Hamburger Beiträge zur Mathematik

Nr. 928, Juli 2022

Zugänge zur Klassenkörpertheorie

von Ernst Kleinert

Zugänge zur Klassenkörpertheorie

Einleitung

Vor mehr als neunzig Jahren setzte Emil Artin mit seinem Reziprozitätsgesetz den Schlußstein in das Gebäude der Klassenkörpertheorie, das von seinen Vorgängern, namentlich Takagi, schon weit aufgeführt worden war. Die Arbeit daran endete natürlich nicht. Zunächst gab es noch ungelöste, sehr konkrete Probleme, wie die Frage nach expliziten Reziprozitätsgesetzen (heute gelöst) und expliziter Konstruktion der Klassenkörper (nicht gelöst), auch das Problem der Klassenkörpertürme (partiell gelöst). Sodann die Frage nach einem Lokal-Global-Prinzip für die Theorie, für das dann Chevalley mit seinem Idelbegriff die Grundlage schuf; gleichzeitig erfüllte er das methodische Desiderat, die Analysis zu vermeiden, also für die rein arithmetisch-algebraischen Aussagen der Theorie ebensolche Beweise zu finden. Wünschenswert erschien weiter, die recht komplexen rein gruppentheoretischen Überlegungen von den arithmetischen abzulösen und so den gesamten Aufbau durchsichtiger zu machen; das gelang zuerst mit der kohomologischen Fassung der Theorie. Und sehr früh schon stand im Hintergrund die größte und sicherlich schwierigste, bis heute nicht gelöste Aufgabe, nämlich einer Ausdehnung der Theorie auf beliebige (galoissche) Erweiterungen; von Takagi schon 1920 angesprochen (siehe [Mi], S.14).

Im Verfolg dieser Probleme entstand eine Reihe von Zugängen zur Theorie, die untereinander sehr verschieden sind, derart, daß sich, wie Shafarevich bemerkte, prima facie nicht leicht entscheiden ließe, ob sie sich überhaupt auf denselben Gegenstand beziehen (siehe [F], S.1). Ziel dieser Arbeit ist, die wichtigsten von ihnen in großen Zügen darzustellen, so daß man die Denkwege nachvollziehen kann und die benutzten Methoden vergleichbar werden. Im Groben wird die historische Entwicklung nachgezeichnet, aber mit der systematischen Absicht, zu einer Synopse aller Zugänge beizutragen, denn „das Wahre ist das Ganze“. Vollständige Beweise können natürlich hier nicht gegeben werden; ich habe mich aber bemüht, das jeweils Wesentliche hervorzuheben. Technische Details bleiben ganz außer acht. Wir beschränken uns auf Zahlkörper und die zentrale Aussage der Theorie, die man, in ihrer klassischen, idealtheoretischen Formulierung so aussprechen kann (die auftretenden Termini werden unten (1.2) definiert):

„Es besteht eine bijektive, inklusionsumkehrende Korrespondenz zwischen den (endlichen) abelschen Erweiterungen L/K eines Zahlkörpers K und den Idealgruppen von K. Ist dabei der Körper L der Gruppe **H** zugeordnet, und ist das Mitglied H von **H** mod **m** erklärt, so liefert die Artinabbildung einen kanonischen Isomorphismus $I^{\mathbf{m}}(K) / H \simeq \mathrm{Gal}(L/K)$.“

Der Isomorphismus heißt kanonisch, weil er, wie unten (1.3) dargestellt wird, in übersichtlicher Weise kompatibel ist mit den Beziehungen, die bei Körpertürmen N/L/K zwischen den Idealgruppen einerseits und den Galoisgruppen andererseits bestehen; es ist dieses „Wohlverhalten“, welches der Artinabbildung und ihren Abkömmlingen, den Normrestsymbolen, ihre überragende Stellung in der Theorie verleiht. Ersichtlich handelt es sich oben um zwei Aussagen, deren erste man den Existenzsatz nennt, während die zweite das Artinsche Reziprozitätsgesetz ist. Unter den Autoren herrscht keine Einigkeit darüber, welche man als *den* Hauptsatz der Theorie anzusehen hat. Von einem „philosophischen" Gesichtspunkt wird der Existenzsatz als die gewichtigere Aussage erscheinen: Klassifikation der Erweiterungen L/K durch konkrete Bestimmungsstücke von K selbst (die auch algorithmisch zugänglich sind, siehe [Co]), mit den Worten von Chevalley ([Ch1], S.394): „...ou, si l'on veut présenter les choses en termes dialectiques, comment un corps possède en soi les éléments de son propre dépassement." Andererseits erscheint das Reziprozitätsgesetz als die arithmetisch interessantere Aussage; auch hängt bei den meisten modernen Zugängen der Beweis des Existenzsatzes vom Reziprozitätsgesetz ab (natürlich nicht bei dem ursprünglichen von Takagi, der ja dieses Gesetz noch nicht hatte). Der Grund dafür ist, daß letzteres den Beweis des ersteren auf beherrschbare Fälle zu reduzieren gestattet; siehe unten 1.8.

Wir beginnen unseren Rundgang mit der idealtheoretischen Formulierung, die ihre erste vollständige Darstellung in Hasses „Zahlbericht" [H1] fand, einem Text, den man das „alte Testament" der Klassenkörpertheorie nennen darf (und dem man noch Hasses wenige Jahre später gehaltene Marburger Vorlesungen zur Seite stellen kann [H2]). Eine vorzüglich organisierte neuere Darstellung, in welche die in der Folge erreichten Vereinfachungen Eingang gefunden haben, ist das Buch [J] von Janusz, an dem wir uns orientieren. Lang [La] bietet bis zum Reziprozitätsgesetz ungefähr denselben Aufbau, bringt aber für den Existenzsatz die Idele ins Spiel, wodurch der Beweis etwas durchsichtiger wird.

Es folgen die ideltheoretische Formulierung des Hauptsatzes und die erste vollständige Durchführung der Theorie in dieser Sprache durch Chevalley [Ch1]. Während seine Einführung der Idele Schule gemacht hat und heute Standard ist, hat seine Version der zentralen Aussage anscheinend nicht viel Verbreitung gefunden, verdient aber doch in ihrer Kompaktheit und Eleganz in Erinnerung gerufen zu werden. Sein „théorème central" ist, soweit ich sehe, die erste Vorwegnahme des eindimensionalen Falles der (globalen) Langlandskorrespondenz, nämlich zwischen arithmetischen Objekten (n-dimensionalen Darstellungen der absoluten Galoisgruppe) und automorphen Objekten (Darstellungen der adelischen Gruppen GL(n)).

Der nächste Schritt der Entwicklung führt uns wieder zu einem „kanonisch" gewordenen Text, den man das „neue Testament" der Theorie nennen kann, die 1967 erschienene Ausarbeitung [AT] eines Seminars, welches Artin und Tate in den Jahren 1951/52 abgehalten haben. (Seither sind, wie wir sehen werden, noch weitere Evangelien erschienen, die zwar nicht apokryph sind, über deren kanonischen Status aber künftige Konzilien entscheiden müssen.) Hier wird zum ersten Mal, in dem Begriff der „Klassenformation", eine „abstrakte" Klassenkörpertheorie präsentiert, nämlich ein rein gruppentheoretischer Apparat, in dem Zahlen gar nicht vorkommen, der aber ein abstraktes Reziprozitätsgesetz und einen abstrakten Existenzsatz liefert. Den technischen Hintergrund bildet die Kohomologietheorie der Gruppen, darin besonders ein Satz von Tate, aus dem das Reziprozitätsgesetz unmittelbar folgt. Für die Anwendung in den „konkreten" Fällen, nämlich der lokalen und der globalen Klassenkörpertheorie, hat man dann die entsprechend spezifizierten Axiome des Apparats zu verifizieren. Dabei kehren natürlich bekannte Argumente wieder; es wird aber doch eine klare Trennung von rein gruppentheoretischen und arithmetischen Sachverhalten erreicht, insofern auch mehr Durchsichtigkeit. Auch erscheint hier zum ersten Mal (soweit ich sehe) die heute üblich gewordene Ableitung der globalen Theorie aus der lokalen. Diesen Weg gehen fast alle in der Folge entwickelten Zugänge – Definition des globalen Normrestsymbols als Produkt der lokalen bzw. der globalen Invariantenabbildung als Summe der lokalen; von diesem Weg versprach sich Hasse schon im „Zahlbericht“ eine technische wie konzeptuelle Vereinfachung ([H1], II, Fußnote zu S.37). In [AT] ist die globale Theorie ausgeführt, Kohomologie und lokale Theorie werden nur skizziert; ich folge der Version von Neukirch ([N1]), der allerdings (wie unten erklärt wird) einen in einigen Punkten abweichenden Aufbau bietet. Anschließend wird noch auf das Buch [Ch2] von Chevalley eingegangen und den Artikel [T] von Tate, der die Hauptsätze noch einmal darstellt, unter Benutzung von Kohomologie, aber ohne abstrakte Klassenformationen.

Einige Jahre später erschien Weils Buch [W], das in gewissem Sinne einen Kontrapunkt zu [AT] bildet (man lese die Einleitung). Auch Weil legt eine abstrakte Klassenkörpertheorie zugrunde, die aber nicht kohomologisch, sondern in der Sprache der topologischen Gruppen formuliert ist. Weiter bringt er die analytischen Methoden wieder zur Geltung, indem er deren Neubegründung in „Tate's Thesis“ auf einfache Algebren ausdehnt, sodann auch die Algebrentheorie; diese wird ja durch die kohomologische Methode auf die Gruppen $H^2(\mathrm{Gal}(L/K), L^\times)$ sozusagen eingedampft, so daß man von Algebren und der Brauergruppe gar nicht mehr sprechen muß.

Auch in den Büchern von Lorenz ([Lo1] mit der lokalen, [Lo2] mit der globalen Klassenkörpertheorie) wird der Algebrentheorie eine tragende Rolle zugewiesen, wie das von Hasse [H3] initiiert worden war. Lorenz benutzt auch Kohomologie, aber nur in den kleinen Dimensionen (von –1 bis 2), wo alles ad hoc definiert werden kann und man die allgemeine Theorie nicht braucht, insbesondere keine Klassenformationen und auch nicht den Satz von Tate. Der Satz von Hasse-Brauer-Noether wird aber nicht, wie bei Weil, analytisch bewiesen, sondern rein arithmetisch-algebraisch. Ich werde unten die Lorenzsche (zeitlich spätere) Darstellung der Weilschen voranstellen, weil die beiden viel gemeinsam haben, die erstere aber zugänglicher ist und mehr an [AT] und [T] anschließt.

Unser Rundgang endet mit der Theorie von Neukirch ([N2] und [N3]), die wieder einen abstrakten gruppentheoretischen Apparat zugrundelegt, eine schwache Version der Klassenformation, mit Kohomologie nur in den Dimensionen -1 und 0 und nur für zyklische Gruppen, dafür aber ausgestattet mit einer Faktorgruppe $\hat{\mathbb{Z}}$ von G (galoistheoretisch: eine $\hat{\mathbb{Z}}$ -Erweiterung des Grundkörpers) und einer abstrakten „Bewertung“ von A, wodurch die Theorie a limine wieder einen arithmetischen Charakter hat.

Damit ist eine Reihe von Zugängen zur Klassenkörpertheorie erfaßt, die als strukturell verschieden gelten können und in denen, soweit ich sehe, alle bisher entwickelten wesentlichen Ideen zum Beweis der zentralen Aussagen vertreten sind. Erwähnen möchte ich aber noch die Darstellungen von Kato u.A. [KKS] (ähnlich wie [W], aber ohne den abstrakten Formalismus, reich an Beispielen), den Enzyklopädieband von Koch [K2] (kohomologisch, kombiniert [S], [T] und [Ch2], sehr knappe Beweise), die (wie stets) sehr inhaltsreichen und engagiert geschriebenen Vorlesungen von Milne [Mi] und das neue Buch von Harari [Ha], welches die Theorie in den Rahmen der Galoiskohomologie stellt und auch die Dualitätssätze (Tate-Poitou) behandelt; der Zugang ist kohomologisch, durch Verwendung stärkerer Hilfsmittel (kohomologische Dimension der Galoisgruppen) ergeben sich einige Varianten.

Die vorliegende Arbeit richtet sich an Leser, die das Grundwissen über Zahlkörper und ihre Komplettierungen beherrschen, vielleicht schon auf irgendeinem Wege mit der Klassenkörpertheorie in Berührung gekommen sind, sei es auch nur durch einen Ausblick, wie ihn die Bücher [K1] und [M] geben, und eine Orientierung über die verschiedenen Zugänge suchen. Fortgeschrittene seien verwiesen auf die Arbeit [F] von Fesenko für einen Überblick in größerem Rahmen. Wesentlich nicht-arithmetische Theorien, die bei den verschiedenen Zugängen eingesetzt werden, sind die komplexe Funktionentheorie, die Kohomologietheorie der Gruppen und die Theorie der Algebren. Die beiden letzteren werde ich (ohne Beweise) referieren, die erste wird vorausgesetzt. Für das hier Benutzte ist aber nur die allererste Konsequenz aus dem Cauchyschen Integralsatz wesentlich, nämlich daß eine meromorphe Funktion an jeder Stelle eine Laurententwicklung hat, die es gestattet, mit Null- und Polstellenordnungen zu rechnen, dazu elementare Tatsachen über Dirichletsche Reihen, wie sie etwa in [J], S.113ff oder [La], Ch.VIII entwickelt werden. Zwei Ausnahmen müssen konstatiert werden: die von Weil benutzten analytischen Methoden sind diejenigen aus Tate's Thesis und können im Rahmen dieser Arbeit nicht adäquat dargestellt werden, und dasselbe gilt für die Theorie von Lubin-Tate, die seit ihrem Entstehen (1965) in der lokalen Klassenkörpertheorie zu Prominenz gekommen ist und die wir nur sehr grob skizzieren können (4.3.2).

Die Bücher [AT], [Lo2] und [W] behandeln auch die Klassenkörpertheorie der Funktionenkörper (der zweiten Klasse „globaler“ Körper neben den Zahlkörpern), die an einigen Stellen spezielle Überlegungen erfordert, hier aber außer acht bleibt.

1 Die idealtheoretische Formulierung

1.1 Das primordiale Beispiel und den sozusagen naturgegebenen Einstieg in die Theorie bieten die Kreiskörper. Sei m eine natürliche Zahl, ζ eine primitive m-te Einheitswurzel und $K = \mathbb{Q}(\zeta)$ der m-te Kreisteilungskörper über den rationalen Zahlen. Bekanntlich ist die Abbildung

$$\varphi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathrm{Gal}(K/\mathbb{Q}) \,,\; r \bmod m \to (\zeta \to \zeta^r)$$

ein Isomorphismus. Wir interessieren uns nun für die Primzerlegung einer rationalen Primzahl p mit $(p, m) = 1$, genauer des Primideals (p) im Ring $O_K = \mathbb{Z}[\zeta]$ der ganzen Zahlen von K; da (p) unverzweigt ist, benötigen wir nur den Restklassengrad. Für einen Primteiler P von (p) in O_K ist der Restklassengrad $f(P/(p))$ gleich dem Grad des Körpers über $\mathbb{Z}/p\mathbb{Z}$, der durch Adjunktion der m-ten Einheitswurzeln zu $\mathbb{Z}/p\mathbb{Z}$ entsteht. Da die multiplikative Gruppe eines endlichen Körpers k eine zyklische Gruppe der Ordnung $|k| - 1$ ist, ist dieser Grad die kleinste Zahl f, derart daß $m \mid p^f - 1$, mit andern Worten die Ordnung von $p \bmod m$. Die Galoisgruppe dieser endlichen Erweiterung hat als kanonischen Erzeuger den Frobeniusautomorphismus $x \to x^p$, und die Abbildung φ bildet, wenn man ihren Argumentbereich nicht als Restklassengruppe von Zahlen, sondern als verallgemeinerte Idealklassengruppe auffaßt (siehe den nächsten Abschnitt), das Primideal (p) auf den Automorphismus $\zeta \to \zeta^p$ ab, der wegen $\varphi(p)(x) \equiv x^p \bmod p$ in der (gemeinsamen) Zerlegungsgruppe der Primteiler P von (p) liegt und ersichtlich auf der Restkörpererweiterung den Frobeniusautomorphismus induziert. *Das ist die einzige Klasse von Zahlkörpern, für welche mit elementaren Mitteln die Artinabbildung angegeben und das Reziprozitätsgesetz bewiesen werden kann* (genau das haben wir soeben getan). Die quadratischen Zahlkörper erfordern für eine analoge Behandlung bereits das quadratische Reziprozitätsgesetz, das zwar elementar beweisbar ist, dessen „strukturelle“ Funktion aber erst im Rahmen der allgemeinen Klassenkörpertheorie durchsichtig wird. Wir gehen nun daran, die Ausdehnung dieses Sachverhalts auf beliebige abelsche Erweiterungen L/K von Zahlkörpern zu formulieren.

1.2 Zunächst führen wir den Argumentbereich der allgemeinen Artinabbildungen ein. Einen *Modulus* von K (bei Lang: *cycle*) nennen wir ein formales Potenzprodukt $\mathbf{m}$ von endlich vielen Stellen von K, wobei wir für die endlichen Stellen nur positive Exponenten zulassen, für die unendlichen nur die Exponenten 0 und 1. Offensichtlich kann man $\mathbf{m}$ in einen endlichen und einen unendlichen Bestandteil zerlegen, $\mathbf{m} = \mathbf{m}_f\, \mathbf{m}_\infty$; der endliche Teil entspricht einem ganzen Ideal von K. Mit $I^{\mathbf{m}}(K)$ bezeichnen wir die Gruppe der Ideale von K, die von den nicht in $\mathbf{m}$ enthaltenen Primidealen erzeugt wird (sie hängt also nur vom endlichen Teil von $\mathbf{m}$ ab, und nur von den tatsächlich vorkommenden p, nicht von ihren Exponenten). Für $a \in K^\times$ definieren wir die Kongruenz $a \equiv 1 \bmod \mathbf{m}$ durch die folgenden Bedingungen:

(i) ist p ein Primideal, das in $\mathbf{m}_f$ mit dem Exponenten r steckt, also $v_p(\mathbf{m}_f) = r$, so sei $v_p(a-1) \geq r$;

(ii) kommt die reelle Stelle v, die einer Einbettung $\sigma : K \to \mathbb{R}$ entspricht, in $\mathbf{m}$ vor, so sei $\sigma(a) > 0$;

(iii) für komplexe unendliche Stellen wird nichts gefordert.

(Man könnte also die letzteren weglassen, doch ist es bei Erweiterungen technisch bequem, sie mitzuführen). Die Bedingung (i) kann man auch so aussprechen: a ist ganz für p und $a \equiv 1 \bmod p^r$; der neue Kongruenzbegriff verfeinert also den gewöhnlichen, durch Restklassenbildung modulo Idealen definierten, durch Forderungen an den reellen Stellen. Die a mit $a \equiv 1 \bmod \mathbf{m}$ bilden eine Untergruppe von $K^\times$, den *Zahlstrahl* mod $\mathbf{m}$; die davon erzeugten Hauptideale den *Idealstrahl* mod $\mathbf{m}$, den wir mit $P^{\mathbf{m}}(K)$ bezeichnen, eine Untergruppe von $I^{\mathbf{m}}(K)$. Es ist nicht schwer zu zeigen, daß die Faktorgruppe $I^{\mathbf{m}}(K)/P^{\mathbf{m}}(K)$, die *Strahlklassengruppe,* endlich und ihre Ordnung durch die Klassenzahl h von K teilbar ist. Für $\mathbf{m} = 1$ ist $I^{\mathbf{m}}(K)/P^{\mathbf{m}}(K)$ die gewöhnliche

Idealklassengruppe. Für $K = \mathbb{Q}$, $\mathbf{m} = (m)\infty$, wird $I^{\mathbf{m}}(K)/P^{\mathbf{m}}(K) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}$; im primordialen Beispiel war es bei der Definition von φ wichtig, daß für die Primideale (p) die *positiven* Erzeuger, eben die Primzahlen genommen werden. Als *verallgemeinerte Idealklassengruppen* bezeichnet man alle $I^{\mathbf{m}}(K)/H$, wo $I^{\mathbf{m}}(K) \supset H \supset P^{\mathbf{m}}(K)$. Solche figurieren auf der linken Seite der Artinabbildungen und kommen so zustande: sei L/K eine endliche Erweiterung; wir fassen einen Modulus **m** von K als einen solchen von L auf, indem wir die in **m** vorkommenden Stellen durch ihre sämtlichen Fortsetzungen auf L ersetzen und die Exponenten beibehalten. Die Idealnorm N bildet dann $I^{\mathbf{m}}(L)$ in $I^{\mathbf{m}}(K)$ ab, und $H = N(I^{\mathbf{m}}(L))\, P^{\mathbf{m}}(K)$ ist von der fraglichen Art.

1.3 Als nächstes definieren wir die Artinabbildungen. Sei L/K galoissch mit der Gruppe G, P ein Primideal in O_L und $p = P \cap O_K$ das von ihm geteilte Primideal in O_K . Mit D(P) bezeichnen wir die Fixgruppe von P für der Operation von G auf der Menge der Primideale von O_L , die *Zerlegungsgruppe* von P. Es ist eine zentrale (und leicht zu beweisende) Lokal-Global-Beziehung, daß sich D(P) mit der Galoisgruppe der von den Komplettierungen L_P und K_p gebildeten Erweiterung lokaler Körper identifizieren läßt. Ist P (äquivalent: p) in L/K unverzweigt, so ist D(P) isomorph zur Galoisgruppe der Restkörpererweiterung $O_L/P \;/\; O_K/p$; diese ist zyklisch mit dem ausgezeichneten Erzeuger $x \to x^q$, wo $q = |O_K/p|$. Dessen Urbild in G heißt der *Frobeniusautomorphismus* von P in L/K und wird mit (P, L/K) bezeichnet; er ist also definiert durch die Kongruenz

$$(P, L/K)(x) \equiv x^q \bmod P, \quad x \in O_L .$$

Bekanntlich operiert nun G transitiv auf der Menge aller Primteiler von p in O_L ; ist also G abelsch, was im folgenden bis auf weiteres angenommen sei, fallen für festes p die Zerlegungsgruppen aller P|p zusammen, und wir können (p, L/K) = (P, L/K) definieren, wo P ein beliebiger Teiler ist. Diese Bildung setzt sich fort zu einem Homomorphismus der Gruppe, die von allen unverzweigten p erzeugt wird, in G ; etwas allgemeiner erhalten wir für jeden Modulus **m** , der alle Verzweigung enthält (die Erweiterung $\mathbb{C}/\mathbb{R}$ wird hier als verzweigt angesehen) einen Homomorphismus

$$\varphi_{L/K} : \; I^{\mathbf{m}}(K) \;\to\; G ,$$

die *Artinabbildung*. Man mache sich klar, daß die verzweigten p hier ausgeschlossen bleiben, weil die zugehörigen Frobeniuselemente nicht in D(p) liegen, sondern in der Faktorgruppe von D(p) nach der *Trägheitsgruppe* $T(p) = \{ \sigma \in G \mid \sigma(x) \equiv x \bmod P,\; x \in O_L\}$. Unmittelbar aus den Definitionen folgt, daß die Ordnung von (p, L/K) in G gleich dem Grad f(P/p) der Restkörpererweiterung ist; *Kenntnis der Artinabbildung impliziert also (im wesentlichen) Kenntnis des Zerlegungsgesetzes für die Erweiterung* L/K. Insbesondere bedeutet (p, L/K) = 1 , daß p in L voll zerfällt.

Das oben erwähnte Wohlverhalten der Artinabbildung manifestiert sich in verschiedenen

Weisen. Am wichtigsten ist ein „Verschiebungssatz": seien L'/K' und L/K abelsche Erweiterungen mit $L \subset L'$, $K \subset K'$. Dann ist das Diagramm

$$\text{(1)} \qquad \begin{array}{ccc} I^{\mathbf{m}}(K') & \longrightarrow & \mathrm{Gal}(L'/K') \\ N \downarrow & & \downarrow \text{res} \\ I^{\mathbf{m}}(K) & \longrightarrow & \mathrm{Gal}(L/K) \end{array}$$

kommutativ; hier bedeutet N die Idealnorm und res die Einschränkung auf L. Im Spezialfall $K = K'$ wird $N = \mathrm{id}$; die Gleichung $\varphi_{L/K} = \varphi_{L'/K} \mid L$, aber mit dem Normrestsymbol anstelle der Artinabbildung, wird später wichtig für die Definition eines *universellen* Symbols (2.3). Im Spezialfall $L = L'$ wird res eine Inklusion. Für den (elementaren) Beweis der Verschiebungsformel siehe etwa [T], S.166. Sie spielt eine wichtige Rolle und figuriert in dem Aufbau von Weil sogar als Axiom V seiner abstrakten Theorie ([W], S.219). In dem zweiten Spezialfall hat man auch ein kommutatives Diagramm mit umgekehrten senkrechten Pfeilen, nämlich

$$\text{(1a)} \qquad \begin{array}{ccc} I^{\mathbf{m}}(K') & \longrightarrow & \mathrm{Gal}(L/K') \\ \text{incl} \uparrow & & \uparrow [K':K] \\ I^{\mathbf{m}}(K) & \longrightarrow & \mathrm{Gal}(L/K) \end{array} ;$$

hier bedeutet incl die Abbildung $I \to IO_{K'}$ und der rechte Pfeil die Potenzierung mit dem Körpergrad; zum Beweis beachte man, daß alle r Primteiler eines p aus K in K' denselben Restklassengrad f haben und $rf = [K' : K]$ ist (die Potenzierung ist übrigens ein Spezialfall der gruppentheoretischen Verlagerung). Schließlich manifestiert sich das Wohlverhalten von $\varphi_{L/K}$ in einer Kompatibilität mit beliebigen Isomorphismen $L/K \to s(L)/s(K)$; das ist intuitiv klar, weil ein solcher Isomorphismus ja auch die hier involvierten arithmetischen Sachverhalte mittransportiert, und wir brauchen das nicht auszuschreiben.

1.4 Es stellt sich nun die Frage nach Bild und Kern der Artinabbildung. Einen "trivialen" Teil des Kerns erkennen wir sofort : die Idealnorm N bildet P auf $p^{f(P/p)}$ ab , und $f(P/p)$ ist die Ordnung von $\varphi_{L/K}(p)$, also liegt $N(I^{\mathbf{m}}(L))$ im Kern. Aber diese Gruppe hat unendlichen Index in $I^{\mathbf{m}}(K)$ (das ist nicht trivial, s.u. 1.5), also muß der Kern größer sein. Wir können jetzt formulieren:

Reziprozitätsgesetz von Artin: *ist* $\mathbf{m}$ *groß genug, so ist* $P^{\mathbf{m}}(K) \subset \ker \varphi_{L/K}$, *und* $\varphi_{L/K}$ *induziert einen Isomorphismus*

$$H^{\mathbf{m}}(L/K) := \quad I^{\mathbf{m}}(K) / P^{\mathbf{m}}(K)\, N(I^{\mathbf{m}}(L)) \quad \to \quad \mathrm{Gal}(L/K)\,.$$

Ein paar Bemerkungen sind angebracht. (1) Was „groß genug“ bedeuten soll, zeigt sich im Verlauf der Beweise, und wir werden es unten nachtragen (1.8); klar ist schon, daß $\mathbf{m}$ alle (endliche) Verzweigung enthalten muß, weil andernfalls $\varphi_{L/K}$ gar nicht definiert ist. Für „groß genug“ sagen wir auch „zulässig“. Aus der Formulierung geht hervor, daß jedes Vielfache eines zulässigen $\mathbf{m}$ ebenfalls zulässig ist; warum das so ist, wird unten klar werden.

(2) Die Inklusion $P^{\mathbf{m}}(K) \subset \mathrm{kern}\ \varphi_{L/K}$ ist ein erstaunliches Faktum und, wie Lang ([La] S.199) mit Recht bemerkt, die crux des klassischen Zugangs; Janusz *definiert* durch sie geradezu das Bestehen des Reziprozitätsgesetzes (S.158). Sie impliziert eine Art Periodizität der Primzerlegung, die a limine geradezu unwahrscheinlich anmutet (gibt es nicht wenigstens ein heuristisches Argument dafür?) und jedenfalls durch die Definition von $\varphi_{L/K}$ in keiner Weise nahegelegt wird; diese ist ja „lokal“ in dem Sinne, daß jede Primstelle für sich und ohne Bezug zu andern genommen wird. Beim primordialen Beispiel, aber nur dort, liegt der Sachverhalt am Tage; der allgemeine Beweis ist indirekt, geschieht letztlich durch Vergleich von Gruppenindices und kann, wie Tate feststellt, „fairly be described as showing that the law holds because it could not be otherwise“ ([T], S.168). Zustimmung also eher durch logischen Zwang als durch Einsicht; Schopenhauer nannte das einen „Mausefallenbeweis“.

(3) Da $\varphi_{L/K}$ ein Isomorphismus ist, kann das Zerlegungsgesetz bereits in der Idealgruppe abgelesen werden: der Restklassengrad eines unverzweigten p ist die Ordnung der Klasse von p in $H^{\mathbf{m}}(L/K)$. Es verdient bemerkt zu werden, daß die Idealgruppen auch für die verzweigten p ein Zerlegungsgesetz hergeben, obwohl $\varphi_{L/K}$ für sie nicht definiert ist, siehe [H2], S.137.

(4) Man fragt sich nach dem Grund für die Benennung „Reziprozitätsgesetz“, denn von einer „echten“ Reziprozität, wie man sie von der Formel $(p/q) = (q^*/p)$ für das Legendresymbol kennt, ist hier nichts zu sehen. Artin wählte den Ausdruck, weil sich aus seinem Gesetz alle Reziprozitätsgesetze auch der höheren Potenzreste auf vergleichsweise einfache (wenn auch keineswegs triviale) Weise ableiten lassen; man findet das in [N3] und [Lo2] oder (für Mutige) als Übungsaufgabe in [CF], S.348ff.

