Hamburger Beiträge zur Mathematik

Nr. 554, Juli 2015

Über Zerlegungsgesetze

von Ernst Kleinert

Über Zerlegungsgesetze

Das Folgende ist weder ein Übersichtsartikel, noch findet man darin neue Resultate. Meine Absicht war, das Wichtigste zusammenzustellen, was über Primzerlegung in Zahlkörpern bekannt ist und im Rahmen des Programms von Langlands erwartet wird, also eine Art Standortbestimmung; zweifellos bedarf sie mannigfacher Ergänzung. Ein paar einfache Überlegungen, die mir in der Literatur selten oder gar nicht begegnet sind, mögen dem von Nutzen sein, dem (um einen Goetheschen Ausdruck abzuwandeln) die "Taten und Leiden" der Primzahlen in endlichen Erweiterungen des rationalen Grundkörpers ein Gegenstand des Interesses sind. Es liegt in der Natur der Sache, daß dabei auch Betrachtungen „philosophischer" Art anfallen.

I Klassische Theorie

1. Die allgemeine Situation, in der ein Zerlegungsproblem vom arithmetischen Typ auftaucht, ist die folgende. Sei R ein Dedekindring mit Quotientenkörper K, L/K eine endliche Körpererweiterung und S der ganze Abschluß von R in L. Dann ist S wieder ein Dedekindring, und jedes (vom Nullideal verschiedene) Primideal p von R erzeugt in S ein Ideal pS mit verschiedenen Primfaktoren $P_1,...,P_r$, Exponenten (Verzweigungsindices) e_i und Restklassengraden $f_i = f(P_i/p) = [S \bmod P_i : R \bmod p]$; ist L/K separabel, gilt dabei die fundamentale Formel

$$n := [L : K] = e_1f_1 + \ldots + e_rf_r .$$

Ein Zerlegungsgesetz für die Erweiterung L/K [1] ist, in erster Annäherung, ein solches, das für jedes vorgegebene p die Paare (e_i, f_i) liefert. Nur für endlich viele p (die "verzweigten") tauchen Exponenten $e > 1$ auf; läßt man diese einmal außer Betracht [2], bleibt die Angabe des Vektors der f_i . Es ist klar, daß bei gegebener Erweiterung L/K, nur endlich viele Zerlegungstypen möglich sind, die natürlich nicht alle vorkommen müssen. Für Erweiterungen von Zahlkörpern jedoch folgt aus dem Satz von Tschebotareff [3], daß ein unverzweigter Typ, der überhaupt vorkommt, unendlich oft vorkommt (sogar mit einer angebbaren Dichte). Unter diesen ist einer ausgezeichnet, nämlich der vollzerlegte Typ (1,...,1), der immer vorkommt; das folgt auch daraus, daß nur die (in $L/\mathbb{Q}$, also a fortiori in L/K) vollzerlegten Primzahlen (bzw. -Ideale) zum Pol der Zetafunktion von L beitragen.

Ist L/K galoissch, operiert die galoissche Gruppe transitiv auf den Primteilern P_i von p, woraus leicht folgt, daß alle e_i und alle f_i (wohlgemerkt, bei festem p) untereinander gleich sind, wodurch sich die Fundamentalformel zu der Gleichung $[L : K] = efr$ vereinfacht, und ein Zerlegungsgesetz, wenn wir wieder von den endlich vielen verzweigten p absehen, einfach in der Angabe von f (oder r) besteht. Die möglichen Typen entsprechen also bestimmten Teilern von n; nur die Elementordnungen kommen als f vor, zum Beispiel alle Primteiler von n, und $f = n$ nur dann, wenn die Gruppe zyklisch ist.

2. Eine allgemeine Antwort auf die Zerlegungsfrage gibt das Polynomzerlegungsgesetz (PZG): Sei a ein ganzes primitives Element für die Erweiterung, also $L = K(a)$, $a \in S$, und $f(x) \in R[x]$ sein Minimalpolynom. Weiter sei p kein Teiler des Annihilators von S mod R[a] (im Zahlkörperfall einfacher: kein Teiler des Index $[S : R(a)]$). Zerfällt dann f(x) mod p in ein Produkt von s verschiedenen irreduziblen Faktoren mit Vielfachheiten d_j und Graden g_j, dann ist $r = s$, und nach eventueller Umnumerierung $d_i = e_i$ und $g_i = f_i$.

Der Beweis ist so einfach, daß wir ihn nicht vorzuenthalten brauchen: ist p wie oben zerlegt, so hat die R/p – Algebra S/pS genau r unzerlegbare Faktoren (oder einfache Moduln, oder primitive Idempotente), ein Faktor S/P^e hat die Länge e (als regulärer Modul über sich selbst), und f ist die Dimension seines einfachen Moduls über R/p. Eine analoge Analyse besteht für den Restklassenring R[x]/(f(x)), der zu R[a] isomorph ist. Aus der Voraussetzung an p folgt aber $R[a]/p \simeq S/p$. Da die genannten Bestimmungsstücke nur vom Isomorphietyp der Algebren abhängen, folgt die behauptete Gleichheit[4].

Die Simplizität des Arguments läßt schon vermuten, daß es sich hier eher um eine Umformulierung als eine Lösung des Problems handelt; was als „wirkliche Lösung" gelten soll, werden wir an Beispielen gleich sehen. Man sollte aber bemerken, daß das PZG im Zahlkörperfall (auf den wir uns von jetzt ab beschränken) wenigstens zu einer algorithmischen Lösung des Zerlegungsproblems führt; denn anders als Primzerlegung ganzer Zahlen ist Primzerlegung von Polynomen über endlichen Körpern effizient durchführbar [5] (für globale Funktionenkörper ist *alles* einfacher als für Zahlkörper). Ein Algorithmus ist kein Ersatz für ein Gesetz; es ist aber nicht einfach, den Unterschied formal klar zu bestimmen (am ehesten durch einen Vergleich, nämlich mit dem Unterschied zwischen einer Wegbeschreibung und einer Karte). Daß ein Algorithmus das richtige Ergebnis liefert, ist auch eine Strukturaussage, wenn auch eine implizite.

3. Eine offensichtliche Schwäche des PZG scheint zu sein, daß es von einem f oder a ausgeht, ein solches aber im Allgemeinen nicht „kanonisch" zu haben ist. Man könnte zurückfragen, wodurch sonst denn ein Zahlkörper überhaupt gegeben werden kann. Immerhin haben die meisten Zahlkörper, mit denen man sich üblicherweise befaßt, durchaus kanonische Erzeuger, wie alle Kummerschen Körper (so alle quadratischen, allgemeiner alle 2-elementaren), Kreisteilungskörper oder solche, die durch Adjunktion (von Koordinaten) von Teilungspunkten abelscher Varietäten entstehen. Das wirft die Frage auf, ob es nicht für *jeden* Zahlkörper ausgezeichnete Erzeuger gibt; der „Kroneckersche Jugendtraum" ist davon ein Spezialfall.

Aber das PZG zeigt gerade durch seine Aussage, daß die „Nicht-Kanonizität" eben an der Oberfläche liegt, indem sie nur endlich viele Primzahlen betrifft. Man kann geradezu den Spieß umdrehen und das PZG weniger als eine Aussage über Zerlegungen als über Polynome betrachten: es gibt nämlich eine notwendige Bedingung dafür, daß zwei Polynome f und g denselben Körper erzeugen: sie müssen für fast alle p in gleicher Weise mod p zerfallen; sind sie Galoissch (ein Wurzelkörper ist schon Zerfällungskörper), ist diese Bedingung nach dem Satz von Bauer (s.u.) auch

hinreichend. Diese keineswegs an der Oberfläche liegende, ohne die Arithmetik der Zahlkörper gar nicht verständliche Tatsache wird selten vermerkt.

4. Wir legen uns nun den einfachsten Fall vor, quadratische Erweiterungen $K = (\mathbb{Q}\sqrt{d})$ mit ganzem quadratfreiem d. Für ungerade Primzahlen p ist PZG mit $f(x) = x^2 - d$ anwendbar und liefert $e = 2$ (p „verzweigt“) falls $p|d$; andernfalls $r = 2$ (p „zerlegt“) wenn $(d/p) = 1$ und $f = 2$ (p „träge“) wenn $(d/p) = -1$ (hier bezeichnet (d/p) das Legendresymbol). Für $p = 2$ sind ein paar spezielle Überlegungen nötig, die wir auslassen.

Bekanntlich kann man es viel besser machen. Es sei D die Diskriminante von K; es ist $D = d$, wenn $d \equiv 1 \bmod 4$, $D = 4d$, wenn $d \equiv 2,3 \bmod 4$. Wir definieren eine Funktion auf $\chi = \chi_D$ auf $\mathbb{Z}$ durch $\chi(p) = (D/p)$ für ungerades p (= 0 für $p|d$); $\chi(2) = 0$ für gerades D, $\chi(2) = 1$ wenn $D \equiv 1 \bmod 8$, $\chi(2) = -1$ wenn $D \equiv 5 \bmod 8$ sowie $\chi(-1) = \operatorname{sgn} d$ und natürlich $\chi(0) = 0$. Gemäß der eindeutigen Primzerlegung ganzer Zahlen setzt sich χ fort zu einer multiplikativen Funktion $\mathbb{Z} \to \{0,1,-1\}$, und es ist $\chi(p) = 0, 1$ oder -1, je nachdem p verzweigt, zerlegt oder träge ist. Bis hierher ist alles nur eine Umformulierung des Vorigen, aber jetzt geschieht ein Mirakel, und dies ist essentiell das Quadratische Reziprozitätsgesetz: χ erweist sich als *periodisch* mit der Periode D, genauer als ein primitiver Dirichletcharakter mod D; das Zerlegungsverhalten der Primzahl p, vom PZG durch $d \bmod p$ bestimmt, hängt also nurmehr ab von $p \bmod D$.

Warum ist das besser? Rein algorithmisch ließe sich sagen: es ist leichter, p mit Rest durch D zu dividieren (also den Kongruenzwert von p mod D zu bestimmen) als (d/p) auszurechnen. Das spielt sicherlich eine sehr untergeordnete Rolle (im Zeitalter elektronischen Rechnens gar keine mehr). Viel bedeutsamer ist, daß wir für die Einteilung der Primzahlen nach ihrem Zerlegungsverhalten jetzt ein Schema benennen können: nämlich die Einteilung nach einem Modul; hiermit kommt in das Problem eine *Struktur*, nämlich die einer abelschen Gruppe. Das setzt uns instand, zu sagen, wann zwei Primzahlen p,q dasselbe Zerlegungsverhalten haben, *ohne daß wir dieses kennen*: nämlich sicher dann, wenn sie zueinander kongruent mod D sind. Für Derartiges bietet das PZG keinerlei Anhalt; es macht keine Aussage über die Art der Partition, anders gesagt über die Gesetzmäßigkeit, nach der die Zerlegungen *verschiedener* p zusammenhängen.

Es lohnt vielleicht die Mühe, die Sachlage ein wenig zu formalisieren. Das Polynom (oder der Zahlkörper) definiert eine Funktion

$$Z(f): \{\text{Primzahlen}\} \to \{\text{Zerlegungstypen}\},$$

und das PZG gibt uns nicht mehr als eine Möglichkeit, diese Funktion für einzelne Argumente auszuwerten. Wir fragen nach einem „inneren Band“, das die verschiedenen Werte von Z(f) korreliert, also einer Art Funktionalgleichung, insbesondere nach einer Charakterisierung der Fasern dieser Abbildung. Die Frage erscheint zuerst töricht, denn was sonst als f selbst kann dieses „innere Band“ sein? Aber f „zeigt“ uns nicht, was wir suchen. Es entsteht die Frage nach dem *quid iuris* unserer Frage: mit welchem Recht

erwarten wir, daß eine Funktion, die irgendwie definiert ist, darüber hinaus noch Gesetzmäßigkeiten irgendwelcher Art aufweist? Die Zahl π definiert die Ziffernfolge ihrer Dezimalentwicklung, aber noch niemand hat darin eine Gesetzmäßigkeit entdecken können. Andererseits, wie kann es in der Mathematik etwas „Zufälliges" geben? Hier kommen wir an methodische Grundfragen: was ist „Zufall", was ist „Gesetzmäßigkeit"? Dieser Fragen sind wir hier enthoben, und zwar durch das Phänomen der quadratischen Reziprozität: dieses gibt den ersten Hinweis darauf, daß die Frage nicht sinnlos ist, daß hinter der Primzerlegung noch eine Gesetzmäßigkeit von ganz anderer Natur und ganz anderm Ursprung steckt, als der elementar-algebraische Kontext, in dem sie formuliert wird, erwarten läßt.

