesetz

Will man heutzutage einen kurzen Abriss der Geschichte der Reziprozitätsgesetze geben (siehe etwa [94], das bis zu den jüngsten Resultaten von Peter Scholze führt), so springt man in der Regel vom quadratischen direkt zu Artins Reziprozitätsgesetz. Um Hilberts Leistung angemessen würdigen zu können, kommen wir um eine Besprechung von Kummers Reziprozitätsgesetz aber nicht herum.

Dabei werden wir uns durchgehend, auch bei Zitaten aus Kummers Arbeiten, der modernen Bezeichnungsweise bedienen. Anstatt des heutigen $\zeta$ schrieb Kummer $\alpha$, die Primzahl $p$ hieß bei ihm $\lambda$, und wirkliche ebenso wie ideale Zahlen bezeichnete er mit $f(\alpha)$. Darüberhinaus war die Kummersche Bezeichnung für den natürlichen Logarithmus ein einfaches $l$, und seine Bernoullizahlen $B_n$ stimmen mit den heutigen $B_{2n}$ überein.

Die erste Hürde auf der Suche nach der Formulierung eines entsprechenden Reziprozitätsgesetzes war es, Bedingungen für $\alpha$ und $\beta$ zu finden, für welche das Reziprozitätsgesetz in seiner einfachsten Form $(\frac{\alpha}{\beta}) = (\frac{\beta}{\alpha})$ gelten würde. Kummer ließ sich dabei von der Vorstellung leiten, dass Jacobisummen

$$J(\chi, \psi) = \sum_{t \bmod p} \chi(t)\psi(1-t),$$

wo $\chi$ und $\psi$ modulo $q$ definierte Dirichletcharaktere mit Werten in den $p$-ten Einheitswurzeln sind, primär sein sollten. Diese von Jacobi und vor allem von Eisenstein ausgiebig untersuchten Summen haben unter anderem die beiden Eigenschaften

$$J(\chi, \chi) \equiv 1 \bmod \lambda^2 \quad \text{und} \quad J(\chi, \chi)\overline{J(\chi, \chi)} = q,$$

wobei der Querstrich komplexe Konjugation bedeutet und $\lambda$ wieder für das Primideal $(1-\zeta)$ über $p$ steht. Kummer nennt nun ein $\alpha \in \mathbb{Z}[\zeta]$ primär, wenn es ganze Zahlen $a$ und $b$ gibt mit

$$\alpha \equiv a \bmod \lambda^2 \quad \text{und} \quad \alpha\overline{\alpha} \equiv b \bmod p.$$

Durch ausgedehnte Rechnungen mit Primzahlen $5 \le p \le 23$ überzeugte er sich davon, dass das Reziprozitätsgesetz für primäre Zahlen tatsächlich in der einfachsten Form gilt:

**Satz 9.1** (Kummers Reziprozitätsgesetz). *Sind $\alpha$ und $\beta$ primäre Zahlen in $\mathbb{Z}[\zeta]$, so gilt*

$$\Big(\frac{\alpha}{\beta}\Big) = \Big(\frac{\beta}{\alpha}\Big).$$

Für $p = 3$ ist Kummers zweite Bedingung dafür, dass $\alpha$ primär ist, automatisch erfüllt, weil $\alpha\overline{\alpha} = N\alpha$ mit der Norm übereinstimmt. In diesem Fall stimmt Kummers Reziprozitätsgesetz genau mit dem Jacobi-Eisensteinschen kubischen Reziprozitätsgesetz überein.

Kummer teilt seine Vermutung Dirichlet und Jacobi in einem Brief vom 20. Januar 1848 mit, bittet sie aber darum, diese nicht weiter zu verbreiten, da er wohl befürchtete, Eisenstein könnte ihm beim Beweis seiner Vermutung zuvorkommen. Eine der vielen von Kummer berechneten Tabellen ziert den Umschlag des Bulletin of the American Mathematical Society vom Januar 2007, wie im dazugehörigen Artikel [20] erklärt wird.

Erst als Eisenstein 1850 eine Arbeit über die Auffindung der Form des allgemeinen Reziprozitätsgesetzes gibt (das cum grano salis der Ableitung der expliziten Reziprozitätsgesetze aus dem Artinschen entspricht) und wenig später den Beweis des Eisensteinschen Reziprozitätsgesetzes nachschiebt, wird Kummer nervös und veröffentlicht seine immer noch unbewiesene Vermutung in [57].

Der erste Schritt Kummers besteht im Nachweis, dass es für jedes zu $p \ge 5$ teilerfremde $\alpha$ eine Einheit $\varepsilon \in \mathbb{Z}[\zeta]$ gibt, sodass $\alpha\varepsilon$ primär ist. Dazu untersucht er die Kreiseinheiten, die für prime $p$ im Wesentlichen von Quotienten $\frac{1-\zeta^a}{1-\zeta}$ erzeugt werden. Kummer bevorzugt die Einheiten

$$\varepsilon_a = \sqrt{\frac{(1-\zeta^a)(1-\zeta^{-a})}{(1-\zeta)(1-\zeta^{-1})}} = \zeta^{\frac{1-a}{2}} \cdot \frac{1-\zeta^a}{1-\zeta} \tag{5}$$

für $2 \le a \le \frac{p-1}{2}$, weil diese im maximalen reellen Teilkörper $\mathbb{Q}(\zeta+\zeta^{-1})$ des Körpers der $p$-ten Einheitswurzeln liegen.

Offenbar muss man zum Beweis der Existenz der Einheit $\varepsilon$, die $\alpha\varepsilon$ primär macht, die Restklassen dieser Kreiseinheiten modulo Potenzen von $\mathfrak{p} = (1-\zeta)$ betrachten. Dazu konstruiert Kummer Homomorphismen $\mathcal{L}^r$ der multiplikativen Gruppe aller zu $p$ teilerfremden Elemente von $\mathbb{Q}(\zeta)$ in die additive Gruppe von Restklassen modulo $p$. Mit diesen logarithmischen Abbildungen beschäftigen wir uns als nächstes.

## 10. Restklassen und Ableitungen

In den nächsten Abschnitten wollen wir anhand der Kummerschen logarithmischen Differentialquotienten die Vorgehensweise von Kummer und Hilbert vergleichen.

Dabei wollen wir nicht sofort mit den Kummerschen Definitionen ins Haus fallen, sondern uns relativ behutsam den etwas sperrigen Objekten nähern. Dazu sei $\zeta$ eine primitive $p$-te Einheitswurzel und $\mathbb{Z}[\zeta]$ der Ring ganzer Zahlen in $\mathbb{Q}(\zeta)$. Die Elemente von $\mathbb{Z}[\zeta]$ haben die Form

$$\alpha = a_0 + a_1\zeta + \ldots + a_{p-1}\zeta^{p-1},$$

wo die $a_j \in \mathbb{Z}$ sind. Diese Darstellung ist eindeutig bis auf Addition ganzzahliger Vielfacher von $1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1} = 0$.