Wir skizzieren jetzt die klassische Strategie zum Beweis des Gesetzes; sie läßt sich in die folgenden Schritte gliedern.

(A) Mittels Zeta- und L-Funktionen beweist man die Surjektivität von $\varphi_{L/K}$ sowie die „universelle Normrestungleichung“ $h^{\mathbf{m}}(L/K) \leq [L:K]$ (wir nennen sie „Ungleichung A“); hier bezeichnet $h^{\mathbf{m}}(L/K)$ die Ordnung von $H^{\mathbf{m}}(L/K)$. Diese Beweise sind (die analytischen Mittel vorausgesetzt) erstaunlich einfach; die Ungleichung gilt sogar ohne Bedingung an $\mathbf{m}$ und für galoissche L/K ([J], S.137).

(B) Es sei L/K zyklisch und **m** groß genug. Normindexberechnungen (wesentlich lokaler Natur) führen zum Beweis von „Ungleichung B“: $[L : K]$ teilt $h^{\mathbf{m}}(L/K)$. Dies ist der am meisten gruppentheoretische und am wenigsten durchsichtige Teil der gesamten Beweisführung. Als „Nebenprodukt“ fällt der Hassesche Normensatz ab.

(C) Unter den Voraussetzungen von (B) gilt jetzt mit (A) die Gleichheit $[L : K] = h^{\mathbf{m}}(L/K)$. Das genügt noch nicht zum Beweis des Reziprozitätsgesetzes, denn man weiß noch nicht, daß es überhaupt einen Modulus **n** mit $P^{\mathbf{n}}(K) \subset \ker \varphi_{L/K}$ gibt. Gibt es aber einen, kann er so groß gewählt werden, daß er alle Verzweigung enthält, denn wenn man **m** vergrößert, verkleinert man $P^{\mathbf{m}}(L/K)$. Das Gesetz folgt dann sofort aus Ungleichung A und der Surjektivität von $\varphi_{L/K}$ ([J], S.158). Die Existenz ergibt sich mittels einer ingeniösen Hilfskonstruktion von Artin („Artinsches Lemma“).

(D) Die Ausdehnung auf den allgemeinen abelschen Fall folgt ohne Mühe ([J] p.164) aus einem weiteren Wohlverhalten der Artinabbildung: sind L_1 und L_2 abelsche Erweiterungen von K und $L = L_1L_2$, kann man Gal(L/K) mit einer Untergruppe von $\mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$ identifizieren, und dabei gilt für unverzweigte p die Gleichung $(p, L/K) = ((p, L_1/K), (p, L_2/K))$. Ist also **m** (**n**) groß genug für L_1/K (L_2/K) , dann ist **mn** groß genug für $L_1 L_2/K$. Damit reduziert man mühelos auf den zyklischen Fall.

Wir beschreiben jetzt die Schritte (A) – (C) etwas näher.

1.5 Ad (A). Die Dedekindsche Zetafunktion von K ist definiert durch

$$\zeta_K(s) = \sum_I \| I \|^{-s} = \sum_n a(n)\, n^{-s} \quad ;$$

hierin bedeutet $\|I\|$ die Absolutnorm des ganzen Ideals I und a(n) die Anzahl der I mit $\|I\| = n$. Durch Vergleich mit der Riemannschen Zetafunktion erkennt man leicht, daß $\zeta_K(s)$ für $\mathrm{Re}\, s > 1$ konvergiert und in dieser Halbebene holomorph ist. Für das Verhalten bei $s = 1$ benötigt man eine Aussage über die Größe

$$A(n) = a(1) + \ldots + a(n) = \text{Anzahl der I mit } \|I\| \leq n.$$

Hierfür gilt

$$A(n) = \kappa(K)\, n + O(n^{1-1/[L:K]})$$

mit einer Konstanten $\kappa(K) > 0$, in welche alle fundamentalen numerischen Invarianten von K eingehen, die uns aber hier nicht weiter interessieren muß. Der Beweis ist langwierig; am durchsichtigsten ist fraglos die Darstellung in Tate's Thesis, wo die Konstante als Volumen eines Fundamentalbereichs für die Operation von $K^{\times}$ auf der Idelgruppe erwiesen wird; siehe [CF], S.337. Aus der elementaren Theorie der

Dirichletschen Reihen erhält man jetzt, daß $\zeta_K(s)$ sich zu einer meromorphen Funktion in einer Umgebung von 1 fortsetzen läßt, mit einem Pol erster Ordnung bei $s = 1$ und dem Residuum $\kappa(K)$.

Hier ist von Erweiterungen keine Rede, aber es ergibt sich sogleich die folgende Anwendung: angenommen, in der Erweiterung L/K seien fast alle p voll zerlegt. Dann unterscheidet sich $\zeta_L(s)$ von $\zeta_K(s)^{[L:K]}$ nur um endlich viele Eulerfaktoren, welche die Ordnung bei $s = 1$ nicht beeinflussen. Da aber beide Zetafunktionen dort einen Pol erster Ordnung haben, folgt $[L : K] = 1$, $L = K$. Diese Aussage (manchmal „Zerfällungssatz" genannt) kann man auch rein arithmetisch beweisen, aber das macht Mühe; siehe etwa [N1], S.220. Beispiel: wenn eine ganze Zahl ein Quadratrest modulo fast aller Primzahlen ist, dann ist sie ein Quadrat. Es folgt auch die oben gemachte Bemerkung, daß der Index $[I^{\mathbf{m}}(K) : N(I^{\mathbf{m}}(L))]$ für echte Erweiterungen stets unendlich ist.

Damit erhalten wir nun leicht die Surjektivität der Artinabbildung $\varphi_{L/K} : I^{\mathbf{m}}(K) \to \mathrm{Gal}(L/K)$, L/K abelsch. Sei nämlich H das Bild und E der Fixkörper von H. Dann ist für unverzweigte p

$$(p, E/K) \; = \; (p, L/K) \mid E \; = \; 1 \, .$$

Das bedeutet aber, daß fast alle p in E voll zerlegt sind, nach dem Vorigen also $E = K$ und damit $H = G$.

Zum Beweis der Ungleichung A ziehen wir die L-Funktionen zu den Charakteren χ von $H^{\mathbf{m}}(L/K) = I^{\mathbf{m}}(K) / H$, mit $H = P^{\mathbf{m}}(K)\, N(I^{\mathbf{m}}(L))$ heran,

$$L(s, \chi) \; = \; \sum \chi(I) \, \| I \|^{-s} \; ,$$

mit Summation über die $I \in I^{\mathbf{m}}(K)$. Es werden nun Argumente benutzt, die vom (funktionentheoretischen) Beweis des Dirichletschen Primzahlsatzes geläufig sind. Zunächst zeigt man, daß $L(s, \chi)$ für $\chi \neq 1$ bei $s = 1$ holomorph ist; für $\chi = 1$ unterscheidet sich $L(s, \chi)$ von $\zeta_K(s)$ um endlich viele Eulerfaktoren. Bezeichnet $m(\chi)$ die Ordnung von $L(s, \chi)$ bei $s = 1$, hat man

$$L(s, \chi) \; = \; (s-1)^{\, m(\chi)} \, g(s, \chi)$$

mit einer Funktion g, die bei $s = 1$ einen endlichen Wert $\neq 0$ annimmt, und damit

$$\log L(s, \chi) \; \sim \; m(\chi) \log (s-1) \; = \; -\, m(\chi) \log (1/(s-1)) \, ,$$

was bedeuten soll, daß sich beide Seiten in einer Umgebung von 1 nur um eine beschränkt bleibende Funktion unterscheiden. Ferner hat man

$$\log\ L(s,\ \chi)\ \sim\ \sum \chi(K)\ \sum \|\mathfrak{p}\|^{-s},$$

wobei die äußere Summe über die Klassen K von $I^{\mathbf{m}}(K) / H$, die innere über die $\mathfrak{p} \in K$ zu bilden ist (die Summe der weggelassenen Summanden bleibt beschränkt). Jetzt summiere man über die χ und beachte außer den Orthogonalitätsrelationen der Charaktere, daß (1) alle in L voll zerfallenden $\mathfrak{p}$ in H liegen, (2) über jedem solchen $\mathfrak{p}$ genau $N := [L : K]$ Ideale $\mathfrak{P}$ von L liegen, (3) unter diesen alle $\mathfrak{P}$ vom Absolutgrad 1 enthalten sind und (4) diese allein aber schon den Pol von $\zeta_L(s)$ erzeugen. Das liefert in ein paar Schritten ([L], p. 165) für reelle $s > 1$ die Ungleichung

$$(1 - \sum m(\chi))\ \log(1/(s-1))\ \geq\ |H|/N\ \log(1/(s-1))\ +\ g(s),$$

mit einem bei 1 beschränkt bleibenden g, wobei links über die $\chi \neq 1$ summiert wird. Läßt man nun s reell gegen 1 gehen, sieht man zunächst, daß alle $m(\chi) = 0$ sind, sodann die angestrebte Ungleichung $|H| \leq N$. Das Nichtverschwinden der L-Reihen bei $s = 1$ wird in diesem eleganten (von Weber stammenden) Argument also mitbewiesen! Hervorzuheben ist aber: das Argument benutzt die Tatsache, daß H durch die Idealnormen einer galoisschen Erweiterung L/K definiert ist; das Nichtverschwinden *aller* L-Reihen für Charaktere der Strahlklassengruppe $I^{\mathbf{m}}(K)/P^{\mathbf{m}}(K)$ folgt daraus, daß *alle* Gruppen H mit $I^{\mathbf{m}}(K) \supset H \supset P^{\mathbf{m}}(K)$, insbesondere $H = P^{\mathbf{m}}(K)$ so gegeben werden können; das aber folgt erst aus dem Existenzsatz (siehe auch [J], p.182) .

1.6 Ad (B). Jetzt sei L/K zyklisch, G = Gal(L/K). Als „Wunderwaffe“ bei den Indexberechnungen hat sich der *Herbrandquotient* bewährt (Lang spricht von „Q-machine“): sei G eine endliche zyklische Gruppe, s ein Erzeuger und A ein G-Modul, den wir additiv schreiben. Wir definieren die Endomorphismen $N\colon a \to \sum_i s^i a$ und $D\colon\ a \to a - sa$, bemerken, daß $\mathrm{im}\, N \subseteq \mathrm{kern}\, D = A^G$ und $\mathrm{im}\, D \subseteq \mathrm{kern}\, N$ ist (diese Untermoduln sind unabhängig von der Wahl von s) und setzen $H^0(A) = \mathrm{kern}\, D/\mathrm{im}\, N$ und $H^{-1}(A) = \mathrm{kern}\, N/\mathrm{im}\, D$ (das sind Tatesche Kohomologiegruppen avant la lettre, aber von Kohomologie braucht man hier noch nicht zu reden). Man beachte, daß $H^0(A)$ eine besondere Affinität zu unseren Problemstellungen hat, denn für G = Gal(L/K) und $A = L^\times$ ist $H^0(A) = K^\times / N(L^\times)$ die Normrestgruppe, und analog für die Idealgruppen. Der *Herbrandquotient* wird nun in [J] definiert als

$$q(A) = |H^{-1}(A)| / |H^0(A)|\ ,\ \text{falls die beiden Ordnungen endlich sind.}$$

Seine meistgebrauchten Eigenschaften sind:

(i) Ist $0 \to A \to B \to C \to 0$ eine exakte Sequenz von G-Moduln, so ist mit je zweien der Quotienten auch der dritte definiert, und es gilt $q(B) = q(A)q(C)$.

(ii) Für endliches A ist $q(A) = 1$.

Insbesondere ist also $q(A) = q(B)$, wenn $A \subseteq B$ mit endlichem Index und $q(A)$ definiert ist (allgemeiner: wenn A und B kommensurable Untermoduln von C sind). Für $A = \mathbb{Z}$ mit trivialer Operation erhält man $q(\mathbb{Z}) = 1 / |G|$.

Es sollte bemerkt werden, daß der Herbrandquotient gewöhnlich als die Inverse $h = q^{-1}$ definiert wird; an den Eigenschaften (i) und (ii) ändert das nichts, und $h(\mathbb{Z}) = |G|$.

Wir kehren jetzt zur Zahlentheorie zurück. Der erste Schritt zum Beweis der Ungleichung B ist die Berechnung von $q(L^S)$; hier bezeichnet S die Menge der endlichen Teiler des Modulus $\mathbf{m}$ (in L) und L^S die S-Einheiten von L, also die Elemente von L, die an allen Stellen außerhalb von S Einheiten sind. Das Resultat ist

$$q(L^S) = [L : K] / \prod n_p ,$$

wobei das Produkt über alle $p|\mathbf{m}$ zu nehmen ist und n_p den lokalen Grad $[L_P : K_p]$ bezeichne. Die wichtigste hier eingehende arithmetische Tatsache ist, daß die Gruppe U_L der absoluten Einheiten von L eine G-invariante Untergruppe W von endlichem Index enthält, welche die Operation von G auf den unendlichen Stellen von L wiederspiegelt; $q(W)$ ist berechenbar und damit auch $q(U_L)$. Der zweite Schritt ist der Beweis von

$$[K^\times : N(L^\times)K^{\mathbf{m}}] = \prod n_p ,$$

wo $K^{\mathbf{m}}$ den Zahlstrahl bezeichne. Die Berechnung des linksstehenden Index wird aufs Lokale zurückgeführt; dort wird dann wichtig, daß die Einseinheitengruppen $U_p^{(n)}$ für genügend großes n vermittels exp und log isomorph zu p^n sind und aus lauter Normen bestehen. Herbrandquotienten spielen eine tragende Rolle in den Beweisen, obgleich sie im Resultat nicht mehr erscheinen. Der Index in der letzten Formel ähnelt schon dem gesuchten, nur daß dort Ideale statt Elemente figurieren. Durch Betrachtung geeigneter exakter Sequenzen, welche Elemente und Ideale verbinden, und einiges *diagram chasing* gelangt man schließlich zu einer Gleichung

$$h^{\mathbf{m}}(L/K) = q(L^S)\ [K^\times : N(L^\times)K^{\mathbf{m}}]\ n(\mathbf{m})$$

mit einer natürlichen Zahl $n(\mathbf{m})$. Die beiden letzten Formeln und Ungleichung A liefern jetzt Ungleichung B und $n(\mathbf{m}) = 1$; aus der letzteren Aussage läßt sich der Hassesche Normensatz unschwer ableiten ([J], S.156).

1.7 Ad (C). Beim Beweis des Reziprozitätsgesetzes (im zyklischen Fall) spielen Einheitswurzeln eine entscheidende Rolle. Das hat zwei Gründe: (1) wir haben eingangs gesehen, daß das Gesetz für Kreiskörper $\mathbb{Q}(\zeta)/\mathbb{Q}$ gilt. Das oben (1.3) beschriebene Wohlverhalten der Artinabbildung zeigt nun, daß das Gesetz, wenn es für L/K gilt, auch für Zwischenkörper L/E/K gilt und auch erhalten bleibt, wenn man die Erweiterung L/K zu einer Erweiterung LE/L für beliebiges E/K „hochschiebt". Daraus folgt, daß es für alle zyklotomischen Erweiterungen aller K gilt. (2) Obwohl die Einheitswurzeln nur für $K = \mathbb{Q}$ zur Erzeugung *aller* abelschen Erweiterungen ausreichen, gestatten sie doch für beliebiges K die Konstruktion von Erweiterungen mit subtilen Eigenschaften, was Grade und Zerlegung vorgegebener p aus K betrifft. Hier ist der benötigte Hilfssatz:

Artinsches Lemma. *Sei* L/K *zyklisch und* p *in* L/K *unverzweigt. Dann existieren ein natürliches* m *und eine Erweiterung* F/K , *so daß für eine primitive* m-*te Einheitswurzel* ζ *das folgende gilt*: (i) $L \cap F = L \cap K(\zeta) = K$; (ii) $L(\zeta) = F(\zeta)$; (iii) p *zerfällt voll in* F . *Dabei kann* m *als teilerfremd zu einem beliebig vorgegebenen* s *gewählt werden*.

Wie aus (ii) hervorgeht, ergibt sich F als Teilkörper des Kompositums $LK(\zeta)$. Was Mühe macht, sind die beiden letzten Bedingungen, die auf elementare, aber delikate Eigenschaften der Primteiler von m hinauslaufen. Mit diesen Hilfssatz gelingt dann der noch ausstehende Beweis: ist L/K zyklisch und gilt für den Modulus **m** die Gleichung $h^{\mathbf{m}}(L/K) = [L : K]$, so ist kern $\varphi_{L/K} \subset P^{\mathbf{m}}(K)\, N(I^{\mathbf{m}}(L))$. Daraus folgt dann die Gleichheit, weil beide Gruppen denselben Index [L : K] in $I^{\mathbf{m}}(K)$ haben. Zum Beweis wendet man das Artinsche Lemma auf die Primteiler eines I mit $\varphi_{L/K}(I) = 1$ an; weitere Details der scharfsinnigen Beweisführung auszubreiten, ist hier nicht der Ort.

1.8 Der nun darzustellende Beweis des Existenzsatzes ist durchsichtiger; wir geben erst die nötigen Definitionen. Eine Gruppe H mit $I^{\mathbf{m}}(K) \supset H \supset P^{\mathbf{m}}(K)$ für irgendeinen Modulus **m** nennen wir eine *Kongruenzgruppe* und sagen, daß H mod **m** *erklärt* ist. Wir haben schon bemerkt, daß der im Reziprozitätsgesetz auftretende Modulus nicht eindeutig bestimmt ist; benötigt wird also eine Äquivalenzrelation auf den Kongruenzgruppen, deren Klassen allen und genau den für eine bestimmte Erweiterung L/K „genügend großen" Moduli entsprechen. Diese ist gegeben durch

$$H_1 \sim H_2 \iff \text{es gibt einen Modulus } \mathbf{m} \text{ mit } H_1 \cap I^{\mathbf{m}}(K) = H_2 \cap I^{\mathbf{m}}(K) .$$

Es ist leicht zu sehen, daß dies eine Äquivalenzrelation ist. Man zeigt, daß die verallgemeinerte Idealklassengruppe $I^{\mathbf{m}}(K)/H$ bis auf Isomorphie nur von der Klasse von H abhängt. Eine Äquivalenzklasse von Kongruenzgruppen heißt eine *Idealgruppe* **H** , und wenn H zu **H** gehört und mod **m** erklärt ist, heißt **m** auch ein *Erklärungsmodul* von **H** . Man zeigt weiter: sind **m** und **n** Erklärungsmoduln für **H** , dann ist auch der ggT von **m** und **n** ein solcher; daraus folgt die Existenz eines kleinsten Erklärungsmoduls, den man den *Führer* von **H** nennt. (Warnung: nicht jeder Modulus ist ein Führer, und **m** nicht immer der Führer von $P^{\mathbf{m}}(K)$; siehe dazu [Co].) Das wesentlichen Hilfsmittel zum Beweis dieser gruppentheoretischen Sachverhalte sind Isomorphiesätze und der Approximationssatz.

Nun sei L/K eine abelsche Erweiterung. Wenn die Moduln **m** und **n** zulässig sind, dann auch **mn** , und daraus folgt leicht, daß der Erweiterung L/K eine Idealgruppe **H**(L/K) eindeutig zugeordnet ist. (Es trifft zu, ist aber hier noch nicht zu sehen, daß jeder Erklärungsmodul von **H**(L/K) auch zulässig ist.) Wir wollen zeigen, daß jede Idealgruppe auf diese Weise zu einer (eindeutig bestimmten) Erweiterung L/K gehört, dem *Klassenkörper* der Gruppe. Dabei stellt sich das Problem, daß die Einheitswurzeln dafür nicht ausreichen (man betrachte die quadratische Erweiterung $\mathbb{Q}(2^{1/4})$ von $\mathbb{Q}(2^{1/2})$), eine andere genügend reichhaltige Klasse abelscher Erweiterungen aber für allgemeine Grundkörper K nicht in Sicht ist. Doch ist ein Ausweg gangbar: wenn K die n-ten Einheitswurzeln enthält, kann jede Abelsche Erweiterung von K mit einem Exponenten n durch Adjunktion von n-ten Wurzeln von Elementen aus K erzeugt werden. Das folgt aus der „Kummertheorie", einem rein galoistheoretischen (nicht sehr tiefliegenden) Satz: enthält der (beliebige) Körper k eine primitive n-te Einheitswurzel, so entstehen abelsche Erweiterungen l/k vom Exponenten n durch Adjunktion n-ter Wurzeln; siehe etwa [J], S.171ff. Die beiden folgenden Aussagen erlauben eine Reduktion unseres Problems auf diesen Fall:

(1) Gegeben seien Kongruenzgruppen $I^{\mathbf{m}}(K) \supset H \supset H' \supset P^{\mathbf{m}}(K)$. Zu H' (genauer: der Idealgruppe von H') gehöre der Klassenkörper L/K. Wir können annehmen, daß $\mathbf{m}$ alle Verzweigung von L/K enthält. Dann hat H als Klassenkörper den Fixkörper der Untergruppe $\varphi_{L/K}(H)$ von Gal(L/K).

Das folgt leicht aus den formalen Eigenschaften von $\varphi_{L/K}$ und dem Reziprozitätsgesetz und erlaubt die Reduktion auf eine feste Menge verzweigter Stellen. Dasselbe gilt für den zweiten Schritt, der es erlaubt, den Grundkörper „hochzuschieben":

(2) Sei E/K zyklisch, H eine mod $\mathbf{m}$ erklärte Kongruenzgruppe von K und $H_E = \{I \in I^{\mathbf{m}}(E) \mid N(I) \in H\}$. Wenn H_E einen Klassenkörper über E hat, dann hat H einen Klassenkörper über K.

Das ermöglicht nun die Reduktion auf den Kummerschen Fall (man zerlegt die Erweiterung $K(\zeta)/K$ in eine Folge zyklischer Erweiterungen und argumentiert induktiv), mit einer festen Menge S von möglichen Verzweigungstellen. Die kleinste Kongruenzgruppe H mod $\mathbf{m}$, für welche $I^{\mathbf{m}}(K)/H$ den Exponenten n hat, ist $P^{\mathbf{m}}(K)I^{\mathbf{m}}(K)^n$, wobei $\mathbf{m}$ jetzt nur durch Elemente von S teilbar sein darf, die Exponenten aber beliebig groß sein können. Den Klassenkörper dazu kann man nun explizit angeben, er entsteht durch Adjunktion der n-ten Wurzeln der S-Einheiten von K; dabei kommt natürlich der Struktursatz für diese ins Spiel, eine (leichte) Erweiterung des Dirichletschen Einheitensatzes. Der Beweis erfordert noch eine langwierige Berechnung von Indices ([J], S.174ff), die aber methodisch über das Frühere nicht hinausgeht (auch die Herbrandquotienten treten wieder auf). Damit ist dann auch der Existenzsatz bewiesen.

Zur Abrundung des Gesamtbilds sei noch erwähnt, daß der Führer $\mathbf{f}(L/K)$ der Idealgruppe $\mathbf{H}(L/K)$ gleichzeitig der Führer der Erweiterung L/K selbst ist, in dem Sinne, daß *genau* die durch $\mathbf{f}(L/K)$ teilbaren Moduli zulässig sind, insbesondere dieser selbst. Er kann explizit beschrieben werden: die Primteiler von $\mathbf{f}(L/K)$ sind genau die verzweigten Stellen, und der Exponent r der endlichen Stelle p ist der kleinste, für welchen die r-te Einseinheitengruppe der Komplettierung K_p in der Normengruppe von L_P enthalten ist

(P|p) beliebig). Das erfordert noch weitere Überlegungen, auf die wir hier nicht mehr eingehen wollen ([J], S.189).

Die Klassenkörper zu den „kleinsten“ Kongruenzgruppen, den Idealstrahlen $P^{\mathbf{m}}(K)$, heißen *Strahlklassenkörper*. Nach den geschilderten Resultaten ist jeder abelsche Körper L/K in einem eindeutig bestimmten kleinsten Strahlklassenkörper enthalten, nämlich dem zum Führer von L/K gehörenden.

2 Die ideltheoretische Formulierung

2.1 Fragt man nach einem Objekt, welches den Körper K und alle seine Lokalisierungen K_p enthält, damit also als eine Art „universelle Komplettierung“ von K angesehen werden kann, so bietet sich, als gröbste Lösung, das Produkt aller K_p an; hier sind die K_p als Komponenten und K diagonal eingebettet. Man kommt aber auch mit weniger aus, nämlich

$$\mathbf{A}(K) := \{(x_p) \in \Pi_p K_p \mid x_p \text{ ganz für fast alle } p\},$$

dem *Adelring* von K . Für uns wichtig ist seine Einheitengruppe

$$J(K) := \{(x_p) \in \Pi_p K_p^\times \mid x_p \text{ ist Einheit für fast alle } p\},$$

die *Idelgruppe* von K . Ihre fundamentalen Eigenschaften sind die folgenden:

(i) Nehmen wir als Umgebungsbasis der Eins die Mengen

$$\Pi_p W_p \text{ , mit } W_p = \text{ offene Umgebung von 1 in } K_p^\times \text{ und } W_p = U_p \text{ für fast alle } p ,$$

so wird J(K) zu einer *lokal kompakten* topologischen Gruppe. Es ist nicht schwer, zu zeigen, daß $K^\times$, diagonal eingebettet, eine *diskrete* Untergruppe von J(K) ist; ihre Elemente nennt man *Hauptidele.*

(ii) Die zu den einzelnen p gehörenden Absolutbeträge lassen sich zu einem Absolutbetrag auf J(K) zusammenfassen ,

$$|(x_p)| = \Pi_p |x_p|_p ,$$

weil fast alle $|x_p|_p = 1$ sind. Dies ist ein stetiger Homomorphismus $J(K) \to \mathbb{R}_+^\times$ und surjektiv, weil der Zahlkörper K mindestens eine unendliche Stelle hat (das ist *einer* der Unterschiede zum Funktionenkörperfall).

(iii) Es existiert eine „Idealabbildung“

$$j: \quad J(K) \to I(K), \qquad (x_p) \quad \to \quad \Pi_{p<\infty}\ p^{r(p)},\ r(p) = v_p(x_p)\ ,$$

wobei v_p die normierte Exponentenbewertung von K_p bezeichnet und das Produkt natürlich nur über die endlichen Stellen zu erstrecken ist. Hier erscheint der Idelbegriff als „Verfeinerung“ des Idealbegriffs, insofern die Einheiten wie auch die Komplettierungen an den unendlichen Stellen ihren Platz haben. („Idel“ ist kurz für „ideales Element“, wie es schon „Ideal“ für „idealer Teiler“ war; es liegt sozusagen eine zweifache „Idealisierung“ vor.) Die Idealabbildung ist ein surjektiver Homomorphismus mit dem Kern $\Pi_p U_p$, wobei für die $p|\infty$ einfach $U_p = K_p^\times$ gesetzt ist.

Nichts von all dem gilt für das volle Produkt $\Pi_p K_p^\times$; es ist bemerkenswert, daß die scheinbar geringfügige Einschränkung auf $J(K)$ ein so brauchbares Objekt hervorbringt. Das zentrale Objekt für die idelisch formulierte Klassenkörpertheorie ist nun die Faktorgruppe

$$C(K) := J(K) / K^\times\ ,$$

die *Idelklassengruppe*. Aus der Produktformel $\Pi_p |x|_p = 1$ für die (richtig normierten) Absolutbeträge von K folgt, daß der Absolutbetrag von $J(K)$ nach $C(K)$ absteigt. Daraus wiederum folgt, daß $C(K)$ nicht kompakt ist, wohl aber ist dies der Kern $C^1(K)$ des Absolutbetrags. Diese Aussage ist (cum grano salis) äquivalent zur Konjunktion aus der Endlichkeit der Klassenzahl und dem Dirichletschen Einheitensatz; siehe etwa [K], S.197 für die Ableitung der Kompaktheit aus diesen beiden und [C], S.71f für die umgekehrte Richtung. Die Betragsabbildung $C(K) \to \mathbb{R}_+^\times$ spaltet (man bilde $t > 0$ auf das Idel mit der einzigen nichttrivialen Komponente t an einer reellen Stelle von K ab, bzw. $\sqrt{t}$ an einer komplexen), so daß ein Isomorphismus $C(K) \cong C^1(K) \times \mathbb{R}_+^\times$ besteht.

Aus der Surjektivität der Idealabbildung folgt, daß sich die verallgemeinerten Idealklassengruppen auch als Faktorgruppen von $C(K)$ darstellen lassen; das ist nicht schwer, siehe [La], S.147.

Für eine endliche Menge S von Primstellen von K (endlich oder unendlich) sei

$$J^S(K) := \{\, (x_p) \mid x_p \text{ ist Einheit für } p \notin S \,\}\ .$$

Offenbar ist $J(K)$ die Vereinigung aller $J^S(K)$. Eine oft gebrauchte Eigenschaft von $J(K)$ ist die folgende: sei S eine endliche Menge von Primstellen und so groß, daß man alle Idealklassen von K durch Ideale repräsentieren kann, deren sämtliche Primteiler in S liegen. Dann ist

(2) $$J(K) = J^S(K)\, K^\times, \text{ also auch } \quad C(K) = J^S(K)\, K^\times / K^\times\ .$$

In Worten: außerhalb von S unterscheidet sich jedes Idel von einem Hauptidel nur um Einheiten. Das wesentliche Ingrediens beim Beweis ist der Approximationssatz.