5. Die Verallgemeinerung des eben für quadratische Körper beschriebenen Sachverhalts auf beliebige (endliche) abelsche Erweiterungen L/K von Zahlkörpern ist das Artinsche Reziprozitätsgesetz. Ordnet man jedem unverzweigten Primideal p von K seinen Frobenius-Automorphismus (L/K, p) zu, ein Element der Galoisschen Gruppe G = Gal(L/K), dessen Ordnung der (gemeinsame) Restklassengrad f(P/p) der Primteiler P von p ist, entsteht zunächst ein Homomorphismus von der Gruppe der unverzweigten K-Ideale in G, die Artin-Abbildung, die im Kern die Relativnormen der (unverzweigten) L-Ideale enthält, insbesondere die in L vollzerlegten Primideale von K. Soviel folgt trivial aus den Definitionen; alles andere als trivial ist nun erstens, daß diese Abbildung surjektiv ist, und zweitens (und das entspricht dem oben als Mirakel bezeichneten Sachverhalt), daß sie in ihrem Kern einen *Strahl* enthält, das sind alle Hauptideale mit einem Erzeuger, der einer bestimmten Kongruenzbedingung genügt (hier müssen auch die unendlichen Primstellen von K berücksichtigt werden; der endliche Teil des „Erklärungsmoduls" muß wenigstens alle verzweigten Primideale in genügend großer Potenz enthalten). Informell gesprochen: das Zerlegungsverhalten ist „periodisch", eine Tatsache, die durch die ursprüngliche Fragestellung in keiner Weise auch nur angedeutet wird. Insgesamt erhält man einen Isomorphismus

$$(L/K, .) : H = \text{Verallgemeinerte Idealklassengruppe} \rightarrow \mathrm{Gal}(L/K),$$

der also das Zerlegungsverhalten der p durch die Ordnung ihrer Klasse in H beschreibt. Um den quadratischen Fall hier zu subsumieren, muß man die Abbildung χ auf die unverzweigten p einschränken und erhält einen Gruppenhomomorphismus

$$\chi : (\mathbb{Z} \bmod D\mathbb{Z})^{\times} \rightarrow \mathrm{Gal}((\mathbb{Q}\sqrt{d})/\mathbb{Q}) = \{\pm 1\},$$

der (im wesentlichen) schon die Artinabbildung ist; jetzt braucht man nur noch zu bemerken, daß das nichttriviale Element von G der Frobenius der trägen p ist.

Bemerkenswert scheint mir, daß in einem „zentralen" Fall, nämlich $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_m)$, ζ_m eine primitive m-te Einheitswurzel, der Beweis des Artinisomorphismus so einfach ist, daß wir ihn hersetzen können: man braucht nur 1), daß der Ganzheitsbereich von L als $\mathbb{Z}$-Modul von ζ_m erzeugt wird, und 2), daß Reduktion nach einem zu m teilerfremden Primideal auf der Einheitswurzelgruppe injektiv ist. Sei also die rationale Primzahl p kein Teiler von m und P ein Teiler von p in L. Aus 1) folgt, daß der

Restkörper mod P über $\mathbb{Z}$ mod p vom Bild von ζ_m erzeugt wird, und aus 2) folgt, daß dieser Körper die kleinste Erweiterung von $\mathbb{Z}$ mod p ist, die eine m-te Einheitswurzel enthält. Da endliche Körper zyklische Multiplikationsgruppen haben, ist der gesuchte Restklassengrad das kleinste f derart, daß m ein Teiler von $p^f - 1$ ist, anders ausgedrückt: f ist die Ordnung von p mod m. Daraus folgt, daß der Artinisomorphismus in diesem Fall nichts anderes ist als der aus jeder Algebravorlesung bekannte Isomorphismus

$$(\mathbb{Z} \bmod m)^\times \quad \rightarrow \quad \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) , \; a \bmod m \; \rightarrow (\zeta_m \; \rightarrow \; \zeta_m^{\,a}) .$$

Das ist einfacher als das Reziprozitätsgesetz für quadratische Körper [6], obwohl diese (wie alle abelschen Erweiterungen von $\mathbb{Q}$) in Einheitswurzelkörpern enthalten sind, und soweit ich sehe, der einzige Fall überhaupt, in dem die Artin-Reziprozität mit elementar-algebraischen Argumenten bewiesen werden kann!

6. Hier ist Anlaß für eine Bemerkung zur Terminologie. Es ist üblich geworden, die Begriffe „Zerlegungsgesetz“ und „Reziprozitätsgesetz“ mehr oder weniger unterschiedslos zu verwenden; schon die Bestimmung der Mengen S(L/K) voll zerlegter Primideale wird „higher reciprocity“ genannt. Im Hinblick auf die Autoritäten, die diesen Gebrauch sanktioniert haben, ist daran wohl nichts mehr zu ändern, aber man sollte sich doch des Unterschieds bewußt sein. Im Allgemeinen reden wir von Reziprozität, wenn sich ein X zu einem Y ebenso oder analog verhält wie Y zu X; das setzt zum mindesten voraus (wenn wir die fragliche Relation R nennen), daß mit R(X,Y) auch R(Y,X) definiert ist. Das erste Beispiel bietet der Begriff selbst: wenn a reziprok zu b ist, dann auch b zu a. Reziprozität ist also ein Verhältnis zwischen Verhältnissen, wie es in der Formel $(p/q) = (q^*/p)$ der quadratischen Reziprozität (und ihrer Verallgemeinerung auf höhere Potenzreste) sogar gestalthaft zum Ausdruck kommt, aber auch, beispielsweise, in der Formel $< \chi, \; \mathrm{res}\, \psi > \; = \; < \mathrm{ind}\; \chi \, , \psi >$ der Frobenius-Reziprozität oder der Formel $\mathrm{Hom}(F(A), B) = \mathrm{Hom}(A, G(B))$ für die Adjunktionsbeziehung von Funktoren F und G.

Artin hat sein Reziprozitätsgesetz selbst so benannt, weil sich aus ihm alle klassischen Reziprozitäten durch mehr oder weniger kanonische (wenn auch keineswegs tautologische) Überlegungen herleiten lassen, während „elementare“ Beweise sämtlich so langwierig oder indirekt sind, daß man selbst im quadratischen Fall nach immer neuen gesucht hat (es gibt weit mehr als hundert). Aber in der Aussage des Artin-Isomorphismus liegt nichts von eigentlicher Reziprozität, wie sie oben umrissen wurde; ihr Kern ist eine Isomorphie zwischen zwei Strukturen, die zunächst nicht viel miteinander zu tun zu haben scheinen[7]. Wenn wir uns dem Sprachgebrauch anschließen, dann nicht ohne Vorbehalt: ein Reziprozitätsgesetz sollte über das PZG mindestens insofern hinausgehen, als es eine a-priori-Bedingung für gleiches Zerlegungsverhalten impliziert; das wiederum ist nur möglich, wenn dieses Verhalten aus irgend einer Art „Struktur“ abgeleitet werden kann, die vom PZG „unabhängig“ ist. „Struktur“ ist ein vager Begriff; im Falle der Klassenkörpertheorie ist diese Struktur eine endliche abelsche Gruppe; wir werden unten sehen (oder ahnen), womit noch zu rechnen ist. Vage ist auch der Begriff der Unabhängigkeit; in einer axiomatischen Theorie ist jede

Beweisführung eine Kette von Tautologien, und nach den Gesetzen der materialen Logik sind alle wahren Aussagen äquivalent. Klar ist aber a limine, daß der Komplexitätsunterschied zwischen dem allgemeinen und dem abelschen Fall nicht geringer sein wird als der zwischen beliebigen und abelschen endlichen Gruppen, und dieser ist schon gewaltig; er wird sogar noch viel größer sein, denn die Gruppentheorie ist ja nur ein Ingrediens der arithmetischen Struktur, in gewisser Weise ihr Rahmen: die galoissche Gruppe legt die möglichen Zerlegungstypen fest, und das Problem ist gerade, die Verteilung der p auf die Typen zu beschreiben.

7. Die durch den Artinisomorphismus gegebene Beschreibung des Zerlegungsverhaltens durch (verallgemeinerte) Kongruenzen ist *nur* für abelsche Erweiterungen möglich. Das ergibt sich aus der Kombination zweier weiterer Sätze: der erste ist (nach dem Artinisomorphismus) der zweite Hauptsatz der Klassenkörpertheorie, der *Existenzsatz*: die abelschen Erweiterungen eines Zahlkörpers K entsprechen bijektiv den verallgemeinerten Idealklassengruppen von K (modulo einer Äquivalenzrelation, auf die es im Augenblick nicht ankommt), und wenn dabei $H \leftrightarrow L$, so ist $H \cong \mathrm{Gal}(L/K)$. vermöge der Artin-Abbildung. Der zweite ist ein Satz von Bauer (der Klassenkörpertheorie übrigens vorausgegangen), der aussagt, daß der ganze Verband der galoisschen (nicht notwendig abelschen) Erweiterungen L eines festen Zahlkörpers K schon durch die zugeordneten Mengen $S(L/K)$ voll zerlegter Primideale bestimmt ist: es ist $S(L/K) \subset S(N/K)$ dann und nur dann, wenn $N \subset L$. Aus diesen beiden Sätzen folgt: enthält $S(L/K)$ die Primideale eines Strahls, so ist L im zugehörigen Strahlklassenkörper enthalten (also insbesondere abelsch); ist $S(L/K)$ in einem Strahl enthalten, so ist dieser Körper Teilkörper von L. Der „abelsche Teil" der Primzerlegung ist leicht zu beschreiben: die maximale über K abelsche Teilerweiterung L^{ab} von L hat die galoissche Gruppe $G_{ab} = G/G'$, wobei G' die Kommutatorgruppe bezeichne, und ist p unverzweigt, P ein Teiler von p in L und (L/K,P) das zugehörige Frobeniuselement, dann ist $p \rightarrow (L/K,P) \bmod G'$ wohldefiniert und induziert die Artinabbildung für L^{ab}/K.

8. Um einen ersten Blick in die nichtabelsche Welt zu tun, betrachten wir den Körper K, der aus $\mathbb{Q}$ durch Adjunktion von a, $a^3 = 2$ und einer primitiven dritten Einheitswurzel ζ entsteht; K ist galoissch über $\mathbb{Q}$ mit der Gruppe D_3 (oder S_3) [8]. Fragen wir nach der Menge $S(K/\mathbb{Q})$, sehen wir sofort, daß die Primzahl p in K genau dann voll zerlegt ist, wenn dies in $\mathbb{Q}(\zeta)$ sowie in $\mathbb{Q}(a)$ der Fall ist. Ersteres ist gleichbedeutend mit $p \equiv 1 \bmod 3$, letzteres mit $(2/p)_3 = 1$, wobei $(x/p)_3$ das Symbol für dritte Potenzreste mod p bezeichne. Dieses „lebt" in $\mathbb{Z}[\zeta]$, und in *diesem* Ring läßt sich, vermöge des Reziprozitätsgesetzes der dritten Potenzreste, die fragliche Eigenschaft (bei gegebenem x) durch Kongruenzen für p ausdrücken. Da eine Primzahl $p \equiv 1 \bmod 3$ in $\mathbb{Z}[\zeta]$ in ein Produkt von zwei Primelementen zerfällt, erhalten wir Kongruenzbedingungen für diese beiden, die sich aber nicht zu einer *Kongruenzbedingung für* p *in* $\mathbb{Z}$ zusammenfassen lassen; man erhält vielmehr als notwendige und hinreichende Bedingung für $p \in S(K/\mathbb{Q})$ die *diophantische* Bedingung, daß p die Form $x^2 + 27y^2$ (mit ganzen x,y) hat; dies wiederum bedeutet, daß p die Norm des Elements $x + 3\sqrt{-3}y$ aus der Ordnung $\mathbb{Z}[3\sqrt{-3}]$ in $\mathbb{Z}[\zeta]$ ist. Überraschen muß, daß diese Bedingung, rein äußerlich wenigstens, nichts zu tun hat mit der durch das PZG für die Erweiterung $\mathbb{Q}(a)$

gegebenen, nämlich der Frage, wie das Polynom $x^3 - 2$ modulo verschiedener p zerfällt (das ist die eigentümliche Wirkung echter Reziprozität). Für $p \equiv 2 \bmod 3$ ist Potenzieren mit 3 ein Automorphismus der Gruppe $(\mathbb{Z} \bmod p)^\times$, also zerfällt $x^3 - 2 \bmod p$ in einen linearen und einen (irreduziblen) quadratischen Faktor; für $p \equiv 1 \bmod 3$ jedoch bilden die dritten Potenzen eine Untergruppe vom Index 3 in dieser Gruppe, und das Polynom bleibt entweder irreduzibel oder zerfällt vollständig. Um hier zu entscheiden, bleibt nur der Weg über den „höheren" Zahlbereich der Einheitswurzeln, und man gelangt zu einer Bedingung, die sich nicht mehr auf (rationale) Kongruenzen bringen läßt, *und zwar aus prinzipiellen Gründen.* Dies ist ein erstes Beispiel für die „Einwirkung" der Klassenkörpertheorie auch auf nichtabelsche Situationen. Es ist jetzt leicht, das vollständige Zerlegungsgesetz für K hinzuschreiben; die Bestimmung der voll zerlegten p war das einzige ernsthafte Problem. Das Resultat (übertragbar auf analog gebaute Körper) ist ein *mixtum compositum* aus Kongruenzbedingungen und einer diophantischen Bedingung; aber es schwer vorstellbar, daß es „besser" geht.

