Karlsruher Institut für Technologie
Fakultät für Mathematik
Institut für Algebra und Geometrie

Über Galoisdeformationen, p-adische L-Funktionen und Iwasawa-Theorie

Diplomarbeit

von

Michael Fütterer

22. Mai 2013

Stand: 1. Juli 2013

Betreuer: PD Dr. Stefan Kühnlein
Dr. Fabian Januszewski

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine außer den angegebenen Quellen und Hilfsmitteln verwendet habe.

Karlsruhe, den 22. Mai 2013

Michael Fütterer

Vorwort

Die Zahlentheorie stellt jeden, der sich mit ihr beschäftigt, vor enorme Herausforderungen: Obwohl die ursprünglich zu untersuchenden Objekte – ganze Zahlen – so simpel erscheinen, verbergen sich hinter ihnen und den Mitteln, mit denen man ihr Verhalten zu beschreiben versucht, Strukturen von ungeahnter Komplexität, deren Eigenschaften auf den ersten Blick mitunter einer verblüffenden Regellosigkeit, ja fast Willkür, zu unterliegen scheinen, obwohl die ganzen Zahlen doch so regelmäßig gebaut sind. Umso faszinierender sind vor diesem Hintergrund Vermutungen oder gar Ergebnisse, die ein solches Verhalten zu erklären versuchen. Die Iwasawa-Theorie möchte für gewisse zahlentheoretische Phänomene genau solche Erklärungen liefern und diesen damit eine konzeptionelle Grundlage geben.

Die arithmetischen Objekte, die man hierbei studiert, sind im allgemeinsten Fall sogenannte *Motive* über algebraischen Zahlkörpern. Dieser Begriff wird an wenigen Stellen in dieser Arbeit verwendet, ohne dass wir präzisieren, was genau darunter zu verstehen ist – jedoch fallen z.B. solch interessante Objekte wie der Zahlkörper selbst oder elliptische Kurven über diesem darunter. Einem solchen Motiv ordnet man nun eine gewisse Gruppe zu, die wichtige Eigenschaften desselben beschreibt: im Falle eines Zahlkörpers ist dies seine Idealklassengruppe, im Falle elliptischer Kurven die Selmer-Gruppe und in anderen Fällen entsprechende Verallgemeinerungen derselben. Aussagen über diese Gruppen liefern Erkenntnisse über das Motiv und haben letztlich auch Auswirkungen auf diophantische Probleme, daher ist man vorrangig daran interessiert, diese Gruppen zu beschreiben. Dies ist im Allgemeinen jedoch ein sehr schwieriges Problem.

Iwasawa hatte dazu eine entscheidende Idee: Anstatt diese Motive über einem einzelnen Zahlkörper zu betrachten, können wir ihr Verhalten in einem unendlichen Körperturm studieren. Dies scheint auf den ersten Blick komplizierter zu sein, hat jedoch aus algebraischer Sicht viele Vorteile und führt zu einer fruchtbaren Theorie. Die Gesamtheit der oben erwähnten Gruppen in dem Körperturm wird dadurch zu einem Modul über einem gewissen Ring, der *Iwasawa-Algebra*, und solche Moduln haben angenehmere Eigenschaften als die entsprechenden Objekte für einen einzelnen Zahlkörper. Auf diesem Wege konnte Iwasawa eine Reihe von Ergebnissen etwa über Idealklassengruppen in solchen Körpertürmen erzielen.

Ein anderer zentraler Untersuchungsgegenstand der Zahlentheorie sind L-Funktionen. Man kann jedem Motiv mit einer einfachen Formel eine solche zuordnen – diese ist dann (zunächst) einfach eine holomorphe Funktion in einem Teil der komplexen Zahlenebene. Im Falle der Zahlkörper ist dies die Riemannsche oder Dedekindsche Zetafunktion, im Falle elliptischer Kurven ihre Hasse-Weil-L-Funktion. Es wurde bereits früh erkannt, dass diese Funktionen benutzt werden können, um Aussagen über die oben erwähnten Gruppen zu treffen: So hat z.B. Kummer gezeigt, dass man durch Auswerten der Riemannschen Zetafunktion an gewissen Stellen entscheiden kann, welche Primzahlen die Klassenzahlen von Kreisteilungskörpern teilen.

Dieser überraschende Zusammenhang lässt sich aus heutiger Sicht mit der Iwasawa-Theorie erklären. Sie bringt p-adische Analysis ins Spiel, um die L-Funktion eines Motivs in ein p-adisches Objekt zu verwandeln, und durch eine sogenannte *Hauptvermutung* wird ein Zusammenhang zwischen dieser p-adischen L-Funktion und dem oben erwähnten Modul über der Iwasawa-Algebra ausgedrückt. Auf diese Weise wird ein Aspekt der gerne geschriebenen Phrase, dass L-Funktionen „arithmetische Informationen kodieren“, präzisiert.

In der klassischen Iwasawa-Theorie hat der erwähnte Körperturm stets eine abelsche Galoisgruppe. Verzichtet man auf diese Bedingung, wird man zur nichtkommutativen Iwasawa-Theorie geführt, die in den letzten Jahren an Bedeutung gewonnen hat. Schon aus technischer Sicht ist die nichtkommutative Theorie komplizierter, und es war zunächst nicht klar, wie eine nichtkommutative Hauptvermutung formuliert werden sollte. Nachdem entscheidende algebraische Resultate u.a. von Venjakob erzielt wurden, wurde eine solche für elliptische Kurven von Coates, Fukaya, Kato, Sujatha und Venjakob aufgestellt. Die Konstruktion nichtkommutativer p-adischer L-Funktionen in diesem Rahmen ist gegenwärtig im Allgemeinen noch ein offenes Problem.

In dieser Arbeit wird erklärt, wie man die Arbeiten von Hida zu Familien von Modulformen und deren Verbindung zur Deformationstheorie benutzen kann, um p-adische L-Funktionen zu solchen Familien (deren Konstruktion bereits bekannt ist!) als Funktionen auf gewissen Galoisdarstellungen und damit als „nichtkommutative p-adische L-Funktionen“ aufzufassen. Dazu verwenden wir sogenannte „$R = T$“-Sätze über die Identifikation gewisser Hecke-Algebren mit Deformationsringen, die von Mazur vermutet und in bestimmten Fällen u.a. von Wiles als Teil seines Beweises von Fermats letztem Satz gezeigt wurden. Die Funktionen, die wir dadurch bekommen, lassen sich leider nicht direkt mit einer nichtkommutativen p-adischen L-Funktion im oben erwähnten Sinne vergleichen (ganz davon abgesehen, dass die in den Formeln auftretenden Perioden einen solchen Vergleich ohnehin stark erschweren). Man könnte darauf hoffen, dass dies für p-adische L-Funktionen zu Familien höherdimensionaler automorpher Formen möglich ist (für solche ist in gewissen Fällen ebenfalls eine Konstruktion bekannt). Hierauf kann in dieser Arbeit jedoch nicht mehr eingegangen werden.

Danksagung. Es bleibt, den vielen Personen zu danken, die zum Entstehen dieser Arbeit beigetragen haben. Ohne die zahlreichen Menschen, die mich in meinem Studium und darüber hinaus unterstützt haben, wäre diese sicher nicht in dieser Form möglich gewesen.

Meine beiden Betreuer haben mir viel Vertrauen entgegengebracht und ließen mich mit großer Selbstständigkeit arbeiten, ohne mich aber jemals alleine zu lassen, wofür ich mich sehr herzlich bedanken möchte. Sie hatten stets ein offenes Ohr für meine Fragen und haben sich immer die Zeit genommen, sich mit diesen auseinanderzusetzen.

Stefan Kühnlein hatte von frühen Semestern an mit vielen schönen Vorlesungen und Seminaren maßgeblichen Anteil daran, dass mein Interesse für die Algebra und Zahlentheorie geweckt wurde. Durch seine erfrischende Art, Wissen zu vermitteln, hat er immer wieder gezeigt, wie viel Spaß die Beschäftigung mit Mathematik bereiten kann. Was die Wahl meines Themas angeht, hat er mir viel Freiheit eingeräumt und sich nicht aus der Ruhe bringen lassen, wenn ich ein wenig wählerisch war. Nicht zuletzt danke ich auch für das bereitwillige Verleihen von Büchern und einen wertvollen Hinweis in der Endphase, mit dem sich ein Argument (p-adisch) vervollständigen ließ.

Fabian Januszewski war immer gerne bereit, sein umfangreiches Wissen über Iwasawa-Theorie und viele andere Bereiche der Mathematik mit mir zu teilen. In zahllosen Gesprächen hat er mir immer wieder große Zusammenhänge in der modernen Zahlentheorie verdeutlicht und mir so ein Gefühl dafür gegeben, was „wichtig“ ist. Seine Weitsicht hat sich bei der richtigen Einordnung der vielen Objekte als sehr wertvoll erwiesen. Aber auch die vielen Feinheiten und Details, die es vor allem in der Hida-Theorie zu beachten gilt, hat er ausführlich mit mir diskutiert und mir so oft einen Ausweg gezeigt, wenn ich nicht weiterkam.

Mein ganz besonderer Dank gilt meinen Eltern, die mir mein Studium überhaupt erst ermöglicht haben und mit deren Unterstützung im Rücken vieles ein großes Stück unbeschwerter möglich ist, und auch meinen beiden Schwestern, die immer hinter mir stehen.

Sehr wichtig war auch die Unterstützung meiner Kommilitonen und Freunde, die nicht nur mit mir über mathematische Fragen diskutierten, sondern mir auch in anderen Situationen immer hilfreich zur Seite stehen und auf die ich mich stets verlassen kann. Hier möchte ich besonders Jonathan Zachhuber, Miriam Schwab, Florian Nisbach, Tobias Columbus, Felix Wellen, Enrica Cherubini und Lisa Kohl erwähnen. Sie alle haben auf die ein oder andere Art meinen Horizont erweitert. Ebenso danke ich vielen Freunden aus verschiedenen Orchestern, mit denen ich viel Spaß an der Musik und anderen Beschäftigungen hatte.

Danken möchte ich auch Prof. C.-G. Schmidt, der mir den Besuch der Konferenz „Iwasawa Theory, Representations and the p-adic Langlands program“ in Münster ermöglichte und mir auch sonst einige Fragen beantwortet hat. Schließlich geht mein Dank an die gesamte Arbeitsgruppe „Algebraische Zahlentheorie und Algebraische Geometrie“ am KIT für das einzigartige Umfeld.

Karlsruhe, den 22. Mai 2013 Michael Fütterer

Notationen und Konventionen

Es bezeichnen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$, $\mathbb{Q}_p$ jeweils die natürlichen, ganzen, rationalen, reellen, komplexen, p-adischen ganzen und p-adischen rationalen Zahlen. Die natürlichen Zahlen beginnen bei 1. Mit $\mathbb{C}_p$ bezeichnen wir die Vervollständigung eines algebraischen Abschlusses von $\mathbb{Q}_p$, was ein algebraisch abgeschlossener Körper ist, der algebraisch (aber nicht topologisch) isomorph zu $\mathbb{C}$ ist [Was82, §5.1].

Alle Ringe haben eine 1 und Ringhomomorphismen seien stets unitär. Der Buchstabe p steht, wenn er ohne weitere Erläuterung verwendet wird, stets für eine beliebige Primzahl. Mit ϕ bezeichnen wir ausschließlich die Eulersche ϕ-Funktion.

Ein Zahlkörper ist eine endliche Erweiterung von $\mathbb{Q}$. Wenn S eine endliche Menge von Primstellen eines solchen Zahlkörpers K ist, bezeichnen wir mit K^S die maximale außerhalb von S unverzweigte Erweiterung von K. Mit $\mathbb{A}_K$ bezeichnen wir den Adelring von K und mit I_K seine Idelgruppe. Wenn v eine archimedische Stelle eines Zahlkörpers K ist und w eine Fortsetzung auf eine Erweiterung L, definieren wir die Zerlegungsgruppe von w wie üblich als die Stabilisatorgruppe von w in $\mathrm{Gal}(L|K)$ und die Trägheitsgruppe als identisch mit der Zerlegungsgruppe. Dadurch sehen wir v in der Erweiterung $L|K$ als verzweigt an, wenn v in K eine reelle Stelle ist, es aber in L eine Fortsetzung zu einer komplexen Stelle w gibt.

Für einen Körper K bezeichnen wir mit $\mu(K)$ die Gruppe der Einheitswurzeln in K, also die Torsionsgruppe von $K^\times$. Für eine natürliche Zahl n bezeichnen wir mit $\mu_n(K)$ die Untergruppe der n-ten Einheitswurzeln und mit $\mu_{n^\infty}(K)$ die Gruppe der Einheitswurzeln, deren Ordnung eine Potenz von n ist. Wenn klar ist, welcher Körper gemeint ist, lassen wir diesen auch weg.

Für jede Primzahl p bezeichnen wir mit $|\cdot|_p$ den p-adischen Betrag auf $\mathbb{Q}_p$, den wir stets als durch $|p|_p = p^{-1}$ normiert voraussetzen. Wenn K eine endliche Erweiterung von $\mathbb{Q}_p$ mit Ganzheitsring $\mathcal{O}$ ist, so heißt die Inklusion

$$\omega_K \colon \mu(K) \hookrightarrow \mathcal{O}^\times$$

der *Teichmüller-Charakter* für K. Mitunter bezeichnen wir diesen auch mit $\omega_\mathcal{O}$ oder einfach nur mit ω.

Für den Ring der quadratischen Matrizen von Dimension $n \in \mathbb{N}$ mit Koeffizienten in einem Ring R schreiben wir $\mathrm{M}_n(R)$, und $\mathrm{GL}_n(R)$ sei seine Einheitengruppe. Wenn in einer Matrix eine Stelle freigelassen wird, so steht dies für eine 0, während ein $*$ für einen beliebigen Eintrag steht. Für einen geordneten kommutativen Ring R (z.B. einen Teilring von $\mathbb{R}$) bezeichnen wir mit $\mathrm{GL}_n^+(R)$ die Untergruppe von $\mathrm{GL}_n(R)$ der Matrizen mit positiver Determinante.

Statt „projektiver Limes“ sagen wir meistens „Limes“ und statt „induktiver Limes“ sagen wir „Kolimes“. Wir schreiben hierfür lim und colim.

Ein kompakter topologischer Raum muss nicht notwendig hausdorffsch sein.

Wenn G eine (möglicherweise topologische) Gruppe ist, bezeichnen wir mit G^{ab} die Abelisierung von G. Damit meinen wir den Quotienten von G nach dem kleinsten Normalteiler, der alle Kommutatoren enthält, und im Falle einer topologischen Gruppe abgeschlossen ist. Wenn R ein kommutativer Ring ist, schreiben wir $\operatorname{Quot} R$ für den totalen Quotientenring von R, d.h. die Lokalisierung von R nach der Menge aller Nichtnullteiler (da Nullteiler keine Einheiten sein können, ist das die größtmögliche Lokalisierung). Wenn R nullteilerfrei ist, bezeichnet also $\operatorname{Quot} R$ seinen Quotientenkörper.

Wir benutzen die folgenden Kategorien:

$\mathcal{Set}$	Kategorie der Mengen
$\mathcal{Top}$	Kategorie der topologischen Räume
$\mathcal{Grp}$	Kategorie der Gruppen
$\mathcal{Ab}$	Kategorie der abelschen Gruppen
$\mathcal{Ring}$	Kategorie der Ringe
$\mathcal{Mod}(R)$	Kategorie der Moduln über einem Ring R; stetige R-Moduln, falls R ein topologischer Ring ist
$\mathcal{Alg}(R)$	Kategorie der R-Algebren für einen Ring R; stetige R-Algebren, falls R ein topologischer Ring ist
$\mathcal{Mod}(G)$	Kategorie der abelschen Gruppen mit Operation einer Gruppe G (stetig, falls G eine topologische Gruppe ist)
$\mathcal{Func}(\mathcal{C}, \mathcal{D})$	Kategorie von Funktoren zwischen zwei Kategorien $\mathcal{C}$ und $\mathcal{D}$

Wenn wir einer dieser Kategorien ein „$\mathcal{Fin}$“ voranstellen, meinen wir damit die volle Unterkategorie, deren Objekte endlich sind, soweit dies sinnvoll ist. So bezeichnet z.B. $\mathcal{FinGrp}$ die Kategorie der endlichen Gruppen.

Inhaltsverzeichnis

I. Algebraische Grundlagen

Wir beginnen, indem wir verschiedene Grundlagen bereitstellen, die wir in den späteren Kapiteln benötigen werden. Die einzelnen Abschnitte dieses Kapitels hängen meist nur lose zusammen.

1. Proendliches

Eine proendliche Gruppe ist bekanntlich eine Gruppe, die (projektiver) Limes von endlichen Gruppen ist. Eine analoge Definition kann man für topologische Räume, Ringe etc. machen. All dies sind jedoch Spezialfälle einer allgemeinen Konstruktion, die wir zu Beginn erklären wollen, um alle diese Definitionen unter einem gemeinsamen Dach zu versammeln.

Es sei dazu zunächst eine proendliche Gruppe G gegeben, die wir als Limes

$$G = \lim_{i \in I} G_i$$

von endlichen Gruppen G_i schreiben, wobei i eine gerichtet geordnete Menge $(I, \leq)$ durchläuft. Hierbei vereinbaren wir die Konvention, dass die Morphismen stets *vom größeren zum kleineren* gehen, d.h. für $i, j \in I$ mit $i \leq j$ gebe es ein zugehöriges $f_{ij} \colon G_j \longrightarrow G_i$. Die Zuordnung

$$i \longmapsto G_i, \quad (i \leq j) \longmapsto f_{ij}$$

können wir als Funktor $I \longrightarrow \mathcal{FinGrp}$ sehen, wenn wir I als (kleine) Ordnungskategorie[1] auffassen. Jeder Funktor von einer kleinen gerichteten Ordnungskategorie in die Kategorie der endlichen Gruppen definiert auf diese Weise eine proendliche Gruppe, und umgekehrt kann jede proendliche Gruppe durch einen solchen Funktor beschrieben werden (der jedoch nicht eindeutig ist).

Wir nehmen uns nun eine weitere proendliche Gruppe

$$H = \lim_{j \in J} H_j$$

und betrachten einen stetigen Gruppenhomomorphismus $\varphi \colon G \longrightarrow H$. Durch Verkettung mit den Projektionen $\pi_j \colon H \longrightarrow H_j$ bekommen wir aus φ eine Familie von stetigen Homomorphismen

$$(\varphi_j \colon G \longrightarrow H_j)_{j \in J} \in \prod_{j \in J} \operatorname{Hom}(G, H_j),$$

[1] Die Eigenschaft, dass die geordnete Menge I *gerichtet geordnet* ist, wird für die zugehörige Ordnungskategorie in der Literatur meist als „filternd“ (engl. „filtrant“) bezeichnet. Wir nennen solche Kategorien hier einfach *gerichtete Ordnungskategorien.*

die mit den Abbildungen $H_j \longrightarrow H_{j'}$ für $j' \leq j$ verträglich ist. Wegen der universellen Abbildungseigenschaft von H liefert umgekehrt jede solche Familie einen stetigen Homomorphismus $G \longrightarrow H$. Deshalb ist

$$\mathrm{Hom}(G, H) \longrightarrow \lim_j \mathrm{Hom}(G, H_j), \quad \varphi \longmapsto (\varphi_j = \pi_j \circ \varphi)_j$$

eine Bijektion.

Sei nun j fest und $\varphi_j \colon G \longrightarrow H_j$ ein Homomorphismus. Da die Topologie auf H_j diskret ist, ist der Kern von φ_j offen in G. Er muss also einen offenen Normalteiler N enthalten, sodass $G/N = G_i$ für ein i gilt, und der induzierte Homomorphismus $\varphi_{ij} \colon G_i \longrightarrow H_j$ legt φ_j bereits fest. Das i ist natürlich nicht eindeutig bestimmt, alle $i' \in I$ mit $i' \geq i$ haben ebenfalls diese Eigenschaft. Wir können aber eine Abbildung

$$\mathrm{Hom}(G, H_j) \longrightarrow \coprod_{i \in I} \mathrm{Hom}(G_i, H_j) \Big/ \sim, \quad \varphi_j \longmapsto [\varphi_{ij}]$$

definieren, wobei wir auf der rechten Seite zwei Homomorphismen $G_i \longrightarrow H_j$ und $G_{i'} \longrightarrow H_j$ identifizieren, wenn $i' \geq i$ und die Morphismen mit der Abbildung $G_{i'} \longrightarrow G_i$ verträglich sind (genauer teilen wir die durch diese Bedingungen erzeugte Äquivalenzrelation heraus). Diese Abbildung ist wieder eine Bijektion. Auf der rechten Seite steht nun der Kolimes der $\mathrm{Hom}(G_i, H_j)$. Wir haben also gezeigt:

Lemma 1.1: *Es gibt eine kanonische Bijektion*

$$\mathrm{Hom}(G, H) \xrightarrow{\sim} \lim_{j \in J} \operatorname*{colim}_{i \in I} \mathrm{Hom}(G_i, H_j).$$

Dies nehmen wir zum Anlass für die folgende Definition.

Definition 1.2: Sei C eine beliebige Kategorie. Wir definieren eine Kategorie $\mathcal{Pro}(C)$, die wir die *pro-Kategorie zu C* nennen, wie folgt: Objekte seien Funktoren $\mathcal{F} : I \longrightarrow C$ von kleinen gerichteten Ordnungskategorien nach C, und

$$\mathrm{Hom}_{\mathcal{Pro}(C)}(\mathcal{F}, \mathcal{G}) = \lim_{j \in J} \operatorname*{colim}_{i \in I} \mathrm{Hom}_C(\mathcal{F}(i), \mathcal{G}(j)).$$

Man hat für jede Kategorie C einen kanonischen Funktor

$$\iota_C : C \longrightarrow \mathcal{Pro}(C)$$

in die zugehörige pro-Kategorie. Dieser ist durch

$$\iota_C(X) \colon \{\bullet\} \longrightarrow C, \quad \bullet \longmapsto X, \quad \mathrm{id}_\bullet \longmapsto \mathrm{id}_X$$

für $X \in C$ gegeben, wobei $\{\bullet\}$ die terminale Kategorie bezeichnet (ι_C soll das Naheliegende mit Morphismen tun). Man sieht sofort, dass dieser volltreu ist, und wir demnach jede Kategorie als Unterkategorie ihrer pro-Kategorie auffassen können.

Wir wollen ein paar abstrakte Aussagen über pro-Kategorien zusammenstellen, die später nützlich sein werden. Dazu sei stets C eine beliebige Kategorie.

Lemma 1.3: *In $\mathcal{P}ro(C)$ gibt es kleine gerichtete Limiten.*

Beweis: [KS06], Thm. 6.1.8 und Bemerkung danach. □

Lemma 1.4: *Es sei $\mathcal{F} : I \longrightarrow C$ ein Objekt in $\mathcal{P}ro(C)$. Dann gilt in $\mathcal{P}ro(C)$*

$$\mathcal{F} \cong \lim_{i \in I} \iota_C(\mathcal{F}(i)).$$

Beweis: Nach Lemma 1.3 existiert der Limes auf der rechten Seite in $\mathcal{P}ro(C)$. Wir betrachten für ein $i \in I$

$$\mathrm{Hom}_{\mathcal{P}ro(C)}(\mathcal{F}, \iota_C(\mathcal{F}(i))) = \operatorname*{colim}_{j \in I} \mathrm{Hom}_C(\mathcal{F}(j), \mathcal{F}(i)).$$

Die Identität auf $\mathcal{F}(i)$ liefert ein Element der obigen Morphismenmenge, das wir mit π_i bezeichnen. Um die Behauptung zu zeigen, genügt der Nachweis, dass $\mathcal{F}$ zusammen mit den $\pi_i : \mathcal{F} \longrightarrow \iota_C(\mathcal{F}(i))$ die universelle Eigenschaft des Limes' $\lim_i \iota_C(\mathcal{F}(i))$ erfüllt. Dies ist eine einfache Rechnung und soll hier nicht ausgeführt werden. □

Lemma 1.5: *Es seien I und J kleine gerichtete Ordnungskategorien. Dann ist auch ihr Produkt wieder eine solche. Es sei ein Bifunktor $\mathcal{F} : I \times J \longrightarrow C$ gegeben. Dieser induziert Funktoren $\mathcal{F}_I : I \longrightarrow \mathcal{F}unc(J, C)$ und $\mathcal{F}_J : J \longrightarrow \mathcal{F}unc(I, C)$, die als Funktoren mit Werten in $\mathcal{P}ro(C)$ aufgefasst werden können. Es gilt dann in $\mathcal{P}ro(C)$*

$$\lim_{i \in I} F_I(i) \cong \lim_{j \in J} F_J(j).$$

Beweis: Die erste Aussage ist [KS06, Prop. 3.2.1 (iii)]. Für die zweite Aussage verwenden wir [KS06, Prop. 2.1.7]. Für die Kategorie, die dort C heißt, setzen wir $\mathcal{P}ro(C)$ ein, was nach Lemma 1.3 die Voraussetzung dort erfüllt. Wir setzen dort $\alpha = \iota_C \circ \mathcal{F}$ und erhalten dann die Behauptung zusammen mit Lemma 1.4. □

Bemerkung 1.6: Wir bleiben in der Situation von Lemma 1.5. Dass die Zuordnung $\mathcal{F} : I \times J \longrightarrow C$ ein Bifunktor ist, ist dazu äquivalent, dass F_I und F_J jeweils Funktoren sind und außerdem für alle $i' \leq i$ in I und $j' \leq j$ in J das Diagramm

$$\begin{tikzcd}
F(i,j) \arrow[r] \arrow[d] & F(i,j') \arrow[d] \\
F(i',j) \arrow[r] & F(i',j')
\end{tikzcd}$$

kommutiert [KS06, S. 17].

Definition 1.7: Die pro-Kategorien der Kategorien der endlichen diskreten topologischen Räume, der endlichen Gruppen, der endlichen Ringe heißen jeweils die Kategorien der *proendlichen Räume*, *proendlichen Gruppen*, *proendlichen Ringe*. Wir bezeichnen sie mit $\mathcal{P}rf\mathcal{T}op$, $\mathcal{P}rf\mathcal{G}rp$, $\mathcal{P}rf\mathcal{R}ing$. Entsprechend sei die Kategorie $\mathcal{P}rf\mathcal{A}lg(R)$ der proendlichen R-Algebren über einem proendlichen Ring R definiert.

Genau genommen ist eine proendliche Gruppe nach dieser Definition also ein gerichtetes System von endlichen Gruppen. Der Funktor lim von der Kategorie der proendlichen Gruppen in die Kategorie der topologischen Gruppen, der ein solches System auf seinen Limes abbildet (der hier zum Glück stets existiert!), ist nach den obigen Überlegungen volltreu und definiert somit eine Äquivalenz von Kategorien auf sein Bild. In diesem Sinne können wir die Kategorie der proendlichen Gruppen als Unterkategorie der topologischen Gruppen sehen, sodass eine proendliche Gruppe auch wirklich eine Gruppe ist.[2] Analog stellen wir uns auch die anderen pro-Kategorien vor, wenn ein geeigneter Limes-Funktor existiert (was für alle bisher genannten Beispiele der Fall ist).

Die proendlichen Räume, Gruppen und Ringe können folgendermaßen charakterisiert werden:

Satz 1.8: *(a) Sei X ein topologischer Raum. Dann sind äquivalent:*

(i) X ist ein proendlicher Raum.

(ii) X ist kompakt, hausdorffsch und total unzusammenhängend.

(iii) X ist kompakt, hausdorffsch und jeder Punkt hat eine Umgebungsbasis aus Mengen, die zugleich offen und abgeschlossen sind.

(b) Sei G eine topologische Gruppe. Dann sind äquivalent:

(i) G ist eine proendliche Gruppe.

(ii) G ist kompakt, hausdorffsch und total unzusammenhängend.

(iii) G ist kompakt, hausdorffsch und das Neutralelement hat eine Umgebungsbasis aus offenen Normalteilern.

(c) Sei R ein topologischer Ring. Dann sind äquivalent:

(i) R ist ein proendlicher Ring.

(ii) R ist kompakt und hausdorffsch.

(iii) R ist kompakt, hausdorffsch und total unzusammenhängend.

(iv) R ist kompakt, hausdorffsch und die 0 hat eine Umgebungsbasis aus offenen Idealen.

Beweis: [RZ00, Thm. 1.1.12, Thm. 2.1.3 und Prop. 5.1.2] □

Beispiel 1.9: Jede Galoisgruppe ist, mit der Krulltopologie versehen, eine proendliche Gruppe. Umgekehrt taucht auch jede proendliche Gruppe als Galoisgruppe einer Körpererweiterung auf (sogar in beliebiger Charakteristik); siehe dazu [RZ00, Thm. 2.11.5].

Eine Untergruppe einer proendlichen Gruppe ist genau dann wieder proendlich, wenn sie abgeschlossen ist. Der Raum der Nebenklassen modulo einer Untergruppe ist auch genau dann proendlich, wenn die Untergruppe abgeschlossen ist, und insbesondere ist eine Faktorgruppe nach einem Normalteiler genau dann proendlich, wenn dieser abgeschlossen ist. Deshalb werden wir in der Regel nur abgeschlossene Untergruppen von proendlichen Gruppen betrachten.

[2] Wenn man ganz genau sein will, sollte man sich die Kategorie der proendlichen Gruppen als den Isomorphieabschluss des Bildes des Limes-Funktors in der Kategorie der topologischen Gruppen vorstellen, d.h. man nimmt zu diesem Bild noch alle isomorphen topologischen Gruppen hinzu.

Definition 1.10: Es sei $\mathcal{C}$ eine Klasse endlicher Gruppen.[3] Eine proendliche Gruppe heißt *pro-$\mathcal{C}$-Gruppe*, wenn sie Limes von Gruppen aus $\mathcal{C}$ ist. Die pro-$\mathcal{C}$-Gruppen bilden eine Kategorie, die wir mit $\mathcal{P}\mathit{rfGrp}_{\mathcal{C}}$ bezeichnen.

Wichtige Beispiele für $\mathcal{C}$ sind die Klassen aller endlichen zyklischen Gruppen und aller p-Gruppen, in welchen Fällen man von *prozyklischen Gruppen* bzw. *pro-p-Gruppen* spricht.

Wir wollen nun für pro-$\mathcal{C}$-Gruppen ein Analogon zu den freien Gruppen aus der abstrakten Gruppentheorie definieren. Dort werden die freien Gruppen dadurch beschrieben, dass man zu dem Vergissfunktor $V\colon \mathcal{G}\mathit{rp} \longrightarrow \mathcal{S}\mathit{et}$ von der Kategorie der Gruppen in die Kategorie der Mengen einen linksadjungierten Funktor $F\colon \mathcal{S}\mathit{et} \longrightarrow \mathcal{G}\mathit{rp}$ hat, der eine Menge auf die von ihr erzeugte freie Gruppe abbildet. Dies bauen wir nun in der proendlichen Welt nach.

Definition 1.11: Sei $V\colon \mathcal{P}\mathit{rfGrp}_{\mathcal{C}} \longrightarrow \mathcal{P}\mathit{rfTop}$ der Vergissfunktor, der eine pro-$\mathcal{C}$-Gruppe auf den zugrundeliegenden proendlichen Raum schickt. Wenn es einen zu V linksadjungierten Funktor $F\colon \mathcal{P}\mathit{rfTop} \longrightarrow \mathcal{P}\mathit{rfGrp}_{\mathcal{C}}$ gibt, so heißt $F(X)$ für einen proendlichen Raum X die *freie pro-$\mathcal{C}$-Gruppe über X*.

Satz 1.12: *Der zu V linksadjungierte Funktor F existiert.*[4]

Beweisskizze: Es sei ein proendlicher Raum X gegeben. Wir müssen also eine pro-$\mathcal{C}$-Gruppe $F(X)$ zusammen mit einer stetigen Abbildung $\iota\colon X \longrightarrow F(X)$ angeben, sodass es für jede weitere stetige Abbildung $f\colon X \longrightarrow G$ in eine pro-$\mathcal{C}$-Gruppe G genau eine Fortsetzung $\varphi\colon F(X) \longrightarrow G$ gibt, mit der das Diagramm

$$\begin{tikzcd} F(X) \arrow[r, dashed, "\varphi"] & G \\ X \arrow[u, "\iota"] \arrow[ur, "f"'] & \end{tikzcd}$$

kommutiert. Wir geben hier nur kurz an, wie $F(X)$ konstruiert wird, die Details finden sich in [RZ00, Prop. 3.3.2].

Sei dazu D die abstrakte freie Gruppe mit Basis X und

$$\mathcal{N} = \{N \subseteq D \mid N \text{ normale Untergruppe}, \ D/N \in \mathcal{C},\ \forall d \in D\colon X \cap dN \text{ offen in } X\}.$$

Wir setzen

$$F(X) = \lim_{N \in \mathcal{N}} D/N$$

und definieren ι als die Komposition $X \hookrightarrow D \longrightarrow F$. Dieses $F(X)$ hat dann die gewünschte universelle Eigenschaft. □

[3] $\mathcal{C}$ enthalte für ein $G \in \mathcal{C}$ stets auch alle zu G isomorphen Gruppen.

[4] Hier müssen noch einige technische Anforderungen an $\mathcal{C}$ gefordert werden, z.B. Abgeschlossenheit unter Quotientenbildung, Untergruppenbildung, etc. Für die Details verweisen wir auf [RZ00, §3.3]. Bei uns werden diese Bedingungen immer erfüllt sein.

Beispiel 1.13: Eine endliche Menge mit n Elementen ist auch ein proendlicher Raum. Die zugehörige freie pro-$\mathcal{C}$-Gruppe heißt die *freie pro-$\mathcal{C}$-Gruppe von Rang n*. Die freie proendliche Gruppe von Rang 1 ist $\widehat{\mathbb{Z}}$. Die freie pro-p-Gruppe von Rang 1 ist $\mathbb{Z}_p$. Dies sieht man direkt an der Konstruktion, die im Beweis von Satz 1.12 angegeben ist.

Wenn G irgendeine (multiplikativ geschriebene) pro-$\mathcal{C}$-Gruppe ist und Z die freie pro-$\mathcal{C}$-Gruppe von Rang 1, deren erzeugendes Element wir mit 1 bezeichnen, dann gibt es für jedes $g \in G$ genau einen Homomorphismus $\varphi\colon Z \longrightarrow G$ mit $\varphi(1) = g$. Wir setzen dann

$$g^z = \varphi(z)$$

für $z \in Z$ und können auf diese Weise Elemente von G mit Elementen aus Z potenzieren. Hierbei gilt $g^{zw} = g^z g^w$ für $z, w \in Z$. Wenn G eine abelsche Gruppe ist, so gilt außerdem $(gh)^z = g^z h^z$ für $g, h \in G$. Im Falle aller proendlichen Gruppen bzw. der pro-p-Gruppen gilt $Z = \widehat{\mathbb{Z}}$ bzw. $Z = \mathbb{Z}_p$, was sogar Ringe sind. Dadurch wird auf G eine Z-Modul-Struktur definiert. Wir haben also gezeigt:

Satz 1.14: *Jede proendliche abelsche Gruppe ist auf eindeutige Weise ein $\widehat{\mathbb{Z}}$-Modul. Jede abelsche pro-p-Gruppe ist auf eindeutige Weise ein $\mathbb{Z}_p$-Modul.*

Wir wollen nun noch eine weitere Konstruktion aus der abstrakten Algebra in die proendliche Welt übertragen, nämlich die des Gruppenrings. Wenn R ein kommutativer Ring ist und G eine Gruppe, dann erfüllt der Gruppenring $R[G]$ die folgende universelle Eigenschaft: für jede R-Algebra A und jeden Gruppenhomomorphismus $G \longrightarrow A^\times$ gibt es genau eine Fortsetzung zu einem R-Algebren-Homomorphismus $R[G] \longrightarrow A$. Anders ausgedrückt: der Funktor $R[\cdot]\colon \mathcal{G}rp \longrightarrow \mathcal{A}lg(R)$ ist linksadjungiert zum Einheitengruppenfunktor $(\cdot)^\times\colon \mathcal{A}lg(R) \longrightarrow \mathcal{G}rp$.

Definition 1.15: Sei R ein proendlicher Ring und $U\colon \mathcal{P}rf\mathcal{A}lg(R) \longrightarrow \mathcal{P}rf\mathcal{G}rp$ der Funktor, der einer proendlichen R-Algebra ihre Einheitengruppe zuordnet.[5] Wenn dieser einen linksadjungierten Funktor $F\colon \mathcal{P}rf\mathcal{G}rp \longrightarrow \mathcal{P}rf\mathcal{A}lg(R)$ hat, so heißt $F(G)$ die *proendliche Gruppenalgebra* (oder der *proendliche Gruppenring*) zu einer proendlichen Gruppe G. Statt $F(G)$ schreiben wir $R[\![G]\!]$.

Der proendliche Gruppenring existiert ebenfalls immer:

Satz 1.16: *Die proendliche R-Algebra*

$$R[\![G]\!] = \varprojlim_N R[G/N]$$

erfüllt die in Definition 1.15 geforderte universelle Eigenschaft. Hierbei durchlaufe N alle offenen Normalteiler in G.

[5] Für beliebige topologische Ringe R definiert die Zuordnung $R \longmapsto R^\times$ *keinen* Funktor in die Kategorie der topologischen Gruppen, da die Inversion nicht stetig sein muss! Für einen proendlichen Ring $R = \varprojlim R_i$ gilt aber $R^\times = \varprojlim R_i^\times$, sodass dieser Funktor wohldefiniert ist.

Beweis: Man beachte zunächst, dass dieser Limes wegen Lemma 1.3 in der Kategorie der proendlichen R-Algebren existiert. Um zu zeigen, dass dieser Ring die gewünschte universelle Eigenschaft erfüllt, sei eine proendliche R-Algebra A und ein Gruppenhomomorphismus $G \longrightarrow A^\times$ gegeben. Wir schreiben A als Limes

$$A = \varprojlim_i A_i$$

endlicher R-Algebren. Wegen der universellen Eigenschaft von A genügt es, für jedes i einen stetigen Homomorphismus $R[\![G]\!] \longrightarrow A_i$ anzugeben, sodass diese alle kompatibel sind. Wir betrachten für ein festes i die Komposition

$$G \longrightarrow A^\times \longrightarrow A_i^\times.$$

Da A_i endlich ist, faktorisiert diese über G/N für einen offenen Normalteiler N von G, und die universelle Eigenschaft des abstrakten Gruppenrings liefert dann einen R-Algebren-Homomorphismus $R[G/N] \longrightarrow A_i$. Indem wir diesem die Projektion $R[\![G]\!] \longrightarrow R[G/N]$ vorschalten, erhalten wir auf diese Weise für jedes i Homomorphismen

$$R[\![G]\!] \longrightarrow A_i,$$

und es ist leicht zu verifizieren, dass diese kompatibel sind. Dies zeigt die Behauptung. □

Wenn $R = \mathcal{O}$ der Ganzheitsring in einer endlichen Erweiterung von $\mathbb{Q}_p$ ist, dann nennt man den proendlichen Gruppenring $\mathcal{O}[\![G]\!]$ mitunter auch die *Iwasawa-Algebra* von G.

Wir haben eine kanonische Abbildung von G in diesen proendlichen Gruppenring, die durch

$$G \longrightarrow R[\![G]\!]^\times, \quad g \longmapsto (gN)_N$$

gegeben ist. Wir schreiben für das Bild eines $g \in G$ unter dieser Abbildung meistens auch wieder g. Auf diese Weise kann der „normale" Gruppenring $R[G]$ nach $R[\![G]\!]$ eingebettet werden und liegt dort dann dicht [RZ00, Lem. 5.3.5 (c)]. Schließlich erhält man genau wie in der abstrakten Algebra:

Satz 1.17: *Wenn M ein proendlicher R-Modul ist und eine proendliche Gruppe G stetig auf M operiert, sodass diese Operation verträglich mit der R-Modul-Struktur ist, dann ist M auf eindeutige Weise ein $R[\![G]\!]$-Modul.*

Beweis: [RZ00, Prop. 5.3.6 (d)] □

Mitunter betrachen wir auch für nicht-proendliche Ringe R (etwa $R = \mathbb{Q}_p$) und eine proendliche Gruppe den Ring

$$R[\![G]\!] = \varprojlim_N R[G/N].$$

2. Iwasawa-Moduln

In der Zahlentheorie treten oft in natürlicher Weise Galois-Moduln auf, d.h. abelsche Gruppen, auf denen eine Galoisgruppe G operiert. Eine solche abelsche Gruppe kann dann, wenn sie proendlich oder diskret ist, als Modul über dem proendlichen Gruppenring $\widehat{\mathbb{Z}}[\![G]\!]$ aufgefasst werden, bzw. über $\mathbb{Z}_p[\![G]\!]$, wenn sie eine pro-p-Gruppe ist (vgl. Sätze 1.14 und 1.17). Daher kommt dem Studium von $\mathbb{Z}_p[\![G]\!]$-Moduln eine besondere Bedeutung zu. Für solche Moduln gibt es in gewissen Fällen eine schöne Strukturtheorie, die im Folgenden kurz zusammengefasst werden soll.

2.1. Vorbemerkungen

In diesem Abschnitt sei p eine Primzahl, $m \in \mathbb{N}$ zu p teilerfremd und R ein kommutativer nullteilerfreier Ring mit Quotientenkörper K und separablem Abschluss $\overline{K}$.

Sei zunächst G eine beliebige Gruppe. Für einen Modul M über dem Gruppenring $R[G]$ und einen Charakter $\chi\colon G \longrightarrow R^\times$ betrachten wir den Untermodul

$$M_\chi = \{m \in M \mid \forall g \in G\colon g \cdot m = \chi(g)m\}, \tag{2.1}$$

welchen wir den *Eigenraum zu* χ nennen. Dann haben wir einen kanonischen Morphismus

$$\bigoplus_\chi M_\chi \longrightarrow M, \tag{2.2}$$

wobei in der Summe χ alle Charaktere von G durchläuft. Wenn G endlich ist, R die Werte aller Charaktere $\chi\colon G \longrightarrow \overline{K}^\times$ enthält und die Gruppenordnung von G in R invertierbar ist, ist dies ein Isomorphismus [Was82, S. 100]. Die Projektion von M auf M_χ kann in diesem Fall durch

$$M \longrightarrow M_\chi, \quad m \longmapsto \varepsilon_\chi m$$

mit

$$\varepsilon_\chi = \frac{1}{\#G} \sum_{g \in G} \chi(g) g^{-1} \in R[G]$$

ausgedrückt werden. Man rechnet leicht nach, dass

$$\varepsilon_\chi g = \chi(g) \varepsilon_\chi \tag{2.3}$$

für alle $g \in G$ gilt.

Definition 2.1: Wir setzen

$$\mathbb{Z}_{p,m} = \lim_{r \in \mathbb{N}} \mathbb{Z}/mp^r\mathbb{Z}\,.$$

Lemma 2.2: *Es gilt kanonisch*

$$\mathbb{Z}_{p,m}^\times \cong \Delta \times \Gamma$$

mit $\Gamma = 1 + p\mathbb{Z}_p$ *und* $\Delta = (\mathbb{Z}/mp\mathbb{Z})^\times$ *für* $p \neq 2$ *und* $\Delta = (\mathbb{Z}/4m\mathbb{Z})^\times$ *für* $p = 2$.

Beweis: Wir zeigen die Aussage nur im Fall $p \neq 2$, der andere Fall geht ähnlich. Sei $n \in \mathbb{N}$. Die kanonische Abbildung

$$1 + p\mathbb{Z}_p \hookrightarrow \mathbb{Z}_p^\times \twoheadrightarrow \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times$$

induziert eine exakte Sequenz

$$1 \longrightarrow \frac{1 + p\mathbb{Z}_p}{1 + p^n\mathbb{Z}_p} \longrightarrow \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times \longrightarrow \left(\mathbb{Z}/p\mathbb{Z}\right)^\times \longrightarrow 1.$$

Diese Sequenz spaltet, denn

$$\left(\mathbb{Z}/p\mathbb{Z}\right)^\times \longrightarrow \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times, \quad a \longmapsto a^{p^{n-1}}$$

ist ein Schnitt für die rechte Abbildung. Zusammen mit dem chinesischen Restsatz liefert das

$$\left(\mathbb{Z}/mp^n\mathbb{Z}\right)^\times \cong \left(\mathbb{Z}/mp\mathbb{Z}\right)^\times \times \frac{1+p\mathbb{Z}_p}{1+p^n\mathbb{Z}_p}. \tag{2.4}$$

Nimmt man hierüber den Limes, folgt die Behauptung. □

Insbesondere erhalten wir Zerlegungen

$$\mathbb{Z}_{p,m}^\times \cong \left(\mathbb{Z}/mp\mathbb{Z}\right)^\times \times \Gamma \cong \left(\mathbb{Z}/m\mathbb{Z}\right)^\times \times \mathbb{Z}_p^\times.$$

Die Gruppe Γ ist zur additiven Gruppe von $\mathbb{Z}_p$ isomorph [Neu07, Kap. II, (5.5)].

Es sei nun $G = \Delta \times \Gamma$ mit Gruppen Γ und Δ, die jeweils (nichtkanonisch) zu $\mathbb{Z}_p$ bzw. einem Quotienten von $(\mathbb{Z}/mp\mathbb{Z})^\times$ isomorph sind (ein Beispiel für ein solches G ist $\mathbb{Z}_{p,m}^\times$). Weiter nehmen wir ab jetzt an, dass R die Werte aller Charaktere von Δ enthält und die Gruppenordnung von Δ in R invertierbar ist. Indem wir $R[\![G]\!]$ als Modul über $R[\Delta]$ auffassen, bekommen wir wie in (2.2) eine Zerlegung

$$R[\![G]\!] = \bigoplus_\delta R[\![G]\!]_\delta$$

in der δ über alle Charaktere von Δ läuft.

Lemma 2.3: *Jeder der Summanden $R[\![G]\!]_\delta$ ist als R-Modul kanonisch zu $R[\![\Gamma]\!]$ isomorph.*

Beweis: Es sei ε_δ wie in (2.3) definiert. Dann gilt $R[\![G]\!]_\delta = \varepsilon_\delta R[\![G]\!]$. Es sei $\Gamma_n = (1 + p\mathbb{Z}_p)/(1 + p^n\mathbb{Z}_p)$ und $G_n = \Delta \times \Gamma_n$. Wir konstruieren einen Isomorphismus $\varepsilon_\delta R[G_n] \cong R[\Gamma_n]$, die Behauptung folgt dann wieder über den Limes.

Sei dazu nun n fest. Für ein $g = (a, \gamma) \in G_n = \Delta \times \Gamma_n$ ist $\varepsilon_\delta g = \delta(a)\gamma\varepsilon_\delta$ nach (2.3). Durch R-lineare Fortsetzung von

$$\varepsilon_\delta g \longmapsto \delta(a)\gamma$$

erhält man einen R-Modul-Homomorphismus $\varepsilon_\delta R[G_n] \longrightarrow R[\Gamma_n]$. Andererseits erhält man durch R-lineare Fortsetzung von

$$R[\Gamma_n] \longrightarrow \varepsilon_\delta R[G_n], \quad \gamma \longmapsto \varepsilon_\delta(1,\gamma) \quad (\gamma \in \Gamma_n)$$

einen Homomorphismus in die umgekehrte Richtung, und man rechnet leicht nach, dass diese zueinander invers sind. □

2.2. Strukturtheorie

Es sei Λ ein kommutativer noetherscher ganzabgeschlossener Ring.

Definition 2.4: Ein Λ-Modul M heißt *pseudo-null*, wenn er endlich erzeugt ist und für alle Primideale $\mathfrak{p}$ von Höhe ≤ 1 gilt $M_\mathfrak{p} = 0$.

Diese Definition hat auch eine geometrische Interpretation. Sei dazu $X = \operatorname{Spec}\Lambda$ das zu Λ gehörende affine Schema. Ein endlich erzeugter Λ-Modul M definiert eine kohärente $\mathcal{O}_X$-Modulgarbe $\widetilde{M}$ auf X. Der Träger von $\widetilde{M}$ ist ein abgeschlossenes Unterschema von X. Die Bedingung, dass M pseudo-null ist, bedeutet dann gerade, dass der Träger von $\widetilde{M}$ in X mindestens Kodimension 2 hat, also in gewissem Sinne „klein“ ist.

Ein Λ-Modul-Homomorphismus $M \longrightarrow N$ heißt *Pseudo-Isomorphismus*, wenn sein Kern und sein Kokern beide pseudo-null sind. Das ist dazu äquivalent, dass für alle Primideale $\mathfrak{p}$ von Höhe ≤ 1 die induzierte Abbildung $M_\mathfrak{p} \longrightarrow N_\mathfrak{p}$ ein Isomorphismus ist. Man beachte, dass Pseudo-Isomorphie im Allgemeinen *keine* Äquivalenzrelation ist! Wenn man sich jedoch auf endlich erzeugte Λ-Torsionsmoduln einschränkt, ist es eine Äquivalenzrelation [NSW00, S. 225].

Ab jetzt nehmen wir Λ als nullteilerfrei an. Die erste wichtige Strukturaussage für Λ-Moduln ist

Satz 2.5: *Sei M ein endlich erzeugter Λ-Modul, T der Torsionsuntermodul und $F = M/T$.*

(a) Es gibt einen Pseudo-Isomorphismus $M \longrightarrow F \oplus T$.

(b) Es gibt endlich viele natürliche Zahlen $n_1, \ldots, n_t$ und Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ von Höhe 1 und einen Pseudo-Isomorphismus

$$T \longrightarrow \bigoplus_{i=1}^{t} \Lambda \big/ \mathfrak{p}_i^{n_i} \ .$$

Diese sind bis auf die Reihenfolge eindeutig bestimmt.

Beweis: [NSW00, Prop. 5.1.7] □

Man sollte sich diesen Satz als eine Analogie zum Struktursatz für Moduln über Hauptidealringen vorstellen. Tatsächlich kann er mithilfe dieses Satzes bewiesen werden.

Eine wichtige Anwendung dieses Satzes ist der Fall, dass $\Lambda = \mathcal{O}[\![T]\!]$ der Ring der formalen Potenzreihen über dem Ganzheitsring $\mathcal{O}$ einer endlichen Erweiterung K von $\mathbb{Q}_p$ ist. Λ ist dann lokal – sein maximales Ideal wird von T und dem maximalen Ideal von $\mathcal{O}$ erzeugt – und vollständig bzgl. der davon induzierten Topologie. In diesem Fall ist ein Modul über Λ genau dann pseudo-null, wenn er endlich ist [NSW00, Rem. 4 nach (5.1.4)], und der Modul F aus Satz 2.5 ist frei [NSW00, (5.1.8), (5.1.9)].

Sei also im Folgenden $\mathcal{O}$ ein solcher Ganzheitsring, $\mathfrak{m}$ sein maximales Ideal, π ein Erzeuger desselben und $\Lambda = \mathcal{O}[\![T]\!]$.

Bemerkung 2.6: Es soll an dieser Stelle bemerkt werden, dass jede Potenzreihe $f \in \mathcal{O}[\![T]\!]$ auf $\mathfrak{m}$ konvergiert. Denn die Koeffizienten $a_n \in \mathcal{O}$ eines solchen f sind alle von Betrag ≤ 1, und wenn wir für T ein Element $x \in \mathfrak{m}$ einsetzen, gilt $|a_n x^n| \leq |\pi|^{-n}$. Also ist $(a_n x^n)_n$ eine Nullfolge, was in einem ultrametrischen Raum bereits für die Konvergenz einer Reihe genügt.

Ein praktisches Hilfsmittel im Umgang mit solchen Potenzreihen ist der Weierstraßsche Vorbereitungssatz und sein Korollar.

Definition 2.7: Sei $f = \sum_{n=0}^{\infty} a_n X^n \in \mathcal{O}[\![T]\!]$. Dann heißt[6]

$$\operatorname{rld} f := \inf \{n \in \mathbb{N}_0 : a_n \notin \mathfrak{m}\} \in \mathbb{N}_0 \cup \{\infty\}$$

der *reduzierte Untergrad* von f. Ein Polynom $f \in \mathcal{O}[T]$ heißt *Weierstraß-Polynom*, wenn es normiert ist und

$$\deg f = \operatorname{rld} f$$

gilt, also genau dann, wenn es normiert ist und alle seine Koeffizienten außer dem Leitkoeffizienten in $\mathfrak{m}$ liegen.

Lemma 2.8 (Division mit Rest): *Seien $f, g \in \mathcal{O}[\![T]\!]$, und sei* $\operatorname{rld} f < \infty$. *Dann kann g eindeutig in der Form*

$$g = fq + r$$

geschrieben werden, wobei $q \in \mathcal{O}[\![T]\!]$ und $r \in \mathcal{O}[T]$ ein Polynom ist mit

$$\deg r < \operatorname{rld} f.$$

Beweis: [Was82, Prop. 7.2] □

Satz 2.9 (Weierstraßscher Vorbereitungssatz): *Es sei $f \in \mathcal{O}[\![T]\!], f \neq 0$. Dann lässt sich f in eindeutiger Weise als Produkt*

$$f = \pi^n \cdot F \cdot u$$

schreiben, wobei $u \in \mathcal{O}[\![T]\!]^\times$ eine Einheit ist und $F \in \mathcal{O}[T]$ ein Weierstraß-Polynom.

Beweis: [Was82, Thm. 7.3] □

Korollar 2.10: *Es sei $f \in \mathcal{O}[\![T]\!], f \neq 0$ eine Potenzreihe, die irgendwo konvergiert. Dann hat die dadurch dargestellte Funktion nur endlich viele Nullstellen.*

Beweis: Mit dem Weierstraßschen Vorbereitungssatz können wir f als

$$f = \pi^m \cdot F \cdot u$$

mit $F \in \mathcal{O}[T]$ und $u \in \mathcal{O}[\![T]\!]^\times$ schreiben, und die Nullstellen von f stimmen dann mit denen von F überein. Davon gibt es nur endlich viele, da F ein Polynom ist. □

Mithilfe des Weierstraßschen Vorbereitungssatzes können nun die Primideale von Höhe 1 in Λ klassifiziert werden.

Lemma 2.11: *Die Primideale von Höhe 1 in Λ sind von der Form (p) oder (F), wobei F ein irreduzibles Weierstraß-Polynom ist.*

Beweis: Das ist eine leichte Konsequenz aus dem Weierstraßschen Vorbereitungssatz 2.9, siehe [NSW00, (5.3.7)]. □

Zusammen mit dem allgemeinen Struktursatz 2.5 ergibt das vorige Lemma den folgenden Struktursatz für $\mathcal{O}[\![T]\!]$-Moduln.

---
[6] „rld“ steht für „reduced lower degree“.

Satz 2.12: *Es sei M ein endlich erzeugter Λ-Modul. Dann gibt es einen Pseudo-Isomorphismus*

$$M \longrightarrow \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda\big/p^{m_i} \oplus \bigoplus_{j=1}^{t} \Lambda\big/F_j^{n_j} \ . \tag{2.5}$$

Hierbei sind die F_j irreduzible Weierstraß-Polynome, die r, s, t, m_i, n_j natürliche Zahlen und die F_j sind bis auf Reihenfolge und Multiplikation mit Einheiten, die m_i, n_j bis auf Reihenfolge eindeutig bestimmt.

Definition 2.13: Das Ideal, das von dem Produkt

$$\prod_{i=1}^{s} p^{m_i} \prod_{j=1}^{t} F_j^{n_j}$$

erzeugt wird, ist durch M eindeutig bestimmt. Es heißt *charakteristisches Ideal* von M.