2.2 Wir haben nun zu untersuchen, wie die Idel- und Idelklassengruppen bei Erweiterungen L/K korreliert sind. Dazu ist zweckmäßig, für ein Idel (x_P) von L und eine Stelle p von K den „Subvektor" $\Pi_{P|p}\, x_P$ als die p-Komponente von (x_P) zu bezeichnen. Die Einbettung $J(K) \to J(L)$ ist nun durch $(x_p) \to (\Pi_{P|p}\, x_p)$ definiert; dabei gehen Hauptidele in ebensolche über, es gilt sogar $J(K) \cap L^\times = K^\times$; also *nur* die Hauptidele von K werden in $J(L)$ zu Hauptidelen, was für Ideale bekanntlich falsch ist. Aus beidem zusammen ergibt sich eine *injektive* Abbildung $C(K) \longrightarrow C(L)$, vermöge derer wir $C(K)$ als Untergruppe von $C(L)$ aufassen dürfen. Die Idelnorm $N: J(L) \longrightarrow J(K)$ bildet die p-Komponente $\Pi_{P|p}\, x_P$ ab auf das Produkt der lokalen Normen der x_P bezüglich der Erweiterungen L_P/K_p; für ein Hauptidel $x \in L$ ergibt sich dabei die Norm $N(x)$ bezüglich der Erweiterung L/K. Daraus folgt, daß die Norm eines Hauptidels ebenfalls ein solches ist; damit steigt die Idelnorm ab zu einer Normabbildung $C(L) \longrightarrow C(K)$.

Etwas komplizierter ist im galoisschen Fall die Untersuchung der G-Operation, $G = \mathrm{Gal}(L/K)$ auf $J(L)$ und $C(L)$; es genügt wieder, die p-Komponenten $\Pi_{P|p}\, x_P$ zu betrachten. Die G-Operation auf diesen kombiniert die Operation auf der Menge der $P|p$ mit der Operation der Zerlegungsgruppen $D(P) = \mathrm{Gal}(L_P/K_p)$ auf den einzelnen L_P/K_p; beides läßt sich in der Formel

$$(g\,(\Pi_{P|p}\, x_P))_{gP} = g(x_P)\,,\ g \in G,$$

zusammenfassen, wo die linke Seite die gP-Komponente von $g(\Pi_{P|p}\, x_P)$ bezeichne. Modultheoretisch gesprochen: der G-Modul $\Pi_{P|p}\,(L_P)$ wird von dem $D(P)$-Modul L_P *induziert*. Es ist klar, daß die Operation zu einer solchen auf $C(L)$ absteigt. Es ergeben sich die glatten Formeln

$$J(L)^G = J(K) \quad\text{und}\quad C(L)^G = C(K)\,.$$

Die letztere liegt nicht auf der Hand; wir beweisen sie unter Vorwegnahme von etwas Kohomologie (siehe unten 4.1.1): die Kohomologiesequenz zur exakten Sequenz

$$1 \longrightarrow L^\times \longrightarrow J(L) \longrightarrow C(L) \longrightarrow 1$$

ergibt die exakte Sequenz

$$1 \longrightarrow K^\times \longrightarrow J(K) \longrightarrow C(L)^G \longrightarrow H^1(G, L^\times) = 1$$

wegen des Satzes „Hilbert 90" und damit die Behauptung. Insbesondere läßt sich $C(K)$

als Untergruppe von $C(L)$ auffassen; damit wird eine „absolute“ Idelklassengruppe definierbar, die Vereinigung (genauer: der induktive Limes) aller $C(L)$, L/K .

2.3 Wir können nun die erste der beiden zentralen Aussagen formulieren:

Reziprozitätsgesetz, ideltheoretische Fassung: *für abelsche* L/K *existiert ein kanonischer Isomorphismus*

$$(\ , L/K) : \ C(K)/N(C(L)) \ \to \ \mathrm{Gal}(L/K) ,$$

die Normrestabbildung (oder das Normrestsymbol).

Die Bezeichnung erklärt sich selbst aus dem obigen Isomorphismus; man beachte, daß sie für die Artinabbildung nicht angebracht wäre, weil bei ihr die Normen nur einen Teil (den trivialen!) des Kerns ausmachen. Die Abbildung $(\ ,L/K)$ heißt kanonisch, weil sie dasselbe Wohlverhalten aufweist wie die Artinabbildung, und ist das globale Gegenstück zu einer lokalen Normrestabbildung mit demselben Wohlverhalten (s.u. 4.3.1); wir bezeichnen mit $(\ , L/K)$ auch die auf $J(K)$ gehobene Abbildung $J(K) \to \mathrm{Gal}(L/K)$. Wir erwarten jetzt, daß die Idealabbildung j für zulässige Moduli $\mathbf{m}$ einen Isomorphismus

$$j: \ C(K)/N(C(L)) \ \to \ H^{\mathbf{m}}(L/K)$$

induziert, und zwar so, daß $(\ , LK) = \varphi_{L/K} \circ j$ gilt. Den Isomorphismus findet man in [La], S.150 oder [N1], S.296; als das eigentliche „Gelenk“ für den Übergang von der ideal- zur ideltheoretischen Formulierung erweist sich wieder der Approximationssatz. Die fragliche Gleichung kann natürlich erst bewiesen werden, wenn das Normrestsymbol genügend bekannt ist. Sie ergibt sich dann so: das globale Symbol ist das Produkt der lokalen; für lokale unverzweigte Erweiterungen bildet das lokale Symbol die Primelemente auf den Frobeniusautomorphismus ab; die Artinabbildung ist durch ihre Werte auf den unverzweigten Primidealen gegeben, und diese Werte sind ebenfalls die Frobeniusautomorphismen, schließlich identifiziert sich die lokale Galoisgruppe mit der Zerlegungsgruppe, einer Untergruppe der globalen Galoisgruppe. (Aus diesem Grund haben wir uns erlaubt, das Normrestsymbol ebenso zu bezeichnen wie oben die Frobeniusautomorphismen.)

Aus dem Wohlverhalten der Normrestabbildung und dem Reziprozitätsgesetz folgt eine bijektive und inklusionsumkehrende Korrespondenz zwischen den abelschen L/K und den Normengruppen $N(C(L))$ in $C(K)$ (das gilt schon auf der abstrakten Ebene der Klassenformationen; s.u. 4.2). Es fragt sich jetzt, welche Untergruppen H von $C(K)$ Normengruppen sind, also die Form $H = N(C(L))$ haben; L heißt dann der Klassenkörper von H. Man beachte den Unterschied zum Existenzproblem beim idealtheoretischen Zugang: dort war die Frage, *ob* es zu jeder Idealgruppe einen Klassenkörper gibt; hier ist die Frage, zu *welchen* Untergruppen von $C(K)$ er existiert. Die glatte Antwort ergibt sich mittels der Topologie, die $C(K)$ als Faktorgruppe von $J(K)$ erbt:

Existenzsatz, ideltheoretische Fassung: *die Normengruppen von* $C(K)$ *sind genau die* *offenen (äquivalent: abgeschlossenen) Untergruppen von endlichem Index.*

2.4 Vergleicht man die beiden Zugänge, so fällt am meisten auf, daß beim ideltheoretischen die Moduli nicht auftreten. Während idealtheoretisch der Verband der abelschen L/K durch die Moduli in die Strahlklassenkörper und ihre Teilkörper gegliedert wird, tritt er hier als Dual zum Verband der offenen Untergruppen einer einzigen Gruppe in Erscheinung. Dieser Umstand und das Wohlverhalten der Normrestabbildung, genauer: die Gleichung

$$(a, N/K) \mid L = (a, L/K) \ , \ N/L/K \text{ abelsch },$$

die einfach sagt, daß die Familie der (a, L/K) , L/K abelsch, ein Element von lim.proj. Gal(L/K) = Gal(K^{ab}/K) konstituiert, ermöglichen die Definition eines „universellen" Normrestsymbols (, K) : C(K) $\rightarrow$ Gal(K^{ab}/K) mit Werten in der Galoisgruppe der maximalen abelschen Erweiterung von K ; dieser ist surjektiv und hat einen in „konkreten" Termini beschreibbaren Kern, so daß sich auch eine Beschreibung von Gal(K^{ab}/K) ergibt (siehe 4.4.5 und [AT], Ch. IX). Ein Nachteil ist die „indirekte" Definition des Normrestsymbols (das wird unten(4.6) deutlicher werden), während die Artinabbildung sich vergleichsweise einfach angeben ließ. Der Grund ist, daß dort nur die unverzweigten Primideale eingehen, während beim Normrestsymbol alle Stellen berücksichtigt werden müssen, die Schwierigkeiten der lokalen Theorie aber gerade in den verzweigten Erweiterungen liegen. Ein Vorzug wiederum ist die leichtere „Lokalisierbarkeit" mancher Überlegungen, die sich natürlich der ziemlich direkten Herkunft von C(K) aus J(K) verdankt. Das wiederum ist bemerkenswert: in J(K) stehen die Lokalisierungen noch unverbunden nebeneinander; die algebraisch höchst simple „Kopplung" durch die Multiplikation mit Elementen von K, die sparsamste denkbare, bringt die Gruppe C(K) hervor – ein „sehr globales" Objekt, denn es enthält die gesamte Information über den Verband der abelschen Erweiterungen von K einschließlich der Primzerlegung in diesen. Ein weiterer Vorzug liegt darin, daß die idelisch formulierte Theorie eine formale Ähnlichkeit der lokalen und globalen Situation schafft, wodurch erstens eine „abstrakte" Klassenkörpertheorie möglich wird, die den gruppentheoretischen Kern des Reziprozitätsgesetzes isoliert, sodann eine Ableitung der globalen aus der lokalen Theorie (die oben schon angedeutet wurde); in der Folge werden wir drei solchen Theorien begegnen. Ein weiteres „Verdienst" der Idele, das wir hier nur am Rande vermerken können, liegt darin, daß sie die Revolution der analytischen Theorie ermöglicht haben, die in Tates‘s Thesis stattgefunden hat. Insgesamt: für „theoretische" Zwecke ist die Sprache der Idele vorzuziehetn, die Resultate sind glatter; will man aber Beispiele in voller Konkretion, bietet die idealtheoretische mehr Anschaulichkeit.

3 Chevalley 1940

3.1 Das „théorème central" dieser Arbeit ist, in heutiger Sprache, ein Isomorphismus zwischen der Charaktergruppe der Galoisgruppe der maximalen abelschen Erweiterung von K und der Charaktergruppe der (geeignet topologisierten!) Idelklassengruppe C(K). Wir beginnen mit vorbereitenden Definitionen.

K ist stets ein Zahlkörper, und wir schreiben $G(K)$ für $\mathrm{Gal}(K^{ab}/K)$. Ist L/K beliebig, N/K abelsch, so ist LN/L abelsch, und die Einschränkung der $G(L)$-Operation auf N gibt einen Homomorphismus $G(L) \longrightarrow G(K)$, dieser wiederum einen Homomorphismus $G(K)^* \longrightarrow G(L)^*$ der Charaktergruppen, den Chevalley mit $N_{K/L}$ bezeichnet; dieser ist multiplikativ in Türmen $N/L/K$ und kompatibel mit Isomorphismen $K \longrightarrow K'$. G^* bezeichnet hier die Gruppe der *stetigen* Charaktere; da G proendlich ist, hat ein solcher ein endliches Bild. Für einen Charakter χ von $G(K)$ sei Z_χ der Fixkörper von Kern χ ; dies ist eine zyklische Erweiterung von K , und χ gibt eine Einbettung von $\mathrm{Gal}(Z_\chi /K)$ in S^1 . Wir nennen χ *unverzweigt* an der Stelle p von K, wenn Z_χ es ist.

Die Idelgruppen $J(K)$ werden von Chevalley anders topologisiert als oben beschrieben. Für eine endliche Stellenmenge S und $n > 0$ sei

$$J(K)^{S,n} = \{(x_p) \mid \ x_p \text{ ist n-te Potenz in } K_p \text{ für } p \in S \text{ und Einheit für } p \notin S \} .$$

Für $n = 1$ ist $J(K)^{S,n}$ das frühere $J(K)^S$. Weiter sei

$I(K)^{S,n} = J(K)^{S,n}\, J(K)^n = \{(x_p) \mid \ x_p$ ist n-te Potenz in K_p für $p \in S$ und Produkt einer Einheit und einer n-ten Potenz für $p \notin S \}$.

Es ist $I(K)^{S\cup T,nm} \subset I(K)^{S,n} \cap I(K)^{T,m}$, woraus folgt, daß die $I(K)^{S,n}$ als Basisumgebungen der Eins in einer Topologie auf $J(K)$ dienen können. Diese Topologie ist gröber als die oben definierte übliche und ist nicht Hausdorffsch; es ist nicht schwer zu zeigen, daß der Durchschnitt aller $I(K)^{S,n}$ aus den Idelen (x_p) besteht, für welche $x_p = 1$ für endliche p und $x_p > 0$ für reelle p ist, also

$$\bigcap I(K)^{S,n} = (\mathbb{R}_+)^r \times (\mathbb{C}^\times)^s ,$$

wobei r die Anzahl der reellen und s die der Paare konjugiert komplexer Einbettungen von K ist. In einer Fußnote ([Ch1], S.399) bemerkt Chevalley, daß diese Topologie für die vorwiegend multiplikativen Strukturen, die in der Klassenkörpertheorie betrachtet werden, angemessener sei als die gewöhnliche; wir werden gleich sehen, daß sein Hauptsatz mit der gewöhnlichen Topologie falsch wäre.

Ein (stetiger) Charakter ψ von $J(K)$ heißt *unverzweigt* an der Stelle p, wenn $\psi(U_p) = 1$ ist (wir betrachten K_p als eingebettet in $J(K)$). Fast alle Stellen sind unverzweigt, denn Kern ψ enthält ein $I(K)^{S,n}$ und damit fast alle U_p .

Ein Charakter ψ von $J(K)$ heißt ein *Differential* von $J(K)$, wenn ψ auf den Hauptidelen verschwindet, $\psi(K^\times) = 1$; mit andern Worten, ein Differential ist ein

Charakter der Idelklassengruppe $C(K)$. Für diese Benennung verweist Chevalley auf die Analogie im Funktionenkörperfall und eine Arbeit von Weil; siehe auch die Diskussion von Kählerschen vs. Weilschen Differentialen in [Lo2], S.255 und [vdW], Kap.19. Aus dem Approximationssatz folgt, daß ein Differential schon durch fast alle seine Komponenten eindeutig bestimmt ist. Für Erweiterungen L/K ist eine Normabbildung $N: C(L) \to C(K)$ definiert und damit auch die „Conorm" $N_{K/L} := N^* : C(K)^* \to C(L)^*$, explizit also $(N_{K/L}(\psi))(x) = \psi(N(x))$ für $x \in C(L)$.

Wir können nun schon den Hauptsatz formulieren:

Es besteht ein Isomorphismus

$$\Phi_K : G(K)^* \to C(K)^* ,$$

derart, daß χ *und* $\Phi_K(\chi)$ *dieselben Verzweigungsstellen haben. Ferner gilt: für Erweiterungen* L/K *sind die Abbildungen* Φ *mit den Normen für Charaktere von* $G(K)$ *und* $C(K)$ *kompatibel,* $\Phi_L \circ N_{K/L} = N_{K/L} \circ \Phi_K$ *, oder: das Diagramm*

$$\begin{array}{ccc} G(L)^* & \to & C(L)^* \\ N_{K/L} \uparrow & & \uparrow N_{K/L} \\ G(K)^* & \to & C(K)^* \end{array}$$

ist kommutativ. Die Isomorphismen Φ_K *sind kompatibel mit Isomorphismen* $K \to K'$.

Die letztere Aussage läßt sich natürlich auch genauer als kommutatives Diagramm schreiben; wir verzichten darauf, weil wir die Aussage nicht explizit brauchen werden.

Ein Isomorphismus $G(K)^* \to C(K)^*$ wäre mit der gewöhnlichen Topologie von $C(K)$ nicht möglich, weil diese Gruppe nicht kompakt ist und wegen der Pontrjagin-Dualität keine diskrete Charaktergruppe haben kann. Hier aber ist $C(K)^* = (C(K) / \bigcap I(K)^{S,n})^*$, und $C(K) / \bigcap I(K)^{S,n}$ ist in der Tat Hausdorffsch und kompakt (wir werden das für $K = \mathbb{Q}$ unten in 4.4.5 explizit sehen). Legt man die gewöhnliche Topologie von $C(K)$ zugrunde, muß man $C(K)^*$ durch die Gruppe der Charaktere endlicher Ordnung ersetzen; siehe [W], S. 271.

Der Isomorphismus Φ_K spricht eine „absolute" oder „universelle" Reziprozität aus; die relativen, auf Erweiterungen L/K bezogenen Reziprozitätsisomorphismen werden natürlich im Verlauf des Beweises konstruiert. Der Existenzsatz folgt nach Dualisieren aus der Galoistheorie: die (endlichen) abelschen L/K entsprechen bijektiv den offenen Untergruppe von $G(K)$ und diese via Φ_K denen der (Hausdorffschen) Gruppe $C(K) / \bigcap I(K)^{S,n}$, die letzteren den offenen Untergruppen von endlichem Index in $C(K)$.

Der Beweis des Hauptsatzes vollzieht sich gewissermaßen stufenweise, entsprechend der Tatsache, daß $G(K)$ = lim.proj. $Gal(L/K)$ ist, wo L/K die abelschen Erweiterungen von K durchläuft. Auf den Idelklassenseite entsprechen den $Gal(L/K)$ die Gruppen $C(K)/N(C(L))$. Chevalley nennt einen Charakter φ von $C(K)$ *assoziiert zur Erweiterung* L/K , wenn $N_{K/L}(\varphi) = 1$ ist, also $\varphi(N_{L/K}(x)) = 1$ für $x \in C(L)$; oder einfacher: φ ist ein Charakter von $C(K)/N(C(L))$. Hier ist das fundamentale Beispiel: sei $\chi \in G(K)^*$, $L = Z_\chi$ und $\varphi = \Phi_K(\chi)$. Dann ist

$$\varphi \circ N_{L/K} = N_{K/L} \circ \Phi_K(\chi) = \Phi_L \circ N_{K/L}(\chi) = 1 ,$$

denn für $s \in G(L) = \text{kern}\,\chi$ ist $(N_{K/L}(\chi))(s) = \chi(s \mid K^{ab}) = 1$. Wir schreiben kurz $D(L/K) := (C(K)/N(C(L)))^*$. Das Beweisschema für den Hauptsatz ist nun das folgende:

(A) Beweis von $|\,Gal(L/K)^*\,| = |\,D(L/K)\,|$ im zyklischen Fall, durch die Indexberechnungen für Normen und Einheiten, welche die Ungleichungen A und B ergeben.

(B) Darauf gestützt Konstruktion eines Isomorphismus $Gal(L/K)^* \longrightarrow D(L/K)$; zunächst nur im zyklotomischen Fall, dann Ausdehnung auf den allgemeinen zyklischen Fall mittels einer Variante des Artinschen Lemmas. Dualisieren ergibt den Reziprozitätsisomorphismus $C(K)/N(C(L)) \longrightarrow Gal(L/K)$. Das im Hauptsatz formulierte Wohlverhalten wird bei diesen Schritten mitbewiesen. Der abelsche Fall folgt dann leicht mit dem Resultat von (A) (S.417).

(C) Beweis der Surjektivität von Φ_K durch Reduktion auf den Kummerschen Fall und L/K zyklisch von Primzahlordnung; dort durch direkte Konstruktion.

3.2 Wir beschreiben nur die zentrale Konstruktion zum Schritt B. Sei $\chi \in G(K)^*$, die endliche Stelle p von K unverzweigt in Z_χ und $(p, Z_\chi/K)$ der Frobenius-automorphismus. Für $x \in J(K)$ und $\nu(p, x)$ = p-Ordnung von x_p sei

$$(x, \chi / p) := \chi((p, Z_\chi/K))^{\nu(p, x)}$$

gesetzt. Als Funktion von x ist dann $(\ ,\ \chi / p)$ ein p-lokaler unverzweigter Charakter von $J(K)$. Er hat die Eigenschaften

(i) $(\ ,\ \chi\chi' / p) = (\ ,\ \chi / p)(\ ,\ \chi' / p)$ (χ' unverzweigt in p) ;

(ii) für jedes L/K ist $(N_{L/K}\,x,\ \chi / p) = \prod_{P|p} (x, N_{K/L}\,\chi / P)$, $x \in J(L)$;

(iii) Kompatibilität mit Isomorphismen $K \longrightarrow K'$.

Sei jetzt χ zyklotomisch, d.h. Z_χ Teilkörper eines Einheitswurzelkörpers $K(\zeta)$, n =

$[Z_\chi : K]$ und S die Menge aller p mit $p \mid \infty$ oder $p \mid m = \mathrm{ord}\,\zeta$. Ziel ist, χ einen Idelklassencharakter zuzuordnen, genauer ein Element von $D(Z_\chi/K)$. Zunächst wird die Existenz eines $a \in K^\times$ gezeigt mit $a \in (K_p)^n$, alle $p \in S$, man kann sogar annehmen, daß a ganz ist, total positiv und $\equiv 1 \bmod m$ (Approximationssatz). Sodann: für solche a ist

$$\Pi_{p \notin S}\ (a,\ \chi / p) = 1 \ ;$$

man beachte, daß in dem (natürlich endlichen) Produkt nur unverzweigte p vorkommen. Das ist im Kern die Hassesche Produktformel für die lokalen Normrestsymbole, und der Beweis ist leicht, weil durch die Bedingung $a \equiv 1 \bmod m$ die Verzweigung umgangen wird (wir werden unten (4.4.3) noch darauf eingehen) . Für $x \in J(K)$ sei nun $b \in K^\times$ gewählt mit $x_p b^{-1} \in (K_p)^n$ für alle $p \in S$, und es sei

$$\varphi_\chi(x) := \Pi_{p \notin S}\ (x b^{-1},\ \chi / p) \ ;$$

dies ist wohldefiniert, nämlich unabhängig von der Wahl der Hilfszahl b ; das Produkt ist wieder endlich, weil alle p unverzweigt und fast alle x_p Einheiten sind. Wie Chevalley selbst anmerkt, geht dieser Kunstgriff, die Verzweigung zu umgehen, ohne sie zu „eliminieren“ (in gewisser Weise ist sie ja durch die Hilfszahl b präsent), auf Hasses Definition des Normrestsymbols zurück. Jetzt kann gezeigt werden, daß φ_χ in $D(Z_\chi / K)$ liegt und durch die Eigenschaft charakterisiert ist, daß fast alle p-Komponenten $=$ $(\ ,\chi / p)$ sind. Weiter hat φ_χ dieselbe Ordnung hat wie χ ; die Zuordnung $\chi \to \varphi_\chi$ ist daher injektiv, und mit dem Resultat von Schritt A folgt das Reziprozitätsgesetz im zyklischen zyklotomischen Fall. Man beachte, wie die verzweigten Stellen hier nur indirekt erfaßt werden.

Jetzt sei χ beliebig von der Ordnung n , und φ ein assoziiertes Differential; χ' sei zyklotomisch von einer durch n teilbaren Ordnung und mit $Z_\chi \cap Z_{\chi'} = K$, und φ' das eben konstruierte zu χ' assoziierte Differential. Für $T := Z_{\chi\chi'^{-1}}$ ist dann $N_{K/T}(\chi) = N_{K/T}(\chi')$, und dieselbe Gleichung gilt für die Conormen der Differentiale. Es folgt, daß die Erweiterung $Z_\chi T/T$ zyklotomisch ist; damit wird das Resultat des letzten Abschnitts anwendbar. Mittels einer Variante des Artinschen Lemmas zeigt Chevalley jetzt, daß für fast alle endlichen p die p-Komponente φ_p von φ die Gestalt $(\ ,\ \chi / p)^v$ hat, wobei v nicht von p abhängt. Da ein Differential durch fast alle Komponenten bereits eindeutig bestimmt ist, nach Schritt (A) aber n Differentiale existieren, muß genau eines darunter sein, für welches $v = 1$ ist. Dies ist das gesuchte $\Phi_K(\chi)$.

Die Arbeit von Chevalley ist eine staunenswerte *tour de force*. Zieht man die einleitenden und vorbereitenden Abschnitte ab, wird auf 20 Seiten alles bewiesen, ohne komplexe Analysis, Kohomologie oder Algebrentheorie. Wenn irgendwo, dann ist hier die „reine

Lehre“ im Sinne der prä-kohomologischen Theorie verwirklicht; mit Recht schreibt Iyanaga ([I], S.71), daß diese hier ihre definitive Formulierung gefunden habe. Chevalley selbst sah die Dinge anders. In der kurzen, aber lesenswerten Einleitung zu seinem Buch [Ch2] von 1954 schreibt er, ohne seine eigene, eben besprochene Arbeit zu erwähnen, daß es seit Takagi und Artin keinen wirklich wichtigen Fortschritt bis zur Einführung der kohomologischen Methoden gegeben habe. Diesen wenden wir uns jetzt zu.

4 Der kohomologische Zugang: Klassenformationen

4.1 Kohomologie

4.1.1 In diesem ersten Abschnitt stellen wir zusammen, was wir aus der Kohomologietheorie der Gruppen benötigen, genauer der Tate-Kohomologie der endlichen Gruppen; nähere Ausführungen und alle Beweise findet man in [N1]. Für ein solches G und einen G-Modul A besteht die Kohomologie aus einer unendlichen Familie

$$H^*(G, A) = \{H^q(G, A),\ q \in \mathbb{Z}\}$$

abelscher Gruppen. Für Dimensionen $q > 0$ sind dies die gewöhnlichen Kohomologiegruppen, für $q < -1$ die Homologiegruppen, welche beide für alle Gruppen definiert sind; Tates Konstruktion ist eine Art Verspleißung der beiden, wobei in der Mitte eine Modifikation nötig ist, die eine G-Norm involviert und daher nur für endliches G möglich ist. (In manchen Darstellungen werden die Tateschen Gruppen für $q < 1$ mit $\hat{H}^q$ bezeichnet.) Für festes G und q ist $A \to H^q(G, A)$ ein kovarianter Funktor; für einen Morphismus $f\colon A \to B$ von G-Moduln hat man also einen Homomorphismus $H^q(f) : H^q(G, A) \to H^q(G, B)$ von abelschen Gruppen, wobei Kompositionen und Identitäten erhalten bleiben. Die definierende Eigenschaft der Kohomologie ist (wir schreiben $H^q(A)$ für $H^q(G, A)$, solange G fest bleibt): eine kurze exakte Sequenz von Moduln

$$0 \to A \to B \to C \to 0$$

liefert eine lange exakte Sequenz von Kohomologiegruppen

$$\ldots \to H^q(A) \to H^q(B) \to H^q(C) \xrightarrow{\delta} H^{q+1}(A) \to \ldots$$

Die Homomorphismen δ heißen *Verbindungshomomorphismen*; sie sind für alle Kohomologie sozusagen das Salz in der Suppe. Für uns wichtig sind nur die Dimensionen $-2 \le q \le 2$, in denen konkrete (und handhabbare) Beschreibungen der Gruppen möglich sind:

$q = 0$: wir definieren eine Normabbildung $N\colon A \to A$ durch $N(a) = \sum_g ga$;

ersichtlich ist $N(A)$ enthalten im Fixmodul A^G, und es ist $H^0(G, A) = A^G / N(A)$. Ist zum Beispiel L/K eine galoissche Körpererweiterung mit der Gruppe G, so wird $H^0(G, L^\times) = K^\times / N(L^\times)$ die Normrestgruppe, die linke Seite beim lokalen Reziprozitätsgesetz. Im globalen Fall ist dies $H^0(G, C(L)) = C(K) / N(C(L))$. Der Funktor H^0 hat, wie oben schon bemerkt, „von Hause“ aus eine besondere Affinität zur Klassenkörpertheorie.

$q = 1$: ein 1-*Kozykel mit Werten in* A ist eine Funktion $x\colon G \to A$ mit $x(gh) = x(g) + gx(h)$ („gekreuzte Homomorphismen“), ein 1-*Korand* ein x der Form $x(g) = ga - a$ für ein $a \in A$, und es ist $H^1(A) = \{\text{1-Kozyklen}\} / /\text{1-Koränder}\}$. Man zeigt, daß aus einer exakten Sequenz

$$0 \to A \to B \to C \to 0$$

eine exakte Sequenz

$$0 \to A^G \to B^G \to C^G \to H^1(A) \to \ldots$$

folgt; in gewisser Weise beschreibt also der Funktor H^1 die Abweichung des Funktors $A \to A^G$ von der Eigenschaft, rechtsexakt zu sein. Operiert G trivial auf A, ist $H^1(A) = \mathrm{Hom}(G, A)$. Der folgende Spezialfall wird uns häufig begegnen: ist L/K eine Galoissche Körpererweiterung mit der Gruppe G, so ist $H^1(G, L^\times) = 1$. Diese (unschwer zu beweisende) Tatsache ist als Satz „Hilbert 90“ bekannt (Hilbert hat ihn aber nur für zyklische G angegeben; die Verallgemeinerung auf beliebige G stammt von Emmy Noether).

$q = 2$: ein 2-*Kozykel mit Werten in* A ist eine Funktion $x\colon G \times G \to A$ mit $x(gh, k) + x(g,h) = gx(k,h) + x(g, kh)$, ein 2-*Korand* ein x der Form $x(g,h) = gy(h) - y(gh) + y(g)$ für eine Funktion $y\colon G \to A$, und $H^2(A) = \{\text{2-Kozyklen}\} / \{\text{2-Koränder}\}$. Die 2-Kozyklen heißen auch *Faktorensysteme;* sie treten bei Gruppenerweiterungen auf, aber auch, für uns wichtiger, bei der Konstruktion von einfachen Algebren; wir kommen darauf zurück (5.1.2). Für alle Dimensionen $q \geq 1$ lassen sich die Gruppen $H^q(A)$ in analoger Weise beschreiben, jedoch werden, wie man hier schon ahnen kann, die dabei auftretenden Funktionalgleichungen immer unübersichtlicher.