9. Wir nehmen das Resultat zum Anlaß, eine sehr klassische Fragestellung ein wenig zu verfolgen, die (neben andern) zur algebraischen Zahlentheorie hingeführt hat und auch heute noch als Leitfaden bis hin zur Klassenkörpertheorie und komplexen Multiplikation dienen kann [9]: gegeben ein natürliches n, welche Primzahlen p haben die Form $p = x^2 + ny^2$ mit ganzen x,y? Für den primordialen Fall $n = 1$ (primordial gleichzeitig für das Zerlegungsproblem überhaupt) gilt bekanntlich

(0) $\quad p \neq 2$ und $p = x^2 + y^2 \quad \Leftrightarrow \quad$ p zerfällt in $\mathbb{Z}[\sqrt{-1}] \quad \Leftrightarrow \quad p \equiv 1 \bmod 4$;

es besteht also eine Äquivalenz zwischen einer diophantischen, einer Zerlegungs- und einer Kongruenzbedingung, wobei die Zerlegungsbedingung als Vermittler erscheint, während das ursprüngliche Interesse den beiden anderen galt. Die Kette der Äquivalenzen bleibt bestehen für $p = x^2 + ny^2$, solange $\mathbb{Z}[\sqrt{-n}]$ erstens der Ganzheitsbereich von $K = \mathbb{Q}[\sqrt{-n}]$, also n quadratfrei und nicht $\equiv 3 \bmod 4$, und zweitens ein Hauptidealring ist, womit nur einige wenige n übrigbleiben (und natürlich die Kongruenzbedingung entsprechend dem Zerlegungsgesetz in quadratischen Körpern zu ändern ist). Ist die erste Bedingung erfüllt, aber nicht die zweite, so bleibt von der ersten Äquivalenz nur die Implikation „$\Rightarrow$" richtig, denn wenn p zerfällt, müssen die Primidealfaktoren keine Hauptideale mehr sein. Trotzdem läßt sich die diophantische Bedingung $p = x^2 + ny^2$ zu einer Zerlegungsbedingung in Äquivalenz setzen, indem man zum Hilbertschen Klassenkörper K^1 von K übergeht. Denn dieser Körper ist dadurch charakterisiert, daß genau die (primen) Hauptideale von K in K^1 voll zerfallen; und wenn p in K^1 voll zerfällt, dann müssen die Primteiler von p in K ebenfalls in K^1 voll zerfallen, also Hauptideale der Norm p sein, woraus sofort die Gleichung folgt. Für die Kongruenzbedingung allerdings gibt es keinen (vergleichbaren) Ersatz mehr, denn K^1 ist zwar noch galoissch, aber nicht mehr abelsch über $\mathbb{Q}$.

Das läßt sich sogar ausdehnen auf den Fall, in dem auch die erste Bedingung nicht mehr erfüllt ist. Schreibt man $n = f^2 d$ mit quadratfreiem d, wird die Gleichung $p = x^2 + ny^2$ explizit zu

$$p = (x + f\sqrt{-d}y)\,(x - f\sqrt{-d}y),$$

was notwendig die Primzerlegung von p im Körper $\mathbb{Q}(\sqrt{-d})$ darstellt und gleichzeitig zeigt, daß die Primfaktoren schon in der Ordnung $\mathbb{Z}[f\sqrt{-d}]$ vom „Führer" f liegen. Die Klassenkörpertheorie garantiert die Existenz einer abelschen Erweiterung L/K, in der *genau* diese primen Hauptideale von K voll zerfallen, den „Ringklassenkörper" zum Führer f, der für f = 1 der Hilbertsche Klassenkörper ist. Dieselbe Schlußweise wie oben zeigt also, daß genau die Primzahlen der Form $p = x^2 + ny^2$ in L voll zerfallen. Das Beispiel aus **8** subsumiert sich hier mit n = 27; der dortige Körper K ist ein Ringklassenkörper über $\mathbb{Q}(\zeta)$; der Führer ist 6 (und nicht 3), weil die Ordnung $\mathbb{Z}[3\sqrt{-3}]$ in $\mathbb{Z}[\zeta]$ den Führer 6 hat. Historisch gesehen löste der Ringklassenkörper ein klassisches diophantisches Problem; uns dient er nur als Beispiel für einen Typus von Zerlegungsgesetzen. So werden Mittel zu Zwecken, und der ursprüngliche Zweck erscheint vom „höheren" Standpunkt aus als eher untergeordneter Nebeneffekt. Erklärt das Zerlegungsgesetz die Gleichung oder umgekehrt?

10. Diophantische Kriterien für die Primzerlegung in Terminis der Norm sind immer vorhanden. Zunächst ein grobes: Sei K ein beliebiger Zahlkörper und N die Absolutnorm $K \to \mathbb{Q}$, die wir als homogene ganzzahlige Form vom Grad $n = [K:\mathbb{Q}]$ in n Variablen denken; gewonnen aus einer Ganzheitsbasis für K (die Form hängt natürlich ab von der Wahl dieser Basis, ihre Wertemenge aber nicht). Dann hat die Primzahl p einen Primteiler vom Grad 1 in K genau dann, wenn N (für ganzzahlige Argumente) einen Wert der Form pz, (p,z) = 1 annimmt. Zum Beweis benutzen wir die elementare Tatsache, daß der Betrag der Norm des ganzen Elements a gleich der Idealnorm des von a erzeugten Hauptideals ist. Ist nun N(a) = pz für ganzes a, muß a gemäß dem eben erwähnten Zusammenhang von Element- und Idealnormen einen Primteiler P von p vom Grade 1 haben. Sei umgekehrt dies der Fall und P ein solcher Primteiler. Wählt man dann das ganze Element a so, daß a in P, aber nicht in P^2 und auch in keinem der übrigen Primteiler von p liegt (was mit Hilfe des Chinesischen Restsatzes leicht möglich ist), dann hat N(a) die angegebene Form. Es ist klar, daß man $z = \pm 1$ genau dann erreichen kann, wenn P ein Hauptideal ist, also sicher, wenn K die Klassenzahl 1 hat. Dies verallgemeinert die erste Äquivalenz in (0). Ist K absolut galoissch, so hat p einen Primteiler vom Grad 1 genau dann, wenn p voll zerfällt [10].

Man kann die Betrachtung verfeinern und den „parasitären" Term z vermeiden, indem man die Idealklassen einzeln heranzieht; wiederum ein sehr klassischer Prozeß. Seien A und B ganze Ideale in zueinander inversen Klassen, also AB = (a) mit einem ganzen a, oder $B = a\,A^{-1}$. Läßt man hierin a alle Elemente von A durchlaufen, durchläuft die linke Seite alle ganzen Ideale in der Klasse von B, und geht man zu Normen über, erhält man alle Normen ganzer Ideale dieser Klasse in der Gestalt $\pm N(a)/N(A)$; berechnet mit einer $\mathbb{Z}$-Basis von A, ist dies ist eine Form mit ganzzahligen Koeffizienten. Genau dann hat die rationale Primzahl p einen Primteiler ersten Grades in K, wenn eine dieser Formen den Wert $\pm p$ annimmt. Im galoisschen Fall liefert die Wertverteilung dieser Formen sogar das volle Zerlegungsgesetz: der Restklassengrad von p in K ist der Exponent der kleinsten p-Potenz, die als Wert einer dieser Formen vorkommt.

11. Wir haben oben gesehen, wie sich in speziellen Fällen durch Heranziehen der Klassenkörpertheorie der Grad der Formen „drücken" läßt, genauer: die zerlegten

Primzahlen schon durch Normformen aus einem echten Teilkörper charakterisiert werden können. Das läßt sich verallgemeinern, wenigstens für den Fall f = 1 des Hilbertschen Klassenkörpers: ist K ein über $\mathbb{Q}$ galoisscher Körper und L sein Hilbertscher Klassenkörper so zerfällt die (in K unverzweigte) Primzahl p in L voll genau dann, wenn ±p Norm eines ganzen Elements aus K ist. Denn wenn dies der Fall ist, ist ±p das Produkt seiner Konjugierten in K, und diese erzeugen verschiedene Primideale, da p unverzweigt ist; diese wiederum zerfallen voll in L, damit auch p. Zerfällt umgekehrt p voll in L, so auch in K, und die Primfaktoren von p in K zerfallen voll in L, müssen also nach Definition des Hilbertschen Klassenkörpers Hauptideale sein, deren Normen = p sein müssen. Wenn wir das auf die Zerlegungsfrage für allgemeines L anwenden, werden wir also zu einer eigenartigen Fragestellung geführt: für welche Teilkörper K ist L der Hilbertsche Klassenkörper? Ist L absolut galoissch mit der Gruppe G, so ist L abelsch genau über den Fixkörpern der abelschen Untergruppen von G; das ist der triviale Teil der „Klassenkörpertheorie nach unten“[11]. Ist L Hilbertscher Klassenkörper zu verschiedenen Unterkörpern, ergibt sich eine Äquivalenz für die Darstellbarkeit von Primzahlen durch Normformen von verschiedenen Körpern.

Eine noch etwas weitergehende Verallgemeinerung bezieht sich auf die folgende Situation: sei L ein absolut galoisscher Zahlkörper mit der Gruppe G, A ein abelscher Normalteiler von G, K sein Fixkörper und H die der abelschen Erweiterung L/K in K zugeordnete Idealgruppe. Dann gilt: genau dann enthält H (fast) alle rationalen Primzahlen, wenn die Verlagerung $V(G \rightarrow A)$ die triviale Abbildung ist [12]. (Ist L der Hilbertsche Klassenkörper von K, ist das sicherlich der Fall, weil H dann *alle* Hauptideale enthält.) Sei dies erfüllt; dann läßt sich zeigen, daß H aus „verallgemeinerten Ringklassen“ zusammengesetzt ist und die Normen der Ideale dieser Klassen wie im letzten Abschnitt durch eine endliche Menge von ganzzahligen Formen gegeben werden, deren Grad jetzt $[K:\mathbb{Q}] = [G:A]$ ist. Da nun die Primzahl p in L genau dann zerlegt ist, wenn H ein Primideal der Norm p enthält, ergibt sich eine Charakterisierung der zerlegten p durch Formen dieses kleineren Grades [13]. In allen hier betrachteten nichtabelschen Beispielen bestand der Beitrag der abelschen Klassenkörpertheorie darin, eine diophantische Bedingung (= Normgleichung) für vollen Zerfall möglichst „klein“ zu halten.

12. Ähnliche Möglichkeiten, den relevanten Grad zu senken, gibt es für die immer vorhandene Kongruenzbedingung, die im PZG besteht, wenigstens wenn wir uns auf die Mengen S(L/K) beschränken. Es gilt nämlich: ist N der galoissche Abschluß von L über K, so ist S(L/K) = S(N/K) (das folgt daraus, daß N das Kompositum der Konjugierten von K ist und eine Primstelle, die in zwei Erweiterungen zerlegt ist, auch in deren Kompositum zerlegt ist). Demnach kann man sich für die Bestimmung von S(N/K) auf möglichst kleine Teilkörper beschränken, von denen N der galoissche Abschluß ist; ihnen entsprechen gruppentheoretisch möglichst große Untergruppen, deren normaler Abschluß die volle Gruppe ist. Ist diese z.B. die symmetrische Gruppe S_n (und das ist der „Normalfall“, „Gleichung ohen Affekt“, wie man früher sagte; alle Zerlegungstypen kommen vor), so kommt man mit einem Grad n statt n! aus. Ist die Gruppe einfach, kann man mit beliebigen maximalen Untergruppen arbeiten. Für die Anwendung des PZG bleibt die Aufgabe, aus einem erzeugenden Polynom für N ein solches für einen Teilkörper abzuleiten; hierfür hat die klassische Invariantentheorie

Methoden entwickelt, die freilich bei theoretischer Durchsichtigkeit algorithmisch schnell sehr aufwendig werden. Es ist trivial, aber doch bemerkenswert, daß im abelschen Fall diese Gradreduktion beim PZG nicht möglich ist; dafür bietet die Klassenkörpertheorie eine Kongruenzbedingung, also, wenn man so will, eine Reduktion auf eine Gleichung vom Grad 1 in einem Restklassenring ganzer Zahlen.