Das charakteristische Ideal ist eine wichtige Invariante eines solchen Moduls. Man kann es als ein Analogon der Gruppenordnung sehen: denn wenn A eine endliche abelsche Gruppe ist, dann gibt es einen Isomorphismus von $\mathbb{Z}$-Moduln

$$A \longrightarrow \bigoplus_{i=1}^{s} \mathbb{Z}\big/p_i^{m_i}\mathbb{Z}$$

für bis auf Reihenfolge eindeutig bestimmte Primzahlen p_i und Exponenten m_i. Das „charakteristische Ideal" von A in $\mathbb{Z}$ wäre dann $(p_1^{m_1} \cdots p_s^{m_s})$, es wird also von der Gruppenordnung erzeugt.

Bemerkung 2.14: Sei E der Λ-Modul, der in (2.5) auf der rechten Seite steht. Der Name „charakteristisches Ideal" kommt daher, dass das Polynom

$$\prod_{j=1}^{t} F_j^{n_j}$$

das charakteristische Polynom des Endomorphismus' des K-Vektorraumes $M \otimes_{\mathcal{O}} K$ ist, der von der Multiplikation mit T induziert wird, falls M ein Torsionsmodul ist (wobei K der Quotientenkörper von $\mathcal{O}$ ist). In diesem Fall gilt nämlich $r = 0$ und jeder der Summanden Λ/p^{m_i} ist bereits ein $\mathcal{O}$-Torsionsmodul, sodass

$$E \otimes_{\mathcal{O}} K \cong \bigoplus_{j=1}^{t} K \otimes_{\mathcal{O}} \Lambda\big/F_j^{n_j}$$

gilt. Sei nun $F = T^d + \sum_{k=0}^{d-1} a_k T^k$ ein Weierstraßpolynom. Dann ist $K \otimes_{\mathcal{O}} \Lambda/F$ ein d-dimensionaler K-Vektorraum mit Basis $1, T, \ldots, T^{d-1}$ und bezüglich dieser Basis hat die Multiplikation mit T die Abbildungsmatrix

$$\begin{pmatrix} & & & -a_0 \\ 1 & & & \vdots \\ & \ddots & & \vdots \\ & & 1 & -a_{d-1} \end{pmatrix},$$

deren charakteristisches Polynom F ist. Ferner sieht man leicht, dass die charakteristischen Polynome der von T induzierten Endomorphismen auf $M \otimes_{\mathcal{O}} K$ und $E \otimes_{\mathcal{O}} K$ übereinstimmen.

Im Hinblick auf arithmetische Anwendungen soll nun die Verbindung zu proendlichen Gruppenringen hergestellt werden. Sei dazu Γ eine multiplikativ geschriebene proendliche Gruppe, die (nichtkanonisch) isomorph zur additiven Gruppe $\mathbb{Z}_p$ ist. Wir wählen einen topologischen Erzeuger $\gamma \in \Gamma$. Dann gilt:

Satz 2.15 (Iwasawa-Isomorphismus): *Die Abbildung*

$$\mathcal{O}[\![T]\!] \longrightarrow \mathcal{O}[\![\Gamma]\!], \quad T \longmapsto \gamma - 1$$

ist ein Isomorphismus von proendlichen $\mathcal{O}$-Algebren.

Beweis: [NSW00, Prop. 5.3.5] □

Die Moduln über $\mathcal{O}[\![T]\!]$ sind also Moduln über einem proendlichen Gruppenring, also einer Iwasawa-Algebra, und heißen deshalb auch *Iwasawa-Moduln*. Da die Wahl eines anderen topologischen Erzeugers von Γ einen Automorphismus von Λ induziert, der insbesondere ein Pseudo-Isomorphismus ist, hängt das charakteristische Ideal eines solchen Iwasawa-Moduls nicht von der Wahl eines topologischen Erzeugers ab.

Es sei nun G von der Gestalt $G = \Delta \times \Gamma$ mit Gruppen Γ und Δ, die jeweils (nichtkanonisch) zu $\mathbb{Z}_p$ bzw. einem Quotienten von $\mathbb{F}_p^\times$ isomorph sind (hier und im folgenden ist $\mathbb{F}_p^\times$ durch $(\mathbb{Z}/4\mathbb{Z})^\times \cong \{\pm 1\}$ zu ersetzen, falls $p = 2$), und M ein endlich erzeugter Modul über $\mathcal{O}[\![G]\!]$. Wir befinden uns also in der Situation von Abschnitt 2.1 mit $m = 1$ und $R = \mathcal{O}$ (beachte, dass dann R die dortigen Voraussetzungen erfüllt!). Die Charaktergruppe von $\mathbb{F}_p^\times$ ist zyklisch und wird vom Teichmüller-Charakter ω erzeugt (vgl. Bemerkung 5.2), und die Charaktergruppe von Δ ist eine Untergruppe derer von $\mathbb{F}_p^\times$. Damit können wir

$$M = \bigoplus_i M_i,$$

und

$$\mathcal{O}[\![G]\!] = \bigoplus_i \mathcal{O}[\![G]\!]_i$$

schreiben, wobei hier i über die in dieser Untergruppe vorkommenden Potenzen von ω läuft und das Subskript i jeweils für den entsprechenden Eigenraum von ω^i steht. Da nach Lemma 2.3 jedes $\mathcal{O}[\![G]\!]_i$ zu $\mathcal{O}[\![\Gamma]\!]$ isomorph ist, können wir jedes M_i als $\mathcal{O}[\![\Gamma]\!]$-Modul auffassen und haben dann wegen Satz 2.15 den Struktursatz 2.12 zur Verfügung. Damit können wir diesen auch auf Moduln über $\Lambda(G) := \mathcal{O}[\![G]\!]$ verallgemeinern; siehe dazu auch [CS06, Thm. 7.2]:

Satz 2.16: *Es sei M ein endlich erzeugter $\Lambda(G)$-Modul. Dann gibt es einen Pseudo-Isomorphismus*

$$M \longrightarrow \Lambda(G)^r \oplus \bigoplus_{j=1}^{s} \Lambda(G)\big/f_j \,. \tag{2.6}$$

Hierbei sind die f_j Nicht-Nullteiler von $\Lambda(G)$.

Beweis: Sei $\Lambda = \mathcal{O}[\![\Gamma]\!]$. Für jedes i wie oben haben wir nach Satz 2.12 einen Pseudo-Isomorphismus

$$M_i \longrightarrow \Lambda^r \oplus \bigoplus_{j=1}^{s_i} \Lambda\big/f_{i,j} \ ,$$

wobei jedes $f_{i,j}$ wie dort entweder eine p-Potenz oder eine Potenz eines irreduziblen Weierstraß-Polynoms ist. Ohne Einschränkung nehmen wir ferner an, dass alle s_i übereinstimmen: dazu definieren wir s als das Maximum der s_i und definieren die „fehlenden" $f_{i,j}$ als 1. Dann definieren wir f_j als das Bild von

$$(f_{i,j})_i \in \bigoplus_i \Lambda \xrightarrow{\sim} \bigoplus_i \Lambda(G)_i = \Lambda(G). \qquad \square$$

Definition 2.17: Wir definieren das *charakteristische Ideal* von M als das Ideal in $\Lambda(G)$, das von dem Produkt $f_1 \cdots f_r$ erzeugt wird.

Dieses ist also gerade

$$\prod_i C_i,$$

wenn C_i das charakteristische Ideal von M_i als Λ-Modul im Sinne von Definition 2.13 bezeichnet.

3. Algebraische K-Theorie

Algebraische K-Theorie ist eine „Homologietheorie für Ringe" oder allgemeiner für gewisse Kategorien. Sie besteht aus einer Familie von Funktoren K_i für jedes $i \in \mathbb{Z}$ von der Kategorie der Ringe in die Kategorie der abelschen Gruppen, oder allgemeiner von einer Kategorie von entsprechenden Kategorien in die Kategorie der abelschen Gruppen. Wenn R und S Ringe sind, kann man zusätzlich zu den K-Gruppen $K_i(R)$ bzw. $K_i(S)$ für jeden Ringhomomorphismus $R \longrightarrow S$ eine relative K-Gruppe $K_i(R,S)$ definieren, und man hat zwischen diesen K-Gruppen eine lange exakte Sequenz

$$\cdots \longrightarrow K_{i+1}(R,S) \longrightarrow K_{i+1}(R) \longrightarrow K_{i+1}(S) \longrightarrow K_i(R,S) \longrightarrow \cdots .$$

Wir wollen hier nicht erklären, wie diese K-Gruppen im Allgemeinen aussehen, denn wir brauchen nur K_0 und K_1. Die höheren K-Gruppen sind viel schwieriger zu definieren, siehe dazu [Ros94, Chap. 5].

3.1. K_0 und K_1 von Kategorien

Definition 3.1: Es sei $\mathcal{C}$ eine Kategorie mit den folgenden Eigenschaften:

- $\mathcal{C}$ ist eine volle additive Unterkategorie einer abelschen Kategorie $\mathcal{A}$.
- Wenn
$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$
eine exakte Sequenz in $\mathcal{A}$ ist und A und C in $\mathcal{C}$ sind, dann auch B.

- $\mathcal{C}$ hat ein kleines Skelett (d. h. es gibt eine kleine volle Unterkategorie $\mathcal{C}'$, sodass die Inklusion $\mathcal{C}' \hookrightarrow \mathcal{C}$ eine Äquivalenz ist).

Eine solche Kategorie heißt *Kategorie mit exakten Sequenzen.* Eine Sequenz in $\mathcal{C}$ heißt *exakt*, wenn sie in der $\mathcal{C}$ umfassenden abelschen Kategorie exakt ist.

In diesem Abschnitt sei $\mathcal{C}$ stets eine Kategorie mit exakten Sequenzen. Ferner nehmen wir von allen Funktoren zwischen solchen Kategorien stets an, dass sie additiv sind.

Wir definieren nun die K-Gruppen K_0 und K_1 durch Angabe von Erzeugern und Relationen. Um die Erzeuger von ihren Äquivalenzklassen bezüglich dieser Relationen zu unterscheiden, schreiben wir diese Äquivalenzklassen als $[\cdot]$.

Definition 3.2: (a) Die Gruppe $K_0(\mathcal{C})$ ist der Quotient der freien abelschen Gruppe, die von den Isomorphieklassen der Objekte aus $\mathcal{C}$ erzeugt wird, nach den Relationen $[B] = [A] + [C]$, wenn es in $\mathcal{C}$ eine exakte Sequenz

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

gibt.

(b) Die Gruppe $K_1(\mathcal{C})$ ist der Quotient der freien abelschen Gruppe, die von Paaren (A, α) mit $A \in \mathcal{C}$ und $\alpha \in \mathrm{Aut}(A)$ erzeugt wird, nach den Relationen $[A, \alpha] + [A, \beta] = [A, \alpha \circ \beta]$ und $[B, \beta] = [A, \alpha] + [C, \gamma]$, wenn es ein kommutatives Diagramm

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d, "\alpha"] & B \arrow[r] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & A \arrow[r] & B \arrow[r] & C \arrow[r] & 0 \end{tikzcd}$$

mit exakten Zeilen gibt.

Aus der Relation in (a) folgt $[A] + [B] = [A \oplus B]$, und aus der zweiten Relation in (b) folgt $[A, \alpha] + [B, \beta] = [A \oplus B, \alpha \oplus \beta]$. Aus der ersten Relation in (b) folgt $[A, \mathrm{id}_A] = [A, \mathrm{id}_A] + [A, \mathrm{id}_A]$ und damit $[A, \mathrm{id}_A] = 0$.

Wenn $\mathcal{D}$ eine weitere Kategorie mit exakten Sequenzen ist und $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$ ein exakter Funktor, so erhält dieser exakte Sequenzen und bildet deshalb die Diagramme aus Definition 3.2, die die Relationen definieren, auf entsprechende Diagramme in $\mathcal{D}$ ab. Dadurch induziert $\mathcal{F}$ Homomorphismen $K_i(\mathcal{C}) \longrightarrow K_i(\mathcal{D})$ für $i = 1, 2$. Auf diese Weise werden K_0 und K_1 zu Funktoren von der Kategorie der Kategorien mit exakten Sequenzen[7] in die Kategorie der abelschen Gruppen.

Definition 3.3: Es sei $\mathcal{D}$ eine weitere Kategorie mit exakten Sequenzen und $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$ ein Funktor. Dann definieren wir die *relative K-Gruppe* $K_0(\mathcal{F})$ als Quotient der freien abelschen Gruppe, die von Tripeln (A_1, A_2, α) erzeugt wird, sodass $A_1, A_2 \in \mathcal{C}$ und $\alpha \in \mathrm{Hom}_{\mathcal{D}}(\mathcal{F}(A_1), \mathcal{F}(A_2))$ ein Isomorphismus ist, nach den Relationen

$$[A_1, A_2, \alpha] + [A_2, A_3, \alpha'] = [A_1, A_3, \alpha' \circ \alpha]$$

[7] Wir können jede Kategorie mit exakten Sequenzen als klein annehmen, deshalb gibt es die Kategorie der Kategorien mit exakten Sequenzen.

und

$$[B_1, B_2, \beta] = [A_1, A_2, \alpha] + [C_1, C_2, \gamma],$$

wenn wir in $\mathcal{C}$ für $i = 1, 2$ exakte Sequenzen

$$0 \longrightarrow A_i \longrightarrow B_i \longrightarrow C_i \longrightarrow 0$$

haben, sodass in $\mathcal{D}$ das Diagramm

$$\begin{tikzcd}
\mathcal{F}(A_1) \arrow[r] \arrow[d, "\alpha"] & \mathcal{F}(B_1) \arrow[r] \arrow[d, "\beta"] & \mathcal{F}(C_1) \arrow[d, "\gamma"] \\
\mathcal{F}(A_2) \arrow[r] & \mathcal{F}(B_2) \arrow[r] & \mathcal{F}(C_2)
\end{tikzcd}$$

kommutiert. Vgl. hierzu auch [Wei13, Def. II.2.10]. Wenn klar ist, welcher Funktor gemeint ist, schreiben wir auch $K_0(\mathcal{C}, \mathcal{D})$ statt $K_0(\mathcal{F})$.

Satz 3.4: *Es seien $\mathcal{C}$ und $\mathcal{D}$ Kategorien mit exakten Sequenzen und $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{D}$ ein exakter Funktor mit der folgenden Eigenschaft:*[8] *Für jedes $D_1 \in \mathcal{D}$ gebe es ein $D_2 \in \mathcal{D}$ und ein $C \in \mathcal{C}$, sodass $D_1 \oplus D_2 \cong \mathcal{F}(C)$.*

Dann gibt es eine exakte Sequenz

$$K_1(\mathcal{C}) \longrightarrow K_1(\mathcal{D}) \xrightarrow{\partial} K_0(\mathcal{F}) \xrightarrow{\varphi} K_0(\mathcal{C}) \longrightarrow K_0(\mathcal{D}).$$

Beweisskizze: Die in der Aussage unbezeichneten Pfeile in der Sequenz werden von $\mathcal{F}$ induziert, wie bereits erklärt wurde. Wir geben an, wie die Abbildungen ∂ und φ definiert sind. Dass die Sequenz exakt ist und die unten angegebenen Abbildungen wohldefiniert sind, wollen wir hier nicht zeigen und verweisen dazu auf [Wei13, Exerc. II.2.17].

Der Homomorphismus φ sei durch

$$\varphi([A_1, A_2, \alpha]) = [A_1] - [A_2]$$

definiert. Um ∂ zu definieren, sei (D_1, δ) ein Repräsentant eines Elements von $K_1(\mathcal{D})$. Da es nach Voraussetzung ein $D_2 \in \mathcal{D}$ und $C \in \mathcal{C}$ gibt mit $D_1 \oplus D_2 \cong \mathcal{F}(C)$, gilt in $K_1(\mathcal{D})$

$$[D_1, \delta] = [D_1, \delta] + [D_2, \mathrm{id}_{D_2}] = [D_1 \oplus D_2, \delta \oplus \mathrm{id}_{D_2}] = [\mathcal{F}(C), \beta]$$

mit einem $\beta \in \mathrm{Aut}(\mathcal{F}(C))$. Wir definieren dann

$$\partial([D_1, \delta]) = [C, C, \beta].$$

Nun kann man nachrechnen, dass dies wohldefiniert ist und die Sequenz aus der Behauptung exakt macht. □

[8] Ein Funktor mit dieser Eigenschaft heißt mitunter auch *kofinal*.

3.2. K_0 und K_1 von Ringen

Es sei nun R ein Ring und $\mathcal{P}roj(R)$ die Kategorie der endlich erzeugten projektiven Moduln über R.

Lemma 3.5: *$\mathcal{P}roj(R)$ ist eine Kategorie mit exakten Sequenzen.*

Beweis: [Ros94, Ex. 3.1.2 (2)] □

Definition 3.6: Wir definieren $K_i(R) = K_i(\mathcal{P}roj(R))$ für $i = 0, 1$. Wenn ein Ringhomomorphismus $f : R \longrightarrow S$ gegeben ist, fassen wir S via f als R-Modul auf und es sei $\mathcal{F}$ der Funktor[9]

$$\mathcal{P}roj(R) \longrightarrow \mathcal{P}roj(S), \quad P \longmapsto P \otimes_R S.$$

Dann definieren wir die relative K-Gruppe durch $K_0(f) = K_0(\mathcal{F})$. Wenn klar ist, welcher Homomorphismus gemeint ist, schreiben wir hierfür auch $K_0(R, S)$.

Der Funktor $\mathcal{F}$ ist exakt, da projektive Moduln über einem beliebigen Ring stets flach sind. Ferner genügt $\mathcal{F}$ der weiteren Forderung aus Satz 3.4: denn wenn ein projektiver S-Modul D_1 gegeben ist, ist dieser direkter Summand in einem freien Modul, wir finden also ein D_2 mit $D_1 \oplus D_2 \cong S^n$, und wir können dann $C = R^n$ wählen. Deshalb bekommen wir eine exakte Sequenz

$$K_1(R) \longrightarrow K_1(S) \longrightarrow K_0(R, S) \xrightarrow{\partial} K_0(R) \longrightarrow K_0(S).$$

Diese ist ein Teil der zu Beginn des Abschnittes erwähnten langen exakten Sequenz von K-Gruppen.

Wir wollen uns nun für die Gruppen $K_0(R)$ und $K_1(R)$ eine konkretere Form überlegen. $K_0(R)$ ist die Grothendieck-Gruppe der Isomorphieklassen projektiver Moduln über R mit der direkten Summe als Gruppenoperation. Das liegt daran, dass in $\mathcal{P}roj(R)$ jede exakte Sequenz

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

spaltet – denn das ist genau die Eigenschaft, dass C projektiv ist.

Um $K_1(R)$ konkreter zu beschreiben, definieren wir zunächst

$$\mathrm{GL}(R) = \operatorname*{colim}_{n \in \mathbb{N}} \mathrm{GL}_n(R),$$

wobei die Einbettung $\mathrm{GL}_n(R) \hookrightarrow \mathrm{GL}_{n+1}(R)$ durch

$$A \longmapsto \begin{pmatrix} A & \\ & 1 \end{pmatrix}$$

gegeben sei. Dann gilt

$$K_1(R) \cong \mathrm{GL}(R)^{\mathrm{ab}}.$$

Wir geben hier an, wie der Isomorphismus aussieht, wollen dies aber nicht beweisen. Dazu sei auf [Ros94, Thm. 3.1.7] verwiesen. Jedes Element von $\mathrm{GL}(R)$ hat einen Repräsentanten

[9] Ein Modul ist genau dann projektiv, wenn er direkter Summand in einem freien Modul ist. Daran sieht man leicht, dass $P \otimes_R S$ wieder projektiv ist.

$A \in \mathrm{GL}_n(R)$ für ein $n \in \mathbb{N}$. Dieses gibt uns einen Automorphismus α von R^n, und wir definieren

$$\mathrm{GL}(R)^{\mathrm{ab}} \longrightarrow K_1(R), \quad A \longmapsto [R^n, \alpha].$$

Eine Umkehrabbildung hierfür kann folgendermaßen konstruiert werden: sei ein $[P, \alpha] \in K_1(R)$ gegeben. Da P ein projektiver R-Modul ist, ist er direkter Summand in einem freien Modul, es gibt also ein $Q \in \mathcal{Proj}(R)$ und ein $n \in \mathbb{N}$ mit $P \oplus Q \cong R^n$. Dann gilt

$$[P, \alpha] = [P, \alpha] + [Q, \mathrm{id}_Q] = [R^n, \alpha \oplus \mathrm{id}_Q],$$

und wenn wir den Automorphismus $\alpha \oplus \mathrm{id}_Q$ von R^n durch eine Matrix A darstellen, können wir

$$K_1(R) \longrightarrow \mathrm{GL}(R)^{\mathrm{ab}}, \quad [P, \alpha] \longmapsto A$$

definieren.

Satz 3.7 (Morita-Invarianz): *Für jeden Ring R und jedes $n \in \mathbb{N}$ gilt*

$$K_i(R) \cong K_i(\mathrm{M}_n(R))$$

für $i = 0, 1$.

Beweis: Für $i = 1$ gilt das, weil wir einen kanonischen Isomorphismus

$$\mathrm{GL}(\mathrm{M}_n(R)) \cong \mathrm{GL}(R)$$

haben. Für $i = 0$ siehe [Ros94, Thm. 1.2.4]. □

Wenn R ein kommutativer Ring ist, haben wir für jedes $n \in \mathbb{N}$ die Determinantenabbildung $\det\colon \mathrm{GL}_n(R) \longrightarrow R^\times$, und diese ist mit den Einbettungen $\mathrm{GL}_n(R) \hookrightarrow \mathrm{GL}_{n+1}(R)$ verträglich und induziert deshalb $\det\colon \mathrm{GL}(R) \longrightarrow R^\times$. Wegen der Kommutativität von R faktorisiert diese über die Abelisierung und liefert deshalb einen Homomorphismus

$$\det\colon K_1(R) \longrightarrow R^\times.$$

Satz 3.8: *Wenn K ein Körper ist, ist*

$$\det\colon K_1(K) \longrightarrow K^\times$$

ein Isomorphismus.

Beweis: [Ros94, Prop. 2.2.2] □

Im Falle eines nichtkommutativen Rings R funktioniert die klassische Definition der Determinante nicht mehr, aber für einen lokalen Ring kann man trotzdem eine Determinante definieren:

Satz 3.9: *Sei R ein (nicht notwendig kommutativer) lokaler Ring ist. Es gibt genau einen Homomorphismus*

$$\det\colon \mathrm{GL}(R) \longrightarrow (R^\times)^{\mathrm{ab}}$$

mit den folgenden Eigenschaften:

- $\det(1) = 1$ *(wenn die erste* 1 *die Einheitsmatrix in* $\mathrm{GL}(R)$ *bezeichnet)*
- $\det$ *ist invariant unter Zeilen- und Spaltenoperationen.*
- *Wenn man eine Zeile oder Spalte einer Matrix A mit einem $a \in R^\times$ multipliziert, ändert dies* $\det(A)$ *um $\overline{a}$, wobei $\overline{a}$ das Bild von a in $(R^\times)^{\mathrm{ab}}$ bezeichnet.*

Dieser induziert einen Isomorphismus

$$\det\colon K_1(R) \xrightarrow{\sim} (R^\times)^{\mathrm{ab}}.$$

Beweis: [Ros94, Thm. 2.2.5, Prop. 2.2.6] □

4. Nichtkommutative charakteristische Elemente

4.1. Einführung

In diesem Abschnitt sei wieder $\mathcal{O}$ der Ganzheitsring in einer endlichen Erweiterung von $\mathbb{Q}_p$, und es bezeichne Λ den proendlichen Gruppenring $\mathcal{O}[\![\Gamma]\!]$ für eine Gruppe Γ, die (nicht-kanonisch) isomorph zu $\mathbb{Z}_p$ ist, und Q den Quotientenkörper von Λ.

In Abschnitt 2 haben wir endlich erzeugte Moduln über Λ betrachtet. Der zentrale Begriff dort war der des charakteristischen Ideals (Definition 2.13), der jedem solchen Modul ein Ideal in Λ zuordnet. Solche Moduln treten oft in natürlicher Weise auf – Γ ist dann meist eine Galoisgruppe – und das charakteristische Ideal ist eine wichtige Invariante eines solchen Moduls.

Wenn wir solche Moduln in größeren, möglicherweise nichtabelschen Erweiterungen studieren wollen, stellt sich die Frage, wie man die Definition eines charakteristischen Ideals auf diese Situation verallgemeinert. Man betrachtet dann also Moduln über $\mathcal{O}[\![G]\!]$ für eine möglicherweise nichtabelsche proendliche Gruppe G. Für gewisse solche Gruppen G haben Coates, Schneider und Sujatha gezeigt, dass es in diesem Fall einen Struktursatz ähnlich Satz 2.12 gibt, aber die Ideale, die dort aus $\mathcal{O}[\![G]\!]$ herausgeteilt werden, sind im Allgemeinen keine Hauptideale. Deshalb (und auch aus anderen Gründen) eignet sich dieser Struktursatz leider nicht zur Definition eines charakteristischen Ideals; siehe hierzu auch [Ven05].

Wir schauen uns noch einmal die kommutative Situation ($G = \Gamma$) an. Das charakteristische Ideals eines Λ-Moduls hängt nur von dessen Torsionsanteil ab, also betrachten wir ohne Einschränkung nur Torsionsmoduln. Die von 0 verschiedenen Hauptideale in Λ entsprechen bijektiv den Elementen von

$$\Lambda \setminus \{0\} \big/ \Lambda^\times \ ,$$

und diese Halbgruppe können wir nach

$$Q^\times \big/ \Lambda^\times$$

einbetten. Wir bezeichnen nun die Grothendieck-Gruppe aller endlich erzeugter Λ-Torsionsmoduln mit $K_0(\Lambda_{\mathrm{tors}})$. Dann ist die Abbildung

$$\mathrm{char}\colon K_0(\Lambda_{\mathrm{tors}}) \longrightarrow Q^\times \big/ \Lambda^\times \ ,$$

die einem solchen Modul einen Erzeuger seines charakteristischen Ideals zuordnet, ein Gruppenhomomorphismus. Wegen Satz 2.9 ist dieser außerdem surjektiv: denn wenn ein $f \in \Lambda, f \neq 0$ gegeben ist, ist $\Lambda/(f)$ ein endlich erzeugter Torsionsmodul mit charakteristischem Ideal (f).

Motiviert durch diese Beobachtungen bringen wir nun die exakte Sequenz aus der algebraischen K-Theorie ins Spiel. Der Ringhomomorphismus

$$\Lambda \hookrightarrow Q$$

induziert eine exakte Sequenz

$$K_1(\Lambda) \longrightarrow K_1(Q) \xrightarrow{\partial} K_0(\Lambda, Q).$$

Wir werden später sehen (Lemma 4.5), dass $K_0(\Lambda, Q) \cong K_0(\Lambda_{\text{tors}})$ gilt. Damit und mit den Sätzen 3.8 und 3.9 sehen wir, dass diese exakte Sequenz die folgende Gestalt annimmt:

$$\begin{tikzcd}
K_1(\Lambda) \arrow[r] \arrow[d, "\det"', "\sim"] & K_1(Q) \arrow[r, "\partial"] \arrow[d, "\det"', "\sim"] & K_0(\Lambda, Q) \arrow[d, "\mathrm{char}"] \\
\Lambda^\times \arrow[r, hook] & Q^\times \arrow[r, two heads] & Q^\times/\Lambda^\times .
\end{tikzcd}$$

Daran sieht man: ein Erzeuger eines charakteristischen Ideals eines Λ-Torsionsmoduls M entspricht kanonisch einem *charakteristischen Element* $\xi_M \in K_1(Q)$, welches $\partial(\xi_M) = [M]$ erfüllt. Das ist genau die Eigenschaft eines charakteristischen Elements, die sich auf die nichtkommutative Situation verallgemeinern lässt.

4.2. Nichtkommutative Lokalisierung

In der kommutativen Situation lag das charakteristische Element in K_1 des Quotientenkörpers der Iwasawa-Algebra. Im nichtkommutativen Fall werden wir nicht diese maximale Lokalisierung betrachten, sondern nur gewisse Elemente invertieren. Lokalisieren ist im Falle eines nichtkommutativen Ringes etwas subtiler als im kommutativen Fall – man muss nämlich nun zwischen „Linksbrüchen“ und „Rechtsbrüchen“ unterscheiden.

Definition 4.1: Es sei R ein Ring und $S \subseteq R$ ein multiplikatives System (damit meinen wir eine unter der Multiplikation abgeschlossene Teilmenge mit $1 \in S$).

(a) S heißt *rechte Ore-Menge*, wenn für alle $s \in S$ und $r \in R$ gilt

$$rS \cap sR \neq \emptyset.$$

(b) S heißt *rechts-reversibel*, wenn für alle $r \in R$ und $s \in S$ gilt

$$sr = 0 \Rightarrow \exists t \in S\colon rt = 0.$$

(c) Eine rechts-reversible rechte Ore-Menge heißt *rechte Nenner-Menge*.

(d) Ein *rechter Quotientenring* von R bezüglich S ist ein Ring Q zusammen mit einem Homomorphismus $\theta\colon R \longrightarrow Q$, sodass
   - $\theta(s) \in Q^\times$ für alle $s \in S$,
   - Jedes $q \in Q$ ist von der Gestalt $q = \theta(r)\theta(s)^{-1}$ mit $r \in R$, $s \in S$,
   - $\theta(r) = 0 \iff \exists s \in S\colon rs = 0$.

Wir definieren die entsprechenden „linken" Begriffe analog.

Lemma 4.2: *(a) Es sei R ein noetherscher Ring und $S \subseteq R$ ein multiplikatives System. Ein rechter Quotientenring existiert genau dann, wenn S eine rechte Nenner-Menge ist. Die analoge Aussage gilt für linke Quotientenringe.*

(b) Jeder (linke oder rechte) Quotientenring (Q, θ) von R erfüllt die folgende universelle Eigenschaft: für jeden Ring T und jeden Ringhomomorphismus $\varphi\colon R \longrightarrow T$, der $\varphi(S) \subseteq T^\times$ erfüllt, gibt es genau einen Ringhomomorphismus $\psi\colon Q \longrightarrow T$ mit $\varphi = \psi \circ \theta$.

(c) Wenn ein rechter Quotientenring existiert, ist er bis auf Isomorphie eindeutig, genauso ein linker Quotientenring. Wenn es einen rechten und einen linken Quotientenring gibt, dann sind diese beiden kanonisch isomorph. In diesem Fall bezeichen wir diesen mit R_S und nennen ihn den Quotientenring *schlechthin.*

Beweis: (a) [MR87, Thm. 2.1.12 und Lem. 2.1.13 (i)]

(b) [MR87, Lem. 2.1.4]

(c) Folgt unmittelbar aus (b). □

Insbesondere existiert der rechte Quotientenring stets, wenn S eine rechte Ore-Menge ist, die keine Nullteiler von R enthält.

Definition 4.3: Es sei R ein noetherscher Ring, $S \subseteq R$ eine linke und rechte Nenner-Menge und M ein R-Modul. M heißt ein *S-Torsionsmodul*, wenn es für jedes $m \in M$ ein $s \in S$ gibt, sodass $sm = 0$. Dies ist dazu äquivalent, dass $R_S \otimes_R M = 0$ gilt. Wir bezeichnen mit $\mathcal{Mod}(R)_{S\text{-tors}}$ die volle Unterkategorie von $\mathcal{Mod}(R)$, die aus den endlich erzeugten S-Torsionsmoduln besteht.

Lemma 4.4: $\mathcal{Mod}(R)_{S\text{-tors}}$ *ist eine Kategorie mit exakten Sequenzen.*

Beweis: $\mathcal{Mod}(R)_{S\text{-tors}}$ ist eine volle Unterkategorie der abelschen Kategorie $\mathcal{Mod}(R)$. Da alle Moduln in $\mathcal{Mod}(R)_{S\text{-tors}}$ endlich erzeugt sind, hat die Kategorie ein kleines Skelett. Eine exakte Sequenz

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

in $\mathcal{Mod}(R)$ wird nach Tensorieren mit R_S zu

$$R_S \otimes_R A \longrightarrow R_S \otimes_R B \longrightarrow R_S \otimes_R C \longrightarrow 0,$$

und wenn $A, B \in \mathcal{Mod}(R)_{S\text{-tors}}$, gilt $R_S \otimes_R A = R_S \otimes_R C = 0$ und damit auch $R_S \otimes_R B = 0$, also $B \in \mathcal{Mod}(R)_{S\text{-tors}}$. □

Wir können also die K-Gruppe $K_0(\mathcal{Mod}(R)_{S\text{-tors}})$ betrachten. Andererseits liefert uns der Ringhomomorphismus $R \longrightarrow R_S$ eine relative K-Gruppe $K_0(R, R_S)$.

Lemma 4.5: *Es gilt kanonisch* $K_0(\mathcal{Mod}(R)_{S\text{-tors}}) \cong K_0(R, R_S)$.

Beweis: [Ven03, (4.3)] □

4.3. Definition der charakteristischen Elemente

Wir wollen die in den vorherigen Abschnitten entwickelte Theorie nun anwenden, um nichtkommutative charakteristische Elemente zu definieren. Dazu sei wieder $\mathcal{O}$ der Ganzheitsring in einer endlichen Erweiterung von $\mathbb{Q}_p$ und G eine kompakte p-adische Lie-Gruppe. Solche p-adischen Lie-Gruppen sind ganz analog zu reellen oder komplexen Lie-Gruppen definiert, siehe dazu [Sch11]. In diesem Fall ist der proendliche Gruppenring $\Lambda(G) = \mathcal{O}[\![G]\!]$ noethersch [Sch11, Thm. 27.1, Thm. 33.4]. Aus technischen Gründen nehmen wir an, dass G einen abgeschlossenen Normalteiler enthält, sodass $G/H \cong \mathbb{Z}_p$ gilt, und dass es in G kein Element von Ordnung p gibt. Als Anwendung haben wir natürlich im Sinn, dass G die Galoisgruppe einer Erweiterung eines Zahlkörpers K ist, und die erste Bedingung an G ist zum Beispiel stets erfüllt, wenn diese Erweiterung die zyklotomische $\mathbb{Z}_p$-Erweiterung von K enthält. Die kommutative Theorie erhalten wir daraus zurück, indem wir $G = \Gamma$ und $H = 1$ setzen.

Definition 4.6: Es sei

$$S = \{f \in \Lambda(G) : {}^{\Lambda(G)}\!\big/_{\Lambda(G)f} \text{ ist als } \Lambda(H)\text{-Modul endlich erzeugt}\}$$

und

$$S^* = \bigcup_{n \in \mathbb{N}_0} p^n S.$$

Satz 4.7: *S und S^* sind linke und rechte Ore-Mengen. Ihre Elemente sind keine Nullteiler.*

Beweis: Die Behauptung für S ist [CFKSV05, Thm. 2.4].[10] Die Behauptung für S^* folgt daraus, da p im Zentrum von $\Lambda(G)$ liegt. □

Wir notieren im Folgenden die Kategorie $\mathcal{Mod}(\Lambda(G)_{S^*\text{-tors}})$ kurz mit $\mathcal{Mod}_H(G)$.

Bemerkung 4.8: Im kommutativen Fall haben wir $S^* = \Lambda(\Gamma) \setminus \{0\}$. Dies folgt leicht aus Satz 2.9 und Lemma 2.8. Deshalb ist in dieser Situation $\Lambda(\Gamma)_{S^*}$ der Quotientenkörper von $\Lambda(\Gamma)$, und die Kategorie $\mathcal{Mod}(\Lambda(\Gamma)_{S^*\text{-tors}})$ ist einfach die Kategorie *aller* endlich erzeugter $\Lambda(\Gamma)$-Torsionsmoduln.

[10] Die Behauptung wird dort nur im Fall $\mathcal{O} = \mathbb{Z}_p$ gezeigt, aber die Autoren bemerken später (S. 203/204), dass sich die Argumente auch auf den Fall eines größeren $\mathcal{O}$ übertragen.

Ab jetzt sei $\mathcal{O} = \mathbb{Z}_p$. Wir betrachten nun erneut die exakte Sequenz aus der K-Theorie, die von dem Ringhomomorphismus

$$\Lambda(G) \longrightarrow \Lambda(G)_{S^*}$$

induziert wird. Dann hat die Sequenz die Gestalt

$$K_1(\Lambda(G)) \longrightarrow K_1(\Lambda(G)_{S^*}) \xrightarrow{\partial} K_0(\mathcal{Mod}_H(G)) \longrightarrow K_0(\Lambda(G)) \longrightarrow \cdots .$$

Lemma 4.9: *Unter unseren Bedingungen an G ist ∂ surjektiv.*

Beweis: [CFKSV05, Prop. 3.4] □

Dies ermöglicht uns die folgende Definition:

Definition 4.10: Es sei $M \in \mathcal{Mod}_H(G)$. Ein *charakteristisches Element* von M ist ein $\xi_M \in K_1(\Lambda(G)_{S^*})$, welches

$$\partial(\xi_M) = [M]$$

erfüllt.

Die Überlegungen in Abschnitt 4.1 und Bemerkung 4.8 zeigen, dass dies tatsächlich die klassische Definition eines charakteristischen Ideals verallgemeinert.

5. Dirichlet-Charaktere und Bernoulli-Zahlen

Definition 5.1: Es sei N eine natürliche Zahl und K ein Körper. Ein *Dirichlet-Charakter modulo N mit Werten in K* ist ein Homomorphismus

$$\chi\colon \left(\mathbb{Z}/N\mathbb{Z}\right)^\times \longrightarrow K^\times.$$

Ein solcher Dirichlet-Charakter kann über $(\mathbb{Z}/n\mathbb{Z})^\times$ für einen Teiler $n \mid N$ faktorisieren. Das minimale solche n heißt der *Führer* von χ. Wenn der Führer N ist, so heißt χ *primitiv*. Ist $K = \mathbb{C}$, so heißt χ ein *komplexer Dirichlet-Charakter*, aber wir sagen dann meist einfach nur Dirichlet-Charakter. Ist K eine endliche Erweiterung von $\mathbb{Q}_p$, so heißt χ ein *p-adischer Dirichlet-Charakter*. Ein Dirichlet-Charakter heißt *gerade*, wenn $\chi(-1) = 1$ und *ungerade*, wenn $\chi(-1) = -1$. Ein Dirichlet-Charakter heißt *unverzweigt* bei einer Primzahl p, wenn p den Führer des Charakters nicht teilt.

Für jedes $N \in \mathbb{N}$ haben wir den *trivialen Charakter*, der alles auf 1 abbildet. Diesen bezeichnen wir mit χ_N^0 oder manchmal nur mit χ^0. Außer für $N = 1$ ist dieser nie primitiv.

Zu jedem Dirichlet-Charakter χ gibt es einen zugehörigen primitiven Charakter, nämlich χ modulo dem Führer von χ.

Wenn zwei Dirichlet-Charaktere χ modulo N und ψ modulo M gegeben sind, können wir ihr Produkt definieren. Sei dazu L das kleinste gemeinsame Vielfache von M und N und seien χ_L bzw. ψ_L jeweils die Kompositionen

$$\left(\mathbb{Z}/L\mathbb{Z}\right)^\times \longrightarrow \left(\mathbb{Z}/N\mathbb{Z}\right)^\times \xrightarrow{\chi} K^\times \quad \text{bzw.} \quad \left(\mathbb{Z}/L\mathbb{Z}\right)^\times \longrightarrow \left(\mathbb{Z}/M\mathbb{Z}\right)^\times \xrightarrow{\psi} K^\times.$$

Dann definieren wir $\chi\psi$ als den Dirichlet-Charakter modulo L, der durch

$$\chi\psi(a) = \chi_L(a)\psi_L(a)$$

gegeben ist. Dieser muss nicht primitiv sein, selbst wenn χ und ψ primitiv waren: denn z.B. ist für jeden Dirichlet-Charakter χ modulo N das $\phi(N)$-fache Produkt von χ mit sich selbst der triviale Charakter modulo N, der für $N > 1$ offensichtlich nicht primitiv ist.

Bemerkung 5.2: Für jede Primzahl $p \neq 2$ können wir den Teichmüller-Charakter $\omega := \omega_{\mathbb{Q}_p}$ als p-adischen Dirichlet-Charakter von Führer p auffassen: denn mit dem Henselschen Lemma können wir $\mu(\mathbb{Q}_p)$ mit $\mathbb{F}_p^\times$ identifizieren, und der Teichmüller-Charakter ist dann ein Schnitt für die rechte Abbildung in der kanonischen exakten Sequenz

$$1 \longrightarrow 1 + p\mathbb{Z}_p \longrightarrow \mathbb{Z}_p^\times \longrightarrow \mathbb{F}_p^\times \longrightarrow 1.$$

Dies gibt uns eine Zerlegung $\mathbb{Z}_p^\times = \mathbb{F}_p^\times \times (1+p\mathbb{Z}_p)$, und der zweite Faktor ist zur additiven Gruppe von $\mathbb{Z}_p$ isomorph. Für $p = 2$ können wir den Teichmüller-Charakter als Dirichlet-Charakter von Führer 4 auffassen, da die Torsionsuntergruppe $\{\pm 1\}$ von $\mathbb{Z}_2$ zu $(\mathbb{Z}/4\mathbb{Z})^\times$ isomorph ist. Mitunter fassen wir ω auch als einen Homomorphismus $\mathbb{Z}_p^\times \longrightarrow \mathbb{Z}_p^\times$ auf, indem wir ihm die Projektion $\mathbb{Z}_p^\times \longrightarrow \mathbb{F}_p^\times$ vorschalten (hier und im Folgenden ist $\mathbb{F}_p^\times$ durch $(\mathbb{Z}/4\mathbb{Z})^\times$ zu ersetzen, falls $p = 2$). Man sieht leicht, dass ω dann durch

$$\omega(x) = \lim_{n\to\infty} x^{p^n}, \quad x \in \mathbb{Z}_p^\times$$

gegeben ist. Wenn wir $\mathbb{F}_p^\times$ mit seinem Bild in $\mathbb{Z}_p^\times \subseteq \mathbb{Q}_p^\times$ identifizieren, können wir den Teichmüller-Charakter auch als die Projektion auf den ersten Faktor

$$\omega\colon \mathbb{Z}_p^\times \cong \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p) \longrightarrow \mathbb{F}_p^\times$$

auffassen. Der Leser möge sich nicht davon verwirren lassen, dass der Charakter nach seiner ursprünglichen Definition genau in die andere Richtung geht.

Dirichlet-Charaktere sind besonders wichtig beim Studium der ihnen zugeordneten L-Funktionen. Diese sollen hier kurz eingeführt und ihre wichtigsten Eigenschaften zusammengestellt werden. Für Beweise derselben verweisen wir auf [Zag81, §I.7].

Die *L-Funktion eines Dirichlet-Charakters* χ modulo N, den wir als primitiv annehmen, ist definiert durch die Reihe

$$L(\chi, s) = \sum_{n=1}^{\infty} \chi(n) n^{-s},$$

die für $\operatorname{Re} s > 1$ konvergiert. Hierbei fassen wir χ als eine Funktion auf $\mathbb{Z}$ auf, indem wir $\chi(a) = 0$ für $(a, N) > 1$ setzen, und sonst als den Wert der Restklasse von a definieren. Für einen nicht-primitiven Charakter definieren wir seine L-Reihe als diejenige des zugehörigen primitiven Charakters.

Für einen trivialen Charakter ist

$$L(\chi_N^0, s) = \zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

die Riemannsche Zetafunktion. Insbesondere hängt seine L-Funktion nicht von N ab, und deshalb sprechen wir in diesem Zusammenhang oft von *dem* trivialen Charakter.

Die Riemannsche Zetafunktion spielt unter den Dirichletschen L-Reihen eine gewisse Sonderrolle, ihre grundlegenden Eigenschaften werden in Abschnitt III.1 aufgeführt. Für die anderen Charaktere gilt:

Satz 5.3: *Sei χ ein nichttrivialer primitiver Dirichlet-Charakter mit Führer N. Wir setzen*

$$\Lambda(\chi,s) = \left(\frac{\pi}{N}\right)^{-\frac{s}{2}} \Gamma\left(\frac{s+\delta}{2}\right) L(\chi,s), \quad \varepsilon(\chi) = \frac{G(\chi)}{\sqrt{N}}.$$

Hierbei bezeichnet Γ die Gamma-Funktion,

$$G(\chi) = \sum_{n=1}^{N} \chi(n) \mathrm{e}^{2\pi \mathrm{i} n/N} \tag{5.1}$$

die Gaußsche Summe *von χ, und es ist $\delta = 0$, wenn χ ein gerader Charakter ist, und sonst $\delta = 1$. Dann hat die L-Funktion von χ eine holomorphe Fortsetzung auf ganz $\mathbb{C}$, und sie erfüllt die Funktionalgleichung*

$$\Lambda(\chi,s) = \mathrm{i}^{-\delta} \varepsilon(\chi) \Lambda(\overline{\chi}, 1-s).$$

Von besonderem Interesse sind die Werte dieser L-Reihen bei negativen ganzzahligen Argumenten. Über solche Werte gibt es einen allgemeinen Satz für Dirichletreihen, den wir hier aus [Zag81, Satz I.7.1] zitieren:

Satz 5.4: *Es sei*

$$L(s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

eine Dirichletreihe mit irgendwelchen $a_n \in \mathbb{C}$, die für mindestens ein $s \in \mathbb{C}$ konvergiert. Wir setzen für[11] $t > 0$

$$f(t) = \sum_{n=1}^{\infty} a_n \mathrm{e}^{-nt}.$$

Es habe f für $t \to 0$ die asymptotische Entwicklung[12]

$$f(t) \sim \sum_{n=-1}^{\infty} b_n \frac{t^n}{n!}$$

mit Koeffizienten $b_n \in \mathbb{C}$. Dann hat die Funktion L eine meromorphe Fortsetzung auf ganz $\mathbb{C}$ mit einem einzigen Pol von Ordnung 1 mit Residuum b_{-1} bei $s = 0$ (holomorph, falls $b_{-1} = 0$), und es gilt

$$L(-n) = (-1)^n b_n$$

für alle $n \in \mathbb{N}_0$.

[11] Diese Reihe konvergiert für alle $t > 0$, da sonst die Dirichletreihe L überall divergent wäre. Dies folgt aus der Formel für die Konvergenzabszisse einer Dirichletreihe, siehe [Zag81, Satz I.1.2].

[12] Das bedeutet in diesem Fall, dass für jedes $N \in \mathbb{N}$ gilt $f(t) = \sum_{n=-1}^{N} b_n \frac{t^n}{n!} + o(t^N)$, was insbesondere erfüllt ist, wenn f bei $t = 0$ analytisch ist oder einen Pol von Ordnung 1 hat. Die Koeffizienten b_n sind dann eindeutig bestimmt. Vgl. hierzu [Erd56, §§1.2, 1.3].

Diesen Satz wollen wir nun auf Dirichlet-L-Reihen anwenden. Sei also χ ein primitiver Dirichlet-Charakter modulo N (der auch der triviale Charakter sein darf) und

$$f(t) = \sum_{a=1}^{N} \frac{\chi(a)\mathrm{e}^{-at}}{1 - \mathrm{e}^{-Nt}}.$$

Unter Benutzung der $N\mathbb{Z}$-Periodizität von χ als Funktion auf $\mathbb{Z}$ und der geometrischen Reihe sieht man leicht, dass dies genau die Funktion f aus Satz 5.4 ist. Es ist jedoch üblich, statt f selbst die Funktion $F(t) = -tf(-t)$ und ihre asymptotische Entwicklung zu betrachten.

Definition 5.5: Es sei

$$F(t) = \sum_{a=1}^{N} \frac{\chi(a)t\mathrm{e}^{at}}{\mathrm{e}^{Nt} - 1}$$

und

$$F(t) = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}$$

die asymptotische Entwicklung von $F(t)$, welche hier einfach die Taylorreihe ist. Die hier auftretenden Koeffizienten $B_{n,\chi}$ heißen die *verallgemeinerten Bernoulli-Zahlen* zum Charakter χ. Falls χ der triviale Charakter ist, schreiben wir B_n statt $B_{n,\chi}$ und nennen diese Zahlen einfach nur *Bernoulli-Zahlen* (deshalb heißen die anderen „verallgemeinert“).

Bemerkung 5.6: Die verallgemeinerten Bernoulli-Zahlen sind stets algebraisch, genauer gesagt liegen sie im Körper $\mathbb{Q}(\chi)$, der über $\mathbb{Q}$ von den Werten von χ erzeugt wird. Dies folgt aus der bekannten Formel für die Taylorkoeffizienten. Insbesondere sind die Standard-Bernoulli-Zahlen rational. Man sieht auch leicht an der Definition, dass $B_n = 0$ für ungerades $n \neq 1$. Mit etwas mehr Rechnen sieht man, dass für nichttriviale Charaktere $B_{n,\chi} = 0$ gilt, wenn n und χ entgegengesetze Parität haben (d.h. für ungerade n, falls χ ein gerader Charakter ist, und für gerade n, falls χ ungerade ist); vgl. hierzu [Iwa72, §2].

Der Übergang von f zu F verschiebt die Nummerierung der Koeffizienten in der asymptotischen Entwicklung um 1 und fügt ihnen den Faktor $(-1)^n n$ hinzu. Diese Beobachtung führt zusammen mit Satz 5.4 sofort zu

Satz 5.7: *Für eine Dirichletsche L-Reihe gilt für alle $n \in \mathbb{N}$*

$$L(\chi, 1-n) = -\frac{B_{n,\chi}}{n}.$$

Die Bernoulli-Zahlen wurden von Jakob Bernoulli gefunden, als er für festes $n \in \mathbb{N}_0$ die Werte des Ausdrucks

$$S_n(k) = \sum_{a=1}^{k} a^n, \quad k \in \mathbb{N}_0,$$

durch ein Polynom in k ausdrücken wollte. Ein derartiges Ergebnis wollen wir hier für die verallgemeinerten Bernoulli-Zahlen aus [Iwa72, §2] zitieren. Man erhält es nach etwas Rechnen als einfache Konsequenz der Definition der Bernoulli-Zahlen.

Satz 5.8: *Für einen Dirichlet-Charakter χ von Führer N und $n, k \in \mathbb{N}_0$ sei*

$$S_{n,\chi}(k) = \sum_{a=1}^{k} \chi(a)a^n.$$

Dann gilt

$$S_{n,\chi}(kN) = \frac{1}{n+1} \sum_{i=1}^{n} \binom{n+1}{i} B_{i,\chi}(kN)^{n+1-i}.$$

Nun wollen wir für einen p-adischen Dirichlet-Charakter ebenfalls Bernoulli-Zahlen definieren.

Definition 5.9: Es sei K eine endliche Erweiterung von $\mathbb{Q}_p$ und $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow K^\times$ ein primitiver p-adischer Dirichlet-Charakter. Dann setzen wir für $n \in \mathbb{N}$

$$B_{n,\chi} = \lim_{j\to\infty} \frac{1}{p^jN} S_{n,\chi}(p^jN).$$

Dass diese Definition sinnvoll ist, zeigt der folgende Satz.

Satz 5.10: *Es sei χ ein komplexer Dirichlet-Charakter mit Führer N. Wir wählen eine Einbettung*

$$\iota\colon \overline{\mathbb{Q}} \longrightarrow \overline{\mathbb{Q}}_p$$

des algebraischen Abschlusses von $\mathbb{Q}$ in den von $\mathbb{Q}_p$. Dann bildet ι für jedes $n \in \mathbb{N}$ die n-te Bernoulli-Zahl des komplexen Charakters χ auf die n-te Bernoulli-Zahl des p-adischen Charakters $\iota \circ \chi$ ab.

Beweis: Es gilt in $\mathbb{Q}(\chi)$ wegen Satz 5.8

$$\frac{1}{p^jN} S_{n,\chi}(p^jN) = \frac{1}{n+1} \sum_{i=1}^{n} \binom{n+1}{i} B_{i,\chi}(p^jN)^{n-i} = B_{n,\chi} + p^j \cdot C_j$$

mit einem $C_j \in \mathbb{Q}(\chi)$. Weiter gilt offenbar $\iota(S_{n,\chi}(k)) = S_{n,\iota\circ\chi}(k)$. Damit bekommen wir

$$B_{n,\iota\circ\chi} = \lim_{j\to\infty} \frac{1}{p^jN} \iota(S_{n,\chi}(p^jN)) = \lim_{j\to\infty} \Big(\iota(B_{n,\chi}) + p^j \cdot \iota(C_j)\Big) = \iota(B_{n,\chi})$$

($\iota(C_j)$ ist zwar nicht unabhängig von j, jedoch ist sein p-adischer Betrag unabhängig von j beschränkt). Insbesondere haben wir damit auch gezeigt, dass der Grenzwert in Definition 5.9 stets existiert. □

Indem wir in Satz 5.10 für χ den trivialen Charakter einsetzen, erhalten wir daraus:

Korollar 5.11: *Für die Bernoulli-Zahlen B_n, $n \in \mathbb{N}_0$, gilt in $\mathbb{Q}_p$*

$$B_n = \lim_{j\to\infty} \frac{1}{p^j} S_n(p^j).$$

6. Darstellungen

Hier sollen einige Aussagen über Darstellungen zusammengestellt werden. Für die allgemeine Darstellungstheorie endlicher Gruppen über Körpern verweisen wir auf [Ser77]. Wir wollen einige Begriffe auf Darstellungen mit Koeffizienten in allgemeineren Ringen übertragen. Es sei dazu G eine Gruppe und A ein kommutativer Ring.

Definition 6.1: Eine *Darstellung einer Gruppe G mit Koeffizienten in A* ist ein Homomorphismus

$$\rho\colon G \longrightarrow \mathrm{Aut}_A(V)$$

für einen freien A-Modul V von endlichem Rang. Wenn G eine topologische (etwa proendliche) Gruppe und A ein topologischer Ring ist, nehmen wir stets an, dass ein solcher Homomorphismus stetig ist. Wenn wir eine Basis von V wählen, ist $\mathrm{Aut}_A(V)$ offenbar zu $\mathrm{GL}_n(A)$ isomorph, wenn n den Rang von V bezeichnet. Deswegen formulieren wir im Folgenden einiges für $\mathrm{GL}_n(A)$, es ist aber in der Regel klar, dass die meisten Aussagen nicht von der Basiswahl abhängen.

Wenn $\rho'\colon G \longrightarrow \mathrm{Aut}_A(V')$ eine weitere Darstellung von G mit Koeffizienten in A ist, dann ist ein *Morphismus* von ρ nach ρ' ein Homomorphismus zwischen den A-Moduln V und V', der mit der Aktion von G auf diesen verträglich ist. Dies macht die Darstellungen von G mit Koeffizienten in A zu einer Kategorie.

Eine Darstellung heißt *irreduzibel*, wenn es keinen nichttrivialen G-stabilen A-Untermodul von V gibt. Eine Darstellung $\rho\colon G \longrightarrow \mathrm{GL}_n(K)$ mit Koeffizienten in einem Körper K heißt *absolut irreduzibel*, wenn für jede algebraische Erweiterung L von K die Darstellung

$$G \xrightarrow{\ \rho\ } \mathrm{GL}_n(K) \hookrightarrow \mathrm{GL}_n(L)$$

irreduzibel ist.

Bemerkung 6.2: Es sei K ein Körper und ρ, τ Darstellungen von G auf endlichdimensionalen K-Vektorräumen V bzw. W. Dann können wir $\mathrm{Hom}_K(V,W)$ zu einer Darstellung von G machen, indem wir die G-Aktion durch

$$g\Phi(v) = \tau(g)\Phi(\rho(g^{-1})v), \quad g \in G,\ \Phi \in \mathrm{Hom}_K(V,W),\ v \in V$$

definieren. Auch das Tensorprodukt $V \otimes_K W$ können wir zu einer G-Darstellung machen, indem wir es mit der diagonalen G-Aktion versehen. Schließlich definieren wir zu V die *duale Darstellung* als $V^* = \mathrm{Hom}_K(V,1)$, wobei 1 die triviale eindimensionale Darstellung bezeichnet. Mit diesen Definitionen gilt dann

$$V^* \otimes W \cong \mathrm{Hom}_K(V,W).$$

Ein Isomorphismus $\Psi\colon V^* \otimes W \xrightarrow{\ \sim\ } \mathrm{Hom}_K(V,W)$ ist durch

$$\Psi(f \otimes w)(v) = f(v) \cdot w$$

für $f \in V^*$, $w \in W$ und $v \in V$ gegeben. Man sieht schnell, dass dies ein injektiver (und aus Dimensionsgründen auch surjektiver) Isomorphismus von K-Vektorräumen ist, und die G-Äquivarianz kann leicht nachgerechnet werden.