Das Element $\lambda = \zeta - 1$ erzeugt das Primideal $\mathfrak{p} = (\lambda)$ der Norm $p$ in $\mathbb{Z}[\zeta]$. Offenbar ist $\zeta \equiv 1 \bmod \mathfrak{p}$ und folglich

$$\alpha = a_0 + a_1\zeta + a_2\zeta^2 + \ldots + a_{p-1}\zeta^{p-1} \equiv a_0 + a_1 + \ldots + a_{p-1} \bmod \mathfrak{p}.$$

Wir setzen

$$D^0(\alpha) = a_0 + a_1 + \ldots + a_{p-1} + p\mathbb{Z}.$$

Dies ist wohldefiniert, weil die Addition eines Vielfachen von $1+\zeta+\zeta^2+\cdots+\zeta^{p-1}$ die Summe der Koeffizienten nur um ein Vielfaches von $p$ ändert. Da $D^0$ jedem Element seine Restklasse modulo $\mathfrak{p}$ zuordnet, ist $D^0 : \mathbb{Z}[\zeta] \longrightarrow \mathbb{F}_p$ ein Ringhomomorphismus mit Kern $\ker D^0 = \mathfrak{p}$.

Die Restklasse von $\alpha$ modulo $\mathfrak{p}^2$ können wir ebenfalls bestimmen:

$$\begin{aligned}\alpha &= a_0 + a_1\zeta + a_2\zeta^2 + \ldots + a_{p-1}\zeta^{p-1} \\ &= (a_0 + a_1 + \ldots + a_{p-1}) + a_1(\zeta - 1) + a_2(\zeta^2 - 1) + \ldots + a_{p-1}(\zeta^{p-1} - 1) \\ &= D^0(\alpha) + (\zeta - 1)(a_1 + a_2(\zeta + 1) + a_3(\zeta^2 + \zeta + 1) + a_{p-1}(\zeta^{p-2} + \ldots + \zeta + 1)) \\ &\equiv D^0(\alpha) + (\zeta - 1)(a_1 + 2a_2 + \ldots + (p-1)a_{p-1}) \bmod \mathfrak{p}^2,\end{aligned}$$

denn es ist ja $\zeta^k(\zeta - 1) \equiv (\zeta - 1) \bmod \mathfrak{p}^2$. Setzen wir

$$D^1(\alpha) = a_1 + 2a_2 + \ldots + (p-1)a_{p-1},$$

so ist $\alpha \equiv D^0(\alpha) + (\zeta - 1)D^1(\alpha) \bmod \mathfrak{p}^2$.

Dass $D^1(\alpha)$ einer Ableitung ähnelt, kann man ausnutzen, indem man das Polynom

$$A_\alpha(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{p-1}x^{p-1}$$

einführt. Dann folgt nämlich $D^0(\alpha) = A_\alpha(1) + p\mathbb{Z}$ und $D^1(\alpha) = A'_\alpha(1) + p\mathbb{Z}$.

Nach der Produktregel gilt offenbar

$$D^1(\alpha\beta) = D^1(\alpha)D^0(\beta) + D^0(\alpha)D^1(\beta).$$

Einfacher als $D^1$ benimmt sich der Quotient $\mathcal{L}^1 = \frac{D^1}{D^0}$, denn für ihn gilt

$$\begin{aligned}\mathcal{L}^1(\alpha\beta) = \frac{D^1(\alpha\beta)}{D^0(\alpha\beta)} &= \frac{D^1(\alpha)D^0(\beta) + D^0(\alpha)D^1(\beta)}{D^0(\alpha)D^0(\beta)} \\ &= \frac{D^1(\alpha)}{D^0(\alpha)} + \frac{D^1(\beta)}{D^0(\beta)} = \mathcal{L}^1(\alpha) + \mathcal{L}^1(\beta).\end{aligned}$$

Also ist $\mathcal{L}^1$ ein Gruppenhomomorphismus der multiplikativen Gruppe der zu $\mathfrak{p}$ teilerfremden Elemente von $\mathbb{Q}(\zeta)$ in die additive Gruppe $\mathbb{F}_p$. Weiter rechnet man leicht nach, dass $\ker \mathcal{L}^1 = \mathfrak{p}^2$ ist; insbesondere ist $\mathcal{L}^1$ auf allen Elementen der Restklasse $\alpha \equiv 1 \bmod \mathfrak{p}^2$ trivial.

Mit Hilfe von $\mathcal{L}^1$ kann man die Einheitswurzel $\zeta^r$ bestimmen, für die $\alpha\zeta^r$ semiprimär wird (vgl. Satz 1.1). Offenbar ist $\alpha\zeta^r$ genau dann semiprimär, wenn $D^1(\alpha\zeta^r) \equiv 0 \bmod p$ ist, was wiederum zu $\mathcal{L}^1(\alpha\zeta^r) \equiv 0 \bmod p$ äquivalent ist. Nun gilt $\mathcal{L}^1(\alpha\zeta^r) \equiv \mathcal{L}^1(\alpha) + r\mathcal{L}^1(\zeta) \equiv \mathcal{L}^1(\alpha) + r \bmod p$, folglich müssen wir $r \equiv -\mathcal{L}^1(\alpha) \bmod p$ wählen.

Das Kummersche Reziprozitätsgesetz für $p$-te Potenzreste gilt in seiner einfachsten Form $(\alpha/\beta) = (\beta/\alpha)$ nur dann, wenn $\alpha$ primär gewählt wird. Ein zu $p$ teilerfremdes Element von $\mathbb{Z}[\zeta]$ heißt dabei primär, wenn $\alpha$ einer ganzen Zahl kongruent modulo $\lambda^2$ ist und wenn darüberhinaus auch $\alpha\overline{\alpha}$ einer ganzen Zahl kongruent modulo $p$ ist, wo $\overline{\alpha}$ die komplexe Konjugierte von $\alpha$ bezeichnet. Um $\alpha$ in primäre Form zu bringen, genügen für $p \geq 5$ die Einheitswurzeln nicht mehr. Vielmehr muss man $\alpha$ geschickt mir Kreiseinheiten multiplizieren, um eine primäre Zahl zu erhalten.

Die genauen Potenzen der Kreiseinheiten kann man dabei mit Hilfe der logarithmischen Differentialquotienten $\mathcal{L}^r$ bestimmen, von denen das oben konstruierte $\mathcal{L}^1$ das einfachste Beispiel ist. Um auch die höheren Differentialquotienten zu konstruieren, bemerken wir, dass $\mathcal{L}_1(\alpha) = \frac{A'_\alpha(1)}{A_\alpha(1)}$ gleich dem Wert der Ableitung von $\log A_\alpha(x)$ an der Stelle $x = 1$ ist. Gleichbedeutend damit ist die Definition $\mathcal{L}^1(\alpha) = \frac{d}{dv} A_\alpha(e^v)|_{v=0}$, und die naheliegende Verallgemeinerung dieser Formel ist es, welche die für Kummers Zwecke einfachsten Gleichungen liefert.