$q = -1$: hier ist $H^{-1}(A) = \{a \mid Na = 0\} / \{\text{Erzeugnis aller } ga - a\}$. Man überzeuge sich, daß für zyklisches G die Definitionen von $H^0(A)$ und $H^{-1}(A)$ mit den früher (1.6) gegebenen übereinstimmen.

$q = -2$: wir brauchen nur den Fall $A = \mathbb{Z}$ mit trivialer G-Operation; hier hat man

$$H^{-2}(\mathbb{Z}) = G^{ab} = G / G' = \text{Faktorkommutatorgruppe};$$

siehe [N1], S.48.

In den Kohomologiegruppen $H^q(G, A)$ sind also verschiedene modultheoretische Aspekte von A, aber auch gruppentheoretische Aspekte von G kodifiziert. „Konkrete“ Interpretationen außerhalb des Bereichs $-2 \leq q \leq 2$ sind selten; siehe [AT], S.67 für eine Interpretation der 3-Kohomologie. Es gibt andererseits keine Garantie dafür, daß es solche überhaupt gibt (vor allem wäre erst zu präzisieren, was man unter einer solchen verstehen soll).

4.1.2 Im Falle eines zyklischen G kann man durch direkte Rechnungen zeigen, daß die zu einer exakten Sequenz $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ gehörende lange Kohomologiesequenz in ein exaktes Sechseck übergeht (siehe [J], S.141), m.a.W. die Kohomologie zyklisch mit der Periode 2 ist; die früher schon definierten Gruppen $H^0(A)$ und $H^{-1}(A) = H^1(A)$ enthalten also bereits die ganze kohomologische Information.

Alle $H^q(G, A)$ sind $|G|$-Torsionsgruppen, $|G|\, H^q(G, A) = 0$. Ist A endlich erzeugt, ist darum $H^q(G, A)$ endlich. Weiter: hat A uneingeschränkte und eindeutige Division, d.h. hat jede Gleichung $nx = a$, $n > 0$, eine eindeutige Lösung in A (äquivalent: Multiplikation mit n ist ein Automorphismus von A), so ist $H^q(G, A) = 0$. Das gilt z.B. für $A = (\mathbb{Q}, +)$ mit trivialer G-Operation. Aus der Sequenz

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

erhalten wir darum Isomorphismen $H^q(G, \mathbb{Q}/\mathbb{Z}) \cong H^{q+1}(G, \mathbb{Z})$ für alle q , insbesondere

$$H^2(G, \mathbb{Z}) \cong H^1(G, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \cong G^* = \text{Charaktergruppe von } G\,.$$

Das Beispiel zeigt die typische Anwendung exakter Sequenzen: aus dem Verschwinden einer Gruppe in einer solchen kann man schließen, daß der vorletzte Morphismus surjektiv und der übernächste injektiv ist. Zu den Charaktergruppen: in unserem Kontext sind die operierenden Gruppen G stets endlich oder proendlich; ein stetiger Charakter einer solchen Gruppe aber hat stets ein endliches Bild, also Einheitswurzeln als Werte. Für unsere Zwecke erweist sich die additive Schreibweise, die durch den Isomorphismus $r + \mathbb{Z} \longrightarrow \exp(2\pi i r)$ von $\mathbb{Q}/\mathbb{Z}$ mit der Gruppe aller Einheitswurzeln verfügbar wird, als notationell praktischer.

Wir haben (in Andeutung) gesehen, daß die $H^q(G, A)$ für $q \geq 1$ durch Funktionen $G \times \ldots \times G$ (q Faktoren) $\longrightarrow A$ definiert werden können. Daraus folgt, daß diese Funktoren kontravariant in G sind. Insbesondere hat man für Untergruppen $H \subset G$ *Restriktionsabbildungen* res: $H^q(G, A) \longrightarrow H^q(H, A)$, für Faktorgruppen G/H *Inflationsabbildungen* inf: $H^q(G/H, A^H) \longrightarrow H^q(G, A)$; man beachte, daß der

Fixmodul A^H ein G/H- und ein G-Modul ist. Die Restriktionen (aber nicht die Inflationen) können auf alle Dimensionen ausgedehnt werden, ihnen treten *Corestriktionen* cor: $H^q(H, A) \to H^q(G, A)$ zur Seite, für $q = 0$ gegeben durch

$$a + N_H A \quad \to \quad N_{G/H}\, a + N_G A \ ,$$

wobei wir die Normen zu den verschiedenen Gruppen durch entsprechende Indices kenntlich gemacht haben und $N_{G/H}$ die Summierung über ein Vertretersystem von G/H in G bedeutet. (Es muß angemerkt werden, daß bezüglich der Verwendung von „Corestriktion“ und „Verlagerung“ (transfer) in der Literatur eine gewisse Sprachverwirrung herrscht; man vergewissere sich jeweils, was gemeint ist. Hier ist die Verlagerung die Restriktion in der Dimension –2.) Alle diese Abbildungen sind kompatibel mit den $H^q(f)$ für $f: A \to B$ und den Verbindungshomomorphismen. Inf und res können kombiniert werden, und man zeigt, daß die Sequenz

$$0 \to H^1(G/H, A^H) \xrightarrow{\text{inf}} H^1(G, A) \xrightarrow{\text{res}} H^1(H, A)$$

exakt ist. Dasselbe gilt für H^2 anstelle von H^1 , wenn $H^1(H, A) = 0$ ist. Diese Sequenzen eignen sich für Induktionsbeweise nach der Ordnung von G und werden einige Male gebraucht; zugrunde liegt dann stets ein galoisscher Körperturm N/L/K , und es ist G = Gal(N/K), H = Gal(N/L) . (Für normale H sind die Kohomologien $H^*(G,A)$, $H^*(H,A)$ und $H^*(G/H, A^H)$ durch eine *Spektralsequenz* miteinander verkoppelt; die obige inf-res-Sequenz ist ein kleiner Teil davon.)

Wir benötigen noch eine Paarung von Kohomologiegruppen, die der Bildung des Tensorprodukts entspricht, das *Cupprodukt*. Sind A und B G-Moduln, so ist auch $A\otimes B$ ein solcher (das Tensorprodukt über $\mathbb{Z}$ genommen) mit der Operation $g(a\otimes b) = ga \otimes gb$. Die bilineare Abbildung $A \times B \to A\otimes B$ ist ein G-Homomorphismus, der die Fixgruppen und Normen erhält und darum eine bilineare Abbildung

$$H^0(G, A) \times H^0(G, A) \to H^0(G, A\otimes B)$$

induziert, das Cupprodukt in der Dimension 0. Allgemein hat man eine Familie bilinearer Abbildungen

$$\cup \ : \ H^p(G, A) \times H^q(G, B) \to H^{p+q}(G, A\otimes B) ,$$

die kompatibel sind mit den Modulabbildungen und den Verbindungshomomorphismen (in der zweiten Komponente nur bis auf ein Vorzeichen), darüber hinaus assoziativ und antikommutativ. Wie schon bei der Restriktion, Corestriktion und Inflation brauchen wir diese Eigenschaften nicht explizit (als kommutative Diagramme) auszuschreiben, weil sie zwar in die Beweise eingehen, für unseren Überblick aber entbehrlich sind.

4.1.3 Wir können nun das für uns zentrale Resultat der Kohomologietheorie formulieren, den

Satz von Tate: *Sei* A *ein* G-Modul *mit der Eigenschaft: für alle Untergruppen* H *von* G *gilt*

$$\text{(i)}\ \ H^1(H, A) = 0\ ;\quad \text{(ii)}\ \ H^2(H, A)\ \textit{ist zyklisch von der Ordnung}\ |H|\ .$$

Dann ist für alle q *und Erzeuger* a *von* $H^2(G, A)$ *die Abbildung*

$$a \cup\ :\ H^q(G, \mathbb{Z}) \ \longrightarrow\ H^{q+2}(G, A)$$

ein Isomorphismus.

Der für uns wichtigste Fall ist $q = -2$; er liefert einen Isomorphismus

$$H^{-2}(G, \mathbb{Z}) \ = \ G^{ab} \ \longrightarrow\ H^0(G, A) \ = \ A^G / N(A)\ ,$$

dessen Inverse eine abstrakte Normrestabbildung darstellt, der also selbst als ein *sehr* abstraktes Reziprozitätsgesetz angesehen werden kann. Was wir hier gegeben haben, ist nur ein Spezialfall einer allgemeineren Aussage; siehe [AW], S.114.

4.2 Abstrakte Klassenkörpertheorie: Klassenformationen

Eine *Formation* ist ein Paar (G , A), bestehend aus einer proendlichen Gruppe G und einem G-Modul A, versehen mit der diskreten Topologie, auf dem G stetig operiert; die Operation $G \times A \longrightarrow A$ ist also stetig, oder äquivalent: die Fixgruppe eines jeden $a \in A$ hat endlichen Index in G . G ist eine kompakte Hausdorffgruppe, und die offenen Untergruppen von G sind genau die Untergruppen von endlichem Index. Indizieren wir sie mit Buchstaben K, L , ... und nennen diese „Körper“, so können wir L/K eine Körpererweiterung nennen (in [AT] suggestiv „Schicht“, „layer“ genannt), wenn $G_L \subset G_K$, und normal, wenn G_L normal in G_K ist, entsprechend abelsch oder zyklisch; bezeichnen wir mit G(L/K) die (endliche) Faktorgruppe G_K/G_L , so entsteht, was man eine formale Galoistheorie nennen könnte, und G_K spielt die Rolle der absoluten Galoisgruppe von K . $[L : K] := |G(L/K)|$ heiße der Grad der Erweiterung L/K . Für eine normale Erweiterung L/K sei A_L der Fixmodul von G_L , ein G(L/K)-Modul, für den also Kohomologiegruppen $H^q(G(L/K), A_L)$ existieren, die wir mit $H^q(L/K)$ abkürzen. In den uns interessierenden Fällen ist natürlich in der Tat $G = Gal(K^{alg}/K)$ die Galoisgruppe eines algebraischen Abschlusses von K, wo K ein lokaler oder globaler Körper ist; im lokalen Fall ist A die multiplikative Gruppe von K^{alg} , im globalen Fall die absolute Idelklassengruppe, die man als den induktiven (direkten) Limes der Idelklassengruppen C(L) der Erweiterungen L/K definieren kann (siehe oben 2.2) ;

lokal ist dann $A_L = L^\times$, global $A_L = C(L)$. (Da wir uns nur für den arithmetischen Fall interessieren, brauchen wir zwischen K^{sep} und K^{alg} nicht zu unterscheiden.)

Wir bewegen uns weiter auf der abstrakten Ebene. Die Formation (G, A) heißt eine *Körperformation*, wenn für normale L/K stets $H^1(G(L/K), A_L) = 1$ ist. Eine Folgerung daraus ist die Exaktheit der inf-res-Sequenz

$$1 \to H^2(L/K) \to H^2(N/K) \to H^2(N/L)$$

für normale $N/L/K$, insbesondere also die Injektivität der Inflation $H^2(L/K) \to H^2(N/K)$, die uns erlaubt, diese als Einbettung anzusehen. Bilden wir den direkten Limes bezüglich dieser Einbettungen, entsteht eine Gruppe $H(K)$, die sich im lokalen und globalen Fall als kanonisch isomorph zur Brauergruppe $B(K)$ erweist; das werden wir später ausführen (5.1.2).

Schließlich heißt die Körperformation (G, A) eine *Klassenformation*, wenn das folgende Axiom erfüllt ist:

Für jede normale Erweiterung L/K besteht ein Isomorphismus

$$\mathrm{inv}(L/K) : H^2(L/K) \to [L:K]^{-1}\,\mathbb{Z} \bmod \mathbb{Z} \subset \mathbb{Q}/\mathbb{Z},$$

die *Invariantenabbildung*, mit den Eigenschaften:

(a) sind $N/L/K$ normal, so ist

$$\mathrm{inv}(L/K) = \mathrm{inv}(N/K) \mid H^2(L/K);$$

(b) ist N/K normal, so ist

$$\mathrm{inv}(N/L)\ \mathrm{res} = [L:K]\,\mathrm{inv}(N/K).$$

In der zweiten Formel bedeutet res die Restriktion $H^2(N/K) \to H^2(N/L)$; in der ersten Formel steht rechts die Einschränkung von $\mathrm{inv}(N/K)$ auf die vermöge der Inflation als Untergruppe von $H^2(N/K)$ aufgefaßte Gruppe $H^2(L/K)$.

Für jede Untergruppe H von G mit dem „Fixkörper“ K' ist L/K' wieder eine galoissche Erweiterung, und das Axiom gilt für sie in gleicher Weise. Damit sind die Voraussetzungen des Satzes von Tate erfüllt, und für den Fall der Dimension $q = 0$ erhalten wir für jeden Erzeuger a von $H^2(L/K)$ Isomorphismen

$$a \cup : H^{-2}(G(L/K), \mathbb{Z}) = G(L/K)^{ab} \to H^0(L/K) = A_K / NA_L .$$

Hierzu einige Bemerkungen. (1) Für die Anwendung des Satzes von Tate würde genügen, daß $H^2(L/K)$ stets zyklisch von der Ordnung $[L : K]$ ist. Natürlich müssen wir aber sicherstellen, daß der Reziprozitätsisomorphismus im globalen Fall mit dem früher beschriebenen übereinstimmt, denn nur dieser weist das Wohlverhalten auf, das ihn unentbehrlich macht. Dahinter steckt, daß im unverzweigten Fall der Frobenius ein ausgezeichneter Erzeuger der Zerlegungsgruppe ist, genauer der einzig natürliche. Der Grund dafür wiederum ist, *in the last resort*, daß die absolute Galoisgruppe eines endlichen Körpers (isomorph zur Komplettierung $\mathbb{Z}^\wedge$ von $\mathbb{Z}$ nach der Idealtopologie) nur zwei (topologische) Erzeuger hat, 1 und -1, entsprechend dem Frobenius und seinem Inversen, aber nur jener ist polynomial definiert. (2) Man beachte, daß G nicht als abelsch vorausgesetzt war; der Formalismus der Formationen liefert also a limine, daß die Normrestgruppe nur vom abelschen Teil der Erweiterung abhängt; siehe unten Folgerung (1). Viel mehr Informationen haben wir aber nicht, vor allem kein Zerlegungsgesetz. (3) Man kann die Axiomatik noch anreichern durch Forderungen an „spezielle Erweiterungen" (im Lokalen die unverzweigten, global die zyklischen zyklotomischen), siehe z.B. [K2], S.123. Dadurch wird deren strukturelle Bedeutung ins Licht gesetzt, allerdings auf Kosten der Allgemeinheit. (4) Die Forderungen (a) und (b), die hier einen eher technischen Charakter zu tragen scheinen, nehmen bei der algebrentheoretischen Interpretation der Gruppen $H^2(L/K)$ einen sehr konkreten Gehalt an; siehe unten 5.2.1.

Die Eigenschaften (a) und (b) ziehen weitere „gute" Eigenschaften der Invariantenabbildung nach sich. Definiert man als *Fundamentalklasse* der Erweiterung L/K das Element $u(L/K)$, welches durch $\mathrm{inv}(L/K)$ auf den „kanonischen" Erzeuger $1/[L : K] + \mathbb{Z}$ abgebildet wird, überträgt sich das Wohlverhalten von der Invariantenabbildung auf die Fundamentalklassen und schließlich auf die Inverse des Reziprozitätsisomorphismus, eben die *Normrestabbildung*

$$(\ , L/K): \quad H^0(L/K) = A_K / N(A_L) \quad \longrightarrow \quad G(L/K)^{ab} = H^{-2}(G(L/K)^{ab}, \mathbb{Z}) .$$

All das ist keineswegs simpel oder „bloß formal", sondern beruht auf einer expliziten Formel für das involvierte Cupprodukt und dessen Verträglichkeit mit den Verbindungshomomorphismen, doch das Innenleben des kohomologischen Apparats wirklich sichtbar zu machen, kann unsere Aufgabe hier nicht sein. Wir geben nur die Formel an, welche Invarianten und Normrestsymbol verbindet:

Sei χ ein Charakter von G und $\delta\chi$ sein Bild unter dem Isomorphismus $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \cong H^1(G, \mathbb{Q}/\mathbb{Z}) \cong H^2(G, \mathbb{Z})$ (s.o. 4.1.2), weiter sei $a \in H^0(L/K)$. Dann ist $a \cup \delta\chi \in H^2(L/K)$, und es gilt

$$\text{(3)} \qquad \chi(a, L/K) = \mathrm{inv}(L/K)(a \cup \delta\chi)$$

(für den Beweis siehe [N1], S.115). Wir werden dieser Formel später in algebrentheoretischer Fassung wiederbegegnen.

Das Wohlverhalten der Normrestabbildung schließlich manifestiert sich in kommutativen

Diagrammen, welche denen für die Artinabbildung angegebenen entsprechen und die wir nicht auszuschreiben brauchen.

Das somit Erreichte zieht nun, ganz wie im klassischen idealtheoretischen Zugang, wichtige Folgerungen nach sich. Nennen wir eine Untergruppe von A_K eine *Normengruppe*, wenn sie die Form $N(A_L)$ für eine Erweiterung L/K hat, so ergibt sich zunächst:

(1) Ist L/K normal und L' die größte abelsche Teilerweiterung von L , so ist

$$N_{L/K}(A_L) = N_{L'/K}(A_{L'}) .$$

Klassisch wird dies als „Abgrenzungssatz" bezeichnet und bedeutet, daß die Normengruppen *nur* über die abelschen L/K etwas aussagen. Die Gleichung folgt einfach daraus, daß die linke Seite in der rechten enthalten ist, aber nach dem Reziprozitätsgesetz beide denselben Index in A_K haben. Nicht schwer ist auch der Beweis von

(2) Die Zuordnung $L/K \rightarrow N(A_L)$ stiftet eine inklusionsumkehrende Bijektion zwischen dem Verband der abelschen L/K und den Normengruppen in A_K (die folglich auch einen Verband bilden).

Schließlich die für den Beweis des Existenzsatzes wichtige Aussage (die nicht aus der Bijektion allein folgt):

(3) Jede Obergruppe einer Normengruppe ist selbst Normengruppe.

Der Beweis ist analog dem der entsprechenden Aussage in der klassischen Theorie.

Das *Existenzproblem* besteht jetzt in der Frage nach einer „intrinsischen" Charakterisierung der Normengruppen in A_K , die also nicht auf Erweiterungen von K rekurriert. Das ist auch im abstrakten Rahmen möglich, und zwar mittels einer Topologie auf den Moduln A_K ([AT], S.231ff). Das (im arithmetischen Fall) wesentliche Axiom ist dann eine Aussage über die universellen Normen (Elemente von A_K , die Normen aus jeder Erweiterung L/K sind). Dann läßt sich der *Existenzsatz* beweisen: die Normengruppen sind genau die offenen Untergruppen von A_K von endlichem Index (S. 234). Die Aussage (3) reduziert den Beweis auf eine geeignete kofinale Klasse von Untergruppen, für welche man die gesuchte Erweiterung direkt angeben kann. Anders als beim Reziprozitätsgesetz ist diese Abstraktion aber wenig erhellend, und mit [N1] verzichten wir auf sie.

Auf eine wenig beachtete Qualität dieses abstrakten Zugangs soll noch hingewiesen werden. Es ist oft bemerkt worden, daß die Klassenkörpertheorie wesentlich multiplikativ ist; Potenzen, Normen und Indices in multiplikativen Gruppen spielen die Hauptrolle.

Diese zunächst eher „philosophische“ Tatsache findet einen prägnanten und streng mathematischen Ausdruck darin, daß eine Klassenformation lediglich einen G-Modul verlangt, also eine Struktur mit nur *einer* Operation, die nicht a priori in „umgebende“ Ringstrukturen eingebettet ist. Das ist zu berücksichtigen, wenn man über eine Ausdehnung der Theorie auf allgemeinere Erweiterungen L/K nachdenkt. Es ist auch ein Hinweis darauf, welch kleinen Ausschnitt die Klassenkörpertheorie, bei aller Glorie, im Gesamtreich der algebraischen Zahlen bildet.

4.3 Lokale Klassenkörpertheorie

4.3.1 Sei jetzt K ein lokaler Körper der Zahlentheorie, also eine endliche Erweiterung eines $\mathbb{Q}_p$. Wir bezeichnen mit U_K die Einheitengruppe, mit π ein beliebiges Primelement und mit ν die normierte Exponentenbewertung von K und beginnen mit einer Klasse von Erweiterungen L/K, die im allgemeinen Rahmen als fast trivial erscheinen muß, aber doch paradigmatisch ist, nämlich den unverzweigten. Drei Standardtatsachen sind hier einschlägig: (1) eine unverzweigte Erweiterung L/K ist zyklisch, und $\mathrm{Gal}(L/K)$ wird vom Frobeniusautomorphismus σ erzeugt, (2) jedes $x \in U_K$ ist Norm aus L, damit Norm eines $y \in U_L$, (3) für jeden Grad f existiert genau ein solches L mit $[L : K] = f$, erzeugt durch Adjunktion einer (q^f-1)-ten Einheitswurzel, wo q die Elementanzahl des Restklassenkörpers von K bezeichne. Da π auch ein Primelement von L ist, folgt mit (2), daß $N(L^\times) = \langle\pi^f\rangle \times U_K$ und damit $K^\times : N(L^\times) =$ zyklisch von der Ordnung f ist. Die Abbildung

$$K^\times \to \mathrm{Gal}(L/K)\,,\ x \to \sigma^{\nu(x)}$$

induziert daher einen Isomorphismus $K^\times / N(L^\times) \to \mathrm{Gal}(L/K)$. Das ist das Reziprozitätsgesetz, und der Existenzsatz ist die Feststellung (3). Allerdings haben wir die unverzweigten L/K damit noch nicht in den Rahmen der Klassenformationen gestellt (siehe dazu [N1], S.135ff); dazu müßte man auf die Kohomologie eingehen, die Invariantenabbildung angeben und die Topologie von $K^\times$ vergröbern: offen sollen nur die U_K enthaltenden Untergruppen sein (offenbar ist diese Topologie nicht hausdorffsch). Man sieht daraus, daß die lokale Klassenkörpertheorie wesentlich mit der Verzweigung zu tun hat; zum Glück ist deren schwierigster Teil, das Verhalten der höheren Verzweigungsgruppen, für die zentralen Aussagen nicht erforderlich.

Wir wenden uns jetzt dem allgemeinen Fall zu; wie oben schon bemerkt, ist die Formation gegeben durch

$$G = \mathrm{Gal}(K^{alg}/K)\ ,\ A = (K^{alg})^\times \ .$$

Das erste Axiom der Klassenformationen, $H^1(L/K) = H^1(\mathrm{Gal}(L/K), L^\times) = 1$ ist der oben schon benutzte, elementar zu beweisende Satz „Hilbert 90“. Die ganze Schwierigkeit steckt im zweiten Axiom, der Existenz eines Isomorphismus $\mathrm{inv}(L/K)$:

$H^2(L/K) \rightarrow 1/[L:K]\ \mathbb{Z} \mod \mathbb{Z}$ durch eine Abbildung inv, die noch weitere Bedingungen erfüllen muß. Während dies für unverzweigte L/K dank der Auszeichnung und des Wohlverhaltens des Frobeniusautomorphismus nicht schwer ist (es ist nichts anderes als das der globalen Artinabbildung $\varphi_{L/K}$ „im Kleinen"), kann der allgemeine Fall nur durch einen Umweg bewältigt werden, nämlich durch Einbettung der $H^2(L/K)$ in die Brauergruppe $H^2(K)$ durch die injektive Inflation. Der erste Schritt ist der Beweis von $|H^2(L/K)| \mid [L:K]$, die kohomologische Version von Ungleichung A (für zyklische L/K geht sie in diese über, weil dann $H^2(L/K) = H^0(L/K) = K^\times : N(L^\times)$ ist). Für L/K zyklisch von Primzahlgrad folgt dies aus der Bestimmung des Index $K^\times : (K^\times)^m$ und einer Formel für die Herbrandquotienten; der allgemeine Fall ergibt sich induktiv, wobei nur der kohomologische Mechanismus gebraucht wird. Damit läßt sich nun zeigen: ist L/K normal und L'/K die unverzweigte Erweiterung vom gleichen Grad, so haben $H^2(L/K)$ und $H^2(L'/K)$ dasselbe Bild in $H^2(K)$, und die Invariantenabbildung für $H^2(L'/K)$ läßt sich einfach auf $H^2(L/K)$ übertragen. Beim Beweis der Aussagen (a) und (b) aus dem Axiom für die Invariantenabbildung wird nun wieder der kohomologische Apparat gefordert. Damit erhält man das Reziprozitätsgesetz, einen kanonischen Isomorphismus

$$(\ \ , L/K) : \ K^\times / N(L^\times) \ \rightarrow \ \mathrm{Gal}(L/K)^{ab}$$

für abelsche Erweiterungen L/K, die *lokale Artinabbildung* oder das *lokale Normrestsymbol*. Man beachte, daß die „natürliche" Definition im Falle unverzweigter L/K jetzt ein nichttrivialer Satz wird ([N1], S.142)! Zu den allgemeinen Folgerungen aus dem Reziprozitätsgesetz ergibt sich noch, als „Nebenprodukt", eine Bestimmung der Brauergruppe $H^2(K)$, nämlich ein Isomorphismus

$$\mathrm{inv}: \ H^2(K) \ \rightarrow \ \mathbb{Q}/\mathbb{Z}\ ;$$

man braucht nur zu bemerken, daß sich $\mathbb{Q}/\mathbb{Z}$ als Vereinigung („direkter Limes") der Gruppen $[L:K]^{-1}\ \mathbb{Z} \mod \mathbb{Z}$ schreiben läßt, ebenso wie $H^2(K)$ als Limes der $H^2(L/K)$. Den Existenzsatz kann man wie im klassischen Fall durch Reduktion auf Kummererweiterungen und dort durch explizite Konstruktion beweisen (die hier im Lokalen natürlich sehr viel einfacher ist); darauf brauchen wir nicht mehr einzugehen.

4.3.2 Die Theorie von Lubin-Tate, eine faszinierende Zauberei mit Polynomen und Potenzreihen, die sich am besten als verallgemeinerte Kreisteilung charakterisieren läßt, soll hier wenigstens im Groben beschrieben werden; einmal wegen ihres systematischen Stellenwerts, zum andern, weil sie später (4.4.3) angewandt wird. Sei R der Bewertungsring (oder Ganzheitsbereich) von K; wir gehen aus von Polynomen der Form

$$f(Z) \ = \ \pi Z + \ldots + \ Z^q + \ldots \ \ \in \ R[Z]\ ,$$

wobei die Punkte Z-Potenzen mit durch π teilbaren Koeffizienten bedeuten sollen (man könnte sogar Potenzreihen dieser Form nehmen). Es bezeichne $f^{(n)}(Z)$ das durch n-maliges Einsetzen von f in sich selbst erhaltene Polynom, also $f^{(n+1)}(Z) = f(f^{(n)}(Z))$, $N(f,n)$ seine Nullstellenmenge und $L(f,n)$ den davon erzeugten Erweiterungskörper von K. Wegen $Z \mid f(Z)$ ist $N(f,n) \subset N(f, n+1)$ und damit auch $L(f,n) \subset L(f, n+1)$. Das primordiale Beispiel ist (mit $K = \mathbb{Q}_p$) das Polynom

$$f(Z) = (1+Z)^p - 1 = pZ + \ldots + Z^p ,$$

dessen Nullstellen die Größen $\zeta - 1$ sind, wo ζ die p-ten Einheitswurzeln durchläuft; $L(f,n)$ ist hier der Körper der p^n – ten Einheitswurzeln über $\mathbb{Q}_p$.

Den Schlüssel zu den folgenden Hauptresultaten bildet die Tatsache, daß die Menge $N(f,n)$ eine (explizit angebbare) R-Modulstruktur trägt, derart daß $N(f,n) \simeq R / \pi^n R$ und damit die Automorphismengruppe bezüglich dieser Struktur isomorph zu $U_K/U_K^{(n)}$ ist ($U_K^{(n)}$ = n-te Einseinheitengruppe); $N(f,n)$ ist also so etwas wie eine (affine) Liesche Gruppe. Diese Operation und die Addition von $N(f,n)$ werden vermittelt durch Potenzreihen, deren Gesamtheit eine *formale Gruppe* konstituiert; darauf können wir nicht näher eingehen. Die Hauptresultate sind nun:

(1) Der Körper $L(f,n)$ hängt nur von π ab, nicht von der Wahl eines f wie oben (!) ; er ist eine abelsche, rein verzweigte Erweiterung von K vom Grad $q^{n-1}(q-1)$, und es ist $Gal(L(f,n)/K) \simeq U_K/U_K^{(n)}$, wobei der Isomorphismus durch die oben erwähnte Operation von U_K gegeben wird.

(2) Bezeichnet s den Homomorphismus $U_K \to Gal(L(f,n)/K)$, so ist $s(u^{-1}) = (u, L(f,n)/K)$, das Normrestsymbol. (Da π hier Norm ist, ist das Normrestsymbol damit vollständig beschrieben.)

(3) $L(\pi) := \bigcup_n L(f,n)$ ist eine maximale rein verzweigte abelsche Erweiterung von K. Bezeichnet T die maximale unverzweigte Erweiterung, so ist das Kompositum $T\,L(\pi) = K^{ab}$.