Lemma 6.3 (Carayol-Serre): *Es sei G eine proendliche Gruppe und A ein proartinscher lokaler Ring mit endlichem Restklassenkörper $\mathbb{F}$. Es seien zwei stetige Darstellungen*

$$\rho_i \colon G \longrightarrow GL_{n_i}(A), \quad i = 1, 2$$

gegeben. Mit

$$\overline{\rho}_i \colon G \longrightarrow \mathrm{GL}_{n_i}(\mathbb{F})$$

sei die Reduktion von ρ_i modulo dem maximalen Ideal von A bezeichnet. Wenn ein $\overline{\rho}_i$ absolut irreduzibel ist und

$$\mathrm{Spur}\, \rho_1(\sigma) = \mathrm{Spur}\, \rho_2(\sigma)$$

für alle $\sigma \in G$ gilt, dann sind ρ_1 und ρ_2 isomorph.

Beweis: [HidMFG, Prop. 2.13] □

Besonders wichtig für uns sind Darstellungen von Galoisgruppen, für die wir nun noch einige Begriffe einführen. Sei dazu im Folgenden K ein Zahlkörper und $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}|K)$ seine absolute Galoisgruppe. Wir bezeichnen zu jeder Primstelle v von K und jeder über v liegenden Primstelle $w \mid v$ von $\overline{\mathbb{Q}}$ mit $I_{w|v} \subseteq G$ die Trägheitsgruppe bei w und mit $\mathrm{Frob}_{w|v}$ ein Frobeniuselement bei w.

Definition 6.4: Es sei $\rho \colon G_K \longrightarrow \mathrm{GL}_n(A)$ eine Darstellung von G_K.

(a) ρ heißt *unverzweigt* bei einer Primstelle v von K, wenn die Trägheitsgruppe jeder über v liegenden Primstelle von L im Kern von ρ liegt.

(b) Das *Frobenius-Polynom* von ρ bei einer Primstelle v von K ist das Polynom

$$F_{\rho,v} = \det\Big((1 - \rho(\mathrm{Frob}_{w|v})T)|_{V^{I_{w|v}}}\Big) \in A[T].$$

Hierbei ist w eine beliebige über v liegende Primstelle und $V^{I_{w|v}}$ der Untermodul von $V = A^n$, der von $I_{w|v}$ festgelassen wird. Da $F_{\rho,v}$ ein charakteristisches Polynom ist, hängt es nur von der Konjugationsklasse von $\mathrm{Frob}_{w|v}$ ab, und diese ist unabhängig von der Wahl von w.

(c) ρ heißt *ungerade*, wenn die Determinante der komplexen Konjugation -1 ist, und sonst *gerade*.

Eine Darstellung $\rho \colon G_K \longrightarrow \mathrm{GL}_n(A)$ ist also genau dann unverzweigt bei v, wenn ρ über die Galoisgruppe der maximalen bei v unverzeigten Erweiterung von K faktorisiert. Eine ungerade Darstellung über dem Grundkörper $K = \mathbb{Q}$ ist stets verzweigt bei der archimedischen Primstelle von $\mathbb{Q}$, denn deren Trägheitsgruppe wird von der komplexen Konjugation erzeugt.

Beispiel 6.5: Über den kanonischen Isomorphismus $\mathrm{Gal}(\mathbb{Q}(\mu_n)|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ können wir jeden Dirichlet-Charakter χ modulo n via

$$G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_n)|\mathbb{Q}) \xrightarrow{\sim} \left(\mathbb{Z}/n\mathbb{Z}\right)^\times \xrightarrow{\chi} \mathbb{C}^\times = \mathrm{GL}_1(\mathbb{C})$$

als eindimensionale Galoisdarstellung auffassen. Diese ist als Galoisdarstellung genau dann im Sinne von Definition 6.4 (a) unverzweigt, wenn χ als Dirichlet-Charakter im Sinne von Definition 5.1 unverzweigt ist. Ebenso ist sie genau dann als Galoisdarstellung ungerade, wenn χ als Dirichlet-Charakter ungerade ist.

Bemerkung 6.6: Sei A ein proartinscher lokaler Ring mit endlichem Restklassenkörper $\mathbb{F}$ und

$$\rho_i\colon \operatorname{Gal}(\overline{\mathbb{Q}}|K) \longrightarrow GL_{n_i}(A), \quad i = 1, 2$$

zwei stetige Darstellungen, sodass eine der reduzierten Darstellungen $\overline{\rho}_i$ absolut irreduzibel ist. Wenn beide Darstellungen nur bei endlich vielen Primstellen von K verzweigt sind und für alle unverzweigten Primstellen $\mathfrak{p}$ gilt

$$\operatorname{Spur} \rho_1(\operatorname{Frob}_{\mathfrak{p}}) = \operatorname{Spur} \rho_2(\operatorname{Frob}_{\mathfrak{p}}),$$

dann sind ρ_1 und ρ_2 isomorph. Dies folgt mit Lemma 6.3 aus dem Tschebotareffschen Dichtheitssatz, der impliziert, dass in jeder Galoiserweiterung von Zahlkörpern, die nur an endlich vielen Stellen verzweigt, die Frobeniuselemente zu den unverzweigten Primstellen dicht in der Galoisgruppe liegen. Die Bedingung an die Spur ist insbesondere dann erfüllt, wenn für alle diese $\mathfrak{p}$ die Frobenius-Polynome der Darstellungen übereinstimmen.

Definition 6.7: Es sei F ein weiterer Zahlkörper, λ eine nichtarchimedische Stelle von F mit zugehöriger Komplettierung F_λ und V ein endlichdimensionaler F_λ-Vektorraum.

(a) Eine *λ-adische Darstellung* ist ein stetiger Homomorphismus

$$\rho_\lambda\colon G_K \longrightarrow \operatorname{Aut}_{F_\lambda}(V).$$

Ein *System von λ-adischen Darstellungen* ist eine Familie $\rho = (\rho_\lambda)_\lambda$ von λ-adischen Darstellungen von G_K für alle nichtarchimedischen Primstellen λ von F.

(b) Es sei $\rho = (\rho_\lambda)_\lambda$ ein System von λ-adischen Darstellungen. Wir bezeichnen stets für jedes λ mit ℓ die unter λ liegende Primzahl in $\mathbb{Q}$ und mit S_ℓ die Menge der über ℓ liegenden Primstellen von F. Wir nennen ρ ein *kompatibles*[13] *System von Galoisdarstellungen*, wenn es eine endliche Menge S von Primstellen von F gibt, sodass gilt:

- Alle ρ_λ sind bei allen $v \notin S \cup S_\ell$ unverzweigt.
- Für jedes λ und jedes $v \notin S_\ell$ hat das Frobenius-Polynom $F_{\rho_\lambda, v}$ Koeffizienten in F und ist unabhängig von λ.

(c) Sei ρ ein kompatibles System. Wir wählen eine Einbettung des Zahlkörpers F nach $\mathbb{C}$. Dann definieren wir die *L-Funktion zu ρ* durch das formale Euler-Produkt

$$L(\rho, s) = \prod_v F_{\rho_\lambda, v}((\mathrm{N}\, v)^{-s})^{-1},$$

in dem v über alle Primstellen von K läuft und wir für jedes v ein λ mit $v \notin S_\ell$ wählen. Hierbei bezeichnet $\mathrm{N}\, v$ die Kardinalität des Restklassenkörpers von v.

[13] Dieser Begriff wird in der Literatur nicht ganz einheitlich verwendet. Unsere Definition ist sehr stark, in manchen Texten heißt ein solches System „strikt kompatibel“.

Beispiel 6.8: Wenn eine Darstellung $\rho\colon \operatorname{Gal}(\overline{\mathbb{Q}}|K) \longrightarrow \operatorname{GL}_n(\mathbb{C})$ gegeben ist, hat diese stets endliches Bild, also gibt es einen Zahlkörper F in $\mathbb{C}$, sodass das Bild von ρ bereits in $\operatorname{GL}_n(F)$ liegt. Damit ist ρ automatisch fast überall unverzweigt. Wenn wir ρ für jede Primstelle λ von F mit der Einbettung $F \hookrightarrow F_\lambda$ von F in seine Komplettierung bei λ verketten, bekommen wir ein System von λ-adischen Darstellungen, und dieses ist trivialerweise kompatibel. Die L-Funktion dieses Systems ist in diesem Fall die Artinsche L-Funktion der Darstellung ρ. Wenn wir einen Dirichlet-Charakter wie in Beispiel 6.5 als Galoisdarstellung über $\mathbb{Q}$ auffassen, stimmt diese außerdem mit der L-Funktion des Dirichlet-Charakters überein.

7. Elliptische Kurven

Hier wollen wir noch einige Dinge über elliptische Kurven bemerken. Für die allgemeine Theorie elliptischer Kurven sei auf [Sil86] verwiesen.

Es sei E eine elliptische Kurve über $\mathbb{Q}$. Für einen Körper K bezeichnet $E(K)$ die Gruppe der K-wertigen Punkte auf E, sofern diese definiert ist (also etwa für einen Erweiterungskörper von $\mathbb{Q}$ oder einen endlichen Körper von Charakteristik p, wenn E bei p gute Reduktion hat). Wir bezeichnen für $n \in \mathbb{N}$ mit $E[n](K)$ die Untergruppe der n-Torsionspunkte in $E(K)$. Zu E gehört eine Familie von ℓ-adischen Galoisdarstellungen für jede Primzahl ℓ

$$\tau_{E,\ell}\colon \operatorname{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \longrightarrow \operatorname{Aut}_{\mathbb{Z}_\ell}(T_\ell(E))$$

auf dem ℓ-adischen Tate-Modul

$$T_\ell(E) = \lim_{n\in\mathbb{N}} E[\ell^n](\overline{\mathbb{Q}}),$$

der als $\mathbb{Z}_\ell$-Modul (nichtkanonisch) zu $\mathbb{Z}_\ell^2$ isomorph ist. Die Darstellung $\tau_{E,\ell}$ ist genau bei den Primzahlen verzweigt, bei denen E schlechte Reduktion hat: das besagt das Kriterium von Néron-Ogg-Shafarevich [Sil86, Thm. VII.7.1].

Die Darstellungen $\tau_{E,\ell}$ bilden ein kompatibles System im Sinne von Definition 6.7 (b), siehe [HidGMF, §2.7.2]. Wir können also die L-Funktion dieses kompatiblen Systems betrachten (vgl. Definition 6.7 (c)). Diese bezeichnen wir mit $L(E,s)$ und nennen sie die *L-Funktion von E*. Sie ist also durch

$$L(E,s) = \prod_q \det\Big((1-\tau_{E,\ell}(\operatorname{Frob}_q)q^{-s})|_{V^{I_q}}\Big)^{-1},$$

gegeben, wobei q über alle (rationalen) Primzahlen läuft und wir für jedes q ein $\ell \neq q$ auswählen.

Es sei p eine Primzahl, bei der E gute Reduktion hat. Dann setzen wir $a_p = p+1-\#E(\mathbb{F}_p)$. Wir sagen, dass E bei p *ordinäre Reduktion* hat, wenn p kein Teiler von a_p ist. Wenn $p \geq 5$ ist, ist das zu $a_p \neq 0$ äquivalent: dies folgt aus der Hasse-Schranke [Sil86, Thm. V.1.1], die $|a_p| \leq 2\sqrt{p}$ besagt.

Bemerkung 7.1: Zwischen den Zahlen a_p und den Eulerfaktoren der L-Funktion besteht ein enger Zusammenhang: für alle Primzahlen p, bei denen E gute Reduktion hat, gilt nämlich

$$\det\Big((1-\tau_{E,\ell}(\operatorname{Frob}_p)T)\Big)^{-1} = 1 - a_pT + pT^2.$$

Die Einschränkung auf den trägheitsinvarianten Unterraum kann hierbei entfallen, da die Darstellung ja bei p unverzweigt ist. Siehe dazu [Sil94, Rem. II.10.1].

II. Klassische Modulformen

Modulformen sind auf den ersten Blick funktionentheoretische Objekte – nämlich gewisse holomorphe Funktionen auf der oberen Halbebene, die sich als Potenzreihen mit sogenannten Fourierkoeffizienten schreiben lassen. Schon früh wurde aber erkannt, dass diese Fourierkoeffizienten interessante arithmetische Informationen beinhalten: so tauchen hier etwa die Summen der Teiler(potenzen) von natürlichen Zahlen oder die Darstellungszahlen quadratischer Formen (d.h. die Anzahl, wie oft eine gegebene Zahl von einer quadratischen Form dargestellt wird) als Koeffizienten auf. Ein neueres (und viel schwierigeres) Ergebnis ist die von Wiles, Taylor, Breuil, Conrad und Diamond bewiesene Modularität elliptischer Kurven über $\mathbb{Q}$ [Wil95; TW95; BCDT01], die einen Zusammenhang zwischen den Fourierkoeffizienten gewisser Modulformen und Anzahlen von Punkten auf elliptischen Kurven angibt.

Wir wollen in diesem Kapitel Modulformen einführen und ihre grundlegenden Eigenschaften zusammenstellen. Natürlich sind nicht alle Modulformen gleich interessant – besonders gute Eigenschaften haben die sogenannten Eigenformen. Es soll vor allem unser Ziel sein, diese und ihre Fourierkoeffizienten zu untersuchen. In Kapitel IV werden wir das Studium der Eigenformen fortsetzen, indem wir diese anstatt über $\mathbb{C}$ über anderen (vor allem p-adischen) Ringen betrachten und sie letztlich als geometrische Objekte (als Punkte in Spektren von Hecke-Algebren) auffassen.

1. Der eindimensionale Fall: Hecke-Charaktere

Dirichlet-Charaktere und ihre L-Funktionen spielen in der Zahlentheorie eine große Rolle, z.B. beim Beweis des Dirichletschen Primzahlsatzes. Etwas allgemeiner sind Hecke-Charaktere (auch Größencharaktere genannt) von großer Bedeutung z.B. in der Klassenkörpertheorie. Modulformen können als eine Art nichtabelsche Verallgemeinerung von Hecke- und damit Dirichlet-Charakteren gesehen werden. Deshalb wollen wir mit einem Abschnitt über Hecke-Charaktere beginnen.

Definition 1.1: Es sei K ein Zahlkörper, $I_K = \mathbb{A}_K^\times$ seine Idelgruppe und $C_K = I_K/K^\times$ die Idelklassengruppe. Ein (stetiger) Charakter $\chi\colon C_K \longrightarrow \mathbb{C}^\times$ heißt *Hecke-Charakter*. Wir nennen χ *von endlicher Ordnung*, wenn sein Bild endlich ist.

Im Fall $K = \mathbb{Q}$ haben wir die Zerlegung $I_\mathbb{Q} = \mathbb{Q}^\times \cdot (\widehat{\mathbb{Z}}^\times \times \mathbb{R}_+^\times)$ mit $\mathbb{R}_+^\times = \{x \in \mathbb{R} : x > 0\}$. Daraus folgt

$$C_\mathbb{Q} = \widehat{\mathbb{Z}}^\times \times \mathbb{R}_+^\times.$$

Wenn wir $U(N) = \{z \in \widehat{\mathbb{Z}}^\times : z \equiv 1 \bmod N\widehat{\mathbb{Z}}\}$ für $N \in \mathbb{N}$ setzen, gilt:

Lemma 1.2: *Die Abbildung*

$$C_\mathbb{Q} \longrightarrow \left(\mathbb{Z}/N\mathbb{Z}\right)^\times, \quad (z,r) \longmapsto z \bmod N$$

induziert einen Isomorphismus

$$C_{\mathbb{Q}}\Big/\left(U(N)\times\mathbb{R}_+^\times\right)\cong\left(\mathbb{Z}\big/N\mathbb{Z}\right)^\times.$$

Beweis: Die Surjektivität ist klar, und auch, dass $\mathbb{R}_+^\times$ im Kern liegt. Der Kern von

$$\widehat{\mathbb{Z}}^\times\longrightarrow\left(\widehat{\mathbb{Z}}\big/N\widehat{\mathbb{Z}}\right)^\times=\left(\mathbb{Z}\big/N\mathbb{Z}\right)^\times$$

ist nach Definition $U(N)$. Dies zeigt die Behauptung. □

Bemerkung 1.3: Im Falle $K=\mathbb{Q}$ können wir jedem Dirichlet-Charakter einen Hecke-Charakter von endlicher Ordnung zuordnen, indem wir ihm die Abbildung $C_{\mathbb{Q}}\longrightarrow(\mathbb{Z}/N\mathbb{Z})^\times$ aus Lemma 1.2 vorschalten. Wenn umgekehrt ein Hecke-Charakter $\chi\colon\widehat{\mathbb{Z}}^\times\times\mathbb{R}_+^\times\longrightarrow\mathbb{C}^\times$ von endlicher Ordnung gegeben ist, dann ist sein Bild diskret, also muss der Kern von χ die Zusammenhangskomponente der 1 in $I_{\mathbb{Q}}$ enthalten – diese ist $\{1\}\times\mathbb{R}_+^\times$ – und eine offene Umgebung der 1 in $\widehat{\mathbb{Z}}$. Die Gruppen $U(N)$ bilden eine Umgebungsbasis der 1 in $\widehat{\mathbb{Z}}^\times$, also enthält der Kern von χ ohne Einschränkung ein $U(N)$. Dies zeigt, dass χ über $C_{\mathbb{Q}}/(U(N)\times\mathbb{R}_+^\times)$ faktorisiert und damit einen Dirichlet-Charakter $(\mathbb{Z}/N\mathbb{Z})^\times\longrightarrow\mathbb{C}^\times$ induziert. Die Dirichlet-Charaktere sind also genau die Hecke-Charaktere von endlicher Ordnung für den Fall $K=\mathbb{Q}$.

Für einen Hecke-Charakter $\chi\colon C_K\longrightarrow\mathbb{C}^\times$ kann durch das Euler-Produkt

$$L(\chi,s)=\prod_{\mathfrak{p}}(1-\chi(a_{\mathfrak{p}})\,\mathrm{N}(\mathfrak{p})^{-s})^{-1}$$

eine *L-Funktion* definiert werden. Hierbei durchläuft $\mathfrak{p}$ alle Primideale von K, $\mathrm{N}(\mathfrak{p})$ bezeichnet die Kardinalität des Restklassenkörpers von $\mathfrak{p}$ und $a_{\mathfrak{p}}\in C_K$ ist die Klasse des Idels $(\dots,1,\dots,1,\pi,1,\dots,1,\dots)$, wobei π ein Primelement der zu $\mathfrak{p}$ gehörenden Komplettierung von K ist. Im Falle eines Dirichlet-Charakters erhalten wir gerade wieder die Dirichletsche L-Funktion. Für diese L-Funktionen kann man ebenfalls analytische Fortsetzbarkeit und eine Funktionalgleichung zeigen, siehe etwa [Tat67a].

Hecke-Charaktere spielen eine wichtige Rolle in der Klassenkörpertheorie. Ihr Hauptsatz, das Artinsche Reziprozitätsgesetz, kann in folgender Form formuliert werden:

Satz 1.4: *Es sei K ein Zahlkörper und $G_K=\mathrm{Gal}(\overline{\mathbb{Q}}|K)$ seine absolute Galoisgruppe. Weiter bezeichne I_K^0 die Zusammenhangskomponente des Neutralelements in der Idelgruppe I_K. Dann gibt es eine kanonische exakte Sequenz*

$$1\longrightarrow\overline{K^\times I_K^0}\longrightarrow I_K\longrightarrow G_K^{\mathrm{ab}}\longrightarrow 1.$$

Hier ist mit $\overline{\cdot}$ der topologische Abschluss gemeint.

Beweis: [Tat67b, §§5.4, 5.6] □

Für jede abelsche Erweiterung L von K und jeden Galois-Charakter

$$\sigma\colon\ \mathrm{Gal}(L|K) \longrightarrow \mathbb{C}^\times$$

gibt uns das einen Hecke-Charakter

$$\chi\colon C_K = I_K\big/K^\times \longrightarrow I_K\big/\overline{K^\times I_K^0} \xrightarrow{\sim} G_K^{\mathrm{ab}} \twoheadrightarrow \mathrm{Gal}(L|K) \xrightarrow{\sigma} \mathbb{C}^\times,$$

und die Pfeile in der exakten Sequenz sind so gebaut, dass für jede endliche unverzweigte Primstelle $\mathfrak{p}$ von K gilt

$$\chi(a_\mathfrak{p}) = \sigma(\mathrm{Frob}_\mathfrak{p}).$$

Hierbei ist $\mathrm{Frob}_\mathfrak{p}$ ein Frobeniuselement bei $\mathfrak{p}$ (da $L|K$ abelsch ist, hängt dieses nur von $\mathfrak{p}$ ab). Anders ausgedrückt bedeutet dies, dass die L-Funktion des Hecke-Charakters χ und die Artinsche L-Funktion der Darstellung σ (vgl. Beispiel 1.6.8) übereinstimmen.

Eines der grundlegendsten Probleme der algebraischen Zahlentheorie – Erweiterungen algebraischer Zahlkörper zu klassifizieren und das Zerlegungsverhalten der Primstellen in diesen zu beschreiben – wird dadurch für abelsche Erweiterungen in zufriedenstellender Weise gelöst. Dabei werden zur Beschreibung dieser Erweiterungen nur *zum Grundkörper gehörende* Daten verwendet, nämlich der aus seinen sämtlichen Komplettierungen gebildete Adelring.

Ein Hecke-Charakter eines Zahlkörpers K ist also insbesondere eine Abbildung

$$\mathrm{GL}_1(K)\big\backslash\mathrm{GL}_1(\mathbb{A}_K) \longrightarrow \mathbb{C}$$

(die natürlich noch weitere Eigenschaften hat). Dies verallgemeinernd, definiert man eine *automorphe Form auf* GL_n als eine komplexwertige Funktion auf $\mathrm{GL}_n(K)\backslash\mathrm{GL}_n(\mathbb{A}_K)$, die gewisse technische Zusatzbedingungen erfüllt. Eine vollständige Definition findet sich in [Bum97, §3.3, S. 299/300]. Diese sind als höherdimensionale Verallgemeinerungen von Hecke-Charakteren anzusehen. Das Langlands-Programm versucht (unter anderem), als Verallgemeinerung von Satz 1.4 und der Bemerkung danach eine Korrespondenz zwischen höherdimensionalen Galoisdarstellungen und solchen automorphen Formen zu finden.

Im Fall $K = \mathbb{Q}$ und $n = 2$ zerfallen die automorphen Formen in zwei Klassen. Beide lassen sich durch gewisse Funktionen auf der oberen Halbebene produzieren, die im einen Fall holomorph sind, im anderen Fall lediglich reell-analytisch: das sind die (elliptischen) *Modulformen* und die *Maaßschen Wellenformen*. Wir wollen uns hier nur mit den Modulformen beschäftigen, die wir in den folgenden Abschnitten einführen werden. Wie diese Funktionen auf der oberen Halbebene zu Funktionen auf $\mathrm{GL}_2(\mathbb{Q})\backslash\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ und damit zu automorphen Formen führen, beschreiben wir in Bemerkung 3.3. Für total reelle Zahlkörper $K|\mathbb{Q}$ gibt es eine Verallgemeinerung von Modulformen, nämlich die *Hilbertschen Modulformen*. Diese sind gewisse Funktionen auf dem m-fachen Produkt der oberen Halbebene, wenn m die Anzahl der reellen Einbettungen von K ist. Sie lassen sich als Funktionen auf $\mathrm{GL}_2(K)\backslash\mathrm{GL}_2(\mathbb{A}_K)$ deuten.

2. Modulare Kurven

Es sei $\mathbb{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$ die obere Halbebene. Wir stellen uns diese als offene Teilmenge in der Riemannschen Zahlenkugel $\mathbb{P}^1(\mathbb{C})$ vor. Weiter setzen wir

$$\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\} = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}).$$

Die Gruppe $\mathrm{SL}_2(\mathbb{R})$ operiert auf $\mathbb{P}^1(\mathbb{C})$ durch Möbiustransformationen, und $\mathbb{H}$ und $\mathbb{H}^*$ sind stabil unter dieser Operation. Wir interessieren uns insbesondere für die Operation der Untergruppe $\mathrm{SL}_2(\mathbb{Z})$.

Definition 2.1: Sei N eine natürliche Zahl. Die *Hauptkongruenzuntergruppe von Level N* von $\mathrm{SL}_2(\mathbb{Z})$ ist der Kern der kanonischen Abbildung

$$\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2\left(\mathbb{Z}/N\mathbb{Z}\right).$$

Wir bezeichnen sie mit $\Gamma(N)$. Eine Untergruppe Γ von $\mathrm{SL}_2(\mathbb{Z})$ heißt *Kongruenzuntergruppe*, wenn sie $\Gamma(N)$ für ein N enthält; das minimale solche N heißt *Level von* Γ.

Für jede Kongruenzuntergruppe ist der Quotientenraum $\Gamma\backslash\mathbb{H}^*$ ein kompakter topologischer Raum, und man kann zeigen, dass man ihn mit einer Struktur als Riemannsche Fläche versehen kann [Shi71, §1.5]. Da die Kategorie der kompakten Riemannschen Flächen äquivalent ist zur Kategorie der projektiven nichtsingulären Kurven über $\mathbb{C}$, können wir $\Gamma\backslash\mathbb{H}^*$ also als komplexe Kurve ansehen. Die Punkte auf dieser Kurve, die von $\mathbb{P}^1(\mathbb{Q})$ herkommen, heißen *Spitzen*.

Definition 2.2: Eine Kurve $\Gamma\backslash\mathbb{H}^*$ für eine Kongruenzuntergruppe $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ heißt *modulare Kurve*. Wir bezeichnen sie mit $X(\Gamma)$. Wir schreiben $Y(\Gamma)$ für die offene Teilmenge $\Gamma\backslash\mathbb{H}$.

Wir definieren zwei spezielle Kongruenzuntergruppen, die in der Theorie der Modulformen eine zentrale Rolle spielen, nämlich

$$\begin{aligned}\Gamma_0(N) &= \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : N \mid c\},\\ \Gamma_1(N) &= \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) : a, d \equiv 1 \pmod N\}.\end{aligned}$$

Diese sind jeweils die Urbilder der Untergruppen der oberen Dreiecksmatrizen bzw. der strikten (d.h. mit 1en auf der Diagonalen) oberen Dreiecksmatrizen in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ unter der kanonischen Projektion von $\mathrm{SL}_2(\mathbb{Z})$. Offenbar gilt $\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N)$. Wir bezeichnen die zugehörigen modularen Kurven mit $X(N), X_1(N), X_0(N)$.

Wir wollen noch kurz erwähnen, dass diese modularen Kurven als Modulräume für elliptische Kurven über $\mathbb{C}$ mit gewissen Zusatzdaten gesehen werden können. Da wir hier nicht erklären wollen, was ein Modulraum ist, verweisen wir dazu auf [HM98] oder [KM85]. In letzterem wird die Interpretation der modularen Kurven als Modulräume elliptischer Kurven in einer abstrakten Sprache gezeigt. Da wir dies im Weiteren nicht benötigen, wollen wir sie hier elementar formulieren.

Wir definieren

$$\begin{aligned}S_0(N) &= \left\{(E, C) : \begin{array}{l} E \text{ elliptische Kurve über } \mathbb{C}, \\ C \subseteq E(\mathbb{C}) \text{ zyklische Untergruppe von Ordnung } N \end{array}\right\} / \sim \\ S_1(N) &= \left\{(E, P) : \begin{array}{l} E \text{ elliptische Kurve über } \mathbb{C}, \\ P \in E(\mathbb{C}) \text{ Punkt von Ordnung } N \end{array}\right\} / \sim \\ S(N) &= \left\{(E, P, Q) : \begin{array}{l} E \text{ elliptische Kurve über } \mathbb{C}, \\ P, Q \in E(\mathbb{C}) \text{ Basis für die Torsionsuntergruppe } E[N] \\ \text{mit Weil-Paarung } e_N(P, Q) = \mathrm{e}^{2\pi\mathrm{i}/N} \end{array}\right\} / \sim \end{aligned} \tag{2.1}$$

Die Äquivalenzrelation $\sim$ sei jeweils dadurch gegeben, dass es zwischen zwei äquivalenten Kurven einen Isomorphismus gibt, der die zusätzlichen Daten respektiert. Weiter sei für $\tau \in \mathbb{H}$ mit Λ_τ das Gitter $\mathbb{Z} \oplus \mathbb{Z}\tau \subseteq \mathbb{C}$ bezeichnet. Dann gilt

Satz 2.3: *Die Abbildungen*

$$
\begin{aligned}
Y_0(N) &\longrightarrow S_0(N), \quad \Gamma_0(N)\tau \longmapsto \left(\mathbb{C}/\Lambda_\tau \,, \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle \right) \\
Y_1(N) &\longrightarrow S_1(N), \quad \Gamma_1(N)\tau \longmapsto \left(\mathbb{C}/\Lambda_\tau \,, \frac{1}{N} + \Lambda_\tau \right) \\
Y(N) &\longrightarrow S(N), \quad \Gamma(N)\tau \longmapsto \left(\mathbb{C}/\Lambda_\tau \,, \frac{\tau}{N} + \Lambda_\tau, \frac{1}{N} + \Lambda_\tau \right)
\end{aligned}
$$

sind jeweils Bijektionen.

Beweis: [DS05, Thm. 1.5.1] □

3. Elliptische Modulformen

Sei $X = X(\Gamma)$ die modulare Kurve zu einer Kongruenzuntergruppe Γ, und sei $\mathbb{C}(X)$ ihr Funktionenkörper. Auf dieser gibt es die Garbe der meromorphen Differentialformen, die wir mit Ω_X bezeichnen. Das ist eine Garbe von $\mathbb{C}(X)$-Vektorräumen, die lokal frei von Rang 1 ist. Mit $\Omega_X^{\otimes k}$ bezeichnen wir das k-fache Tensorprodukt von Ω_X mit sich selbst für eine natürliche Zahl k. Die kanonische Projektion $\pi : \mathbb{H} \longrightarrow X$ liefert uns die inverse Bildgarbe $\pi^*\Omega_X^{\otimes k}$ auf $\mathbb{H}$. Sei nun $\omega \in \Omega_X^{\otimes k}(X)$ ein globaler Schnitt und $\pi^*\omega$ sein Pullback nach $\mathbb{H}$. Dann können wir $\pi^*(\omega) = f(z)(dz)^{\otimes k}$ mit einer meromorphen Funktion f auf $\mathbb{H}$ schreiben. Da $\pi^*(\omega)$ von $X(\Gamma)$ kommt, muss es Γ-invariant sein, d.h.

$$f(\gamma z)d(\gamma z)^{\otimes k} = f(z)dz^{\otimes k}$$

für alle $\gamma \in \Gamma$ erfüllen. Man kann leicht nachrechnen, dass

$$d(\gamma z) = (cz+d)^{-2}dz \qquad (\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma)$$

gilt. Deshalb muss die Funktion f die Bedingung

$$f(\gamma z) = (cz+d)^{-2k}f(z) \tag{3.1}$$

erfüllen.

Dies nehmen wir zum Anlass, für jede ganze Zahl k eine Rechtsaktion von $\mathrm{SL}_2(\mathbb{Z})$ auf dem Ring $\mathcal{O}(\mathbb{H})$ der holomorphen Funktionen auf $\mathbb{H}$ durch

$$h[\gamma]_k(z) = (cz+d)^{-k}h(\gamma z), \quad h \in \mathcal{O}(\mathbb{H}),\ z \in \mathbb{H},\ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

zu definieren, die wir die *Gewicht-k-Aktion* nennen. Die Gleichung (3.1) sagt dann also aus, dass f invariant unter der $2k$-Aktion von Γ ist. Wir dehnen diese Operation auf die Gruppe $\mathrm{GL}_2^+(\mathbb{R})$ aus, indem wir für $\alpha \in \mathrm{GL}_2^+(\mathbb{R})$ und $f : \mathbb{H} \longrightarrow \mathbb{C}$ definieren

$$h[\alpha]_k(z) = (\det \alpha)^{k/2}(cz+d)^{-k}h(\alpha z). \tag{3.2}$$

Definition 3.1: Sei $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ eine Kongruenzuntergruppe von Level N. Eine *elliptische Modulform von Gewicht k und Level N bzgl.* Γ ist eine holomorphe Funktion f auf $\mathbb{H}$, die $f[\gamma]_k = f$ für alle $\gamma \in \Gamma$ erfüllt und für die der Grenzwert

$$\lim_{y \to \infty} f[\gamma]_k(\mathrm{i}y)$$

für alle $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ existiert und endlich ist. Wenn dieser Grenzwert 0 ist, so heißt f *Spitzenform.* Die elliptischen Modulformen von Gewicht k zur Gruppe Γ bilden einen $\mathbb{C}$-Vektorraum, den wir mit $\mathcal{M}_k(\Gamma)$ bezeichnen. Den Unterraum der Spitzenformen bezeichnen wir mit $\mathcal{S}_k(\Gamma)$.

Wir wollen uns in dieser Arbeit auf elliptische Modulformen beschränken und werden deshalb ab jetzt statt „elliptische Modulform" einfach „Modulform" schreiben.

Definition 3.2: Sei f eine Modulform zu einer Kongruenzuntergruppe Γ von Level N, und sei h die kleinste natürliche Zahl, sodass die Matrix $\left(\begin{smallmatrix} 1 & h \\ & 1 \end{smallmatrix}\right)$ in Γ liegt. (Für $\Gamma_0(N)$ und $\Gamma_1(N)$ gilt $h = 1$.) Ein solches h existiert, denn Γ enthält z.B. die Matrix $\left(\begin{smallmatrix} 1 & N \\ & 1 \end{smallmatrix}\right)$. Dann gilt für alle $z \in \mathbb{H}$

$$f(z) = f[\left(\begin{smallmatrix} 1 & h \\ & 1 \end{smallmatrix}\right)]_k = f(z+h),$$

d.h. f ist $h\mathbb{Z}$-periodisch, und wir können f in eine Fourierreihe entwickeln:

$$f(z) = \sum_{n=0}^{\infty} a_n q^n$$

mit $q = \mathrm{e}^{2\pi \mathrm{i}z/h}$. Die Koeffizienten a_n heißen die *Fourierkoeffizienten von f*. Eine Modulform heißt *normalisiert*, wenn $a_1 = 1$ gilt.

Bemerkung 3.3: Wir wollen nun kurz andeuten, wie Spitzenformen zu Funktionen auf $\mathrm{GL}_2(\mathbb{Q})\backslash\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ führen und damit als automorphe Formen im Sinne von Abschnitt 1 angesehen werden können. Da wir hierbei sehr knapp bleiben, verweisen wir für Details auf die hier zitierten Werke. Wir schreiben im Folgenden $\mathbb{A}$ für $\mathbb{A}_\mathbb{Q}$.

Sei also $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ eine Kongruenzuntergruppe und ein $f \in \mathcal{S}_k(\Gamma)$ gegeben. Zu diesem f definieren wir eine Funktion φ_f auf $\mathrm{SL}_2(\mathbb{R})$ durch

$$\varphi_f(g) = f[g]_k(i).$$

Die Invarianz von f unter der Gewicht-k-Aktion von Γ übersetzt sich für die Funktion φ_f in die Eigenschaft

$$\varphi_f(\gamma g) = \varphi_f(g) \quad \forall g \in \mathrm{SL}_2(\mathbb{R}),\ \gamma \in \Gamma.$$

Wir können φ_f also auffassen als eine stetige Funktion auf $\Gamma\backslash\mathrm{SL}_2(\mathbb{R})$. Auf diesem Raum kann man ein $\mathrm{SL}_2(\mathbb{R})$-invariantes Radon-Maß[1] wählen, und bezüglich dieses Maßes ist φ_f quadratisch integrierbar (hier benutzt man, dass f eine Spitzenform ist). Also ist

$$\mathcal{S}_k(\Gamma) \longrightarrow L^2(\Gamma\backslash\mathrm{SL}_2(\mathbb{R})), \quad f \longmapsto \varphi_f$$

[1] Das ist ein Maß auf der Borel-σ-Algebra, das kompakten Mengen endliches Maß gibt und von oben und unten regulär ist. Es ist eindeutig bis auf Multiplikation mit einem Skalar.

eine wohldefinierte Abbildung, und diese ist sogar eine isometrische Injektion von komplexen Hilberträumen, wenn wir $\mathcal{S}_k(\Gamma)$ mit dem Petersson-Skalarprodukt versehen (welches wir in Abschnitt 5 einführen werden). Siehe hierzu [Dei10, §3.3].

Wir benötigen nun eine Variante der sogenannten *starken Approximation*, die wir aus [Dei10, Prop. 7.2.4, Satz 7.2.5] zitieren. Sei dazu K der Abschluss von Γ in $\mathrm{SL}_2(\widehat{\mathbb{Z}})$ und $Z(\mathbb{R})$ das Zentrum von $\mathrm{GL}_2(\mathbb{R})$. Dann induziert die Inklusion $\mathrm{SL}_2(\mathbb{R}) \hookrightarrow \mathrm{GL}_2(\mathbb{A})$ einer reellen Matrix in die archimedische Komponente der adelischen Matrizen einen Homöomorphismus

$$\Gamma\backslash \mathrm{SL}_2(\mathbb{R}) \xrightarrow{\sim} \mathrm{GL}_2(\mathbb{Q})Z(\mathbb{R})\backslash \mathrm{GL}_2(\mathbb{A})/K .$$

Dieser ist sogar $\mathrm{SL}_2(\mathbb{R})$-äquivariant und liefert deshalb wegen der Eindeutigkeit des Radon-Maßes einen Isomorphismus von Hilberträumen

$$L^2(\Gamma\backslash\mathrm{SL}_2(\mathbb{R})) \cong L^2(Z(\mathbb{R})\,\mathrm{GL}_2(\mathbb{Q})\backslash\mathrm{GL}_2(\mathbb{A})/K).$$

Wir bekommen also eine isometrische Inklusion von $\mathcal{S}_k(\Gamma)$ in den rechten Hilbertraum. Insbesondere können wir $\mathcal{S}_k(\Gamma)$ als Unterraum des Raums der komplexwertigen Funktionen auf $\mathrm{GL}_2(\mathbb{Q})\backslash\mathrm{GL}_2(\mathbb{A})$ auffassen. Das Bild dieser Abbildung ist in [Gel75, Prop. 3.1] beschrieben. Es sei noch erwähnt, dass das auch mit den Fourierkoeffizienten „zusammenpasst", siehe dazu Bemerkung 6.8.

Auch Maaßsche Wellenformen können als Funktionen auf $\mathrm{GL}_2(\mathbb{Q})\backslash\mathrm{GL}_2(\mathbb{A})$ aufgefasst werden [Dei10, Satz 7.2.6]. Das Analogon zu Modulformen für total reelle Zahlkörper $K|\mathbb{Q}$, die Hilbertschen Modulformen, können als Funktionen auf $\mathrm{GL}_2(K)\backslash\mathrm{GL}_2(\mathbb{A}_K)$ gesehen werden [Gel75, S. 52].

Bemerkung 3.4: Die Überlegungen am Anfang dieses Abschnittes kann man benutzen, um mit Hilfe des Satzes von Riemann-Roch zu zeigen, dass die Räume $\mathcal{M}_k(\Gamma)$ endlichdimensional sind und ihre Dimension explizit bestimmen. Dies geschieht z.B. in [Shi71, §§2.3–2.6]. Als Spezialfall der dort hergeleiteten Formeln sei exemplarisch die Dimension von $\mathcal{M}_k(\Gamma_1(N))$ bzw. $\mathcal{S}_k(\Gamma_1(N))$ für $k \geq 3$ und $N \geq 5$ genannt. Diese ist [DS05, Fig. 3.4]

$$\frac{(k-1)N^2}{24}\prod_{p|N}\left(1-\frac{1}{p^2}\right) \pm \frac{1}{4}\sum_{d|N}\phi(d)\phi(\tfrac{N}{d}),$$

wobei dort „+" für $\mathcal{M}_k(\Gamma_1(N))$ und „−" für $\mathcal{S}_k(\Gamma_1(N))$ einzusetzen ist. Das Produkt läuft hier über alle Primteiler von N und die Summe über alle Teiler von N. Insbesondere sieht man daran, dass diese Dimensionen unbeschränkt sind, wenn k und N wachsen.

Bemerkung 3.5: Wenn $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ eine beliebige Kongruenzuntergruppe von Level N ist, dann gilt $\mathcal{M}_k(\Gamma) \subseteq \mathcal{M}_k(\Gamma(N))$. Weiter gilt für $f \in \mathcal{M}_k(\Gamma(N))$, dass $(z \longmapsto f(Nz)) \in \mathcal{M}_k(\Gamma_1(N^2))$: denn es gilt

$$f(Nz) = N^{-k/2} f\left[\begin{pmatrix} N & \\ & 1\end{pmatrix}\right]_k(z)$$

und

$$\Gamma_1(N^2) \subseteq \begin{pmatrix} N & \\ & 1\end{pmatrix}^{-1}\Gamma(N)\begin{pmatrix} N & \\ & 1\end{pmatrix},$$

wie man sich leicht überlegt. Wenn

$$f(z) = \sum_{n=0}^{\infty} a_n \mathrm{e}^{2\pi i n z/N}$$

die Fourierentwicklung von $f \in \mathcal{M}_k(\Gamma(N))$ ist, so ist

$$f(Nz) = \sum_{n=0}^{\infty} a_n \mathrm{e}^{2\pi i n z}.$$

Wir haben also für jede Kongruenzuntergruppe Γ von Level N eine Einbettung

$$\mathcal{M}_k(\Gamma) \hookrightarrow \mathcal{M}_k(\Gamma_1(N^2)),$$

die die Fourierkoeffizienten erhält. Da uns die Fourierkoeffizienten besonders interessieren, werden wir uns im Folgenden meistens auf die Kongruenzuntergruppe $\Gamma_1(N)$ zurückziehen.[2]

Es seien nun $\Gamma \subseteq \Delta$ Kongruenzuntergruppen, so dass Γ in Δ normal ist. Dann definieren wir eine Operation von Δ auf $\mathcal{M}_k(\Gamma)$ durch $(\alpha, f) \longmapsto f[\alpha]_k$. Um zu sehen, dass dies wohldefiniert ist, müssen wir zeigen, dass die Funktion $f[\alpha]_k$ invariant unter Γ ist (die Holomorphie auf $\mathbb{H}$ und an den Spitzen bleibt von der Operation natürlich ungestört). Dazu sei $\gamma \in \Gamma$ gegeben. Wegen $\alpha\Gamma = \Gamma\alpha$ gibt es ein $\widetilde{\gamma} \in \Gamma$ mit $\alpha\gamma = \widetilde{\gamma}\alpha$. Damit bekommen wir dann

$$(f[\alpha]_k)[\gamma]_k = f[\widetilde{\gamma}\alpha]_k = f[\alpha]_k,$$

also gilt tatsächlich $f[\alpha]_k \in \mathcal{M}_k(\Gamma)$.

Per Definition operiert die Untergruppe Γ trivial, sodass eine Aktion des Quotienten Δ/Γ induziert wird. Dieser Quotient ist endlich, da jede Kongruenzuntergruppe in $\mathrm{SL}_2(\mathbb{Z})$ endlichen Index hat. Also definiert die obige Operation eine Darstellung

$$\Delta/\Gamma \longrightarrow \mathrm{Aut}_{\mathbb{C}}(\mathcal{M}_k(\Gamma))$$

einer endlichen Gruppe auf einem endlichdimensionalen komplexen Vektorraum, und diese können wir in irreduzible Darstellungen zerlegen. Im Falle, dass der Quotient Δ/Γ abelsch ist, lässt sich diese Zerlegung besonders leicht hinschreiben, da dann alle irreduziblen Darstellungen eindimensional sind.

Definition 3.6: Es seien $\Gamma \subseteq \Delta$ Kongruenzuntergruppen, so dass Γ in Δ normal und der Quotient Δ/Γ abelsch ist. Für jeden Charakter ε von Δ/Γ definieren wir

$$\mathcal{M}_k(\Delta, \varepsilon) = \{f \in \mathcal{M}_k(\Gamma) \mid \forall \gamma \in \Delta\colon f[\gamma]_k = \varepsilon(\gamma) f\}.$$

[2] Wir können zwar jedes $M_k(\Gamma)$ auch nach $\mathcal{M}_k(\Gamma(N))$ einbetten, jedoch hat die Gruppe $\Gamma_1(N)$ angenehmere Eigenschaften: so ist in Definition 3.2 $h = 1$, und die von der zugehörigen modularen Kurve klassifizierten elliptischen Kurven (vgl. Satz 2.3) sind in diesem Fall einfacher.

Dies ist der Eigenraum des Charakters ε in der oben erwähnten Darstellung (vgl. (1.2.1)). In dieser Situation gilt dann

$$\mathcal{M}_k(\Gamma) = \bigoplus_{\varepsilon} \mathcal{M}_k(\Delta, \varepsilon),$$

wobei ε alle Charaktere von Δ/Γ durchläuft.

Besonders wichtig ist die obige Diskussion für den Fall $\Gamma = \Gamma_1(N)$ und $\Delta = \Gamma_0(N)$. Man kann sich leicht überlegen, dass die Abbildung

$$\Gamma_0(N) \longrightarrow \left(\mathbb{Z}/N\mathbb{Z}\right)^{\times}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto d$$

ein surjektiver Gruppenhomomorphismus ist und $\Gamma_1(N)$ als Kern hat. Der Quotient Δ/Γ ist in diesem Fall also $(\mathbb{Z}/N\mathbb{Z})^{\times}$, und wir notieren seine Darstellung auf $\mathcal{M}_k(\Gamma_1(N))$ mit $\langle\cdot\rangle$ und nennen diese Abbildungen die *Diamant-Operatoren.*

Definition 3.7: Für $\delta \in \mathbb{Z}$ mit $(\delta, N) = 1$ sei

$$\langle\delta\rangle f = f[\gamma]_k, \quad \text{für ein } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \text{ mit } d \equiv \delta \pmod N.$$

Wir setzen $\langle\delta\rangle f = 0$ für $\delta \in \mathbb{Z}$ mit $(\delta, N) > 1$.

Es gilt dann

$$\mathcal{M}_k(\Gamma_1(N)) = \bigoplus_{\chi} \mathcal{M}_k(\Gamma_0(N), \chi),$$

wobei χ alle Dirichlet-Charaktere modulo N durchläuft. Wir schreiben meistens $\mathcal{M}_k(N, \chi)$ statt $\mathcal{M}_k(\Gamma_0(N), \chi)$. Ein Element von $\mathcal{M}_k(N, \chi)$ heißt *Modulform von Gewicht k, Level N und Nebentyp χ.*

Zusammen mit Bemerkung 3.5 heißt dies also, dass es im Wesentlichen genügt, die Räume $\mathcal{M}_k(N, \chi)$ zu verstehen, wenn man Modulformen zu einer beliebigen Kongruenzuntergruppe verstehen möchte. Deshalb werden wir im Weiteren vor allem diese Räume betrachten.

Schließlich merken wir noch an, dass all dies ganz analog auch für die Räume $\mathcal{S}_k(\Gamma)$ statt $\mathcal{M}_k(\Gamma)$ funktioniert. Wir definieren also die Räume $\mathcal{S}_k(N, \chi)$ entsprechend.

4. Hecke-Operatoren

Der Definition eines Hecke-Operators liegt folgendes einfache Prinzip zugrunde: Seien S, X, Y Mengen und seien Abbildungen $p\colon S \longrightarrow X$ und $q\colon S \longrightarrow Y$ gegeben.

$$\begin{tikzcd} & S \arrow[dl, "p"'] \arrow[dr, "q"] & \\ X & & Y \end{tikzcd}$$

Aus dieser Situation kann man unter geeigneten Voraussetzungen einen Hecke-Operator T basteln, der aus einer Funktion auf X eine Funktion auf Y macht. Sei dazu f eine (etwa reell- oder komplexwertige) Funktion auf X. Durch Komposition mit p machen wir daraus zunächst eine Funktion $f \circ p$ auf S. Schließlich „definieren“ wir die Funktion Tf auf Y durch

$$Tf(y) = \int_{q^{-1}(y)} f \circ p,$$

wobei wir annehmen, dass auf S ein geeignetes Maß gegeben ist und die Abbildungen p, q und f hinreichend schön sind, sodass dieses Integral existiert. Wenn z.B. die Abbildung q endliche Fasern hat, kann man auf S das Zählmaß wählen und

$$Tf(y) = \sum_{s \in q^{-1}(y)} f \circ p(s)$$

definieren. Da die Situation symmetrisch ist, können die Rollen von X und Y natürlich auch vertauscht werden.

In unserer Situation seien Γ_1, Γ_2 Kongruenzuntergruppen, $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ und sei $\Gamma' = \Gamma_2 \cap \alpha^{-1}\Gamma_1\alpha$ (was dann ebenfalls wieder eine Kongruenzuntergruppe ist, siehe [Shi71, Lem. 3.9]). Wir haben dann folgendes Diagramm, in dem alle Abbildungen kanonische Projektionen sind:

$$\begin{tikzcd}
 & & \mathbb{H}^* \arrow[d] \arrow[ddll] \arrow[ddr] & \\
 & & \Gamma'\backslash\mathbb{H}^* \arrow[dl] \arrow[dr] & \\
\Gamma_1\backslash\mathbb{H}^* & \alpha^{-1}\Gamma_1\alpha\backslash\mathbb{H}^* & & \Gamma_2\backslash\mathbb{H}^*
\end{tikzcd}$$

Zwischen den beiden linken unteren Einträgen gibt es einen Isomorphismus

$$\alpha^{-1}\Gamma_1\alpha\Big\backslash\mathbb{H}^* \longrightarrow \Gamma_1\Big\backslash\mathbb{H}^*, \quad [z] \longmapsto [\alpha z].$$

Diesen verketten wir mit der kanonischen Projektion $\Gamma'\backslash\mathbb{H}^* \longrightarrow \alpha^{-1}\Gamma_1\alpha\backslash\mathbb{H}^*$ und erhalten so ein Diagramm

$$\begin{tikzcd}
 & \Gamma'\backslash\mathbb{H}^* \arrow[dl, "p"'] \arrow[dr, "q"] & \\
\Gamma_1\backslash\mathbb{H}^* & & \Gamma_2\backslash\mathbb{H}^*,
\end{tikzcd}$$

das die Rolle unseres ersten Diagramms mit $S = \Gamma'\backslash\mathbb{H}^*$, $X = \Gamma_1\backslash\mathbb{H}^*$ und $Y = \Gamma_2\backslash\mathbb{H}^*$ spielen soll. Da die Abbildungen p und q hier (Einschränkungen von) Überlagerungen von Kurven sind, haben beide endliche Fasern.

Wir wollen in dieser Situation einen Homomorphismus zwischen den Divisorengruppen von Y und X definineren. Einen Divisor auf Y können wir als eine Abbildung von Y nach $\mathbb{Z}$

sehen (mit endlichem Träger). Die oben erklärte Konstruktion produziert aus einem solchen Divisor einen Divisor auf X, und wir bekommen einen Homomorphismus

$$T\colon \operatorname{Div}(Y) \longrightarrow \operatorname{Div}(X).$$

In [Shi71, S. 76/77] wird gezeigt, dass dieser durch die folgende Formel gegeben ist. Sei $[z] \in Y$ und $z \in \mathbb{H}^*$ ein Urbild auf der oberen Halbebene. Wir betrachten die Doppelnebenklasse $\Gamma_1\alpha\Gamma_2$ und zerlegen sie in eine disjunkte endliche Vereinigung von Linksnebenklassen

$$\Gamma_1\alpha\Gamma_2 = \bigcup_{i=1}^{e} \Gamma_1\beta_i.$$

Dann gilt

$$T([z]) = \sum_{i=1}^{e} [\beta_i z].$$

Diese Formel legt die folgende Definition nahe, die eine Aktion von solchen Doppelnebenklassen auf Modulformen liefert.

Definition 4.1: Seien Γ_1, Γ_2 Kongruenzuntergruppen, $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ und

$$\Gamma_1\alpha\Gamma_2 = \bigcup_{i=1}^{e} \Gamma_1\beta_i, \quad \beta_i \in \mathrm{GL}_2^+(\mathbb{Q}) \tag{4.1}$$

eine disjunkte Zerlegung der Doppelnebenklasse $\Gamma_1\alpha\Gamma_2$ in Linksnebenklassen. Der *Doppelnebenklassenoperator*

$$[\Gamma_1\alpha\Gamma_2]_k\colon \mathcal{M}_k(\Gamma_1) \longrightarrow \mathcal{M}_k(\Gamma_2)$$

ist gegeben durch

$$f[\Gamma_1\alpha\Gamma_2]_k = (\det\alpha)^{k/2-1} \sum_{i=1}^{e} f[\beta_i]_k. \tag{4.2}$$

Der Faktor $(\det\alpha)^{k/2-1}$ dient hierbei der Normalisierung (vgl. Bemerkung 4.4).

Dies ist ein Homomorphismus von $\mathbb{C}$-Vektorräumen. Er bildet Spitzenformen auf Spitzenformen ab [Shi71, Prop. 3.37], es gibt also den genauso definierten Operator

$$[\Gamma_1\alpha\Gamma_2]_k\colon \mathcal{S}_k(\Gamma_1) \longrightarrow \mathcal{S}_k(\Gamma_2).$$

Besonders wichtig für uns ist der Fall, dass $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$.

Beispiel 4.2: Wenn $\Gamma \subseteq \Delta$ Kongruenzuntergruppen sind, sodass Γ in Δ normal ist, haben wir eine Operation von Δ/Γ auf $\mathcal{M}_k(\Gamma)$ (siehe Seite 40). Diese ist durch solche Doppelnebenklassenoperatoren gegeben: denn sei für ein $\delta \in \Delta/\Gamma$ ein Lift $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Delta$ gegeben. Wegen der Normalität gilt

$$\Gamma\alpha\Gamma = \Gamma\alpha(\alpha^{-1}\Gamma\alpha) = \Gamma\alpha,$$

und es folgt

$$f[\Gamma\alpha\Gamma]_k = f[\alpha]_k.$$

Insbesondere sind also die Diamant-Operatoren $\langle\cdot\rangle$ aus Definition 3.7 solche Doppelnebenklassenoperatoren.

Definition 4.3: Wir setzen

$$\Delta = \{\alpha \in \mathrm{M}_2(\mathbb{Z}) : \alpha \equiv \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \pmod N,\ \det \alpha > 0\} \tag{4.3}$$

und definieren T_n für jede natürliche Zahl n als die formale Summe

$$T_n = \sum_{\substack{\alpha \in \Delta \\ \det \alpha = n}} [\Gamma_1(N)\alpha\Gamma_1(N)]_k. \tag{4.4}$$

Hinter der Wahl von Δ und dieser Definition steckt die Interpretation von $Y_1(N)$ als Modulraum (siehe (2.1) und Satz 2.3): die Punkte auf $Y_1(N)$ entsprechen Paaren (E, P), wobei E eine komplexe elliptische Kurve und P ein Punkt von Ordnung N in $E(\mathbb{C})$ ist. Eine komplexe elliptische Kurve ist nichts anderes als ein Gitter in $\mathbb{C}$. Jedes T_n definiert einen Endomorphismus der Divisorengruppe von $Y_1(N)$. Wenn wir T_n auf ein Gitter $L \subseteq \mathbb{C}$ mit gewähltem Punkt P von Ordnung N in $\mathbb{C}/L$ anwenden, gilt

$$n \cdot T_n(L, P) = \sum_{L'} (L', P), \tag{4.5}$$

wobei L' hier alle Gitter in $\mathbb{C}$ durchläuft, die L als Teilgitter von Index n enthalten, und so, dass P auch in $\mathbb{C}/L'$ Index N hat; siehe hierzu [Lan76, §§VII.2,VII.4].