## 11. Kummers logarithmische Differentialquotienten

Kummer hat sich diesen Abbildungen $\mathcal{L}^r$ auf anderem Weg genähert als wir bei der Konstruktion von $\mathcal{L}^1$. Ein erster spezieller Fall der logarithmischen Differentialquotienten taucht das erste Mal in Kummers Arbeit [55] (deren Resultate er in [56] auf französisch publiziert) auf, und zwar im Beweis des Satzes, dass die Klassenzahl des Zahlkörpers der $p$-ten Einheitswurzeln genau dann durch $p$ teilbar ist (man sagt dann auch, $p$ sei irregulär), wenn $p$ eine der Bernoullizahlen $B_{2k}$ mit $k \leq \frac{p-3}{2}$ teilt. Dazu muss Kummer das Verhalten einer Determinante von Kreiseinheiten $\varepsilon_a$ modulo $p$ betrachten. Zur Herleitung dieser Kongruenzen ersetzt er die Kreiseinheiten durch Funktionen, indem er $\zeta$ in der Gleichung (5) durch die Variable $x$ ersetzt:

$$\varepsilon_a(x) = \sqrt{\frac{(1-x^a)(1-x^{-a})}{(1-x)(1-x^{-1})}}.$$

Von dieser Gleichung nimmt er die Ableitung der Logarithmen, also $\frac{d}{dx}\log(\varepsilon_a(x))$ und setzt dann wieder $x = \zeta$.

Vor allen Dingen zwei Ergebnisse seiner Überlegungen sind für seinen Beweis der Fermatschen Vermutung wesentlich. Zum einen ist es die Aussage, dass der zweite Faktor der Klassenzahl nur dann durch $p$ teilbar sein kann, wenn es der erste ist, dass also eine Primzahl $p$ genau dann regulär ist, wenn sie die ersten $\frac{p-3}{2}$ Bernoullizahlen nicht teilt, zum andern das fundamentale Kummersche Lemma über Einheiten, die einer rationalen Zahl kongruent modulo $p$ sind:

**Satz 11.1** (Kummers Lemma). *Ist $\varepsilon \in \mathbb{Z}[\zeta]$ eine Einheit, welche modulo $p$ einer ganzen rationalen Zahl kongruent ist, und ist $p$ regulär, dann ist $\varepsilon$ die $p$-te Potenz einer Einheit in $\mathbb{Z}[\zeta]$.*

Klassenkörpertheoretisch sieht die Sache so aus: ist $\varepsilon$ einer rationalen Zahl kongruent modulo $p$, dann ist $\varepsilon$ modulo $p$ zu einer $p$-ten Potenz kongruent, und daher $K(\sqrt[p]{\varepsilon})/K$ eine unverzweigte abelsche Erweiterung von $K = \mathbb{Q}(\zeta)$. Da $p$ die Klassenzahl nicht teilt, muss diese Erweiterung trivial sein, folglich ist $\varepsilon$ eine $p$-te Potenz.

Dieselbe Idee wendet Kummer in seiner nächsten Arbeit [58] zur Herleitung des Potenzrestcharakters von Kreiseinheiten mit Mitteln der Kreisteilung auch auf

Gaußsche Summen $F(\zeta,\xi)$ an. Eine der dabei auftretenden Kongruenzen erinnert ihn an die Produktregel für $m$-te Ableitungen, und dies führt ihn dazu, Differentialquotienten

$$\frac{d_0^r F(e^v,\xi)}{dv^r}$$

einzuführen,

> *wo die dem Zeichen des Differentials d zugefügte Null bedeutet, daß nach der Differentiation $v = 0$ zu setzen ist.*

Nach einigen Zeilen erscheint dann der Ausdruck

$$\frac{d_0^{m+1} \log F(e^v,\xi)}{dv^{m+1}},$$

also der logarithmische Differentialquotient.

Im Laufe der nächsten Jahre arbeitet Kummer mit seinen logarithmischen Differentialquotienten. Diese ermöglichen ihm, auf direktem Weg den Zusammenhang zwischen Kreiseinheiten $\varepsilon_a$ und Bernoullizahlen herzuleiten; es gilt nämlich (S. 531)

**Satz 11.2.** *Für die Kreiseinheiten $\varepsilon_a$ aus (5) gilt*

$$\frac{d_0^{2n} \log \varepsilon_a(e^v)}{dv^{2n}} = (-1)^{n+1}(a^{2n}-1)\frac{B_{2n}}{2n}.$$

Dieser Satz ist der wesentliche Bestandteil, den Kummer zur Lösung der folgenden Aufgabe braucht ([58, S. 138]):

> **Aufgabe.** *Eine gegebene complexe Zahl durch Multiplikation mit Einheiten in eine solche Form zu bringen, daß sie, mit ihrer reciproken multipliziert, ein Product giebt, welches einer nichtcomplexen ganzen Zahl congruent ist, für den Mod. p.*

Wie Kummer schreibt, hat diese Aufgabe immer dann eine Lösung, wenn $p$ regulär ist, also keine der ersten $\frac{p-3}{2}$ Bernoullizahlen $B_{2k}$ durch $p$ teilbar ist.

Kummer versucht nun, sein Reziprozitätsgesetz mit Mitteln der Kreisteilung zu beweisen, muss aber schließlich kapitulieren, weil er die auftretenden Probleme mit Primidealen, nach welchen sämtliche Einheiten $p$-te Potenzreste sind, nicht in den Griff bekommt.

Daraufhin wendet sich Kummer dem zweiten Gaußschen Beweis des quadratischen Reziprozitätsgesetzes zu, das die Theorie der Geschlechter quadratischer Formen oder, aus Kummers Sicht, der Theorie idealer Zahlen in quadratischen Erweiterungen benutzt. Die naturgemäße Verallgemeinerung wäre eine Theorie der Geschlechter in Erweiterungen $L = K(\mu^{1/p})$ des Körpers $K = \mathbb{Q}(\zeta)$ der $p$-ten Einheitswurzeln.