Ein erstes Beispiel hierfür bietet schon der Körper K aus **8**, der die galoissche Hülle von $\mathbb{Q}(a)$ ist; man beachte, daß die notwendige und hinreichende Bedingung für den Zerfall von p in $\mathbb{Q}(a)$, nämlich $p = x^2 + 27y^2$, schon $p \equiv 1 \bmod 3$ und damit den Zerfall auch im Einheitswurzelkörper impliziert. Hier ist ein anspruchsvolleres Beispiel: sei E eine über dem Zahlkörper K definierte elliptische Kurve und K(E(4)) die Erweiterung, die durch Adjunktion der Koordinaten der 4-Torsion von E entsteht; diese ist stets galoissch, und nach einem Satz von Serre ist es keine sehr einschneidende Voraussetzung, anzunehmen, daß Gal(K(E(4))/K) die volle Automorphismengruppe der 4-Torsion ist, nämlich GL(2,4). Diese Gruppe enthält einen zur Kleinschen Vierergruppe isomorphen Normalteiler, der eine zur symmetrischen Gruppe S_4 isomorphe Faktorgruppe liefert; ihr entspricht eine galoissche Teilerweiterung L/K , die den „Hauptteil“ für die Primzerlegung ausmacht. Nach dem oben Gesagten kann man hoffen, ein Polynom vierten Grades über K zu finden, dessen Wurzelkörper L als galoisschen Abschluß hat; und in der Tat findet sich sogar ein solches, in dessen Koeffizienten die numerischen Invarianten von E auf sehr einfache Weise eingehen, was nach dem Formelwust, durch den man sich bei der Herleitung hindurchzukämpfen hat, erstaunen muß [14].

13. Wir haben hier auch die Frage zu streifen, in welchem Grade Zahlkörper durch ihre Zerlegungsgesetze bestimmt sind. Schon erwähnt wurde der Satz von Bauer, demzufolge galoissche Erweiterungen L/K schon durch die Mengen S(L/K) determiniert sind; klar ist weiter, daß algebraisch konjugierte Körper dasselbe Zerlegungsgesetz haben. Die ersten Beispiele für (notwendig nicht galoissche) nicht konjugierte Körper mit demselben Zerlegungsgesetz wurden in den 20er Jahren des letzten Jahrhunderts entdeckt; zu den kleinsten Beispielen (aus neuerer Zeit stammend) gehören die beiden Erweiterungen $\mathbb{Q}(a)$, $a^8 = 3$, und $\mathbb{Q}(b)$, $b^8 = 48$ des rationalen Grundkörpers. Dieses Phänomen der „arithmetischen Äquivalenz“ läßt sich gruppentheoretisch durchsichtig machen. Zugrunde liegt der folgende allgemeine Sachverhalt: Sei L/K eine beliebige Erweiterung von Zahlkörpern, N/L ein über K galoisscher Körper, G = Gal(N/K) und H die Fixgruppe von L; G operiert als Permationsgruppe auf der Menge der Nebenklassen G/H. Ist nun p ein Primideal von K, P ein Primteiler von p in N und s ein zugehöriges Frobeniuselement, so entspricht der Zerlegungstyp von p in L dem Zykeltyp von s bei seiner Operation auf G/H (Genaueres brauchen wir jetzt nicht) [15]. Daraus folgt: sind die Untergruppen H und H´ nicht konjugiert, liefern aber isomorphe Permutationsdarstellungen von G, so sind ihre Fixkörper arithmetisch äquivalent, aber nicht konjugiert, und alle Fälle von arithmetischer Äquivalenz entstehen auf diese Weise. Insbesondere sind immer nur endlich viele L zueinander arithmetisch äquivalent. Es versteht sich, daß arithmetisch äquivalente Körper viele weitere Invarianten gemeinsam haben, zum Beispiel dieselbe Zetafunktion (das ist klar), auch dieselbe Diskriminante, aber nicht notwendig dieselbe Klassenzahl; worauf wir aber hier nicht weiter eingehen müssen [16].

II Was verspricht das Programm von Langlands?

14. Solange man mit auflösbaren Galoisgruppen zu tun hat, kann man von der Klassenkörpertheorie wenigstens qualitative Beiträge erhoffen, wenngleich die Übertragung der Information von den abelschen Stufen auf die Gesamterweiterung schon in den einfachsten (metabelschen) Fällen beträchtliche Schwierigkeiten macht [17]. Hat aber die Galoisgruppe nichtabelsche einfache Kompositionsfaktoren, sind qualitativ neue (und wesentlich komplexere) Phänomene zu erwarten. Das ist der Fall für G = GL(2,q), q prim, in deren Kompositionsreihe als Faktor die Gruppe PSL(2,q) erscheint, die für q > 3 einfach ist; so für q = 5 die alternierende Gruppe A_5 der Ordnung 60, die kleinste nichtabelsche einfache Gruppe. Dieser Gruppentyp spielt die Hauptrolle in einem berühmten Beispiel von Shimura [18] , das man vielleicht, wenigstens vom arithmetischen Gesichtspunkt aus, als „Morgendämmerung" des Langlandsprogramms ansehen kann, und das wir zunächst besprechen wollen [19] .

Es sei $E = X_0(11)$ die Modulkurve der Stufe 11; sie gehört zu den wenigen Modulkurven vom Geschlecht Eins und kann über $\mathbb{Q}$ durch die Gleichung $y^2 + y = x^3 - x^2 - 10x - 20$ beschrieben werden. Für eine Primzahl q bezeichne $\mathbb{Q}(q)$ den Körper, der durch Adjunktion der Koordinaten der q-Torsion E(q) von E entsteht. Für $q > 5$ besteht ein Isomorphismus $R: Gal(\mathbb{Q}(q)/\mathbb{Q}) \cong Aut(E(q)) \cong GL(2,q)$ [20] ; die Erweiterung ist unverzweigt für Primzahlen $p \neq 11,q$. Für solche p hat E gute Reduktion zu einer elliptischen Kurve E_p über $\mathbb{Z}/p\mathbb{Z}$, und aus allgemeinen Sätzen folgt $E(q^n) \cong (E_p)(q^n)$ für alle natürlichen n. Bei dem Isomorphismus R geht ein Frobeniuselement F(p) für p (bis auf Konjugation) über in den Frobeniusautomorphismus π_p auf $E_p(q)$,

$$\pi_p (x, y) = (x^p, y^p)$$

für Punkte (x,y) auf dem affinen Teil von E_p ; π_p ist ein Automorphismus des zweidimensionalen $\mathbb{Z}/q\mathbb{Z}$ – Vektorraums $E_p(q)$. Daher stimmen ihre charakteristischen Polynome überein,

$$\det (X - R(F(p))) = \text{char pol } (\pi_p , E_p(q); X) , \ X \text{ eine Variable;}$$

dies ist eine Gleichung über $\mathbb{Z}/q\mathbb{Z}$. Der Frobenius π_p operiert nun auch auf dem Tate-Modul

$$\lim \text{proj } (E_p)(q^n) =: T_q(E_p) \cong T_q(E) \cong \mathbb{Z}_q \times \mathbb{Z}_q ,$$

und nach einem klassischen Resultat von Weil gilt

$$\text{char pol } (\pi_p , T_q(E_p)) = \det (X - \pi_p) = X^2 - a_pX + p ,$$

wobei

$$a_p = p + 1 - \text{card } E_p (\mathbb{Z}/p\mathbb{Z});$$

diese Gleichung, aufgelöst nach card E_p ($\mathbb{Z}/p\mathbb{Z}$), lesen wir heute als Fixpunktformel à la Lefschetz in der q-adischen Kohomologie; der Summand 1 kommt von der trivialen Operation auf H^0, der Summand p von H^2 (die Operation ist Multiplikation mit dem Abbildungsgrad). Daraus folgt

(1) $$\det (X - R(F(p))) \equiv X^2 - a_p X + p \mod q .$$

Soviel gilt für allgemeinere E, aber nun kommt die entscheidende Wendung: bei Modulkurven $X_o(n)$ identifizieren sich die Spitzenformen vom Gewicht 2 für die Gruppe $\Gamma_0(n)$ mit den holomorphen Differentialformen auf der Kurve, die einen Vektorraum der Dimension g = Geschlecht von $X_o(n)$ bilden; in diesem Falle ist also der Raum der Spitzenformen eindimensional mit dem normierten Erzeuger

(2) $$\Delta(z) = \Sigma_{n \geq 1} c_n q^n = q \prod_{n \geq 1} (1 - q^n)^2 (1 - q^{11n})^2 ;$$

hier ist $q = \exp(2\pi i z)$, im $z > 0$. Notwendig ist $\Delta(z)$ eine Eigenform aller Heckeoperatoren, und $T_p(\Delta) = c_p \Delta$. Die Theorie von Eichler-Shimura sagt uns, daß $a_p = c_p$, und damit

(3) $$\det (X - R(F(p))) \equiv X^2 - c_p X + p \mod q .$$

Das ist nur beinahe ein Zerlegungsgesetz, denn die Ordnung von F(p) ist durch die Eigenwerte von R(F(p)) nicht gänzlich bestimmt: sind diese verschieden (also das Polynom rechts separabel), ist die Ordnung von F(p) das kgV von deren Ordnungen, im andern Fall aber die Ordnung des Eigenwerts oder das q-fache; jedenfalls ist $c_p \equiv 2 \mod q$ eine notwendige Bedingung für $p \in S(\mathbb{Q}(q)/\mathbb{Q})$. Scharfe (wenn auch bescheidene) Aussagen erhält man für Teilkörper: ist ein Eigenwert = 1, also $c_p \equiv 1 + p \mod q$, liegt R(F(p)) (bis auf Konjugation) in der Gruppe oberer Dreiecksmatrizen mit oberem Diagonaleintrag = 1; diese Gruppe hat einen Fixkörper L vom Grad $q^2 - 1$ über $\mathbb{Q}$. Das Argument läßt sich umkehren, und mittels des allgemeinen Mechanismus von Galoistheorie und Primzerlegung erhält man eine notwendige und hinreichende Bedingung dafür, daß p im Teilkörper L einen Primteiler vom Grad 1 hat. Bemerkt zu werden verdient (worauf Shimura ausdrücklich hinweist), daß der Koeffizient c_p für die Zerlegung von p in verschiedenen Körpern „zuständig“ ist; dafür gibt es im Klassenkörperfall kein Analogon [21].

Warum kann (3) trotz der oben bemerkten Einschränkung als Reziprozitätsgesetz angesehen werden? Die beiden Gleichungen (1) und (3) stehen in einem Verhältnis, das demjenigen zwischen dem PZG und dem Klassenkörpergesetz in gewisser Weise analog ist: die Größen a_p entstammen der mod p reduzierten Kurvengleichung, ähnlich wie beim PZG die Faktoren der Polynomzerlegung mod p; und wie diese geben jene keinen Hinweis auf eine Gesetzmäßigkeit, welche das jeweilige Verhalten modulo verschiedener p miteinander verbindet, insbesondere kein a-priori-Kriterium dafür, wann dieses gleich ausfällt. Erst das Klassenkörpergesetz spricht eine solche aus, und dies kann kann man auch von den c_p sagen, denn sie sind Koeffizienten (und Hecke-Eigenwerte) einer Modulform, und das Gesetz, das sie „zusammenhält“, ist implizit in

der Formel (2) enthalten. Wollen wir freilich dieses a-priori-Kriterium „explizit“ sehen, finden wir uns in keiner besseren Lage als beim PZG, denn es scheint kein allgemeines Kriterium dafür zu geben, wann zwei Hecke-Eigenwerte gleich sind, nicht einmal für diesen *sehr* klassischen Fall [22]. Die allgemeine Theorie sagt uns, daß die Koeffizienten c_n multiplikativ sind und für Potenzen einer festen Primzahl der bekannten Rekursion genügen; über das „innere Band“ zwischen den einzelnen c_p erfahren wir dadurch nichts, außer daß es durch eine Modulform kodifiziert wird. Wir kennen nicht das Gesetz, nur ein Gesetz für das Gesetz. Es ist durchaus möglich, daß die implizite Definition der c_p durch die Formel (2) schon die maximale uns erreichbare Explikation ist; es gibt nie eine Garantie dafür, daß für ein Objekt oder einen Sachverhalt über die Definition hinaus eine Beschreibung gegeben werden kann, die uns „mehr sehen“ läßt.

Es ist aufschlußreich, die Erweiterung $\mathbb{Q}(q)$ parallel zum Körper der q-ten Einheitswurzeln zu betrachten. Beide entstehen, indem die Koordinaten der q-Torsion einer algebraischen Gruppe zum rationalen Grundkörper adjungiert werden; im elliptischen Fall der abelschen Varietät E, im zyklotomischen Fall der multiplikativen Gruppe G_m; da diese in G_a enthalten ist, sind die Elemente ihre eigenen Koordinaten. Da beide kommutativ sind, ist die q-Torsion eine Untergruppe (und zwar funktoriell, also besser ein Unterschema). In beiden Fällen erweist sich die galoissche Gruppe G, eingeführt zunächst als Permutationsgruppe einer Menge von Nullstellen, als *volle* Automorphismengruppe der q-Torsion,

$$G = \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^{\times} = GL(1,q) \quad \text{bzw.} \quad G = \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}) \cong GL(2,q).$$

In beiden Fällen bleibt die q-Torsion bei Reduktion modulo fast aller p unverändert,

$$G_m(q) \cong G_{m,p}(q) \quad \text{bzw.} \quad E(q) \cong E_p(q).$$

Der Frobeniusautomorphismus im Restkörper ist natürlich immer derselbe, $x \to x^p$; aber in Charakteristik Null ist diese Abbildung, koordinatenweise angewandt, nur für zerfallende Tori ein Morphismus algebraischer Gruppen, der auf der q-Torsion und damit auf dem von ihr über $\mathbb{Q}$ erzeugten Körper einen Automorphismus induziert. Daher kann er im zyklotomischen Fall einfach „gehoben“ werden, und das ist der „tiefere“ Grund dafür, daß hier die Reziprozitätsabbildung so mühelos angebbar ist. Nun sind wir, solange es um das Zerlegungsproblem geht, nur an der Ordnung des Frobenius interessiert, und hier haben wir im elliptischen Fall, da die galoissche Gruppe eine *lineare* Gruppe über einem Körper ist, das charakteristische Polynom als eine etwas schwächere Invariante, wie oben beschrieben. Es liegt nahe, zu fragen, was diese Prozedur für den zyklotomischen Fall liefert: der Mechanismus der Lefschetzformel ist gar nicht verfügbar, da G_m nicht projektiv ist; wohl aber gibt es den Tatemodul der Einheitswurzeln von q-Potenzordnung, isomorph zu $\mathbb{Z}_q$, auf dem der p-Frobenius durch Multiplikation mit p operiert, mit dem charakteristischen Polynom $X - p$, was uns natürlich nichts Neues sagt [23].