Bemerkung 4.4: Wir wollen an dieser Stelle erwähnen, dass man die Aktion von $\mathrm{GL}_2^+(\mathbb{R})$ auf $\mathcal{O}(\mathbb{H})$ statt wie in (3.2) auch durch

$$f[\alpha]_k(z) = (\det \alpha)^{k-1}(cz+d)^{-k} f(\alpha z)$$

definieren könnte. In diesem Fall kann dann der Normalisierungsfaktor $(\det \alpha)^{k/2-1}$ in (4.2) entfallen. Wenn man jedoch die Relationen aus Satz 4.6 für die Operatoren T_n erhalten möchte, gilt in diesem Fall (4.4) nur, falls n eine Primzahl ist. Auch (4.5) gilt nur, falls n prim ist, dafür kann der Faktor n auf der linken Seite entfallen.

In [DS05] wird mit dieser alternativen Normierung gearbeitet. Die Operatoren T_p für Primzahlen p werden dort durch

$$T_p = [\Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N)]_k$$

definiert und für zusammengesetztes n dann über die Relationen aus Satz 4.6. Die Wirkung dieser Operatoren auf $\mathcal{M}_k(\Gamma_1(N))$ ist in beiden Fällen dieselbe.

Im Folgenden betrachten wir T_n als Endomorphismus von $\mathcal{M}_k(\Gamma_1(N))$. Dabei gilt insbesondere $T_1 = \mathrm{id}$. Wenn Φ eine Kongruenzuntergruppe mit $\Gamma_1(N) \subseteq \Phi \subseteq \Gamma_0(N)$ ist, haben wir eine Zerlegung

$$\mathcal{M}_k(\Gamma_1(N)) = \bigoplus_{\varepsilon} \mathcal{M}_k(\Phi, \varepsilon),$$

in der ε die Charaktere von $\Phi/\Gamma_1(N)$ durchläuft.

Lemma 4.5: *Die Endomorphismen* $[\Gamma_1(N)\alpha\Gamma_1(N)]_k$ *für* $\alpha \in \Delta(\Gamma_1(N))$ *sind mit der Zerlegung*

$$\mathcal{M}_k(\Gamma_1(N)) = \bigoplus_{\varepsilon} \mathcal{M}_k(\Phi, \varepsilon),$$

verträglich, d.h. es gilt $[\Gamma_1(N)\alpha\Gamma_1(N)]_k\mathcal{M}_k(\Phi,\varepsilon) \subseteq \mathcal{M}_k(\Phi,\varepsilon)$ *für jeden Charakter* ε *von* $\Phi/\Gamma_1(N)$. *Insbesondere sind die* T_n *mit dieser Zerlegung verträglich.*

Beweis: Wir greifen hier auf [Shi71] zurück. Dort wird die Behauptung in (3.5.5), (3.5.6) und dem nachfolgenden Absatz (S. 79) für $\Phi = \Gamma_0(N)$ gezeigt, der Beweis überträgt sich aber direkt auf unsere Situation. □

Satz 4.6: *Die Endomorphismen* T_n *von* $\mathcal{M}_k(\Gamma_1(N))$ *erfüllen die folgenden Relationen:*

(a) Für Primzahlen p und $r \in \mathbb{N}$ *gilt*
   (i) als Endomorphismus von $\mathcal{M}_k(\Gamma_1(N))$: $T_{p^r} = T_pT_{p^{r-1}} - \langle p\rangle p^{k-1}T_{p^{r-2}}$
   (ii) als Endomorphismus von $\mathcal{M}_k(N,\chi)$: $T_{p^r} = T_pT_{p^{r-1}} - \chi(p)p^{k-1}T_{p^{r-2}}$
   (iii) $T_{p^r} = (T_p)^r$, *falls* $p \mid N$

(b) $T_mT_n = T_{mn}$ *für teilerfremde m und n*

(c) $T_mT_n = T_nT_m$ *für alle* $m, n \in \mathbb{N}$.

Beweis: Wir verwenden wieder [Shi71]. Auf S. 70 definiert Shimura einen Operator $T'(n)$, welches unser T_n ist.

(a) Wir verwenden Thm. 3.35 und Thm. 3.24 (4) aus [Shi71]: Dies zeigt, dass für T_{p^r} als Endomorphismus von $\mathcal{M}_k(\Gamma_1(N))$ (in Shimuras Notation)

$$T'(p^r) = T'(p)T'(p^{r-1}) - pT'(p,p)T'(p^{r-2})$$

gilt . Die Gleichungen (3.5.6) und (3.5.8) auf S. 79/80 zeigen dann, dass $T'(p,p)f = p^{k-2}\chi(p)f$ als Endomorphismus von $\mathcal{M}_k(N,\chi)$. Beachte hierbei, dass in (3.5.6) $\mathfrak{h} = \{1\}$ gilt und dass (3.5.8) auch für $p \mid N$ gilt, da dann $\chi(p) = 0$ und $T'(p,p) = 0$ nach Thm. 3.35, und außerdem nicht nur für Spitzenformen.

Dies zeigt Gleichung (ii). Die Relationen (i) und (iii) folgen hieraus unmittelbar (vgl. Definition von $\langle\cdot\rangle$).

(b) [Shi71, Thm. 3.34 (4)]

(c) Folgt aus [Shi71, Prop. 3.8]. □

Man kann nachrechnen, dass der Effekt der Hecke-Operatoren auf den Fourierkoeffizienten durch die folgende Formel gegeben ist:

Lemma 4.7: *Sei $f \in \mathcal{M}_k(\Gamma_1(N))$. Dann gilt für alle $m, n \in \mathbb{N}$*

$$a_m(T_n f) = \sum_{d|(m,n)} d^{k-1} a_{mn/d^2}(\langle d \rangle f).$$

Insbesondere gilt für $f \in \mathcal{M}_k(N, \chi)$

$$a_m(T_n f) = \sum_{d|(m,n)} \chi(d) d^{k-1} a_{mn/d^2}(f).$$

Beweis: Die zweite Behauptung ist Formel (3.5.12) in [Shi71]. Die erste Behauptung folgt hieraus mit der Definition von $\langle \cdot \rangle$. □

Daraus kann man folgern, dass die Eigenwerte von Eigenvektoren der Hecke-Operatoren mit den entsprechenden Fourierkoeffizienten übereinstimmen:

Satz 4.8: *Es sei ein normalisiertes $f \in \mathcal{S}_k(N, \chi)$ mit Fourierentwicklung*

$$f = \sum_{n=1}^{\infty} a_n q^n$$

gegeben, welches für jedes $n \in \mathbb{N}$ mit $(n, N) = 1$ ein Eigenvektor von T_n zum Eigenwert c_n ist. Dann gilt

$$a_n = c_n \text{ für } (n, N) = 1.$$

Beweis: Sei $n \in \mathbb{N}$ mit $(n, N) = 1$. Da f normalisiert ist und Eigenvektor von T_n zum Eigenwert c_n, gilt

$$a_1(T_n f) = c_n a_1 = c_n.$$

Die Behauptung folgt dann aus Lemma 4.7 mit $m = 1$, was

$$a_1(T_n f) = a_n$$

für alle $n \in \mathbb{N}$ besagt. □

Bemerkung 4.9: Es sei M ein Teiler von N. Dann gilt $\Gamma_1(N) \subseteq \Gamma_1(M)$ und daher $\mathcal{S}_k(\Gamma_1(M)) \subseteq \mathcal{S}_k(\Gamma_1(N))$. Für ein $d \in \mathbb{Z}$ hängt die Wirkung von $\langle d \rangle$ auf $\mathcal{S}_k(\Gamma_1(N))$ per Definition nur von der Restklasse von d modulo N ab, und diese bestimmt die Restklasse von d modulo M. Dies zeigt, dass die Einschränkung von $\langle d \rangle$ auf den Unterraum $\mathcal{S}_k(\Gamma_1(M))$ mit der Wirkung von $\langle d \rangle$ auf diesem Unterraum übereinstimmt. Mit Lemma 4.7 folgt, dass dies auch für die Operatoren T_n gilt. Mit anderen Worten: das Diagramm

$$\begin{tikzcd}
\mathcal{S}_k(\Gamma_1(M)) \arrow[r, hook] \arrow[d] & \mathcal{S}_k(\Gamma_1(N)) \arrow[d] \\
\mathcal{S}_k(\Gamma_1(M)) \arrow[r, hook] & \mathcal{S}_k(\Gamma_1(N)),
\end{tikzcd}$$

in dem die horizontalen Pfeile die natürlichen Inklusionen und die vertikalen entweder $\langle d \rangle$ oder T_n sind, kommutiert.

5. Das Petersson-Skalarprodukt und Atkin-Lehner-Theorie

Wir wollen nun ein Skalarprodukt auf den Räumen $S_k(\Gamma)$ für eine Kongruenzuntergruppe Γ einführen. Dafür definieren wir zunächst ein $\mathrm{SL}_2(\mathbb{R})$-invariantes Maß μ auf der oberen Halbebene $\mathbb{H}$ durch

$$\mathrm{d}\mu(z) = \frac{\mathrm{d}x\mathrm{d}y}{y^2}, \quad z = x + \mathrm{i}y.$$

Seien nun $f, g \in \mathcal{M}_k(\Gamma)$ gegeben. Dann ist die Funktion

$$z \longmapsto f(z)\overline{g(z)}y^k, \quad z = x + \mathrm{i}y \in \mathbb{H}$$

Γ-invariant, wie man leicht nachrechnet. Sei D ein Fundamentalbereich für Γ. Dann ist demnach das Integral

$$\int_D f(z)\overline{g(z)}y^k \frac{\mathrm{d}x\mathrm{d}y}{y^2} = \int_D f(z)\overline{g(z)}y^{k-2}\mathrm{d}x\mathrm{d}y$$

wohldefiniert, wenn es existiert. Man kann zeigen, dass dieses Integral konvergiert, sobald das Produkt fg an allen Spitzen von Γ verschwindet, also insbesondere für $f, g \in \mathcal{S}_k(\Gamma)$ [Lan76, §III.4].

Lemma 5.1: *Die Zuordnung*

$$\langle f, g \rangle = \frac{1}{\mu(D)} \int_D f(z)\overline{g(z)}y^{k-2}\mathrm{d}x\,\mathrm{d}y$$

definiert ein Skalarprodukt auf $\mathcal{S}_k(\Gamma)$. Es heißt Petersson-Skalarprodukt.

Dieses Skalarprodukt ist verträglich mit der Zerlegung

$$\mathcal{S}_k(\Gamma_1(N)) = \bigoplus_{\chi} \mathcal{S}_k(N, \chi)$$

in dem Sinne, dass die Unterräume $\mathcal{S}_k(N, \chi)$ paarweise orthogonal sind [Shi71, (3.5.4)].

Das wichtigste Resultat, welches dieses Skalarprodukt mit Hecke-Operatoren in Verbindung bringt, ist der folgende Satz.

Satz 5.2: *Auf dem Raum $\mathcal{S}_k(N, \chi)$ sind die adjungierten Endomorphismen der Hecke-Operatoren für alle n mit $(n, N) = 1$ durch*

$$T_n^* = \chi(n)^{-1} T_n$$

gegeben. Insbesondere sind die Hecke-Operatoren T_n normal für $(n, N) = 1$ (d.h. die kommutieren mit ihren Adjungierten).

Beweis: [Lan76, Thm. VII.5.1] □

Der Spektralsatz aus der linearen Algebra impliziert dann unmittelbar:

Korollar 5.3: *Der Raum $\mathcal{S}_k(N, \chi)$ hat eine Orthogonalbasis, die aus simultanen Eigenformen für alle T_n mit $(n, N) = 1$ besteht.*

Wir wollen nun noch Beziehungen zwischen Modulformen zu verschiedenen Level studieren. Sei dazu $N \in \mathbb{N}$ und d ein Teiler von N. Dann gilt wegen $\Gamma_1(N) \subseteq \Gamma_1(d)$

$$\mathcal{M}_k(\Gamma_1(d)) \subseteq \mathcal{M}_k(\Gamma_1(N)).$$

Außerdem haben wir außer der Inklusion eine weitere kanonische Abbildung

$$\iota_d \colon \mathcal{M}_k(\Gamma_1(d)) \longrightarrow \mathcal{M}_k(\Gamma_1(N)), \quad f(\cdot) \longmapsto f(\tfrac{N}{d}\,\cdot).$$

Modulformen, die auf eine dieser Weisen von kleineren Leveln herkommen, wollen wir „alt" nennen.

Definition 5.4: Der Unterraum von $\mathcal{M}_k(\Gamma_1(N))$, der von den Bildern der beiden eben beschriebenen kanonischen Abbildungen

$$\mathcal{M}_k(\Gamma_1(d)) \longrightarrow \mathcal{M}_k(\Gamma_1(N))$$

für alle $d \mid N$ erzeugt wird, heißt der *Raum der Altformen* und wird mit $\mathcal{M}_k(\Gamma_1(N))^{\mathrm{old}}$ bezeichnet. Analog definieren wir $\mathcal{S}_k(\Gamma_1(N))^{\mathrm{old}}$. Sein orthogonales Komplement in $\mathcal{S}_k(\Gamma_1(N))$ bezeichnen wir mit $\mathcal{S}_k(\Gamma_1(N))^{\mathrm{new}}$ und nennen die Elemente *Neuformen.*[3]

Die Räume der Alt- und Neuformen sind stabil unter den Hecke-Operatoren [DS05, Prop. 5.6.2].

Satz 5.5 (Atkin-Lehner): *Sei $f \in \mathcal{S}_k(\Gamma_1(N))$ mit Fourierentwicklung*

$$f = \sum_{n=1}^{\infty} a_n q^n.$$

Dann gilt $a_n = 0$ für $(n, N) = 1$ genau dann, wenn f von der Form

$$f = \sum_{p \mid N} \iota_{N/p}(f_p)$$

für $f_p \in \mathcal{S}_k(\Gamma_1(N/p))$ ist.

Beweis: [DS05, Thm. 5.7.1] □

Satz 5.6: *Wenn $f \in \mathcal{S}_k(\Gamma_1(N))$ ein Eigenvektor aller T_n mit $(n, N) = 1$ ist, dann gibt es einen Teiler M von N und eine Neuform, $f_0 \in \mathcal{S}_k^{\mathrm{new}}(\Gamma_1(M))$, die ebenfalls ein Eigenvektor aller T_n mit $(n, N) = 1$ ist und deren Fourierkoeffizienten für alle diese n mit denen von f übereinstimmen.*

Beweis: [Miy89, Cor. 4.6.14] □

[3] Der englische Begriff „newform" wird in der Literatur oft für Neuformen in unserem Sinne verwendet, die zusätzlich Eigenvektoren aller Hecke-Operatoren sind; unsere Neuformen heißen dann oft „primitiv".

Wir definieren nun noch

$$\mathcal{E}_k(\Gamma) = \mathcal{M}_k(\Gamma) \big/ \mathcal{S}_k(\Gamma)$$

für eine Kongruenzuntergruppe Γ. Mithilfe des Petersson-Skalarprodukts kann dieser Raum mit dem orthogonalen Komplement von $\mathcal{S}_k(\Gamma)$ in $\mathcal{M}_k(\Gamma)$ identifiziert werden (man beachte, dass dieses zwar kein Skalarprodukt auf dem ganzen Raum $\mathcal{M}_k(\Gamma)$ ist, aber konvergiert, wenn eines der beiden Argumente eine Spitzenform ist, weshalb dieses orthogonale Komplement sinnvoll definiert werden kann). Der Raum $\mathcal{E}_k(\Gamma)$ heißt der *Raum der Eisensteinreihen*. Vieles von dem, was wir im folgenden für Spitzenformen machen werden, würde auch für die Eisensteinreihen funktionieren. Wir sind aber vorwiegend an den *L*-Funktionen und Galoisdarstellungen interessiert, die uns Modulformen liefern (siehe Abschnitte 6 und IV.3), und diese sind für Eisensteinreihen nicht so interessant: die *L*-Funktionen sind nämlich das Produkt zweier Dirichlet-*L*-Reihen [Shi71, S. 78], und die Galoisdarstellungen sind reduzibel [DS05, Thm. 9.6.6]. Aus diesem Grund werden wir uns meistens nur mit den Spitzenformen beschäftigen.

6. Eigenformen und L-Funktionen

Definition 6.1: Wir nennen ein $f \in \mathcal{M}_k(N, \chi)$ eine *Eigenform*, wenn es ein Eigenvektor aller Hecke-Operatoren T_n für $n \in \mathbb{N}$ ist.

Satz 6.2: *Sei $f \in \mathcal{S}_k(\Gamma_1(N))^{\text{new}}$ ein normalisierter Eigenvektor aller Hecke-Operatoren T_n für alle $n \in \mathbb{N}$ mit $(n, N) = 1$. Dann ist f eine Eigenform.*

Beweis: Sei $n \in \mathbb{N}$ und $g = T_n f - a_n(f) f$. Als Linearkombination zweier Neuformen ist g eine Neuform. Der erste Fourierkoeffizient von g ist

$$a_1(g) = a_1(T_n f) - a_1(a_n f) = 0.$$

Wegen Lemma 4.7 gilt

$$a_1(T_m g) = a_m g$$

für alle $m \in \mathbb{N}$, und da g ebenfalls Eigenvektor aller Hecke-Operatoren T_m für $(m, N) = 1$ ist, folgt $a_m(g) = 0$ für $(m, N) = 1$. Nach Satz 5.5 ist dann g auch eine Altform, also muss $g = 0$ gelten. □

Bemerkung 6.3: Es sei $f \in \mathcal{S}_k(\Gamma_1(N))$ eine Eigenform. Die Relation (i) aus Satz 4.6 (a) zeigt

$$p^{k-1} \langle p \rangle = T_p^2 - T_{p^2}.$$

Also muss f auch ein Eigenvektor der Operatoren $\langle n \rangle$ für alle $n \in \mathbb{N}$ mit $(n, N) = 1$ sein. Daraus folgt, dass es für jede solche Eigenform genau einen Dirichlet-Charakter χ modulo N gibt, sodass $f \in \mathcal{S}_k(N, \chi)$: denn wenn c_n der Eigenwert zu $\langle n \rangle$ ist, können wir

$$\chi(n) = c_n$$

definieren, und es ist klar, dass dies ein Dirichlet-Charakter ist und dass $f \in \mathcal{S}_k(N, \chi)$ gilt.

Satz 6.4: *Sei $f \in \mathcal{M}_k(\Gamma_1(N))$ mit Fourierentwicklung*

$$f = \sum_{n=1}^{\infty} a_n q^n.$$

Dann ist f genau dann eine normalisierte Eigenform, wenn es einen Dirichlet-Charakter χ modulo N gibt, sodass die Fourierkoeffizienten die folgenden Relationen erfüllen:

(a) $a_1 = 1$,

(b) $a_{p^r} = a_p a_{p^{r-1}} - \chi(p) p^{k-1} a_{p^{r-2}}$ *für alle Primzahlen p und $r > 2$,*

(c) $a_{mn} = a_m a_n$ *für teilerfremde m und n.*

Dieses χ ist dann der Nebentyp von f.

Beweis: Dass die Fourierkoeffizienten einer normalisierten Eigenform von Nebentyp χ diese Relationen erfüllen, folgt sofort aus den entsprechenden Relationen für die Hecke-Operatoren aus Satz 4.6. Die andere Richtung folgt durch eine leichte Rechnung aus Lemma 4.7 und Satz 4.8; siehe dazu auch [DS05, Prop. 5.8.5]. □

Definition 6.5: Sei $f \in \mathcal{M}_k(\Gamma)$ eine Modulform zu einer Kongruenzuntergruppe Γ, und sei

$$f = \sum_{n=0}^{\infty} a_n q^n$$

die zugehörige Fourierreihe. Die *L-Funktion zu f* ist definiert als die Dirichletreihe

$$L(f, s) = \sum_{n=0}^{\infty} a_n n^{-s}.$$

Wenn χ ein primitiver Dirichlet-Charakter ist, definieren wir weiter die *um χ getwistete L-Funktion* zu f als

$$L(f, \chi, s) = \sum_{n=0}^{\infty} \chi(n) a_n n^{-s}.$$

Die guten analytischen Eigenschaften von Modulformen (Holomorphie oder sogar Verschwinden an den Spitzen) sorgen für Konvergenz dieser Dirichletreihe: Wenn f eine Spitzenform ist, konvergiert $L(f, \chi, s)$ absolut für $\operatorname{Re} s > \frac{k}{2} + 1$, sonst für $\operatorname{Re} s > k$ [DS05, Prop. 5.9.1].[4] Im Falle von Spitzenformen lässt sich diese Funktion zu einer ganzen Funktion auf $\mathbb{C}$ fortsetzen; sonst lässt sie sie im Allgemeinen nur zu einer meromorphen Funktion fortsetzen [Bum97, Prop. 1.3.6].

[4] Die Aussage wird dort nur für $f \in \mathcal{M}_k(\Gamma_1(N))$ gezeigt, was aber wegen Bemerkung 3.5 genügt. Auch wird dort lediglich eine ungetwistete L-Funktion betrachtet (d.h. χ ist trivial), aber da die Koeffizienten der Dirichletreihe durch das Twisten jeweils um Faktoren von Betrag ≤ 1 abgeändert werden, folgt leicht, dass dies die Konvergenz nicht verschlechtert.

Die *Mellin-Transformation* von f ist definiert durch das Integral

$$\mathrm{M}f(s) = \int_0^\infty f(\mathrm{i}t)t^s \frac{\mathrm{d}t}{t}.$$

Sie hängt mit der L-Funktion über die Beziehung

$$\mathrm{M}f(s) = (2\pi)^{-s}\Gamma(s)L(f,s)$$

zusammen. Dies kann man benutzen, um im Falle einer Spitzenform $f \in \mathcal{S}_k(N,\chi)$ eine Funktionalgleichung für die L-Funktion zu zeigen. Sei dazu $\Lambda(f,s) = N^{s/2}\mathrm{M}f(s)$. Dann gilt

$$\Lambda(f,s) = \mathrm{i}^k\Lambda(f[\tau]_k, k-s), \quad \tau = \begin{pmatrix} & -1 \\ N & \end{pmatrix}$$

nach [Shi71, Thm. 3.66].

Satz 6.6: *Es sei $f \in \mathcal{M}_k(N,\chi)$. Dann hat die zugehörige L-Funktion genau dann eine Darstellung als Eulerprodukt*

$$L(f,s) = \prod_p (1 - a_p p^{-s} + \chi(p)p^{k-1-2s})^{-1},$$

wenn f eine normalisierte Eigenform ist.

Beweis: Dies folgt leicht aus Satz 6.4. Siehe dazu auch [DS05, Thm. 5.9.2]. □

Definition 6.7: Das Polynom $1 - a_pX + \chi(p)p^{k-1}X^2 \in \mathbb{C}[X]$ heißt das *p-te Hecke-Polynom von f*.

Solche Eigenformen und ihre Hecke-Polynome werden uns in Kapitel IV im Zusammenhang mit modularen Galoisdarstellungen erneut begegnen.

Bemerkung 6.8: In Bemerkung 3.3 hatten wir angedeutet, wie man Spitzenformen als automorphe Formen auf GL_2 über $\mathbb{Q}$ ansehen kann. Wir wollen zum Schluss noch erwähnen, dass man solchen automorphen Formen in gewissen Fällen ebenfalls eine L-Funktion zuordnen kann – insbesondere dann, wenn sie zu einer Eigenform gehören – und dass diese mit der L-Funktion zu einer klassischen Eigenform zusammenpasst, d.h. sie stimmen überein bis auf eine (konstante) Verschiebung des Arguments. Siehe dazu [Dei10, Kap. 8], wo dies in einem Spezialfall gezeigt wird.

III. Kommutative p-adische L-Funktionen

Bei der Untersuchung von L-Funktionen stehen zuerst meist funktionentheoretische Gesichtspunkte im Vordergrund. Studiert man spezielle Werte dieser Funktionen, so zeigt sich aber, dass diese auch ein p-adisches Verhalten an den Tag legen können. Dies wurde zuerst von T. Kubota und H.-W. Leopoldt beobachtet, und damit konnten sie für Dirichletsche L-Funktionen und insbesondere die Riemannsche Zetafunktion ein p-adisches Analogon konstruieren.

Heute wird für eine große Klasse von L-Funktionen vermutet, dass diese ein p-adisches Pendant haben. Im Allgemeinen ist dessen Konstruktion aber völlig unklar – mehr noch, sogar wesentliche Eigenschaften der komplexen L-Funktionen, die als Voraussetzungen für die Existenz des p-adischen Avatars unabdingbar sind, sind nicht bekannt. In gewissen Fällen gelang es aber, eine solche Konstruktion durchzuführen, unter anderem für die L-Funktionen von Modulformen.

Wir werden uns in diesem Kapitel zuerst mit p-adischen Dirichlet-L-Funktionen beschäftigen, um klar zu machen, wie man p-adische L-Funktionen richtig auffassen sollte, und am Ende die entsprechenden Ergebnisse für die L-Funktionen von Modulformen zusammenstellen. Warum wir diese p-adischen L-Funktionen „kommutativ“ nennen, wird erst später klar werden; siehe dazu Abschnitt V.2.

1. Motivation

1.1. Die Grundidee

Bernhard Riemann hat die später nach ihm benannte *Riemannsche Zetafunktion*

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}, \quad s \in \mathbb{C},\ \operatorname{Re} s > 1$$

untersucht und gezeigt, dass sie eine meromorphe Fortsetzung auf ganz $\mathbb{C}$ mit einem einzigen Pol der Ordnung 1 bei $s = 1$ hat und der Funktionalgleichung

$$\Lambda(s) = \Lambda(1-s) \text{ mit } \Lambda(s) = \frac{s(s-1)}{2}\pi^{-\frac{s}{2}}\Gamma(\tfrac{s}{2})\zeta(s)$$

genügt. Bereits Euler war die Produktentwicklung

$$\zeta(s) = \prod_p (1-p^{-s})^{-1},\ \operatorname{Re} s > 1$$

bekannt, in der p alle Primzahlen durchläuft, und er fand außerdem die Formel

$$\zeta(2n) = (-1)^{n-1}\frac{(2\pi)^{2n}B_{2n}}{2(2n)!}$$

für die Werte der Zetafunktion bei positiven geraden Zahlen (hier bezeichnet B_n die n-te Bernoulli-Zahl, vgl. Definition I.5.5).

Zusammen mit der Funktionalgleichung liefert Eulers Formel[1]

$$\zeta(1-n) = -\frac{B_n}{n} \text{ für } n \in \mathbb{N},$$

was ein Spezialfall von Satz I.5.7 ist. Insbesondere sind die Werte bei den nichtpositiven ganzen Zahlen rational – eine überaus erstaunliche Tatsache, wenn man bedenkt, dass ζ dort durch analytische Fortsetzung einer durch eine konvergente Reihe definierten meromorphen Funktion definiert ist! Diese Rationalität ist die Voraussetzung für die arithmetische Interpretation dieser speziellen Werte der Zetafunktion.

Ein erster Schritt zu einer solchen Interpretation sind die *Kummer-Kongruenzen*:

Satz 1.1: *Sei $p \neq 2$ eine Primzahl, $k \in \mathbb{N}$ und seien $m, n \in \mathbb{N}$ nicht durch $p-1$ teilbar. Es gelte $m \equiv n \pmod{p^k(p-1)}$. Dann gilt*

$$(1-p^{m-1})\frac{B_m}{m} \equiv (1-p^{n-1})\frac{B_n}{n} \pmod{p^{k+1}}.$$

Dies wollen wir hier nicht beweisen, wir zeigen später (Satz 1.4) eine Variante davon. Ein elementarer Beweis findet sich z.B. in [Lan76, Thm. X.1.1].

Bemerkung: Üblicherweise wird dieser Satz nur für *gerade* m, n formuliert, dann allerdings auch für die Primzahl $p = 2$. Wenn $p \neq 2$, dann gilt die Kongruenz sogar für alle $m, n \in \mathbb{N}$: denn aus der Voraussetzung $m \equiv n \pmod{p^k(p-1)}$ folgt, dass m und n entweder beide gerade oder beide ungerade sind (da $p-1$ gerade ist). Wenn m ungerade und nicht 1 ist, ist die entsprechende Bernoulli-Zahl $B_m = 0$, und für $m = 1$ ist $1 - p^{m-1} = 0$. Deshalb ist die Kongruenz trivialerweise erfüllt, wenn m und n ungerade sind.

Wir wollen diese Kongruenzen nun neu interpretieren. Dies war im Wesentlichen die Idee von Kubota und Leopoldt, die auf diese Weise als Erste zu p-adischen L-Funktionen gelangt sind [KL64].

Dazu wählen wir eine Primzahl $p \neq 2$ und ein beliebiges $a \in \mathbb{N}$ mit $(p-1) \nmid a$ und setzen

$$D_a = \big(a + (p-1)\mathbb{Z}\big) \cap \mathbb{N} = \{n \in \mathbb{N} : n \equiv a \pmod{p-1}\}.$$

Wir betrachten dann die Funktion[2]

$$f\colon D_a \longrightarrow \mathbb{Q}^\times, \quad n \longmapsto (1-p^{n-1})\zeta(1-n).$$

Das ist im Prinzip die Riemannsche Zetafunktion eingeschränkt auf $1 - D_a$, wobei der p-te Eulerfaktor entfernt wurde. Der Inhalt der Kummerschen Kongruenzen ist dann gerade, dass diese Funktion gleichmäßig stetig ist, wenn wir beide Seiten mit der p-adischen Metrik versehen. Daraus folgt dann, dass sich die Funktion zu einer p-adischen Funktion fortsetzen lässt.

[1] Die Bernoulli-Zahlen B_n sind 0 für ungerade $n \neq 1$, und die Zetafunktion hat bei den negativen geraden Zahlen triviale Nullstellen, was leicht aus der Funktionalgleichung folgt. Für gerade n folgt die Beziehung dann aus Eulers Formel zusammen mit der Funktionalgleichung.

[2] Wenn a ungerade ist, ist diese Funktion konstant 0 und daher langweilig. Wer möchte, kann also a als gerade annehmen.

Lemma 1.2: *f ist gleichmäßig stetig bezüglich der p-adischen Metrik.*

Beweis: Wir müssen zeigen:

$$\forall \varepsilon > 0\, \exists \delta > 0\, \forall m, n \in D_a\colon\ |m-n|_p < \delta \Rightarrow \left|f(m) - f(n)\right|_p < \varepsilon.$$

Für alle $m, n \in D_a$ ist die Kongruenz $m \equiv n \pmod{p-1}$ automatisch erfüllt. Wenn wir ohne Einschränkung $\varepsilon = p^{-(k+1)}$ für ein $k \in \mathbb{N}$ annehmen, können wir $\delta = p^{-k}$ setzen und die Aussage folgt direkt aus den Kummer-Kongruenzen. □

Satz 1.3: *Es gibt genau eine stetige Funktion*

$$f\colon \mathbb{Z}_p \longrightarrow \mathbb{Q}_p,$$

die

$$f(n) = (1-p^{n-1})\zeta(1-n)$$

für $n \in D_a$ erfüllt.

Beweis: Diese Funktion entsteht aus dem oben definierten f durch stetige Fortsetzung auf die Vervollständigung von D_a; dass diese existiert, folgt aus der gleichmäßigen Stetigkeit. Wir zeigen, dass D_a in $\mathbb{Z}_p$ dicht liegt, indem wir zeigen, dass es für jede ganze Zahl $z \in \mathbb{Z}$ und jedes $k \in \mathbb{N}$ ein $l \in \mathbb{Z}$ gibt mit $p^k l - z \in D_a$ (denn dann liegt z und damit $\mathbb{Z}$ im Abschluss von D_a). Dazu wählen wir l einfach als eine ganze Zahl, die

$$l \equiv \frac{a-z}{p^k} \pmod{p-1}$$

erfüllt, und groß genug, damit $p^k l - z \in \mathbb{N}$. Wir bemerken hier noch, dass der Beweis der Dichtheit nicht $p-1 \nmid a$ benutzt. □

Eine solche Funktion ist als ein erster Prototyp eines p-adisches Analogons der Riemannschen Zetafunktion anzusehen. Allerdings hat dieser noch ein erhebliches Manko: die Funktion hängt so noch von der Wahl von a ab, und a unterliegt hierbei der Einschränkung, dass es nicht in der trivialen Restklasse modulo $p-1$ liegen darf.

1.2. Die p-adische Zetafunktion

Um zuerst die Einschränkung an die Restklasse von a modulo $p-1$ loszuwerden, zeigen wir folgende Variante der Kummer-Kongruenzen:

Satz 1.4: *Sei $p \neq 2$ eine Primzahl und $m, n \in \mathbb{N}$, und sei $c \in \mathbb{Z}$ zu p teilerfremd. Es gelte $m \equiv n \pmod{p^k(p-1)}$. Dann gilt*

$$(1-c^m)(1-p^{m-1})\frac{B_m}{m} \equiv (1-c^n)(1-p^{n-1})\frac{B_n}{n} \pmod{p^{k+1}}.$$

Beweis (nach [Pan97]): Zunächst bemerken wir, dass wegen $p^k(p-1) = \#\left(\mathbb{Z}/p^{k+1}\mathbb{Z}\right)^\times$ für alle $x \in \mathbb{Z}$ mit $(x,p) = 1$ gilt

$$x^m \equiv x^n \pmod{p^{k+1}}. \tag{$*$}$$

Mit Korollar I.5.11 sieht man leicht, dass in $\mathbb{Q}_p$ gilt

$$(1-p^{m-1})B_m = \lim_{j\to\infty} \frac{1}{p^j} \sum_{\substack{a=1\\ p\nmid a}}^{p^j} a^m,$$

wir können also ein großes $j \in \mathbb{N}$ mit

$$\left|(1-p^{m-1})B_m - \frac{1}{p^j}\sum_{\substack{a=1\\ p\nmid a}}^{p^j} a^m\right|_p \le p^{-(k+1)}$$

wählen. Mit diesem j gilt dann

$$(1-c^m)(1-p^{m-1})\frac{B_m}{m} \equiv (1-c^m)\frac{1}{mp^j}\sum_{\substack{a=1\\ p\nmid a}}^{p^j} a^m \pmod{p^{k+1}}.$$

Die hier auf der rechten Seite stehende rationale Zahl bezeichnen wir vorübergehend mit A. Hierbei ist zu beachten, dass es sich nicht um eine Gleichheit in $\mathbb{Z}/p^{k+1}\mathbb{Z}$ handelt, denn beide Seiten der Kongruenz können nichttriviale p-Potenzen im Nenner enthalten. Jedoch gilt dies nicht für ihre Differenz, und deren Zähler ist durch p^{k+1} teilbar.

Es ist

$$A = \frac{1}{m}\sum_{\substack{a=1\\ p\nmid a}}^{p^j} \frac{a^m - (ca)^m}{p^j}.$$

Für jedes solche in der Summe vorkommende a sei nun $b_a \in \{1,\dots,p^j\}$ die eindeutige Zahl mit $b_a \equiv ca \pmod{p^j}$. Da $(c,p) = 1$, also $c \in (\mathbb{Z}/p^j\mathbb{Z})^\times$, ist $a \longmapsto b_a$ eine Permutation der Menge

$$\{a \in \{1,\dots,p^j\} : p \nmid a\},$$

und wir bekommen

$$A = \frac{1}{m}\sum_{\substack{a=1\\ p\nmid a}}^{p^j} \frac{b_a^m - (ca)^m}{p^j}.$$

Wir setzen nun $t = \frac{b_a - ca}{p^j} \in \mathbb{Z}$. Es gilt dann

$$b_a^m - (ca)^m = (ca + p^j t)^m - (ca)^m = \sum_{i=1}^{m} \binom{m}{i} (ca)^{m-i}(p^j t)^i = mp^j t (ca)^{m-1} + K\cdot p^{2j}$$

für ein $K \in \mathbb{Z}$. Setzen wir dies in die vorherige Rechnung ein, so erhalten wir

$$A = t\sum_{\substack{a=1\\ p\nmid a}}^{p^j} (ca)^{m-1} + p^j \frac{K(p-1)p^{j-1}}{m}.$$

Wir wählen nun j ohne Einschränkung so groß, dass der rechte Term keine p-Potenz im Nenner hat und der Zähler durch p^{k+1} teilbar ist. Dann erhalten wir unter Benutzung von $(*)$ die gewünschte Kongruenz modulo p^{k+1}:

$$(1-c^m)(1-p^{m-1})\frac{B_m}{m} \equiv A \equiv t \sum_{\substack{a=1\\ p\nmid a}}^{p^j} (ca)^{m-1} \overset{(*)}{\equiv} t \sum_{\substack{a=1\\ p\nmid a}}^{p^j} (ca)^{n-1} \equiv (1-c^n)(1-p^{n-1})\frac{B_n}{n}. \quad \square$$

Im Vergleich zu der weiter oben zitierten Variante der Kummer-Kongruenzen (Satz 1.1) ist es nun also erlaubt, dass m und n durch $p-1$ teilbar sind, dafür wurde auf beiden Seiten der Kongruenz ein Faktor $(1-c^?)$ eingefügt. Dies benutzen wir, um nun endlich das Analogon der p-adischen Zetafunktion zu definieren.

Satz 1.5: *Es gibt genau eine stetige Funktion*

$$\zeta_p \colon \mathbb{Z}_p \setminus \{1\} \longrightarrow \mathbb{Q}_p,$$

die

$$\zeta_p(1-n) = (1-p^{n-1})\zeta(1-n)$$

*für alle $n \in \mathbb{N}$ mit $n \equiv 0 \pmod{p-1}$ erfüllt. Sie heißt p-*adische Riemannsche Zetafunktion.

Beweis: Da die Menge der $n \in \mathbb{N}$ mit $n \equiv 0 \pmod{p-1}$ dicht in $\mathbb{Z}_p \setminus \{1\}$ liegt (vgl. Beweis von Satz 1.3), gibt es höchstens eine solche Funktion. Zur Konstruktion derselben verfahren wir wie in Lemma 1.2 und Satz 1.3: wir setzen $a = 0$, wählen ein beliebiges zu p teilerfremdes $c \neq 1$ und setzen die Funktion

$$f \colon D_0 \longrightarrow \mathbb{Q}, \quad n \longmapsto (1-c^n)(1-p^{n-1})\frac{B_n}{n}$$

zu einer stetigen Funktion $f \colon \mathbb{Z}_p \longrightarrow \mathbb{Q}_p$ fort. Dann definieren wir ζ_p durch

$$\zeta_p \colon \mathbb{Z}_p \setminus \{1\} \longrightarrow \mathbb{Q}_p, \quad 1-n \longmapsto -\frac{f(n)}{1-c^n}.$$

Diese Funktion hat dann offensichtlich die gewünschte Eigenschaft, und wegen der Eindeutigkeit hängt sie nicht von der Wahl von c ab. $\square$

Was macht diese Funktion bei natürlichen Zahlen, die nicht durch $p-1$ teilbar sind?

Satz 1.6: *Es gilt*

$$\zeta_p(1-n) = -(1-\omega^{-n}(p)p^{n-1})\frac{B_{n,\omega^{-n}}}{n}$$

für alle $n \in \mathbb{N}$. Hierbei ist ω der Teichmüller-Charakter, siehe Bemerkung 1.5.2.

Beweis: Es sei n eine beliebige natürliche Zahl. Wir wählen eine Folge von natürlichen Zahlen $(n_k)_{k\in\mathbb{N}}$ in der trivialen Restklasse modulo $p-1$, die in $\mathbb{Z}_p$ gegen n konvergiert, nämlich

$$n_k = n(p^k(p-2)+1) = n\big((p^k-1)^2 - p^{k+1}(p^{k-1}-1)\big).$$

Es gilt nach Korollar 1.5.11

$$-(1-p^{n_k-1})B_{n_k} = -\lim_{j\to\infty}\frac{1}{p^j}\sum_{\substack{a=1\\ p\nmid a}}^{p^j} a^{n_k}.$$

Wir möchten in dieser Gleichung den Grenzübergang $k \to \infty$ ausführen und diesen mit dem Grenzübergang $j \to \infty$ vertauschen. Um zu rechtfertigen, dass wir dies dürfen, müssen wir zeigen, dass die Konvergenz für $j \to \infty$ gleichmäßig bezüglich k ist. Der Übersichtlichkeit halber tun wir dies im nachfolgenden Lemma.

Wenn wir die Grenzwerte bezüglich k und j nun also vertauschen, bekommen wir

$$\lim_{k\to\infty}(1-p^{n_k-1})B_{n_k} = \lim_{j\to\infty}\frac{1}{p^j}\sum_{\substack{a=1\\ p\nmid a}}^{p^j}\lim_{k\to\infty} a^{n_k}.$$

Wegen $n_k = n - np^k + n(p-1)p^k$ gilt in $\mathbb{Z}_p$

$$\lim_{k\to\infty} a^{n_k} = \lim_{k\to\infty} a^n(a^{p^k})^{-n}(a^{p^k})^{(p-1)n} = a^n\omega(a)^{-n}\omega(a)^{(p-1)n} = \omega^{-n}(a)a^n,$$

da $\omega(a)$ eine $(p-1)$-te Einheitswurzel ist. Zusammen mit Definition 1.5.9 erhalten wir daraus

$$\lim_{k\to\infty}(1-p^{n_k-1})B_{n_k} = \lim_{j\to\infty}\frac{1}{p^j}\sum_{\substack{a=1\\ p\nmid a}}^{p^j}\omega^{-n}(a)a^n = B_{n,\omega^{-n}}$$

und damit wie gewünscht

$$\lim_{k\to\infty}\zeta_p(1-n_k) = -\frac{B_{n,\omega^{-n}}}{n}$$

(beachte, dass ω^{-n} Führer p hat, falls n nicht durch $p-1$ teilbar ist). □

Es bleibt die Gleichmäßigkeit der Konvergenz zu zeigen, die es uns erlaubte, die Grenzwerte zu vertauschen. Da diese nicht von der speziellen Gestalt der Folge $(n_k)_{k\in\mathbb{N}}$ abhängt, formulieren wir die Aussage in der folgenden Form:

Lemma 1.7: *Es gilt*

$$\forall\varepsilon>0\,\exists J_\varepsilon\in\mathbb{N}\,\forall j\geq J_\varepsilon\,\forall n\in\mathbb{N}: \left|\frac{1}{p^j}\sum_{\substack{a=1\\ p\nmid a}}^{p^j} a^n - (1-p^{n-1})B_n\right|_p \leq \varepsilon.$$

Beweis: Es seien $n, j \in \mathbb{N}$. Wir benutzen die Notation und die Aussage aus Satz 1.5.8 (wobei wir für χ den trivialen Charakter einsetzen). Setzt man in die Beziehung

$$\sum_{\substack{a=1\\ p\nmid a}}^{p^j} a^n = S_n(p^j) - p^n S_n(p^{j-1})$$

die Formel aus dem Satz ein, erhält man nach ein wenig Rechnen

$$\frac{1}{p^j}\sum_{\substack{a=1\\ p\nmid a}}^{p^j} a^n = \frac{1}{n+1}\sum_{i=1}^{n}\binom{n+1}{i}B_i p^{j(n-i)}(1-p^{i-1}).$$

Ist in der Summe auf der rechten Seite $i = n$, so ist der entsprechende Summand gerade $(n+1)(1-p^{n-1})B_n$, also gilt

$$\begin{aligned}\Big(\frac{1}{p^j}\sum_{\substack{a=1\\ p\nmid a}}^{p^j} a^n - (1-p^{n-1})B_n\Big) &= \frac{1}{n+1}\sum_{i=1}^{n-1}\binom{n+1}{i}B_i p^{j(n-i)}(1-p^{i-1})\\ &= p^j\sum_{i=1}^{n-1}\frac{p^{n-i}}{n+1-i}\binom{n}{i}B_i(1-p^{i-1}).\end{aligned}$$

Diesen Ausdruck müssen wir nun also geeignet abschätzen. Offenbar gilt $\left|\binom{n}{i}\right|_p \leq 1$ und $|1-p^{i-1}|_p = 1$.

Wir zeigen zunächst, dass für alle $i = 1, \dots, n-1$ gilt

$$\left|\frac{p^{n-i}}{n+1-i}\right|_p \leq 1,$$

was zu $v_p(n+1-i) \leq n-i$ äquivalent ist, wenn wir mit v_p die p-adische Bewertung bezeichnen. Für jedes $k \in \mathbb{N}$ ist p^k die kleinste natürliche Zahl, für die v_p den Wert k annimmt. Da stets $p^k \geq k+1$ gilt, muss also $v_p(k+1) \leq k$ sein. Setzen wir hier $k = n-i$ ein, bekommen wir die gewünschte Ungleichung.

Um die Bernoulli-Zahlen abzuschätzen, benutzen wir den *Satz von Clausen-von Staudt*, den wir aus [Was82, Thm. 5.10] zitieren. Er besagt, dass für gerades $n \in \mathbb{N}$

$$B_n + \sum_{(\ell-1)\mid n}\frac{1}{\ell} \in \mathbb{Z}$$

gilt, wobei über alle Primzahlen ℓ summiert wird, sodass $\ell - 1$ ein Teiler von n ist. Da für ungerades n die entsprechende Bernoulli-Zahl 0 ist, folgt daraus insbesondere, dass für alle $n \in \mathbb{N}$ gilt

$$|B_n|_p \leq p.$$

Es sei nun ein $\varepsilon > 0$ gegeben, welches ohne Einschränkung von der Form $\varepsilon = p^{-J}$ mit einem $J \in \mathbb{N}$ ist. Wir setzen dann $J_\varepsilon = J+1$ und haben dann wie gewünscht für $j \geq J_\varepsilon$ und alle $n \in \mathbb{N}$:

$$\Big|\frac{1}{p^j}\sum_{\substack{a=1\\ p\nmid a}}^{p^j} a^n - (1-p^{n-1})B_n\Big|_p \leq p^{-j+1} \leq p^{-J_\varepsilon+1} = \varepsilon. \qquad \square$$

Wir haben nun also für die Riemannsche Zetafunktion ein p-adisches Analogon gefunden. Diese Konstruktion kann in ähnlicher Form für die L-Funktionen von Dirichlet-Charakteren durchgeführt werden. Hierbei muss man allerdings eine Einbettung $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$

wählen, um die verallgemeinerten Bernoulli-Zahlen als p-adische Zahlen, bzw. die Dirichlet-Charaktere als p-adische Dirichlet-Charaktere interpretieren zu können (vgl. Satz I.5.10) – die p-adische L-Funktion hängt dann natürlich von dieser Einbettung ab. In [Iwa72, §3] wird dies durchgeführt, und die Konstruktion ist sogar etwas feiner, sodass wir nicht nur eine stetige Funktion bekommen, sondern sogar eine holomorphe (bzw. meromorphe für den trivialen Charakter), d.h. eine Funktion, die durch eine konvergente Potenzreihe gegeben ist. Das Resultat ist folgendes [Iwa72, Thm. 3.2]:

Satz 1.8: *Es sei χ ein primitiver Dirichlet-Charakter, und es sei eine Einbettung $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ gewählt. Dann gibt es genau eine Funktion $L_p(\chi, s)$, gegeben durch eine Potenzreihe*

$$L_p(\chi, s) = \frac{a_{-1}}{s-1} + \sum_{n=0}^{\infty} a_n (s-1)^n$$

mit $a_n \in \mathbb{Q}_p(\chi)$, die

$$L_p(\chi, 1-n) = (1 - \chi\omega^{-n}(p)p^{n-1}) L(\chi\omega^{-n}, 1-n)$$

für alle $n \in \mathbb{N}$ erfüllt. Die Potenzreihe konvergiert auf

$$\{s \in \mathbb{C}_p : |s-1| < p^{\frac{p}{p-1}}\}$$

(insbesondere also auf $\mathbb{Z}_p$) und es ist $a_{-1} = 0$, falls χ ein nichttrivialer Charakter ist, und sonst $a_{-1} = 1 - \frac{1}{p}$.

Mit Bemerkung I.5.6 folgt sofort, dass die p-adische L-Funktion eines ungeraden Charakters konstant 0 ist. Das ist aber nicht so schlimm, da die verbleibenden L-Funktionen durch die Potenzen des (ungeraden!) Teichmüller-Charakters trotzdem Informationen über Bernoulli-Zahlen von ungeraden Charakteren enthalten.

2. Iwasawas Konstruktion p-adischer Dirichlet-L-Funktionen

Iwasawa hat noch eine alternative Möglichkeit zur Konstruktion der p-adischen L-Funktionen aus Satz 1.8 angegeben, die zu einem besseren Verständnis des Wesens dieser Funktionen führt und für die weitere Verallgemeinerung besonders wichtig ist. Diese ist in [Iwa72, §6] erklärt und soll hier kurz zusammengefasst werden. Ihre grundlegende Idee ist, Stickelberger-Elemente zu verwenden, um zu einem Dirichlet-Charakter ein Element in einer Iwasawa-Algebra zu konstruieren, das uns die p-adische L-Funktion liefert.

Wir wollen uns in diesem Abschnitt auf den Fall einer ungeraden Primzahl beschränken. Diese Einschränkung ist nicht notwendig, die Konstruktion funktioniert auch für $p = 2$, allerdings werden manche Formeln durch $p \neq 2$ etwas einfacher. Außerdem werden wir nur die Konstruktion für einen nichttrivialen Charakter erklären. Diese Einschränkung ist ebenfalls nicht nötig, macht aber die Darstellung etwas übersichtlicher. Wir wählen für den gesamten Abschnitt eine Einbettung $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ und fassen damit alle Dirichlet-Charaktere bei Bedarf als p-adische Charaktere auf.

Definition 2.1: Es sei $K = \mathbb{Q}(\mu_n)$ der n-te Kreisteilungskörper und $G = \mathrm{Gal}(K|\mathbb{Q})$ seine Galoisgruppe. Für ein $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ sei $\sigma_a \in G$ der a zugeordnete Automorphismus von K unter dem natürlichen Isomorphismus $(\mathbb{Z}/n\mathbb{Z})^\times \cong G$. Das *Stickelberger-Element* von K ist[3]

$$\Sigma_K = -\frac{1}{n} \sum_{\substack{a=1 \\ (a,n)=1}}^{n} a\sigma_a^{-1} \in \mathbb{Q}[G].$$

Ein Grund, warum dieses Element interessant ist, ist der *Satz von Stickelberger* [Was82, Thm. 6.10], der besagt, dass das *Stickelberger-Ideal* $I := \mathbb{Z}[G] \cap \Sigma_K \mathbb{Z}[G]$ die Idealklassengruppe von K annuliert, d.h. für jedes gebrochene Ideal $\mathfrak{a}$ von K und jedes $f \in I$ ist $f(\mathfrak{a})$ ein gebrochenes Hauptideal.

Mithilfe solcher Stickelberger-Elemente wollen wir nun die p-adischen L-Funktionen neu konstruieren. Sei dazu p eine ungerade Primzahl und $m \in \mathbb{N}$ zu p teilerfremd. Wir betrachten den Körperturm

$$\mathbb{Q} \subseteq K_0 \subseteq K_1 \subseteq \cdots \subseteq K_\infty = \bigcup_{n \in \mathbb{N}_0} K_n, \quad K_n = \mathbb{Q}(\mu_{mp^n}).$$

Offenbar ist dann

$$\widetilde{G} := \mathrm{Gal}(K_\infty|\mathbb{Q}) \cong \mathbb{Z}_{p,m}^\times,$$

wobei $\mathbb{Z}_{p,m}$ in Definition 1.2.1 definiert wurde.

Wir setzen $\Gamma = 1 + p\mathbb{Z}_p$, $\Delta = (\mathbb{Z}/mp\mathbb{Z})^\times$ und haben dann

$$\widetilde{G} \cong \Delta \times \Gamma$$

nach Lemma 1.2.2. Weiter setzen wir

$$\Gamma_n = \frac{1 + p\mathbb{Z}_p}{1 + p^n\mathbb{Z}_p} \cong \mathbb{Z}/p^{n-1}\mathbb{Z}\,, \quad \widetilde{G}_n = \mathrm{Gal}(K_n|\mathbb{Q})$$

und schreiben

$$\pi_n \colon \widetilde{G}_n \cong \Delta \times \Gamma_n \longrightarrow \Gamma_n$$

für die Projektion auf Γ_n. Den topologischen Erzeuger $1 + mp$ von Γ bezeichnen wir mit γ.

Wir fassen nun $M := \overline{\mathbb{Q}}_p[\![\widetilde{G}]\!]$ als Modul über $\overline{\mathbb{Q}}_p[\Delta]$ auf und zerlegen ihn in Eigenräume

$$M = \bigoplus_{\delta} M_\delta$$

wie in (1.2.2). Nach Lemma 1.2.3 ist dann jeder der Summanden M_δ als $\overline{\mathbb{Q}}_p$-Modul zu $\overline{\mathbb{Q}}_p[\![\Gamma]\!]$ isomorph.

Für jedes $n \in \mathbb{N}$ haben wir das Stickelberger-Element $\Sigma_n := \Sigma_{K_n} \in \mathbb{Q}[\widetilde{G}_n]$. Man rechnet leicht nach, dass diese ein kompatibles System für die natürlichen Abbildungen $\mathbb{Q}[\widetilde{G}_{n+1}] \longrightarrow \mathbb{Q}[\widetilde{G}_n]$ bilden, und dies liefert uns daher ein Element $\Sigma \in \mathbb{Q}[\![\widetilde{G}]\!] \subseteq \overline{\mathbb{Q}}_p[\![\widetilde{G}]\!]$.

[3] In den meisten Texten findet man eine Definition mit entgegengesetzem Vorzeichen. Für uns wird jedoch diese Vorzeichenwahl praktischer sein.

Wir projizieren nun dieses Stickelbergerelement in jeden der Eigenräume M_δ und benutzen den Isomorphismus aus dem vorigen Lemma. Dies liefert uns für jeden Charakter δ von Δ ein zugehöriges Element $\xi_\delta \in \overline{\mathbb{Q}}_p[\![\Gamma]\!]$, welches konkret durch $\xi_\delta = (\xi_{\delta,n})_n$ mit

$$\xi_{\delta,n} = -\frac{1}{mp^n} \sum_{\substack{a=1 \\ (a,mp^n)=1}}^{mp^n} a\delta^{-1}(a)\pi_n(\sigma_a)^{-1} \in \overline{\mathbb{Q}}_p[\Gamma_n]$$

gegeben ist. Offenbar ist ξ_δ bereits ein Element von $K[\![\Gamma]\!]$, wenn K die endliche Erweiterung von $\mathbb{Q}_p$ ist, die von den Werten von δ erzeugt wird.

Wir betrachten nun einen bei p unverzweigten nichttrivialen Dirichlet-Charakter χ, dessen Führer m sei. Auf

$$\Delta = \left(\mathbb{Z}/m\mathbb{Z}\right)^\times \times \mathbb{F}_p^\times$$

betrachten wir die Charaktere

$$\delta_i := \chi^{-1}\omega^i, \quad i = 1, \ldots, p-1$$

und setzen

$$\lambda_{\chi,i} = \xi_{\delta_i}. \tag{2.1}$$

Dies ist ein Element von $K[\![\Gamma]\!]$, wenn K der Erweiterungskörper von $\mathbb{Q}_p$ ist, der von den Werten von χ erzeugt wird.