Kummers Problem bestand nun erst einmal darin, dass es ihm nicht gelang, eine ordentliche Theorie der idealen Zahlen in $L$ aufzubauen, was wenig verwunderlich ist, da er den Begriff der ganzen algebraischen Zahl nicht besaß. Er konnte daher nur mit idealen Zahlen in Ordnungen arbeiten, was notwendig zum Ausschluss der verzweigten Stellen führte. Dies macht man sich leicht am Beispiel quadratischer Zahlkörper klar. So zeigt etwa die Gleichung $(1+\sqrt{-3}\,)(1-\sqrt{-3}\,) = 2\cdot 2$ in der Ordnung $\mathbb{Z}[\sqrt{-3}]$ nicht nur, dass $\mathbb{Z}[\sqrt{-3}]$ kein ZPE-Ring ist (ein ZPE-Ring ist ein Integritätsbereich mit eindeutiger Primfaktorzerlegung, auch faktorieller Ring genannt), vielmehr ist sie auch dafür verantwortlich, dass das Ideal $I = (2, 1+\sqrt{-3}\,)$ in dieser Ordnung der Gleichung $I^2 = 2I$ genügt, während doch $I \neq (2)$ ist. Die

Kürzungsregel für Ideale wird also falsch, was Kummer dazu zwang, die idealen Primteiler von $p\mu$ in $L$ aus seinen Betrachtungen auszuschließen.

Auch Arnold Meyer, der in seinem Artikel [75] aus dem Jahre 1870 die Theorie der Formen über dem Ring $\mathbb{Z}[\omega]$ mit Hilfe idealer Zahlen studiert, muss mangels des Begriffs der ganz-algebraischen Zahl gewisse ideale Zahlen aus seiner Theorie ausschließen:

> *Von idealen Primfaktoren der Zahlen $s$ und $t$, sowie der Zahl 3 sehe ich ab, da die Einführung solcher für das folgende keinen Vorteil gewährt. Wenn daher im folgenden von idealen Zahlen die Rede ist, so sind damit immer solche gemeint, deren Normen zu $3D$ prim sind.*

Kummer wird dadurch in seinem ersten Beweis des Reziprozitätsgesetzes gezwungen, zwei verschiedene Ordnungen zu betrachten; einmal arbeitete er in den „complexen Zahlen in $w$", also in der Ordnung $\mathcal{O}_K[w]$, wo $\mathcal{O}_K = \mathbb{Z}[\zeta]$ und $w^p = \mu \in \mathbb{Z}[\zeta]$ ist, zum andern musste er zur glatten Formulierung seiner Geschlechtertheorie eine weitere Ordnung einführen, nämlich die Unterordnung der „complexen Zahlen in $z$", die aus Kombinationen von Konjugierten der Zahl

$$z_0 = (1-\zeta)(1 + w + w^2 + \ldots + w^{p-1})$$

besteht.

Durch die Betrachtung dieser Ordnung gewinnt Kummer, ähnlich wie wir das oben im quadratischen Fall vorgeführt haben, „zusätzliche" Geschlechtercharaktere, und ist dadurch in der Lage, wie André Weil im Vorwort zu [54] bemerkt, zu unserem und zu Hilberts Erstaunen (siehe [39, § 163]) seine lückenhaften Kenntnisse in einen Vorteil zu verwandeln.

Einer der wichtigsten Bausteine in Kummers Beweis ist ein notwendiges Kriterium dafür, dass ein Element aus $K$ Norm einer Zahl aus $L$ ist. In [61, S. 125] schreibt er:

> (I.) *Wenn eine complexe Zahl $F(\zeta)$ die Norm einer wirklichen complexen Zahl in $w$, der Determinante $D(\zeta)$ ist, so muß sie der Congruenz*
>
> $$D_{p-1}C_1 - D_{p-2}C_2 + D_{p-3}C_3 - \ldots - D_1C_{p-1} \equiv 0 \bmod p$$
>
> *genügen, in welcher*
>
> $$C_n = \frac{d_0^n \log F(e^v)}{dv^n}, \qquad D_n = \frac{d_0^n \log D(e^v)}{dv^n}$$
>
> *für $N = 1, 2, 3, \ldots, p-2$ und*
>
> $$C_{p-1} = \frac{1 - NF(\zeta)}{p}, \qquad D_{p-1} = \frac{1 - ND(\zeta)}{p},$$
>
> *und wenn die Zahlenwerthe der Größen $C_1, C_2, C_3, \ldots, C_{p-1}$ irgend wie gegeben sind, mit der alleinigen Bedingung, daß sie dieser Congruenz genügen, so kann man stets eine wirkliche complexe Zahl $F(w)$ der Determinante $D(\zeta)$ angeben, deren Norm $F(\zeta)$ diese gegebenen Zahlenwerthe der Größen $C_1, C_2, C_3, \ldots, C_{p-1}$ hat.*

Man muss schon sehr genau hinsehen um zu erkennen, dass und wie dieses Kummersche Resultat in die Klassenkörpertheorie eingeordnet werden kann. Deutlicher wird dies, wenn wir uns dieses Resultat mit Hilberts Augen ansehen.

## 12. Hilberts Verbesserungen

Wir wollen uns nun einige der „unwesentlichen Verbesserungen“ ansehen, die Hilbert am Kummerschen Zugang angebracht hat.

Hilbert beginnt seine Ausführungen über die Kummerschen Körper damit, die ganzen Elemente in $L = K(\sqrt[p]{\mu}\,)$ zu charakterisieren, die Diskriminante von $L$ zu bestimmen und die Primidealzerlegung in $L/K$ anzugeben. Dann überträgt er Kummers Beweis aus den Ordnungen der Zahlen in $w$ und in $z$ in die Maximalordnung von $L$.

Hilbert definiert die logarithmischen Differentialquotienten wie Kummer. Für ein $\alpha \in \mathbb{Z}[\zeta]$ mit $\alpha \equiv 1 \bmod \lambda$ wählt er eine Funktion $A_\alpha(x)$ mit $A_\alpha(\zeta) = \alpha$ und $A_\alpha(1) = 1$ und setzt

$$\mathcal{L}^r(\alpha) = \frac{d^r \log A_\alpha(e^v)}{dv^r}\Big|_{v=0}$$

für $1 \le r \le p-1$. Dann zeigt er, dass er für $1 \le r \le p-2$ die Bedingung $A_\alpha(1) = 1$ zu $\alpha \equiv 1 \bmod \lambda$ abschwächen darf, während für $r = p-1$

$$\mathcal{L}^r(\alpha) = \frac{d^r \log A_\alpha(e^v)}{dv^r}\Big|_{v=0} + \frac{A_\alpha(1)-1}{p}$$

gilt. Wie Kummer zeigt auch Hilbert [39, Hilfssatz 24, S. 267], dass

$$\mathcal{L}^{p-1}(\alpha) \equiv \frac{1-N\alpha}{p} \bmod p$$

ist. Dann kommt Hilbert zu den wesentlichen Sätzen. Kummers Ergebnis, dass Normen aus Kummererweiterungen $L = K(\mu^{\frac{1}{p}})$ der Kongruenz

$$\kappa(\alpha,\mu) = \mathcal{L}^1(\alpha)\mathcal{L}^{p-1}(\mu) - \mathcal{L}^2(\alpha)\mathcal{L}^{p-2}(\mu) \pm \cdots - \mathcal{L}^{p-1}(\alpha)\mathcal{L}^1(\mu) \equiv 0 \bmod p$$