15. Wir wenden uns nun dem zu, was uns das allgemeine Langlandsprogramm für unsere Frage erwarten läßt. Sei K ein Zahlkörper. Die Klassenkörpertheorie stiftet eine Bijektion

{verallgemeinerte Idealklassengruppen H von K} $\leftrightarrow$ {abelsche Erweiterungen von K}

derart daß, wenn H der Erweiterung L/K entspricht, die Artinabbildung einen Isomorphismus

$$H \cong \mathrm{Gal}(L/K), \quad \mathrm{cl}(p) \rightarrow (L/K, p)$$

induziert; der Isomorphismus ist kompatibel mit verschiedenen natürlichen Operationen, die in diesem Kontext möglich sind. Hier wird also eine Existenzaussage für abelsche Erweiterungen mit dem in diesen jeweils geltenden Zerlegungsgesetz verbunden, denn für Primteiler P von p in L ist $f(P/p) = \mathrm{ord}\,(L/K, p)$ nach Definition des Frobenius. Die erste Frage bei der Verallgemeinerung auf beliebige galoissche Erweiterungen ist, was auf die linke Seite tritt. Wohl jeder denkt spontan: nichtkommutative über K definierte Strukturen findet man in Matrizen. Die Idee ist richtig, aber nicht in naiver Weise realisierbar. Zuvor muß das Ganze umformuliert werden: die Existenzaussage für Körper in eine solche für Darstellungen der absoluten Galoisgruppe von K, das Reziprozitätsgesetz in eine Gleichheit von Eulerfaktoren in gewissen L-Reihen. Wir beschränken uns (nur der Einfachheit halber) auf $K = \mathbb{Q}$.

Die Isomorphie $H \cong \mathrm{Gal}(L/K)$ ist gleichbedeutend mit einer Isomorphie der Charaktergruppen. Für $K = \mathbb{Q}$ ist H eine Faktorgruppe einer primen Restklassengruppe $(\mathbb{Z} \bmod m)^\times$, und ein Charakter χ dieser Gruppe kann zu einem Dirichletschen Charakter auf $\mathbb{Z}$ gehoben werden, mit $\chi(n) = 0$ für $(n,m) > 1$. Wir interpretieren jetzt χ anders, nämlich als Charakter der *Idelklassengruppe* von $\mathbb{Q}$ und führen dazu den Adelring $\mathbf{A}(\mathbb{Q})$ und seine Einheitengruppe, die *Idelgruppe* $\mathbf{I}(\mathbb{Q})$ ein,

$$\mathbf{A}(\mathbb{Q}) = \mathbb{R} \times \Pi_p{}' \mathbb{Q}_p \ , \quad \mathbf{I}(\mathbb{Q}) = \mathbb{R}^\times \times \Pi_p{}' \mathbb{Q}_p{}^\times ,$$

wobei der Strich am Produktzeichen bedeutet, daß die p-Komponente für fast alle p ganz ist. In $\mathbf{I}(\mathbb{Q})$ ist $\mathbb{Q}^\times$ diagonal eingebettet, und mit der Bezeichnung $\hat{\mathbb{Z}}^\times = \Pi_p \mathbb{Z}_p{}^\times$ erhalten wir, wie man leicht nachprüft, die direkte Produktzerlegung

$$\mathbf{I}(\mathbb{Q}) = \mathbb{Q}^\times \mathbb{R}_+{}^\times \hat{\mathbb{Z}}^\times .$$

Mittels des Chinesischen Restsatzes zerlegen wir χ in ein Produkt $\chi = \Pi_p \chi_p$ von Charakteren modulo der in m aufgehenden Primzahlpotenzen und setzen $\chi_p = 1$, wenn p kein Teiler von n ist; das ist ein Charakter von $\hat{\mathbb{Z}}^\times$. Aus diesem gewinnen wir einen Charakter für Idele $x = q\, r\, u \in \mathbf{I}(\mathbb{Q}) = \mathbb{Q}^\times \mathbb{R}_+{}^\times \hat{\mathbb{Z}}^\times$ durch die Definition

$$\pi(x) = \chi(u^{-1}).$$

Damit erhalten wir einen Charakter endlicher Ordnung von $\mathbf{I}(\mathbb{Q}) = GL(1, \mathbf{A}(\mathbb{Q})) = G_m(\mathbf{A}(\mathbb{Q}))$, der auf $\mathbb{Q}^\times = GL(1, \mathbb{Q})$ (und der Zusammenhangskomponente $\mathbb{R}_+^\times$) trivial ist, und man zeigt leicht, daß alle solchen Charaktere auf diese Weise erhalten werden [24]. Um die „Wirkungsweise“ dieser Konstruktion zu sehen, betrachten wir für eine Primzahl p die Einbettung

$$i_p: \ \mathbb{Q}_p^\times \ \rightarrow \ \mathbf{I}(\mathbb{Q}) , \ \ y \ \rightarrow \ (1,...,1,y,1...), \quad y \text{ an der p-Stelle,}$$

und rechnen (für (p,n) = 1)

$$\pi\,(i_p(p)) \ = \ \pi\,(\ p(1/p,...,1/p,1,1/p,...)) \ = \quad \Pi_{\,q \neq p}\ \chi_q(p) \ = \ \chi(p).$$

Ein Charakter wie π ist aber nichts anderes als eine (spezielle) automorphe Darstellung von GL(1) über $\mathbb{Q}$ (und automorphe Darstellungen werden in der einschlägigen Literatur stets mit dem Buchstaben π bezeichnet). Durch $\pi_p := \pi\, i_p$ erhalten wir einen Charakter von $\mathbb{Q}_p^\times$, der für (p,n) = 1 *unverzweigt* ist, d.h. trivial auf $\mathbb{Z}_p^\times$, und können $\pi = \otimes \pi_p$ schreiben. Fassen wir weiter einen Charakter von $Gal(L/\mathbb{Q})$ als einen Charakter der absoluten Galoisgruppe $G(\mathbb{Q})$ auf, gelangen wir zu einer Bijektion [25]

$$\{\text{irreduzible abelsche Charaktere } \chi \text{ von } G(\mathbb{Q})\} \quad \leftrightarrow$$
$$\{\text{spezielle automorphe Darstellungen } \pi \text{ von GL(1) über } \mathbb{Q}\}$$

mit der folgenden Eigenschaft: ist K der Fixkörper des Kerns von χ (eine *zyklische* Erweiterung von $\mathbb{Q}$), so ist für unverzweigte p

$$\chi\,((K/\mathbb{Q}, p)) \ = \ \pi_p(p). \tag{4}$$

Dies ist immer noch die Klassenkörpertheorie *in nuce*, denn ein Existenzsatz für zyklische Erweiterungen schließt einen solchen für abelsche ein, und weil χ eine *treue* Darstellung von $Gal(K/\mathbb{Q})$ ist, erhalten wir aus (4) die Ordnung von $(K/\mathbb{Q}, p)$ und damit das Zerlegungsgesetz. Man kann (4) ersetzen durch eine Gleichheit zugeordneter (partieller) L-Funktionen

$$L_u(s, \chi) \ = \ \Pi_{\,p \text{ unverzweigt}}\, L_p(s, \chi\,) \quad \text{bzw.} \quad L_u(s, \pi) \ = \ \Pi_{\,p \text{ unverzweigt}}\, L_p(s, \pi)$$

mit den Eulerfaktoren

$$L_p(s, \chi\,) = \ (1 - \chi((K/\mathbb{Q}, p))p^{-s})^{-1} \quad \text{bzw.} \quad L_p(s, \pi\,) = (1 - \ \pi_p(p)p^{-s})^{-1} \quad (p \text{ unverzweigt}),$$

weil die Eulerfaktoren aus den Dirichletschen Reihen zurückgewonnen werden können [26]. Für den gegenwärtigen Zweck wäre das nicht erforderlich, aber weil die L-Funktionen so wichtig sind, wollen wir uns im Folgenden so ausdrücken. $L_u(s, \chi)$ ist eine Artinsche L-Reihe (s.u.), $L_u(s, \pi\,)$ eine Dirichletsche (oder Heckesche) L-Reihe.

16. Jetzt haben wir eine Situation erreicht, die wir – wenigstens vermutungsweise – verallgemeinern können. Zunächst die arithmetische (oder „motivische“) Seite: sei L/K eine galoissche Erweiterung von Zahlkörpern mit der Gruppe G und

$$r: \quad G \quad \to \quad GL(d, \mathbb{C})$$

eine d-dimensionale Darstellung von G mit dem Charakter χ . Für ein unverzweigtes Primideal p von K und einen Primteiler P von p in L ist das Polynom $\det(1 - r((L/K, P))X)$ unabhängig von der Wahl von P (und auch von der Wahl von r unter Konjugierten); wir setzen

$$L_p(s, \chi, L/K) = \quad \det(1 - r((L/K, P))N(p)^{-s})^{-1}$$

mit der Absolutnorm N(p) von p und bilden die *Artinsche L-Funktion*

$$L(s, \chi, L/K) \quad = \quad \Pi_p \, L_p(s, \chi, L/K)$$

(für die verzweigten p ist eine Modifikation erforderlich, die wir uns hier schenken können). Man zeigt mit Standardargumenten, daß $L(s, \chi, L/K)$ für $\mathrm{Re}\ s > 1$ gleichmäßig konvergiert und dort eine holomorphe Funktion darstellt (man braucht nur zu beachten, daß die Eigenwerte von $r((L/K,P))$ Einheitswurzeln sind). Diese Funktionen haben eine Reihe erfreulicher Eigenschaften:

(i) Ist r die triviale Darstellung mit d = 1, so ist $L(s, \chi, L/K) = \zeta_K(s)$ die Dedekindsche Zetafunktion von K.

(ii) $\quad L(s, \chi_1 + \chi_2, L/K) \quad = \quad L(s, \chi_1, L/K)\, L(s, \chi_2, L/K)$.

(iii) Ist $K \subset E \subset L$ ein Zwischenkörper, galoissch über K mit der Gruppe H und χ ein Charakter von H, so können wir χ zu einem Charakter $\inf \chi$ von G hochheben, und es gilt

$$L(s, \chi, E/K) = L(s, \inf \chi, L/K).$$

Diese Eigenschaften folgen glatt aus den Definitionen; das gilt nicht für die folgende, deren Beweis subtilere Arithmetik und Gruppentheorie verlangt:

(iv) Ist E nicht mehr notwendig galoissch über K, H die Fixgruppe von E und χ ein Charakter von H, so können wir den induzierten Charakter $\mathrm{ind}\ \chi$ von G bilden, und es gilt

$$L(s, \chi, L/E) = L(s, \mathrm{ind}\, \chi, L/K).$$

Das Eulerprodukt links erstreckt sich über die Primideale von E, das rechte über die von K. „Dazwischen“ steht das Zerlegungsgesetz für die Erweiterung E/K, über das wir allgemein nichts wissen; aber dieser Mangel an Information wird genau kompensiert

durch die Vergröberung, die im Übergang von χ zu ind χ besteht. Es ist diese Invarianz unter der Induktion, die den Artinschen L-Funktionen eigentlich ihr Interesse verleiht.

Ist χ eindimensional, so ist nach der Klassenkörpertheorie, wie oben für $K = \mathbb{Q}$ expliziert, $L(s, \chi, L/K)$ eine Heckesche (oder verallgemeinerte Dirichletsche) L-Reihe, und als solche, wenn χ nichtrivial ist, zu einer auf der ganzen komplexen Ebene holomorphen Funktion fortsetzbar, die einer Funktionalgleichung vom Typ $s \leftrightarrow (1 - s)$, $\chi \leftrightarrow \chi^*$ genügt. Artin hat vermutet, daß dasselbe für seine $L(s, \chi, L/K)$ gilt, wenn χ nicht den Einscharakter enthält. Das folgt aus (iv) und dem eben Gesagten, wenn χ *monomial* ist, d.h. induziert von einem eindimensionalen Charakter einer Untergruppe, was z.B. für alle irreduziblen Darstellungen von nilpotenten Gruppen der Fall ist [27]. Nach einem Satz von Brauer ist jedes χ ganzzahlige Linearkombination von monomialen Charakteren (und im Falle eines irreduziblen χ können natürlich nicht alle Koeffizienten positiv sein). Daraus folgt, daß jedes $L(s, \chi, L/K)$ ein *Quotient* von (Produkten von) abelschen L-Reihen ist; das beweist die *meromorphe* Fortsetzbarkeit sowie die Funktionalgleichung, aber noch nicht die Holomorphievermutung.