Man beachte, daß $L(\pi)$ selbst von π abhängt. Die Theorie von Lubin-Tate ermöglicht also (zusammen mit den leicht zu handhabenden unverzweigten Erweiterungen) eine explizite Erzeugung der maximalen abelschen Erweiterung von K, was für Zahlkörper immer noch der „Kroneckersche Jugendtraum“ bleibt, erfüllt nur für den rationalen Grundkörper und imaginär-quadratische K ; darüber hinaus gibt sie eine explizite Beschreibung der Normrestsymbole. Dieses glatte und überaus befriedigende Resultat legt den Gedanken nahe, sozusagen umgekehrt die lokale Klassenkörpertheorie durch die Lubin-Tate-Theorie aufzubauen. Mühe macht dabei der Beweis der Gleichung $T\,L(\pi) = K^{ab}$ (das ist nicht schwer, wenn man den Existenzsatz schon hat, weil die Normengruppen der Körper L(f,n) bekannt sind und zusammen mit denen der unverzweigten L/K ein kofinales System offener Untergruppen von endlichem Index liefern); das ganze Programm hat Iwasawa in seinem Buch [Iw] durchgeführt; siehe auch [Mi], Ch.I. Der Vollständigkeit halber soll auch die Methode von Hazewinkel [Haz] erwähnt werden; und natürlich darf das klassische Buch über lokale Körper nicht fehlen, Serres „Corps locaux" [SC] (mit der kohomologischen Theorie). Iwasawa diskutiert S.146ff die logischen Beziehungen zwischen den verschiedenen Zugängen, für eine neuere Diskussion siehe [FV], S.162ff.

4.3.3 Was die unendlichen (archimedischen) Stellen der Zahlkörper betrifft, so tritt bei den Komplettierungen nur ein einziger nichttrivialer Fall auf, $K_p = \mathbb{R}$ und $L_P = \mathbb{C}$, und dieser ist fast trivial, denn es gibt nur eine einzige Möglichkeit für reelle $x \neq 0$ ein Normrestsymbol in $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ zu definieren, nämlich durch

$$(x, \mathbb{C}/\mathbb{R})(i) = i^{\,\mathrm{sgn}(x)} .$$

Daß damit ein Reziprozitätsgesetz gilt, bedarf keiner Erläuterung, und ein Existenzproblem besteht nicht.

4.4 Globale Klassenkörpertheorie

4.4.1 Sei jetzt K ein Zahlkörper. Die ihm zugeordnete Formation besteht aus der absoluten Galoisgruppe von K und dem direkten Limes der Idelklassengruppen C(L) für beliebige L/K . Für das Reziprozitätsgesetz muß gezeigt werden: (1) $H^1(G, C(L)) = 1$ für normale L/K , G = Gal(L/K) ; (2) die Existenz einer Invariantenabbildung, eines Isomorphismus $H^2(G, C(L)) \longrightarrow [L:K]^{-1}\, \mathbb{Z} \bmod \mathbb{Z}$ mit dem verlangten Wohlverhalten.

Wir gehen zunächst ein auf die Kohomologie der Idelgruppe (L/K normal, G = Gal(L/K)) und gruppieren wieder die Komponenten der L-Idele nach den Primteilern P eines festen p von K. Die Tatsache, daß der G-Modul $\prod_{P|p} L_P^{\times}$ von dem D(P)-Modul $L_P^{\times}$ induziert wird (P|p beliebig), münzt sich kohomologisch um in einen Isomorphismus $H^q(G, \prod_{P|p} L_P^{\times}) \cong H^q(D(P), L_P^{\times})$, alle q (Lemma von Shapiro, siehe [N1], S.68). Für unverzweigte p ist weiter $H^q(D(P), U_P) = 1$, alle q, eine Verallgemeinerung der bekannten Tatsache, daß in diesem Fall jede Einheit Norm ist (der Fall q = 0). Dieser Beweis ist nicht "formal", er benutzt die Arithmetik der höheren Einseinheitengruppen ([N1], S.137); weil hier D(P) zyklisch ist, braucht man nur q = 0, 1 zu behandeln.

Sei nun S eine endliche Menge von Stellen von K , die alle Verzweigung enthält; ebenfalls mit S bezeichnen wir die Menge der Primteiler P der $p \in S$. Das bisher Gezeigte liefert

$$H^q(G, J^S(L)) = \prod_{p\in S} H^q(D(P), L_P^{\times}) \;,\quad H^q(G, J(L)) = \bigoplus_p H^q(D(P), L_P^{\times}) \,,$$

wobei für jedes p ein $P|p$ zu wählen ist. Damit ist für die Kohomologie der Idelgruppen ein glattes Lokal-Prinzip bewiesen; insbesondere für $q = 0$ ein „Normensatz für Idele": ein Idel von K ist genau dann eine Norm eines Idels von L, wenn dies überall lokal der Fall ist. Für $q = 1$ erhält man $H^1(G, J(L)) = \oplus_p H^1(D(P), L_P^\times) = 1$ mit Hilbert 90. Für Türme $N/L/K$ (alles galoissch) erhält man daraus die exakte Inf-Res-Sequenz

$$1 \to H^2(G(L/K), J(L)) \xrightarrow[\text{inf}]{} H^2(G(N/K), J(N)) \xrightarrow[\text{res}]{} H^2(G(N/L), J(N))$$

und insbesondere die Injektivität der Inflation, die es erlaubt, alle Gruppen $H^2(G(L/K), J(L))$ in einem direkten Limes zusammenzufassen, ganz ebenso wie dies für die $H^2(G(L/K), L^\times)$ möglich ist, wodurch sich die Brauergruppe ergibt. Es genügt bei beiden Limesbildungen sogar, nur die zyklischen zyklotomischen Erweiterungen zu berücksichtigen, in Analogie zu der Tatsache, daß die Brauergruppe sich im Lokalen als Limes der $H^2(G(L/K), L^\times)$ für die unverzweigten L/K schreiben läßt. Der Beweis dafür ergibt sich mittels eines Hilfssatzes, den man als „schwaches Artinsches Lemma" bezeichnen kann, die Existenz zyklischer zyklotomischer L/K mit genügend teilbaren lokalen Graden an endlich vielen Stellen, aber ohne Bedingungen an die Primzerlegung; das folgt aus Standardinformationen über Einheitswurzelkörper ([N1], S.213). Den Rest besorgt der kohomologische Apparat.

4.4.2 Jetzt wenden wir uns zur Idelklassengruppe. Der Beweis von $H^1(G, C(L)) = 1$ erfolgt in gewisser Weise „indirekt". Wir nehmen zunächst an, daß L/K zyklisch von Primzahlgrad p mit der Gruppe G ist. Der erste Schritt ist der Beweis von Ungleichung B in der Form

$$h(C(L)) = |H^0(G, C(L))| \,/\, |H^1(G, C(L))| = p\,.$$

Die Beweisstrategie ist: wählt man S mit $J(L) = J^S(L)\, L^\times$, ergibt sich

$$C(L) = J^S(L)\, L^\times / L^\times = J^S(L) / J^S(L) \cap L^\times$$

und dieselbe Gleichung für die Herbrandquotienten dieser Gruppen. Eine Formel für $h(J^S(L))$ergibt sich aus der Lokalisierung der Kohomologie und der lokalen Klassenkörpertheorie. Die Gruppe $J^S(L) \cap L^\times$ ist die Gruppe der S-Einheiten in L, ihre Fixgruppe unter G die der S-Einheiten in K; die Berechnung des Herbrandquotienten geht wie in 1.6. Alternativ kann man eine Formel von Chevalley für die Quotienten verwenden, die auf diesen Fall zugeschnitten ist (so in [N1], S. 219). Setzt man beides zusammen, folgt die behauptete Gleichung.

Als Folgerungen erhält man: In einer normalen Erweiterung gibt es stets unendlich viele Primideale, die nicht voll zerfallen; in zyklischen Erweiterungen von Primzahlpotenzgrad sogar unendlich viele träge. (Die erste Aussage, den Zerfällungssatz, haben wir schon als fast triviale Konsequenz aus dem Polverhalten der Zetafunktionen kennengelernt, sie ist aber auch, wie die zweite, ein Spezialfall des Dichtigkeitssatzes von Frobenius, der ohne Klassenkörpertheorie beweisbar ist; siehe [J], S.134.)

Der nächste Schritt ist nun Ungleichung A in der Form $|H^0(G, C(L))| = |C(K) : N(C(L))| \leq p$, zunächst noch mit der zusätzlichen Annahme, daß K die p-ten Einheitswurzeln enthält, so daß Kummertheorie zur Anwendung kommt. Obwohl das Problem damit auf den einfachsten denkbaren Fall reduziert ist, liegt hier der „harte Kern“ dieses Zugangs. In [N1] wird, neben umfangreichen Indexberechnungen, eine komplizierte Hilfskonstruktion herangezogen, die wir nicht en detail beschreiben können; in [AT] wird der Ungleichung ein eigenes Kapitel gewidmet (Ch. 6). Die Indexberechnungen sind hier eng verwandt mit denen, die in [J] beim klassischen Zugang zum Beweis des Existenzsatzes benutzt werden.

Aus den beiden Ungleichungen zusammen folgt jetzt $|C(K) : N(C(L))| = |Gal(L/K)| = p$ und damit sogar ein Isomorphismus beider Gruppen, aber kein „kanonischer“; die Rechnungen ergeben nur die Gleichung, keine Abbildung zwischen den Gruppen; man ist hier sozusagen noch auf der „Prä-Artin-Stufe“. Weiter folgt $H^1(G, C(L)) = 1$, zunächst nur in dem zuletzt betrachteten primzyklischen Fall. Die Ausdehnung auf allgemeine normale L/K gelingt mit Standardargumenten durch Induktion nach der Gruppenordnung ([N1], S.229). Damit ist unsere Formation als Körperformation erwiesen. Für zyklische G ist übrigens

$$H^{-1}(G, C(L)) = H^1(G, C(L)) = 1 ,$$

und daraus folgt fast unmittelbar der Hassesche Normensatz: die exakte Sequenz

$$1 \to L^\times \to J(L) \to C(L) \to 1$$

liefert als Teil der Kohomologiesequenz die Exaktheit von

$$1 = H^{-1}(G, C(L)) \to H^0(G, L^\times) \to H^0(G, J(L)) ,$$

und das ist gerade die Aussage des Normensatzes: ein $a \in K$ ist Norm aus L *genau* dann, wenn dies überall lokal der Fall ist. (Die naheliegende Vermutung, daß dies für abelsche L/K richtig bleibt, erweist sich als falsch, schon bei biquadratischen Erweiterungen.)

Als weitere Folgerung ergibt sich, daß für beliebige normale L/K die Ordnung von $H^2(G, C(L))$ den Grad $[L : K]$ teilt; der Beweis geschieht durch Induktion nach dem Grad. Ein rein kohomologischer Satz erlaubt die Reduktion auf p-Gruppen, und dort kann der Fall eines Primzahlgrades als Induktionsanfang dienen, weil eine p-Gruppe stets einen Normalteiler vom Index p hat ([N1], S.231).

4.4.3 Zum Reziprozitätsgesetz fehlt jetzt noch eine Invariantenabbildung. Eine solche läßt sich zunächst für Elemente aus $H^2(G, J(L)) = \bigoplus_p H^2(D(P), L_P^\times)$ einfach durch Summenbildung definieren, da für die Elemente der $H^2(D(P), L_P^\times)$ schon eine Invariantenabbildung mit Werten in $[L_P : K_p]^{-1}\,\mathbb{Z} + \mathbb{Z} \subset [L{:}K]^{-1}\,\mathbb{Z} + \mathbb{Z}$ definiert ist und in der direkten Summe rechts fast alle Terme = 0 sind (wir setzen also eine Art Lokal-Global-Prinzip per definitionem ein). Die Sequenz

$$1 \;\to\; L^\times \;\to\; J(L) \;\to\; C(L) \;\to\; 1$$

liefert wegen $H^1(G, J(L)) = 1$ die exakte Kohomologieseqenz

$$1 \;\to\; H^2(G,\, L^\times) \;\to\; H^2(G, J(L)) \;\underset{j}{\to}\; H^2(G, C(L))$$

und wir können zumindest für die Elemente von im j eine Invariantenabbildung definieren, wenn die oben definierte idelische Invariantenabbildung auf $H^2(G, L^\times)$ verschwindet; das bedeutet eine „Summenformel“ für die lokalen Invarianten. Der Beweis davon erfordert eine Reihe von Schritten, die näher beschrieben werden sollen, weil wir uns hier im Zentrum der Sachen befinden:

(1) Der Mechanismus erlaubt zuerst eine Reduktion auf $K = \mathbb{Q}$: man nehme eine absolut Galoissche Erweiterung N/L und wende erst inf an (für $L/K \to N/K$), sodann cores (für $N/K) \to N/\mathbb{Q})$; das ist übrigens dasselbe Verfahren, mit dem man zeigt, daß jede Artinsche L-Funktion als eine solche über $\mathbb{Q}$ aufgefaßt werden kann, nur daß man die Corestriktion durch die Induktion ersetzen muß. Aus 4.4.1 folgt weiter, daß man L als zyklische zyklotomische Erweiterung annehmen darf.

(2) Wir ziehen nun die Formel (3) heran, welche – schon im abstrakten Rahmen der Klassenformationen – die Invariantenabildung mit dem Normrestsymbol verbindet. Ein solches, mit einer entsprechenden Formel, haben wir bis jetzt nur im Lokalen. Wir *definieren* jetzt ein globales idelisches Symbol, das sich dann im Nachhinein als das „richtige“, nämlich zum Reziprozitätsisomorphismus inverse herausstellt, nämlich

$$((x_p),\ L/\mathbb{Q}) \;=\; \Pi_p\,(x_p\ , L_P/\mathbb{Q}_p) \;\in\; \mathrm{Gal}(L/\mathbb{Q})\,;$$

man beachte, daß fast alle $L_P/\mathbb{Q}_p$ unverzweigt und fast alle x_p Einheiten sind, so daß rechts nur endlich viele Faktoren stehen, und daß die Galoisgruppe kommutativ ist, so daß es auf ihre Reihenfolge nicht ankommt. Da wir die globale Invariantenabbildung genau analog, nämlich durch Summenbildung über die lokalen Invarianten definiert haben, ist plausibel, daß dieselbe Formel, welche lokale Invarianten und Symbole verbindet, auch hier gilt ([N1], S.237). Es ergibt sich aus ihr, daß es genügt, $(x,\ L/\mathbb{Q}) = 1$ für Hauptidele x zu beweisen. Es genügt weiter, $L = \mathbb{Q}(\zeta)$ als vollen Kreiskörper anzunehmen, und weiter die Ordnung von ζ als Potenz p^r einer Primzahl p.

(3) Im lokalen unverzweigten Fall, also für alle endlichen Stellen $\neq p$, sind die Normrestsymbole wohlbekannt (wir haben sie eingangs beschrieben); die kritische Stelle ist p, denn $\mathbb{Q}_p(\zeta) / \mathbb{Q}_p$ ist rein verzweigt. Da die Norm von $1 - \zeta$ ein Primelement ist, genügt es, das Normrestsymbol für Einheiten u anzugeben. Es gilt nun

$$(*) \qquad (u^{-1}, \mathbb{Q}_p(\zeta) / \mathbb{Q}_p) = \zeta^u .$$

(Die Potenz ist so zu verstehen: man wähle eine ganze Zahl m mit $u \equiv m \bmod p^r$ und setze $\zeta^u = \zeta^m$.) Das zu beweisen, ist außerordentlich mühsam und auf direktem Wege (bisher) nur mittels transzendenter Methoden gelungen (siehe aber [Lo2], S.229 für einen „elementaren“ Beweis im zahmen Fall $r = 1$). In [N1] wird dazu die Theorie von Lubin-Tate verwendet (die noch nicht existierte, als das in [AT] referierte Seminar stattfand). Setzt man nun alle Faktoren zusammen und benutzt noch die Produktformel für die Absolutbeträge, erhält man die gewünschte Gleichung

$$\Pi_p (x , L_P /\mathbb{Q}_p) = 1 \quad (x \neq 0) .$$

Die allgemeine, von Hasse stammende *Produktformel für die lokalen Symbole*, also die Gleichung

$$\Pi_p (x , L_P /K_p) = 1 , \quad L/K \text{ abelsch} , \; x \in K^\times ,$$

kann man nun auch direkt beweisen ([J], S. 189, wobei die klassischen analytischen Methoden eingehen, oder mit [Lo2], S. 224 arithmetisch-algebraisch (s.u. 5.3.4)) und erhält dann ebenfalls die Formel (*) , indem man die zuletzt beschriebene Rechnung rückwärts liest: wenn man in einem Produkt alle Faktoren bis auf einen kennt, aber a priori weiß, daß das Produkt = 1 ist, hat man auch den verbleibenden Faktor.

4.4.4 Damit hat man nun eine Invariantenabbildung für die Elemente von $H^2(G, C(L))$, die im Bild von

$$j: \; H^2(G, J(L)) \;\to\; H^2(G, C(L))$$

liegen. Man stößt nun noch auf das Problem, daß diese Abbildung i.A. nicht surjektiv ist (hinreichend wäre $H^3(G, L^\times) = 0$, aber das ist nicht immer der Fall.). Im zyklischen Fall folgt die Surjektivität von

$$\text{inv}: \; H^2(G, J(L)) \;\to\; [L:K]^{-1} \mathbb{Z} + \mathbb{Z}$$

leicht aus dem lokalen Reziprozitätsgesetz und der Tatsache, daß bei zyklischen Erweiterungen von Primzahlpotenzgrad dieser Grad auch lokal angenommen wird (s.o. 4.4.2); genauer hat man eine exakte Sequenz

$$1 \quad \rightarrow \quad H^2(G,\ L^\times) \ \rightarrow \quad H^2(G, J(L)) \ \rightarrow \quad [L:K]^{-1}\,\mathbb{Z} + \mathbb{Z} \ \rightarrow \ 1 \ ,$$

([N1], S.241) die zusammen mit $|\,H^2(G, C(L))\,| \;\big|\; [L : K]$ die Surjektivität von j zur Folge hat. Die Ausdehnung der Invariantenabbildung auf den allgemeinen Fall gelingt nun mit dem Verfahren, das schon lokal angewandt wurde: dort hatten wir den allgemeinen Fall auf den unverzweigten zurückgeführt, hier spielen die zyklischen Erweiterungen die Rolle der unverzweigten (was erstaunlich ist, denn lokal existiert zu jedem Grad genau *eine* unverzweigte Erweiterung, global aber existieren unendlich viele zyklische). Entscheidend ist dabei die Gleichung $\mathrm{inv}(N/L)\ \mathrm{res} = [L : K]\ \mathrm{inv}(N/K)$ in Türmen $N/L/K$, die zeigt, daß die linke Seite bei festem N/K eben nur vom Grad $[L : K]$ abhängt. Gleichzeitig ergibt sich die Surjektivität von $\mathrm{inv}\colon H^2(G, C(L)) \rightarrow [L:K]^{-1}\,\mathbb{Z} + \mathbb{Z}$, und die Bijektivität folgt aus $|H^2(G, C(L))| \;\big|\; [L:K]$. Das Wohlverhalten der Invariantenabbildung schließlich folgt rein kohomologisch aus dem der Idelinvarianten und dieses aus dem der lokalen Komponenten. Damit ist unsere Formation $(\mathrm{Gal}(K^{alg}/K)$, absolute Idelklassengruppe $= \mathrm{lim.ind.}_{L/K}\ C(L))$ als Klassenformation erwiesen, und es folgt das Reziprozitätsgesetz wie auch die Tatsache, daß das oben nur für $K = \mathbb{Q}$ definierte Symbol

$$((\,x_p\,)\,,\ L/K\,) \ = \ \Pi_p\,(\,x_p\ , L_P/K_p\,) \ \in\ \mathrm{Gal}(L/K)$$

das „richtige“ Normrestsymbol ist. Daraus ergibt sich unmittelbar eine sehr durchsichtige Kompatibilität von lokalen und globalen Symbolen: die Abbildung $i(p)\colon K_p^\times \rightarrow J(K)$, die ein $x_p \in K_p^\times$ auf das Idel mit den Komponenten x_p an der Stelle p und 1 sonst abbildet, steigt ab zu einer *Einbettung* $i(p)\colon K_p^\times \rightarrow C(K)$, und man erhält ein kommutatives Diagramm

$$\begin{array}{ccc} K_p^\times & \longrightarrow & \mathrm{Gal}(\,L_P/K_p\,) \\ {\scriptstyle i(p)}\downarrow & & \downarrow \\ C(K) & \longrightarrow & \mathrm{Gal}(L/K)\ , \end{array}$$

in dem die waagerechten Pfeile die Normrestsymbole sind. Der Existenzsatz wird in schon bekannter Weise durch Reduktion auf den Kummerschen Fall und direkte Konstruktion bewiesen.

Vergleicht man den eben beschriebenen Zugang mit dem klassischen idealtheoretischen, so zeigt sich ein gewisses Dilemma: das (globale) Normrestsymbol hat eine natürliche Definition als Produkt der lokalen Symbole, diese aber sind (außer im unverzweigten Fall) nur auf Umwegen zu bekommen (wir werden in den nächsten drei Abschnitten noch weitere kennenlernen). Die Artinabbildung dagegen hat eine natürliche explizite Definition, aber sozusagen auf Kosten der verzweigten Stellen, die ausgeschlossen bleiben.

4.4.5 Wie schon erwähnt, ist der Aufbau in [AT] etwas anders. Zum Beweis des Reziprozitätsgesetzes wird auf elementarem Wege ein Homomorphismus

$$C(\mathbb{Q}) \;\longrightarrow\; \mathrm{Gal}(\mathbb{Q}^{cyc}/\mathbb{Q}) \;,\quad \mathbb{Q}^{cyc} = \text{maximale zyklotomische Erweiterung von } \mathbb{Q}$$

konstruiert, der sich dann als die „richtige“ universelle Normrestabbildung herausstellt. Fassen wir ihn als Abbildung auf $J(\mathbb{Q})$ mit dem Kern $\mathbb{Q}^{\times}$ auf, erhalten wir, wie oben beschrieben, das Verschwinden der Invariantenabbildung auf $H^2(G, L^{\times})$ auch im allgemeinen Fall. Die Pointe ist, daß sich das so schwierig zu bestimmende Normrestsymbol im verzweigten lokalen Fall hier auf verblüffend einfache Weise ergibt – nur weiß man zunächst noch nicht, daß es sich wirklich um jenes Symbol handelt! Hier ist die Konstruktion: bekanntlich ist

$$\mathrm{Gal}(\mathbb{Q}^{cyc}/\mathbb{Q}) = \text{lim.proj.}\,(\mathbb{Z}/n\mathbb{Z})^{\times} = \prod_p \mathbb{Z}_p^{\times} =: U\,.$$

Die Operation von U auf den Einheitswurzeln ζ ist eine Ausdehnung der in 4.4.3 beschriebenen: sei m die Ordnung von ζ; zu gegebenem $u = (u_p)$ wähle man eine natürliche Zahl n mit $n \equiv u_p \bmod p^r$ für die Primzahlpotenzen in m (Chinesischer Restsatz) und setze $\zeta^u = \zeta^n$.

Wir haben aber auch

$$J(\mathbb{Q}) = \mathbb{Q}^{\times}\,(\mathbb{R}_+ \times U)$$

(man ziehe aus den endlichen Komponenten die p-Potenzen und aus der reellen das Vorzeichen nach vorn); das äußere Produkt ist ebenfalls direkt, weil 1 die einzige positive rationale Zahl ist, die an allen Stellen Einheit ist. In trivialer Weise ersieht man so die Existenz eines surjektiven Homomorphismus $s\colon C(\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}^{cyc}/\mathbb{Q})$ mit dem Kern $\mathbb{R}_+$ (dieser ist übrigens die Zusammenhangskomponente der Eins von $C(\mathbb{Q})$). Um die Operation eines Idels (via s) auf den Einheitswurzeln zu beschreiben, muß man dieses als Produkt entsprechend der obigen Zerlegung darstellen und dann das Inverse der U-Komponente verwenden (um an den unverzweigten Stellen den Frobenius und nicht sein Inverses zu erhalten). Man erkennt den Mechanismus am Beispiel eines Idels mit allen Komponenten = 1 außer an der endlichen Stelle p : $(x_p) = (1, p^r u_p, 1, 1, \ldots)$ (die erste Stelle sei die reelle Komponente). Die drei Faktoren sind

$$(p^r, p^r, \ldots) \in \mathbb{Q}^{\times}\,,\quad (p^{-r}, 1, \ldots) \in \mathbb{R}_+ \text{ und } (1, u_p, p^{-r}, p^{-r}, \ldots) \in U\,.$$

Daß man damit die „richtige“ Normrestabbildung hat, folgt mittels der lokalen Klassenkörpertheorie und Ungleichung A ([AT], S. 46ff).

Etwas anders verläuft auch der Beweis des Existenzsatzes. Wir definieren zunächst das *universelle Normrestsymbol*: die Gleichung $(c, L/K) = (c, N/K)\,\big|\,L$ für abelsche

$N_{L/K}$ besagt einfach, daß die Elemente $(c, L/K)$ bei festem c ein Element des projektiven Limes aller $Gal(L/K)$, L/K abelsch konstituieren; damit erhält man einen Homomorphismus

$$\omega := (\ , K) : C(K) \quad \to \quad Gal(K^{ab}/K) \ ,$$

der leicht als stetig nachzuweisen ist und dessen Kern $D(K)$ aus den universellen Normen besteht, also den Idelklassen, die Normen aus jedem abelschen (und damit jedem Galoisschen) L/K sind. Für die Surjektivität beachte man zunächst, daß das Bild jedenfalls dicht ist, weil ω auf jeder „Schicht" L/K surjektiv ist. Jetzt schreibe man $C(K) = C^1(K) \times \mathbb{R}_+^\times$ (s.o. 2.1) und beachte, daß $\mathbb{R}_+^\times$ als dividierbare Gruppe im Kern von ω liegt (eine dividierbare Gruppe kann in eine proendliche nur trivial abgebildet werden), also ist $\omega(C(K)) = \omega(C^1(K))$. Aber $C^1(K)$ ist kompakt, das Bild also abgeschlossen; daraus folgt die Surjektivität. Im Anschluß an den Beweis von Ungleichung A wird nun in [AT], S.37 gezeigt, daß der *ganze* Kern $D(K)$ von ω eine dividierbare Gruppe ist. Damit und mit dem Reziprozitätsgesetz ergibt sich ein *sehr* kurzer Beweis des Existenzsatzes ([AT], S.72): sei H eine offene Untergruppe von $C(K)$ von endlichem Index h ; H enthält $D(K)$, weil andernfalls der Index nicht endlich sein könnte. Der Fixkörper L von $\omega(H)$ ist eine endliche abelsche Erweiterung von K vom Grad h , und H ist im Kern der Normrestabbildung $(\ , L/K)$ enthalten. Nach dem Reziprozitätsgesetz ist dieser Kern genau gleich $N(C(L))$ und hat denselben Index h in $C(K)$, also ist $H = N(C(L))$. Man sieht allerdings, daß es sich um einen reinen Existenzbeweis handelt, während der traditionelle Zugang wenigstens im Kummerschen Fall eine Konstruktion gibt. In [N1], S.280 wird die Dividierbarkeit von $D(K)$ aus dem Beweis des Existenzsatzes abgeleitet. Es könnte also scheinen, als seien die beiden Aussagen (im üblichen Sinne) äquivalent; sie sind das allerdings erst auf dem Boden sehr weitgehender Vorarbeiten zum Existenzsatz.

Adnote zu $D(K)$: der Kern des universellen Normrestsymbols auf der Idelebene $J(K)$ ist leicht zu bestimmen und ist uns in 3.1 schon begegnet, nämlich die Gruppe $(\mathbb{R}_+)^r \times (\mathbb{C}^\times)^s$. Die gruppentheoretische Struktur jedoch, die sich durch Übergang in $C(K)$ ergibt, also durch Austeilen der Multiplikation mit Elementen von K, ist nicht leicht zu fassen; man findet das in [AT], Ch.9.

4.5 An dieser Stelle darf Chevalleys Nagoya-Buch ([Ch2]) nicht unerwähnt bleiben, anscheinend die erste in Buchform erschienene Darstellung des kohomologischen Zugangs, wenn es sich auch, wie es im Vorwort heißt, nur um „preparatory notes" und nicht um eine „satisfactory exposition" handelt. Chevalley entwickelt zunächst die Kohomologietheorie auf eigene Weise (und mit ziemlich ungewöhnlichen Notationen, die ich hier in die oben eingeführten übersetzt habe), nämlich nach dem Prinzip der „Dimensionsverschiebung"; siehe [N1], S. 46 für eine Erläuterung dieses Sachverhalts. Wir können das übergehen, denn die entwickelten Resultate entsprechen ungefähr dem, was oben referiert wurde. Die Zahlentheorie beginnt mit der Kohomologie der Idelklassengruppen in Galoisschen Erweiterungen L/K (§§ 11, 12). Es folgt der Beweis von Ungleichung B im primzyklischen Fall, wie oben in der Form $h(C(L)) = p$, mit dem Zerfällungssatz als wichtiger Folgerung, sodann von $H^1(C(L)) = 0$ sowie Ungleichung A für beliebige Galoissche L/K (§§ 13, 14). Dann aber schlägt Chevalley einen eigenen Weg ein. Der Grundgedanke ist, daß man einen Isomorphismus von (endlichen abelschen) Gruppen A, B erhält, wenn man eine nichtentartete Paarung $A \times B^* \to \mathbb{C}^\times$ konstruieren kann. Er definiert nun (L/K beliebig Galoissch, $G = \mathrm{Gal}(L/K)$) eine Paarung

$$C(K) \times G^* \to H^2(G, C(L)) \quad \text{durch} \quad (a, \chi) \to \langle a, \chi \rangle := \hat{a} \cup \delta(\chi) \;;$$

hier bezeichne $\hat{a}$ die Klasse von a in $H^0(G, C(L)) = C(K)/N(C(L))$; vgl. Formel (3) oben. Der Linkskern der Paarung ist der Durchschnitt D aller $N(C(N))$, wo N die zyklischen Teilerweiterungen von L/K durchläuft, der Rechtskern ist trivial (S.76). Daraus folgt: ist L/K zyklisch, so ist $D = N(C(L))$, und man erhält eine nichtentartete Paarung $C(K)/N(C(L)) \times G^* \to H^2(G, C(L))$ und damit schon einen Isomorphismus $C(K)/N(C(L)) \to G^{ab}$, also ein „vorläufiges" Reziprozitätsgesetz im zyklischen Fall; „vorläufig" deswegen, weil der Isomorphismus noch nicht „kanonisch" ist und damit das Wohlverhalten fehlt. Dieses wird dadurch hergestellt, daß der Isomorphismus mittels „kanonischer Klassen" normiert wird. Hierzu führt Chevalley zuerst die Artinabbildung für zyklotomische Erweiterungen von $\mathbb{Q}$ ein (also unser primordiales Beispiel) und erweitert diese zunächst auf Idelklassen und dann zu einem Homomorphismus $(\;\;, Z/K)$: $C(K) \to \mathrm{Gal}(Z/K)$ für zyklotomische Z/K, K beliebig. Dieser ist surjektiv und enthält $N(C(Z))$ in seinem Kern. Für zyklische Z/K ist $H^0(G, C(Z)) = H^2(G, C(Z))$, und da G nun als Faktorgruppe von $H^0(G, C(Z))$ erwiesen ist, folgt mit Ungleichung A die Gleichheit $|G| = |H^0(G, C(Z))|$ (S.81/82).