genügen müssen, verwandelt Hilbert in sein Normenrestsymbol

$$\Big(\frac{\alpha,\mu}{\mathfrak{p}}\Big) = \zeta^{\kappa(\alpha,\mu)}$$

und zeigt, dass dieses Symbol bimultiplikativ und symmetrisch ist. Hilbert bleibt aber nicht bei diesem Symbol stehen, sondern führt entsprechende Symbole auch für unverzweigte Primideale ein, die über gewöhnliche Potenzrestsymbole definiert werden können und die technisch weitaus einfacher zu handhaben sind als die „wilden“ Symbole an der Stelle $(1-\zeta)$. Das Kummersche Reziprozitätsgesetz erweist sich dann als äquivalent zur formal vollendeten Produktformel

$$\prod_{\mathfrak{q}} \Big(\frac{\alpha,\mu}{\mathfrak{q}}\Big) = 1.$$

Damit nicht genug: ist $\alpha$ Normenrest für alle Primideale $\mathfrak{q}$, also $(\frac{\alpha,\mu}{\mathfrak{q}}) = 1$ für alle $\mathfrak{q}$, dann ist $\alpha$ schon eine Norm (Satz 167). Zum Hasseschen Lokal-Global-Prinzip fehlt hier nur noch die Verallgemeinerung des Satzes von Kummererweiterungen auf beliebige zyklische Erweiterungen und die explizit $p$-adische Sprache.

Kummers logarithmische Differentialquotienten tauchen auch in der jüngeren Literatur auf. Herbrand benutzte sie in seiner Arbeit [35] über den Zusammenhang zwischen der $p$-Klassengruppe des Körpers der $p$-ten Einheitswurzeln, und Coates & Wiles studierten damit lokale Einheiten, etwa im Zusammenhang mit der Hauptvermutung der Iwasawa-Theorie (siehe etwa [90, § 13.7], [63, Kap. 7], [12, § 2.6]).

## 13. Der Zahlbericht als Wegweiser

Mit dem *Zahlbericht* hat Hilbert das Tor zu weiteren Forschungen aufgestoßen. Durch die Formulierung des quadratischen und des Kummerschen Reziprozitätsgesetzes als Produktformel war klar, wie das allgemeine Reziprozitätsgesetz in beliebigen Zahlkörpern mit den erforderlichen Einheitswurzeln aussehen muss. Ebenso klar war, dass der Kummersche Weg in diesen Fällen nicht gangbar ist, weil sich dessen logarithmische Differentialquotienten nicht auf beliebige Erweiterungen verallgemeinern ließen (ob dies für abelsche Erweiterungen imaginärquadratischer Körper vielleicht doch möglich ist, indem man die Exponentialfunktion durch geeignete elliptische Funktionen ersetzt, ist eine Frage, über die nachzudenken sich wohl lohnen würde). Damit stand Hilbert vor dem Problem, sein Normenrestsymbol an verzweigten Primidealen auf anderem Weg zu definieren.

Im zweiten Beweis des Kummerschen Reziprozitätsgesetzes, den Hilbert ab § 166 in seinem Bericht gibt, umgeht er die Kummerschen Methoden, indem er nur die Normenrestsymbole an den Primstellen $\neq (1-\zeta)$ definiert und das fehlende Symbol mit Hilfe der Produktformel festlegt. Mit einem kleinen Trick gelingt es ihm, diese Technik in seinen Arbeiten über relativ-quadratische und relativ-abelsche Zahlkörper auch auf Erweiterungen mit mehr als einem verzweigten Primideal anzuwenden. Furtwängler setzte Hilberts Programm des Studiums unverzweigter abelscher Erweiterungen um, und Takagi gelang die Einbindung verzweigter Erweiterungen.

Der Weg zur Klassenkörpertheorie war mit einer ganzen Reihe von Problemen gepflastert, die erkannt und dann gelöst werden mussten. Hilberts Weg führte über die Reziprozitätsgesetze: Seine Formulierung des Kummerschen Reziprozitätsgesetzes als Produktformel des Normenrestsymbols erlaubte ihm die Frage, wie man ein allgemeines Reziprozitätsgesetz in beliebigen Zahlkörpern (welche die dazu notwendigen Einheitswurzeln enthalten mussten) formulieren und beweisen könne. Im von Hilbert zuerst betrachteten quadratischen Fall erwies es sich als notwendig, den Begriff eines primären Primideals zu klären und als ersten Schritt den „ersten Ergänzungssatz“ zu beweisen. Bereits in diesem Spezialfall des quadratischen Reziprozitätsgesetzes wurde die Rolle, welche unverzweigte quadratische Erweiterungen für die allgemeine Theorie spielen sollten, deutlich: Hilbert musste zuerst annehmen, dass die Klassenzahl des Grundkörpers ungerade ist und dann beweisen, dass in diesem Fall keine solchen unverzweigten quadratischen Erweiterungen existieren. Nachdem ihm für solche Grundkörper der Beweis des quadratischen Reziprozitätsgesetzes gelungen war, bewies er dieses für Grundkörper $k$ mit Klassenzahl 2 auf dem folgenden Weg:

(1) Es gibt genau eine unverzweigte quadratische Erweiterung $K/k$.
(2) Diese Erweiterung ist „Klassenkörper“ in dem Sinne, dass genau die Primideale in der Hauptidealklasse in $K/k$ zerlegt sind.
(3) Die Klassenzahl dieses Klassenkörpers $K$ ist ungerade.
(4) Das quadratische Reziprozitätsgesetz in $k$ folgt aus demjenigen in $K$.

Seine Vermutung, dass dieser Weg im Allgemeinen gangbar ist, führte Hilbert auf seine einzige falsche Vermutung über die Theorie des Klassenkörpers, dass nämlich der Klassenkörper eines Zahlkörpers mit Klassenzahl 4 eine ungerade Klassenzahl besitzt. Als Furtwängler begann, das Hilbertsche Programm umzusetzen, ist er über diese Stelle gestolpert. In einem Brief an Hilbert vom 6. Nov. 1905 schreibt er:

> *Ich habe einen Grundkörper $k$ mit der Klassenzahl $\ell^2$ [...] betrachtet, um zunächst den einfachsten Fall einer nichtzyclischen Klassengruppe zu haben. [...] Dagegen kann ich nicht beweisen, dass die Klassenzahl von $K$ zu $\ell$ prim ist oder, was schliesslich auf dasselbe hinausläuft, dass bereits in den unverzweigten Körpern vom Relativgrad $\ell$ in bezug auf $K$ sämtliche Ideale aus $k$ Hauptideale werden. Ich habe sehr viele vergebliche Versuche zum Beweise der genannten Tatsachen gemacht, sodass sich mir schliesslich die Vermutung aufgedrängt hat, dass sie am Ende gar nicht richtig sind.*