Jetzt wenden wir uns der automorphen Seite der vermuteten Verallgemeinerung zu: dort stehen natürlich automorphe Darstellungen π von GL(d) über $\mathbb{Q}$. Diese haben die Form $\pi = \otimes \pi_v$, wo v alle Primstellen von $\mathbb{Q}$ durchläuft und das Tensorprodukt einer der Definition der Adele korrespondierenden Restriktion unterworfen ist; dabei sind die π_v Darstellungen von $GL(d, \mathbb{Q}_v)$ und für fast alle $v = p$ *unverzweigt*. Wir brauchen das hier nicht zu definieren, sondern können uns mit der Feststellung begnügen, daß diese Darstellungen durch einen Vektor $(t_{1,p},....,t_{d,p})$ komplexer Zahlen, die *Satake-Parameter* von π_p, determiniert werden; für $d = 1$ ist $t_{1,p} = \chi(p)$ in der Notation von oben. Mit ihnen definiert man die Eulerfaktoren

$$L_p(s, \pi) = (1 - t_{1,p}\, p^{-s})^{-1}...(1 - t_{d,p}\, p^{-s})^{-1}$$

und erhält als deren Produkt den „unverzweigten Teil“ der L-Funktion. Jacquet, Langlands und andere haben gezeigt, wie man die vollständige L-Funktion $L(s, \pi)$ zu definieren hat, daß diese (wenn π nicht trivial ist) zu einer auf ganz $\mathbb{C}$ holomorphen Funktion fortsetzbar ist und einer Funktionalgleichung vom Typ $s \leftrightarrow 1 - s$, $\pi \leftrightarrow \pi^t$ (= kontragrediente Darstellung) genügt; man hat also eine glatte Verallgemeinerung des Falls $d = 1$, in dem die automorphen Darstellungen nichts anderes sind als die Heckecharaktere und ihre L-Reihen die Heckeschen.

17. Die Verallgemeinerung unserer Klassenkörpertheorie *in nuce* (für den Grundkörper $\mathbb{Q}$) bestünde nun in einer Bijektion

{irreduzible Charaktere von $G(\mathbb{Q})$ vom Grad d} $\leftrightarrow$
{gewisse automorphe Darstellungen von GL(d) über $\mathbb{Q}$};

dies für alle natürlichen d und derart, daß, wenn $\chi \leftrightarrow \pi$, die zugehörigen L-Reihen gleich sind,

$$L(s, \chi) = L(s, \pi);$$

das ist in der Tat die allgemeine Erwartung, die sich aus der Langlandskorrespondenz ergibt. Daraus würde, nach dem eben Gesagten, sofort die Artinsche Vermutung folgen[28]. Wir wollen nun genauer zusehen, in welchem Sinne damit von einer allgemeinen Klassenkörpertheorie gesprochen werden könnte.

Sei $L(s, \chi)$ gegeben; nach Eigenschaft (iii) können wir annehmen, daß χ einer *treuen* irreduziblen Darstellung r von $Gal(K/\mathbb{Q})$ entspricht, K der Fixkörper von Kern χ . Mit der L-Reihe sind die Eulerfaktoren gegeben, und aus deren Definition liest man ab, daß mit ihnen auch die Eigenwerte von $r((K/\mathbb{Q}, P))$, p unverzweigt in $K/\mathbb{Q}$ und P ein Primteiler in K, gegeben sind; weil r treu ist, damit auch $f(P/p) = ord(K/\mathbb{Q}, P)$ und damit das Zerlegungsgesetz für $K/\mathbb{Q}$. Insbesondere sind die voll zerfallenden p gegeben; und damit ist, nach dem Satz von Bauer, der Körper K selbst eindeutig bestimmt, und nach demselben Satz ist anhand der L-Funktionen auch entscheidbar, ob die verschiedenen L-Reihen zugeordneten Körper in einer Inklusionsbeziehung stehen. Mit anderen Worten: die Kenntnis aller L-Reihen $L(s, \chi)$ für irreduzible Charaktere χ von $G(\mathbb{Q})$ impliziert die Kenntnis aller derjenigen galoisschen Erweiterungen von $\mathbb{Q}$, deren Galoisgruppe eine treue irreduzible Darstellung besitzt [29], sowie der Inklusionsbeziehungen unter ihnen; schließlich für $L(s, \chi) = L(s, \chi, K/\mathbb{Q})$ die Kenntnis des Zerlegungsgesetzes für $K/\mathbb{Q}$.

Aus diesen speziellen absolut galoisschen Körpern lassen sich alle andern zusammensetzen, ähnlich wie die abelschen Körper aus den zyklischen. Zu jeder Gruppe $Gal(K/\mathbb{Q})$ lassen sich nämlich endlich viele irreduzible Darstellungen finden, deren Summe treu ist; dann ist K das Kompositum der Fixkörper K_i der Kerne dieser Darstellungen; die K_i sind speziell, und $S(K/\mathbb{Q})$ ist der Durchschnitt der $S(K_i/\mathbb{Q})$; allgemeiner ist die Ordnung eines Frobiuselements $(K/\mathbb{Q}, P)$, P ein Teiler der Primzahl p, das kgV der Ordnungen entsprechender Frobeniuselemente in den K_i (das liest man ab aus den Eulerfaktoren der L-Reihen, oder aus den allgemeinen Eigenschaften von Frobeniuselementen). Umgekehrt bestimmen je endlich viele spezielle K_i ein K wie oben, nämlich ihr Kompositum. Die Kenntnis aller $L(s, \chi, K/\mathbb{Q})$ impliziert also die Kenntnis des ganzen Verbandes aller (endlichen) galoisschen Erweiterungen von $\mathbb{Q}$ und für jede einzelne ihr Zerlegungsgesetz [30]. Was könnte man mehr wünschen?

18. Nun verspricht das Langlandsprogramm keine „Kenntnis“, sondern eine Korrespondenz. Um wenigstens eine Ahnung von dem zu bekommen, was allgemein zu erwarten ist, betrachten wir den Fall d = 2, in dem schon substantielle Resultate vorliegen; das liegt daran, daß sich die automorphen Darstellungen von GL(2) über $\mathbb{Q}$ mittels Modulformen beschreiben lassen, klassische (holomorphe) oder weniger klassische (Maassche Wellenformen), für welche eine ziemlich entwickelte Theorie dem Langlandsprogramm vorausging. Der genaue Übergang von Modulformen zu Darstellungen ist etwas aufwendig, erscheint sogar auf den ersten Blick als artifiziell; uns genügt hier, daß – in dem uns interessierenden Fall – die L-Reihen der Darstellungen mit den L-Reihen der ihnen entsprechenden Modulformen (bis auf einen

„Gammafaktor“ ihre Mellintransformierten) übereinstimmen [31] . Sei nun χ der Charakter einer irreduziblen Darstellung $r : Gal(K/\mathbb{Q}) \rightarrow GL(2,\mathbb{C})$ und die Artinsche L-Reihe $L(s, \chi)$ *modular*, d.h. die L-Reihe L(s, f) einer (holomorphen) Modulform; notwendig hat dann f das Gewicht 1 und ist Eigenform aller Heckeoperatoren T_p für unverzweigte p. Für solche p besteht dann Gleichheit der Eulerfaktoren, also

$$(1 - a\,p^{-s})(1 - b\,p^{-s}) = 1 - c_p\,p^{-s} + \varepsilon(p)\,p^{-2s} \quad ,$$

wo a und b die Eigenwerte von $r((K/\mathbb{Q}, P))$ sind (P ein Teiler von p), c_p der Hecke-Eigenwert und ε der „Nebentypus“ von f [32]. Daraus folgt sofort, daß $r((K/\mathbb{Q}, P)) = 1$ gleichbedeutend ist mit $c_p = 2$; man erhält damit eine *notwendige* Bedingung für $p \in S(K/\mathbb{Q})$ (die auch hinreicht, wenn r noch injektiv ist, was allerdings nur für eine Handvoll Gruppen möglich ist, s.u.), allgemeiner eine notwendige Bedingung dafür, daß verschiedene p und q dasselbe Zerlegungsverhalten haben, denn die Ordnung von $r((K/\mathbb{Q}, P))$ ist das kgV der Nullstellen des Polynoms $1 - c_p X + \varepsilon(p) X^2$ [33]. Für diese letztere Frage gibt die abelsche Klassenkörpertheorie eine hinreichende Bedingung, nämlich daß p und q in dieselbe (verallgemeinerte) Idealklasse fallen.

Vergleichen wir das mit Shimuras Beispiel aus **14** : dort figurierte die Galoisgruppe als ihre eigene Darstellung [34], zweidimensional, treu, aber in der Charakteristik q, was zur Folge hatte, daß der Rückschluß vom charakteristischen Polynom auf die Frobeniuselemente nicht eindeutig war; auch dort kamen Eulerfaktoren einer Modulform ins Spiel, aber einer solchen vom Gewicht 2, deren L-Funktion keine Artinsche sein kann. Diese ganze Konfiguration von Primzerlegung, Darstellung und Modulform ist verschieden von derjenigen, die wir für den allgemeinen Fall beschrieben haben; sie steht sozusagen quer dazu. „Morgendämmerung“ habe ich sie genannt, weil die Verbindung von Primzerlegung mit Modulformen hier zum ersten Mal an einem substantiellen und „essentiell nichtabelschen“ Beispiel aufgewiesen wurde.

Die Modularität (im Fall d = 2) scheint mittlerweile bewiesen für „ungerade“ r, d.h. det r(komplexe Konjugation) = – 1 . Ausgangspunkt ist die Klassifikation der (irreduziblen) endlichen Untergruppen von $PGL(2,\mathbb{C})$: Diedergruppen, Tetraeder-, Oktaeder- und Ikosaedergruppe; dabei haben die Diedergruppen isomorphe Urbilder in $GL(2,\mathbb{C})$, die Polyedergruppen nur zentrale Erweiterungen (anders gesagt: sie besitzen irreduzible zweidimensionale *projektive*, nicht aber gewöhnliche Darstellungen). Der Diederfall ist klar, weil diese Gruppen monomial sind [35] ; der Tetraederfall wurde von Langlands, der Oktaederfall von Langlands und Tunnell bewiesen; der Ikosaederfall scheint ebenfalls den langjährigen Bemühungen vieler nachzugeben [36] .

19. Die (vermutete) Langlandskorrespondenz läßt sich lesen als Parametrisierung von Galoisdarstellungen durch automorphe Darstellungen, aber auch umgekehrt; so daß ein „Informationsfluß“ in beiden Richtungen stattfindet [37] . Wir haben schon gesehen, was uns die Modularität einer Artinschen L-Funktion bringt, nämlich ihre holomorphe Fortsetzbarkeit [38] . Was den uns hier leitenden Gesichtspunkt betrifft, das Zerlegungsproblem, scheint mir der Informationsfluß eher in der Gegenrichtung zu erwarten. Es ist vom „Gesichtspunkt“ der Modulformen, die primär analytische Objekte

sind, gar kein rechter Anhaltspunkt zu erkennen, um über einzelne Hecke-Eigenwerte etwas auszumachen; hingegen hat die Zahlentheorie, für die das Zerlegungsproblem ein natürliches ist, zu seiner Behandlung einen schlagkräftigen Begriffsapparat entwickelt (mit den Frobeniusautomorphismen als Protagonisten, und nicht nur hier, sondern in der ganzen arithmetischen Geometrie). Ein Analogon des Satzes von Tschebotareff ist, soweit ich sehe, auf der automorphen Seite nicht vorhanden; hier wird also etwas für Modulformen gewonnen, wenn ihre L-Reihen als artinsche bekannt sind. In diese Richtung geht ein Satz von Deligne und Serre: die L-Reihe einer normalisierten Neuform vom Gewicht 1 und ungeradem Nebentyp ist artinsch; daraus kann man Aussagen über die Dimensionen gewisser Räume von Modulformen gewinnen [39].