Jetzt kann die kanonische Klasse für solche Z/K definiert werden: für einen Erzeuger s von G sei $\hat{a}$ das Element von $C(K)/N(C(Z))$ mit $(\hat{a}, Z/K) = s$ und χ der Charakter von G mit $\chi(s) = 1/[Z : K] \bmod \mathbb{Z}$. Dann erweist sich das Element $\langle \hat{a}, \chi \rangle \in H^2(G, C(Z))$ als unabhängig von der Wahl von s (S.82) und wird als die kanonische Klasse $u(Z/K)$ der Erweiterung Z/K definiert. Die Ausdehnung der Definition auf beliebige Galoissche L/K gelingt nun mittels inf und res und einem (schwachen) Artinschen Lemma. Der nächste Paragraph ist dem Wohlverhalten der $u(L/K)$ gewidmet; es ergibt sich dabei auch, daß $H^2(G, C(L))$ zyklisch von der Ordnung $n = [L : K]$ ist und von $u(L/K)$ erzeugt wird. Da wir $H^1(G, C(L)) = 0$ schon wissen und dasselbe natürlich für alle Untergruppen von G gilt, können wir den Satz von Tate anwenden und erhalten die Isomorphie $C(K)/N(C(L)) \to \mathrm{Gal}(L/K)^{ab}$ im allgemeinen Fall (S.86). Schließlich kann die „richtige" Normrestabbildung definiert werden: inv sei diejenige Einbettung $H^2(G, C(L)) \to \mathbb{Q}/\mathbb{Z}$, die $u(L/K)$ auf $(1/n)\,\mathbb{Z} \bmod \mathbb{Z}$ abbildet (von Chevalley mit ρ bezeichnet). Dann ist $\mathrm{inv}(\langle\, , \rangle) : C(K)/N(C(L)) \times G^* \to \mathbb{Q}/\mathbb{Z}$ wieder eine nichtentartete Paarung und liefert damit eine Abbildung $C(K) \to G^{ab}$, welche im zyklischen zyklotomischen Fall mit dem oben definierten $(\;\;, Z/K)$ übereinstimmt und daher auch so bezeichnet werden kann; dies ist die „richtige"

Normrestabbildung, für welche das allgemeine Reziprozitätsgesetz gilt (S.90) und die das gewünschte Wohlverhalten aufweist. Im vorletzten Paragraphen des Buchs leitet Chevalley (wohl als letzter) das lokale Normrestsymbol und Reziprozitätsgesetz aus dem Globalen ab und beweist die Produktformel, im letzten den Existenzsatz (Reduktion auf den Kummerschen Fall und explizite Konstruktion).

4.6 Anhang: Tate 1965

In seinem material- und gedankenreichen Artikel „Global Class Field Theory" [T] hat Tate die Hauptsätze noch einmal dargestellt, aber ohne dabei die Theorie der Klassenformationen zu benutzen; er entwickelt ihre Voraussetzungen, benutzt sie aber nur für weitere Anwendungen ([T], S.197ff). Ausgangspunkt ist eine „rohe Form" („crude form") des Reziprozitätsgesetzes, welche dieses von einer mehr topologischen Seite beleuchtet und den Übergang von den Idealen zu den Idelen durchsichtiger erscheinen läßt. Sei L/K abelsch und S eine Menge von Stellen von K, die alle unendlichen und alle in L/K verzweigten enthält. Für ein $a \in K^\times$ sei $(a) = aO_K$ das von a erzeugte Hauptideal und $(a)^S$ das um die p-Potenzen für die endlichen $p \in S$ gekürzte Ideal; dies ist ein Element der Idealgruppe $I^S(K)$, die von den $p \notin S$ erzeugt wird. Die „Rohform" des Reziprozitätsgesetzes lautet nun:

(RR) *Es existiert* $\varepsilon > 0$ *so daß* $\varphi_{L/K}((a)^S) = 1$, *wenn* $|a-1|_p < \varepsilon$ *für alle* $p \in S$.

Wie früher erklärt, ist die Existenz eines Modulus **m** mit $P^{\mathbf{m}}(K) \subset \ker \varphi_{L/K}$ das Hauptproblem beim klassischen Zugang zum Reziprozitätsgesetz; es ist nicht schwer zu sehen, daß (RR) dazu äquivalent ist (ε entspricht dem Minimum der inversen Normen der beteiligten Primidealpotenzen). Die Aussage hat Analoga in der algebraischen Geometrie; siehe dazu [T], S.168. Tate beweist nun, daß (RR) in idelischer Fassung äquivalent ist zu der folgenden Aussage:

(RR*) *Es existiert ein stetiger Homomorphismus* $\psi: J(K) \to Gal(L/K)$ *mit* $\psi(K^\times) = 1$ *und der Eigenschaft* $\psi(x) = \varphi_{L/K}(j(x)^S)$, $x \in J^S(K)$, *für* S *wie oben*.

Dabei bestimmen ψ (die Normrestabbildung) und $\varphi_{L/K}$ einander wechselseitig, und ψ ist de facto auf $C(K)$ definiert. Die Pointe ist, daß ψ auch die verzweigten Stellen einbeziehen muß, die bei $\varphi_{L/K}$ ausgeschlossen sind; dementsprechend ist die Definition von ψ indirekt und benutzt den Approximationssatz: zu jedem Idel (x_p) kann man ein Hauptidel x finden derart, daß das Ideal $j(x(x_p))$ keine Verzweigung mehr enthält, so daß $\varphi_{L/K}$ anwendbar ist; diesem von Hasse erfundenen Kunstgriff zur „Verdrängung" der Verzweigung sind wir oben schon begegnet (3.2, 4.4.3). Die lokalen Normrestsymbole an den verzweigten Stellen sind qua Stetigkeit durch diejenigen an den unverzweigten festgelegt, aber (leider) nicht explizit, ebenso wie in [Ch1]. Die Galoisgruppe ist hier natürlich diskret topologisiert; die Stetigkeit bedeutet also einfach, daß der Kern von ψ eine offene Untergruppe von $J(K)$ enthält. Der Grundgedanke der Konstruktion entstammt [Ch2], S.80.

Der weitere Beweisgang ist nun der folgende: Ungleichung A wie oben (4.4.2), B nach Chevalley [Ch1]. B impliziert, daß $\varphi_{L/K}$ surjektiv ist (8.7, S.180); wenn also ψ wie in (RR*) existiert, ist auch ψ surjektiv. A impliziert jetzt, daß ψ einen Isomorphismus $C(K)/N(C(L)) \to Gal(L/K)$ induzieren muß (9.4, S.184), also das „eigentliche" Reziprozitätsgesetz. Jetzt folgt der Beweis von (RR*): ψ wird definiert als das Produkt der lokalen Normrestsymbole (die lokale Theorie wird von Tate vorausgesetzt, der sich auf die Darstellung von Serre [S] in demselben Band bezieht). Zu beweisen ist jetzt noch $\psi(K^\times) = 1$, also die Produktformel für diese Symbole. Tate kombiniert den Beweis dafür mit dem für die Hassesche Summenformel der lokalen Invarianten zentral-einfacher Algebren; die Brauergruppe wird wieder rein kohomologisch definiert (für die „eigentliche" Definition siehe den nächsten Abschnitt). Damit läßt sich die Aussage reduzieren auf den Fall zyklotomischer Erweiterungen von $\mathbb{Q}$. Das war unser primordiales Beispiel; aber jetzt können die verzweigten Primstellen nicht mehr umgangen werden. Tate gibt nun zwei Beweise; der erste stützt sich auf eine Charakterisierung der lokalen Symbole ([S], S.145), der zweite auf die in [S] ebenfalls dargestellte Lubin-Tate-Theorie ([T], S.190f); das wurde oben erklärt (4.4.3).

5 Der algebrentheoretische Zugang

5.1 Die Brauergruppe eines Körpers

Wir referieren das für uns Wesentliche; Näheres und alle Beweise findet man in [Lo1]; sehr empfehlenswert ist auch das Buch [R] von I.Reiner, das sich allerdings in erster Linie der allgemeinen nichtkommutativen Arithmetik widmet.

5.1.1 Sei K ein beliebiger Körper; wir betrachten Algebren A von endlicher Dimension über K. Eine solche Algebra heißt *zentral-einfach über* K, wenn sie keine echten zweiseitigen Ideale hat und K ihr Zentrum ist; das erste Beispiel ist der Matrixring $M_n(K)$. Nach einem fundamentalen Satz von Wedderburn ist ein solches A ein Matrixring $M_n(D)$ über einem Schiefkörper (oder Divisionsalgebra) D, der natürlich selbst zentral-einfach über K ist und eindeutig bestimmt als Endomorphismenring eines minimalen Rechtsideals ([R], S.91). Das bekannteste Beispiel (und das einzige allgemein bekannte!) für einen echten Schiefkörper bilden die Hamiltonschen Quaternionen, eine zentral-einfache $\mathbb{R}$-Algebra.

Sind A und B zentral-einfach über K , so ist es auch das (über K genommene) Tensorprodukt $A \otimes B$; das Produkt ist assoziativ und kommutativ. A und B sollen *ähnlich* heißen, wenn sie isomorphe Schiefkörperanteile haben (denselben „harten Kern"); eine Ähnlichkeitsklasse besteht also aus allen $M_n(D)$ mit festem D . Die Klassen lassen sich nun zu einer Gruppe machen, in der die Klasse der $M_n(K)$ als Einselement figuriert; man zeigt nämlich $A \otimes A^{op} \cong M_n(K)$, $n = [A : K]^2$; hier bezeichnet A^{op} die zu A *duale* Algebra mit Elementen a^0 für $a \in A$ und den Operationen $a^0 + b^0 = (a +$

$b)^0$ und $a^0 b^0 = (ba)^0$ (mehr „strukturell“: A^{op} ist der Ring der A-Endomorphismen des regulären A-Moduls A). Die Gruppe der Ähnlichkeitsklassen heißt die *Brauergruppe* $B(K)$ von K. Ist K algebraisch abgeschlossen, so ist $B(K) = 1$, denn ein echter (endlichdimensionaler) Schiefkörper über K würde echte Erweiterungs*körper* enthalten. Auch für endliche K ist $B(K) = 1$; man kann durch elementare gruppentheoretische Überlegungen zeigen, daß ein endlicher Schiefkörper ein Körper ist (siehe [W], S.1), aber mit etwas Theorie geht es einfacher (zum Beispiel, weil bei Erweiterungen endlicher Körper die Normabbildung surjektiv ist, s.u. 5.1.3). $B(\mathbb{R})$ enthält als einziges nichttriviales Element die Klasse der Quaternionen. Für uns wichtig sind die Brauergruppen der p-adischen und der Zahlkörper (dezidiert nichttriviale Objekte).

5.1.2 Ist L/K ein Erweiterungskörper und A zentral-einfach über K, so ist $L\otimes A$ eine zentral-einfache L-Algebra; das gibt einen Homomorphismus $b(L/K)\colon B(K) \to B(L)$. L heißt ein *Zerfällungskörper* von A, oder *A zerfällt über L*, wenn $L\otimes A \cong M_n(L)$, also die Klasse von A im Kern von $b(L/K)$ liegt, der mit $B(L/K)$ bezeichnet wird. Ein algebraisch abgeschlossenes L ist stets Zerfällungskörper; daraus folgt, daß $[A : K]$ stets eine Quadratzahl ist; ist $A = D$ ein Schiefkörper und $[D : K] = d^2$, so nennt man d den *Schurindex* von D. Ein maximaler (kommutativer) Teilkörper E von D ist stets Zerfällungskörper, und $[E : K] = d$. Ein Oberkörper eines Zerfällungskörper ist wieder ein solcher; insbesondere existiert ein über K endlicher und galoisscher Zerfällungskörper L. Ein wichtiger Satz ist nun: es existiert dann eine zu A ähnliche Algebra A', in welche L als maximaler kommutativer Teilkörper eingebettet werden kann, derart daß L sein eigener Zentralisator in A' und $[A' : K] = [L : K]^2$ ist (siehe [R], S.240). Nun wenden wir ein fundamentales Resultat der Algebrentheorie an, den *Satz von Skolem-Noether*: sei $K \subset B \subset A$, B ein einfacher Unterring von A. Dann kann jeder Isomorphismus $B \cong C$, wo C ein weiterer Unterring von A ist, durch Konjugation mit einem $u \in A^\times$ erzeugt werden. In unserem Fall ist $B = L$ ein maximaler kommutativer und A zerfällender Teilkörper sowie galoissch über K, $G = \mathrm{Gal}(L/K)$. Der Satz von Skolem-Noether gibt uns zu jedem $g \in G$ ein $u(g) \in A^\times$ derart, daß

$$g(x) = u(g)\, x\, u(g)^{-1} \quad \text{oder} \quad u(g)\, x = g(x)\, u(g)\,,\ \text{alle } x \in L$$

gilt. Aus dieser Gleichung folgt, daß $u(g)\, u(h)\, u(gh)^{-1}$ mit allen $x \in L$ vertauschbar ist. Da L sein eigener Zentralisator ist, folgt

$$u(g)\, u(h) = f(g,h)\, u(gh) \quad \text{für ein } f(g,h) \in L\,.$$

Schreibt man nun aus, daß die Multiplikation der $u(g)$ assoziativ ist, erkennt man f als Faktorensystem, genauer als 2-Kozykel von G mit Werten in $L^\times$; f kann so normiert werden, daß $u(1)$ die Eins von A ist, was wir stets annehmen werden. Weiter ist nicht schwer zu beweisen, daß A die direkte Summe der L-Unterräume $Lu(g)$ ist. Geht man umgekehrt von einem Faktorensystem f aus, kann man zunächst einen L-Vektorraum mit Basiselementen $u(g)$ bilden; definiert man nun eine Multiplikation auf diesem Raum durch die obigen Gleichungen, erhält man eine zentral-einfache K-Algebra mit L als maximalem kommutativem Teilkörper, die mit $(L/K, f)$ bezeichnet wird; eine Art

Amalgam der Gruppenstruktur von G, der Körperstruktur von L und der Operation von G auf L. Man spricht darum von *verschränkten Produktalgebren* (*crossed product algebras*). Die Konstruktion führt schließlich zu einem Isomorphismus

$$B(L/K) \;\to\; H^2(G, L^\times)\,, \tag{4}$$

der weiter das folgende Wohlverhalten aufweist: sei H eine (normale) Untergruppe und $F = L^H$ ihr Fixkörper; dann bestehen kommutative Diagramme

$$\begin{array}{ccc} B(L/K) & \to & B(L/F) \\ \downarrow & & \downarrow \\ H^2(G, L^\times) & \underset{\text{res}}{\to} & H^2(H, L^\times) \end{array} \qquad\qquad \begin{array}{ccc} B(F/K) & \to & B(L/K) \\ \downarrow & & \downarrow \\ H^2(G/H, F^\times) & \underset{\text{inf}}{\to} & H^2(G, L^\times) \end{array}$$

(nur im zweiten muß H normal sein). Die senkrechten Pfeile sind Isomorphismen (4), der obere waagerechte Pfeil ist im ersten Diagramm die Abbildung $A \to F\otimes A$ (beachte $L \otimes_F (F \otimes A) = L \otimes A$), im zweiten eine Inklusion (wird A von F zerfällt, dann a fortiori von L; die Injektivität der kohomologischen Inflation ist also algebrentheoretisch trivial). Es gibt auch eine Korestriktion der Algebren mit einem entsprechenden Diagramm, worauf wir aber nicht mehr eingehen. Da offensichtlich

$$B(K) = \bigcup_{L/K} B(L/K) \quad \text{oder genauer} = \text{lim.ind. } B(L/K)\,,$$

erhalten wir die früher angekündigte Identifikation $B(K) = H^2(K) = \text{lim.ind. } H^2(G, L^\times)$.

5.1.3 Besonders einfach werden die Verhältnisse für zyklische Erweiterungen, $G = \langle s \rangle$. Wir wissen bereits, daß in diesem Fall $H^2(G, L^\times) \cong H^0(G, L^\times) = K^\times / N(L^\times)$ ist, so daß auch die Algebren aus $B(L/K)$ durch Normenreste beschreibbar sein müssen. In der Tat: mit $u = u(s)$ bilden auch die Potenzen $u^0, \ldots, u^{n-1}$, $n = [L : K]$, eine K-Basis von $(L/K, f)$, und man berechnet

$$u^n = \prod_{i=0,\ldots n-1} f(s^i, s) =: a \in K^\times$$

([R], S.259). Das Produkt ist übrigens ein Spezialfall eines Cupprodukts, nämlich

$$H^2(G, L^\times) \times H^{-2}(G, \mathbb{Z}) \to H^0(G, L^\times)\,, \quad (f, s) \to a\,,$$

siehe [N1], S.80; diese Abbildung ist gerade diejenige, welche im Satz von Tate zum abstrakten Reziprozitätsgesetz führt. Die „innere Verwandtschaft" des algebrentheoretischen und des kohomologischen Zugangs zur Klassenkörpertheorie, schon im Isomorphismus $B(K) \cong H^2(K)$ zutage getreten, wird damit noch deutlicher.

Bezeichnet man die so beschriebene Algebra mit $(L/K, s, a)$, so gilt, wie man jetzt schon erwartet,

$(L/K, s, a) \cong (L/K, s, b) \Leftrightarrow a/b \in N(L^{\times})$, $(L/K, s, a)$ zerfällt über K $\Leftrightarrow a \in N(L^{\times})$.

Die Abhängigkeit von der Wahl von s kommt in der Formel $(L/K, s, a) \cong (L/K, s^m, a^m)$ zum Ausdruck, für $(n, m) = 1$.

5.2 Lokale Klassenkörpertheorie

5.2.1 Der Schlüssel zur algebrentheoretischen Definition der lokalen Normrestabbildung ist Hasses Klassifikation der lokalen Schiefkörper und die daraus resultierende Isomorphie der Brauergruppe mit $\mathbb{Q}/\mathbb{Z}$, die wir in 4.3.1 mit kohomologischen Mitteln erhalten haben. Sei also jetzt K ein p-adischer Körper und D ein über K zentraler endlichdimensionaler Schiefkörper vom Schurindex d. Wichtigstes Ingrediens für das Folgende ist die Tatsache, daß man den Absolutbetrag (und die Exponentenbewertung) von K auf D fortsetzen kann, wie im Kommutativen durch die (reduzierte) Norm. Die Nichtkommutativität von D stört diesen Prozeß nicht, weil man die Bewertung elementweise definieren kann und jedes Element von D eine kommutative Körpererweiterung von K erzeugt. Als endlicher Vektorraum über K ist D automatisch vollständig, und ganz wie im Kommutativen erhält man einen eindeutigen Ganzheitsbereich O_D, einen Verzweigungsindex e, einen Restklassengrad f und die Gleichung $ef = d^2 = [D : K]$. Ein Primelement von O_D erzeugt einen Körper von einem Grad $\geq e$ über K. Da ein kommutativer Teilkörper von D höchstens den Grad d über K haben kann, folgt $e = f = d$. Der Restkörper von O_D, der als endlicher Schiefkörper kommutativ ist, wird über dem Restkörper von K durch die Restklasse eines $x \in O_D$ erzeugt, das in D einen Körper mit einem Restklassengrad $\geq f$ erzeugt, also hat dieser Körper den Grad f und ist die einzige unverzweigte Erweiterung W von K von diesem Grad. Damit ist D ein zyklisches verschränktes Produkt $(W/K, s, a)$, wobei wir für s natürlich den Frobenius der Erweiterung W/K wählen. Da jede Einheit von O_K eine Norm aus W ist, kann man a als Potenz π^r eines Primelements von K wählen, wobei natürlich $0 < r < d$ angenommen werden kann. Umgekehrt zeigt man: die Algebra $(W/K, s, \pi^r)$ ist ein Schiefkörper genau dann, wenn $(r, n) = 1$ ist. Wir definieren nun die *Hasseinvariante* von D (genauer: der von D in B(K) repräsentierten Brauerklasse) durch

$$\mathrm{inv}\, D := r/d + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$$

und konstatieren den fundamentalen

Satz: *Die Hasseinvariante definiert einen Isomorphismus* $\mathrm{inv}: B(K) \to \mathbb{Q}/\mathbb{Z}$. *Für eine Erweiterung* L/K *ist das Diagramm*

$$
(5) \qquad \begin{array}{ccc} B(K) & \to & \mathbb{Q}/\mathbb{Z} \\ \downarrow & & \downarrow [L:K] \\ B(L) & \to & \mathbb{Q}/\mathbb{Z} \end{array}
$$

kommutativ.

Hier bezeichnet der rechte senkrechte Pfeil die Multiplikation mit $[L : K]$; die noch fehlenden Argumente liefert der Mechanismus der zyklischen Algebren. Man sieht nun auch, daß $B(L/K)$ als Kern von $B(K) \to B(L)$ isomorph zu der von $[L:K]^{-1} + \mathbb{Z}$ erzeugten Untergruppe von $\mathbb{Q}/\mathbb{Z}$ ist und die algebrentheoretische Invariantenabbildung mit der kohomologischen übereinstimmt; die Fundamentalklasse von $H^2(G, L^\times)$ (L/K galoissch) wird algebrentheoretisch repräsentiert durch den Schiefkörper $(W/K, s, \pi)$, wo W die unverzweigte Erweiterung mit $[W : K] = [L : K]$ und s ihr Frobeniusautomorphismus ist. Man erkennt auch die algebrentheoretischen Analoga der beiden Axiome (a) und (b) für die kohomologische Invariantenabbildung: (a) kommt algebrentheoretisch einfach daher, daß $B(L/K)$ eine Untergruppe von $B(N/K)$ ist (N/L/K normal); (b) rührt daher, daß die kohomologischen Restriktionen $H^2(N/K) \longrightarrow H^2(L/K)$ algebrentheoretisch den Abbildungen $B(N/K) \longrightarrow B(L/K)$ entsprechen, folgt also aus Diagramm (5) , eingeschränkt auf die „Schichten“ N/K und N/L.

Das Diagramm (5) hat noch eine weitere Konsequenz, die nicht unerwähnt bleiben soll: ist D ein Schiefkörper über K vom Schurindex d , ist jede Erweiterung E/K von einem durch d teilbaren Grad Zerfällungskörper von D. Ist $[E : K] = d$, so kann, nach einem in 5.1.2 zitierten allgemeinen Satz, E als maximaler Teilkörper in D eingebettet werden. D enthält also (bis auf Isomorphie) alle solchen E, oder, etwas spektakulär ausgedrückt: jedes irreduzible Polynom über K vom Grad d hat eine Nullstelle in D. Dieses „strukturelle Potential“ der lokalen Schiefkörper ist ein erstaunlicher Kontrast zu ihrer leichten Handhabbarkeit in der Brauergruppe; in gewissem Sinne sind sie weniger „schief“ als die kommutativen L/K.

5.2.2 Wir können nun das lokale Normrestsymbol definieren. Sei L/K normal, $G = \mathrm{Gal}(L/K)$, und $\chi \in G^* = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ ein Charakter von G ; ferner L_χ der Fixkörper von Kern χ , also L_χ / K zyklisch mit $\mathrm{Gal}(L_\chi / K) = \mathrm{Im}\ \chi$, sowie $s(\chi)$ das (eindeutig bestimmte) Element von $\mathrm{Gal}(L_\chi / K)$ mit $\chi(s(\chi)) = 1/[L_\chi : K] + \mathbb{Z}$. Wir definieren eine Paarung

$$
K^\times \times G^* \longrightarrow \mathbb{Q}/\mathbb{Z} \text{ durch } (a, \chi) \longrightarrow \mathrm{inv}\,(L_\chi / K , s(\chi), a) =: \langle a, \chi \rangle .
$$

Die Linearität in der ersten Variablen folgt aus dem Mechanismus der zyklischen Algebren; für die Linearität in den Charakteren bildet man die Faktorensysteme zu den beteiligten $(L_\chi / K , s(\chi), a)$ und ihre Inflation auf G und bestätigt die Additivität; hier geht die Injektivität der Inflation ein ([Lo1), S.311). Die Definition hat ihren Ursprung in [H3], 5.3.

Klar ist weiter, daß der Linkskern dieser Paarung die Gruppe $N(L^\times)$ enthält; wir erhalten also einen Homomorphismus

$$K^\times \;\longrightarrow\; K^\times / N(L^\times) \;\longrightarrow\; (G^*)^* = ((G^{ab})^*)^* = G^{ab} ,$$

den wir mit $(a, L/K)$ bezeichnen, das Normrestsymbol zur Erweiterung L/K. Es ist *charakterisiert* durch die Gleichungen

$$\chi((a, L/K)) = \mathrm{inv}\,(L_\chi / K , s(\chi), a) , \text{ alle } \chi \in G^* ,$$

weil ein Element von G^{ab} durch seine Werte unter allen Charakteren festgelegt ist. Diese Gleichung ist die algebrentheoretische Version der Gleichung (3), welche den Zusammenhang zwischen $(a, L/K)$ und der kohomologischen Invariantenabbildung darstellte. Eine leichte Folgerung aus der Definition ist auch, daß sie für unverzweigtes L/K das richtige Ergebnis liefert, nämlich $(a, L/K) = s^{\nu(a)}$, wo s den Frobenius der Erweiterung L/K und ν die normierte Exponentenbewertung von K bezeichne.

Für das Reziprozitätsgesetz, die Isomorphie der Abbildung $(\;, L/K)$: $K^\times / N(L^\times) \longrightarrow G^{ab}$, muß jetzt gezeigt werden, daß die Paarung

$$K^\times / N(L^\times) \times G^* \longrightarrow \mathbb{Q}/\mathbb{Z}$$

in beiden Argumenten nichtentartet ist. Für die Charakterseite ist das einfach: ist $\chi \neq 1$, so ist $[L_\chi : K] > 1$, und es gibt Elemente $a \in K^\times$, die keine Normen aus L_χ / K sind (ist ein Primelement eine Norm, ist die Erweiterung rein verzweigt, sind alle Einheiten Normen, ist sie unverzweigt); dann ist auch $\mathrm{inv}\,(L_\chi / K , s(\chi), a) \neq 0$. Für die Normrestseite ist zu zeigen: ist a Norm aus allen *zyklischen* Teilerweiterungen $L/Z/K$, dann auch Norm aus L; das gelingt durch eine Induktion nach dem Grad $[L : K]$ unter Benutzung der Tatsache, daß Galoisgruppen p-adischer Erweiterungen stets auflösbar sind ([Lo1], S.315). Der Beweis des Existenzsatzes vollzieht sich nach schon bekanntem Muster.

Vergleicht man dies mit dem Zugang in 4.3, erkennt man den Vorzug der lokalen Schiefkörper: man muß sich nicht eigens bemühen, die Verzweigung zu umgehen; es ist $B(L/K) = B(N/K)$ genau dann, wenn $[L : K] = [N : K]$ ist; mit der Invariantenabbildung für die D hat man die für alle L/K mit $[L : K]$ = Schurindex von D. Dahinter steckt natürlich die oben erwähnte „Reichhaltigkeit“ der D.

5.3 Globale Klassenkörpertheorie

5.3.1 Der erste Schritt ist, wie in [AT] und mit demselben Beweis, Ungleichung B in der Form $h(C(L)) = |H^0(G, C(L))| / |H^1(G, C(L))| = [L : K]$, zunächst nur für zyklische L/K , mit der Folgerung, daß in jedem normalen L/K unendlich viele Primideale nicht voll zerfallen (Zerfällungssatz). Dann geht es anders weiter, zunächst mit einer Diskussion des Lokal-Global-Prinzips für n-te Potenzen in Zahlkörpern. Die Fragestellung wird dann eingeschränkt auf S-Einheiten von K, mit der Voraussetzung, daß K die n-ten Einheitswurzeln enthält. Es zeigt sich, daß diese schon n-te Potenzen in K sind, wenn sie es an den *endlich vielen* Stellen aus S sind; S muß dafür alle unendlichen Stellen und alle Teiler von n enthalten und so groß sein, daß $J(K) = J^S(K)\, K^\times$ ist ([Lo2], S.179, siehe auch [T], Remark 9.3, S.184). Das entscheidende Resultat ist: ist zusätzlich noch n eine Primzahlpotenz und L/K zyklisch mit $[L : K] = n$, so existiert eine Untergruppe C von N(C(L)) mit $C(K) : C = [L : K]$, woraus Ungleichung A folgt. Der Beweis, den wir hier nicht en detail angeben können, ist ein subtiles Jonglieren mit einer endlichen Hilfsmenge von Stellen; benutzt werden einschlägige Aussagen über Indices von Potenzgruppen in lokalen Körpern, die sich im Rahmen der lokalen Klassenkörpertheorie ergeben, und natürlich Kummertheorie. Zusammen mit Ungleichung B ergeben sich jetzt gleichzeitig die beiden Folgerungen

$$|H^0(G, C(L))| = [L : K] \quad \text{und} \quad |H^1(G, C(L))| = 1 ,$$

zunächst nur unter den angegebenen Voraussetzungen an L/K (S.183).