Hilbert schickte ihm darauf ein Manuskript, in welchem er diesen Satz im Falle $h = 4$ bewiesen zu haben glaubte. Am 13. Mai 1906 schickt Furtwängler das Manuskript an Hilbert zurück mit dem Kommentar

> *Gleichzeitig sende ich Ihnen mit herzlichem Dank einige handschriftliche Notizen zurüuck, die Sie mir früher freundlichst zugesandt hatten. Wenn sie mir auch nicht von direktem Nutzen gewesen sind, so bin ich Ihnen doch für die Übersendung dankbar, da ich dadurch veranlasst bin, die fragliche Untersuchung definitiv zu erledigen. Es hat sich dabei herausgestellt, dass die von Ihnen über die unverzweigten relativ Abel'schen Körper vom Relativgrad 4 aufgestellten Sätze unrichtig sind.*

Furtwängler gibt den Körper $\mathbb{Q}(\sqrt{-195}\,)$ als Gegenbeispiel an, der Klassengruppe vom Typ $(2, 2)$ besitzt, und dessen Hilbertklassenkörper $\mathbb{Q}(\sqrt{-3}, \sqrt{5}, \sqrt{13}\,)$ eine gerade Klassenzahl hat. Weiter schreibt er:

> *Wo die Lücke in Ihrem Beweise liegt, habe ich aus Ihren Notizen nicht festzustellen versucht, da dieselben schwer zu entziffern sind und ich keine Zeit verlieren wollte, zumal da durch das Beispiel die Sachlage geklärt war.*

Furtwängler hat diese Beispiele in [27] genauer untersucht und später die Frage gestellt, ob Klassenkörpertürme immer abbrechen; dass das nicht immer der Fall ist, haben dann Golod und Schafarewitsch gezeigt (siehe [79] für eine meisterhafte Darstellung dieses Resultats).

Abgesehen von den zur Umschiffung dieser Klippe notwendigen Schritten gehen die meisten Beweisideen in den Arbeiten von Furtwängler und auch Takagi auf Hilbert und Weber zurück. Hasse hat dann die Argumente, die auf der Basisdarstellung von Gruppen beruhten, durch strukturelle Beweise ersetzt, und zwar zur gleichen Zeit, als in der Physik der Begriff der „Gruppenpest“ die Runde machte. Die nächsten großen Schritte tat Artin mit seinem Reziprozitätsgesetz, was den Beweis des Hauptidealsatzes durch Furtwängler ermöglichte, Herbrand mit seinen Techniken zur Indexberechnung, und Chevalley mit der Einführung der Idele. Diese erlaubten nicht nur, das Lokal-Global-Prinzip von Grund auf in der Theorie zu verankern, sondern sie ermöglichten es auch, die von Brauer, Hasse und Emmy Noether geschaffene Theorie der Algebren durch kohomologische Techniken zu ersetzen. Auf dieser Basis konnten Weil und Shafarevich dann die klassische Theorie mit ihrem Satz über die Fundamentalklasse abrunden.

Die Entwicklung danach konzentrierte sich auf die Realisierung von Teilen des Langlands-Programms, dem die Klassenkörpertheorie als der eindimensionale abelsche Spezialfall untergeordnet ist. Man darf wohl sagen, dass das Bindeglied zwischen Hilberts *Zahlbericht* und Langlands Ideen die zentrale Rolle ist, welche die Galoisgruppen der algebraischen Erweiterungen von $\mathbb{Q}$ und der Komplettierungen $\mathbb{Q}_p$ in der algebraischen Zahlentheorie spielen.

Die Rolle des *Zahlberichts* bei der Ersteigung dieser Gipfel hat Felix Hausdorff in einem Brief zu Hilberts 70. Geburtstag (siehe etwa [45]) so beschrieben:

> *Meine Lieblingsspeise unter all den Delikatessen, mit denen Sie uns bewirtet haben, ist der Zahlbericht. Das ist die glücklichste Mischung von Vergangenheit, Gegenwart und Zukunft (den drei Dimensionen der Zeit, nach Hegel): vollendete Beherrschung und Darstellung des bereits Geleisteten, Lösung neuer Probleme, und feinstes Vorgefühl für die kommenden Dinge – ich denke z.B. an Ihren Begriff des Klassenkörpers. Nun ja, inzwischen ist Einiges hinzugekommen; nicht jeder Gipfel ist von Ihnen selbst erreicht worden, aber kein Gipfel wäre ohne Sie erreicht worden!*

*Danksagung.* Herrn Thomas Bartsch möchte ich für die Einladung danken, diesen Artikel zu schreiben, obwohl es mit [72, 82] bereits zwei Würdigungen des *Zahlberichts* gibt. Weiter bin ich ihm und einem Gutachter, sowie vor allem Norbert Schappacher für viele hilfreiche Hinweise zu großem Dank verpflichtet.

## Literatur

[1] E. Artin, *Die Bedeutung Hilberts für die moderne Mathematik*, Vortrag anlässlich Hilberts 100. Geburtstag 1962; in *Colllected Papers* (S. Lang. J. Tate, Hrsg.), 547–551
[2] P. Bachmann, *Ueber Galois' Theorie der algebraischen Gleichungen*, Math. Ann. **18** (1881), 449–468
[3] P. Bachmann, *Elemente der Zahlentheorie*, Leipzig 1892
[4] P. Bachmann, *Zahlentheorie, II. Teil. Die analytische Zahlentheorie*, Leipzig 1894
[5] P. Bachmann, *Zahlentheorie, III. Teil. Die Lehre von der Kreisteilung*,
[6] P. Bachmann, *Zahlentheorie, IV. Teil. Die Arithmetik der quadratischen Formen*, Leipzig 1898
[7] P. Bachmann, *Niedere Zahlentheorie*, Leipzig 1902
[8] P. Bachmann, *Zahlentheorie, V. Teil: Allgemeine Arithmetik der Zahlenkörper*, Leipzig 1905
[9] O. Baumgart, *Ueber das quadratische Reciprocitätsgesetz. Eine vergleichende Darstellung der Beweise*, Diss. Göttingen 1885; Zeitschrift Math. Phys. 30 (1885), 169–236, 241–277; engl. Übersetzung *The Quadratic Reciprocity Law. A Collection of Classical Proofs* (F. Lemmermeyer, Hrsg.), Birkhäuser Basel 2015
[10] O. Blumenthal, *Lebensgeschichte*, in [43, Bd. 3, S. 388–429]
[11] R. Bölling, *Jacobi als Wegbereiter für Kummers Idee der idealen Zahlen*, Mitt. DMV **16** (2008), 274–281
[12] J. Coates, R. Sujatha, *Cyclotomic fields and zeta values*, Springer-Verlag 2006
[13] P. Colmez, J.-P. Serre (Hrsg.), *Correspondance Serre-Tate*, I, II, Soc. Math. France 2015
[14] R. Dedekind, *Vorlesungen über Zahlentheorie von P. Lejeune-Dirichlet*, 3. Auflage Braunschweig 1879
[15] R. Dedekind, *Über die Begründung der Idealtheorie*, Gött. Nachr. (1895), 106–113; Werke II, 50–58
[16] R. Dedekind, *Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern*, J. Reine Angew. Math. **121** (1900), 40–123; Gesammelte Mathematische Werke vol. 2, 148–233
[17] L.E. Dickson, *History of the Theory of Numbers*, vol I (1920); vol II (1920); vol III (1923); Chelsea reprint 1952