Existenzsatz und Reziprozitätsgesetz sind die zentralen Aussagen der Klassenkörpertheorie, und eine Theorie, welche diese beiden als Spezialfälle enthält, kann mit Fug und Recht eine verallgemeinerte Klassenkörpertheorie genannt werden, wie das ja auch regelmäßig geschieht [40]. Zu bedenken ist natürlich, daß jede Verallgemeinerung auch eine Verdünnung oder Vergröberung impliziert und man nicht erwarten kann, daß jedes Strukturmoment erhalten bleibt oder ein Analogon findet [41]. Zum Beispiel führt die Korrespondenz der Darstellungen nur im abelschen Fall zu einem Isomorphismus von Gruppen (weil hier die Darstellungen (Charaktere) selbst eine Gruppe bilden); selbst wo wir in nichtabelschen Fällen ein Zerlegungsgesetz haben, kann von derlei keine Rede sein [42]. Dennoch wird, wer von der klassischen Zahlentheorie her zum ersten Mal mit den Langlandsschen Ideen in Berührung kommt, ein anfängliches Unbehagen nicht unterdrücken können. Ein besonderes Faszinosum der Klassenkörpertheorie liegt doch darin, daß sie etwas zunächst gar nicht Sichtbares und in der Tat nicht ohne weiteres Zugängliches, nämlich abelsche Erweiterungen, in Verbindung bringt mit einem durch den Grundkörper selbst unmittelbar Gegebenen, auch strukturell (vergleichsweise) leicht Verständlichen, nämlich den Idealgruppen; besonders frappant im Falle des rationalen Grundkörpers, wo man ja nur die primen Restklassengruppen und ihre Untergruppen aufzählen muß und durch den Satz von Kronecker-Weber auch noch explizite und gut verstandene Erzeuger der Strahlklassenkörper in der Hand hat. Einfache Beziehungen im „gruppentheoretischen Untergrund“ münzen sich um zu höchst konkreten diophantischen Aussagen, die anders nicht verständlich sind (wir haben das oben in **9** gesehen). Dagegen scheint es bei der Langlandskorrespondenz für Dimensionen $d > 1$, daß man ein unbekanntes X durch ein Y beschreiben möchte, das man ebensowenig kennt, ja sogar noch weniger (was sicherlich für $d > 2$ der Fall ist [43]). Das betrifft Existenzsatz wie Reziprozitätsgesetz; automorphe Darstellungen sind noch weniger „sichtbar“ als galoissche Erweiterungen, und die Verteilung von Hecke-Eigenwerten ist nicht weniger mysteriös als die von Zerlegungstypen.

Das kann natürlich kein Einwand gegen das Programm sein, dessen epochale Bedeutung darin liegt, daß zwei mathematische Weltteile miteinander in Verbindung treten, ja möglicherweise sich „im Innersten“ als identisch erweisen, deren wechselseitige Beziehungen vordem eher zufällig erschienen, jedenfalls nicht in einen systematischen Rahmen gebracht waren. Vor einer Sache von solcher Wichtigkeit muß die Frage zurücktreten, was wir als Zahlentheoretiker „davon haben“. Es ist oben schon deutlich geworden, daß beim Übergang vom abelschen zum allgemeinen Fall eine Steigerung der

Komplexität zu erwarten ist, der unser Vermögen zur Anschauung vielleicht nicht mehr gewachsen ist, oder genauer: die Anschauung, derer wir immer bedürfen, wird genötigt, den Boden des „Konkreten“, das heißt des Bekannten und Vertrauten zu verlassen und auf eine Symbolik höherer Stufe überzugehen. Es ist, wie wenn man ein hohes und weitläufiges Gebirge erwandert: zu Anfang freut man sich an jedem Hügel und Felsklotz, aber je höher man gelangt, desto mehr tritt das Einzelne zurück, und zuletzt sieht man nur noch die großen Linien [44].

20. „Wir müssen wissen, wir werden wissen“, schrieb Hilbert. Das Wissen kann freilich, wie wir seither gelernt haben, auch darin bestehen, daß wir etwas als nicht wißbar wissen. Wenn eine Gruppe ein unlösbares Wortproblem hat (und das geschieht schon in „kleinen“ arithmetischen Gruppen), dann wissen wir, daß wir die Elementarithmetik in ihr aus prinzipiellen Gründen nicht beherrschen können, was übrigens andere und vielleicht wichtigere Aussagen nicht ausschließt. In dem engeren Bereich zahlentheoretischer Forschung, der uns hier beschäftigt hat, sind solche Barrieren, soweit ich sehe, bisher nicht aufgetaucht. Daß nicht „alles explizit“ zu haben ist, liegt in der Natur der Dinge, und schon bei Ganzheitsbasen, Idealklassen und Einheiten von Zahlkörpern begnügen wir uns mit einer Handvoll explizit ausgearbeiteter Beispiele, einigen allgemeinen Struktursätzen und schließlich damit, daß wir über Algorithmen verfügen, die für jeden konkreten Fall von räsonabler Größenordnung gut genug sind. Aber hier wird die Grenze durch Quantität definiert; ein Resultat wie die Unlösbarkeit des Wortproblems ist qualitativer Natur und zwingt zum Nachdenken darüber, was sinnvoll anzustreben ist [45].

Vielleicht ist ja die abelsche Welt eine Insel der Ordnung, die wir gerade noch verstehen, vergleichbar einem Garten, umgeben von einem zunehmend undurchdringlichen Wald, in den wir nur hier und da eine Begriffsschneise schlagen, im übrigen aber nur noch mit elektronischer Hilfe eintreten können [46]. Freilich, wenn wir schon den Wald nicht zum Garten machen können, wollen wir ihn irgendwie „überschauen“. Naturgemäß ändert sich dabei der Stil mathematischer Betrachtung und dessen, was wir in der Mathematik „Sehen“ und „Verstehen“ nennen; manchem zum Verdruß [47]. Die *querelle des anciens et des modernes* ist aber in der Mathematik nicht wirklich virulent, denn in ihr bedeutet eine Änderung des Stils keine Preisgabe von Inhalten. Wo der Fortschritt beweisbar ist und keine Geschmacksfrage, ist es die Sache selbst, die seinen Methoden Geltung verschafft [48].

Immer aber kann man darauf zählen, daß ein Rettendes mitwächst. In dem Maße, in dem eine Sache verstanden wird, werden ja auch die Zugänge zu ihr leichter; heute lernt jeder im Grundstudium, was einmal der Gipfel der Gelehrsamkeit war (und das nicht nur in der Mathematik). Erst wenn die „richtigen“ Grundbegriffe etabliert sind, stellt sich die Durchsicht ein, die wir anstreben, vereinfacht sich auch die Sprache. Wenn wir eine Sache nicht durchschauen, kann das ja auch daran liegen, daß wir sie von der falschen Seite betrachten, mit einer inadäquaten Begrifflichkeit. Nicht nur über die Schwierigkeit, sondern auch über den wahren Gehalt eines Problems können wir erst dann etwas sagen, wenn wir es gelöst haben.

Anmerkungen und Nachweise

1 Um genau zu sein, muß man noch R zu den datis hinzunehmen.

2 Die Zerlegung fast aller p in einem Zahlkörper determiniert die der restlichen; das folgt daraus, daß die Zetafunktion einer Funktionalgleichung genügt, was für ein Aggregat endlich vieler Eulerfaktoren nicht möglich ist (das ist eine Art „multiplicity one“).

3 Zunächst nur für galoissche Erweiterungen, vermittels der „Fernsteuerung“ des Zerlegungsverhaltens durch Frobeniuselemente in galoisschen Oberkörpern (siehe **12**) aber auch allgemein.

4 Bewertungstheoretisch betrachtet, folgt das PZG aus dem allgemeinen (auch für archimedische Bewertungen gültigen) Fortsetzungsprinzip. Schreibt man die Zerlegung von $f(x)$ mod p in der Form $f(x) \equiv F_1(x)...F_r(x)$ mod p mit teilerfremden F_i , so zeigt das Henselsche Lemma, daß diese Zerlegung auf die Komplettierung R_p gehoben werden kann; die Faktoren liefern verschiedene Erweiterungen von K_p , auf welche die Fortsetzung der p-Bewertung von K_p eindeutig ist und in die L eingebettet werden kann; so erhält man alle Fortsetzungen der p-Bewertung von K auf L.

5 Siehe H.Cohen, A Course in Computational Algebraic Number Theory, Springer 1996, S.124.

6 Der durchsichtigste Beweis des quadratischen Reziprozitätsgesetzes besteht übrigens darin, daß man, ausgehend von der Beobachtung, daß der p-te Kreisteilungskörper den quadratischen Körper $\mathbb{Q}(\sqrt{p^*}$ enthält ($p^* = p^{(p-1)/2}$), für ungerades $q \neq p$ die Zerlegung im quadratischen Körper mit der im Einheitswurzelkörper vergleicht. Es verdient hier auch bemerkt zu werden, daß die Reziprozitätsformel, wenn man die Legendresymbole im Sinne des PZG versteht, eine Aussage über Primzerlegung in *zwei verschiedenen* Körpern ist.

7 Man wird natürlich nicht jede symmetrische Relation (wie Isomorphie von Gruppen) als Reziprozität bezeichnen. Der Sprachgebrauch und die ihn tragende Intuition sind nicht leicht zu präzisieren, aber Entitäten, die in einer Beziehung der Reziprozität stehen, sollten „vom selben Typus“ sein, was man von Idealklassen und Automorphismen nicht sagen kann. Hasse rechtfertigt die Benennung im Zahlbericht II (Nachdruck 1965), S.52/53, aber er bezieht sich dabei auf das Potenzrestsymbol, wo eine Rechtfertigung überflüssig ist. Für den allgemeinen Fall siehe den Jugendtraum-Aufsatz von Langlands, in dem Band: Mathematical Developments Arising from Hilbert Problems, AMS Proc.Symp.Pure Math. XXVIII, Providence 1976, Bd.2, S.408/409.

8 Das Beispiel ist vielerorts behandelt und findet sich schon in Hasses Zahlbericht II, S.67; siehe auch H.Cohn, A Classical Invitation to Algebraic numbers and Class Fields, Springer 1978, p.236. Eine sehr durchsichtige Behandlung gibt H.M.Stark in seinem Beitrag zu dem Band „From Number Theory to Physics“, Waldschmidt/ Moussa/Luck/Izykson (edts.), Springer 1992, S.391. Für einen „elementaren“ Beweis

(ohne Explikation des klassenkörpertheoretischen Zusammenhangs) siehe K.Ireland/ M.Rosen, A Modern Introduction to Classical Number Theory, Springer, 1982, S. 119. Vor allem natürlich: D.Cox, Primes of the Form $p = x^2 + ny^2$, Wiley 1989.

9 Siehe das in Anm.8 genannte Buch von Cox.

10 Noch ein ähnliches Kriterium: p hat einen Primteiler vom Grad 1 genau dann, wenn $p = (N(a), N(b))$ für ganze a, b ist. Denn ist $f(P/p) = 1$, schreibe $P = (a,b)$, wo b in keinem der andern Primteiler von p liege; die Umkehrung ist klar.

11 Ein mehr systematischer Ansatz könnte so aussehen: sei L/K eine Galoissche Erweiterung mit der Gruppe G. Dann ist L das Kompositum der Fixkörper aller Elemente von G, außer wenn G zyklisch von Primzahlpotenzordnung ist (und damit ist man im Bereich der Klassenkörpertheoretie). Denn ein Element, welches dieses Kompositum elementweise fixiert, muß im Durchschnitt aller zyklischen Untergruppen von G liegen, und dieser ist, wie man leicht sieht, trivial außer in dem angegebenen Fall. L ist also Kompositum von Teilkörpern, über denen L zyklisch ist. Sollte es nicht möglich sein, die klassenkörpertheoretischen Informationen für all diese einzelnen Erweiterungen zu substantiellen Aussagen über die Arithmetik von L, insbesondere die Primzerlegung umzumünzen?

12 Hasse, Zahlbericht II, § 27, VIII.

13 G.Bruckner, Eine Charakterisierung der in algebraischen Zahlkörpern voll zerlegten Primzahlen, Math.Nachr.36 (1968), S.153 ff.

14 C. Adelmann, The Decomposition of Primes in Torsion Point Fields, SLN 1761. Das fragliche Polynom findet man S.105 unten.

15 Siehe etwa Janusz, Algebraic Number Theory, Acad.Press 1977, prop. III.2.8. Das ist die oben versprochene „Fernsteuerung“.

16 Für eine umfassende Behandlung des Themas siehe N. Klingen, Arithmetic Similarities, Oxford 1998. Sogar $K_p \cong L_p$ für alle p ist möglich, siehe S.236.

17 Die Schwierigkeiten sind in der Tat so beträchtlich, daß Hasse es in einem Vortrag von 1952 für „kaum möglich“ erklärte, die Verhältnisse ähnlich explizit zu machen wie in unserm Beispiel (Über das Problem der Primzerlegung in algebraischen Zahlkörpern, Sitz.Ber.Berl.Mathem.Ges., 1951/52, S.20). Ein metabelsches G sitzt in einer exakten Sequenz

$$1 \rightarrow A \rightarrow G \rightarrow B \rightarrow 1, \ A, B \text{ abelsch},$$

ist also eine Erweiterung von B mit A. Es zeigt sich, daß die Primzerlegung in einer Körpererweiterung L/K mit $G = Gal(L/K)$ ziemlich empfindlich von der Natur dieser Erweiterung abhängt (diese kann ja auch abelsch sein); siehe die Diskussion schon im Zahlbericht II (§ 13) und bei H.Cohn, Introduction to the Construction of Class Fields, Cambridge UP 1985, ch.8. Mittlerweile gibt es natürlich eine reiche Literatur zur

Arithmetik von Zahlkörpern mit spezifischen Galoisgruppen; aber selbst wo die Gruppen, vom rein gruppentheoretischen Gesichtspunkt, einfach strukturiert sind, wird die arithmetische Komplexität enorm, und ein Durchbruch zu einer allgemeinen Theorie scheint auf diesem Wege nicht erreichbar.