5.3.2 Es folgt eine Diskussion des Hasseschen Normensatzes (H) und seiner Beziehung zum Satz von Hasse-Brauer-Noether (HBN) , den wir zunächst beschreiben wollen: ist $[A] \in B(K)$, so ist $K_p \otimes A$ für alle Stellen p von K eine zentral-einfache K_p-Algebra; das gibt einen Homomorphismus $B(K) \longrightarrow \bigoplus_p B(K_p)$ (wir werden unten sehen, daß das Bild in der direkten Summe liegt); die Stellen p , an denen $[K_p \otimes A] \neq 1$ in $B(K_p)$ ist, diese Algebra also einen echten Schiefkörperanteil hat, heißen auch die *Verzweigungsstellen* von A. HBN ist die Aussage, daß dieser Homomorphismus injektiv ist, in Worten: A zerfällt über K genau dann, wenn A über allen K_p zerfällt (die Implikation $\Rightarrow$ ist trivial), oder auch: für das Zerfallen zentral-einfacher Algebren besteht ein strenges Lokal-Global-Prinzip. Nun läßt sich direkt zeigen, daß H und HBN äquivalent sind (in dem üblichen Sinn dieses Ausdrucks für wahre Aussagen). Die Implikation HBN $\Rightarrow$ H ist leicht: ist L/K zyklisch, $Gal(L/K) = \langle s \rangle$ und $a \in K^\times$, so ist a eine Norm aus L genau dann, wenn die zyklische Algebra (L/K, s a) zerfällt, und dasselbe gilt für alle $K_p \otimes A$. Die Implikation H $\Rightarrow$ HBN wird S.194f indirekt bewiesen; der Beweis ist kurz und erfordert nur die Algebrentheorie, es zeigt sich dabei sogar, daß man H nur im Fall primzyklischer Erweiterungen braucht. Siehe auch [R], S.276.

Diese letzte Bemerkung zeigt weiter, daß für den Beweis von H nur der primzyklische Fall nötig ist, denn daraus folgt ja HBN und damit, wie eben gesehen, H im allgemeinen. Der primzyklische Fall wird mittels einer inf-res-Sequenz auf den Kummerschen Fall zurückgeführt, und dieser wurde zuvor schon abgehandelt.

Der Zusammenhang mit der Kohomologie ergibt sich durch die Sequenz

$$1 \to L^\times \to J(L) \to C(L) \to 1 ,$$

L/K jetzt beliebig galoissch, die wegen $H^1(G, J(L)) = 1$ die exakte Kohomologiesequenz

$$1 \to H^1(G, C(L)) \to H^2(G, L^\times) \to H^2(G, J(L))$$

nach sich zieht, und die Identifikationen

$$H^2(G, L^\times) = B(L/K) , \quad H^2(G, J(L)) = \bigoplus_p B(L_P/K_p) .$$

Weil jedes $[A] \in B(K)$ in einem $B(L/K)$ liegt, sieht man jetzt, daß HBN mit dem Verschwinden der $H^1(G, C(L))$ äquivalent ist, welch letzteres damit allgemein bewiesen ist. Zusammen mit der Formel $h(C(L)) = | H^0(G, C(L))| \,/\, | H^1(G, C(L))| = [L : K]$ ergibt sich jetzt im zyklischen Fall

$$| H^0(G, C(L)) | = C(K) : N(C(L)) = [L : K] .$$

5.3.4 Das Normrestsymbol für Idele wird wie früher als Produkt der lokalen Symbole definiert,

$$((x_p) , L/K) = \Pi_p (x_p , L_P /K_p) \in Gal(L/K)^{ab} .$$

Wie schon früher bemerkt, impliziert die Definition sofort eine Kompatibilität von lokalen und globalen Normrestsymbolen. Die Surjektivität von $(, L/K)$ folgt ähnlich wie zuvor aus dem Zerfällungssatz: ist H das Bild von $(, L/K)$ und E der Fixkörper von H, so ist $((x_p) , E/K) = 1$ für alle Idele (x_p) ; da die lokalen Symbole alle surjektiv sind, sind alle D(P) trivial, der Zerfällungssatz gibt also $E = K$, $H = Gal(L/K)^{ab}$.

Zum Beweis der für den Abstieg dieser Funktion nach C(K) nötigen Produktformel $(x, L/K) = 1$ für Hauptidele x wird nun noch einmal die Algebrentheorie in sehr eleganter Weise herangezogen. Wir erinnern zunächst an die Formel

$$\chi ((a, L/K)) = inv (L_\chi / K , s(\chi), a) , \text{ alle } \chi \in G^* ,$$

die für lokale L/K den Zusammenhang zwischen Normrestsymbol und Hasseinvarianten beschreibt (5.2.2). Ist nun wieder K global, so liefert ein $\chi \in G^*$ Charaktere $\chi_p \in D(P)^*$ und Erzeugende $s(\chi_p)$ von D(P) . Bilden wir für $a \in K^\times$ wie im Lokalen die zyklische

Algebra $A = (L_\chi / K, s(\chi), a)$, so zeigt sich unschwer, daß die lokalen Algebren

$$A_p = K_p \otimes A \quad \text{und} \quad (L_{\chi_p} / K_p, s(\chi_p), a)$$

ähnlich sind ([Lo2], S.222). Daraus folgt

$$(6) \qquad \chi((a, L/K)) = \sum_p \operatorname{inv}(L_\chi / K, s(\chi), a)_p \; .$$

Es genügt demnach, zu beweisen, daß für globale A stets

$$\sum_p \operatorname{inv}(A_p) = 0$$

ist; das ist Hasses Summenformel für die lokalen Invarianten. Sei also A zentral-einfach über K. Wir haben schon gesehen: eine (endliche) Erweiterung L/K ist Zerfällungskörper von A genau dann, wenn die lokalen Grade $[L_P : K_p]$ Vielfache der Schurindices der A_p sind ; da diese fast alle $= 1$ sind, genügt es, dies an endlich vielen Stellen p zu fordern. Nun folgt ein Satz, der als Variante des Artinschen Lemmas anzusehen ist:

Sei S eine endliche Menge von Primstellen und $d > 1$ eine natürliche Zahl. Dann existiert ein zyklischer zyklotomischer Körper L/K, $L \subset K(\zeta)$, mit den Eigenschaften: (i) $d \mid [L_P : K_p]$, alle $p \in S$; (ii) L ist nicht reell; (iii) die Ordnung m von ζ ist durch kein $p \in S$ teilbar.

Die beiden ersten Bedingungen sind relativ leicht zu erfüllen (die zweite stellt sicher, daß L auch an reellen Verzweigungsstellen von A Zerfällungskörper ist); es ist die dritte, welche Mühe kostet. Wie in 1.7 kann die Aussage auf den rationalen Grundkörper reduziert und mit elementaren Mitteln bewiesen werden ([Lo2], S.199).

Für unser Problem nehmen wir für S die Menge der Verzweigungsstellen von A und für d das kgV der lokalen Schurindices. Demnach ist A ähnlich zu einer zyklischen Algebra $(L/K, s, a)$, $\langle s \rangle = \mathrm{Gal}(L/K)$, $a \in K^\times$. Das Strukturelement a kann noch durch Normen aus L abgeändert werden, und mittels des Approximationssatzes läßt sich zeigen, daß man $a \equiv 1 \bmod m$ erreichen kann. Nun kommt die Pointe: statt jetzt in der Gleichung (6) die rechtsstehenden lokalen Invarianten auszurechnen, zeigen wir direkt $(a, L/K) = 1$. Das sieht aus, als seien wir wieder beim ursprünglichen Problem angelangt, aber wir haben jetzt die starke Voraussetzung $a \equiv 1 \bmod m$, und m enthält alle Verzweigung von L/K. Wieder reduziert man auf $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta)$, $m = p^r$. In dem kritischen Fall $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ brauchen wir jetzt das schwierig zu bestimmende Normrestsymbol nicht explizit zu kennen, denn vergleichsweise einfach läßt sich zeigen, daß Elemente $\equiv 1 \bmod m$ Normen sind, siehe [Lo1], S.323. Hier ist also die Algebrentheorie als „bypass“ benutzt, um den allgemeinen Fall auf einen speziellen und einfacheren zu reduzieren, und ermöglicht wurde das letzten Endes durch das sehr einfache lokale Kriterium für die Zerfällung von Algebren.
Der Beweis des Reziprozitätsgesetzes fällt nun nicht mehr schwer. Die eben bewiesene

Produktformel für das idelische Normrestsymbol gibt uns ein solches für die Idelklassen, das wir ebenso bezeichnen,

$$(\ ,L/K)\ :C(K)\ \longrightarrow\ \mathrm{Gal}(L/K)^{ab},$$

und das $N(C(L))$ in seinem Kern enthält; das folgt sofort aus der entsprechenden lokalen Tatsache und der Definition der Idelnorm. Das Reziprozitätsgesetz besagt, daß $(\ ,L/K) : C(K)/N(C(L)) \longrightarrow \mathrm{Gal}(L/K)^{ab}$ ein Isomorphismus ist. Die Surjektivität haben wir schon bewiesen, und für zyklisches L/K folgt damit auch die Injektivität, denn wir wissen schon, daß $C(K) : N(C(L)) = [L : K]$ ist. Der Rest folgt durch Induktion nach $[L : K]$ unter Verwendung des Wohlverhaltens von $(\ ,L/K)$ und elementarer gruppen- und galoistheoretischer Argumente, siehe [Lo2], S.231ff. Der Beweis des Existenzsatzes in [Lo2] entspricht dem in [AT].

6 Die Theorie von Weil

6.1 Ich referiere zunächst den abstrakten Teil, von Weil „Formalismus der Klassenkörpertheorie“ genannt ([W], Ch. XII). Sei K ein Körper (später spezifiziert als lokaler oder globaler Körper), $G(K)$ die absolute Galoisgruppe und $X(K) = G(K)^* = (G(K)^{ab})^*$ ihre Charaktergruppe, versehen mit der diskreten Topologie (entsprechend der Tatsache, daß das Dual einer kompakten Gruppe stets diskret ist). An den Anfang stellt Weil eine Paarung, hierin [Ch2] folgend, $(\ ,\ )_K : X(K) \times M(K) \longrightarrow \mathbb{C}^\times$, wo $M(K)$ eine lokalkompakte kommutative Gruppe ist (später spezifiziert zu $M(K) = K^\times$ (lokaler Fall) bzw. $M(K) = C(K)$ (globaler Fall)); die Paarung liegt hier also beiden Fällen zugrunde und ist von vornherein für die volle Gruppe $G(K)^*$ formuliert. Die folgenden Axiome sollen erfüllt sein:

(I) Die Paarung ist bihomomorph und stetig.

Für jedes $g \in M(K)$ ist also $\chi \longrightarrow (\chi , g)_K$ ein Element von $G(K)^{**} = G(K)^{ab}$; das ergibt einen Homomorphismus $\mathbf{a} : M(K) \longrightarrow G(K)^{ab}$, den *kanonischen* Homomorphismus, der also durch die Gleichung

$$\chi(\mathbf{a}(g)) = (\chi , g)_K$$

charakterisiert ist; in unseren Anwendungen wird natürlich **a** die Normrestabbildung.

(II) Der Linkskern der Paarung ist trivial, aus $(\chi , g)_K = 1$ für alle g folgt $\chi = 1$.

Äquivalent dazu sind (II'): $\chi \longrightarrow \chi \circ \mathbf{a}$ ist ein injektiver Morphismus $X(K) \longrightarrow M(K)^*$, oder: (II''): das Bild $\mathbf{a}(M(K))$ ist dicht in $G(K)^{ab}$.

Der Rechtskern der Paarung ist der Kern von **a** ; er wird mit U(K) bezeichnet. Er ist gleichzeitig der Kern aller Charaktere von M(K) der Form $\chi \circ \mathbf{a}$, weil die Elemente von G(K) durch die Charaktere dieser Gruppe getrennt werden. Das dritte Axiom enthält eine erste Spezifikation der Struktur von M(K) :

(III) M(K) ist das Produkt einer kompakten Gruppe $M^1(K)$ und einer Gruppe N ; dabei ist N isomorph zu $\mathbb{R}$ (globaler Fall) oder zu $\mathbb{Z}$ (lokaler Fall). Im lokalen Fall gibt es zu jedem natürlichen n einen Charakter χ der Ordnung n mit $(\chi , g)_K = 1$ für alle $g \in M^1(K)$.

Im globalen Fall ist $M(K) = C(K) = C^1(K) \times \mathbb{R}$; im lokalen Fall ist $M(K) = K^\times = <\pi> \times R^\times$, wo π ein Primelement und $R^\times$ die (kompakte) Einheitengruppe des Bewertungsrings von K ist. Das Normrestsymbol bildet hier $R^\times$ auf $Gal(K^{ab}/K_0)$ ab, wo K_0 die maximale unverzweigte Erweiterung bezeichne; die Aussage über die Charaktere entspricht der Tatsache, daß K zu jedem n genau eine unverzweigte Erweiterung vom Grad n hat (die Anzahl der Charaktere der Ordnung n ist dann $\varphi(n)$, die Eulerfunktion von n).

Erste Folgerungen sind: im Fall (IIIa) ist der kanonische Morphismus ein Isomorphismus $\mathbf{a} : M(K)/U(K) \longrightarrow G(K)^{ab}$; der Beweis ist derselbe wie beim Beweis des Existenzsatzes in [AT]. Die Folgerungen im Fall (IIIb) sind etwas komplexer, weil $\mathbb{Z}$ anders als $\mathbb{R}$ Charaktere endlicher Ordnung besitzt; es gilt: $\chi \longrightarrow \chi \circ \mathbf{a}$ ist ein Isomorphismus von X(K) mit der Gruppe der Charaktere endlicher Ordnung von M(K), die auf U(K) verschwinden.

Obwohl (III) eine recht schwache Spezifikation von M(K) ist, folgt an dieser Stelle schon eine Aussage, die dem Hauptsatz der Klassenkörpertheorie erstaunlich nahe kommt: sei L/K eine abelsche Erweiterung, $B \subset G(K)^{ab}$ ihre Fixgruppe und $N(L) := \mathbf{a}^{-1}(B)$ deren Urbild unter dem kanonischen Morphismus. Dann ist B der Abschluß von $\mathbf{a}(N(L))$ in $G(K)^{ab}$; L ist der Fixkörper von $\mathbf{a}(N(L))$, und **a** vermittelt einen Isomorphismus $M(K)/N(L) \longrightarrow Gal(L/K)$, Ferner ist die Abbildung $L \longrightarrow N(L)$ eine Bijektion zwischen den endlichen L/K und den offenen Untergruppen von endlichem Index in M(K), die den Kern U(K) von **a** enthalten ([W], S.217). Wie beim kohomologischen Zugang erhält man also ein Reziprozitätsgesetz und einen Existenzsatz *in abstracto.*

Der Beweis benutzt nur elementare gruppentheoretische und topologische Argumente. In den beiden für uns relevanten Fällen erweist sich natürlich N(L) als die Menge der Normen aus M(L); in der hier zugelassenen Allgemeinheit kann von solchen noch keine Rede sein. Es folgen zwei weitere Axiome, welche, im Falle zyklischer Erweiterungen L/K, die Kompatibilität der Paarung mit der Operation von Gal(L/K) betreffen (Axiom (IV)) (in den Anwendungen mehr oder weniger automatisch) sowie die Existenz einer Abbildung $F: L \longrightarrow K$, für welche die „Verschiebungsformel“ $r \circ \mathbf{a'} = \mathbf{a} \circ F$ gilt (Axiom (V); hier bedeutet r die Einschränkung der Elemente von G(L) auf N in

„hochgeschobenen“ Erweiterungen NL/L, N/K ; siehe Diagramm (1). In den Anwendungen ist F die Norm; die beiden letzten Axiome betreffen also im wesentlichen das Wohlverhalten des kanonischen Morphismus. Die wichtigste Folge dieser Axiome ist eine Aussage über die Kerne U(K) : ist L/K eine zyklische Erweiterung, so ist $F(U(L)) = U(K) \cap F(M(L))$ und $U(K) \cap F(M^1(L)) = F(U(L) \cap M^1(L))$ (S. 219).

Die Axiomatik ist sichtlich (besonders im Axiom (III)) unsere beiden Anwendungsfälle zugeschnitten (hier jedoch mit Einschluß der Funktionenkörper); ich weiß nicht, ob es noch weitere gibt. Was man allein mit ihrer Hilfe und auf elementarem Wege, ohne eigentliche Arithmetik erreichen kann, wirft ein Licht darauf, wo die wirklichen Probleme der Klassenkörpertheorie liegen. Man bemerke den Unterschied zum kohomologischen Zugang: dort folgt mit der Bestätigung der Axiome für eine Klassenformation das Reziprozitätsgesetz *automatisch*; hier muß man noch zeigen, daß das obige $N(L) = \mathbf{a}^{-1}(B)$ tatsächlich die Normengruppe von M(L) ist. Das läuft hinaus auf die Bestimmung von U(K) und macht natürlich Mühe; dafür ist der Nachweis der Axiome weniger aufwendig, nur an einer Stelle wirklich tiefgehend. Der Kern des kanonischen Morphismus erscheint hier so als der Kern des Problems; hierin trifft sich Weils Zugang mit dem klassischen.

6.2 Nun zur Durchführung der Theorie, zunächst im lokalen Fall. Die Brauergruppe eines p-adischen Körpers haben wir schon beschrieben, und die Definition der kanonischen Paarung ist dieselbe wie im letzten Abschnitt (nur daß Weil die Hasseinvariante nicht in $\mathbb{Q}/\mathbb{Z}$, sondern als Einheitswurzel ansetzt). Axiom (I) ergibt sich wie oben, und Axiom (III) ist eine Standardtatsache für lokale Körper. Es folgt der Beweis des Verschiebungssatzes (S.224); als Korollar ergibt sich Axiom (II). Es sollte bemerkt werden, daß die Verschiebungsformel für die Artinabbildung $\varphi_{L/K}$ in 1.3 sehr einfach zu beweisen war, weil dort nur *unverzweigte* p eingingen, während man sich hier der Verzweigung stellen muß; entscheidendes Ingrediens im Beweis ist der Mechanismus der zyklischen Algebren.

Als nächstes wird $U(K) = 1$ bewiesen. Nach Definition von **a** ist $U(K) = \text{Kern } \mathbf{a}$ der Durchschnitt der Kerne aller Charaktere $x \longrightarrow (\chi, x)_K$ von $K^\times$, für $\chi \in X(K)$; nach Definition der Paarung in Verbindung mit dem Mechanismus ist dies auch der Durchschnitt aller $N_{L/K}(L^\times)$, wo L die zyklischen Erweiterungen von K durchläuft. Betrachtung der unverzweigten L zeigt nur, daß ein Element des fraglichen Durchschnitts eine Einheit sein muß; aber weiter führen die unverzweigten L nicht, da in solchen stets alle Einheiten Normen sind, und die Normengruppen anderer L sind nicht ohne weiteres zugänglich. Nun konstruiert Weil, für jedes natürliche n, eine Familie F von Charakteren χ von G derart, daß der Durchschnitt der Kerne aller $x \longrightarrow (\chi, x)_K$ für die χ aus F in $(K^\times)^n$ enthalten ist (S.227); der Durchschnitt aller $(K^\times)^n$ aber ist leicht als trivial zu erkennen. Die Charaktere χ entstehen so: K enthalte die n-ten Einheitswurzeln (darauf kann man reduzieren), für $x \in K^\times$ sei $a \in K^{alg}$ mit $a^n = x$. Für $\sigma \in G$ ist $\sigma(a)/a$ eine n-te Einheitswurzel in K , unabhängig von der Wahl von a und als Funktion von σ ein Homomorphismus; jetzt braucht man nur noch die Einheitswurzeln in K mit den komplexen zu identifizieren (was auf die Wahl einer primitiven hinausläuft). Die so gebildeten Charaktere von G hängen von n und x ab, $\chi = \chi_{n,x}$ (S.185). (Die von Weil nicht behandelte Theorie von Lubin-Tate liefert übrigens die Aussage $U(K) = 1$ sozusagen gratis; siehe [N1], S.179.)

Es folgt der Beweis, daß die Abbildung $\chi \to \chi \circ \mathbf{a}$ ein Isomorphismus von $X(K)$ mit der Gruppe aller Charaktere von $K^\times$ von endlicher Ordnung ist; dies und die Verschiebungsformel führen schließlich zum Beweis, daß in dem Isomorphismus $M(K)/N(L) \to \mathrm{Gal}(L/K)$, L/K abelsch, der schon abstrakt aus den Axiomen (I) – (III) folgte, die Gruppe $N(L)$ die Normengruppe $N_{L/K}(L^\times)$ ist, wie es sein sollte (S.229). Damit sind Reziprozitätsgesetz und Existenzsatz im lokalen Fall bewiesen; das Resumé wird auf S.230 ausgesprochen.

6.3 Wir kommen zur globalen Theorie; im folgenden sei also K ein Zahlkörper und $M(K) = C(K)$, die Idelklassengruppe. Hatte Lorenz nur im Lokalen das Normrestsymbol durch die kanonische Paarung definiert und dann das globale Symbol als Produkt der lokalen, so etabliert Weil auch im Globalen seine abstrakte Axiomatik, also eine Paarung $(\, , \,)_K : X(K) \times C(K) \to \mathbb{C}^\times$; ebenfalls als Produkt der lokalen Paarungen. Auf der Idelebene, also mit $J(K)$ anstelle von $C(K)$, bereitet das keine Schwierigkeit. Sei p eine Stelle von K ; bekanntlich ist jede endliche (abelsche) Erweiterung von K_p Komplettierung einer (abelschen) Erweiterung von K an einer Stelle über p ; die lokale Restriktionsabbildung $r_p : G(K_p^{ab}) \to G(K^{ab})$ liefert durch Dualisieren einen Homomorphismus $X(K) \to X(K_p)$, den wir als $\chi \to \chi_p$ schreiben. Schreiben wir $(\, , \,)_p$ für die lokalen Paarungen, können wir

$$(\chi , x)_K \ := \ \Pi_p \ (\chi_p , x_p)_p \ , \ x = (x_p) \in J(K)$$

definieren; das Produkt ist endlich, weil fast alle x_p Einheiten und fast alle χ_p unverzweigt sind. Axiom (I) ist klar. Für Axiom (II) ist zu zeigen: wenn fast alle χ_p trivial sind, ist auch χ trivial; das ist eine Form des Zerfällungssatzes, den Weil analytisch beweist (S.126). Die Verschiebungsformel (Axiom (V)) folgt ebenfalls ohne weiteres aus dem entsprechenden lokalen Sachverhalt: ist L/K endlich und $r: G(L) \to G(K)$ die Restriktionsabbildung , so ist

$$(\chi \circ r , y)_L = (\chi , N(y))_K \ , \text{ für } \chi \in X(K), \ y \in J(L) ;$$

hier bezeichnet N die Idelnorm $J(L) \to J(K)$.

Ganz ebenso wie zuvor für das Normrestsymbol hat man nun für die kanonische Paarung zu zeigen, daß sie auf die Idelklassen absteigt, m.a.W. daß $(\chi , x)_K = 1$ für Hauptidele $x \in K^\times$ gilt, oder daß $K^\times$ im Kern des kanonischen Morphismus der Paarung $X(K) \times$

$J(K) \longrightarrow \mathbb{C}^\times$ liegt. Hierfür wird wieder die Algebrentheorie herangezogen: sei $A = (L_\chi / K , s(\chi), x)$ die mit dem Paar (χ , x) konstruierte zyklische Algebra; für die Hasseinvarianten an den Stellen p von K gilt dann $\mathrm{inv}(A\otimes K_p) = (\chi_p , x)_p$ (bei Weil multiplikativ geschrieben), so daß die Behauptung auf die Hassesche Summenformel (oder Produktformel) für die Invarianten einfacher Algebren hinausläuft. Der Beweis vollzieht sich wie zuvor: sei A *irgendeine* zentral-einfache K-Algebra; eine Form des Artinschen Lemmas gibt eine zyklische zyklotomische Erweiterung L/K, die an den Verzweigungsstellen von A unverzweigt über K ist, aber lokale Grade hat, welche Vielfache der Schurindices von A an diesen Stellen sind (S.254). Dann ist A ähnlich zur einer Algebra $(L/K, \chi' , a)$ mit einem Charakter χ' von Gal(L/K) und $a \in K^\times$; der Verschiebungssatz erlaubt eine Reduktion auf $K = \mathbb{Q}$, wo unter den angenommenen Voraussetzungen eine direkte Rechnung möglich ist, also wieder mit „Neutralisierung" der Verzweigungsstellen von A.

Benutzt wird natürlich wieder der Satz von Hasse-Brauer-Noether (nämlich bei dem Schluß, daß L Zerfällungskörper von A ist, wenn dies an allen Stellen der Fall ist). Für diesen Satz bringt Weil einen geradezu spektakulären analytischen Beweis, den wir hier nicht übergehen wollen, aber nur im Groben skizzieren können. Zunächst definiert Weil nach dem Vorgang von Tate's Thesis die Zetafunktionen $Z_K(\Phi, s)$ von K (Weil behandelt auch hier die Funktionenkörper simultan mit den Zahlkörpern) als Integral einer „Standardfunktion" Φ, multipliziert mit einem „Quasicharakter" von $J(K)$, trivial auf $K^\times$, über die Gruppe $J(K)$, versehen mit einem (kanonischen) Haarschen Maß; das ist eine Funktion von s, weil die Quasicharaktere durch die komplexe Variable s parametrisiert werden. Für ein „kanonisches" Φ , das in der Notation weggelassen wird, erweist sich $Z_K(s)$ als das Produkt der Dedekindschen Zetafunktion $\zeta_K(s)$ mit einem Aggregat von Gamma- und Potenzfunktionen, traditionell als „Gammafaktoren" bezeichnet, und ist fortsetzbar zu einer meromorphen Funktion auf der komplexen Ebene mit Polen erster Ordnung an den Stellen $s = 0$ und $s = 1$. Ist nun A eine zentral-einfache K-Algebra der Dimension n^2 , kann man in analoger Weise verfahren. Die Idelgruppe $J(K)$ ist dabei durch die „idelisch gemachte" Gruppe $(A\otimes\mathbf{A}(K))^\times$ zu ersetzen, die Quasicharaktere von $J(K)$ wendet man an auf die Idele, deren Komponenten die reduzierten Normen aus den lokalen Gruppen $(A\otimes K_p)^\times$ sind. Die lokalen Rechnungen (S.195ff) ergeben eine Formel

(7) $$Z_A(s) = C \times \prod_{i = 0,\dots,n-1} Z_K(s-i) \times P ;$$

hierin ist C eine positive Konstante und P ein endliches Produkt aus sehr einfachen (holomorphen) Funktionen, welches nur von den Verzweigungsstellen von A abhängt, also $= 1$ ist, wenn solche nicht vorhanden sind, die Algebra also überall zerfällt. Der Konvergenzbereich des Integrals ist die Halbebene $\mathrm{re}\, s > n$; da die Faktoren $Z_K(s-i)$ auf die ganze Ebene meromorph fortsetzbar und ihre Pole bekannt sind, gilt dasselbe für $Z_A(s)$. Nun hat Weil gesehen, und das ist die hier entscheidende Wendung, daß man den Beweis für die Fortsetzbarkeit vom Körperfall auf den Schiefkörperfall $A = D$ ausdehnen kann; möglich wird das vor allem dadurch, daß das Analogon von $C^1(K)$, die

Faktorgruppe der Norm-Eins-Gruppe von $(D\otimes\mathbf{A}(K))^{\times}$ modulo der Norm-Eins-Gruppe von D , immer noch kompakt ist (das wird falsch, wenn $A = M_m(D)$ mit $m > 1$ ist). Das Ergebnis ist, daß $Z_D(s)$ nur Pole erster Ordnung bei $s = 0$ und $s = d$ hat, wo d der Schurindex von D ist. Wenn nun D überall zerfällt, ist in der Formel (7) $P = 1$, also bis auf eine Konstante $Z_D(s) = \prod_{i = 0,\dots,d-1} Z_K(s - i)$; zählt man die Polordnungen auf beiden Seiten, sieht man sofort, daß diese Gleichung nur für $d = 1$, also $D = K$ bestehen kann. Das beweist den Satz von Hasse-Brauer-Noether.