[18] P. G. L. Dirichlet, *Recherches sur les formes quadratiques à coefficients et à indéterminées complexes*, J. Reine Angew. Math. **24** (1842), 291–371; Werke I, 533–618

[19] H. Edwards, *The background of Kummer's proof of Fermat's Last Theorem for regular primes*, Arch. Hist. Exact Sci. **14** (1975), 219–236

[20] H. Edwards, *About the cover: Kummer's tables*, Bull. Amer. Math. Soc. **44** (2007), 133–135

[21] G. Eisenstein, *Allgemeine Untersuchungen über die Formen dritten Grades mit drei Variabeln, welche der Kreistheilung ihre Entstehung verdanken*, J. Reine Angew. Math. **28** (1844), 289–374 Math. Werke I, 167–286

[22] L. Euler, *Tractatus de numerorum doctrina capita sedecim, quae supersunt*, Commentationes arithmeticae **2** (1849), 503–575; Opera Omnia, **I 5**, 182–283

[23] G. Frei (Hrsg.), *Der Briefwechsel David Hilbert – Felix Klein (1886 – 1918)*, Göttingen 1985

[24] G. Frei, F. Lemmermeyer, P. Roquette, *Emil Artin and Helmut Hasse. The Correspondence 1923–1958* Springer-Verlag 2014

[25] A. Fröhlich, M. J. Taylor, *Algebraic Number Theory*, Cambridge Univ. Press 1993

[26] R. Fueter, *Der Klassenkörper der quadratischen Körper und die komplexe Multiplikation*, Diss. Göttingen 1903

[27] Ph. Furtwängler, *Über das Verhalten der Ideale des Grundkörpers im Klassenkörper*, Monatsh. f. Math. **27** (1916), 1–15

[28] C.F. Gauss, *Disquisitiones Arithmeticae*, Braunschweig 1801; French transl. 1807

[29] C.F. Gauss, *Theoria residuorum biquadraticorum, Commentatio secunda*, Comment. Soc. regiae sci. Göttingen **7** (1832), 93–148; Werke II, 93–148

[30] C. Goldstein, N. Schappacher, *A book in search of a discipline (1801–1860)*, in *he shaping of arithmetic after C.F. Gauss's Disquisitiones Arithmeticae* (C. Goldstein, N. Schappacher, J. Schwermer (Hrsg.), Springer-Verlag (2007), 3–61

[31] C. Goldstein, N. Schappacher, *Several disciplines and a book (1860–1901)*, in *he shaping of arithmetic after C.F. Gauss's Disquisitiones Arithmeticae* (C. Goldstein, N. Schappacher, J. Schwermer (Hrsg.), Springer-Verlag (2007), 67–103

[32] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag 1952; Springer-Verlag 1985

[33] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig 1923

[34] E. Hecke, *Analysis und Zahlentheorie*, Vorlesung Hamburg 1920, P. Roquette (Hrsg.), Vieweg 1987

[35] J. Herbrand, *Sur les classes des corps circulaires*, J. Math. Pures Appl. (9) **11** (1932), 417–441

[36] D. Hilbert, *Über die Zerlegung der Ideale eines Zahlkörpers in Primideale*, Math. Ann. **44** (1894), 1–8

[37] D. Hilbert, *Grundzüge einer Theorie des Galoisschen Zahlkörpers*, Gött. Nachr. (1894), 224–236; Gesammelte Abhandlungen I, 13–23

[38] D. Hilbert, *Über den Dirichletschen biquadratischen Zahlkörper*, Math. Ann. **45** (1894), 309–340; Gesammelte Abhandlungen I, 24–52

[39] D. Hilbert, *Die Theorie der algebraischen Zahlkörper*, Jahresber. Deutsche Math. Ver. **4** (1897), 175–546

[40] D. Hilbert, *Théorie des corps de nombres algébriques*, übersetzt von A. Lévy, mit Kommentaren durch G. Humbert und Th. Got, Annales Fac. Sci. Univ. Toulouse (3) **1** (1909), 257–328; **2** (1910), 225–456; **3** (1911), 1–62

[41] D. Hilbert, *Teoria corpurilor de numere algebrice*, rumänische Übersetzung durch Marcel Tena, Bukarest 1998

[42] D. Hilbert, *Zahlentheorie*, Vorlesungen Wintersemester 1897/98; Göttingen 1990

[43] D. Hilbert, *Gesammelte Abhandlungen*, Springer-Verlag 1932, 1933, 1935

[44] D. Hilbert, *Über das Unendliche*, Math. Ann. **95** (1925), 161–190

[45] F. Hirzebruch, *Der Mathematiker David Hilbert*, in *Reden und Gedenkworte*, Orden Pour Le Mérite **37**, 2008–2009, 237–251

[46] C. R. Hobby, *The derived series of a p-group*, Diss. Caltech 1960

[47] A. Hurwitz, *Über die Theorie der Ideale*, Gött. Nachr. (1894), 291–298

[48] A. Hurwitz, *Zur Theorie der algebraischen Zahlen*, Gött. Nachr. (1895), 324–331

[49] A. Hurwitz, *Der Euklidische Divisionssatz in einem endlichen algebraischen Zahlkörper*, Math. Z. **3** (1919), 123–126

[50] C.G.J. Jacobi, *Vorlesungen über Zahlentheorie*, F. Lemmermeyer, H. Pieper (Hrsg.), Erwin Rauner-Verlag 2007