Lemma 2.2: *Wenn i und χ gerade sind, dann ist $\lambda_{\chi,i} = 0$.*

Beweis: Unter dieser Voraussetzung ist auch δ_i gerade, also gilt in der Summe

$$\xi_{\delta_i,n} = -\frac{1}{mp^n} \sum_{\substack{a=1 \\ (a,mp^n)=1}}^{mp^n} a\delta_i^{-1}(a)\pi_n(\sigma_a)^{-1}$$

jeweils $\delta_i^{-1}(a) = \delta_i^{-1}(-a) = \delta_i^{-1}(mp^n - a)$. Andererseits gilt auch $\pi_n(\sigma_a) = \pi_n(\sigma_{-a})$, da die komplexe Konjugation im Kern von π_n liegt. Wenn man in der Summe die Summanden zu a und $mp^n - a$ zusammenfasst, sieht man damit

$$\xi_{\delta_i,n} = -\frac{1}{2} \sum_{\substack{a=1 \\ (a,mp^n)=1}}^{mp^n} \delta_i^{-1}(a)\pi_n(\sigma_a)^{-1}.$$

Der Koeffizient von $\pi_n(\sigma_a)^{-1}$ in dieser Summe ist für jedes a ein Vielfaches von

$$\sum_{d\in\Delta} \delta_i^{-1}(d).$$

Dies ist das Skalarprodukt von δ_i^{-1} mit dem trivialen Charakter auf Δ, und da δ_i^{-1} ein nichttrivialer Charakter ist (denn χ ist nichttrivial), folgt das Verschwinden dieses Ausdrucks aus der Orthogonalitätsrelation für Charaktere, siehe z.B. [Ser77, Thm. 1.3]. □

Satz 2.3: *Es sei $\mathcal{O}$ der Ganzheitsring in K, und es sei χ ein gerader Charakter. Dann gilt $\lambda_{\chi,i} \in \mathcal{O}[\![\Gamma]\!]$ für alle i.*

Beweis: Für gerades i ist das wegen Lemma 2.2 klar. Für ungerades i ist $\chi\omega^{-(i-1)}$ gerade, und die Aussage folgt dann aus [Was82, Prop. 7.6 (b), (c)] (setze dort $\theta = \chi\omega^{-(i-1)}$). □

Sei also im Folgenden χ gerade. Am Ende des vorherigen Abschnittes hatten wir bemerkt, dass im Falle eines ungeraden χ die zugehörige p-adische L-Funktion verschwindet, sodass dies keine wirkliche Einschränkung darstellt.

Es sei nun $G = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})|\mathbb{Q})$ und $\kappa\colon G \xrightarrow{\sim} \mathbb{Z}_p^\times$ der kanonische Isomorphismus, der auch der *zyklotomische Charakter* genannt wird. Es gilt

$$G \cong \mathbb{F}_p^\times \times \Gamma.$$

Die hiervon induzierte Einbettung

$$\Gamma \hookrightarrow \mathbb{Z}_p^\times \tag{2.2}$$

bezeichnen wir mit $\widetilde{\kappa}$, sodass $\kappa = \omega \times \widetilde{\kappa}$ gilt. Da die Charaktere von $\mathbb{F}_p^\times$ gerade die Potenzen $\omega^1, \ldots, \omega^{p-1}$ des Teichmüller-Charakters sind, haben wir wie in (1.2.2) eine Zerlegung

$$\mathcal{O}[\![G]\!] \cong \bigoplus_{i=1}^{p-1} \varepsilon_i \mathcal{O}[\![G]\!] \quad \text{(wobei } \varepsilon_i = \varepsilon_{\omega^i}\text{)}.$$

Wir bringen nun noch die Isomorphismen

$$\varphi_i\colon \varepsilon_i \mathcal{O}[\![G]\!] \xrightarrow{\sim} \mathcal{O}[\![\Gamma]\!]$$

aus Lemma 1.2.3 ins Spiel und erhalten dann

$$(\varphi_i \circ \varepsilon_i)_i\colon \mathcal{O}[\![G]\!] \xrightarrow{\sim} \bigoplus_{i=1}^{p-1} \mathcal{O}[\![\Gamma]\!]. \tag{2.3}$$

Der hierzu inverse Isomorphismus liefert uns ein zu

$$(\lambda_{\chi,i})_{1 \le i \le p-1} \in \bigoplus_{i=1}^{p-1} \mathcal{O}[\![\Gamma]\!] \tag{2.4}$$

gehörendes Element $\mu_\chi \in \mathcal{O}[\![G]\!]$.

Nun nehmen wir einen beliebigen weiteren Dirichlet-Charakter ψ vom Führer p^r für ein $r \in \mathbb{N}$. Dieser nehme Werte in einer genügend großen Erweiterung K' von K an, und wir bezeichnen mit $\mathcal{O}'$ den Ganzheitsring von K'. Wir fassen ψ via

$$G \xrightarrow{\kappa} \mathbb{Z}_p^\times \twoheadrightarrow \left(\mathbb{Z}/p^r\mathbb{Z}\right)^\times \xrightarrow{\psi} \mathcal{O}'^\times$$

als Charakter von G auf. Damit definieren wir für jede ganze Zahl t einen Homomorphismus

$$G \longrightarrow \mathcal{O}'^\times, \quad a \longmapsto \psi(a)^{-1}\kappa(a)^t.$$

Die universelle Eigenschaft des proendlichen Gruppenrings (vgl. Definition 1.1.15) beschert uns eine eindeutige Fortsetzung zu einem Homomorphismus von $\mathcal{O}$-Algebren

$$\Phi_t^\psi\colon \mathcal{O}[\![G]\!] \longrightarrow \mathcal{O}'. \tag{2.5}$$

Die fundamentale Aussage lautet dann

Satz 2.4: *Es gilt für alle $n \in \mathbb{N}$*

$$\Phi_{1-n}^{\psi}(\mu_\chi) = (1 - \chi\psi(p)p^{n-1})L(\chi\psi, 1-n). \tag{2.6}$$

Beweis: Es sei $t \in \mathbb{Z}$ beliebig. Die Zerlegung $G \cong \mathbb{F}_p^\times \times \Gamma$ liefert eine Zerlegung von ψ in einen Charakter von $\mathbb{F}_p^\times$ und einen von Γ. Den letzteren bezeichnen wir mit η, und ersterer ist eine Potenz des Teichmüller-Charakters ω^j. Wir bezeichnen den von

$$\eta^{-1}\widetilde{\kappa}^t : \Gamma \longrightarrow \mathcal{O}'^\times$$

induzierten $\mathcal{O}$-Algebren-Homomorphismen

$$\mathcal{O}[\![\Gamma]\!] \longrightarrow \mathcal{O}'$$

mit $\widetilde{\Phi}_t^\eta$. Zuerst zeigen wir, dass das Diagramm

$$\begin{tikzcd}
\mathcal{O}[\![G]\!] \arrow[r, two heads] \arrow[d, "\Phi_t^\psi"] & \varepsilon_{t-j}\mathcal{O}[\![G]\!] \arrow[r, "\varphi_{t-j}", "\sim"'] & \mathcal{O}[\![\Gamma]\!] \arrow[dll, "\widetilde{\Phi}_t^\eta"] \\
\mathcal{O}' & &
\end{tikzcd} \tag{2.7}$$

kommutiert. Hierbei sind φ_{t-j} und ε_{t-j} als φ_i und ε_i für das i mit $1 \leq i \leq p-1$ und $i \equiv t - j \pmod{p-1}$ zu verstehen.

Sei dazu $g \in G$. Über die Zerlegung $G = \mathbb{F}_p^\times \times \Gamma$ schreiben wir $g = (a, \gamma)$. Wegen $\psi = \eta \times \omega^j$ gilt $\psi(g) = \omega^j(a)\eta(\gamma)$, also $\eta^{-1}(\gamma) = \psi^{-1}(g)\omega^j(a)$. Weiter gilt $\varphi_{t-j}(\varepsilon_{t-j}g) = \omega^{t-j}(a)\gamma$ (vgl. Beweis von Lemma 1.2.3). Damit folgt

$$\widetilde{\Phi}_t^\eta(\varphi_{t-j}(\varepsilon_{t-j}g)) = \omega^{t-j}(a)\eta^{-1}(\gamma)\widetilde{\kappa}^t(\gamma) = \psi^{-1}(g)\omega^t(a)\widetilde{\kappa}^t(\gamma) = \Phi_t^\psi(g).$$

Aufgrund der Kommutativität des Diagramms (2.7) und der Definition von μ_χ gilt nun

$$\Phi_t^\psi(\mu_\chi) = \widetilde{\Phi}_t^\eta(\lambda_{\chi,t-j}).$$

Nach Definition gilt $\lambda_{\chi,t-j} = 0$, falls $t - j$ gerade ist. Wenn wir hier $t = 1 - n$ einsetzen, ist $t - j$ genau dann gerade, wenn $n \not\equiv j \pmod 2$. Die Parität von $\psi = \omega^j \times \eta$ ist die von j, da η als Charakter auf Γ gerade ist. Da nach Voraussetzung auch χ gerade ist, sind in diesem Fall die Paritäten von $\chi\psi$ und n entgegengesetzt. Nach Bemerkung 1.5.6 ist in diesem Fall $L(\chi\psi, 1-n) = 0$. Wir können uns also im Folgenden auf den Fall zurückziehen, dass $t - j$ ungerade und damit $\lambda_{\chi,t-j}$ nichttrivial ist.

Nun benutzen wir ein Resultat aus [Iwa72, §6]. Iwasawa zerlegt dort (S. 66) einen beliebigen Dirichlet-Charakter in einen ersten und zweiten Faktor. Wenn man das auf $\beta_t = \chi\omega^{j-t+1}\eta$ anwendet, ist der erste Faktor $\chi\omega^{j-t+1}$ und der zweite ist η. Auf S. 70 definiert Iwasawa einen Homomorphismus Φ_t, der unser $\widetilde{\Phi}_{-t}^\eta$ ist. Auf S. 76 wird weiter ein Element ξ_∞ definiert, welches in unserer Notation $\xi_{(\chi\omega^{j-t+1})^{-1}\omega} = \xi_{\chi^{-1}\omega^{t-j}} = \lambda_{\chi,t-j}$ ist. Die Lemmata 2 und 3 bei Iwasawa zeigen für $t = 1 - n$

$$\widetilde{\Phi}_t^\eta(\lambda_{\chi,t-j}) = -(1 - \beta_{1-n}\omega^{-n}(p)p^{n-1})\frac{B_{n,\beta_{1-n}\omega^{-n}}}{n}.$$

Wegen
$$\beta_{1-n}\omega^{-n} = \chi\omega^{j-(1-n)+1}\eta\omega^{-n} = \chi\omega^j\eta = \chi\psi$$
folgt daraus die Behauptung. □

Satz 2.5: *Das Element $\mu_\chi \in \mathcal{O}[\![G]\!]$ ist durch (2.6) eindeutig bestimmt.*

Beweis: Wenn es zwei solche Elemente gibt, liegt ihre Differenz im Kern aller Φ^{ψ}_{1-n} für alle $n \in \mathbb{N}$. Es genügt also zu zeigen
$$\bigcap_n \operatorname{Kern} \Phi^{\psi}_{1-n} = 0.$$
Wir benutzen das kommutative Diagramm (2.7) und zeigen stattdessen
$$\bigcap_n \operatorname{Kern} \widetilde{\Phi}^{\eta}_{1-n} = 0.$$
Dies genügt wegen des Isomorphismus' (2.3).

Ein Element in diesem Schnitt entspricht via dem Isomorphismus $\mathcal{O}[\![\Gamma]\!] \cong \mathcal{O}[\![T]\!]$ einer Potenzreihe f. Da die Komposition
$$\mathcal{O}[\![T]\!] \xrightarrow{\sim} \mathcal{O}[\![\Gamma]\!] \xrightarrow{\widetilde{\Phi}^{\eta}_t} \mathcal{O}$$
durch
$$f \longmapsto f(\eta(\gamma)^{-1}\widetilde{\kappa}(\gamma)^t - 1) \tag{2.8}$$
gegeben ist, gilt dann
$$f(\eta(\gamma)^{-1}\widetilde{\kappa}(\gamma)^{1-n} - 1) = 0$$
für alle n. Insbesondere hat also f unendlich viele Nullstellen. Mit Korollar 1.2.10 folgt dann $f = 0$. □

Bemerkung 2.6: Wir haben bei unseren bisherigen Betrachtungen den trivialen Charakter χ^0 ausgeschlossen. Dies geschah vornehmlich aus Bequemlichkeit und um die Darstellung übersichtlich zu halten. Die Konstruktion, die wir erklärt haben, funktioniert aber für den trivialen Charakter ganz ähnlich. Was sich dabei ändert, ist die Aussage aus Satz 2.3: die Elemente $\lambda_{\chi,i}$ liegen dann nur für $i \neq 1$ in $\mathcal{O}[\![\Gamma]\!]$, für $i = 1$ ist $\lambda_{\chi,1}$ ein Element des Quotientenkörpers von $\mathcal{O}[\![\Gamma]\!]$. Dessen Nenner können wir aber explizit angeben: wenn wir
$$h = 1 - \frac{\widetilde{\kappa}(\gamma)}{1+T} \in \mathcal{O}[\![T]\!] \cong \mathcal{O}[\![\Gamma]\!]$$
setzen, gilt $h\lambda_{\chi,1} \in \mathcal{O}[\![\Gamma]\!]$ [Was82, Prop. 7.6 (a) und S. 122].

Wenn wir in (2.8) $f = h$ einsetzen, sehen wir, dass dieser Wert genau dann 0 wird, $\eta = \widetilde{\kappa}^{t-1}$ gilt. Wenn wir das Bild von
$$(h, 1, \ldots, 1) \in \bigoplus_{i=1}^{p-1} \mathcal{O}[\![\Gamma]\!]$$

in $\mathcal{O}[\![G]\!]$ mit g bezeichnen (vgl. (2.3)), sehen wir damit und mithilfe des Diagramms (2.7) leicht, dass $\Phi_t^\psi(g) = 0$ genau dann gilt, wenn $\psi = \kappa^{t-1}$.

Wenn wir also $\psi \neq \kappa^{t-1}$ fordern und μ_{χ^0} wie gehabt definieren, können wir für die verbleibenden t und ψ

$$\Phi_t^\psi(\mu_{\chi^0}) := \frac{\Phi_t^\psi(g\mu_{\chi^0})}{\Phi_t^\psi(g)} \in K$$

definieren. Wenn $\psi = \kappa^{t-1}$ gilt, ist entweder $t = 1$ und ψ trivial, oder ψ hat unendliche Ordnung. Beides ist in Satz 2.4 ausgeschlossen (dort ist $t = 1 - n$ und $n \in \mathbb{N}$). Also ist $\Phi_{1-n}^\psi(\mu_{\chi^0})$ für ψ und n wie dort stets wohldefiniert, und die Aussagen der Sätze 2.4 und 2.5 gelten dann ganz genauso (dies wird in [Iwa72, §6] ebenfalls gezeigt).

Der nächste Abschnitt wird uns eine Möglichkeit an die Hand geben, die hier konstruierten Elemente μ_χ in einem neuen Licht zu betrachten. Dies werden wir in Satz 4.1 tun und anschließend erklären, wie wir hieraus die Funktion aus Satz 1.8 zurückgewinnen (wir könnten das auch hier schon sehen, aber später lässt es sich eleganter ausdrücken).

3. Maße und Integrale

In diesem Abschnitt soll p-adische Maß- und Integrationstheorie für proendliche Räume entwickelt werden. Wir betrachten hier jedoch keine σ-additiven Maße, sondern nur endlich additive, d.h. es handelt sich nach der üblichen Terminologie um Inhalte. Diese sind auch nicht auf der vollen Borel-σ-Algebra eines proendlichen Raumes definiert, sondern auf den Teilmengen, die zugleich offen und abgeschlossen sind. Diese bilden immerhin einen *Ring*, d.h. sie sind abgeschlossen unter endlichen Durchschnitten und Bilden der symmetrischen Differenz, und sie enthalten nach Satz I.1.8 (a) eine Basis der Topologie. Für unsere Zwecke werden solche Inhalte ausreichen.

Die Theorie p-adischer Maße wurde von Mazur in [MS74] eingeführt. Dort wurden etwas andere Bezeichnungen verwendet, die in der Literatur üblich geworden sind und an die wir uns deshalb halten werden.

3.1. Integrale

Definition 3.1: Sei X ein proendlicher Raum und $R \subseteq \mathcal{P}(X)$ der Ring der offen-abgeschlossenen Teilmengen. Weiter sei W eine abelsche Gruppe. Eine *Distribution*[4] auf X mit Werten W ist eine Funktion

$$\mu \colon R \longrightarrow W,$$

die *endlich additiv* ist, d.h. für disjunkte $A, B \in R$ gilt $\mu(A \cup B) = \mu(A) + \mu(B)$.

Wenn W ein normierter Vektorraum ist und die Distribution μ beschränkt ist (d.h. die Menge der $|\mu(A)|$ für $A \in R$ ist beschränkt), dann nennen wir sie ein *Maß*.

Die Menge der W-wertigen Distributionen auf X bezeichnen wir mit $\mathrm{Dist}(X, W)$; dies ist eine abelsche Gruppe. Offenbar erfüllt jede Distribution $\mu(\varnothing) = 0$.

Sei nun K eine endliche Erweiterung von $\mathbb{Q}_p$ und W ein K-Banachraum, d.h. ein K-Vektorraum, der mit einer homogenen ultrametrischen Norm $|\cdot|$ versehen ist und bezüglich

[4] Nach der üblichen Terminologie ein *Inhalt*.

dieser vollständig ist. Ein wichtiges Beispiel ist der Fall $W = \mathbb{C}_p$. Sei weiter μ ein Maß auf einem proendlichen Raum X mit Werten in W. Wir wollen das Integral einer stetigen Funktion $X \longrightarrow W$ bezüglich des Maßes μ erklären. Dabei gehen wir ähnlich vor wie bei der Konstruktion des Lebesgue-Integrals.

Sei dazu $C(X, W)$ der K-Vektorraum der stetigen Funktionen von X nach W und $S(X, W)$ der Unterraum der *einfachen Funktionen*, d.h.

$$S(X, W) = \{f \in C(X, W) : f \text{ nimmt nur endlich viele Werte an}\}.$$

Wir versehen $C(X, W)$ mit der Supremumsnorm

$$\|f\| = \sup_{x \in X} |f(x)|.$$

Damit wird $C(X, W)$ zu einem Banachraum.

Jede einfache Funktion $f \in S(X, W)$ lässt sich als W-Linearkombination von charakteristischen Funktionen

$$f = \sum_{i=1}^{n} x_i \mathbb{1}_{A_i}$$

mit $A_i \in R$ und $x_i \in W$ schreiben: denn wenn $x_1, \ldots, x_n$ die paarweise verschiedenen endlich vielen Werte sind, können wir $A_i = f^{-1}(x_i)$ wählen. Da f stetig und W hausdorffsch ist, sind die A_i jeweils offen und abgeschlossen, also Elemente von R. Für eine solche Darstellung definieren wir das Integral von f bezüglich μ durch

$$\int_X f \,\mathrm{d}\mu = \sum_{i=1}^{n} x_i \mu(A_i).$$

Es ist wegen der Additivität von μ klar, dass dies nicht von der Wahl der Linearkombination abhängt. Dies definiert einen Homomorphismus von K-Vektorräumen[5]

$$i_\mu \colon S(X, W) \longrightarrow W, \quad f \longmapsto \int_X f \,\mathrm{d}\mu.$$

Lemma 3.2: *(a) $S(X, W)$ liegt dicht in $C(X, W)$.*

(b) Der Homomorphismus i_μ ist Lipschitz-stetig mit der Lipschitz-Konstanten[6]

$$C = \sup_{A \in R} |\mu(A)|.$$

Beweis: (a) Sei ein $\varepsilon > 0$ und eine stetige Funktion $f : X \longrightarrow W$ gegeben. Für jedes w im Bild von f sei $B(w, \varepsilon) \subseteq W$ die Kugel mit Radius ε um w. Diese ist offen und abgeschlossen, da W ein ultrametrischer Raum ist. Wir setzen $U_w = f^{-1}(B(w, \varepsilon))$, was dann ebenfalls offen und abgeschlossen, also ein Element von R ist. Die U_w bilden offensichtlich eine offene Überdeckung von X, und da X kompakt ist (Satz 1.1.8 (a)),

[5] Zusammen mit dem folgenden Lemma rechtfertigt dies die Bezeichnung *Distribution*.

[6] Hier brauchen wir zum ersten Mal, dass μ ein Maß ist. Davor funktioniert alles auch für Distributionen.

können wir endlich viele $w_1, \dots, w_n$ wählen, sodass die zugehörigen U_{w_i} eine Überdeckung von X sind. Wir machen diese disjunkt, indem wir

$$A_i = U_{w_i} \setminus \bigcup_{j=i+1}^{n} U_{w_j}, \quad i = 1, \dots, n$$

setzen (beachte, dass immer noch $A_i \in R$ gilt), und definieren eine einfache Funktion

$$f_0 = \sum_{i=1}^{n} w_i \mathbb{1}_{A_i}.$$

Es gilt dann

$$\left\|f - f_0\right\| = \sup_{x \in X} \left|f(x) - f_0(x)\right| = \max_{i=1,\dots,n} \sup_{x \in A_i} \left|f(x) - w_i\right| \leq \varepsilon.$$

(b) Es seien zwei einfache Funktionen

$$f = \sum_{i=1}^{n} x_i \mathbb{1}_{A_i}, \quad g = \sum_{i=1}^{n} y_i \mathbb{1}_{A_i}$$

gegeben, wobei wir ohne Einschränkung annehmen, dass die Mengen A_i in der Linearkombination von charakteristischen Funktionen die gleichen sind. Es gilt dann unter Benutzung der ultrametrischen Dreiecksungleichung

$$\begin{aligned} \left|\int_X f \mathrm{d}\mu - \int_X g \mathrm{d}\mu\right| &= \left|\sum_{i=1}^{n} (x_i - y_i)\mu(A_i)\right| \\ &\leq C \cdot \max_{i=1,\dots,n} \left|x_i - y_i\right| = C \cdot \sup_{x \in X} \left|f(x) - g(x)\right| = C \cdot \left\|f - g\right\|. \end{aligned}$$ □

Aus Lemma 3.2 folgt sofort, dass sich i_μ zu einem eindeutigen Homomorphismus

$$C(X, W) \longrightarrow W$$

fortsetzt. Für das Bild einer stetigen Funktion $f : X \longrightarrow W$ unter diesem Homomorphismus schreiben wir dann ebenfalls

$$\int_X f \mathrm{d}\mu.$$

3.2. Maße auf proendlichen Räumen

Wir wollen nun überlegen, welche Maße und Distributionen es auf einem proendlichen Raum geben kann. Dazu nehmen wir zunächst wieder an, dass W nur eine abelsche Gruppe ist. Wir schreiben

$$X = \lim_{i \in I} X_i$$

als Limes von endlichen diskreten Räumen und bezeichnen mit π_i die kanonische Projektion $X \longrightarrow X_i$. Ist nun μ eine W-wertige Distribution auf X, so induziert dies für jedes i eine Distribution μ_i auf X_i durch $\mu_i(A) = \mu(\pi_i^{-1}(A))$.

Eine Distribution (oder ein Maß) auf einer endlichen Menge X_i mit Werten in W ist offenbar nichts anderes als eine Abbildung $\mu_i\colon X_i \longrightarrow W$: für eine beliebige Teilmenge $A \subseteq X_i$ kann man dann $\mu_i(A) = \sum_{a\in A} \mu_i(a)$ setzen, dies definiert dann ein W-wertiges Maß auf X_i und jedes W-wertige Maß kommt so zustande.

Die Maße μ_i, die wir wie eben beschrieben als Abbildungen $X_i \longrightarrow W$ auffassen, erfüllen offenbar die folgende Kompatibilitätsrelation:

$$\mu_j(a) = \sum_{b\in f_{ij}^{-1}(a)} \mu_i(b) \text{ für } i \geq j. \tag{3.1}$$

Wenn wir für $i \geq j$ eine Abbildung $N_{ij}\colon \operatorname{Meas}(X_i, W) \longrightarrow \operatorname{Meas}(X_j, W)$ durch $N_{ij}(\mu_i) = \mu_j$ wie in (3.1) definieren, erhalten wir dadurch eine Abbildung

$$\operatorname{Dist}(X, W) \longrightarrow \varprojlim_i \operatorname{Dist}(X_i, W),$$

wobei der Limes auf der rechten Seite bezüglich der Abbildungen N_{ij} gebildet wird.

Satz 3.3: *Die natürliche Abbildung*

$$\operatorname{Dist}(X, W) \longrightarrow \varprojlim_i \operatorname{Dist}(X_i, W)$$

ist eine Bijektion.

Beweis: Wir zeigen dies, indem wir eine Umkehrabbildung konstruieren. Wenn eine im Sinne von (3.1) kompatible Familie $(\mu_i)_i$ von Abbildungen $X_i \longrightarrow W$ gegeben ist, so legt dies den Wert der zu definierenden Distribution $\mu \in \operatorname{Dist}(X, W)$ für Mengen der Form

$$U = \Big(\prod_{m\in M} U_m \times \prod_{i\notin M} X_i\Big) \cap X, \quad M \subseteq I \text{ endlich}, A_m \subseteq X_m \text{ beliebig} \tag{$*$}$$

fest: denn dann muss

$$\mu(U) = \sum_{u\in\pi_{i_0}(U)} \mu_{i_0}(u)$$

gelten, wobei i_0 eine obere Schranke von M ist. Da M endlich ist und die Indexmenge I gerichtet geordnet ist, existiert ein solches i_0, und wegen der Kompatibilitätsbedingung (3.1) hängt die rechte Seite nicht von der Wahl von i_0 ab.

Die Mengen der Form ($*$) bilden eine Basis der Topologie auf X. Wenn nun eine beliebige offene und abgeschlossene Teilmenge $A \subseteq X$ gegeben ist, können wir diese also als Vereinigung von Mengen der Form ($*$) schreiben, und da A abgeschlossen und damit kompakt ist, reicht eine Vereinigung endlich vieler solcher $U_1, \ldots, U_n$. Weiter sieht man leicht, dass der Schnitt zweier Mengen der Form ($*$) wieder von dieser Form ist. Wir definieren dann durch eine Inklusions-Exklusions-Formel

$$\mu(A) = \sum_{k=1}^{n} (-1)^{k+1} \sum_{\substack{J\subseteq\{1,\ldots,n\}\\ \#J=k}} \mu\Big(\bigcap_{j\in J} A_j\Big).$$

Nun muss man sich überlegen, dass dies nicht von der Wahl der Zerlegung von A abhängt, dass das so definierte μ eine Distribution ist, und dass die Zuordnung $(\mu_i)_i \longmapsto \mu$ eine Umkehrabbildung definiert. Darauf soll hier verzichtet werden. □

Besondere Bedeutung wird dem Falle zukommen, dass der proendliche Raum X eine proendliche Gruppe $G = \lim_i G_i$ ist, etwa eine Galoisgruppe, und W eine Banachalgebra über einer endlichen Erweiterung K von $\mathbb{Q}_p$ (z.B. einfach K selbst, oder $\mathbb{C}_p$). Dann können wir $\mathrm{Dist}(X, W)$ auf naheliegende Weise zu einem W-Modul machen. Wenn wir weiter für zwei Distributionen μ und ν ihre Faltung $\mu * \nu$ durch

$$\int_G f \mathrm{d}(\mu * \nu) = \int_G \int_G f(xy) \mathrm{d}\mu(x) \mathrm{d}\nu(y)$$

für $f \in S(G, W)$ definieren, gibt dies $\mathrm{Dist}(X, W)$ eine Struktur als W-Algebra.

Korollar 3.4: *Es gibt einen kanonischen Isomorphismus von W-Algebren*

$$\mathrm{Dist}(G, W) \xrightarrow{\sim} W[\![G]\!].$$

Beweis: Es besteht eine Bijektion (von Mengen) zwischen $\mathrm{Dist}(G_i, W)$ und dem Gruppenring $W[G_i]$. Außerdem überlegt man sich leicht, dass die durch (3.1) definierten Abbildungen N_{ij} gerade den natürlichen Abbildungen $W[G_i] \longrightarrow W[G_j]$ für $i \geq j$ entsprechen. Damit folgt die Bijektivität sofort aus Satz 3.3. Dass die W-Algebren-Struktur respektiert wird, kann leicht nachgerechnet werden. □

Beispiel 3.5: Das Bild eines $g \in G$ unter dem kanonischen Homomorphismus $G \longrightarrow W[\![G]\!]^\times$ ist das Dirac-Maß bei g.

Offensichtlich ist jede K-wertige Distribution $\mu \in \mathrm{Dist}(G, K)$ auf einer proendlichen Gruppe G, die Werte in $\mathcal{O}$ annimmt, stets ein Maß. Das Bild der solchen Distributionen in $K[\![G]\!]$ unter dem Isomorphismus aus Korollar 3.4 ist offensichtlich $\mathcal{O}[\![G]\!]$. Deshalb können wir die Elemente der Iwasawa-Algebra einer proendlichen Gruppe G stets als Maße auf G auffassen.

Beispiel 3.6: Wenn $\chi \colon G \longrightarrow K^\times$ ein stetiger Charakter ist, so gilt wegen Beispiel 3.5 für alle $g \in G$

$$\int_G \chi \mathrm{d}g = \chi(g).$$

Dies zeigt, dass der von χ durch die universellen Eigenschaft des proendlichen Gruppenrings $\mathcal{O}[\![G]\!]$ induzierte $\mathcal{O}$-Algebren-Homomorphismus $\mathcal{O}[\![G]\!] \longrightarrow K$ durch

$$\mu \longmapsto \int_G \chi \mathrm{d}\mu$$

gegeben ist.

3.3. Pseudo-Maße

Es sei nun G eine kommutative proendliche Gruppe, K weiterhin eine endliche Erweiterung von $\mathbb{Q}_p$ mit Ganzheitsring $\mathcal{O}$ und $Q = \operatorname{Quot} \mathcal{O}[\![G]\!]$ der totale Quotientenring von $\mathcal{O}[\![G]\!]$. Der in Beispiel 3.6 von einem Charakter induzierte Homomorphismus $\Phi\colon \mathcal{O}[\![G]\!] \longrightarrow K$ setzt sich auf ein Element $\frac{a}{b} \in Q$ fort, wenn $b \notin \operatorname{Kern} \Phi$.

Definition 3.7: Ein Element $\mu \in Q$ heißt *Pseudo-Maß* auf G mit Werten in $\mathcal{O}$, wenn $(g-1)\mu \in \mathcal{O}[\![G]\!]$ für alle $g \in G$ gilt.

Für Pseudo-Maße $\mu = \frac{a}{b}$ ist $b \notin \operatorname{Kern} \Phi$ stets erfüllt, falls Φ wie in Beispiel 3.6 von einem *nichttrivialen* Charakter χ induziert wird: denn $(g-1)\mu \in \mathcal{O}[\![G]\!]$ für alle $g \in G$ bedeutet, dass es für jedes g ein $c_g \in \mathcal{O}[\![G]\!]$ gibt mit $g - 1 = c_g b$. Wenn wir uns ein $g \in G$ mit $\chi(g) \neq 1$ wählen, dann gilt $\Phi(b)\Phi(c_g) = \Phi(g-1) = \chi(g) - 1 \neq 0$ und deshalb $\Phi(b) \neq 0$. Wir können also bezüglich eines Pseudo-Maßes zwar nicht beliebige stetige Funktionen $G \longrightarrow \mathcal{O}$ integrieren, aber immerhin stetige nichttriviale Charaktere $\chi\colon G \longrightarrow K^\times$. Das Integral von χ bezüglich eines Pseudo-Maßes μ ist dann durch

$$\int_G \chi \mathrm{d}\mu = \frac{1}{\chi(g) - 1} \int_G \chi \mathrm{d}((g-1)\mu)$$

gegeben, wobei $g \in G$ ein beliebiges Element mit $\chi(g) \neq 1$ ist. Es ist klar, dass dieser Wert nicht von der Wahl von g abhängt.

3.4. Amice-Transformation

Wir wollen zum Schluss dieses Abschnittes noch einmal den Zusammenhang zwischen der Iwasawa-Algebra, Potenzreihen und Maßen herausstellen. Sei dazu nach wie vor K eine endliche Erweiterung von $\mathbb{Q}_p$, $\mathcal{O}$ der Ganzheitsring, Γ eine proendliche Gruppe, die zu $\mathbb{Z}_p$ isomorph ist, und $\gamma \in \Gamma$ ein topologischer Erzeuger.

Für eine natürliche Zahl n bezeichnen wir mit $\binom{X}{n}$ das Polynom

$$\binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n!} \in \mathbb{Q}[X]$$

und setzen $\binom{X}{0} = 1$. Die hierdurch auf $\mathbb{Z}$ definierte Polynomfunktion nimmt stets ganzzahlige Werte an: für natürliche Zahlen ist das klar, und man sieht leicht, dass

$$\binom{m}{n} = (-1)^n \binom{n-m-1}{n}$$

für $m \in \mathbb{Z}$ gilt. Da sie durch ein Polynom gegeben ist, ist sie stetig bzgl. des p-adischen Betrags, und sogar gleichmäßig stetig, da sie beschränkt ist. Wir erhalten also als Fortsetzung eine gleichmäßig stetige Funktion

$$\binom{\cdot}{n}\colon \mathbb{Z}_p \longrightarrow \mathbb{Z}_p, \quad x \longmapsto \binom{x}{n}.$$

Wir haben Isomorphismen von $\mathcal{O}$-Algebren

$$\operatorname{Dist}(\Gamma, \mathcal{O}) \cong \mathcal{O}[\![\Gamma]\!] \cong \mathcal{O}[\![T]\!].$$

Lemma 3.8: *Der Isomorphismus*

$$A\colon \operatorname{Dist}(\Gamma, \mathcal{O}) \xrightarrow{\sim} \mathcal{O}[\![T]\!]$$

ist durch

$$\mu \longmapsto \sum_{n=0}^{\infty} c_n(\mu) T^n \qquad \textit{mit } c_n(\mu) = \int_\Gamma \binom{\cdot}{n} \mathrm{d}\mu$$

gegeben. Hierbei benutzen wir die durch die Wahl des topologischen Erzeugers γ festgelegte Identifikation von Γ mit $\mathbb{Z}_p$, um $\binom{\cdot}{n}$ als Funktion auf Γ aufzufassen.

Beweis: Es sei μ das Maß auf Γ, das dem topologischen Erzeuger γ unter dem Isomorphismus $\mathcal{O}[\![\Gamma]\!] \xrightarrow{\sim} \operatorname{Dist}(\Gamma, \mathcal{O})$ zugeordnet wird. Da A durch das Bild von μ bereits eindeutig festgelegt ist und die Komposition

$$\operatorname{Dist}(\Gamma, \mathcal{O}) \xrightarrow{\sim} \mathcal{O}[\![\Gamma]\!] \xrightarrow{\sim} \mathcal{O}[\![T]\!]$$

μ auf $1+T$ abbildet (vgl. Satz I.2.15), genügt es zu zeigen, dass die oben angegebene Zuordnung μ auf $1+T$ abbildet.

Das Maß μ ist nach Beispiel 3.5 das Dirac-Maß bei γ, und γ wird von dem Isomorphismus $\Gamma \xrightarrow{\sim} \mathbb{Z}_p$ auf 1 abgebildet. Daraus folgt sofort

$$c_n(\mu) = \int_\Gamma \binom{\cdot}{n} \mathrm{d}\mu = \binom{1}{n}$$

und damit die Behauptung. □

Hieraus folgt sofort die folgende Verallgemeinerung des binomischen Lehrsatzes: in $\mathcal{O}[\![T]\!]$ gilt für alle $s \in \mathbb{Z}_p$

$$(1+T)^s = \sum_{n=0}^{\infty} \binom{s}{n} T^n.$$

Damit können wir den Isomorphismus A auch in der Form

$$A(\mu) = \int_\Gamma (1+T)^s \mathrm{d}\mu(s)$$

schreiben.

Definition 3.9: Für ein Maß μ heißt $A(\mu) \in \mathcal{O}[\![T]\!]$ die *Amice-Transformation* von μ. Von manchen Autoren wird sie auch als *Mahler-Transformation* bezeichnet.

An Lemma 3.8 sieht man, dass ein Maß μ durch die Folge der $c_n(\mu)$, $n \in \mathbb{N}_0$ bereits eindeutig festgelegt ist. Da diese durch Integrale von Polynomfunktionen gegeben sind und das Integral linear ist, folgt daraus sofort:

Korollar 3.10: *Ein Maß $\mu \in \operatorname{Dist}(\Gamma, \mathcal{O})$ ist durch die Integrale aller Monome*

$$\int_\Gamma x^n \mathrm{d}\mu(x), \quad n \in \mathbb{N}_0$$

eindeutig bestimmt.

4. p-adische Dirichlet-L-Funktionen als Maße

Wir wollen die Ergebnisse aus Abschnitt 2 nun maßtheoretisch formulieren. Sei dazu erneut $\mathcal{O}$ der Ganzheitsring einer endlichen Erweiterung von $\mathbb{Q}_p$ und χ ein bei p unverzweigter Dirichlet-Charakter von Führer m mit Werten in $\mathcal{O}^\times$. Ferner sei wieder $G = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})|\mathbb{Q})$ und $\kappa\colon G \xrightarrow{\sim} \mathbb{Z}_p^\times$ der zyklotomische Charakter. Gemäß Korollar 3.4 können wir das in Abschnitt 2 konstruierte Element μ_χ der Iwasawa-Algebra $\mathcal{O}[\![G]\!]$ als Maß auf G auffassen. Wegen Beispiel 3.6 können wir die Aussage der Sätze 2.4 und 2.5 auch in der folgenden Form formulieren:

Satz 4.1: *Es sei χ ein bei p unverzweigter nichttrivialer Dirichlet-Charakter. Dann gibt es genau ein Maß μ_χ auf G, sodass für alle $n \in \mathbb{N}$ und alle Dirichlet-Charaktere ψ von p-Potenz-Führer gilt:*

$$\int_G \psi^{-1}\kappa^{1-n}\mathrm{d}\mu_\chi = (1-\chi\psi(p)p^{n-1})L(\chi\psi, 1-n). \tag{4.1}$$

In vielen Texten findet man auch die folgende, ähnlich aussehende Formulierung: es gibt genau ein Maß μ'_χ auf G, sodass für n und ψ wie oben gilt

$$\int_G \psi\kappa^n\mathrm{d}\mu'_\chi = (1-\chi\psi(p)p^{n-1})L(\chi\psi, 1-n). \tag{4.2}$$

Wir wollen kurz erklären, wie diese Aussage mit der aus Satz 4.1 zusammenhängt. Dazu setzen wir wie in Abschnitt 2 $\Gamma = 1 + p\mathbb{Z}_p$, $\gamma = 1 + mp$, $\Lambda = \mathcal{O}[\![\Gamma]\!]$ und $\widetilde{\kappa}$ wie in (2.2). In (2.4) haben wir das Maß μ_χ als Element von

$$\bigoplus_{i=1}^{p-1} \Lambda$$

definiert. Wir definieren nun eine Involution ν von $\Lambda \cong \mathcal{O}[\![T]\!]$ durch

$$\nu\colon \Lambda \longrightarrow \Lambda, \quad T \longmapsto \widetilde{\kappa}(\gamma)(1+T)^{-1} - 1 \tag{4.3}$$

und definieren $\mu'_\chi = \nu(\mu_\chi)$, indem wir ν in jeder Komponente $i = 1, \dots, p-1$ anwenden. Eine leichte Rechnung zeigt, dass dann

$$\int_G \psi\kappa^n\mathrm{d}\mu'_\chi = \int_G \psi^{-1}\kappa^{1-n}\mathrm{d}\mu_\chi$$

gilt (etwa indem man in (2.8) ν anwendet).

Für den trivialen Charakter gibt es die folgende Variante der Aussage (siehe auch [CS06, Prop. 4.2.4]):

Satz 4.2: *Es gibt genau ein Pseudo-Maß μ'_ζ auf G, sodass für alle $n \in \mathbb{N}$ und alle Dirichlet-Charaktere ψ von p-Potenz-Führer*

$$\int_G \psi\kappa^n\mathrm{d}\mu'_\zeta = (1-p^{n-1})L(\psi, 1-n).$$

Beweis: Wir benutzen Bemerkung 2.6 und definieren

$$\mu'_\zeta = \nu(\mu_{\chi^0}).$$

Man rechnet leicht nach, dass $\nu(h) = -T$, was unter dem Isomorphismus $\mathcal{O}[\![T]\!] \xrightarrow{\sim} \mathcal{O}[\![\Gamma]\!]$ auf $1 - \gamma$ abgebildet wird. Deshalb ist μ'_ζ ein Pseudomaß. Die Aussage folgt dann aus dem, was in Bemerkung 2.6 erwähnt wurde. □

Dass wir hier nur ein Pseudo-Maß anstelle eines Maßes bekommen, spiegelt die Tatsache wider, dass die Riemannsche Zetafunktion im Gegensatz zu den Dirichletschen L-Funktionen einen Pol hat. Wir haben diesen Satz hier in der zu (4.2) passenden Form formuliert, da die Eigenschaft, Pseudo-Maß zu sein, leider nicht invariant unter ν ist – dementsprechend ist $\mu_\zeta := \nu(\mu'_\zeta)$ kein Pseudo-Maß.

Iwasawas Konstruktion liefert also für jeden Dirichlet-Charakter χ ein (Pseudo-)Maß auf der Galoisgruppe G des Körpers aller p-Potenz-Einheitswurzeln, dessen Integrale spezielle Werte der komplexen L-Funktion des Charakters mitsamt aller Twists mit Charakteren von p-Potenz-Führer interpolieren. In diesem Sinne sollte man die p-adischen L-Funktionen eigentlich als Funktionen auf der *Charaktergruppe* $X_p = \mathrm{Hom}(G, \mathbb{C}_p)$ von G auffassen und nicht als Funktionen auf $\mathbb{Z}_p$, ähnlich wie man klassische L-Funktionen als Funktionen auf der Charaktergruppe der Idelgruppe eine Zahlkörpers ansehen kann (vgl. Tate's Thesis, [Tat67a, Def. 4.4.1 und §4.5]). Eine solche p-adische L-Funktion ist durch ein Element μ_χ in der Iwasawa-Algebra $\mathcal{O}[\![G]\!]$ von G bestimmt und durch

$$X_p \longrightarrow \mathbb{C}_p, \quad x \longmapsto \int_G x \mathrm{d}\mu_\chi$$

gegeben. Die Funktion, die zur Riemannschen Zetafunktion gehört, hat einen Pol beim trivialen Charakter (nämlich für $\psi = \kappa^{-n}$, wie wir in Bemerkung 2.6 angemerkt hatten).

Wir können $\mathbb{Z}_p$ als Teilmenge von X_p auffassen, indem wir ein $s \in \mathbb{Z}_p$ auf den Charakter

$$\omega \times \widetilde{\kappa}^s \colon G \cong \mathbb{F}_p^\times \times \Gamma \longrightarrow \mathbb{Z}_p^\times \subseteq \mathbb{C}_p^\times$$

abbilden. Als Einschränkung auf $\mathbb{Z}_p$ erhalten wir dann genau die Funktion aus Satz 1.8: denn für $n \in \mathbb{N}$ gilt

$$\int_G \omega\widetilde{\kappa}^{1-n} \mathrm{d}\mu_\chi = \int_G \omega^n \kappa^{1-n} \mathrm{d}\mu_\chi = (1 - \chi\omega^{-n}(p)p^{n-1})L(\chi\omega^{-n}, 1-n) = L_p(\chi, 1-n).$$

Iwasawa zeigt in [Iwa72, §6], dass die Funktion

$$\mathbb{Z}_p \longrightarrow \mathbb{C}_p, \quad s \longmapsto \int_G \omega\widetilde{\kappa}^s \mathrm{d}\mu_\chi$$

analytisch in s ist, also durch eine konvergente Potenzreihe gegeben ist, und die Eindeutigkeit aus Satz 1.8 zeigt dann die Behauptung.

5. p-adische L-Funktionen für Modulformen

Nachdem wir nun für Dirichlet-Charaktere bereits p-adische L-Funktionen konstruiert haben, legen die Betrachtungen aus Abschnitt II.1 nahe, als nächstes nach der Konstruktion von p-adischen L-Funktionen für Modulformen zu suchen. Die Konstruktion von p-adischen L-Funktionen zu allgemeineren automorphen Formen ist gegenwärtig noch ein offenes Problem, auch wenn diese in gewissen Fällen bereits gelang.

Es stellt sich nun die Frage, wie eine p-adische L-Funktion zu einer Modulform oder zu anderen L-Funktionen überhaupt aussehen soll. Das erste Problem, das hierbei auftaucht, ist das der Algebraizität: bevor wir irgendwelche speziellen Werte von komplexen L-Funktionen überhaupt p-adisch interpretieren können, müssen wir wissen, dass diese Werte (bzw. geeignete Modifikationen derselben) algebraisch sind, denn sonst gibt es keine Möglichkeit, sie auf konsistente Weise in einer Erweiterung von $\mathbb{Q}_p$ wiederzufinden. Für die Dirichletschen L-Funktionen gibt Satz I.5.7 Auskunft über die Algebraizität gewisser spezieller Werte. Für motivische L-Funktionen wurde von Pierre Deligne in [Del79] eine Vermutung darüber aufgestellt, wie eine solche Aussage in diesem Fall aussehen sollte und die Satz I.5.7 verallgemeinert. Wir wollen dies hier nicht im Detail erklären, sondern nur sagen, welche Gestalt diese Vermutung für die L-Funktionen von Modulformen annimmt. In diesem Falle ist die Vermutung ein Satz von Shimura.

Satz 5.1: *Es sei $f \in \mathcal{S}_k^{\mathrm{new}}(\Gamma_1(N))$ eine normalisierte Eigenform und K_f der Körper, der über $\mathbb{Q}$ von den Fourierkoeffizienten von f erzeugt wird (vgl. Bemerkung IV.3.4). Dann gibt es Perioden $\Omega_f^\pm \in \mathbb{C}^\times$, sodass für jeden Dirichlet-Charakter ψ und $n = 1, \ldots, k-1$ gilt*

$$\frac{G(\overline{\psi})}{(2\pi \mathrm{i})^n \Omega_f^\pm} L(f, \psi, n) \in K_f(\psi).$$

In dieser Formel ist der Exponent von $\Omega_f^\pm$ als das Vorzeichen von $(-1)^n\psi(-1)$ zu wählen, und $G(\cdot)$ bezeichnet die Gauß-Summe (vgl. (I.5.1)).

Beweis: [Shi77, Thm. 1 (ii)] □

Die Perioden aus diesem Satz werden von Shimura auch konkret angegeben. Die in diesem Satz vorkommenden Twists der L-Funktion benötigen wir, da wir ansonsten nur für *endlich viele* Werte der (ungetwisteten) L-Funktion eine Algebraizitätsaussage haben. Wenn wir uns eine p-adische L-Funktion wünschen, die an diesen Stellen mit der komplexen übereinstimmt, lägen diese endlich vielen Werte liegen keineswegs mehr dicht in $\mathbb{Z}_p$, und eine solche p-adische L-Funktion wäre alles andere als eindeutig bestimmt.

Aufbauend auf der Vermutung von Deligne haben John Coates und Bernadette Perrin-Riou in [CP89] und [Coa89] erklärt, wie die p-adischen Pendants zu diesen motivischen L-Funktionen vermutlich aussehen. Ihre Vermutung orientiert sich an den Sätzen 4.1 und 5.1. Im Falle der L-Funktionen zu Modulformen ist eine solche p-adische L-Funktion erfolgreich konstruiert worden – für Gewicht 2 bereits in [MS74], für allgemeines Gewicht, aber Level 1 in [Man73; Man74] und später allgemein in [MTT86]. Wir zitieren das Ergebnis hier aus [Kit94, Thm. 4.8].

Satz 5.2: *Es sei $f \in \mathcal{S}_k(\Gamma_1(N))$ eine normalisierte Eigenform, K_f der Körper, der über $\mathbb{Q}$ von den Fourierkoeffizienten von f erzeugt wird, und es sei eine Einbettung $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ gewählt. Für den p-ten Fourierkoeffizient a_p gelte in $\overline{\mathbb{Q}}_p$, dass $|a_p|_p = 1$.*

Dann gibt es ein Maß μ_f auf G, sodass für $n = 0, \dots, k-2$ und jeden Dirichlet-Charakter ψ vom Führer p^m für ein $m \in \mathbb{N}_0$ gilt:

$$\int_G \psi^{-1}\kappa^n d\mu_f = \frac{G(\overline{\psi})p^{mn}(n-1)!}{(2\pi \mathrm{i})^n \Omega_f^{\pm} a_p^m}(1 - a_p^{-1}\overline{\psi}(p)p^n)L(f, \psi, n+1).$$

In dieser Formel ist der Exponent von $\Omega_f^{\pm}$ als das Vorzeichen von $(-1)^n\psi(-1)$ zu wählen.

Man vergleiche dieses Ergebnis mit der entsprechenden Aussage für Dirichlet-Charaktere aus Satz 4.1!

IV. Hida-Theorie und Galoisdeformationen

Wir haben in Kapitel II die Räume der Modul- und Spitzenformen eingeführt und gewisse Endomorphismen dieser Räume, die Hecke-Operatoren, studiert. Besonders interessant waren dabei die Spitzenformen und unter diesen die Eigenformen, die gemeinsame Eigenvektoren aller dieser Hecke-Operatoren sind. Sie haben herausragende Eigenschaften, denn ihre Fourierkoeffizienten (für die wir uns besonders interessieren, da sie arithmetische Informationen beinhalten) erfüllen gewisse Relationen, die zum Beispiel dazu führen, dass ihre L-Funktionen ein Eulerprodukt haben. Auch werden wir später sehen, dass man solchen Eigenformen Galoisdarstellungen zuordnen kann, die eng mit den Fourierkoeffizienten verknüpft sind.

Es sollte uns also ein Anliegen sein, diese Eigenformen genauer zu untersuchen. Die erste wichtige Aussage, die uns dabei hilft, ist Satz 1.1, der es uns ermöglicht, Spitzenformen über anderen Ringen als $\mathbb{C}$ zu betrachten. Die Hecke-Operatoren, deren Eigenvektoren wir studieren wollen, bilden eine Teilalgebra der Endomorphismen der Räume der Spitzenformen, die *Hecke-Algebra*, und eine der wichtigsten Aussagen in dieser Theorie ist der Dualitätssatz 2.3. Er und die Folgerung aus Satz 2.6 reduzieren das Studium der Eigenformen letztlich auf die Untersuchung der Geometrie dieser Hecke-Algebren und rücken diese damit in den Mittelpunkt des Interesses.

Diese Sichtweise führte Hida dazu, p-adische Hecke-Algebren zu verschiedenen Gewichten und Leveln zu einer großen Hecke-Algebra zusammenzufassen (Definition 4.1), welche er ursprünglich benutze, um Kongruenzen zwischen Fourierkoeffizienten von Modulformen zu untersuchen (Lemma 3.5). Diese Hecke-Algebra enthält als direkten Summanden die sogenannte *ordinäre* Teilalgebra, welche in Hidas Theorie eine zentrale Rolle spielt. Die Galoisdarstellungen zu Eigenformen, für die wir uns vorrangig interessieren, lassen sich zu einer großen Galoisdarstellung mit Werten in dieser Teilalgebra zusammensetzen, welche vermutlich (und teilweise bewiesen) eine gewisse universelle Eigenschaft erfüllt.

Für dieses Kapitel wählen wir ein für alle mal eine Einbettung $\overline{\mathbb{Q}}_p \hookrightarrow \mathbb{C}$ und fassen damit bei Bedarf komplexwertige Charaktere irgendwelcher Gruppen als p-adische auf und umgekehrt, ohne dies im Einzelfall explizit zu erwähnen.

1. Modulformen über beliebigen Ringen

Als erstes wollen wir erklären, wie wir uns von der Vorstellung von Modulformen als komplex-analytische Objekte lösen können und diese über (nahezu) beliebigen Ringen betrachten können.

Es sei dazu Φ eine Kongruenzuntergruppe mit $\Gamma_1(N) \subseteq \Phi \subseteq \Gamma_0(N)$ und ε ein komplexer

Charakter von[1] $\Phi/\Gamma_1(N)$. Für einen Teilring A von $\mathbb{C}$, der alle Werte von ε enthält, definieren wir

$$\mathcal{S}_k(\Phi,\varepsilon,A) = \{f \in \mathcal{S}_k(\Phi,\varepsilon) : \text{alle Fourierkoeffizienten von } f \text{ liegen in } A\}$$

(vgl. Definition II.3.6). Insbesondere haben wir für einen beliebigen Teilring A von $\mathbb{C}$

$$\mathcal{S}_k(\Gamma_1(N),A) = \{f \in \mathcal{S}_k(\Gamma_1(N)) : \text{alle Fourierkoeffizienten von } f \text{ liegen in } A\},$$

und falls A die Werte eines Dirichlet-Charakters χ modulo N enthält

$$\mathcal{S}_k(N,\chi,A) = \{f \in \mathcal{S}_k(N,\chi) : \text{alle Fourierkoeffizienten von } f \text{ liegen in } A\}.$$

Falls $\phi(N)$ in A invertierbar ist und A die Werte aller solcher Charaktere ε enthält, gilt

$$\mathcal{S}_k(\Gamma_1(N),A) = \bigoplus_{\varepsilon} \mathcal{S}_k(\Phi,\varepsilon,A).$$

Die zentrale Aussage über diese Räume ist der folgende Satz. Hierbei bezeichnet $\mathbb{Z}[\varepsilon]$ den Ring, der über $\mathbb{Z}$ von den Werten von ε erzeugt wird.

Satz 1.1 (Ganzheit): *Die natürliche Abbildung*

$$\mathcal{S}_k(\Phi,\varepsilon,\mathbb{Z}[\varepsilon]) \otimes_{\mathbb{Z}[\varepsilon]} A \longrightarrow \mathcal{S}_k(\Phi,\varepsilon,A), \quad f \otimes a \longmapsto af$$

ist ein Isomorphismus. Insbesondere ist $\mathcal{S}_k(\Gamma_1(N),\mathbb{Z}) \otimes_{\mathbb{Z}} A \cong \mathcal{S}_k(\Gamma_1(N),A)$ *für jeden Teilring von* $\mathbb{C}$ *und* $\mathcal{S}_k(N,\chi,\mathbb{Z}[\chi]) \otimes_{\mathbb{Z}[\chi]} A \cong \mathcal{S}_k(N,\chi,A)$*, wenn A die Werte von χ enthält.*

Beweis: [HidMFG, Thm. 3.12] □

Wegen Satz 1.1 hätten wir also $\mathcal{S}_k(\Phi,\varepsilon,A)$ auch durch die linke Seite *definieren* können, und dies verallgemeinert sich sofort zu einer Definition für einen *beliebigen* Ring A, der nicht notwendigerweise in $\mathbb{C}$ liegen muss.

Definition 1.2: Für eine beliebige kommutative $\mathbb{Z}[\varepsilon]$-Algebra A sei

$$\mathcal{S}_k(\Phi,\varepsilon,A) := \mathcal{S}_k(\Phi,\varepsilon,\mathbb{Z}[\varepsilon]) \otimes_{\mathbb{Z}[\varepsilon]} A.$$

Die Einbettung

$$\mathcal{S}_k(\Phi,\varepsilon,\mathbb{Z}[\varepsilon]) \hookrightarrow \mathbb{Z}[\varepsilon][\![q]\!],$$

die eine Spitzenform auf ihre Fourierentwicklung schickt, liefert eine natürliche Abbildung $\mathcal{S}_k(\Phi,\varepsilon,A) \longrightarrow A[\![q]\!]$. Den Raum $\mathcal{S}_k(\Phi,\varepsilon,A)$ können wir uns dann als die A-lineare Hülle von $\mathcal{S}_k(\Phi,\varepsilon,\mathbb{Z}[\varepsilon])$ in $A[\![q]\!]$ vorstellen.