18 G.Shimura, A Reciprocity Law in Nonsolvable Extensions, Crelle 1966.

19 Die Morgendämmerung hätte vielleicht schon eher stattfinden können, nämlich als Artin und Hecke gleichzeitig an derselben Universität ihre L-Reihen kreierten, anscheinend ohne sich darüber auszutauschen. Siehe dazu die Bemerkungen von Tate in seinem Beitrag „The general reciprocity law" zu dem in Anm. 7 angegebenen Werk, Bd. 2. S.321.

20 Siehe Adelmann (Anm. 14), prop.3.5.3. Shimura hatte dieses Resultat noch nicht und begnügte sich mit ad-hoc-Argumenten für $7 \leq q \leq 97$.

21 Adelmann (Anm. 14) formuliert prop. 5.6.3 ein Zerlegungsgesetz für Erweiterungen dieses Typs über einem beliebigen Zahlkörper; natürlich ohne Rekurs auf den „modularen" Aspekt, der allgemein (noch) nicht verfügbar ist. Die „Hauptarbeit" in seinem Resultat leistet das PZG, insofern eine Spezifikation der klassischen Modulpolynoms für den „nichtabelschen" Teil der Erweiterung verantwortlich ist.

22 Siehe dazu S.Lang/H.Trotter, Frobenius Distribution in GL(2)-Extensions, SLN 504, p.271s. Möglicherweise ist die Anwendung von PZG in solchen Fällen nicht aufwendiger als die Berechnung der Koeffizienten.

23 Man fragt sich hier, was die Adjunktion von Torsion aus andern algebraischen Gruppen ergibt. Das Beispiel von E (nach Wiles et al. mittlerweile auf beliebige elliptische Kurven über $\mathbb{Q}$ übertragbar), verallgemeinert sich auf abelsche Varietäten. Eine irreduzible endliche affine Matrixgruppe H erzeugt eine einfache Algebra $\mathbb{Q}(H)$ (im zyklischen Fall ein Kreisteilungskörper) mit einer natürlichen Ordnung $\mathbb{Z}(H)$, die in aller Regel nicht maximal ist, so daß die Frage nach einer Primzerlegung nicht ohne weiteres einen Sinn hat.

24 Siehe S.Gelbart, Automorphic Forms on Adele Groups, Princeton UP 1975, oder S.Kudla, From Modular Forms to Automorphic Representations, in: Bernstein/Gelbart (edts.), An Introduction to the Langlands Program, Birkhäuser 2004. Eine etwas andere, sorgfältige Diskussion bei D.Bump, Automorphic Forms and Representation Theory, Cambridge UP 1996, prop.3.1.2.

25 Diese Bijektion ist vielleicht das beste Argument für die gelegentlich begegnende Behauptung, die Klassenkörpertheorie sei eine „multiplikative" Theorie. Demnach wäre ihre Verallgemeinerung (s.u.) jedenfalls nicht mehr „rein multiplikativ" zu nennen. Es gibt aber noch weitere multiplikative Momente: Primzerlegung der Ideale, auch die Frobeniusautomorphismen, die auch in der Verallgemeinerung eine zentrale Rolle spielen.

26 Das geht allerdings nur für den Grundkörper $\mathbb{Q}$; im allgemeinen erhält man aus der Dirichletreihe nur die „semilokalen“ Eulerfaktoren, das Produkt der Faktoren für alle Primteiler der Primzahl p im Erweiterungskörper.

27 Siehe z.B. C.Curtis/I.Reiner, Representation Theory of Finite Groups and Associative Algebras, Wiley 1962, § 52. Eine rein gruppentheoretische Charakterisierung der M-Gruppen scheint es nicht zu geben. Für die Artinsche Vermutung genügt übrigens, daß ein ganzes Vielfaches $m\chi$ positive Linearkombination monomialer Charaktere ist (diese Bedingung ist z.B. für A_5 nicht erfüllt).

28 Langlands hat darauf hingewiesen, daß es *kein einziges* Beispiel für eine motivische L-Funktion gibt, die als holomorph fortsetzbar, aber nicht als automorph bekannt ist.

29 Nach einem Satz von Gaschütz hat eine endliche Gruppe genau dann eine treue irreduzible Darstellung, wenn ihr Sockel (das Produkt der minimalen abelschen Normalteiler) von einer einzigen Konjugationsklasse erzeugt wird; im abelschen Fall sind dies genau die zyklischen (wie es sein muß).

30 Diese Betrachtungen führen mit einer gewissen Konsequenz dazu, nicht einen Zahlkörper, sondern eine Darstellung von $G(\mathbb{Q})$ als „primäres“ Datum anzusehen.

31 Siehe dazu die in Anm.24 angeführten Arbeiten von Gelbart und Kudla. Allgemein gilt diese Gleichheit nur bis auf eine Argumentverschiebung, welche daher rührt, daß die ersteren einer Funktionalgleichung vom Typ $s \leftrightarrow 1 - s$ genügen, die letzteren aber einer vom Typ $s \leftrightarrow k - s$, wo k das Gewicht der Form bezeichne. Da aber die Artinschen L-Reihen den Typ $s \leftrightarrow 1 - s$ aufweisen, spielt dieser Umstand für uns keine Rolle.

32 Weiter sollte die Stufe von f dem Artinführer von χ und der Nebentypus der Determinante von r entsprechen; siehe etwa Ehud de Shalit, Artin L-Functions, in Bernstein/Gelbart (Anm.24).

33 Das Defizit bei Shimuras Beispiel tritt hier nicht auf, da Matrizen endlicher Ordnung in Charakteristik Null halbeinfach sind.

34 Die dort auftretenden Gruppen GL(2,q) besitzen übrigens für $q > 3$ keine irreduziblen zweidimensionalen Darstellungen.

35 Die L-Reihen sind abelsch über einem quadratischen Zahlkörper und wurden schon von Hecke bzw. Maass als L-Reihen von Modulformen erkannt (erstes Beispiel für automorphe Induktion *avant la lettre*). Genauer: die Diedergruppe D_n hat treue irreduzible Darstellungen vom Grad 2, induziert von der zyklischen Rotationsgruppe mit der Ordnung n und dem Index 2. Diedererweiterungen über $\mathbb{Q}$ treten zum Beispiel auf als Hilbertsche Klassenkörper von quadratischen Zahlkörpern mit zyklischer Idealklassengruppe, siehe auch die Ringklassenkörper aus **9**. Explizit ausgearbeitete Beispiele findet man in T.Hiramatsu, Theory of Automorphic Forms of Weight 1, in:

Advanced Studies in Pure Math., Vol. 13, ed, T. Kubota, Academic Press 1988 (ich verdanke Herrn H.Opolka (Braunschweig) den Hinweis auf diese Arbeit); auch bei J.-P.Serre, Modular Forms of Weight One and Galois Representations, Durham Symposium on Algebraic Number Fields, Academic Press 1977 (= Œuvres III, Nr. 110).

36 Ich weiß nicht, ob alle einschränkenden Bedingungen mittlerweile eliminiert sind; die Resultate, die ich gesehen habe, lassen wenig Zweifel daran, daß dies früher oder später der Fall sein wird.

37 Siehe etwa J.Cogdell in Bernstein/Gelbart (Anm.24), p.229, 235.

38 Hier muß Weils „converse theorem“ erwähnt werden, das beinahe die Umkehrung darstellt: ist $L(s,\chi)$ zusammen mit „genügend vielen“ $L(s,\chi\otimes\psi)$, wo die ψ eindimensionale Charaktere sind, holomorph fortsetzbar, dann ist $L(s,\chi)$ modular; die Artinsche Vermutung für *alle* diese $L(s,\chi\otimes\psi)$ ist also äquivalent zur Modularität *von allen*.

39 Siehe die in Anm. 35 genannte Arbeit von Serre, § 9. Man beachte auch die scharfe „multiplicity one“- Aussage am Schluß von § 5.

40 In seinem populären Aufsatz „What is a Reciprocity Law?“ (Amer.Math.Monthly 79, 1972) verlangt B.F.Wyman von einem „guten“ (allgemeinen) Reziprozitätsgesetz, daß es das Artinsche als Spezialfall enthält. Dem kann man zustimmen, wenngleich damit die Meßlatte reichlich hoch gehängt wird. Wenn er aber von einem „sehr guten“ noch einen verallgemeinerten Existenzsatz fordert, vermengt er zwei Aspekte, die man auseinanderhalten kann und sollte (der Existenzsatz wurde vor dem Reziprozitätsgesetz bewiesen, moderne Darstellungen bevorzugen die umgekehrte Reihenfolge).

41 Wenn freilich die Verallgemeinerung zu weit geht, verliert sich der Bezug; man kann nicht ohne weiteres, wenn X ein Spezialfall von Y ist, Y eine Verallgemeinerung von X nennen. Ein Fahrrad ist ein Fahrzeug, aber es wäre absurd, ein Fahrzeug als verallgemeinertes Fahrrad zu bezeichnen.

42 Um auf beiden Seiten zu Gruppen zu gelangen, muß man die Leiter der Vermutungen noch viel weiter hinaufklettern bis zur motivischen bzw. automorphen Galoisgruppe. Sehr weitgehende Erwartungen formuliert L.Clozel, Motifs et Formes Automorphes, in: L.Clozel/J.Milne (edts.), Automorphic Forms, Shimura Varieties and L-Functions, Academic Press 1990.

43 Für $d = 3$ gibt es Ansätze, die Langlandskorrespondenz wenigstens in Einzelfällen in Evidenz zu setzen; siehe z.B. van Geemen u.a., Hecke Eigenforms in the Cohomology of Congruence Groups of $SL(3, \mathbb{Z})$, Exper.Math. Vol 6 (1997), Nr.2. Der numerische Aufwand ist hier schon sehr groß. Nur im Fall $d = 2$ lassen sich die geometrischen, arithmetischen und analytischen Aspekte, deren Synthese das Ziel des Langlandsprogramms ist, noch in der „gewöhnlichen“, also mehr oder weniger traditionellen Anschauung vereinigen; was natürlich damit zu tun hat, daß der zugehörige

symmetrische Raum (die obere Halbebene) hier zweidimensional ist und obendrein eine komplexe Struktur trägt, was für d = 3 schon nicht mehr der Fall ist.

44 Ob eine Zahl Summe von zwei Quadratzahlen ist, erscheint als elementares und natürliches Problem, das man auch einem Laien nahebringen kann, die Verallgemeinerung auf beliebige Normformen dagegen als nur noch akademisch. Die Wissenschaft kann solche Unterscheidung natürlich nicht gelten lassen; aber sie macht sich von selbst geltend, einfach dadurch, daß die allgemeinen Resultate schwächer sind als die speziellen. Das ist eine Banalität; trotzdem fällt es mitunter schwer, sich den Konsequenzen zu fügen.

45 Hier kommt auch der Hegelsche Umschlag von Quantität in Qualität ins Spiel. Man kann leicht Aufgaben formulieren, die theoretisch problemlos sind, an denen aber das ganze (bekannte) Universum, in einen Supercomputer verwandelt, scheitern müßte. Welchen Sinn hat es dann noch, von „prinzipieller“ Lösbarkeit zu sprechen?

46 Hierzu eine bekannte Passage von Nietzsche: „Hüten wir uns, etwas so Formvolles wie die zyklischen Bewegungen unserer Nachbarsterne überhaupt und überall vorauszusetzen; schon ein Blick in die Milchstraße läßt Zweifel auftauchen, ob es dort nicht viel rohere und widersprechendere Bewegungen gibt, ebenfalls Sterne mit ewigen geradlinigen Fallbahnen und dergleichen...“ (Fröhliche Wissenschaft, § 109). Vielleicht haben wir uns zu sehr gewöhnt an die Erfahrung beständigen Fortschritts (wie in der Wirtschaft an beständiges Wachstum).

47 Siehe zum Beispiel die Präambel zu dem Buch von Cohn (Anm. 8).

48 Es scheint derzeit kein anderer Weg zu einer nichtabelschen Klassenkörpertheorie erkennbar als der von Langlands gewiesene. Der naheliegende, von Hasse und andern verfolgte Gedanke, die (seit dem Hauptsatz von Hasse-Brauer-Noether) gut verstandene Theorie der Algebren über Zahlkörpern zu diesem Zweck nutzbar zu machen, hat offenbar nicht zu den gewünschten Resultaten geführt; ganz neue Ideen scheinen nötig. Freilich ist das Programm von Langlands keine Weiterentwicklung der klassischen Theorie, sondern ein radikaler, auch nur teilweise durch das Zerlegungsproblem motivierter Neuansatz.