[51] K. Ireland, M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag 1990
[52] W. Jehne, *On knots in algebraic number theory*, J. Reine Angew. Math. **311/312** (1979), 215–254
[53] L. Kronecker, *De Unitatibus Complexis*, Diss. Universität Berlin 1845
[54] E. E. Kummer, *Collected Papers I. Contributions to Number Theory* (A. Weil, Hrsg.), Springer-Verlag 1975
[55] E. E. Kummer, *Zwei besondere Untersuchungen über die Classen-Anzahl und über die Einheiten der aus $\lambda$ten Wurzeln der Einheit gebildeten complexen Zahlen*, J. Reine Angew. Math. **40** (1850), 117–129
[56] E. E. Kummer, *Memoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers*, J. math. pures appl. **16** (1851), 377–498; Coll. Papers I, 363–484
[57] E. E. Kummer, *Allgemeine Reziprozitätsgesetze für beliebig hohe Potenzreste*, Berliner Akad. Ber. (1850), 154–165; Coll. Papers I, 345–357
[58] E. E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reziprozitätsgesetzen*, J. Reine Angew. Math. **44** (1852), 93–146; Coll. Papers I, 485–538
[59] E. E. Kummer, *Über eine besondere Art, aus complexen Einheiten gebildeter Ausdrücke*, J. Reine Angew. Math. **50** (1855), 212–232
[60] E. E. Kummer, *Über die allgemeinen Reziprozitätsgesetze der Potenzreste*, Berliner Akad. Ber. (1858), 158–171; Coll. Papers I, 673–687
[61] E. E. Kummer, *Über die allgemeinen Reziprozitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist*, Berliner Akad. Abh. (1859), 19–159; Coll. Papers I, 699–839
[62] E. E. Kummer, *Zahlentheorie*, Vorlesung im Wintersemester 1880/81 in Berlin, Mitschrift von Dr. P. Richert
[63] S. Lang, *Cyclotomic Fields, I, II*, Springer-Verlag 1978, 1980; combined edition 1990
[64] D. Laugwitz, *Bernhard Riemann, 1826–1866. Wendepunkte in der Auffassung der Mathematik*, Birkhäuser 1996
[65] A.-M. Legendre, *Recherches d'analyse indéterminée*, Hist. Acad. Sci. Paris 1785 (1788), 465–559
[66] A.-M. Legendre, *Essai sur la Théorie des Nombres*, Paris 1798
[67] F. Lemmermeyer, *Galois action on class groups*, J. Algebra **264** (2003), 553–564
[68] F. Lemmermeyer, *The development of the principal genus theorem*, in „The Shaping of Arithmetic“ (C. Goldstein, N. Schappacher, J. Schwermer, eds.), Springer Verlag 2007
[69] F. Lemmermeyer, *Jacobi and Kummer's ideal numbers*, Abh. Math. Sem. Hamburg **79** (2009), 165–187
[70] F. Lemmermeyer, *Zur Zahlentheorie der Griechen. II: Gaußsche Lemmas und Rieszsche Ringe*, Math. Semesterber. **56** (2009), 39–51
[71] F. Lemmermeyer, P. Roquette (Hrsg.), *Der Briefwechsel Hasse - Scholz - Taussky*, Universitätsverlag Göttingen 2016;
`http://univerlag.uni-goettingen.de/handle/3/isbn-978-3-86395-253-2`
[72] F. Lemmermeyer, N. Schappacher, *Introduction*, English translation of Hilbert's Zahlbericht by I. Adamson, Springer Verlag 1998
[73] H.W. Lenstra, *Euclidean number fields of large degree*, Invent. Math. **38** (1977), 237–254
[74] H.W. Lenstra, P. Stevenhagen, *Primes of degree one and algebraic cases of Čebotarev's theorem*, Enseign. Math. **37** (1991), 17–30
[75] A. Meyer, *Zur Theorie der zerlegbaren Formen, insbesondere der kubischen*, Vierteljahresschrift. Naturf. Ges. Zürich **42** (1897), 149–201
[76] E. Noether, *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern*, Math. Ann. **96** (1926), 26–61
[77] B. Petri, N. Schappacher, *On Arithmetization*, in *he shaping of arithmetic after C.F. Gauss's Disquisitiones Arithmeticae* (C. Goldstein, N. Schappacher, J. Schwermer (Hrsg.), Springer-Verlag (2007), 343–374
[78] L.W. Reid, *The elements of the theory of algebraic numbers*, New York 1910
[79] P. Roquette, *On class field towers*, in *Algebraic Number Theory* (J.W.S. Cassels, A. Fröhlich, Hrsg.), 1967, 231–249

[80] P. Roquette, *Briefwechsel Hasse - Hensel*, online verfügbar auf https://www.mathi.uni-heidelberg.de/~roquette/Transkriptionen/manutrans.html#hashen; aufgerufen am 20.04.2017
[81] G.-C. Rota, *Ten lessons I wish I had been taught*, Notices Amer. Math. Soc. **44** (1997), 22–25
[82] N. Schappacher, *David Hilbert, Report on algebraic number fields ('Zahlbericht') (1897)*, Landmark Writings in Western Mathematics, 1640–1940 (I. Grattan-Guinness, editor), 2005, 700–709
[83] F. K. Schmidt, *Algebraische Zahlentheorie I, II*, Vorlesungen Münster, WS 1949/50 und SS 1950
[84] A. Scholz, *Totale Normenreste, die keine Normen sind, als Erzeuger nicht-abelscher Körpererweiterungen. II*, J. Reine Angew. Math. **182** (1940), 217–234
[85] H.J.S. Smith, *Report on the theory of numbers*, 1859–1865; reprint Chelsea 1965
[86] J. Sommer, *Vorlesungen über Zahlentheorie. Einführung in die Theorie der algebraischen Zahlkörper*, Leipzig 1907
[87] E. Steinitz, *Algebraische Theorie der Körper*, J. Reine angew. Math. **137** (1910), 167–309
[88] O. Taussky, *Some non-commutativity methods in algebraic number theory*, in *A Century of Mathematics in America. Part II*, (P. Duren, ed.), 493–511
[89] O. Taussky-Todd, *Autobiography*, Mary Terrall (Hrsg.), Calif. Inst. Technology, Pasadena (1980); http://oralhistories.library.caltech.edu/43/1/OH_Todd.pdf
[90] L. C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag New York 1982; 2. Aufl. 1997
[91] L. C. Washington, *Stickelberger's theorem for cyclotomic fields, in the spirit of Kummer and Thaine*, Théorie des nombres (1989), 990–993
[92] A. Weil, *Une lettre et un extrait de lettre à Simone Weil*, Collected Papers I, 244–255
[93] A. Weil, *L'avenir des mathématiques*, in *Les Grands Courants de la Pensée Mathématique* (F. Le Lionnais, Hrsg.), Paris 1962, 307–320; Collected Papers I, 359–372
[94] J. Weinstein, *Reciprocity laws and Galois representations: recent breakthroughs*, Bull. Amer. Math. Soc. **53** (2016), 1–39
[95] H. Weyl, *David Hilbert and his mathematical work*, Bull. Amer. Math. Soc. **50** (1944), 612–654
[96] Wikipedia, *David Hilbert*, https://en.wikipedia.org/wiki/David_Hilbert; aufgerufen am 06.03.2017
[97] H. Zasssenhaus, *Zur Vorgeschichte des Zahlberichts*, in *Hermann Minkowski. Briefe an David Hilbert* (L. Rüdenberg, H. Zassenhaus, Hrsg.), Springer-Verlag 1973, 17–21

Mörikeweg 1, 73489 Jagstzell, Germany
*Email address*: hb3@ix.urz.uni-heidelberg.de