Satz 1.3: *Für eine beliebige kommutative $\mathbb{Z}[\varepsilon]$-Algebra A ist $\mathcal{S}_k(\Phi,\varepsilon,A)$ ein endlich erzeugter A-Modul. Für einen beliebigen kommutativen Ring A ist $\mathcal{S}_k(\Gamma_1(N),A)$ ein freier A-Modul.*

[1] Dieser Quotient ist abelsch, da $\Phi/\Gamma_1(N) \subseteq \Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$.

Beweis: Wir zeigen die Behauptung zuerst für $\mathcal{S}_k(\Gamma_1(N), \mathbb{Z})$. Dazu betrachten wir für $n \in \mathbb{N}$ das kommutative Diagramm

$$\begin{tikzcd}
\mathcal{S}_k(\Gamma_1(N), \mathbb{C}) \arrow[r, hook] & \mathbb{C}[\![q]\!] \arrow[r] & \mathbb{C}^n \\
\mathcal{S}_k(\Gamma_1(N), \mathbb{Z}) \arrow[r, hook] \arrow[u, hook] & \mathbb{Z}[\![q]\!] \arrow[r] \arrow[u, hook] & \mathbb{Z}^n, \arrow[u, hook]
\end{tikzcd}$$

in dem die linken horizontalen Pfeile jeweils eine Spitzenform auf ihre Fourierentwicklung und die rechten eine Potenzreihe auf das Tupel ihrer ersten n Koeffizienten abbilden. Da $\mathcal{S}_k(\Gamma_1(N), \mathbb{C})$ ein endlichdimensionaler $\mathbb{C}$-Vektorraum ist (vgl. Bemerkung II.3.4), ist die Komposition

$$\mathcal{S}_k(\Gamma_1(N), \mathbb{C}) \hookrightarrow \mathbb{C}[\![q]\!] \longrightarrow \mathbb{C}^n$$

für genügend großes n injektiv. Mit einer einfachen Diagrammjagd sieht man, dass dann auch

$$\mathcal{S}_k(\Gamma_1(N), \mathbb{Z}) \hookrightarrow \mathbb{Z}[\![q]\!] \longrightarrow \mathbb{Z}^n$$

injektiv sein muss. Dies zeigt die Behauptung für $\mathcal{S}_k(\Gamma_1(N), \mathbb{Z})$. Mit Satz 1.1 und Definition 1.2 folgt daraus die Aussage für beliebiges A.

Für $\mathcal{S}_k(\Phi, \varepsilon, A)$ funktioniert das obige Argument analog und wir erhalten die Injektivität von

$$\mathcal{S}_k(\Phi, \varepsilon, \mathbb{Z}[\varepsilon]) \hookrightarrow \mathbb{Z}[\varepsilon][\![q]\!] \longrightarrow \mathbb{Z}[\varepsilon]^n,$$

woraus wir folgern können, dass $\mathcal{S}_k(\Phi, \varepsilon, \mathbb{Z}[\varepsilon])$ ein endlich erzeugter $\mathbb{Z}[\varepsilon]$-Modul ist (da $\mathbb{Z}[\varepsilon]$ noethersch ist), und damit auch jedes $\mathcal{S}_k(\Phi, \varepsilon, A)$. Da $\mathbb{Z}[\varepsilon]$ kein Hauptidealring sein muss, erhalten wir aber nicht unbedingt, dass $\mathcal{S}_k(\Phi, \varepsilon, \mathbb{Z}[\varepsilon])$ frei ist. □

Bemerkung 1.4: Dass die A-Moduln $\mathcal{S}_k(\Phi, \varepsilon, A)$ und $\mathcal{S}_k(\Gamma_1(N), A)$ endlich erzeugt sind, sieht man auch direkt an Satz 1.1 und Definition 1.2: denn wegen Bemerkung II.3.4 wissen wir, dass die Räume für $A = \mathbb{C}$ endlichdimensional sind, also müssen sie auch über $\mathbb{Z}$ bzw. $\mathbb{Z}[\varepsilon]$ endlich erzeugt sein. Überdies zeigt das

$$\operatorname{Rang}_A \mathcal{S}_k(\Gamma_1(N), A) = \dim_{\mathbb{C}} \mathcal{S}_k(\Gamma_1(N))$$

für jeden kommutativen Ring A.

Bemerkung 1.5: Es sei Φ wie oben, $G = \Phi/\Gamma_1(N)$ und A ein kommutativer Ring, der die Werte aller Charaktere von G enthält. Wir können $S := \mathcal{S}_k(\Gamma_1(N), A)$ als Modul über $A[G]$ auffassen und dann für jeden Charakter ε von G seinen Eigenraum S_ε wie in (I.2.1) definieren. Wir wollen uns nun überlegen, dass dieser mit $\mathcal{S}_k(\Phi, \varepsilon, A)$ übereinstimmt. Wir notieren die Aktion von G auf S mit $\langle\cdot\rangle$.

Wenn ein $f = a \otimes f_0 \in \mathcal{S}_k(\Phi, \varepsilon, A)$ mit $f_0 \in \mathcal{S}_k(\Phi, \varepsilon, \mathbb{Z}[\varepsilon]) \subseteq \mathcal{S}_k(\Gamma_1(N), \mathbb{Z}[\varepsilon])$ gegeben ist, dann gilt für $g \in G$

$$\langle g\rangle f = a \otimes (\langle g\rangle f_0) = a \otimes (\varepsilon(g) f_0) = \varepsilon(g) f,$$

also liegt das Bild von f unter der natürlichen Abbildung $\mathcal{S}_k(\Phi, \varepsilon, A) \longrightarrow S$ in S_ε. Wenn umgekehrt ein $f = a \otimes f_0 \in S_\varepsilon$ mit $f_0 \in \mathcal{S}_k(\Gamma_1(N), A)$ und $a \neq 0$ gegeben ist, gilt für $g \in G$

$$a \otimes (\varepsilon(g) f_0) = \varepsilon(g) f = \langle g \rangle f = a \otimes (\langle g \rangle f_0),$$

also

$$a \otimes (\varepsilon(g) f_0 - \langle g \rangle f_0) = 0,$$

und da S ein freier A-Modul ist, folgt $\langle g \rangle f_0 = \varepsilon(g) f_0$, also $f_0 \in \mathcal{S}_k(\Phi, \varepsilon, \mathbb{Z}[\varepsilon])$ und damit $f \in \mathcal{S}_k(\Phi, \varepsilon, A)$.

2. Hecke-Algebren und Dualität

Wir haben in Abschnitt II.4 Hecke-Operatoren als Endomorphismen der Vektorräume von Modul- oder Spitzenformen eingeführt, die durch Doppelnebenklassen gegeben sind. Um die Wirkung der Doppelnebenklassen auf diesen Räumen abstrakter zu modellieren, führt Shimura in [Shi71, §3.1] einen Ring $R(\Gamma, \Delta)$ von Doppelnebenklassen ein. Wir wollen diesen hier für den Fall $\Gamma = \Gamma_1(N)$ und Δ wie in Definition II.4.3 betrachten. Für einen beliebigen kommutativen Ring A definieren wir $R(\Gamma, \Delta, A)$ als freien A-Modul, der von allen Doppelnebenklassen $\Gamma\alpha\Gamma$ mit $\alpha \in \Delta$ erzeugt wird. Um das Produkt zweier solcher Doppelnebenklassen $\Gamma\alpha\Gamma$ und $\Gamma\beta\Gamma$ zu erklären, zerlegen wir diese wie in (II.4.1) in Linksnebenklassen:

$$\Gamma\alpha\Gamma = \bigcup_{i=1}^{e} \Gamma\alpha_i, \quad \Gamma\beta\Gamma = \bigcup_{i=1}^{f} \Gamma\beta_i.$$

Die Multiplikation ist dann durch

$$\Gamma\alpha\Gamma \cdot \Gamma\beta\Gamma = \sum m_\xi \, \Gamma\xi\Gamma$$

definiert, wobei über alle Doppelnebenklassen $\Gamma\xi\Gamma \subseteq \Gamma\alpha\Gamma\beta\Gamma$ summiert wird und

$$m_\xi = \#\{(i,j) : \Gamma\alpha_i\beta_j = \Gamma\xi\}.$$

Shimura zeigt, dass dies wohldefiniert ist und $R(\Gamma, \Delta, A)$ zu einem Ring macht, der in diesem Fall kommutativ ist [Shi71, Prop. 3.8] (dort wird nur $R(\Gamma, \Delta, \mathbb{Z})$ betrachtet, aber es gilt offensichtlich $R(\Gamma, \Delta, A) = R(\Gamma, \Delta, \mathbb{Z}) \otimes_{\mathbb{Z}} A$). Das Produkt in diesem Ring ist gerade so gemacht, dass die Aktion der Doppelnebenklassen auf $\mathcal{M}_k(\Gamma)$ widergespiegelt wird [Shi71, Prop. 3.38]: wir bekommen einen Ringhomomorphismus

$$R(\Gamma, \Delta, \mathbb{Z}) \longrightarrow \mathrm{End}_{\mathbb{C}}(\mathcal{M}_k(\Gamma)).$$

Für $n \in \mathbb{N}$ definieren wir $T_n \in R(\Gamma, \Delta, A)$ wie in (II.4.4).

Wir wollen nun die Aktion dieser Doppelnebenklassen auf den Räumen $\mathcal{S}_k(\Phi, \varepsilon, A)$ für beliebige Ringe bzw. $\mathbb{Z}[\varepsilon]$-Algebren A betrachten. In [HidGMF, Prop. 3.2.12 (1)] wird gezeigt, dass die Räume $\mathcal{S}_k(\Phi, \varepsilon, \mathbb{Z}[\varepsilon])$ stabil unter allen Doppelnebenklassenoperatoren sind.[2] Dadurch können wir für beliebiges A Algebrenhomomorphismen

$$R(\Gamma, \Delta, A) \longrightarrow \mathrm{End}_A(\mathcal{S}_k(\Phi, \varepsilon, A))$$

[2] Streng genommen brauchen wir hier bereits das Argument aus Bemerkung 2.2, da dort nur gezeigt wird, dass die Räume unter den T_n stabil sind.

definieren. Man überlegt sich leicht, dass diese so gemacht sind, dass für $\mathcal{S}_k(\Gamma_1(N), A)$ und $\mathcal{S}_k(N, \chi, A)$ die Formeln aus Lemma II.4.7 für den Effekt der Operatoren T_n auf den Fourierkoeffizienten gültig bleibt.

Definition 2.1: Wenn ein A-Modul M zusammen mit einem A-Algebren-Homomorphismus

$$R(\Gamma, \Delta, A) \longrightarrow \mathrm{End}_A(M)$$

gegeben ist, dann definieren wir die *Hecke-Algebra von M mit Koeffizienten in A* als das Bild dieses Homomorphismus'.

Im Falle $M = S_k(\Phi, \varepsilon, A)$ bezeichnen wir diese Hecke-Algebren mit $\hbar_k(\Phi, \varepsilon, A)$. Entsprechend sind $\hbar_k(\Gamma_1(N), A)$ und $\hbar_k(N, \chi, A)$ zu verstehen.

Bemerkung 2.2: Die Hecke-Algebra $\hbar_k(\Gamma_1(N), A)$ enthält wegen Beispiel II.4.2 die Endomorphismen $\langle\cdot\rangle$, da $\Gamma_0(N) \subseteq \Delta$. In [Shi71, Prop. 3.35] wird gezeigt, dass $R(\Gamma, \Delta, \mathbb{Z})$ von den T_n (die dort $T'(n)$ heißen) zusammen mit Elementen $T'(p,p)$ für Primzahlen $p \nmid N$ erzeugt wird, und dass gilt $pT'(p,p) = T_p^2 - T_{p^2}$. Aus Satz II.4.6 (a) (i) folgt andererseits $p^{k-1}\langle p\rangle = T_p^2 - T_{p^2}$, also sehen wir, das $\hbar_k(\Gamma_1(N), A)$ von den T_n und den $\langle p\rangle$ für Primzahlen $p \nmid N$ erzeugt wird. Wegen des Dirichletschen Primzahlsatzes finden wir für jedes solche p eine weitere Primzahl $q \neq p$ mit $p \equiv q \pmod N$ (also $\langle p\rangle = \langle q\rangle$), die ebenfalls N nicht teilt, und wir finden weiter ganze Zahlen a, b, sodass $ap^{k-1} + bq^{k-1} = 1$. Damit folgt

$$\langle p\rangle = (ap^{k-1} + bq^{k-1})\langle p\rangle = a(T_p^2 - T_{p^2}) + b(T_q^2 - T_{q^2}),$$

und wir sehen, dass die T_n als Erzeugendensystem genügen. Vgl. dazu auch [RS11, Prop. 9.4.1]. Das gleiche Argument funktioniert auch für $\hbar_k(\Phi, \varepsilon, A)$.

Wir definieren nun eine Paarung

$$\langle\cdot,\cdot\rangle : \hbar_k(\Phi, \varepsilon, A) \times \mathcal{S}_k(\Phi, \varepsilon, A) \longrightarrow A, \quad \langle h, f\rangle = a_1(hf).$$

Hierbei meinen wir mit $a_n(\cdot)$ den n-ten Fourierkoeffizient einer Modulform. Insbesondere gilt dann

$$\langle T_n, f\rangle = a_n(f) \tag{2.1}$$

nach Lemma II.4.7. Über diese Paarung haben wir den wichtigen folgenden Satz, der in unserer Theorie eine zentrale Rolle spielt.

Satz 2.3 (Dualität): *Die oben definierte Paarung ist perfekt, d.h. sie induziert Isomorphismen von A-Moduln*

$$\mathrm{Hom}_A(\mathcal{S}_k(\Phi, \varepsilon, A), A) \cong \hbar_k(\Phi, \varepsilon, A) \quad \textit{und} \quad \mathrm{Hom}_A(\hbar_k(\Phi, \varepsilon, A), A) \cong \mathcal{S}_k(\Phi, \varepsilon, A).$$

Hierbei sind jeweils Homomorphismen von A-Moduln gemeint.

Beweis: [HidMFG, Thm. 3.17] □

Korollar 2.4: *Die Hecke-Algebra $\hbar_k(\Phi, \varepsilon, A)$ ist als A-Modul endlich erzeugt. $\hbar_k(\Gamma_1(N), A)$ ist ein freier A-Modul.*

Beweis: Folgt direkt aus Satz 1.3 und Satz 2.3. □

Korollar 2.5: *Die natürliche Abbildung*

$$\hbar_k(\Phi, \varepsilon, \mathbb{Z}[\varepsilon]) \otimes_{\mathbb{Z}[\varepsilon]} A \longrightarrow \hbar_k(\Phi, \varepsilon, A), \quad h \otimes a \longmapsto ah$$

ist ein Isomorphismus.

Beweis: Unter Verwendung der Tensor-Hom-Adjunktion und $\mathrm{Hom}_A(A, A) = A$ (hier sind A-Modul-Homomorphismen gemeint) gilt nach Satz 2.3

$$\begin{aligned}\hbar_k(\Phi, \varepsilon, A) &= \mathrm{Hom}_A(\mathcal{S}_k(\Phi, \varepsilon, A), A) = \mathrm{Hom}_A(\mathcal{S}_k(\Phi, \varepsilon, \mathbb{Z}[\varepsilon]) \otimes_{\mathbb{Z}[\varepsilon]} A, A)\\ &= \mathrm{Hom}_{\mathbb{Z}[\varepsilon]}(\mathcal{S}_k(\Phi, \varepsilon, \mathbb{Z}[\varepsilon]), A) = \mathrm{Hom}_{\mathbb{Z}[\varepsilon]}(\mathcal{S}_k(\Phi, \varepsilon, \mathbb{Z}[\varepsilon]), \mathbb{Z}[\varepsilon]) \otimes_{\mathbb{Z}[\varepsilon]} A\\ &= \hbar_k(\Phi, \varepsilon, \mathbb{Z}[\varepsilon]) \otimes_{\mathbb{Z}[\varepsilon]} A.\end{aligned}$$ □

Wie im klassischen Fall nennen wir ein $f \in \mathcal{S}_k(\Phi, \varepsilon, A)$ eine *Eigenform*, wenn es ein Eigenvektor aller Hecke-Operatoren T_n für alle $n \in \mathbb{N}$ ist. Man überlegt sich leicht, dass die Sätze II.4.6 und II.4.8 und damit auch Satz II.6.4 in dieser Situation ihre Gültigkeit behalten. In Bemerkung II.6.3 hatten wir gesehen, dass im klassischen Fall jede Eigenform $f \in \mathcal{S}_k(\Gamma_1(N))$ einen Nebentyp hat. Das Argument aus Bemerkung 2.2 zeigt zusammen mit Bemerkung 1.5, dass dies auch in unserer Situation gültig bleibt, wenn A so groß ist, dass es alle Werte aller Dirichlet-Charaktere modulo N enthält. Satz 2.3 ermöglicht es uns dann, Eigenformen als geometrische Objekte aufzufassen.

Satz 2.6: *Es gibt eine kanonische Bijektion zwischen der Menge der normalisierten Eigenformen in $\mathcal{S}_k(\Phi, \varepsilon, A)$ und $\mathbb{Z}[\varepsilon]$-Algebrenhomomorphismen $\hbar_k(\Phi, \varepsilon, \mathbb{Z}[\varepsilon]) \longrightarrow A$.*

Beweis: Die Elemente von $\mathcal{S}_k(\Phi, \varepsilon, A)$ stehen nach Satz 2.3 in Bijektion mit den A-Modul-Homomorphismen der Hecke-Algebra $\hbar_k(\Phi, \varepsilon, A)$ nach A. Ein solcher ist genau dann multiplikativ, also ein A-Algebren-Homomorphismus, wenn er die Relationen zwischen den T_n aus Satz II.4.6 respektiert, da die T_n die Hecke-Algebra erzeugen (Bemerkung 2.2). Wegen (2.1) gilt das genau dann, wenn die Fourierkoeffizienten der zugehörigen Spitzenform die entsprechenden Relationen aus Satz II.6.4 erfüllen, also genau dann, wenn die zugehörige Spitzenform eine normalisierte Eigenform ist. Dies gibt uns zunächst eine Bijektion zwischen der Menge der normalisierten Eigenformen in $\mathcal{S}_k(\Phi, \varepsilon, A)$ und A-Algebren-Homomorphismen $\hbar_k(\Phi, \varepsilon, A) \longrightarrow A$.

Um die restliche Behauptung einzusehen, benutzen wir wieder die Tensor-Hom-Adjunktion, die uns

$$\mathrm{Hom}_A(\hbar_k(\Phi, \varepsilon, A), A) = \mathrm{Hom}_{\mathbb{C}}(\hbar_k(\Phi, \varepsilon, \mathbb{Z}[\varepsilon]) \otimes_{\mathbb{Z}[\varepsilon]} A, A) = \mathrm{Hom}_{\mathbb{Z}[\varepsilon]}(\hbar_k(\Phi, \varepsilon, \mathbb{Z}[\varepsilon]), A)$$

gibt (zunächst als Bijektion von Modulhomomorphismen, aber damit auch von Algebrenhomomorphismen). □

Bemerkung 2.7: Wenn A eine $\mathbb{Z}[\varepsilon]$-Algebra und B eine A-Algebra ist, gilt offenbar $B = A \otimes_{\mathbb{Z}[\varepsilon]} B$. Das gleiche Argument zeigt dann, dass es ebenso eine Bijektion zwischen normalisierten Eigenformen in $\mathcal{S}_k(\Phi, \varepsilon, B)$ und B-Algebrenhomomorphismen $\hbar_k(\Phi, \varepsilon, A) \longrightarrow B$ gibt. Für $A = B$ haben wir insbesondere eine Bijektion zwischen normalisierten Eigenformen in $\mathcal{S}_k(\Phi, \varepsilon, A)$ und A-Algebrenhomomorphismen $\hbar_k(\Phi, \varepsilon, A) \longrightarrow A$. In dieser letzten Form werden wir diese Aussage meistens verwenden.

Korollar 2.8: *Der von den Fourierkoeffizienten einer normalisierten Eigenform* $f \in \mathcal{S}_k(\Phi, \varepsilon, A)$ *erzeugte Teilring von* A *ist ganz über* $\mathbb{Z}$.

Beweis: Dieser Teilring ist nach Konstruktion das Bild des zu f gehörenden Homomorphismus' $\mathfrak{h}_k(\Phi, \varepsilon, \mathbb{Z}[\varepsilon]) \longrightarrow A$ und deshalb nach Korollar 2.4 als $\mathbb{Z}[\varepsilon]$-Modul endlich erzeugt. Die Behauptung folgt daraus mit [Eis95, Cor. 4.5, Thm. 4.2]. □

Satz 2.6 besagt also, dass die normalisierten Eigenformen in $\mathcal{S}_k(\Phi, \varepsilon, A)$ genau den A-wertigen Punkten des $\mathbb{Z}[\varepsilon]$-Schemas $\operatorname{Spec} \mathfrak{h}_k(\Phi, \varepsilon, \mathbb{Z}[\varepsilon])$ entsprechen und gibt damit der Geometrie der Hecke-Algebren eine Bedeutung. Das folgende Lemma gibt für gewisse Ringe A genauere Auskunft über diese Geometrie.

Lemma 2.9: *Es sei* A *ein lokaler noetherscher Ring mit maximalem Ideal* m, *der* m*-adisch vollständig ist, und* H *eine* A*-Algebra, die als* A*-Modul endlich erzeugt ist. Dann hat* H *nur endlich viele maximale Ideale und ist das Produkt*

$$H = \prod_{\mathfrak{m}} H_{\mathfrak{m}}$$

seiner Lokalisierungen bei diesen maximalen Idealen. Jeder der lokalen Ringe $H_{\mathfrak{m}}$ *ist* $\mathfrak{m}$*-adisch vollständig.*

Beweis: [Eis95, Cor. 7.6] □

Dieses Lemma wollen wir für den Fall anwenden, dass $A = \mathcal{O}$ der Ganzheitsring in einer endlichen Erweiterung von $\mathbb{Q}_p$ ist, die alle Werte aller Dirichlet-Charaktere modulo N enthält, und $H = \mathfrak{h}_k(\Gamma_1(N), \mathcal{O})$. Wegen Satz 1.3 sind die Voraussetzungen dafür erfüllt. Also hat $\mathfrak{h}_k(\Gamma_1(N), \mathcal{O})$ nur endlich viele maximale Ideale und ist ein endliches Produkt

$$\mathfrak{h}_k(\Gamma_1(N), \mathcal{O}) = \prod_{\mathfrak{m}} \mathfrak{h}_k(\Gamma_1(N), \mathcal{O})_{\mathfrak{m}}$$

lokaler Ringe. Geometrisch bedeutet dies also, dass $\operatorname{Spec} \mathfrak{h}_k(\Gamma_1(N), \mathcal{O})$ die disjunkte Vereinigung der Spektren der lokalen Ringe $\mathfrak{h}_k(\Gamma_1(N), \mathcal{O})_{\mathfrak{m}}$ ist. Insbesondere sieht man daran leicht, dass jeder $\mathcal{O}$-Algebrenhomomorphismus $\mathfrak{h}_k(\Gamma_1(N), \mathcal{O}) \longrightarrow \mathcal{O}$ über genau einen dieser lokalen Ringe faktorisieren muss (jeder $\mathcal{O}$-wertige Punkt liegt in genau einer irreduziblen Komponente, da $\mathcal{O}$ nullteilerfrei ist). Auf diese Weise können wir jeder normalisierten Eigenform $f \in \mathcal{S}_k(\Gamma_1(N), \mathcal{O})$ genau ein maximales Ideal $\mathfrak{m}$ und einen lokalen Ring $\mathfrak{h}_k(\Gamma_1(N), \mathcal{O})_{\mathfrak{m}}$ von $\mathfrak{h}_k(\Gamma_1(N), \mathcal{O})$ zuordnen.

Lemma 2.10: *Es sei* A *lokaler Ring mit maximalem Ideal* M, H *eine* A*-Algebra,*

$$f : H \longrightarrow A$$

ein A*-Algebren-Homomorphismus und* $\mathfrak{m}$ *ein maximales Ideal von* H. *Dann gelten:*

(a) f *ist surjektiv*

(b) $f(\mathfrak{m}) = M$

(c) *Der induzierte Homomorphismus*

$$f_{\mathfrak{m}}\colon\ H\big/\mathfrak{m} \longrightarrow A\big/M$$

ist ein Isomorphismus.

(d) *Ist $f'\colon H \longrightarrow A$ ein weiterer A-Algebren-Homomorphismus, so ist die Komposition*

$$A\big/M \xrightarrow{f_{\mathfrak{m}}^{-1}} H\big/\mathfrak{m} \xrightarrow{f'_{\mathfrak{m}}} A\big/M$$

die Identität.

Beweis: (a) Klar, da f A-linear ist.

(b) Klar.

(c) Er ist wegen (a) surjektiv und als Körperhomomorphismus sowieso injektiv.

(d) Die Komposition ist A-linear und muss deshalb die Identität sein. □

Aus Lemma 2.10 (c) folgt sofort:

Lemma 2.11: *Sei $f \in \mathcal{S}_k(\Gamma_1(N), \mathcal{O})$ eine normalisierte Eigenform und $\mathfrak{m}$ das maximale Ideal von $\mathfrak{h}_k(\Gamma_1(N), \mathcal{O})$, zu dem f gehört. Dann stimmt $\mathfrak{h}_k(\Gamma_1(N), \mathcal{O})/\mathfrak{m}$ mit dem Restklassenkörper $\mathbb{F}$ von $\mathcal{O}$ überein.*

3. Modulare Galoisdarstellungen

Im folgenden sei χ ein Dirichlet-Charakter modulo N und K eine endliche Erweiterung von $\mathbb{Q}_p$, die alle Werte von χ enthält. Mit $\mathcal{O}$ bezeichnen wir den Ganzheitsring von K, mit $\mathfrak{m}_{\mathcal{O}}$ das maximale Ideal und mit $\mathbb{F}$ seinen Restklassenkörper. Wir wollen nun Spitzenformen mit Koeffizienten in $\mathcal{O}$ betrachten. Sind diese Eigenformen, kann man ihnen eine Galoisdarstellung zuordnen.

Satz 3.1: *Es sei $f \in \mathcal{S}_k^{\mathrm{new}}(N, \chi, \mathcal{O})$ eine normalisierte Eigenform, deren Fourierkoeffizienten wir mit a_n für $n \in \mathbb{N}$ bezeichnen. Dann gilt:*

(a) *Es gibt eine bis auf Isomorphie eindeutig bestimmte stetige absolut irreduzible ungerade Galoisdarstellung*

$$\rho_f\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathcal{O}),$$

die außerhalb von $Np\infty$ unverzweigt ist, und sodass für alle Primzahlen $\ell \nmid Np$ gilt

$$\mathrm{Spur}(\mathrm{Frob}_\ell) = a_\ell, \quad \det(\mathrm{Frob}_\ell) = \chi(\ell)\ell^{k-1}.$$

Hierbei ist Frob_ℓ ein Frobeniuselement bei ℓ.

(b) Wenn $k \geq 2$ und $a_p \in \mathcal{O}^\times$, dann ist die Einschränkung von ρ_f auf die Zerlegungsgruppe[3] D_p isomorph zu einer oberen Dreiecksdarstellung

$$\rho_f|_{D_p} \cong \begin{pmatrix} \varepsilon & * \\ & \delta \end{pmatrix},$$

und δ ist unverzweigt.

Beweis: [HidMFG, Thm. 3.26]. Dort wird nicht gesagt, dass diese Darstellung ungerade ist, siehe dazu [DS05, S. 393]. □

Diese Darstellung hat also die Eigenschaft, dass für Primzahlen $\ell \nmid Np$ das ℓ-te Hecke-Polynom von f (Definition II.6.7) mit dem ℓ-ten Frobenius-Polynom (Definition I.6.4 (b)) von ρ_f übereinstimmt.

Definition 3.2: Für eine Eigenform $f \in \mathcal{S}_k(\Gamma_1(N), \mathcal{O})$ bezeichnen wir mit

$$\overline{\rho}_f = \rho_f \bmod \mathfrak{m}_{\mathcal{O}} \colon \operatorname{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F})$$

die Darstellung, die wir aus ρ_f bekommen, wenn wir modulo dem maximalen Ideal von $\mathcal{O}$ reduzieren. Sie heißt die *Restklassendarstellung* zu f. Wenn diese Restklassendarstellung absolut irreduzibel ist, ist ρ_f nach Lemma I.6.3 eindeutig bestimmt.

Bemerkung 3.3: Die im Satz behauptete Eindeutigkeit ist mit Bemerkung I.6.6 leicht zu sehen, falls die Restklassendarstellung $\overline{\rho}_f$ absolut irreduzibel ist. Daran sieht man insbesondere, dass die Galoisdarstellung dann nur von den Fourierkoeffizienten a_n für $(n, N) = 1$ abhängt. Deshalb ist die Forderung, dass f eine Neuform ist, keine wirkliche Einschränkung: denn wenn lediglich $f \in \mathcal{S}_k(\Gamma_1(N), \mathcal{O})$ ein Eigenvektor aller T_n für $(n, N) = 1$ ist, gibt es nach Satz II.5.6 eine zugehörige Neuform, deren Fourierkoeffizienten für alle n mit $(n, N) = 1$ mit denen von f übereinstimmen. Es ist jedoch günstig, durch die Forderung, dass f eine Neuform ist, das Level N minimal zu halten, um keine Primzahlen unnötig als verzweigt anzusehen.

Bemerkung 3.4: Mithilfe von Korollar 2.8 können wir auch klassischen komplexen Eigenformen Galoisdarstellungen zuordnen: denn wenn $f \in \mathcal{S}_k(\Gamma_1(N))$ eine normalisierte (komplexe) Eigenform ist, sind die Fourierkoeffizienten von f ganz über $\mathbb{Z}$ und erzeugen somit eine endliche Erweiterung K_f von $\mathbb{Q}$ in $\mathbb{C}$. Das liefert uns eine ganze Familie von Galoisdarstellungen: denn für jede endliche Primstelle λ von K_f können wir f als Element von $\mathcal{S}_k(\Gamma_1(N), \mathcal{O})$ auffassen, wenn $\mathcal{O}$ der Ganzheitsring in der Komplettierung von K_f bei λ ist, und das gibt uns ein System von λ-adischen Darstellungen (vgl. Definition I.6.7). Dieses ist „fast kompatibel", d.h. die Frobenius-Polynome der *unverzweigten* Primzahlen haben Koeffizienten in K_f und stimmen überein.

Es sei nun $\mathcal{O}$ wieder wie vorher der Ganzheitsring in einer endlichen Erweiterung von $\mathbb{Q}_p$, die die Werte aller Dirichlet-Charaktere modulo N enthält und $\mathfrak{m}_{\mathcal{O}}$ das maximale Ideal in $\mathcal{O}$.

[3] Diese Zerlegungsgruppe hängt von der Wahl einer über p liegenden Primstelle in der maximalen außerhalb von Np unverzweigten Erweiterung von $\mathbb{Q}$ ab. Eine andere Wahl führt aber zu einer konjugierten Zerlegungsgruppe, und die Gültigkeit von (b) bleibt davon unberührt.

Lemma 3.5: *Es seien $f, g \in \mathcal{S}_k(\Gamma_1(N), \mathcal{O})$ normalisierte Eigenformen, die zum gleichen maximalen Ideal $\mathfrak{m}$ von $\mathfrak{h}_k(\Gamma_1(N), \mathcal{O})$ gehören. Wir bezeichnen ihre Fourierkoeffizienten mit a_n bzw. b_n für $n \in \mathbb{N}$. Dann gilt*

$$a_n \equiv b_n \mod \mathfrak{m}_{\mathcal{O}}$$

für alle $n \in \mathbb{N}$.

Beweis: Es seien $\lambda, \eta\colon \mathfrak{h}_k(\Gamma_1(N), \mathcal{O})_\mathfrak{m} \longrightarrow \mathcal{O}$ die zu f bzw. g gehörenden $\mathcal{O}$-Algebren-Homomorphismen. Nach Lemma 2.11 induzieren diese Isomorphismen

$$\overline{\lambda}, \overline{\eta}\colon \left. \mathfrak{h}_k(\Gamma_1(N), \mathcal{O})_\mathfrak{m} \middle/ \mathfrak{m} \right. \xrightarrow{\sim} \left. \mathcal{O} \middle/ \mathfrak{m}_{\mathcal{O}} \right. = \mathbb{F},$$

und wegen Lemma 2.10 (c) stimmen diese überein. Wegen $\lambda(T_n) = a_n$ und $\eta(T_n) = b_n$ folgt daraus die Behauptung. □

Lemma 3.6: *Es seien $f, g \in \mathcal{S}_k(\Gamma_1(N), \mathcal{O})$ Eigenformen, die zum gleichen maximalen Ideal $\mathfrak{m}$ von $\mathfrak{h}_k(\Gamma_1(N), \mathcal{O})$ gehören. Wenn eine der Restklassendarstellungen $\overline{\rho}_f$ und $\overline{\rho}_g$ absolut irreduzibel ist, dann gilt $\overline{\rho}_f \cong \overline{\rho}_g$.*

Beweis: Es gilt nach Lemma 3.5 für Primzahlen $\ell \nmid Np$

$$\operatorname{Spur} \rho_f(\operatorname{Frob}_\ell) = a_\ell \equiv b_\ell = \operatorname{Spur} \rho_g(\operatorname{Frob}_\ell) \mod \mathfrak{m}_{\mathcal{O}},$$

wobei mit a_n bzw. b_n wieder die Fourierkoeffizienten von f bzw. g bezeichnet seien. Daraus folgt die Behauptung mit Bemerkung 1.6.6. □

Das vorherige Lemma besagt also, dass die Restklassendarstellungen der Eigenformen, die zu einem festen maximalen Ideal $\mathfrak{m}$ gehören, entweder alle absolut irreduzibel sind oder alle nicht absolut irreduzibel sind, und im ersteren Fall stimmen alle diese Restklassendarstellungen überein. Das ermöglicht es uns, für ein solches maximales Ideal $\mathfrak{m}$ die *Restklassendarstellung zu* $\mathfrak{m}$ als $\overline{\rho}_\mathfrak{m}$ zu definieren. Für die anderen maximalen Ideale kann man ebenfalls eine (reduzible) Restklassendarstellung definieren [HidMFG, S. 115], dies werden wir aber nicht benötigen.

4. Die universelle Hecke-Algebra

In Abschnitt 2 haben wir Hecke-Algebren zu festem Level und Gewicht über p-adischen Ringen betrachtet. Wie bereits erwähnt, kann man diese p-adischen Hecke-Algebren für alle Level und Gewichte zu einer „großen" Hecke-Algebra zusammensetzen. Aus dieser kann man die einzelnen Hecke-Algebren und damit einzelne Eigenformen wieder zurückgewinnen (mit Satz 4.7). Diese große Hecke-Algebra enthält dadurch Informationen zu sehr vielen Eigenformen auf einmal und fasst diese zu sogenannten Hida-Familien zusammen. Diese Theorie wurde von Hida in [Hid86b; Hid86a] entwickelt. Ein anderer Zugang wurde von Wiles in [Wil88] angegeben.

4.1. Die große Hecke-Algebra

Sei im folgenden stets p eine Primzahl und N zu p teilerfremd. Außerdem fixieren wir wieder eine endliche Erweiterung K von $\mathbb{Q}_p$ und bezeichnen mit $\mathcal{O}$ ihren Ganzheitsring.

Für (im Moment noch feste) $r, i \in \mathbb{N}$ setzen wir

$$\mathcal{S}^i(Np^r) = \bigoplus_{k=1}^{i} \mathcal{S}_k(\Gamma_1(Np^r), \mathcal{O}).$$

Nach Satz 1.3 ist das ein freier $\mathcal{O}$-Modul von endlichem Rang. Zu jeder Doppelnebenklasse $\Gamma_1(N)\alpha\Gamma_1(N)$ für $\alpha \in \Delta$ (Δ wie in Definition II.4.3) bekommen wir einen Endomorphismus von $\mathcal{S}^i(Np^r)$, indem wir in der k-ten Komponente den Doppelnebenklassenoperator $[\Gamma_1(N)\alpha\Gamma_1(N)]_k$ wirken lassen. Dies definiert einen $\mathcal{O}$-Algebren-Homomorphismus

$$R(\Gamma, \Delta, \mathcal{O}) \longrightarrow \mathrm{End}_{\mathcal{O}}(\mathcal{S}^i(Np^r))$$

wie in Definition 2.1, und wir bekommen eine Hecke-Algebra, die wir mit $\mathfrak{h}^i(Np^r, \mathcal{O})$ bezeichnen. Diese ist eine proendliche $\mathcal{O}$-Algebra: denn $\mathrm{End}_{\mathcal{O}}(\mathcal{S}^i(Np^r))$ ist isomorph zu einem Matrizenring über $\mathcal{O}$, deshalb ist die Teilalgebra $\mathfrak{h}^i(Np^r, \mathcal{O})$ hausdorffsch, und außerdem ist sie als stetiges Bild des kompakten Rings $R(\Gamma, \Delta, \mathcal{O})$ kompakt und damit nach Satz I.1.8 (c) proendlich.

Sei jetzt $r \leq s$ und $i \leq j$. Dann haben wir kommutierende kanonische Einbettungen

$$\begin{tikzcd}
\mathcal{S}^i(Np^r, \mathcal{O}) \arrow[r, hook] \arrow[d, hook] & \mathcal{S}^i(Np^s, \mathcal{O}) \arrow[d, hook] \\
\mathcal{S}^j(Np^r, \mathcal{O}) \arrow[r, hook] & \mathcal{S}^j(Np^s, \mathcal{O}).
\end{tikzcd}$$

Die Aktionen der Doppelnebenklassenoperatoren auf jedem dieser Räume ist mit diesen Einbettungen verträglich (siehe Bemerkung II.4.9). Deshalb bekommen wir ein analoges kommutatives Diagramm für die Hecke-Algebren

$$\begin{tikzcd}
\mathfrak{h}^i(Np^r, \mathcal{O}) & \mathfrak{h}^i(Np^s, \mathcal{O}) \arrow[l, two heads] \\
\mathfrak{h}^j(Np^r, \mathcal{O}) \arrow[u, two heads] & \mathfrak{h}^j(Np^s, \mathcal{O}), \arrow[l, two heads] \arrow[u, two heads]
\end{tikzcd} \tag{4.1}$$

in dem die Pfeile durch Einschränken dieser Operatoren auf die eingebetteten Teilräume gegeben sind. Dies ermöglicht uns die folgende Definition.

Definition 4.1: Die *universelle Hecke-Algebra von Level Np^∞* ist

$$\mathfrak{h}(N, \mathcal{O}) = \varprojlim_{i,r} \mathfrak{h}^i(Np^r, \mathcal{O}).$$

Wegen Bemerkung I.1.6 und Lemma I.1.5 ist dies in der Kategorie der proendlichen $\mathcal{O}$-Algebren wohldefiniert.

Bemerkung 4.2: In [Hid86a] definiert Hida zunächst zwei große Hecke-Algebren, bei denen jeweils das Gewicht bzw. das Level festgehalten werden und der Limes nur über das andere genommen wird:

$$\mathcal{h}_k(Np^\infty, \mathcal{O}) = \varprojlim_r \mathcal{h}_k(\Gamma_1(Np^r), \mathcal{O}) \quad \text{und} \quad \mathcal{h}(Np^r, \mathcal{O}) = \varprojlim_j \mathcal{h}^j(Np^r, \mathcal{O}).$$

Überraschenderweise kommt jedoch in beiden Fällen das gleiche heraus (wenn man $k = 1$ auslässt): es gilt kanonisch

$$\mathcal{h}(Np^r, \mathcal{O}) \cong \mathcal{h}_k(Np^\infty, \mathcal{O}) \text{ für alle } k \geq 2 \text{ und } r \geq 1$$

[Hid86a, (1.4), (1.7)]. Diese Hecke-Algebra ist dann natürlich isomorph zu der, die wir in Definition 4.1 definiert haben.

Wir wollen $\mathcal{h}(N, \mathcal{O})$ nun zu einer Algebra über $\mathcal{O}[\![\mathbb{Z}_{p,N}^\times]\!]$ machen, wobei $\mathbb{Z}_{p,N}$ wie in Definition I.2.1 definiert ist. Dazu setzen wir $\Gamma^{\mathrm{wt}} = 1 + p\mathbb{Z}_p \subseteq \mathbb{Z}_{p,N}^\times$ (die Bedeutung des Superskripts „wt" erklären wir später) und haben dann eine Zerlegung

$$\mathbb{Z}_{p,N}^\times \cong \left(\mathbb{Z}/Np\mathbb{Z}\right)^\times \times \Gamma^{\mathrm{wt}} \cong \left(\mathbb{Z}/N\mathbb{Z}\right)^\times \times \mathbb{Z}_p^\times. \tag{4.2}$$

Wir bezeichnen mit π_p die Projektion von $\mathbb{Z}_{p,N}^\times$ auf den Faktor $\mathbb{Z}_p^\times$ und schreiben $z \bmod Np^r$ für das Bild eines $z \in \mathbb{Z}_{p,N}^\times$ unter der Projektion

$$\mathbb{Z}_{p,N}^\times \twoheadrightarrow \left(\mathbb{Z}/Np^r\mathbb{Z}\right)^\times.$$

Für festes r und i definieren wir zu jedem $z \in \mathbb{Z}_{p,N}^\times$ einen Endomorphismus $[z]_{r,i}$ von

$$\mathcal{S}^i(Np^r) = \bigoplus_{k=1}^{i} \mathcal{S}_k(\Gamma_1(Np^r), \mathcal{O}),$$

der in der k-ten Komponente durch

$$f_k \longmapsto \pi_p(z)^k \langle z \bmod Np^r \rangle f_k \tag{4.3}$$

gegeben ist; vgl. hierzu [Hid86b, (1.12), S. 242]. Hierbei ist $\langle\cdot\rangle$ der Diamant-Operator aus Definition II.3.7 und $\pi_p(z)$ ist als Element von $\mathcal{O}^\times$ anzusehen.

Lemma 4.3: *Der Endomorphismus $[z]_{r,i}$ ist ein Element von $\mathcal{h}^i(Np^r)^\times$.*

Beweis: Wenn $[z]_{r,i} \in \mathcal{h}^i(Np^r)$ gilt, dann ist es auch eine Einheit, denn $[z^{-1}]_{r,i}$ ist dann ein Inverses. Es genügt also, $[z]_{r,i} \in \mathcal{h}^i(Np^r)$ zu zeigen. Dazu wählen wir ein $\gamma \in \Gamma_0(Np^r)$ mit

$$\gamma \equiv \begin{pmatrix} * & * \\ 0 & z \end{pmatrix} \bmod Np^r$$

und setzen $\alpha = \pi_p(z) \in \mathcal{O}^\times$. Wir schreiben ein $f \in \mathcal{S}^i(Np^r)$ als Summe $f = \sum_{k=1}^i f_k$ mit $f_k \in \mathcal{S}_k(\Gamma_1(Np^r), \mathcal{O})$. Auf $\mathcal{S}_k(\Gamma_1(Np^r), \mathcal{O})$ gilt nach (II.4.2)

$$[\Gamma_1(N)\alpha\gamma\Gamma_1(N)]_k f_k = (\alpha^2)^{k/2-1}(\det\gamma)^{k/2-1}\sum_{i=1}^{e} f_k[\beta_i]_k = \alpha^{k-2}[\Gamma_1(N)\gamma\Gamma_1(N)]_k f_k,$$

wenn die β_i wie dort Repräsentanten für die Linksnebenklassen sind. Wegen Beispiel II.4.2 gilt ferner $[\Gamma_1(N)\gamma\Gamma_1(N)]_k f_k = \langle z \bmod Np^r\rangle f_k$, also bekommen wir

$$[z]_{r,i} f = \sum_{k=1}^{i} \alpha^k \langle z \bmod Np^r\rangle f_k = \alpha^2 \sum_{k=1}^{i} [\Gamma_1(N)\alpha\gamma\Gamma_1(N)]_k f_k,$$

also $[z]_{r,i} = \alpha^2[\Gamma_1(N)\alpha\gamma\Gamma_1(N)]$ gemäß der Definition der Aktion von Doppelnebenklassen auf $\mathcal{S}^i(Np^r)$. Dies zeigt die Behauptung. □

Also definiert

$$\mathbb{Z}_{p,N}^\times \longrightarrow \hbar^i(Np^r)^\times, \quad z \longmapsto [z]_{r,i} \tag{4.4}$$

einen Gruppenhomomorphismus, und man überlegt sich leicht, dass dieser mit den Restriktionsabbildungen zwischen den Hecke-Algebren verträglich ist. Daraus bekommen wir einen Homomorphismus

$$\mathbb{Z}_{p,N}^\times \longrightarrow \hbar(N, \mathcal{O})^\times, \quad z \longmapsto [z], \tag{4.5}$$

und die universelle Eigenschaft der proendlichen Gruppenalgebra induziert wiederum einen $\mathcal{O}$-Algebren-Homomorphismus

$$\mathcal{O}[\![\mathbb{Z}_{p,N}^\times]\!] \longrightarrow \hbar(N, \mathcal{O}).$$

Auf diese Weise können wir $\hbar(N, \mathcal{O})$ zu einer Algebra über $\mathcal{O}[\![\mathbb{Z}_{p,N}^\times]\!]$ machen.

Es sei nun $\Lambda^{\mathrm{wt}} = \mathcal{O}[\![\Gamma^{\mathrm{wt}}]\!]$. Da Γ^{wt} eine Untergruppe von $\mathbb{Z}_{p,N}^\times$ ist, gibt dies $\hbar(N, \mathcal{O})$ insbesondere die Struktur einer Λ^{wt}-Algebra.

4.2. Die ordinäre Teilalgebra

Die Hecke-Algebra $\hbar(N, \mathcal{O})$ ist so noch „zu groß“: sie ist als Λ^{wt}-Modul nicht endlich erzeugt. Das wollen wir zunächst einsehen, indem wir zeigen, dass der Rang von $\mathcal{S}_k(\Gamma_1(Np^r), \mathcal{O})$ als $\mathcal{O}[\![\mathbb{Z}_{p,N}^\times]\!]$-Modul unbeschränkt ist, wenn k und r wachsen.

Dazu sei G eine beliebige endliche Gruppe und M ein $\mathcal{O}[G]$-Modul, der als $\mathcal{O}$-Modul frei von endlichem Rang ist. Für jedes $s \in M$ ist dann $\mathrm{Rang}_{\mathcal{O}}(\mathcal{O}[G]s) \le \#G$, und da der Rang subadditiv ist, gilt für jedes endliche $\mathcal{O}[G]$-Erzeugendensystem S von M, dass

$$\mathrm{Rang}_{\mathcal{O}}(M) = \mathrm{Rang}_{\mathcal{O}}\Big(\sum_{s\in S} \mathcal{O}[G]s\Big) \le \#S \cdot \#G.$$

Daraus folgt

$$\min\{\#S \mid S \subseteq M \text{ erzeugt } M \text{ als } \mathcal{O}[G]\text{-Modul}\} \ge \frac{\mathrm{Rang}_{\mathcal{O}}(M)}{\#G}.$$

Wenn wir in der Definition (4.3) der Aktion von $\mathcal{O}[\![\mathbb{Z}_{p,N}^\times]\!]$ auf $\mathcal{S}_k(\Gamma_1(Np^r), \mathcal{O})$ den Faktor $\pi_p(z)^k$ weglassen, faktorisiert diese Aktion über $\mathcal{O}[G]$ mit $G = (\mathbb{Z}/Np^r\mathbb{Z})^\times$. Da dieser Faktor den Rang nicht beeinflusst, genügt es uns also zu zeigen, dass

$$\frac{\operatorname{Rang}_{\mathcal{O}}(\mathcal{S}_k(\Gamma_1(Np^r), \mathcal{O}))}{\phi(Np^r)}$$

unbeschränkt ist. Wegen Bemerkung 1.4 stimmt $\operatorname{Rang}_{\mathcal{O}}(\mathcal{S}_k(\Gamma_1(Np^r), \mathcal{O}))$ mit der Dimension von $\mathcal{S}_k(\Gamma_1(Np^r))$ als $\mathbb{C}$-Vektorraum überein, und für diese hatten wir in Bemerkung II.3.4 eine Formel angegeben. An dieser sieht man bereits mit sehr groben Abschätzungen die Unbeschränktheit des obigen Ausdrucks.

Man kann aber eine bestimmte Teilalgebra von $\hbar(N, \mathcal{O})$ ausschneiden, die endlichen Λ^{wt}-Rang hat. Um dies zu erklären, benötigen wir das folgende Lemma, welches wir aus [HidLFE, §7.2, Lemma 1] zitieren:

Lemma 4.4: *Sei $\mathcal{O}$ der Ganzheitsring in einer endlichen Erweiterung von $\mathbb{Q}_p$ und H eine kommutative $\mathcal{O}$-Algebra, die als $\mathcal{O}$-Modul endlich erzeugt ist. Dann existiert für jedes $x \in H$ der Grenzwert*

$$e := \lim_{n\to\infty} x^{n!} \in H$$

und e ist idempotent.

Wir wollen dies auf den Fall $H = \hbar^i(Np^r, \mathcal{O})$ und $x = T_p$ anwenden und setzen also

$$e_{i,r} := \lim_{n\to\infty} T_p^{n!} \in \hbar^i(Np^r, \mathcal{O}).$$

Die Kommutativität des Diagramms (4.1) zeigt, dass diese Elemente von den Pfeilen im Diagramm aufeinander abgebildet werden. Dadurch können wir ein $e \in \hbar(N, \mathcal{O})$ definieren, welches immer noch idempotent ist.

Definition 4.5: Die *universelle ordinäre Hecke-Algebra von Level Np^∞* ist

$$\hbar^{\mathrm{ord}}(N, \mathcal{O}) = e\hbar(N, \mathcal{O}).$$

Das Element $e \in \hbar(N, \mathcal{O})$ heißt die *ordinäre Projektion.*

Dann gilt:

Satz 4.6: *Sei $p \geq 5$. Dann ist $\hbar^{\mathrm{ord}}(N, \mathcal{O})$ als Λ^{wt}-Modul frei von endlichem Rang.*

Beweis: [Hid86b, Thm. 3.1] □

Für festes Level und Gewicht definieren wir analog für eine Kongruenzuntergruppe Φ mit $\Gamma_1(Np^r) \subseteq \Phi \subseteq \Gamma_0(Np^r)$ und einen Charakter ε von $\Phi/\Gamma_1(Np^r)$

$$e := \lim_{n\to\infty} T_p^{n!} \in \hbar_k(\Phi, \varepsilon, \mathcal{O})$$

und setzen $\hbar_k^{\mathrm{ord}}(\Phi, \varepsilon, \mathcal{O}) = e\hbar_k(\Phi, \varepsilon, \mathcal{O})$ und $\mathcal{S}_k^{\mathrm{ord}}(\Phi, \varepsilon, \mathcal{O}) = e\mathcal{S}_k(\Phi, \varepsilon, \mathcal{O})$. Die Elemente $f \in \mathcal{S}_k^{\mathrm{ord}}(\Phi, \varepsilon, \mathcal{O})$ nennen wir *ordinär.* Es ist also f genau dann ordinär, wenn $ef = f$. Wenn f ein Eigenvektor von T_p mit Eigenwert $a \in \mathcal{O}$ ist, dann gilt

$$ef = \begin{cases} f, & |a|_p = 1, \\ 0, & |a|_p < 1. \end{cases}$$

Insbesondere ist eine Eigenform genau dann ordinär, wenn ihr p-ter Fourierkoeffizient eine Einheit in $\mathcal{O}$ ist.

4.3. Kontrolltheorie und Hida-Familien

Aus der Hecke-Algebra $\mathfrak{h}^{\mathrm{ord}}(N,\mathcal{O})$ können wir durch Reduktion modulo gewisser Primideale die Hecke-Algebren zu festem Gewicht und Level zurückerhalten. Dies wird als Kontrolltheorie bezeichnet. Wir wollen nun erklären, wie das funktioniert.

Sei dazu $r \in \mathbb{N}$. Mit Γ_r^{wt} bezeichnen wir die Untergruppe $1+p^r\mathbb{Z}_p \subseteq \Gamma^{\mathrm{wt}}$. Wir definieren $\Phi_r = \Gamma_1(Np) \cap \Gamma_0(p^r)$ und wollen nun Definition II.3.6 auf den Fall $\Delta = \Phi_r$ und $\Gamma = \Gamma_1(Np^r)$ anwenden. Der Quotient Δ/Γ ist in dieser Situation isomorph zu $\Gamma^{\mathrm{wt}}/\Gamma_r^{\mathrm{wt}}$, der Isomorphismus wird von

$$\Phi_r \ni \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto d \in 1+Np\mathbb{Z} \subseteq 1+p\mathbb{Z}_p = \Gamma^{\mathrm{wt}} \twoheadrightarrow \Gamma^{\mathrm{wt}}\big/\Gamma_r^{\mathrm{wt}}$$

induziert. Wir bezeichnen also für einen Charakter ε von $\Gamma^{\mathrm{wt}}/\Gamma_r^{\mathrm{wt}}$ (den wir mit der obigen Abbildung als Charakter von Φ_r auffassen können) mit

$$\mathcal{S}_k(\Phi_r,\varepsilon) = \{f \in \mathcal{S}_k(\Gamma_1^{\mathrm{wt}}(Np^r)) \mid \forall \gamma \in \Phi_r : f[\gamma]_k = \varepsilon(\gamma)f\}$$

seinen Eigenraum und haben dann

$$\mathcal{S}_k(\Gamma_1(Np^r)) = \bigoplus_{\varepsilon} \mathcal{S}_k(\Phi_r,\varepsilon).$$

Wegen (I.2.4) gilt

$$\left(\mathbb{Z}\big/Np^r\mathbb{Z}\right)^{\times} \cong \left(\mathbb{Z}\big/Np\mathbb{Z}\right)^{\times} \times \Gamma^{\mathrm{wt}}\big/\Gamma_r^{\mathrm{wt}},$$

deshalb können wir jeden Dirichlet-Charakter χ modulo Np^r auf eindeutige Weise als Produkt $\chi = \varepsilon\psi$ eines Charakters ε von $\Gamma^{\mathrm{wt}}/\Gamma_r^{\mathrm{wt}}$ und eines Dirichlet-Charakters ψ modulo Np schreiben. Da auch

$$\mathcal{S}_k(\Gamma_1(Np^r)) = \bigoplus_{\chi} \mathcal{S}_k(Np^r,\chi)$$

gilt, erhalten wir

$$\mathcal{S}_k(\Phi_r,\varepsilon) = \bigoplus_{\psi} \mathcal{S}_k(Np^r,\varepsilon\psi), \tag{4.6}$$

wobei in dieser letzten Summe ψ alle Dirichlet-Charaktere modulo Np durchläuft.