Damit ist eine Paarung $X(K) \times C(K) \longrightarrow \mathbb{C}^{\times}$ gewonnen, die alle Axiome erfüllt; als wesentliche Aufgabe bleibt jetzt die Bestimmung des Kerns U(K) des kanonischen Morphismus $\mathbf{a} : C(K) \longrightarrow G(K)$. Ein Teil des Kerns auf der Idelebene ist leicht auszumachen, nämlich die Idele (x_p) mit $x_p = 1$ an den endlichen und $x_p > 0$ an den reellen Stellen, insgesamt also $(\mathbb{R}_+)^r \times (\mathbb{C}^{\times})^s$ oder $\bigcap I(K)^{S,n}$ in der Notation von Chevalley (siehe oben 3); das folgt sofort aus der expliziten (sehr einfachen) Struktur der Paarung an den unendlichen Stellen (oder daraus, daß diese Gruppe dividierbar ist, aber kein nichttrivialer Morphismus einer solchen Gruppe in eine proendliche Gruppe existieren kann). Als abgeschlossene Gruppe enthält U(K) damit den Abschluß des Bilds dieser Gruppe in C(K) ; es wird nun bewiesen, daß U(K) genau dieser Abschluß ist. Das geschieht ähnlich wie im Lokalen: zunächst wird gezeigt, daß U(K) im Durchschnitt aller $C(K)^n$ enthalten ist, $n > 0$; aus dem abstrakten Formalismus folgt jetzt schon, daß er gleich diesem Durchschnitt ist (S.272); es ist dann nicht mehr schwierig, zu zeigen, daß er auch mit der oben genannten Gruppe übereinstimmt (l.c.). Damit sind die entscheidenden Argumente vorhanden; die zentralen Aussagen folgen jetzt, weitgehend analog zum lokalen Fall, aus dem abstrakten Formalismus (S. 275f).

7 Die Theorie von Neukirch

7.1 Wie beim kohomologischen Zugang steht auch hier eine Formation am Anfang, also ein Paar (G, A), bestehend aus einer proendlichen Gruppe G, die wir uns gleich als absolute Galoisgruppe eines Körpers k vorstellen, und einem diskreten G-Modul mit stetiger G-Operation (in abstracto (4.2) entspricht k der vollen Gruppe G). Nun treten zwei neue Bestimmungsstücke arithmetischen Charakters hinzu. Das erste ist eine stetige Surjektion $d: G \longrightarrow \mathbb{Z}^\wedge = \text{lim.proj. } \mathbb{Z}/n\mathbb{Z}$, körpertheoretisch also eine $\mathbb{Z}^\wedge$ - Erweiterung von k. Sie gibt Anlaß zu einigen Begriffsbildungen, die unmißverständlich auf die Anwendung in der lokalen Zahlentheorie vorausweisen: für jeden Körper K sei I(K) der Kern von $d: G(K) \longrightarrow \mathbb{Z}^\wedge$, die *Trägheitsgruppe* von K. Mit $I = I(k)$ und $k^\sim$ = Fixkörper von I ist dann $I(K) = G(K) \cap I = G(K) \cap G(k^\sim) = G(Kk^\sim)$, und der Fixkörper $K^\sim$ von I(K) ist das Kompositum $K^\sim = Kk^\sim$, die *maximale unverzweigte Erweiterung* von K . Ist K/k endlich, seien

$$f(K) : = \mathbb{Z}^\wedge : d(G(K)) \quad \text{und} \quad e(K) = I : I(K)$$

gesetzt und (absoluter) *Restklassengrad* und (absoluter) *Verzweigungsindex* genannt. Es besteht dann ein surjektiver Homomorphismus

$$d(K) := 1/f(K) \times d\colon\ G(K) \longrightarrow \mathbb{Z}\hat{}$$

mit dem Kern $I(K)$ und damit ein Isomorphismus $d(K)\colon\ G(K^{\sim}/K) \to \mathbb{Z}\hat{}$. Das Element $\varphi(K)$ von $G(K^{\sim}/K)$ mit $d(K)(\varphi(K)) = 1$ heißt der *Frobenius* von K.

Für eine endliche Erweiterung L/K seien Restklassengrad und Verzweigungsindex durch

$$f(L/K) := d(G(K)) : d(G(L)) \ \text{ und }\ e(L/K) := I(K) : I(L)$$

definiert; diese Funktionen sind multiplikativ in Körpertürmen M/L/K, also $f(M/K) = f(M/L)\, f(L/K)$ und ebenso für e, und es gilt die „Fundamentalformel"

$$[L : K] = G(K) : G(L) = e(L/K)\, f(L/K) .$$

L/K heißt *unverzweigt*, wenn $e(L/K) = 1$, also $L \subset K^{\sim}$, und *rein verzweigt,* wenn $f(L/K) = 1$, also $L \cap K^{\sim} = K$ ist. Stets gilt $L^{\sim} = L K^{\sim}$ und $f(L/K) = [L \cap K^{\sim} : K]$. Für unverzweigte L/K sei $\varphi(L/K)$ das Bild von $\varphi(K)$ in $Gal(L/K)$, der Frobeniusautomorphismus der Erweiterung L/K; da $Gal(K^{\sim}/K)$ topologisch von $\varphi(K)$ erzeugt wird, ist $Gal(L/K)$ zyklisch und wird von $\varphi(L/K)$ erzeugt.

7.2 Bis jetzt haben wir wohlbekannte Tatsachen der lokalen Zahlentheorie in eine rein gruppentheoretische Sprache übersetzt (wie sich diese Begriffe dann im Globalen ausmachen, werden wir später sehen). Nun folgt die für die ganze Theorie grundlegende Beobachtung: wie wir oben (4.3.1) sahen, ist das Reziprozitätsgesetz im (lokalen) unverzweigten Fall sehr einfach zu formulieren und zu beweisen. Neukirch hat nun gesehen, wie man im allgemeinen (galoisschen) Fall beliebige Elemente der Galoisgruppe zu Frobeniuselementen „hochheben" und dann durch eine Normbildung für eine Reziprozitätsabbildung nutzbar machen kann; die Frobeniuselemente beherrschen also „indirekt" auch den allgemeinen Fall! Das erinnert an das oben in der lokalen (globalen) Theorie angewandte Verfahren, die Gruppen $H^2(L/K)$ für allgemeine Galoissche L/K durch die injektive Inflation mit solchen zu identifizieren, die von unverzweigten (zyklischen zyklotomischen) Erweiterungen herkommen, und ist schon im Artinschen Lemma als eine Art „Kreuzung" mit Einheitswurzelkörpern angelegt. Die Konstruktion vollzieht sich in mehreren Schritten:

Für eine galoissche Erweiterung L/K ist auch $L^{\sim}/K$ galoissch; wegen $G(L^{\sim}) = I(L) \subset I(K)$ faktorisiert $d(K)$ über $G(L^{\sim}/K)$, und wir können

$$Frob(L^{\sim}/K) := \{s \in G(L^{\sim}/K) \mid d(K)(s) \in \mathbb{N}\}$$

definieren. Hierfür gilt zunächst: für $s \in Frob(L^{\sim}/K)$ ist der Fixkörper S von s eine endliche Erweiterung von K mit $f(S/K) = d(K)(s)$, und s ist der Frobenius $\varphi(S)$ von S . Ferner ist die Abbildung $Frob(L^{\sim}/K) \to G(L/K)$, $s \to s|L$ surjektiv. In Worten also: jedes $s \in G(L/K)$ kann zu einem Frobenius einer endlichen Erweiterung von K hochgehoben werden.

Nun kommen der Modul der Formation (G, A) und ein weiteres Bestimmungsstück ins Spiel: eine *Bewertung* v *von* A(k) *bezüglich* d ist ein Homomorphismus $v\colon A(k) \to \mathbb{Z}^\wedge$ mit den Eigenschaften

(i) $v(A(k)) = : Z \supset \mathbb{Z}$, und $Z/nZ = \mathbb{Z}/n\mathbb{Z}$, alle n ,

(ii) für endliche K/k ist $v(N_{K/k}(A(K))) = f(K)\, Z$.

Die Abhängigkeit von d liegt in der Eigenschaft (ii), denn $f(K)$ war ja mittels d definiert. Sie hat zur Folge, daß sich v ebenso wie d auf endliche Erweiterungen fortpflanzt: für endliche K/k ist $v(K): = 1/f(K)\, v \circ N_{K/k} : A(K) \to Z$ ein surjektiver Homomorphismus, und es gilt

$$f(L/K)\, v(L) = v(K) \circ N_{L/K} \quad , \ K/L \text{ endlich.}$$

Weiter ist $v(K)$ kompatibel mit der G-Operation im Sinne der Gleichung $v(K) = V(s(K)) \circ s$, $s \in G$; insbesondere ist $v(K)$ invariant unter der Operation von $G(K)$ auf $A(K)$. Ein *Primelement* von $A(K)$ ist ein $p \in A(K)$ mit $v(K)(p) = 1$. Ferner sei

$$U(K) : = \{u \in A(K) \mid v(K)(u) = 0\} ;$$

dies ist ein $G(K)$-Untermodul von $A(K)$.

Für die Definition einer Reziprozitätsabbildung ist nun noch ein Axiom erforderlich, das im folgenden stets als erfüllt angesehen werden soll:

(*) für unverzweigtes endliches L/K ist $H^i(G(L/K), U(L)) = 1$, $i = 0, -1$.

Zunächst wird eine Abbildung

$$r(L^{\sim}/K) : \ Frob(L^{\sim}/K) \to A(K)/N_{L\sim/K}(A(L^{\sim}))$$

definiert (hier ist $N_{L\sim/K}(A(L^{\sim}))$ der Durchschnitt der Normengruppen aller endlichen Teilerweiterungen von $L^{\sim}/K$) : für $s \in Frob(L^{\sim}/K)$ sei S der Fixkörper und $p(S)$ ein Primelement von S; damit sei

$$r(L^{\sim}/K)(s) : = N_{S/K}(p(S) \bmod N_{L\sim/K}(A(L^{\sim})) .$$

Es folgt aus (*), daß die Definition nicht von der Wahl von $p(S)$ abhängt. Als nächstes wird bewiesen, daß $r(\tilde{L}/K)$ multiplikativ, also ein Homomorphismus von Halbgruppen ist (das macht einige Mühe), sodann, daß $r(\tilde{L}/K)$ von $Frob(\tilde{L}/K)$ auf $Gal(L/K)$ „absteigt", genauer: für $s \in Gal(L/K)$ wähle ein Urbild $s\sim$ in $Frob(\tilde{L}/K)$ und bilde $r(\tilde{L}/K)(s\sim)$; das erweist sich unabhängig von der Wahl von $s\sim$ und ergibt den gesuchten *Reziprozitätshomomorphismus*

$$r(L/K) : Gal(L/K) \rightarrow A(K) \bmod N_{L/K}(A(L)) .$$

Ist dabei L/K unverzweigt, so wird $r(L/K)(\varphi(L/K)) = p(K) \bmod N_{L/K}(A(L))$, wie es sein sollte. Weiter kann nun auch das Wohlverhalten von $r(L/K)$ bewiesen werden, welches (mit umgedrehten Pfeilen) dem früher (1.3) beschriebenen der Artinabbildung entspricht.

Für ein Reziprozitätsgesetz, also die Aussage, daß $r(L/K)$ einen Isomorphismus von $Gal(L/K)^{ab}$ mit der Normrestgruppe induziert, wird noch ein stärkeres Axiom gefordert, nämlich

(**) Für zyklische L/K ist $|H^0(G(L/K), A(L)| = [L : K]$ und $|H^1(G(L/K), A(L)| = 1$.

Beide Aussagen werden (für galoissche L/K) auch beim kohomologischen Zugang postuliert; man beachte, daß für zyklische G stets $H^0 = H^2$ ist. Was hier fehlt, ist die Invariantenabbildung; sie ist entbehrlich, weil die Konstruktion von Neukirch die Frobeniusautomorphismen sozusagen direkt ins Spiel bringt und so die „Kanonizität" der Reziprozitätsabbildung sichert. Man beachte auch, daß hier die Abbildungen d und v gar nicht involviert sind; trotzdem ist (*) , wo v durch die Gruppe $U(K)$ eingeht, eine Folge von (**) . Der Beweis des Reziprozitätsgesetzes (S.316ff) vollzieht sich nun durch Reduktion (i) auf den abelschen Fall (Induktion nach der Gruppenordnung), (ii) auf den zyklischen (wieder Induktion) und (iii) den zyklischen reinverzweigten Fall; erst hier geht die Definition der Reziprozitätsabbildung explizit ein. Das Normrestsymbol wird dann definiert als deren Inverse und erbt von ihr das Wohlverhalten.

Wie sonst liefert das Reziprozitätsgesetz eine bijektive und inklusionsumkehrende Korrespondenz zwischen den in $A(K)$ enthaltenen Normengruppen endlicher galoisscher L/K und den (endlichen) abelschen Erweiterungen L/K . Man kann die Normengruppen zur Basis einer Topologie von $A(K)$ machen, dann sind sie genau die offenen Untergruppen von endlichem Index (S.321); das könnte man einen „formalen Existenzsatz" nennen. Damit haben wir den wesentlichen Gehalt von Neukirchs „Allgemeiner Klassenkörpertheorie" dargestellt. Ausdrücklich sollte hervorgehoben werden, daß die Beweise sich (wie schon bei den Klassenformationen) strikt in dem vorgegebenen rein gruppentheoretischen Rahmen halten und von der galoistheoretischen Konkretisierung, die wir sozusagen haben mitlaufen lassen, kein Gebrauch gemacht wird. Die Argumente sind also, wenn man will, elementar, wenngleich subtil.

7.3 Für die Anwendungen muß man, bei gegebener Formation (G, A), (1) zwei Abbildungen d und v mit den verlangten Eigenschaften konstruieren, (2) das Axiom (**) verifizieren und (3) zeigen, daß die natürliche Topologie (wenn es eine gibt) der A(K) mit der Normtopologie übereinstimmt. Für die beiden uns interessierenden Fälle, die lokale und die globale Klassenkörpertheorie, ist die Formation dieselbe wie früher, und die Schritte (2) und (3) erfordern nur Argumente, die schon früher (explizit oder implizit) begegnet sind; wir konzentrieren uns darum auf (1). (Es sollte übrigens bemerkt werden, daß Neukirch auf weitere Anwendungen hinweist, darunter solche außerhalb der Zahlentheorie; siehe die Aufgaben auf den Seiten 322ff.)

Der lokale Fall ist klar. Ein p-adischer Körper k besitzt (wie schon mehrmals erwähnt) für jeden Grad genau eine unverzweigte Erweiterung dieses Grades, und sie ist zyklisch; die maximale unverzweigte Erweiterung $k^\sim$ von k ist also eine $\mathbb{Z}$^ - Erweiterung, und d ist einfach die Restklassenabbildung $\mathrm{Gal}(k^{alg}/k) \to \mathrm{Gal}(k^\sim/k)$. Die Begriffe „Restklassengrad“ und „Verweigungsindex“ haben ihre gewöhnliche Bedeutung, auch der Frobeniusautomorphismus ist der übliche. Sodann ist v(k) die normierte Exponentenbewertung von k , und aus bekannten Tatsachen der Bewertungsfortsetzung folgt dasselbe für die oben konstruierten v(K) .

7.4 Ein ganz anderes Bild bietet der globale Fall; wir legen jetzt $k = \mathbb{Q}$ zugrunde. Um Begriffsverwirrungen vorzubeugen, setzen wir im folgenden die Begriffe aus Neukirchs allgemeiner Theorie in Anführungszeichen. Für die „maximale unverzweigte Erweiterung“ $\mathbb{Q}^\sim/\mathbb{Q}$ haben wir keine Wahl: nach dem Satz von Kronecker-Weber muß sie im Körper aller Einheitswurzeln enthalten sein, und darin findet sich nur *eine* $\mathbb{Z}$^-Erweiterung von $\mathbb{Q}$. Man kann sie so erhalten: für eine ungerade Primzahl p und n > 1 enthält der Körper der p^n-ten Einheitswurzeln genau einen zyklischen Teilkörper vom Grad p^{n-1} über $\mathbb{Q}$; deren Vereinigung ist eine Erweiterung mit der Galoísgruppe lim.proj. $\mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$; für p = 2 kann man analog verfahren. Da diese Erweiterungen paarweise linear disjunkt sind, ist ihr Kompositum eine Erweiterung mit der Galoisgruppe $\prod_p \mathbb{Z}_p \cong \mathbb{Z}$^ ; dies ist der gesuchte Körper $\mathbb{Q}^\sim$ (mehr dazu findet sich S.403f). Für einen Zahlkörper K ist demnach der (absolute) „Restklassengrad“ f(K) = $[K \cap \mathbb{Q}^\sim : \mathbb{Q}]$; er kommt also dem *Körper* K zu, nicht einem seiner Primideale, und dasselbe gilt für den „Verzweigungsindex“ und den „Frobenius“, der also mit den Frobeniusautomorphismen der Artinabbildung nichts zu tun hat. Die Abbildung d ergibt sich dann aus der Restklassenabbildung $G(\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}^{alg}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}^\sim/\mathbb{Q})$ und einem topologischen Isomorphismus $\mathrm{Gal}(\mathbb{Q}^\sim/\mathbb{Q}) \cong \mathbb{Z}$^ (hierfür gibt es zwei Möglichkeiten, aber es kommt auf die Wahl nicht an).

Ein größeres Problem stellt die Definition der „Bewertung“ v dar; denn jetzt ist $A(\mathbb{Q}) = C(\mathbb{Q})$ die Idelklassengruppe, und ein „natürlicher“ Homomorphismus $C(\mathbb{Q}) \to \mathbb{Z}$^ ist gar nicht in Sicht. Die überraschende Lösung ist: man schaltet die Gruppe $\mathrm{Gal}(\mathbb{Q}^\sim/\mathbb{Q})$ dazwischen und hat dann schon d: $\mathrm{Gal}(\mathbb{Q}^\sim/\mathbb{Q}) \to \mathbb{Z}$^ ; ein Morphismus $C(\mathbb{Q}) \to$

$\mathrm{Gal}(\mathbb{Q}^{\sim}/\mathbb{Q})$ wäre die Normrestabbildung – aber die soll doch erst konstruiert werden! Diese Klippe wird nun umschifft, indem als „vorläufiges“ Normrestsymbol das Produkt der lokalen, aus der lokalen Theorie schon verfügbaren Normrestsymbole angesetzt wird. Da dieses Produkt zunächst nur auf der Idelebene definiert ist, muß – wie schon in 4.4.3 und 5.3.4 – zuvor die Hassesche Produktformel für die lokalen Symbole bewiesen werden; das geschieht wie in [N1] mit Hilfe der Lubin-Tate-Theorie. Damit erhält man die gesuchte „Bewertung“ v ; die Eigenschaft (ii) seiner Definition ergibt sich mittels der Verschiebungsformel für das vorläufige Symbol, welches aus derjenigen der lokalen Symbole folgt, und der entsprechenden Eigenschaft der lokalen Symbole (S.408). Da nun alle Voraussetzungen für die Anwendung der Allgemeinen Klassenkörpertheorie erfüllt sind, folgt automatisch das Reziprozitätsgesetz. Um die Kompatibilität der lokalen mit globalen Theorie zu sichern, muß allerdings noch bewiesen werden, daß das „vorläufige“ Normrestsymbol mit demjenigen übereinstimmt, welches der Allgemeinen Theorie als Inverse der Reziprozitätsabbildung entspringt; das erfordert noch einmal den Rückgriff auf die abstrakte Definition von $r(L/K)$ (S.409ff).

Man kann sich fragen, welches Bild sich ergibt, wenn man einen beliebigen Zahlkörper K zum Grundkörper macht. Es können dann verschiedene $\mathbb{Z}_p$-Erweiterungen von K und damit auch verschiedene $\mathbb{Z}^\wedge$ -Erweiterungen existieren; siehe dazu [Wa], S.265. Die Klassenkörpertheorie bleibt aber immer dieselbe. Denn die abstrakte Theorie liefert ja im lokalen unverzweigten Fall die „richtigen“ Frobeniusautomorphismen, damit auch die korrekten Normrestsymbole und damit das globale Zerlegungsgesetz für fast alle p ; dadurch ist aber, wie oben schon bemerkt wurde (4.6), das globale Normrestsymbol bereits festgelegt.

Was den Leser, der irgendeinen andern Zugang zur Klassenkörpertheorie schon kennt, an Neukirchs Theorie zunächst befremden wird, ist die Übertragung der bewertungstheoretischen Begriffe vom Lokalen ins Globale, wo sie eine ganz andere Bedeutung annehmen als die vertraute. Das ist natürlich nur eine Frage der Nomenklatur. Schön wäre, wenn man für diese Begriffe Verallgemeinerungen hätte, die bei Spezialisierung aufs Lokale bzw. Globale die üblichen Bedeutungen annehmen bzw. nicht mit ihnen in Konflikt geraten. Statt „maximale unverzweigte Erweiterung“ könnte man einfach „kanonische $\mathbb{Z}^\wedge$-Erweiterung“ sagen; aber bei „Restklassengrad“ ect. käme man in Schwierigkeiten; das Einfachste wäre, auf Namen ganz zu verzichten und sich mit den Symbolen zu begnügen, wie es bei der Abbildung d ja auch geschieht. Die Funktion der Abbildungen d und v ist allein, einen gruppentheoretischen Apparat zu konstituieren, der ein Reziprozitätsgesetz liefert. In diesem selbst kommen sie explizit nicht mehr vor; sie bilden, mit Wittgenstein zu reden, die Leiter, die man wegstoßen kann, wenn man auf ihr heraufgestiegen ist.

8 Schlußbemerkungen

Am Ende seines Aufsatzes über die Entwicklung der Klassenkörpertheorie bis zum 2.Weltkrieg ([H4]) schrieb Hasse: „...The sharply profiled lines and individual features of this magnificent edifice seem to me to have lost somewhat of their original splendour and plasticity by the penetration of class field theory with cohomological concepts and methods, which set in so powerfully after the war.“ Wenn man in seinen Marburger Vorlesungen im § 10 die Parade der Hauptsätze dieser älteren Theorie liest, wird man geneigt sein, ihm zuzustimmen. Man wird aber auch korrigieren: die alten Linien haben nichts verloren, nur sind neue ans Licht getreten. Hierzu Lang: „If there is one piece of moral which deserves emphasis, however, it is that no one piece of insight which has been evolved since the beginning of the subject has ever been „superseded“ by subsequent pieces of insight“ ([La], S.176). Bei einem Gegenstand von solcher Bedeutung muß jeder neue Zugang willkommen sein, jeder Aspekt ausgeleuchtet werden. Eine Methode überflüssig zu machen, ist nicht *per se* ein Verdienst; dieses liegt dann darin, daß eine andere zur Geltung gebracht wird. Gerade daß es so verschiedene Zugänge gibt, unterstreicht die Bedeutung des Gegenstands. Diese einfache Feststellung gewinnt noch ein besonderes Gewicht, wenn man die abelsche Klassenkörpertheorie als den ersten Schritt zu einer allgemeinen ansieht, die beliebige galoissche Erweiterungen erfaßt. Frühestens dann, wenn Resultate vorliegen, welche die zentralen Aussagen der abelschen Theorie, also ein Zerlegungsgesetz und einen Existenzsatz, als Spezialfälle enthalten, wird man den Wert, oder besser: den „strukturellen Ort“ der verschiedenen Zugänge beurteilen können. Von Vereinfachungen sollte man übrigens nur reden, wo *innerhalb desselben begrifflichen Systems* ein kürzerer Weg von den Voraussetzungen zu den Resultaten gefunden wird. Zu bedenken ist bei Abwägungen solcher Art auch, daß der kürzeste Weg nicht notwendig der ist, auf dem man am meisten sieht.

Der erwachsene Zahlentheoretiker sollte die herangezogenen Hilfsdisziplinen ohnehin kennen. Die Algebrentheorie kann zweifellos ein unabhängiges Interesse beanspruchen, allein schon deswegen, weil unsere algebraischen Grundbegriffe mit einer gewissen Zwangsläufigkeit zu ihr hinführen. Die Kohomologie wird nicht nur in der Klassenkörpertheorie, sondern auch in der Struktur- und Darstellungstheorie allgemeiner Gruppen angewandt, nicht zu reden von den Verbindungen zur Topologie. Sie erscheint leicht als ein „rätselvoller formaler Mechanismus“ (Neukirch), als eine Art *black box*, die aus Eingaben Resultate produziert. Aber das ist eine Umkehrung der wahren Verhältnisse – die wahre *black box* ist das Genie, welches seiner Intuition folgend das Richtige tut, und nicht die nachträgliche Aufklärung, warum eben das richtig war. Die Kohomologie zerlegt gruppen- und modultheorische Schlußweisen in ihre logischen Atome, und ihre Komplexität entsteht durch die Iteration einfacher Schritte (wobei freilich irgendwann ein Umschlag von Quantität in Qualität stattfindet). Die weitesten Perspektiven scheint die Analysis zu bieten – sie liefert nicht nur den einfachsten Beweis von Ungleichung A, sondern auch Resultate wie Dichtigkeits- und Primzahlsätze, die rein algebraisch gar nicht formulierbar sind, nicht zu reden von den Vermutungen, die sich um spezielle Werte oder Ordnungen der Zeta- und L-Funktionen an speziellen Stellen ranken. In den Artinschen L-Funktionen (genauer: ihren Eulerfaktoren) sind die Zerlegungsgesetze kodifiziert (siehe dazu meine Arbeit [Kl]). Weil erschienen die klassischen Anwendungen als „some magician's bag of tricks“ entsprungen, und er wollte mehr Systematik, wozu er die Methoden aus Tate's Thesis ausbaute (in Rahmen des Langlandsprogramms ist der Ausbau weiter fortgeschritten); aber sein eigener, oben skizzierter Beweis des Satzes von Hasse-Brauer-Noether verblüfft auf dieselbe Weise wie Dirichlets analytischer Beweis seines Primzahlsatzes.

Das leitet über zu dem Befund, daß sich in der Vielfalt der Zugänge einmal mehr die zentrale Stellung der Zahlen und arithmetischen Fragestellungen im Gesamtgefüge der Mathematik erweist. Die Zahlen erzeugen aus sich selbst heraus die Grundrechenarten und damit, durch eine lange Folge natürlicher Abstraktionen, das Gesamtreich der Algebra; wie wir gesehen haben, sind auch die nichtkommutativen Algebren für die Klassenkörpertheorie fruchtbar zu machen. Mit den verschiedenen Komplettierungen der Zahlkörper kommen Topologie und Analysis ins Spiel, reelle, komplexe und p-adische. Der (gegenwärtig) aussichtsreichste Weg zu einer nichtabelschen Klassenkörpertheorie, das Programm von Langlands, involviert algebraische Gruppen und ihre Darstellungen und damit weitere Gebiete der Analysis und Funktionalanalysis. Kurz, es gibt wohl kaum eine mathematische Disziplin, die nicht früher oder später in der Zahlentheorie Anwendung findet, und wenn irgendwo, dann manifestiert sich darin die wahre Einheit aller Mathematik. Aber damit verlassen wir unser Thema.

Literatur

[AT] E.Artin, J.Tate, Class Field Theory, Harvard 1967

[AW] M.Atiyah, C.T.C.Wall, Cohomology of Groups, in [CF]

[C] J.Cassels, Global Fields, in [CF]

[CF] J.Cassels, A.Fröhlich (edts.), Algebraic Number Theory, Academic Press 1967

[Ch1] C.Chevalley, La théorie du corps de classes, Ann.Math. 41 (1940), 394-418

[Ch2] C.Chevalley, Class Field Theory, Nagoya 1953

[Co] H.Cohen, Advanced Topics in Computational Number Theory, Springer-Verlag 2000

[F] I.Fesenko, Class Field Theory, Its three Main Generalizations and Applications, www

[FV] I.Fesenko, S.Vostokov, Local Fields, AMS 1993

[H1] H.Hasse, Bericht über neuere Untersuchungen...[„Zahlbericht"], I und II, Jahresberichte DMV 35 (1926), 36 (1927), 39 (1930) ; zitiert aus dem Nachdruck Physica-Verlag 1965

[H2] H.Hasse, Vorlesungen über Klassenkörpertheorie (Marburger Vorlesungen), Physica-Verlag 1967

[H3] H.Hasse, Die Struktur der R.Brauerschen Algebrenklassengruppe... Math.Annalen 107 (1933), 731-760 = Mathem. Abhandlungen, Band 1, Nr.31

[H4] H.Hasse, History of Class field Theory, in [CF]

[Ha] D.Harari, Galois Cohomology and Class Field Theory, Springer-Verlag 2020

[Haz] M.Hazewinkel, Local Class Field Theory is Easy, Adv.in Math. 18 (1975), 148-181

[I] S.Iyanaga, Travaux de Claude Chevalley sur la théorie du corps de classes: Introduction, Japan.J.Math. 1 (2006), 25-85

[Iw] K.Iwasawa, Local Class Field Theory, Oxford UP 1986

[J] G.Janusz, Algebraic Number Fields, Academic Press 1973

[K1] H.Koch, Zahlentheorie, Braunschweig 1997

[K2] H.Koch, Algebraic Number Theory, in: Number Theory, ed. A.N.Parshin, Springer-Verlag 1988

[KKS] K.Kato, N.Kurokawa, T.Saito, Introduction to Class Field Theory, AMS, Providence 2011

[Kl] E.Kleinert, Über Zerlegungsgesetze, Hamb.Beitr.z.Math. Nr.554, 2015

[La] S.Lang, Algebraic Number Theory, Springer-Verlag 1986 (GT 110)

[Lo1] F.Lorenz, Algebra II, Mannheim 1990

[Lo2] F.Lorenz, Algebraische Zahlentheorie, Mannheim 1993

[M] D.Marcus, Number Fields, Springer-Verlag 1977

[Mi] J.Milne, Class Field Theory, www (2008)

[N1] J.Neukirch, Klassenkörpertheorie, Mannheim 1969

[N2] J.Neukirch, Class Field Theory, Springer-Verlag 1986

[N3] J.Neukirch, Algebraische Zahlentheorie, Springer-Verlag 1992

[S] J.-P.Serre, Local Class Field Theory, in [CF]

[SC] J.-P.Serre, Corps Locaux, Paris 1962, engl. Local fields, Springer-Verlag 1979

[T] J.Tate, Global Class Field Theory, in [CF]

[vdW] B.L.van der Waerden, Algebra 2, Springer-Verlag 1967

[W] A.Weil, Basic Number Theory, Springer-Verlag 1974

[Wa] L.Washington, Introduction to Cyclotomic Fields, Springer-Verlag 1982
(GT 83)