Die Charaktere ε von $\Gamma^{\mathrm{wt}}/\Gamma_r^{\mathrm{wt}}$ für ein $r \in \mathbb{N}$ können mit den Charakteren von Γ^{wt} von endlicher Ordnung identifiziert werden. Mit ι bezeichnen wir die kanonische Einbettung

$$\Gamma^{\mathrm{wt}} \hookrightarrow \mathcal{O}^{\times}.$$

Wir betrachten den von

$$\Gamma^{\mathrm{wt}} \longrightarrow \mathcal{O}^{\times}, \quad \gamma \longmapsto \varepsilon(\gamma)\iota(\gamma)^k$$

induzierten $\mathcal{O}$-Algebren-Homomorphismus $\eta_{k,\varepsilon}\colon \Lambda^{\mathrm{wt}} \longrightarrow \mathcal{O}$ und bezeichen mit $P_{k,\varepsilon} \subseteq \Lambda^{\mathrm{wt}}$ dessen Kern. Da $\mathcal{O}$ nullteilerfrei ist, ist dieser ein Primideal. Dann lautet die fundamentale Aussage [Hid86a, Thm. 1.2]

Satz 4.7 (Hidas Kontrolltheorem): *Die Zuordnung $T_n \longmapsto T_n$ induziert einen kanonischen Isomorphismus von $\mathcal{O}$-Algebren*

$$\mathscr{h}^{\mathrm{ord}}(N, \mathcal{O}) \Big/ P_{k,\varepsilon}\mathscr{h}^{\mathrm{ord}}(N, \mathcal{O}) \cong \mathscr{h}_k^{\mathrm{ord}}(\Phi_r, \varepsilon, \mathcal{O})$$

für jeden Charakter ε von Γ^{wt} von endlicher Ordnung mit Werten in $\mathcal{O}$ und $k \geq 2$. Hierbei ist r durch $\mathrm{Kern}\,\varepsilon = \Gamma_r^{\mathrm{wt}}$ *definiert.*

Daran sehen wir, dass die Gruppe Γ^{wt} die Rolle einer *Gewichtsgruppe* spielt: denn jedes $\gamma \in \Gamma^{\mathrm{wt}}$ ist von der Form $\gamma = (1+p)^s$ mit einem $s \in \mathbb{Z}_p$, und indem wir k durch s ersetzen, können wir $P_{\gamma,\varepsilon} := P_{s,\varepsilon}$ genauso definieren wie oben. Für die ganzzahligen s „ist" dann γ gerade das Gewicht. Dadurch wird nun auch die Bedeutung des Superskripts „wt" klar: dieses steht für „weight". Entsprechend bezeichnen wir Λ^{wt} als die *Gewichts-Iwasawa-Algebra.*

Gemäß der Philosophie, dass Eigenformen Punkte der Hecke-Algebra sind, machen wir nun die folgende Definition.

Definition 4.8: Wir setzen

$$\mathcal{S}^{\mathrm{ord}}(N, \mathcal{O}) = \mathrm{Hom}(\mathscr{h}^{\mathrm{ord}}(N, \mathcal{O}), \mathcal{O}[\![\mathbb{Z}_{p,N}^{\times}]\!]).$$

Hier sind $\mathcal{O}[\![\mathbb{Z}_{p,N}^{\times}]\!]$-Modulhomomorphismen gemeint.

Die natürliche Aktion der Hecke-Algebra $\mathscr{h}^{\mathrm{ord}}(N, \mathcal{O})$ auf $\mathcal{S}^{\mathrm{ord}}(N, \mathcal{O})$ ist dann durch

$$Tf(h) = f(Th), \quad T, h \in \mathscr{h}^{\mathrm{ord}}(N, \mathcal{O}),\ f \in \mathcal{S}^{\mathrm{ord}}(N, \mathcal{O})$$

gegeben. Nach Definition ist $\mathcal{S}^{\mathrm{ord}}(N, \mathcal{O})$ ein $\mathcal{O}[\![\mathbb{Z}_{p,N}^{\times}]\!]$ Modul. Damit können können wir wie in Abschnitt I.2.1 für jeden Dirichlet-Charakter ψ modulo Np den Unterraum

$$\mathcal{S}^{\mathrm{ord}}(N, \psi, \mathcal{O})$$

definieren, auf der $(\mathbb{Z}/Np\mathbb{Z})^{\times}$ durch ψ operiert (vgl. (I.2.1)). Wenn $\phi(N)$ in $\mathcal{O}$ invertierbar ist und $\mathcal{O}$ die Werte aller Dirichlet-Charaktere modulo Np enthält, haben wir eine Zerlegung

$$\mathcal{S}^{\mathrm{ord}}(N, \mathcal{O}) = \bigoplus_{\psi} \mathcal{S}^{\mathrm{ord}}(N, \psi, \mathcal{O}).$$

Die Unterräume $\mathcal{S}^{\mathrm{ord}}(N, \psi, \mathcal{O})$ sind unter der Aktion der Hecke-Operatoren stabil, wie man mit Beispiel II.4.2 und der Kommutativität der Hecke-Algebra leicht sieht. Damit erhalten wir durch Einschränken der Hecke-Operatoren von $\mathcal{S}^{\mathrm{ord}}(N, \mathcal{O})$ auf den Unterraum $\mathcal{S}^{\mathrm{ord}}(N, \psi, \mathcal{O})$ einen Homomorphismus

$$\mathscr{h}^{\mathrm{ord}}(N, \mathcal{O}) \longrightarrow \mathrm{End}(\mathcal{S}^{\mathrm{ord}}(N, \psi, \mathcal{O})).$$

Dessen Bild bezeichnen wir mit $\mathscr{h}^{\mathrm{ord}}(N, \psi, \mathcal{O})$.

Definition 4.9: Eine *ordinäre Λ^{wt}-adische Eigenform mit Nebentyp ψ* ist ein Λ^{wt}-Algebren-Homomorphismus

$$\mathscr{h}^{\mathrm{ord}}(N, \psi, \mathcal{O}) \longrightarrow \Lambda^{\mathrm{wt}}.$$

Da wir nur ordinäre Λ^{wt}-adische Eigenformen betrachten werden, lassen wir „ordinär" meist weg.

Korollar 4.10: *Es gilt für k, ε und r wie in Satz 4.7*

$$\hbar^{\mathrm{ord}}(N,\psi,\mathcal{O})\Big/P_{k,\varepsilon}\hbar^{\mathrm{ord}}(N,\psi,\mathcal{O}) \cong \hbar_k^{\mathrm{ord}}(Np^r,\varepsilon\psi\omega^{-k},\mathcal{O}).$$

Hierbei bezeichnet ω den Teichmüller-Charakter, siehe Bemerkung 1.5.2

Beweis: Die Algebra H in dem Diagramm

$$\begin{tikzcd}
\hbar^{\mathrm{ord}}(N,\mathcal{O}) \arrow[r, two heads] \arrow[d, two heads] & \hbar^{\mathrm{ord}}(N,\mathcal{O})/(P_{k,\varepsilon}) \arrow[r, "\sim"] \arrow[d, two heads] & \hbar_k^{\mathrm{ord}}(\Phi_r,\varepsilon,\mathcal{O}) \arrow[d, two heads] \\
\hbar^{\mathrm{ord}}(N,\psi,\mathcal{O}) \arrow[r, two heads] & \hbar^{\mathrm{ord}}(N,\psi,\mathcal{O})/(P_{k,\varepsilon}) \arrow[r, "\sim"] & H
\end{tikzcd}$$

entspricht über die Dualität aus Satz 2.3 dem Teilraum U von $\mathcal{S}_k^{\mathrm{ord}}(\Phi_r,\varepsilon,\mathcal{O})$, auf dem die Operation der Gruppe $(\mathbb{Z}/Np\mathbb{Z})^\times$, die in (4.4) definiert ist, durch ψ gegeben ist. An der Zerlegung (4.2) sehen wir, dass die Komposition

$$\left(\mathbb{Z}\big/Np\mathbb{Z}\right)^\times \hookrightarrow \left(\mathbb{Z}\big/Np\mathbb{Z}\right)^\times \times \Gamma^{\mathrm{wt}} = \mathbb{Z}_{p,N}^\times = \left(\mathbb{Z}\big/N\mathbb{Z}\right)^\times \times \mathbb{Z}_p^\times \xrightarrow{\pi_p} \mathbb{Z}_p^\times$$

durch ω gegeben ist, wenn wir diesen als Charakter von $(\mathbb{Z}/Np\mathbb{Z})^\times$ auffassen. Deshalb ist die Aktion eines $a \in (\mathbb{Z}/Np\mathbb{Z})^\times$ auf einem $f \in U$ durch

$$[a]f = \omega(a)^k \langle a\rangle f$$

gegeben. Da diese andererseits durch Multiplikation mit $\psi(a)$ gegeben ist, folgt

$$\langle a\rangle f = \psi\omega^{-k}(a)f$$

für $a \in (\mathbb{Z}/Np\mathbb{Z})^\times$. Damit folgt für

$$z = (a,b) \in \left(\mathbb{Z}\big/Np\mathbb{Z}\right)^\times \times \Gamma^{\mathrm{wt}}\big/\Gamma_r^{\mathrm{wt}} = \left(\mathbb{Z}\big/Np^r\mathbb{Z}\right)^\times$$

und $f \in U$, dass

$$\langle z\rangle f = \psi\omega^{-k}(a)\varepsilon(b)f = \varepsilon\psi\omega^{-k}(z)f$$

und deshalb $U = \mathcal{S}_k^{\mathrm{ord}}(Np^r,\varepsilon\psi\omega^{-k},\mathcal{O})$ wie behauptet. □

Wenn eine Λ^{wt}-adische Eigenform $F\colon \hbar^{\mathrm{ord}}(N,\psi,\mathcal{O}) \longrightarrow \Lambda^{\mathrm{wt}}$ gegeben ist, können wir diesen Homomorphismus für jedes $k \geq 2$ und jeden Charakter ε von Γ^{wt} von endlicher Ordnung modulo $P_{k,\varepsilon}$ reduzieren und erhalten daraus einen Homomorphismus

$$\hbar_k^{\mathrm{ord}}(Np^r,\varepsilon\psi\omega^{-k},\mathcal{O}) \xrightarrow{\sim} \hbar^{\mathrm{ord}}(N,\psi,\mathcal{O})\Big/P_{k,\varepsilon}\hbar^{\mathrm{ord}}(N,\psi,\mathcal{O}) \longrightarrow \Lambda^{\mathrm{wt}}\big/P_{k,\varepsilon} \longrightarrow \mathcal{O}.$$

Dieser entspricht einer Eigenform $f_{k,\varepsilon} \in \mathcal{S}_k^{\mathrm{ord}}(Np^r, \varepsilon\psi\omega^{-k}, \mathcal{O})$. Eine Λ^{wt}-adische Eigenform produziert also eine ganze Familie $(f_{k,\varepsilon})_{k,\varepsilon}$ von Eigenformen mit Koeffizienten in $\mathcal{O}$. Wenn wir aus F eine formale q-Entwicklung

$$F(q) = \sum_{n=1}^{\infty} F(T_n) q^n \in \Lambda^{\mathrm{wt}}[\![q]\!]$$

bilden, bekommen wir hieraus die q-Entwicklung von $f_{k,\varepsilon}$, indem wir $\eta_{k,\varepsilon}$ auf die Koeffizienten anwenden:

$$f_{k,\varepsilon}(q) = \eta_{k,\varepsilon}(F(q)) = \sum_{n=1}^{\infty} \eta_{k,\varepsilon}(F(T_n)) q^n \in \mathcal{O}[\![q]\!].$$

Aus diesem Grund nennen wir eine Λ^{wt}-adische Eigenform auch eine *Hida-Familie*.

Die Fourierkoeffizienten einer normalisierten Eigenform $f \in \mathcal{S}_k^{\mathrm{ord}}(Np^r, \varepsilon\psi\omega^{-k})$ liegen wegen Korollar 2.8 in einer endlichen algebraischen Erweiterung von $\mathbb{Q}$ in K, und mit unserer gewählten Einbettung $\overline{\mathbb{Q}}_p \hookrightarrow \mathbb{C}$ können wir sie als komplexe Zahlen auffassen. Daran sehen wir mit Satz 1.1, dass die Mitglieder eine Hida-Familie sogar klassische komplexe Eigenformen sind.

Es sei abschließend noch erwähnt, dass jede ordinäre Eigenform in einer Hida-Familie lebt: dies wird z.B. in [Wil88, Thm. 1.4.1] gezeigt.

4.4. Die große Galoisdarstellung

Wir haben in Satz 3.1 einer Eigenform $f \in \mathcal{S}_k(\Gamma_1(N), \mathcal{O})$ eine Galoisdarstellung zugeordnet, deren Frobenius-Polynome bei den unverzweigten Primzahlen mit den entsprechenden Hecke-Polynomen der Eigenform übereinstimmt. Diese Darstellungen wollen wir nun zu einer großen Galoisdarstellung zusammenbauen, die Werte in der universellen Hecke-Algebra annimmt.

Wegen Satz 4.6 erfüllt $\hbar^{\mathrm{ord}}(N, \mathcal{O})$ die Voraussetzungen von Lemma 2.9 und ist deshalb ein endliches Produkt lokaler Ringe:

$$\hbar^{\mathrm{ord}}(N, \mathcal{O}) = \prod_{\mathfrak{m}} \hbar_{\mathfrak{m}}.$$

Wenn eine Λ^{wt}-adische Eigenform $F\colon \hbar^{\mathrm{ord}}(N, \psi, \mathcal{O}) \longrightarrow \Lambda^{\mathrm{wt}}$ mit einem Nebentyp ψ gegeben ist, faktorisiert die Komposition

$$\hbar^{\mathrm{ord}}(N, \mathcal{O}) \twoheadrightarrow \hbar^{\mathrm{ord}}(N, \psi, O) \xrightarrow{F} \Lambda^{\mathrm{wt}}$$

über genau einen dieser lokalen Ringe, und auf diese Weise können wir jeder Λ^{wt}-adischen Eigenform ein maximales Ideal zuordnen, genauso wie wir dies Abschnitt 3 für eine einzelne Eigenform gemacht hatten. Wir wählen einen solchen lokalen Ring aus, der zu einem maximalen Ideal $\mathfrak{m}$ von $\hbar^{\mathrm{ord}}(N, \mathcal{O})$ gehört. Für jedes $k \geq 2$ und $r \in \mathbb{N}$ können wir $\mathfrak{m}$ nach $\hbar_k^{\mathrm{ord}}(\Gamma_1(Np^r), \mathcal{O})$ projizieren, wenn wir mit Bemerkung 4.2

$$\hbar(N, \mathcal{O}) = \lim_{r} \hbar_k(\Gamma_1(Np^r), \mathcal{O})$$

schreiben, und erhalten dann dort ein maximales Ideal $\mathfrak{m}_{k,r}$. Daran sehen wir zunächst, dass die Restklassenkörper

$$\mathscr{h}^{\mathrm{ord}}(N,\mathcal{O})\big/\mathfrak{m} \quad \text{und} \quad \mathscr{h}_k^{\mathrm{ord}}(\Gamma_1(Np^r),\mathcal{O})\big/\mathfrak{m}_{k,r}$$

übereinstimmen, und wegen Lemma 2.11 ist dieser der Restklassenkörper $\mathbb{F}$ von $\mathcal{O}$.

Mit Korollar 4.10 sehen wir, dass es zu jeden $k \geq 2$ und $r \in \mathbb{N}_0$ eine Eigenform $f \in \mathcal{S}_k^{\mathrm{ord}}(Np^r, \varepsilon\psi\omega^{-k}, \mathcal{O})$ für ein passendes ε gibt, sodass $\mathfrak{m}_{k,r}$ das zu f gehörende maximale Ideal ist. Also können wir die Restklassendarstellung $\overline{\rho}_{k,r}$ von $\mathfrak{m}_{k,r}$ betrachten. Wir nehmen an, dass diese absolut irreduzibel ist.

Lemma 4.11: $\overline{\rho}_{k,r}$ *ist unabhängig von* k *und* r.

Beweis: Wir nehmen ein $j \geq 2$ und ein $s \in \mathbb{N}$, sodass die Restklassendarstellung $\overline{\rho}_{j,s}$ ebenfalls absolut irreduzibel ist. In diesem Fall finden wir $\mathcal{O}$-Algebren-Homomorphismen

$$\lambda_{k,r}\colon \mathscr{h}_k^{\mathrm{ord}}(\Gamma_1(Np^r),\mathcal{O}) \longrightarrow \mathcal{O}, \quad \lambda_{j,s}\colon \mathscr{h}_j^{\mathrm{ord}}(\Gamma_1(Np^s),\mathcal{O}) \longrightarrow \mathcal{O},$$

sodass die Restklassendarstellungen die Reduktionen der Darstellungen $\rho_{k,r}$ bzw. $\rho_{j,s}$ der zu $\lambda_{k,r}$ bzw. $\lambda_{j,s}$ gehörenden Eigenformen modulo dem maximalen Ideal (π) von $\mathcal{O}$ sind. Wir bezeichnen mit $g_{k,r}$ die Komposition

$$\mathscr{h}^{\mathrm{ord}}(N,\mathcal{O}) \longrightarrow \mathscr{h}_k^{\mathrm{ord}}(\Gamma_1(Np^r),\mathcal{O}) \xrightarrow{\lambda_{k,r}} \mathcal{O}$$

und entsprechend für $g_{j,s}$. Diese induzieren dann Isomorphismen

$$\overline{g}_{k,r}, \overline{g}_{j,s}\colon \ \mathscr{h}^{\mathrm{ord}}(N,\mathcal{O})\big/\mathfrak{m} \xrightarrow{\ \sim\ } \mathbb{F},$$

und wegen Lemma 2.10 (d) stimmen diese überein. Damit gilt

$$\mathrm{Spur}(\rho_{k,r}(\mathrm{Frob}_\ell)) = \lambda_{k,r}(T_\ell) = g_{k,r}(T_\ell) \equiv g_{j,s}(T_\ell) = \mathrm{Spur}(\rho_{f_{j,s}}(\mathrm{Frob}_\ell)) \mod \pi,$$

und deshalb folgt die Behauptung aus Bemerkung 1.6.6. □

Definition 4.12: Die *Restklassendarstellung eines maximalen Ideals* $\mathfrak{m}$ von $\mathscr{h}^{\mathrm{ord}}(N,\mathcal{O})$ ist $\overline{\rho}_{k,r}$, falls diese für ein k und r absolut irreduzibel ist.

Wenn kein $\overline{\rho}_{k,r}$ absolut irreduzibel ist, lassen wir die Restklassendarstellung von $\mathfrak{m}$ undefiniert. Wir sind manchmal etwas ungenau und sagen, dass die Restklassendarstellung eines $\mathfrak{m}$ absolut irreduzibel sein soll; damit sei dann stets gemeint, dass diese definiert sein soll.

Wir bezeichnen nun mit $W \subseteq \mathcal{O}$ den Ganzheitsring der maximalen unverzweigten Teilerweiterung von $K|\mathbb{Q}_p$. Damit stimmen die Restklassenkörper $\mathbb{F}$ von W und $\mathcal{O}$ überein, und W ist der Ring der Witt-Vektoren dieses Restklassenkörpers [Ser79, Chap. II, Thm. 3 und Thm. 7]. Weiter sei nun $p \neq 2$.

Satz 4.13: *Es sei $\mathfrak{m}$ ein maximales Ideal von $\mathfrak{h}^{\mathrm{ord}}(N,W)$, sodass die Restklassendarstellung von $\mathfrak{m}$ absolut irreduzibel und bei p verzweigt ist. Dann gibt es eine bis auf Isomorphie eindeutige ungerade Galoisdarstellung*

$$\rho_{\mathfrak{m}}\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathfrak{h}_{\mathfrak{m}}),$$

die außerhalb von $Np\infty$ unverzweigt ist, und so, dass

$$\mathrm{Spur}(\mathrm{Frob}_\ell) = T_\ell, \quad \det(\mathrm{Frob}_\ell) = \frac{1}{\ell}[\ell]$$

für alle Primzahlen $\ell \nmid Np$ gilt. Hierbei bezeichnet $[\cdot]$ den Homomorphismus aus (4.5). Die Einschränkung von $\rho_{\mathfrak{m}}$ auf die Zerlegungsgruppe D_p ist isomorph zu einer oberen Dreiecksdarstellung

$$\rho_f|_{D_p} \cong \begin{pmatrix} \varepsilon & * \\ & \delta \end{pmatrix},$$

und δ ist unverzweigt.

Beweis: [Gou90, Thm. 4] und [Gou88, Thm. III.5.6]. Dort wird $p \geq 7$ angenommen, aber in [Böc01, S. 991] wird ein Weg erwähnt, wie die Argumente für $p = 3$ und $p = 5$ angepasst werden können. □

Satz 4.14: *Es sei $f \in \mathcal{S}_k^{\mathrm{ord}}(\Phi_r, \varepsilon, \mathcal{O})$ eine Eigenform,*

$$\lambda\colon\ \mathfrak{h}_k^{\mathrm{ord}}(\Phi_r, \varepsilon, W) \longrightarrow \mathcal{O}$$

der zugehörige Homomorphismus (vgl. Bemerkung 2.7) und ρ_f die Galoisdarstellung zu f. Es bezeichne P_f den Kern des Homomorphismus'

$$\mathfrak{h}^{\mathrm{ord}}(N,W) \twoheadrightarrow \mathfrak{h}^{\mathrm{ord}}(N,W)\Big/P_{k,\varepsilon}\mathfrak{h}^{\mathrm{ord}}(N,W) \xrightarrow{\ \sim\ } \mathfrak{h}_k^{\mathrm{ord}}(\Phi_r, \varepsilon, W) \xrightarrow{\ \lambda\ } \mathcal{O}$$

und es sei $\mathfrak{m}$ das maximale Ideal von $\mathfrak{h}^{\mathrm{ord}}(N,W)$, über das dieser faktorisiert. Unter den Voraussetzungen aus Satz 4.13 gilt dann

$$\rho_{\mathfrak{m}} \bmod P_f = \rho_f.$$

Beweis: Nach Konstruktion gilt für Primzahlen $\ell \nmid Np$

$$\mathrm{Spur}(\rho_{\mathfrak{m}}(\mathrm{Frob}_\ell)) \bmod P_f = T_\ell \bmod P_f = a_\ell = \mathrm{Spur}(\rho_f(\mathrm{Frob}_\ell)),$$

und damit folgt die Behauptung aus Bemerkung I.6.6. □

5. Deformationstheorie

Wir haben in Abschnitt 4.4 eine absolut irreduzible Darstellung

$$\overline{\rho}\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F})$$

mit Koeffizienten in einem endlichen Körper betrachtet, die von einer Modulform herkam, und dazu in Satz 4.13 eine Darstellung $\rho_{\mathfrak{m}}$ mit Koeffizienten in dem sehr viel größeren Ring $\mathbb{h}_{\mathfrak{m}}$ angegeben. Diese hat nach Satz 4.14 die Eigenschaft, dass wir für jede weitere Eigenform f, deren Restklassendarstellung mit $\overline{\rho}$ übereinstimmt, die zu f gehörende Darstellung ρ_f mit Koeffizenten in $\mathcal{O}$ aus der großen Darstellung $\rho_{\mathfrak{m}}$ zurückgewinnen können, indem wir letztere mit einem geeigneten Homomorphismus $\mathbb{h}_m \longrightarrow \mathcal{O}$ verketten. Diese Situation wollen wir nun abstrakt nachbauen.

Dass zwei Eigenformen dieselbe Restklassendarstellung haben, bedeutet nichts anderes, als dass ihre Darstellungen (und damit ihre n-ten Fourierkoeffizienten für $(n, Np) = 1$) modulo π übereinstimmen, wenn π ein Primelement von $\mathcal{O}$ bezeichnet. Die zu einer gegebenen Restklassendarstellung gehörenden Eigenformen und ihre Galoisdarstellungen liegen also π-adisch nahe beieinander. Deshalb stellt man sie sich als „Deformationen" voneinander vor.

5.1. Deformationsringe

Im Folgenden sei $\mathcal{O}$ stets der Ganzheitsring in einer endlichen Erweiterung von $\mathbb{Q}_p$ und $\mathbb{F}$ der Restklassenkörper.

Definition 5.1: Es sei G eine proendliche Gruppe und $\overline{\rho}$ eine gegebene Darstellung

$$\overline{\rho}\colon G \longrightarrow \mathrm{GL}_n(\mathbb{F}).$$

Weiter sei A eine lokale $\mathcal{O}$-Algebra, deren Restklassenkörper mit dem von $\mathcal{O}$ übereinstimmt, und $\mathfrak{m}$ das maximale Ideal in A.

Eine Darstellung

$$\rho\colon G \longrightarrow \mathrm{GL}_n(A)$$

heißt eine *Deformation* von $\overline{\rho}$, wenn

$$\rho \bmod \mathfrak{m} = \overline{\rho}.$$

Es war eine Idee von Mazur, solche Deformationen systematisch zu studieren [Maz89]. Um diese zu erklären, bezeichnen wir mit $\mathcal{PAL}\text{-}\mathcal{Alg}(\mathcal{O})$ die Kategorie der pro-artinschen lokalen $\mathcal{O}$-Algebren mit Restklassenkörper $\mathbb{F}$ mit $\mathcal{O}$-Algebren-Homomorphismen.[4] Durch die Forderung der übereinstimmenden Restklassenkörper sind automatisch alle Morphismen in dieser Kategorie lokal. Weiter fixieren wir eine proendliche Gruppe G und eine Restklassendarstellung

$$\overline{\rho}\colon G \longrightarrow \mathrm{GL}_n(\mathbb{F}).$$

[4] Sie ist die pro-Kategorie der Kategorie der artinschen lokalen $\mathcal{O}$-Algebren mit Restklassenkörper $\mathbb{F}$, wie man sich leicht überlegt.

Wir nennen zwei Deformationen $\rho, \rho' : G \longrightarrow \mathrm{GL}_n(A)$ *strikt äquivalent*, wenn es ein $x \in 1 + \mathrm{M}_n(\mathfrak{m}_A)$ gibt, sodass $\rho(g) = x\rho'(g)x^{-1}$ für alle $g \in G$ gilt, und notieren dies als $\rho \sim \rho'$. Nun betrachten wir den *Deformationsfunktor*

$$\begin{aligned} \mathrm{Def}_{\overline{\rho}} \colon \mathcal{PAL}\text{-}\mathcal{Alg}(\mathcal{O}) &\longrightarrow \mathcal{Set}, \\ A &\longmapsto \{\rho \colon G \longrightarrow \mathrm{GL}_n(A) : \rho \text{ ist Deformation von } \overline{\rho}\} \big/ \sim . \end{aligned}$$

Da alle Homomorphismen in $\mathcal{PAL}\text{-}\mathcal{Alg}(\mathcal{O})$ lokal sind, erhalten sie Deformationen und $\mathrm{Def}_{\overline{\rho}}$ kann auf die naheliegende Weise auf Morphismen wirken.

Definition 5.2: Wenn der Deformationsfunktor $\mathrm{Def}_{\overline{\rho}}$ darstellbar ist, heißt ein darstellendes Objekt $R_{\overline{\rho}}$ ein *universeller Deformationsring* für $\overline{\rho}$.

In diesem Fall haben wir also für jedes $A \in \mathcal{PAL}\text{-}\mathcal{Alg}(\mathcal{O})$ eine Bijektion

$$\mathrm{Def}_{\overline{\rho}}(A) \cong \mathrm{Hom}_{\mathcal{O}}(R_{\overline{\rho}}, A).$$

Wenn wir hier $A = R_{\overline{\rho}}$ einsetzen, bekommen wir eine zur Identität gehörende universelle Deformation

$$\varrho \colon G \longrightarrow \mathrm{GL}_n(R_{\overline{\rho}}),$$

und $R_{\overline{\rho}}$ klassifiziert strikte Äquivalenzklassen aller Deformationen der gegebenen Restklassendarstellung, indem jedem $A \in \mathcal{PAL}\text{-}\mathcal{Alg}(\mathcal{O})$ und jedem $\rho \in \mathrm{Def}_{\overline{\rho}}(A)$ ein eindeutiger $\mathcal{O}$-Algebren-Homomorphismus $f_\rho \colon R_{\overline{\rho}} \longrightarrow A$ zugeordnet wird, sodass

$$\rho \sim f \circ \varrho.$$

Satz 5.3: *Wenn $\overline{\rho}$ absolut irreduzibel ist, existiert $R_{\overline{\rho}}$ in $\mathcal{PAL}\text{-}\mathcal{Alg}(\mathcal{O})$. Wenn G die Endlichkeitsbedingung Φ_p erfüllt, ist $R_{\overline{\rho}}$ noethersch.*

Beweis: [HidMFG, Thm. 2.26, Prop. 2.30] □

Wir wollen hier nicht erklären, was die Φ_p-Endlichkeitsbedingung genau ist – dazu verweisen wir auf die obige Referenz – sondern merken nur an, dass die absolute Galoisgruppe $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ diese erfüllt. In unserem Fall sind also die betrachteten Deformationsringe stets noethersch.

5.2. Kommutative Deformationen

Für den einfachen Fall, dass $n = 1$ ist (also $\overline{\rho}$ ein Charakter), wollen wir zeigen, wie der universelle Deformationsring aussieht. Hierbei orientieren wir uns an [HidMFG, §2.3.1].

Lemma 5.4: *Für jedes $A \in \mathcal{PAL}\text{-}\mathcal{Alg}(\mathcal{O})$ und jede abelsche pro-p-Gruppe H ist der proendliche Gruppenring $A[\![H]\!]$ ein Element von $\mathcal{PAL}\text{-}\mathcal{Alg}(\mathcal{O})$.*

Beweis: Wir benutzen zunächst, dass $\mathcal{PAL}\text{-}\mathcal{Alg}(\mathcal{O})$ die pro-Kategorie der Kategorie der artinschen lokalen $\mathcal{O}$-Algebren mit Restklassenkörper $\mathbb{F}$ ist. Daran und an Lemma 1.1.3 sehen wir, dass es genügt, die Aussage zu zeigen, wenn A eine lokale artinsche $\mathcal{O}$-Algebra und H eine endliche abelsche p-Gruppe ist.

Wir zeigen zuerst, dass $A[H]$ artinsch ist. Dazu benutzen wir, dass ein Ring R genau dann artinsch ist, wenn er als R-Modul endliche Länge hat (d.h. wenn es eine Kompositionsreihe von endlicher Länge gibt), vgl. hierzu [Eis95, Thm. 2.14]. Als A-Modul ist $A[H]$ isomorph zu $A^{\#H}$, und daraus folgt leicht, dass $A[H]$ Länge $l \cdot \#H$ hat, wenn l die Länge von A bezeichnet. Also ist $A[H]$ artinsch.

Als nächstes zeigen wir, dass $A[H]$ lokal ist, und benutzen dazu, dass die maximalen Ideale eines Rings in Bijektion mit den Isomorphieklassen einfacher Moduln über diesem Ring stehen. Es genügt also, zu zeigen, dass es nur eine Isomorphieklasse irreduzibler Darstellungen von H mit Koeffizienten in A gibt, also, dass jede irreduzible Darstellung $\rho\colon H \longrightarrow \mathrm{Aut}_A(V)$ für einen A-Modul $V \neq 0$ trivial ist. Da A abelsch ist, ist jeder A-lineare Automorphismus von V sogar $A[H]$-linear, und wir können ρ als Abbildung nach $\mathrm{Aut}_{A[H]}(V)$ auffassen. Da A abelsch ist, ist jeder A-lineare Automorphismus von V sogar $A[H]$-linear, und wir können ρ als Abbildung nach $\mathrm{Aut}_{A[H]}(V)$ auffassen. Nach dem Lemma von Schur ist $\mathrm{End}_{A[H]}(V)$ ein Schiefkörper. Da H trivial auf A operiert, ist $\mathfrak{m}_A V$ eine Unterdarstellung von ρ, und nach dem Lemma von Nakayama gilt $\mathfrak{m}_A V \neq V$, da $V \neq 0$. Also folgt $\mathfrak{m}_A V = 0$ wegen der Irreduzibilität, und deshalb hat $\mathrm{End}_{A[H]}(V)$ Charakteristik p. Wenn wir mit K den Erweiterungskörper von $\mathbb{F}_p$ bezeichnen, der in $\mathrm{End}_{A[H]}(V)$ von $\rho(H)$ erzeugt wird, können wir ρ als Charakter nach $K^\times$ auffassen. Da H eine endliche pro-p-Gruppe ist, muss jedes $\rho(h)$ für $h \in H$ eine p-Potenz-Einheitswurzel in K sein. Da K aber Charakteristik p hat, folgt $\rho(h) = 1$ und damit, dass ρ trivial ist.

Schließlich zeigen wir noch, dass $A[H]$ Restklassenkörper $\mathbb{F}$ hat. Der Restklassenkörper ist als $\mathbb{F}$-Vektorraum isomorph zu V. Für $v \in V \setminus \{0\}$ ist

$$\mathbb{F} = {}^{A}\!\big/_{\mathfrak{m}_A} \longrightarrow V, \quad a \longmapsto av$$

wegen $\mathfrak{m}_A V = 0$ wohldefiniert und definiert eine Einbettung von $\mathbb{F}$ als $A[H]$-Untermodul nach V. Da V irreduzibel ist, folgt $V \cong \mathbb{F}$. □

Nun können wir universelle Deformationsringe für Charaktere konstruieren. Sei also ein Charakter $\overline{\rho}\colon G \longrightarrow \mathbb{F}^\times$ einer proendlichen Gruppe G gegeben. Wir mithilfe des Teichmüller-Charakters[5] $\omega_{\mathcal{O}}\colon \mathbb{F}^\times \longrightarrow \mathcal{O}^\times$ können wir $\overline{\rho}$ zu einem Charakter $\widetilde{\rho} = \omega_{\mathcal{O}} \circ \overline{\rho}$ nach $\mathcal{O}^\times$ liften. Wir bezeichnen mit G_p^{ab} die p-Sylowgruppe der Abelisierung von G. Alle Charaktere von G faktorisieren über die Abelisierung, und da diese das Produkt ihrer Sylowgruppen ist, können wir jeden Charakter von G auch als einen dieser Sylowgruppe auffassen.

Satz 5.5: *Der universelle Deformationsring für $\overline{\rho}$ ist $\mathcal{O}[\![G_p^{\mathrm{ab}}]\!]$, wenn die universelle Deformation durch*

$$\varrho\colon G_p^{\mathrm{ab}} \longrightarrow \mathcal{O}[\![G_p^{\mathrm{ab}}]\!]^\times, \quad g \longmapsto \widetilde{\rho}(g)g$$

definiert wird.

[5] Wenn die Restklassencharakteristik 2 ist, ist das streng genommen nicht der Teichmüller-Charakter, sondern ein Quotient desselben, aber aufgrund des Henselschen Lemmas existiert der Lift trotzdem.

Beweis: Wegen Lemma 5.4 ist $\mathcal{O}[\![G_p^{\mathrm{ab}}]\!]$ ein Element von $\mathcal{PAL}\text{-}\mathcal{Alg}(\mathcal{O})$. Wenn irgendeine Deformation $\rho\colon G \longrightarrow A^\times$ gegeben ist, sei f_ρ der von

$$G \longrightarrow A^\times, \quad g \longmapsto \rho(g)\widetilde{\overline{\rho}}(g)^{-1}$$

durch die universelle Eigenschaft des proendlichen Gruppenrings induzierte $\mathcal{O}$-Algebren-Homomorphismus $\mathcal{O}[\![G_p^{\mathrm{ab}}]\!] \longrightarrow A$. Dann kann man leicht nachrechnen, dass $f_\rho \circ \varrho = \rho$ gilt. □

Beispiel 5.6: Wenn S eine endliche Menge von Primstellen von $\mathbb{Q}$ ist und wir Darstellungen von $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ klassifizieren wollen, die außerhalb von S unverzweigt sind, müssen wir die Galoisgruppe $G_S = \mathrm{Gal}(\mathbb{Q}^S|\mathbb{Q})$ der maximalen abelschen außerhalb von S unverzweigten Erweiterung von $\mathbb{Q}$ betrachten. Für $S = \{p, \infty\}$ ist deren Abelisierung nach Klassenkörpertheorie kanonisch isomorph zu $\mathbb{Z}_p^\times$, und die p-Sylowgruppe ist hier $1+p\mathbb{Z}_p$. Wir bezeichnen diese zur Unterscheidung zur Gewichtsgruppe Γ^{wt} mit Γ^{cyc} und schreiben $\Lambda^{\mathrm{cyc}} = \mathcal{O}[\![\Gamma^{\mathrm{cyc}}]\!]$ für die zugehörige *zyklotomische Iwasawa-Algebra*. In diesem Fall ist also der Deformationsring eines jeden Charakters $\Lambda^{\mathrm{cyc}} \cong \mathcal{O}[\![T]\!]$.

Für eine Restklassendarstellung

$$\overline{\rho}\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\mathbb{F})$$

beliebiger Dimension ist der Deformationsring für den Charakter $\det\overline{\rho}$ nach Satz 5.5 der proendliche Gruppenring $\mathcal{O}[\![\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})_p^{\mathrm{ab}}]\!]$. Wenn der universelle Deformationsring $R_{\overline{\rho}}$ und die universelle Deformation ϱ existiert, dann ist $\det\varrho$ eine Deformation von $\det\overline{\rho}$, und es wird ein Homomorphismus

$$\mathcal{O}[\![\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})_p^{\mathrm{ab}}]\!] \longrightarrow R_{\overline{\rho}}$$

induziert. Auf diese Weise können wir jeden Deformationsring $R_{\overline{\rho}}$ zu einer Algebra über $R_{\det\overline{\rho}}$ machen.

5.3. Eingeschränkte Deformationen

Da wir vornehmlich an Galoisdarstellungen interessiert sind und wir in Satz 5.3 und der Bemerkung danach gesehen hatten, dass in diesem Fall alle Deformationsringe noethersch sind, wollen wir nunmehr mit der vollen Unterkategorie $\mathcal{PANL}\text{-}\mathcal{Alg}(\mathcal{O})$ von $\mathcal{PAL}\text{-}\mathcal{Alg}(\mathcal{O})$ arbeiten, in der alle Ringe noethersch sind.

In den Abschnitten 3 und 4.4 hatten wir Galoisdarstellungen zu Modulformen betrachtet. Wenn wir diese mit Mitteln der Deformationstheorie untersuchen wollen, ist es günstig, nur solche Deformationen zuzulassen, die ähnliche Eigenschaften wie die modularen Galoisdarstellungen haben. Dies führt zu Deformationsringen mit gewissen Einschränkungen an die Deformationen, welche wir nun erklären wollen. Insbesondere schränken wir uns nun auf den Fall $n = 2$ ein, da dies die Dimension der modularen Galoisdarstellungen ist.

Definition 5.7: Es sei $\rho\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \longrightarrow \mathrm{GL}_2(A)$ eine Darstellung für ein $A \in \mathcal{PANL}\text{-}\mathcal{Alg}(\mathcal{O})$ und v eine Primstelle von $\mathbb{Q}$.

(a) ρ heißt *fast ordinär bei* v, wenn die Einschränkung von ρ auf die Zerlegungsgruppe (vgl. Fußnote 3) D_v isomorph ist zu einer oberen Dreiecksdarstellung

$$\rho|_{D_v} \cong \begin{pmatrix} \varepsilon & * \\ & \delta \end{pmatrix}.$$

(b) ρ heißt *ordinär bei* v, wenn ρ fast ordinär bei v und δ unverzweigt ist.

Diese Bezeichung orientiert sich an Satz 3.1 (b), der besagt, dass die Galoisdarstellung zu einer ordinären Eigenform ordinär bei p ist. Es sei darauf hingewiesen, dass jede Galoisdarstellung bei der archimedischen Stelle von $\mathbb{Q}$ stets ordinär ist.

Wir fixieren nun eine endliche Menge S von Primstellen von $\mathbb{Q}$ und bezeichnen mit G_S die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}^S|\mathbb{Q})$ der maximalen Erweiterung von $\mathbb{Q}$, die außerhalb von S unverzweigt ist.

Es seien nun $S_0 \subseteq S_1 \subseteq S$ Teilmengen und $\overline{\rho}$ eine gegebene Restklassendarstellung von G_S. Wir betrachten den Unterfunktor

$$\mathrm{Def}_{\overline{\rho}}^{S,S_0,S_1} : \mathcal{PANL}\text{-}\mathcal{Alg}(\mathcal{O}) \longrightarrow \mathcal{S}et$$

des Deformationsfunktors $\mathrm{Def}_{\overline{\rho}}$, der durch

$$A \longmapsto \left\{ \rho\colon G_S \longrightarrow \mathrm{GL}_2(A) : \begin{array}{l} \rho \text{ ist Deformation von } \overline{\rho}, \\ \text{ordinär bei allen } \ell \in S_0, \\ \text{fast ordinär bei allen } \ell \in S_1 \end{array} \right\} / \sim$$

gegeben ist. Wenn das zugehörige darstellende Objekt existiert, bezeichnen wir dieses mit $R_{\overline{\rho}}(S, S_0, S_1)$ und nennen es den *universellen eingeschränkten Deformationsring* von $\overline{\rho}$ bzgl. S, S_0, S_1.

Satz 5.8: *Wenn $S_0 = S_1$ und $\overline{\rho}$ absolut irreduzibel und ordinär bei allen $\ell \in S_0$ ist, dann existiert der Deformationsring $R_{\overline{\rho}}(S, S_0, S_0)$.*

Beweis: [Gou90, Thm. 2] □

Lemma 5.9: *Es sei $p \in S$, $S_0 \subseteq S$ eine Teilmenge mit $p \notin S_0$ und $S_1 = S_0 \cup \{p\}$ und $\overline{\rho}$ fast ordinär bei p. Es existiere $R_{\overline{\rho}}(S, S_1, S_1)$. Dann existiert auch $R_{\overline{\rho}}(S, S_0, S_1)$, und wir haben einen kanonischen Isomorphismus von $\mathcal{O}$-Algebren*

$$R_{\overline{\rho}}(S, S_0, S_1) \cong R_{\overline{\rho}}(S, S_1, S_1)[\![\Gamma^{\mathrm{cyc}}]\!].$$

Beweis: Wir bezeichnen mit $\overline{\delta}$ den Charakter δ aus Definition 5.7 (a) für $\overline{\rho}$. Es sei

$$\rho \in \mathrm{Def}_{\overline{\rho}}^{S,S_0,S_1}(A)$$

für ein $A \in \mathcal{PANL}\text{-}\mathcal{Alg}(\mathcal{O})$, ρ ist also fast ordinär bei p. Für ρ bezeichnen wir den Charakter δ aus Definition 5.7 (a) mit

$$\delta_\rho\colon D_p \longrightarrow A^\times.$$

Die Trägheitsgruppe $I_p \subseteq D_p$ ist unter der Identifikation $D_p \cong \mathrm{Gal}(\overline{\mathbb{Q}}_p|\mathbb{Q}_p)$ isomorph zu $I_p \cong \mathrm{Gal}(\overline{\mathbb{Q}}_p|\mathbb{Q}_p^{\mathrm{nr}})$, wenn $\mathbb{Q}_p^{\mathrm{nr}}$ die maximale unverzweigte Erweiterung von $\mathbb{Q}_p$ bezeichnet.

Nach lokaler Klassenkörpertheorie ist I_p^{ab} zu $\mathbb{Z}_p^\times$ isomorph [Ser67, §2, Thm. 3a]. Andererseits gilt

$$G_S^{\mathrm{ab}} \cong \prod_{\ell \in S} \mathbb{Z}_\ell^\times,$$

und da $p \in S$, können wir $\overline{\delta}|_{I_p}$ und $\delta_\rho|_{I_p}$ zu Charakteren von G_S fortsetzen, die wir ebenfalls mit $\overline{\delta}$ bzw. δ_ρ bezeichnen. Diese sind nach Konstruktion außerhalb von p unverzweigt. Mit dieser Definition ist dann

$$\rho \otimes \delta_\rho^{-1} \in \mathrm{Def}_{\overline{\rho}}^{S,S_1,S_1}(A)$$

und δ_ρ ist eine Deformation von $\overline{\delta}$.

Dies liefert uns eine Abbildung,

$$\mathrm{Def}_{\overline{\rho}}^{S,S_0,S_1}(A) \longrightarrow \mathrm{Def}_{\overline{\rho}}^{S,S_1,S_1}(A) \times \mathrm{Def}_{\overline{\delta}}^{\{p\}}(A), \quad \rho \longmapsto (\rho \otimes \delta_\rho^{-1}, \delta_\rho).$$

wobei wir hier mit $\mathrm{Def}_{\overline{\delta}}^{\{p\}}$ den Deformationsfunktor für $\overline{\delta}$ meinen, der außerhalb von p unverzweigte Deformationen klassifiziert. Für den entsprechenden Deformationsring $R_{\overline{\delta}}^{\{p\}}$ gilt nach Beispiel 5.6 $R_{\overline{\delta}}^{\{p\}} \cong \mathcal{O}[\![\Gamma^{\mathrm{cyc}}]\!]$. Man überlegt sich leicht, dass die obige Abbildung eine natürliche Äquivalenz dieser Deformationsfunktoren ist. Damit folgt

$$\begin{aligned}
\mathrm{Def}_{\overline{\rho}}^{S,S_0,S_1}(A) &\cong \mathrm{Def}_{\overline{\rho}}^{S,S_1,S_1}(A) \times \mathrm{Def}_{\overline{\delta}}^{\{p\}}(A) \\
&\cong \mathrm{Hom}_{\mathcal{O}}(R_{\overline{\rho}}(S,S_1,S_1),A) \times \mathrm{Hom}_{\mathcal{O}}(R_{\overline{\delta}}^{\{p\}},A) \\
&\cong \mathrm{Hom}_{\mathcal{O}}(R_{\overline{\rho}}(S,S_1,S_1),A) \times \mathrm{Hom}_{\mathcal{G}rp}(\Gamma^{\mathrm{cyc}},A^\times) \\
&\cong \mathrm{Hom}_{\mathcal{O}}(R_{\overline{\rho}}(S,S_1,S_1)[\![\Gamma^{\mathrm{cyc}}]\!],A),
\end{aligned} \tag{5.1}$$

und dies zeigt die Behauptung. □

Definition 5.10: Wir schreiben $R_{\overline{\rho}}^{\mathrm{ord}}(S,S_0)$ für $R_{\overline{\rho}}(S,S_0,S_0)$ und nennen diesen den *ordinären Deformationsring*. Falls $p \in S \setminus S_0$, schreiben wir[6] $R_{\overline{\rho}}^{\mathrm{nord}}(S,S_0)$ für $R_{\overline{\rho}}(S,S_0,S_0 \cup \{p\})$ und nennen ihn den *fast ordinären Deformationsring*.

5.4. $R = T$-Sätze

In diesem Abschnitt sei $p \neq 2$, K eine endliche Erweiterung von $\mathbb{Q}_p$ mit Ganzheitsring $\mathcal{O}$ und Restklassenkörper $\mathbb{F}$ und W der Ring der Witt-Vektoren von $\mathbb{F}$, den wir wieder mit dem Ganzheitsring der maximalen unverzweigten Teilerweiterung von $K|\mathbb{Q}_p$ identifizieren. Die Rolle, die bisher $\mathcal{O}$ innehatte, wird nun von W übernommen, wir arbeiten also in der Kategorie $\mathcal{PANL}$-$\mathcal{Alg}(W)$.

Wir betrachten nun wieder die universelle ordinäre Hecke-Algebra $\mathcal{h} = \mathcal{h}^{\mathrm{ord}}(N,W)$ aus Abschnitt 4. Wenn $\mathfrak{m}$ ein maximales Ideal von $\mathcal{h}$ ist, dann ist der zugehörige lokale Ring $\mathcal{h}_{\mathfrak{m}}$ ein Element von $\mathcal{PANL}$-$\mathcal{Alg}(W)$: denn in Abschnitt 4.4 hatten wir bemerkt, dass der Restklassenkörper $\mathbb{F}$ ist, und weil $\mathcal{h}$ wegen Satz 4.6 proartinsch und noethersch ist (da Λ^{wt} proartinsch und noethersch ist), gilt dies auch für den Teilring $\mathcal{h}_m$.

[6] Das Superskript „nord“ steht für „nearly ordinary“.

Im Falle, dass die Restklassendarstellung $\overline{\rho}_{\mathfrak{m}}$ zu $\mathfrak{m}$ absolut irreduzibel und bei p verzweigt ist, hatten wir in Satz 4.13 eine bei p ordinäre Darstellung

$$\rho_{\mathfrak{m}}\colon \operatorname{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \longrightarrow \operatorname{GL}_2(\mathfrak{h}_{\mathfrak{m}})$$

angegeben, die außerhalb von $Np\infty$ unverzweigt ist. Man könnte vermuten, dass diese eine universelle Deformation von $\overline{\rho}_{\mathfrak{m}}$ ist. Um dies genau zu formulieren, ist jedoch einige Vorsicht geboten.

Die Darstellung $\overline{\rho}_{\mathfrak{m}}$ ist die Restklassendarstellung einer Eigenform $f \in \mathcal{S}_k(\Gamma_1(Np^r), \mathcal{O})$ (vgl. Satz 4.14). Der universelle Deformationsring von $\overline{\rho}_{\mathfrak{m}}$ „sieht" aber das N nicht mehr, und es wäre ja möglich, dass es zu verschiedenen solchen N (mit den gleichen Primteilern) Eigenformen mit den gleichen Restklassendarstellungen gibt. Also müssen wir das „richtige" N irgendwie aus $\overline{\rho}_{\mathfrak{m}}$ extrahieren.

Es sei dazu eine beliebige Darstellung

$$\overline{\rho}\colon \operatorname{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \longrightarrow \operatorname{GL}_2(\mathbb{F})$$

gegeben. Da diese endliches Bild hat, faktorisiert sie über eine endliche normale Teilerweiterung $L|\mathbb{Q}$. Für jede Primzahl $\ell \neq p$ wählen wir eine Stelle von L, die über ℓ liegt, und bezeichnen mit G_i für $i \in \mathbb{N}_0$ die höheren Verzweigungsgruppen in der zugehörigen Erweiterung der komplettierten Körper (vgl. [Neu07, §II.10]; insbesondere ist G_0 die Trägheitsgruppe) und mit V_i den Unterraum von $V = \mathbb{F}^2$, der von G_i festgelassen wird. Dann setzen wir

$$n(\ell, \overline{\rho}) = \sum_{i=0}^{\infty} \frac{1}{(G_0 : G_i)} \dim V/V_i \ ,$$

was eine nichtnegative ganze Zahl ist, siehe [Ser79, §VI.2] und [Ser77, §19.3]. Wenn ℓ in L unverzweigt ist, ist G_0 und damit alle G_i trivial, also ist dann $n(\ell, \overline{\rho}) = 0$. Da dies für fast alle ℓ der Fall ist, ist die folgende Definition sinnvoll.

Definition 5.11: Der *Führer* von $\overline{\rho}$ ist

$$N(\overline{\rho}) = \prod_{\ell \neq p} \ell^{n(\ell, \overline{\rho})}.$$

Wir nehmen nun weiter an, dass $\overline{\rho}$ absolut irreduzibel und bei p verzweigt und ordinär ist. Mit $N = N(\overline{\rho})$ sei der Führer von $\overline{\rho}$ bezeichnet. Wir fordern, dass es eine Eigenform $f \in \mathcal{S}_k^{\mathrm{ord}}(\Gamma_1(Np^r), \mathcal{O})$ für ein $r \in \mathbb{N}_0$ gibt, sodass $\overline{\rho}$ die Restklassendarstellung von f ist. Dieses f bestimmt dann ein maximales Ideal $\mathfrak{m}$ der Hecke-Algebra $\mathfrak{h} = \mathfrak{h}^{\mathrm{ord}}(N, W)$, und wir bezeichnen die entsprechende Lokalisierung wieder mit $\mathfrak{h}_{\mathfrak{m}}$. Weiter setzen wir[7]

$$S = \{p, \infty\} \cup \{\text{Primteiler von } N\}, \quad S_0 = \{\ell \in S : \overline{\rho} \text{ ist ordinär bei } \ell\}.$$

Lemma 5.12: *(a) Jede Eigenform $f \in \mathcal{S}_k^{\mathrm{ord}}(\Gamma_1(Np^r), \mathcal{O})$, deren Restklassendarstellung $\overline{\rho}$ ist, ist eine Neuform.*

[7] In manchen Texten, z.B. [Böc01], kann S auch größer sein. Unseren Fall bekommen wir daraus zurück, indem wir dort $\Sigma = \varnothing$ setzen.

(b) *Für jede Primzahl $\ell \mid N$ ist die Darstellung $\rho_{\mathfrak{m}}$ ist genau dann ordinär bei ℓ, wenn $\overline{\rho}$ dies ist.*

Beweis: [Gou90, Lem. 7, Prop. 8] □

Aufgrund dieses Lemmas bekommen wir also einen kanonischen Homomorphismus[8]

$$R^{\mathrm{ord}}_{\overline{\rho}}(S, S_0) \longrightarrow \mathscr{h}_{\mathfrak{m}}.$$

Vermutung 5.13: *Der kanonische Homomorphismus*

$$R^{\mathrm{ord}}_{\overline{\rho}}(S, S_0) \longrightarrow \mathscr{h}_{\mathfrak{m}}$$

ist ein Isomorphismus.

Diese Vermutung stammt ursprünglich von Mazur. In einem Spezialfall wurde sie in [MT90] formuliert, die hier angegebene Version stammt aus [Gou90]. In [Gou90, Thm. 12] wurde gezeigt, dass dieser Homomorphismus stets surjektiv ist.

Da in vielen Texten Hecke-Algebren mit $\mathbb{T}$ (und nicht wie bei uns mit $\mathscr{h}$) bezeichnet werden, und die universellen Deformationsringe meist R heißen, nennt man eine Aussage von diesem Typ auch einen $R = T$-Satz. Ein solcher besagt also, dass *alle* Deformationen (mit passendem Verzweigungsverhalten) der Galoisdarstellung einer festen ordinären Eigenform selbst wieder modular sind, also von einer solchen Eigenform herkommen. Geometrisch stellt man sich das Spektrum des Deformationsrings als den „Deformationsraum" vor, und das Spektrum von $\mathscr{h}_{\mathfrak{m}}$ ist der Unterraum der modularen Deformationen. Die $R = T$-Aussage besagt dann, dass dieser Unterraum bereits der ganze Deformationsraum ist.

Inzwischen ist über diese Vermutung einiges bekannt. In Hidas Buch findet sich ein Beweis im Falle $N = 1$ und gewissen weiteren Voraussetzungen [HidMFG, Thm. 5.29]. Die Arbeiten von Wiles und Taylor [Wil95; TW95] zu Fermats letztem Satz zeigen eine Isomorphie zwischen Hecke-Algebren zu festem Level und Gewicht und weiter eingeschänkten Deformationsringen (mit fester Determinante für alle Deformationen); im Falle $N = 1$ wird dies auch in [HidMFG, Thm. 3.31] gezeigt. In [Böc01] wird erklärt, wie man die Resultate von Wiles und Taylor benutzen kann, um auf die Isomorphie der „großen" Ringe in Vermutung 5.13 zu schließen. Für die genauen Bedingungen, unter denen dieses Resultat erzielt wird, siehe [Böc01, Ass. 2.1].

In Anlehnung an Lemma 5.9 und Definition 5.10 definieren wir nun noch:

Definition 5.14: Die *universelle fast ordinäre Hecke-Algebra* ist

$$\mathscr{h}^{\mathrm{nord}}(N, \mathcal{O}) = \mathscr{h}^{\mathrm{ord}}(N, \mathcal{O})[\![\Gamma^{\mathrm{cyc}}]\!].$$

Entsprechend definieren wir $\mathscr{h}^{\mathrm{nord}}(N, \psi, \mathcal{O})$.

[8] In manchen Texten – z.B. in [Böc01] – geht dieser Homomorphismus nicht in einen lokalen Ring der vollen Hecke-Algebra $\mathscr{h}^{\mathrm{ord}}(N, \mathcal{O})$, sondern in einen entsprechenden lokalen Ring der *eingeschränkten Hecke-Algebra*, welche die Unteralgebra ist, die nur von den T_n mit $(n, Np) = 1$ erzeugt wird. Wegen [Gou90, Thm. 10, Thm. 12] macht dies aber keinen Unterschied.

6. p-adische L-Funktionen für Hida-Familien

Nachdem wir in Abschnitt 4.4 die Galoisdarstellungen zu den Mitgliedern einer Hida-Familie zu einer großen Galoisdarstellung zusammengefasst haben, stellt sich die Frage, ob man etwas ähnliches auch mit ihren L-Funktionen machen kann. In Satz III.5.2 haben wir angegeben, wie eine p-adische L-Funktion für eine einzelne Eigenform aussieht. Diese war ein Maß auf der Gruppe $G = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})|\mathbb{Q})$, dessen Integrale spezielle Werte der (Twists der) L-Funktion dieser Eigenform interpoliert.

Für eine Hida-Familie wurde eine p-adische L-Funktion von Kitagawa als Maß auf $G \times \Gamma^{\mathrm{wt}}$ konstruiert. Er erhielt das folgende Ergebnis:

Satz 6.1 (Kitagawa): *Es sei $F\colon \mathfrak{h}^{\mathrm{ord}}(N, \psi, \mathcal{O}) \longrightarrow \Lambda^{\mathrm{wt}}$ eine Λ^{wt}-adische Eigenform mit formaler q-Entwicklung*

$$F(q) = \sum_{n=1}^{\infty} a_n q^n \in \Lambda^{\mathrm{wt}}[\![q]\!],$$

und es seien

$$f_{k,\varepsilon} \in \mathcal{S}_k^{\mathrm{ord}}(Np^r, \varepsilon\psi\omega^{-k}, \mathcal{O})$$

die Mitglieder der zugehörigen Hida-Familie. Wir definieren ι und $\eta_{k,\varepsilon}$ wie in Abschnitt 4.3.

Dann gibt es ein $\mathcal{O}$-wertiges Maß μ_F auf $G \times \Gamma^{\mathrm{wt}}$, sodass für alle Dirichlet-Charaktere χ vom Führer p^m, alle $k \geq 2$, alle Charaktere ε von Γ^{wt} von endlicher Ordnung und $n = 0, \dots, k-2$ gilt

$$\int_G \int_{\Gamma^{\mathrm{wt}}} \chi^{-1}(z)\kappa(z)^n \varepsilon(w)\iota(w)^k \mathrm{d}\mu_F(z,w) = \frac{(-1)^n G(\overline{\chi}) p^{mn} n! E^{\pm}_{k,\varepsilon}}{(2\pi \mathrm{i})^n \Omega^{\pm}_{f_{k,\varepsilon}} \eta_{k,\varepsilon}(a_p)^m} (1 - \eta_{k,\varepsilon}(a_p)^{-1}\overline{\chi}(p)p^n) L(f_{k,\varepsilon}, \chi, n+1).$$

Dabei sind $\Omega^{\pm}_f \in \mathbb{C}^\times$ die Perioden aus Satz III.5.1, $G(\cdot)$ ist die Gauß-Summe (vgl. (I.5.1)), die $E^{\pm}_{k,\varepsilon} \in \mathcal{O} \setminus \{0\}$ gewisse Korrekturterme und die Menge $\{|E^{\pm}_{k,\varepsilon}| : k, \varepsilon$ wie oben$\}$ ist endlich. Die Exponenten „$\pm$“ sind als das Vorzeichen von $(-1)^n\chi(-1)$ zu wählen.

Beweis: [Kit94, Thm. 1.1] □

Dieses μ_F können wir als Element in $\mathcal{O}[\![G \times \Gamma^{\mathrm{wt}}]\!]$ auffassen.

Wir betrachten nun wie in Abschnitt 4.1 die Zerlegung

$$\mathbb{Z}_{p,N}^\times \cong \left(\mathbb{Z}/Np\mathbb{Z}\right)^\times \times \Gamma^{\mathrm{wt}} \cong \left(\mathbb{Z}/N\mathbb{Z}\right)^\times \times \mathbb{Z}_p^\times$$

und bezeichnen mit π_p die Projektion von $\mathbb{Z}_{p,N}^\times$ auf $\mathbb{Z}_p^\times$. Dann sehen wir, dass die Komposition

$$\Gamma^{\mathrm{wt}} \hookrightarrow \mathbb{Z}_{p,N}^\times \xrightarrow{\pi_p} \mathbb{Z}_p^\times \hookrightarrow \mathcal{O}^\times$$

gerade ι ist (wobei der letzte Pfeil die kanonische Einbettung ist). Wenn nun k und ε wie in Satz 6.1 sind, betrachten wir die Komposition

$$\Gamma^{\mathrm{wt}} \longrightarrow \mathfrak{h}^{\mathrm{ord}}(N, \psi, \mathcal{O})^\times \twoheadrightarrow \left(\mathfrak{h}^{\mathrm{ord}}(N, \psi, \mathcal{O})\big/P_{k,\varepsilon}\mathfrak{h}^{\mathrm{ord}}(N, \psi, \mathcal{O})\right)^\times \xrightarrow{\sim} (\mathfrak{h}_k^{\mathrm{ord}}(N, \varepsilon\psi\omega^{-k}, \mathcal{O}))^\times,$$

in welcher der erste Pfeil die Einschränkgung des Strukturmorphismus' aus (4.5) auf Γ^{wt} ist. Aus unseren Überlegungen folgt dann leicht, dass diese Komposition durch $\varepsilon\iota^k$ gegeben ist (vgl. auch Beweis von Korollar 4.10).

Wir nehmen nun das zu (k,ε) gehörende Element $f_{k,\varepsilon} \in \mathcal{S}_k^{\mathrm{ord}}(Np^r, \varepsilon\psi\omega^{-k}, \mathcal{O})$ der Hida-Familie zu F und bezeichnen mit

$$\lambda_{k,\varepsilon} \colon \mathscr{h}_k^{\mathrm{ord}}(N, \varepsilon\psi\omega^{-k}, \mathcal{O}) \longrightarrow \mathcal{O}$$

den zugehörigen $\mathcal{O}$-Algebren-Homomorphismus. Die obige Komposition induziert einen $\mathcal{O}$-Algebren-Homomorphismus $\mathcal{O}[\![\Gamma^{\mathrm{wt}}]\!] \longrightarrow \mathscr{h}_k^{\mathrm{ord}}(N, \varepsilon\psi\omega^{-k}, \mathcal{O})$, und wenn wir diesen mit $\lambda_{k,\varepsilon}$ verketten, erhalten wir einen Homomorphismus

$$\mathcal{O}[\![\Gamma^{\mathrm{wt}}]\!] \longrightarrow \mathcal{O},$$

der dann gerade der von $\varepsilon\iota^k$ induzierte ist. Dieser liefert weiter einen Homomorphismus

$$\mathcal{O}[\![\Gamma^{\mathrm{wt}} \times G]\!] \longrightarrow \mathcal{O}[\![G]\!],$$

und wir bezeichnen das Bild von μ_F unter diesem mit $\mu_{k,\varepsilon}$, was ein $\mathcal{O}$-wertiges Maß auf G ist. Unsere Überlegung zeigt dann, dass

$$\int_G \chi^{-1}\kappa^n \mathrm{d}\mu_{k,\varepsilon} = \frac{(-1)^n G(\overline{\chi}) p^{mn} n! E_{k,\varepsilon}^{\pm}}{(2\pi \mathrm{i})^n \Omega_{f_{k,\varepsilon}}^{\pm} \eta_{k,\varepsilon}(a_p)^m} (1 - \eta_{k,\varepsilon}(a_p)^{-1}\overline{\chi}(p)p^n) L(f_{k,\varepsilon}, \chi, n+1) \qquad (6.1)$$

für χ und n wie in Satz 6.1 gilt. Dies ist, bis auf die Korrekturterme $E_{k,\varepsilon}^{\pm}$ und einen Faktor $(-1)^n$, die p-adische L-Funktion zu $f_{k,\varepsilon}$, wie sie in Satz III.5.2 angegeben war.

V. Nichtkommutative p-adische L-Funktionen

Bisher haben uns p-adische L-Funktionen schon eine Weile begleitet, aber wir haben noch gar nicht erklärt, welche Rolle diese in der Iwasawa-Theorie spielen. Dies wird durch sogenannte *Hauptvermutungen* beschrieben, die einen Zusammenhang zwischen einer p-adischen L-Funktion und dem charakteristischen Ideal oder Element eines Iwasawa-Moduls behaupten. Sie sollen in dieser Arbeit nicht unerwähnt bleiben und sind wichtig zum Verständnis der Bedeutung p-adischer L-Funktionen, deshalb wollen wir zu Beginn dieses Kapitels die ursprüngliche, von Iwasawa selbst formulierte Hauptvermutung erklären.

In dem Bestreben, solche Vermutungen in noch allgemeinerem Rahmen aufzustellen, wird versucht, den Definitionsbereich der kommutativen p-adischen L-Funktionen (welcher die Charaktergruppe einer kommutativen Galoisgruppe war, siehe Abschnitt III.4) auszudehnen und so zu nichtkommutativen p-adischen L-Funktionen zu gelangen. Die nichtkommutative Iwasawa-Theorie bietet dafür einen natürlichen Rahmen. Eine andere Möglichkeit, die von der Geometrie von Hida-Familien inspiriert wurde, hat Ochiai in [Och06] vorgeschlagen.

In diesem abschließenden Kapitel wollen wir diese beiden Herangehensweisen kurz zusammenfassen und mit der Deformationstheorie aus Kapitel IV verbinden. Dadurch wird der Anschein erweckt, dass man diese p-adischen L-Funktionen miteinander vergleichen könnte. Um einen solchen Vergleich tatsächlich durchzuführen, fehlen uns jedoch die nötigen Methoden, weswegen es unklar bleiben muss, ob dies tatsächlich sinnvoll möglich ist.

1. Die klassische Hauptvermutung

Es gibt viele Hauptvermutungen, die sich dadurch unterscheiden, welcher Grundkörper zugrundegelegt wird, welches Motiv betrachtet wird, und in welchem Körperturm dies geschieht. Wir wollen hier die einfachste Variante erklären: bei dieser ist $\mathbb{Q}$ der Grundkörper, und wir betrachten die Idealklassengruppen in dem Körperturm $\mathbb{Q}(\mu_{p^\infty})|\mathbb{Q}$.

Wir setzen für jedes $n \in \mathbb{N}_0 \cup \{\infty\}$

$$K_n = \mathbb{Q}(\mu_{p^n}).$$

Dann vermittelt der zyklotomische Charakter einen Isomorphismus

$$\kappa\colon G := \mathrm{Gal}(K_\infty|\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}_p^\times.$$

Für jedes $n \in \mathbb{N}_0$ bezeichnen wir mit X_n die p-Sylowgruppe der Idealklassengruppe $\mathrm{Cl}(K_n)$ von K_n. Wenn L_n den p-Hilbert-Klassenkörper von K_n bezeichnet (also die maximale unverzweigte abelsche p-Erweiterung von K_n) und wir $A_n = \mathrm{Gal}(L_n|K_n)$ definieren, definiert die Artin-Abbildung aus der Klassenkörpertheorie einen Isomorphismus [Neu07, §VI.7]

$$\left(\frac{L_n|K_n}{\cdot}\right) : X_n \xrightarrow{\sim} A_n, \quad [\mathfrak{p}] \longmapsto \mathrm{Frob}_{\mathfrak{p}} . \tag{1.1}$$

Wir betrachten die exakte Sequenz von Galoisgruppen

$$1 \longrightarrow \mathrm{Gal}(L_n|K_n) \longrightarrow \mathrm{Gal}(L_n|\mathbb{Q}) \longrightarrow \mathrm{Gal}(K_n|\mathbb{Q}) \longrightarrow 1$$

und definieren eine Aktion von $\mathrm{Gal}(K_n|\mathbb{Q})$ auf $A_n = \mathrm{Gal}(L_n|K_n)$, indem wir für ein $\sigma \in \mathrm{Gal}(K_n|\mathbb{Q})$ mit Urbild $\tilde{\sigma} \in \mathrm{Gal}(L_n|\mathbb{Q})$ und ein $\tau \in \mathrm{Gal}(L_n|K_n)$

$$\sigma \bullet \tau := \tilde{\sigma}\tau\tilde{\sigma}^{-1}$$

setzen, was wegen der Exaktheit und der Kommutativität von A_n wohldefiniert ist. Andererseits haben wir auf $X_n = \mathrm{Cl}(K_n)_p$ eine natürliche Galois-Aktion von $\mathrm{Gal}(K_n|\mathbb{Q})$. Wenn $\mathfrak{p}$ ein Primideal von K_n ist, folgt aus der Gleichheit $\mathrm{Frob}_{\mathfrak{p}^\sigma} = \sigma \,\mathrm{Frob}_{\mathfrak{p}}\, \sigma^{-1}$ leicht, dass

$$\sigma \bullet \left(\frac{L_n|K_n}{\mathfrak{p}}\right) = \left(\frac{L_n|K_n}{\mathfrak{p}^\sigma}\right)$$

für alle $\sigma \in \mathrm{Gal}(K_n|\mathbb{Q})$ gilt. Also ist (1.1) sogar ein Isomorphismus von $\mathrm{Gal}(K_n|\mathbb{Q})$-Moduln.

Wir bezeichnen nun mit

$$\mathrm{N}_n \colon X_{n+1} \longrightarrow X_n$$

die Relativnorm von Idealen. Man kann sich dann leicht überlegen, dass das Diagramm

$$\begin{tikzcd} X_{n+1} \arrow[r, "\sim"] \arrow[d, "\mathrm{N}_n"'] & A_{n+1} \arrow[d, "\cdot|_{L_n}"] \\ X_n \arrow[r, "\sim"] & A_n \end{tikzcd}$$

für genügend großes n kommutiert (man braucht dazu $L_n \cap K_{n+1} = K_n$, was für genügend großes n gilt; siehe dazu [Was82, S. 277 und Lem. 13.3]).

Wir definieren nun

$$X = \varprojlim_{n\in\mathbb{N}_0} X_n, \quad A = \varprojlim_{n\in\mathbb{N}_0} A_n,$$

wobei der Limes bezüglich der Idealnorm bzw. der Einschränkung genommen wird. Als Limiten abelscher p-Gruppen sind X und A auf kanonische Weise Moduln über $\mathbb{Z}_p$ (vgl. Satz I.1.14), und die $\mathrm{Gal}(K_n|\mathbb{Q})$-Aktionen auf X_n bzw. A_n setzen sich zusammen zu einer Aktion von $G = \varprojlim_n \mathrm{Gal}(K_n|\mathbb{Q})$ auf X bzw. A. Damit erhalten X und A eine Struktur als Moduln über $\Lambda := \mathbb{Z}_p[\![G]\!]$ (vgl. Satz I.1.17), und unsere Überlegungen zeigen, dass sie als solche kanonisch isomorph sind. Deshalb betrachten wir im Weiteren nur noch X.

Wir zerlegen nun

$$X = \bigoplus_{i=1}^{p-1} X_i, \quad \Lambda = \bigoplus_{i=1}^{p-1} \Lambda_i,$$

wobei der Summand mit Index i jeweils den Eigenraum des Charakters ω^i bezeichne (vgl. (I.2.1) und (I.2.2)). Weiter setzen wir

$$X^+ = \bigoplus_{\substack{i=1 \\ i \text{ gerade}}}^{p-1} X_i, \quad X^- = \bigoplus_{\substack{i=1 \\ i \text{ ungerade}}}^{p-1} X_i$$

und definieren $\Lambda^\pm$ entsprechend. Dann ist der mit dem Exponenten $\pm$ versehenene Summand von X gerade der Teilraum, auf dem die komplexe Konjugation als ± 1 operiert, und $X^\pm$ ist jeweils ein $\Lambda^\pm$-Modul.

In Abschnitt III.2 hatten wir zu einem Dirichlet-Charakter ein Element in einer Iwasawa-Algebra konstruiert, welches einer p-adischen L-Funktion entspricht. Wir betrachten das Element, welches zum trivialen Charakter gehört (vgl. Bemerkung III.2.6): dieses war ein Element $\mu_\zeta := \mu_{\chi^0}$ im Quotientenkörper von Λ, sodass $g\mu_\zeta \in \Lambda$ (mit g wie dort). Wegen Lemma III.2.2 gilt sogar $h\mu_\zeta \in \Lambda^-$.

Auf der anderen Seite haben wir Definition I.2.17 hatten wir für Iwasawa-Moduln eine wichtige Invariante definiert, nämlich das charakteristische Ideal. Wir bezeichnen das charakteristische Ideal von X^- in Λ^- mit $\operatorname{char}^-(X)$. Der von der Hauptvermutung für die Klassengruppe behauptete Zusammenhang zwischen diesen beiden Objekten kann dann in der folgenden Form formuliert werden:

Satz 1.1 (Hauptvermutung): *Es gilt*

$$\operatorname{char}^-(X) = (g\mu_\zeta).$$

Der $+$-Anteil tritt also in der Hauptvermutung nicht auf. Auf der Seite der p-adischen Zetafunktion verschwindet er, und passend dazu wird vermutet:

Vermutung 1.2 (Vandiver): *Es gilt* $X^+ = 0$.

Über Vandivers Vermutung ist jedoch nur wenig bekannt. Wenn diese stimmt, kann man die Hauptvermutung auch formulieren, ohne zwischen den $\pm$-Teilen der beteiligten Objekte zu unterscheiden.

Nach der Definition des charakteristischen Ideals und der Elemente μ_ζ und g ist dies also dazu äquivalent, dass für alle ungeraden $i = 3, \dots, p-2$ das charakteristische Ideal des $\mathcal{O}[\![\Gamma]\!]$-Moduls X_i im Sinne von Definition I.2.13 von $\lambda_{\chi^0,i}$ erzeugt wird (vgl. (III.2.1)) und für $i = 1$ von $h\lambda_{\chi^0,1}$ mit h wie in Bemerkung III.2.6. In dieser Version wurde die Vermutung von Mazur und Wiles in [MW84] bewiesen. Ein Beweis findet sich auch in [CS06], wo die Aussage in einer alternativen Form formuliert wird, welche aber zu unserer Formulierung äquivalent ist.[1]

Durch die Hauptvermutung wird das Phänomen, dass die Riemannsche Zetafunktion Informationen über arithmetische Eigenschaften von Erweiterungen von $\mathbb{Q}$ enthält, ein Stück weit erklärt. Die viel ältere Aussage von Kummer, dass eine Primzahl p genau dann die Ordnung der Klassengruppe C von $\mathbb{Q}(\mu_p)$ teilt, wenn sie einen der Zähler der rationalen

[1] Diese Äquivalenz sieht man, indem man auf unsere Formulierung die Involution ν aus (III.4.3) anwendet: dadurch geht μ_ζ in das Pseudo-Maß aus Satz III.4.2 über und das von g erzeugte Ideal wird zum Augmentationsideal. Dass die verschiedenen Iwasawa-Moduln zueinander passen, zeigt ein Satz von Iwasawa, siehe [Gre01, Prop. 2.6].

Zahlen $\zeta(1-i)$ für gerades i mit $2 \leq i \leq p-3$ teilt, kann aus der Hauptvermutung gefolgert werden. Auch der Satz von Herbrand-Ribet ist eine Konsequenz der Hauptvermutung. Dieser besagt, dass für ungerades n mit $3 \leq n \leq p-2$ die Potenz κ^n des zyklotomischen Charakters genau dann in der Charakterzerlegung der natürlichen Darstellung der Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})|\mathbb{Q})$ auf dem $\mathbb{F}_p$-Vektorraum C/C^p vorkommt, wenn p den Zähler von $\zeta(n+1-p)$ teilt. Siehe hierzu auch [CS06, Chap. 1] und [Kat07].

Eine andere Sicht auf die Hauptvermutung ergibt sich, wenn man die enge Analogie zwischen Zahlkörpern und Funktionenkörpern ins Blickfeld rückt. Für Kurven über endlichen Körpern zeigte André Weil einen Zusammenhang zwischen der Zetafunktion einer solchen Kurve und den Nullstellen des charakteristischen Polynoms des Frobeniusautomorphismus' auf der Jacobischen der Kurve (vgl. [NSW00, Thm. 11.6.2]), was später in den Weil-Vermutungen verallgemeinert wurde. Auf Iwasawa geht die Idee zurück, dass man im Sinne dieser Analogie nach einer ähnlichen Aussage für Zahlkörper suchen könnte. Dabei soll die Dedekindsche Zetafunktion des Zahlkörpers die Rolle der Zetafunktion der Kurve übernehmen, und das charakteristische Polynom des Frobenius' wird durch das charakteristische Ideal eines aus den Klassengruppen gebildeten Iwasawa-Moduls ersetzt (welches ja von einem charakteristischen Polynom erzeugt wird, siehe Bemerkung 1.2.14). Dies war die ursprüngliche Motivation für die Hauptvermutung und wird in [Iwa69] erklärt.

In [Gre91] wurde von Greenberg eine weitreichende Verallgemeinerung dieser Vermutung auf beliebige Motive (über $\mathbb{Q}$) vorgeschlagen. Diese schließt auch eine entsprechende Hauptvermutung für elliptische Kurven ein, wie sie von Mazur in [Maz72, §1 c)] formuliert wurde. Die Rolle der Idealklassengruppe übernimmt in diesem Fall die Selmer-Gruppe der elliptischen Kurve, für deren Definition auf [Sil86, §x.4] verwiesen sei.

All diesen Hauptvermutungen ist gemein, dass der Körperturm $K_\infty|K$, in dem die Motive betrachtet werden, stets eine abelsche Galoisgruppe hat. Deshalb zählen sie zur kommutativen Iwasawa-Theorie. Im nächsten Abschnitt wollen wir kurz beschreiben, wie dies auf einen nicht notwendig kommutativen Körperturm verallgemeinert werden kann.

2. Nichtkommutative Iwasawa-Theorie

Die Idee der nichtkommutativen Iwasawa-Theorie ist es, die Situation aus der kommutativen Situation in einem noch größeren Körperturm $K_\infty|K$ zu studieren, dessen Galoisgruppe $\mathrm{Gal}(K_\infty|K)$ im Allgemeinen nicht abelsch ist. In Abschnitt 1.4 hatten wir erklärt, wie man in dieser Situation das charakteristische Ideal verallgemeinert und waren auf diesem Wege zum Begriff des *charakteristischen Elements* gelangt, welches ein Element in K_1 einer lokalisierten Iwasawa-Algebra war. Im Hinblick auf eine Hauptvermutung ist es daher natürlich, eine zugehörige nichtkommutative p-adische L-Funktion ebenfalls in K_1 zu suchen.

Die kommutativen p-adischen L-Funktionen können bei Charakteren der entsprechenden Galoisgruppe ausgewertet werden, welche aufgrund der Kommutativität dieser Gruppe gerade die irreduziblen Darstellungen derselben sind. Da man jede Darstellung in irreduzible zerlegen kann, könnte man dadurch für jede Darstellung den Wert einer p-adischen L-Funktion definieren. Im Falle einer nichtkommutativen Gruppe gibt es auch höherdimensionale irreduzible Darstellungen. Dies legt nahe, nach einem Weg zu suchen, um die Elemente in der K_1-Gruppe bei solchen auszuwerten.

2.1. Auswerten bei Darstellungen

Wir begeben uns wieder in die Situation von Abschnitt 1.4.3: es sei also G eine kompakte p-adische Lie-Gruppe, $H \subseteq G$ eine abgeschlossene Untergruppe, sodass $\Gamma := G/H$ zu $\mathbb{Z}_p$ isomorph ist, K eine endliche Erweiterung von $\mathbb{Q}_p$, $\mathcal{O}$ der Ganzheitsring in K und S^* wie in Definition 1.4.6 definiert. Wir schreiben $\Lambda(G) = \mathcal{O}[\![G]\!]$ und entsprechend für H und Γ. Weiter sei eine Darstellung $\rho\colon G \longrightarrow \mathrm{GL}_n(\mathcal{O}')$ für ein $n \in \mathbb{N}$ und den Ganzheitsring $\mathcal{O}'$ in einer endlichen Erweiterung K' von K gegeben.[2] Für das Bild eines $\sigma \in G$ in Γ schreiben wir $\overline{\sigma}$, und wir schreiben $\Lambda'(G) = \mathcal{O}'[\![G]\!]$ und wieder entsprechend für H und Γ.

Wir betrachten den Homomorphismus

$$G \longrightarrow (\mathrm{M}_n(\mathcal{O}') \otimes_{\mathcal{O}} \Lambda(\Gamma))^\times, \quad \sigma \longmapsto \rho(\sigma) \otimes \overline{\sigma}.$$

Da $\mathcal{O}'$ als $\mathcal{O}$-Modul frei von endlichem Rang ist, gilt $\mathrm{M}_n(\mathcal{O}') \otimes_{\mathcal{O}} \Lambda(\Gamma) = \mathrm{M}_n(\Lambda'(\Gamma))$, und deshalb induziert der obige Homomorphismus einen Homomorphismus

$$\Phi_\rho\colon \Lambda(G) \longrightarrow \mathrm{M}_n(\Lambda'(\Gamma)).$$

Man kann zeigen, dass

$$\forall s \in S^*\colon \det \Phi_\rho(s) \neq 0$$

gilt [CFKSV05, Lem. 3.3].[3] Also setzt sich Φ_ρ zu einer Abbildung

$$\Phi_\rho\colon \Lambda(G)_{S^*} \longrightarrow \mathrm{M}_n(Q)$$

fort, wobei wir mit Q den Quotientenkörper von $\Lambda'(\Gamma)$ bezeichnen. Dieses liefert weiter

$$\Phi'_\rho\colon K_1(\Lambda(G)_{S^*}) \longrightarrow K_1(\mathrm{M}_n(Q)) = Q^\times,$$

wobei wir für das letzte Gleichheitszeichen die Sätze 1.3.7 und 1.3.8 benutzt haben. Wir betrachten nun den Augmentationshomomorphismus

$$\varphi\colon \Lambda'(\Gamma) \longrightarrow \mathcal{O}'$$

und bezeichnen dessen Kern mit $\mathfrak{p}$ und mit $\Lambda'(\Gamma)_{\mathfrak{p}} \subseteq Q$ die Lokalisierung bei diesem. Die Augmentation induziert schließlich

$$\varphi\colon \Lambda'(\Gamma)_{\mathfrak{p}} \longrightarrow K'.$$

Definition 2.1: Es sei $\xi \in K_1(\Lambda(G)_{S^*})$. Dann definieren wir die *Auswertung von ξ bei ρ* durch

$$\xi(\rho) = \begin{cases} \varphi(\Phi'_\rho(\xi)), & \text{falls } \Phi'_\rho(\xi) \in \Lambda'(\Gamma)_{\mathfrak{p}}, \\ \infty, & \text{sonst.} \end{cases}$$

[2] Dies ist analog zu Situation auf Seite 63, wo wir einen Dirichlet-Charakter ψ betrachtet haben, der Werte in einem solchen $\mathcal{O}'$ annahm.

[3] Die Behauptung wird dort nur im Fall $\mathcal{O} = \mathbb{Z}_p$ gezeigt, aber die Autoren bemerken später (S. 203/204), dass sich die Argumente auch auf den Fall eines größeren $\mathcal{O}$ übertragen.

Im kommutativen Fall reduziert sich dies zu $G = \Gamma$ und $n = 1$. In diesem Fall ist $\Phi_\rho\colon \Lambda \longrightarrow \Lambda'$ von $\sigma \longmapsto \rho(\sigma)\sigma$ induziert und die Komposition

$$\varphi \circ \Phi_\rho\colon \Lambda \longrightarrow \mathcal{O}'$$

daher von $\sigma \longmapsto \rho(\sigma)$. Daran sieht man leicht, dass Definition 2.1 die kommutative Situation verallgemeinert.

2.2. Nichtkommutative p-adische L-Funktionen elliptischer Kurven

Es sei E eine elliptische Kurve über $\mathbb{Q}$, die bei p gute ordinäre Reduktion hat. Wir wollen nun kurz erklären, eine nichtkommutative p-adische L-Funktion für E aussehen könnte. Dabei bleiben wir allerdings sehr knapp, da all dies im Originalartikel [CFKSV05] sehr gut beschrieben ist wir nicht nur eine bloße Abschrift desselben präsentieren wollen.

Für jede Primzahl ℓ bezeichnen wir mit $T_\ell(E)$ den ℓ-adischen Tate-Modul, mit $\tau_{E,\ell}$ die zugehörige Galoisdarstellung und setzen $V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Wir bezeichnen mit $K_\infty = \mathbb{Q}(E[p^\infty])$ den Körper, der über $\mathbb{Q}$ von den Koordinaten aller p-Potenz-Torsionspunkte auf E erzeugt wird. Er ist gerade der Fixkörper des Kerns von $\tau_{E,p}$. Seine Galoisgruppe $G = \mathrm{Gal}(K_\infty|\mathbb{Q})$ ist daher isomorph zum Bild von $\tau_{E,p}$, welches eine abgeschlossene Untergruppe von $\mathrm{GL}_2(\mathbb{Z}_p)$ und als solche eine kompakte p-adische Lie-Gruppe ist. Wenn E keine komplexe Multiplikation hat, ist dieses Bild nach einem Satz von Serre [Ser72] auch offen und hat daher endlichen Index, also handelt es sich tatsächlich um eine „große“ p-adische Lie-Gruppe.

Der Körper K_∞ enthält die zyklotomische $\mathbb{Z}_p$-Erweiterung von $\mathbb{Q}$ (dies kann man mithilfe der Weil-Paarung sehen, siehe [Sil86, Cor. III.8.1.1]). Wenn $p \geq 5$, gibt es in $\mathrm{GL}_2(\mathbb{Z}_p)$ kein Element von Ordnung p: denn wenn es ein solches gäbe, müsste sein Minimalpolynom ein Teiler des p-ten Kreisteilungspolynoms sein. Letzteres ist aber über $\mathbb{Z}_p$ irreduzibel, da $\mathbb{Z}_p$ keine p-ten Einheitswurzeln enthält, und sein Grad ist $p - 1 \geq 4$. Da das Minimalpolynom Grad ≤ 2 hat, kann dies nicht sein. Wenn wir also $p \geq 5$ annehmen, ist G eine Gruppe, die den Voraussetzungen der Theorie aus Abschnitt I.4.3 genügt.

Es sei nun eine Darstellung $\rho\colon G \longrightarrow \mathrm{GL}_n(\mathcal{O}')$ gegeben, die endliches Bild hat (wobei $\mathcal{O}'$ der Ganzheitsring einer endlichen Erweiterung von $\mathbb{Q}_p$ ist). Eine solche nennen wir eine *Artin-Darstellung*. Die Endlichkeit des Bildes führt dazu, dass es einen Zahlkörper K_ρ gibt, sodass ρ bereits Werte in $\mathrm{GL}_n(K_\rho)$ annimmt. Für jede Primzahl ℓ und eine über ℓ liegende Primstelle λ von K_ρ mit Komplettierung $K_{\rho,\lambda}$ bezeichnen wir mit $V_{\rho,\lambda}$ den $K_{\rho,\lambda}$-Vektorraum, auf dem G via ρ operiert. Wir definieren den *Twist der L-Funktion von E um* ρ

$$L(E, \rho, s)$$

als die L-Funktion im Sinne von Definition I.6.7 (c), die zu dem (kompatiblen!) System

$$(\mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(E), V_{\rho,\lambda}))_\ell$$

gehört (vgl. Bemerkung I.6.2).

Die vermutete p-adische L-Funktion von E ist von der Gestalt, dass ihre Auswertung bei einer Artin-Darstellung ρ mit einer Modifikation des getwisteten L-Werts $L(E, \rho, 1)$ übereinstimmt, ähnlich wie im kommativen Fall die Auswertung bei einem Charakter endlicher Ordnung mit ein modifizierter um diesen Charakter getwisteter L-Wert ist (vgl. Sätze III.4.1

und III.5.2). Wir wollen die vorzunehmenden Modifikationen nicht genau erklären, sondern präsentieren lediglich die Formel, ohne die Bedeutung der Objekte im einzelnen zu erklären. Dies wird in [CFKSV05, S. 202–204] getan und soll hier nicht wiederholt werden.

Es sei dazu F die maximale abelsche Teilerweiterung von $K_\infty|\mathbb{Q}$, in der p nicht verzweigt (das ist eine endliche Erweiterung von $\mathbb{Q}$, siehe dort) und W der Ganzheitsring in der Komplettierung von F bei einer beliebigen über p liegenden Primstelle. Weiter sei $\Lambda(G) = W[\![G]\!]$.

Vermutung 2.2: *Es gibt ein $\mathcal{L}_E \in K_1(\Lambda(G)_{S^*})$, sodass für alle Artin-Darstellungen ρ von G gilt*

$$\mathcal{L}_E(\rho) = \frac{\varepsilon_p(\rho)u^{-f_\rho}}{\Omega^+(E)^{d^+(\rho)}\Omega^-(E)^{d^-(\rho)}}\frac{L_p(\widehat{\rho}, u^{-1})}{L_p(\rho, w^{-1})}L_R(E, \rho, 1),$$

insbesondere $\mathcal{L}_E(\rho) \neq \infty$.

Für diese p-adische L-Funktion wird in [CFKSV05, Conj. 5.8] eine Hauptvermutung formuliert, die im wesentlichen besagt, dass $\mathcal{L}_E$ ein charakteristisches Element eines gewissen Iwasawa-Moduls ist, der mithilfe der Selmer-Gruppen von E im Körperturm $K_\infty|\mathbb{Q}$ gebildet wird. Es sei an dieser Stelle noch erwähnt, dass auch für andere Motive als elliptische Kurven nichtkommutative Hauptvermutungen formuliert wurden. Für die Klassengruppe wird eine solche in [Kat07] skizziert.

3. Der Schluss

In der nichtkommutativen Iwasawa-Theorie wird der Definitionsbereich der im klassischen Fall auf einer Charaktergruppe definierten p-adischen L-Funktionen so vergrößert, dass diese auf p-adischen Darstellungen der Galoisgruppe des Körperturms ausgewertet werden können. Ochiai hat in [Och06] eine andere Möglichkeit vorgeschlagen, den Definitionsbereich der klassischen p-adischen L-Funktionen zu erweitern. Diese beruht auf der folgenden Beobachtung: wenn Γ eine zu $\mathbb{Z}_p$ isomorphe Gruppe und $\gamma \in \Gamma$ ein topologischer Erzeuger ist, dann ist

$$\mathrm{Hom}(\Gamma, \mathbb{C}_p^\times) \longrightarrow \{x \in \mathbb{C}_p : |x-1|_p < 1\}, \quad \chi \longmapsto \chi(\gamma)$$

eine Bijektion. Also besteht der Definitionsbereich $\mathrm{Hom}(G, \mathbb{C}_p^\times)$ (mit $G = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})|\mathbb{Q}) \cong \mathbb{F}_p^\times \times \Gamma$) einer kommutativen p-adischen L-Funktion aus $p-1$ Kopien von offenen Einheitskugeln in $\mathbb{C}_p$. Diese Kugeln bilden einen *rigid-analytischen Raum*, was wir hier aber nicht definieren wollen. Die Idee besteht nun darin, nach einer p-adischen L-Funktion zu suchen, die auf einem größeren rigid-analytischen Raum definiert ist. In [Och06, Def. 2.1, Prob. 2.3] wird eine – sehr vage bleibende – Andeutung gemacht, wie eine solche L-Funktion aussehen könnte. Dies wollen wir hier nicht wiederholen, sondern lediglich erwähnen, dass bei richtiger Sicht der Dinge Kitagawas p-adische L-Funktion aus Satz IV.6.1 als eine solche aufgefasst werden kann (dies wird in [Och06, §3] erklärt).

Wir wollen nun zeigen, dass man die „$R = T$"-Aussage aus Vermutung IV.5.13 benutzen kann, um Kitagawas Funktion ebenfalls auf Galoisdarstellungen auszuwerten. Es sei dazu eine Λ^{wt}-adische Eigenform

$$F\colon \mathfrak{h}^{\mathrm{ord}}(N, \psi, \mathcal{O}) \longrightarrow \Lambda^{\mathrm{wt}}$$

gegeben, die wir für den Rest des Abschnittes fixieren. Wir bezeichnen mit $\mathfrak{m}$ das maximale Ideal in $\mathfrak{h}^{\mathrm{ord}}(N, \mathcal{O})$, zu dem F gehört, mit $\mathfrak{h}_{\mathfrak{m}}$ die zugehörige Lokalisierung und mit

$$f_{k,\varepsilon} \in \mathcal{S}_k^{\mathrm{ord}}(Np^r, \varepsilon\psi\omega^{-k}, \mathcal{O})$$

die Mitglieder der zugehörigen Hida-Familie. Kitagawas L-Funktion ist ein Element $\mu_F \in \mathcal{O}[\![\Gamma^{\mathrm{cyc}} \times \Gamma^{\mathrm{wt}}]\!]$, wenn wir es nur auf der Untergruppe Γ^{cyc} von G betrachten. Der Strukturmorphismus

$$\Lambda^{\mathrm{wt}} \longrightarrow \mathfrak{h}^{\mathrm{ord}}(N, \mathcal{O})$$

liefert eine Abbildung

$$\mathcal{O}[\![\Gamma^{\mathrm{cyc}} \times \Gamma^{\mathrm{wt}}]\!] \longrightarrow \mathfrak{h}^{\mathrm{nord}}(N, \mathcal{O}) = \mathfrak{h}^{\mathrm{ord}}(N, \mathcal{O})[\![\Gamma^{\mathrm{cyc}}]\!],$$

mit der wir μ_F nach $\mathfrak{h}_{\mathfrak{m}}[\![\Gamma^{\mathrm{cyc}}]\!]$ abbilden können. Auf diese Weise können wir Kitagawas Maß als Element der fast ordinären Hecke-Algebra auffassen.

Wir nehmen nun an, dass die Vermutung IV.5.13 in unserem Fall stimmt, was uns ein zu μ_F gehörendes Element

$$\mathcal{L}_F \in R_{\overline{\rho}}^{\mathrm{nord}}(S, S_0)$$

im fast ordinären Deformationsring beschert. Das ermöglicht es uns, eine Auswertung der Kitagawaschen Funktion bei Deformationen zu definieren.

Definition 3.1: Es sei $A \in \mathcal{PANL}\text{-}\mathcal{Alg}(\mathcal{O})$ und $\rho\colon \operatorname{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \longrightarrow \mathrm{GL}_2(A)$ eine Deformation von $\overline{\rho}$, die außerhalb von S unverzweigt ist, bei allen $\ell \in S_0$ ordinär und fast ordinär bei p. Den von der universellen Eigenschaft des Deformationsrings induzierten $\mathcal{O}$-Algebren-Homomorphismus $R_{\overline{\rho}}^{\mathrm{nord}}(S, S_0) \longrightarrow A$ bezeichnen wir mit φ_ρ. Dann definieren wir die *Auswertung von $\mathcal{L}_F$ bei ρ* durch

$$\mathcal{L}_F(\rho) := \varphi_\rho(\mathcal{L}_F) \in A.$$

Bemerkung 3.2: Wir könnten μ_F auch direkt (ohne $R = T$ zu benutzen) mithilfe eines entsprechenden Strukturmorphismus' in den Deformationsring abbilden. Der Isomorphismus aus Vermutung IV.5.13 ist sogar Λ-linear, wenn wir Λ^{wt} und Λ^{cyc} geeignet identifizieren [MT90, Lem. 13]. Dies spiegelt aber nicht die natürliche Λ-Algebren-Struktur des *fast ordinären* Deformationsringes wider, da der Isomorphismus aus Lemma IV.5.9 kein Λ-Algebren-Isomorphismus ist. Da die Formel aus Satz IV.6.1 a priori alles ist, was wir über die Auswertungen von μ_F wissen, ist $R = T$ wichtig, wenn wir das Verhalten von μ_F als Element des Deformationsrings verstehen wollen.

Wir haben nun also eine „nichtkommutative“ p-adische L-Funktion, die ein Element eines Deformationsringes ist und bei Deformationen ausgewertet werden kann. Dies passt schön zur kommutativen Situation: denn dort war die p-adische L-Funktion ein Element der Iwasawa-Algebra, welche nach Beispiel IV.5.6 der Deformationsring eines Charakters ist.

Wir bezeichnen nun für k, ε, χ und n wie in Satz IV.6.1 den dort auf der rechten Seite auftretenden Ausdruck

$$\frac{(-1)^n G(\overline{\chi}) p^{mn} n! E_{k,\varepsilon}^{\pm}}{(2\pi\mathrm{i})^n \Omega_{f_{k,\varepsilon}}^{\pm} \eta_{k,\varepsilon}(a_p)^m}(1 - \eta_{k,\varepsilon}(a_p)^{-1}\overline{\chi}(p)p^n) L(f_{k,\varepsilon}, \chi, n+1)$$

mit $L_p^{\mathrm{Kit}}(f_{k,\varepsilon},\chi,n+1)$. Weiter schreiben wir

$$\widetilde{\kappa}\colon \Gamma^{\mathrm{cyc}} \longrightarrow \mathbb{Z}_p^\times \hookrightarrow \mathcal{O}^\times$$

für die Einschränkung des zyklotomischen Charakters κ auf Γ^{cyc}.

Satz 3.3: *Es seien k, ε und n wie in Satz IV.6.1, ρ die Galoisdarstellung zu $f = f_{k,\varepsilon}$ und χ ein Charakter endlicher Ordnung von Γ^{cyc}. Dann gilt*

$$\mathcal{L}_F(\rho \otimes \chi^{-1}\widetilde{\kappa}^n) = L_p^{\mathrm{Kit}}(f,\chi,n+1).$$

Beweis: Wir bezeichnen mit λ die Komposition

$$\begin{aligned}\mathfrak{h}^{\mathrm{ord}}(N,\mathcal{O}) \twoheadrightarrow \mathfrak{h}^{\mathrm{ord}}(N,\psi,\mathcal{O}) \twoheadrightarrow \mathfrak{h}^{\mathrm{ord}}(N,\psi,\mathcal{O})\Big/P_{k,\varepsilon}\mathfrak{h}^{\mathrm{ord}}(N,\psi,\mathcal{O})\\ \xrightarrow{\sim} \mathfrak{h}_k^{\mathrm{ord}}(N,\varepsilon\psi\omega^{-k},\mathcal{O}) \longrightarrow \mathcal{O},\end{aligned}$$

in der der letzte Pfeil der zu f gehörende $\mathcal{O}$-Algebren-Homomorphismus ist. Weiter seien $\rho_{\mathfrak{m}}$ die Galoisdarstellung aus Satz IV.4.13 und $\varphi_{\mathfrak{m}}$ bzw. φ_f die von $\rho_{\mathfrak{m}}$ bzw. ρ induzierten $\mathcal{O}$-Algebren-Homomorphismen $R^{\mathrm{ord}}(S,S_0) \longrightarrow \mathfrak{h}_{\mathfrak{m}}$ bzw. $R^{\mathrm{ord}}(S,S_0) \longrightarrow \mathcal{O}$. Dann kommutiert das Diagramm

$$\begin{tikzcd} R^{\mathrm{ord}}(S,S_0) \arrow[rr, "\sim", "\varphi_{\mathfrak{m}}"'] \arrow[dr, "\varphi_f"'] & & \mathfrak{h}^{\mathrm{ord}}(N,\mathcal{O})_{\mathfrak{m}} \arrow[dl, "\lambda"] \\ & \mathcal{O}, & \end{tikzcd} \tag{3.1}$$

denn $\lambda \circ \varphi_{\mathfrak{m}}$ erfüllt nach Satz IV.4.14 die universelle Eigenschaft, die auch φ_f erfüllt.

Die Darstellung $\rho \otimes \chi^{-1}\widetilde{\kappa}^n$ ist eine bei passende Deformation von $\rho_{\mathfrak{m}}$: denn die Bilder des Charakters $\chi^{-1}\widetilde{\kappa}^n$ sind p-Potenz-Einheitswurzeln, also in Charakteristik p trivial, und da ρ bei p ordinär ist und $\chi^{-1}\widetilde{\kappa}^n$ lediglich das Verzweigungsverhalten bei p beeinflusst, ist das Produkt bei p fast ordinär und hat bei den anderen Primzahlen das gleiche Verhalten wie ρ. Wenn wir auf diese Deformation das Argument aus Lemma IV.5.9 anwenden, erhalten wir, dass dort der Charakter δ_ρ von G_S gerade $\chi^{-1}\widetilde{\kappa}^n$ ist.

Wir schreiben nun $\varphi_{f,\chi,n}$ für den von $\rho \otimes \chi^{-1}\widetilde{\kappa}^n$ induzierten Homomorphismus

$$R^{\mathrm{nord}}(S,S_0) \longrightarrow \mathcal{O}$$

und $(\chi^{-1}\widetilde{\kappa}^n)_*$ für den von $\chi^{-1}\widetilde{\kappa}^n$ induzierten Homomorphismus $\mathcal{O}[\![\Gamma^{\mathrm{cyc}}]\!] \longrightarrow \mathcal{O}$. Ferner induziert φ_f einen Homomorphismus $R^{\mathrm{ord}}(S,S_0)[\![\Gamma^{\mathrm{cyc}}]\!] \longrightarrow \mathcal{O}[\![\Gamma^{\mathrm{cyc}}]\!]$, den wir ebenfalls mit φ_f bezeichnen. Unsere obigen Überlegungen zeigen dann, dass das Diagramm

$$\begin{tikzcd} R^{\mathrm{nord}}(S,S_0) \arrow[r, "\sim"] \arrow[d, "\varphi_{f,\chi,n}"] & R^{\mathrm{ord}}(S,S_0)[\![\Gamma^{\mathrm{cyc}}]\!] \arrow[d, "\varphi_f"] \\ \mathcal{O} & \mathcal{O}[\![\Gamma^{\mathrm{cyc}}]\!] \arrow[l, "(\chi^{-1}\widetilde{\kappa}^n)_*"] \end{tikzcd}$$

kommutiert (vgl. (IV.5.1)).

Wir schreiben jetzt μ_f für das Bild von $\mathcal{L}_F \in R^{\mathrm{nord}}(S, S_0)$ in $\mathcal{O}[\![\Gamma^{\mathrm{cyc}}]\!]$. In (IV.6.1) hatten wir bereits gezeigt, dass

$$\int_{\Gamma^{\mathrm{cyc}}} \chi^{-1}\kappa^n \mathrm{d}\mu_f = L_p^{\mathrm{Kit}}(f, \chi, n+1)$$

(um dies verwenden zu können, brauchen wir die Kommutativität des Diagramms (3.1)). Dies zeigt die Behauptung. □

Der Modularitätssatz, der in [Wil95; TW95; BCDT01] bewiesen wurde, besagt, dass es zu jeder elliptischen Kurve E über $\mathbb{Q}$ eine normalisierte Eigenform $f \in \mathcal{S}_2^{\mathrm{new}}(\Gamma_0(N))$ gibt, sodass die komplexen L-Funktionen von E und f übereinstimmen. Hierbei ist N der *Führer* von E, der ähnlich wie in Definition IV.5.11 definiert wird. Für die genaue Definition sei auf [Sil94, §IV.10] verwiesen. Dieses f ist nach Bemerkung I.7.1 und Satz II.6.6 genau dann ordinär bei p, wenn E dies ist.

Wir wählen nun eine elliptische Kurve E wie in Abschnitt 2.2 und bezeichnen mit f die zugeordnete Modulform. Wenn wir in unseren Formeln alle Perioden und Modifikationen großzügig ignorieren, bekommen wir aus Satz 3.3 eine ähnliche Interpolationseigenschaft, wie sie in Vermutung 2.2 gefordert wird, allerdings nur für eindimensionale Artin-Darstellungen. Deshalb lässt sich Kitagawas p-adische L-Funktion so leider nicht direkt mit $\mathcal{L}_E$ aus Vermutung 2.2 vergleichen. Es sei aber darauf hingewiesen, dass einige Nebenbedingungen zueinander passen: so wird in beiden Fällen gefordert, dass die jeweiligen Objekte bei p ordinär sind, und der p-adische Ring W, über dem die L-Funktionen jeweils definiert werden, ist in beiden Fällen unverzweigt über $\mathbb{Z}_p$.

Auf diese Weise ist also Kitagawas Funktion eine p-adische L-Funktion, in die wir das Produkt einer Modulform mit einem Dirichlet-Charakter einsetzen können. Im Sinne von Abschnitt II.1 ist so etwas eine automorphe Form auf $\mathrm{GL}_2 \times \mathrm{GL}_1$ über $\mathbb{Q}$. Man könnte hoffen, dass man mithilfe automorpher Formen auf $\mathrm{GL}_2 \times \mathrm{GL}_n$ für $n \geq 1$ mit einer ähnlichen Theorie zu einer p-adischen L-Funktion gelangen könnte, die entsprechende höherdimensionale Twists der L-Funktion von E interpoliert. Für $n = 2$ wurden solche Formen von Hida studiert [Hid88]. Januszewski (mündliche Mitteilung, 21. Mai 2013) konstruierte auf Grundlage der Arbeiten [Sch93; Sch00; KMS00; KS13; Jan11] ein modulares Symbol (siehe auch [Jan12]), welches unter geeigneten Annahmen über die Kohomologie arithmetischer Gruppen eine derartige p-adische L-Funktion für automorphe Formen auf $\mathrm{GL}_n \times \mathrm{GL}_{n-1}$ für beliebiges $n \in \mathbb{N}$ produziert. Die automorphen Formen können dabei insbesondere in Familien variieren. Dies führt aber weit über den Rahmen dieser Arbeit hinaus.

Literaturverzeichnis

[BCDT01] Conrad Breuil, Brian Conrad, Fred Diamond und Richard Taylor. „On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises". In: *Journal of the American Mathematical Society* 14.4 (2001), S. 843–939 (zit. auf S. 33, 116).

[Böc01] Gebhard Böckle. „On the Density of Modular Points in Universal Deformation Spaces". In: *American Journal of Mathematics* 123.5 (2001), S. 985–1007 (zit. auf S. 96, 103 f.).

[Bum97] Daniel Bump. *Automorphic Forms and Representations.* Cambridge Studies in Advanced Mathematics 55. Cambridge University Press, 1997 (zit. auf S. 35, 50).

[CFKSV05] John Coates, Takako Fukaya, Kazuya Kato, Ramdorai Sujatha und Otmar Venjakob. „The GL_2 Main Conjecture for Elliptic Curves without Complex Multiplication". In: *Publications Mathématiques de l'I.H.E.S.* 101 (2005), S. 163–208 (zit. auf S. 22 f., 111–113).

[Coa89] John Coates. „On p-adic L-functions attached to motives over $\mathbb{Q}$ II". In: *Boletim da Sociedade Brasileira de Matemática* 20.1 (1989), S. 101–112 (zit. auf S. 75).

[CP89] John Coates und Bernadette Perrin-Riou. „On p-adic L-functions attached to motives over $\mathbb{Q}$". In: *Advanced Studies in Pure Mathematics* 17 (1989), S. 23–54 (zit. auf S. 75).

[CS06] John Coates und Ramdorai Sujatha. *Cyclotomic Fields and Zeta Values.* Springer Monographs in Mathematics. Berlin, Heidelberg: Springer-Verlag, 2006 (zit. auf S. 13, 73, 109 f.).

[Dei10] Anton Deitmar. *Automorphe Formen.* Berlin, Heidelberg: Springer-Verlag, 2010 (zit. auf S. 39, 51).

[Del79] Pierre Deligne. „Valeurs de fonctions L et périods d'intégrales". In: *Proceedings of Symposia in Pure Mathematics* 33 (1979), S. 313–346 (zit. auf S. 75).

[DS05] Fred Diamond und Jerry Shurman. *A First Course in Modular Forms.* Graduate Texts in Mathematics 228. New York: Springer-Verlag, 2005 (zit. auf S. 37, 39, 44, 48–51, 85).

[Eis95] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry.* Graduate Texts in Mathematics 150. New York: Springer-Verlag, 1995 (zit. auf S. 83, 99).

[Erd56] Arthur Erdélyi. *Asymptotic Expansions.* New York: Dover Publications, Inc., 1956 (zit. auf S. 25).

[Gel75] Stephen S. Gelbart. *Automorphic Forms on Adele Groups.* Annals of Mathematics Studies 83. Princeton: Princeton University Press, 1975 (zit. auf S. 39).

[Gou88] Fernando Q. Gouvêa. *Arithmetic of p-adic Modular Forms.* Lecture Notes in Mathematics 1304. Berlin, Heidelberg: Springer-Verlag, 1988 (zit. auf S. 96).

[Gou90] Fernando Q. Gouvêa. „Deforming Galois Representations: Controlling the Conductor". In: *Journal of Number Theory* 34 (1990), S. 95–113 (zit. auf S. 96, 101, 104).

[Gre01] Ralph Greenberg. „Iwasawa theory – past and present". In: *Advanced Studies in Pure Mathematics* 30 (2001), S. 335–385 (zit. auf S. 109).

[Gre91] Ralph Greenberg. „Iwasawa theory for motives". In: London Mathematical Society Lecture Notes Series 153 (1991): *L-functions and Arithmetic*, S. 211–233 (zit. auf S. 110).

[Hid86a] Haruzo Hida. „Galois representations into $\mathrm{GL}_2(\mathbb{Z}_p[\![X]\!])$ attached to ordinary cusp forms". In: *Inventiones mathematicae* 85 (1986), S. 545–613 (zit. auf S. 86, 88, 91).

[Hid86b] Haruzo Hida. „Iwasawa modules attached to congruences of cusp forms". In: *Annales Scientifiques de l'École Normale Supérieure* 19.2 (1986), S. 231–273 (zit. auf S. 86, 88, 90).

[Hid88] Haruzo Hida. „A p-adic measure attached to the zeta functions associated with two elliptic modular forms. II". In: *Annales de l'institut Fourier* 38.3 (1988), S. 1–83 (zit. auf S. 116).

[HidGMF] Haruzo Hida. *Geometric Modular Forms and Elliptic Curves.* Singapur: World Scientific, 2000 (zit. auf S. 31, 80).

[HidLFE] Haruzo Hida. *Elementary theory of L-functions and Eisenstein series.* London Mathematical Society Student Texts 26. Cambridge: Cambridge University Press, 1993 (zit. auf S. 90).

[HidMFG] Haruzo Hida. *Modular Forms and Galois Cohomology.* Cambridge Studies in Advanced Mathematics 69. Cambridge: Cambridge University Press, 2000 (zit. auf S. 29, 78, 81, 85 f., 98, 104).

[HM98] Joe Harris und Ian Morrison. *Moduli of Curves.* Graduate Texts in Mathematics. New York: Springer-Verlag, 1998 (zit. auf S. 36).

[Iwa69] Kenkichi Iwasawa. „Analogies between Number Fields and Function Fields". In: *Annual Science Conference Proceedings* 2 (1969): *Some Recent Advances in the Basic Sciences.* Hrsg. von A. Gelbart, S. 203–208 (zit. auf S. 110).

[Iwa72] Kenkichi Iwasawa. *Lectures on p-adic L-functions.* Annals of Mathematics Studies 74. Princeton: Princeton University Press und University of Tokyo Press, 1972 (zit. auf S. 26, 60, 64, 66, 74).

[Jan11] Fabian Januszewski. „Modular symbols for reductive groups and p-adic Rankin-Selberg convolutions over number fields". In: *Journal für die reine und angewandte Mathematik* 653 (2011), S. 1–45 (zit. auf S. 116).

[Jan12] Fabian Januszewski. *On p-adic L-functions of* $\mathrm{GL}(n)\times\mathrm{GL}(n-1)$ *over totally real fields.* Version 6. Preprint, eingereicht. 28. Nov. 2012. arXiv: `math/11111818` (zit. auf S. 116).

[Kat07] Kazuya Kato. „Iwasawa Theory and Generalizations“. In: *Proceedings of the International Congress of Mathematicians* I (2007), S. 335–357 (zit. auf S. 110, 113).

[Kit94] Koji Kitagawa. „On standard p-adic L-functions of families of elliptic cusp forms“. In: *Contemporary Mathematics* 165 (1994): *p-Adic Monodromy and the Birch and Swinnerton-Dyer Conjecture*. Hrsg. von Glenn Stevens und Barry Mazur, S. 81–110 (zit. auf S. 75, 105).

[KL64] Tomio Kubota und Heinrich-Wolfgang Leopoldt. „Eine p-adische Theorie der Zetawerte. I. Einführung der p-adischen Dirichletschen L-Funktionen“. In: *Journal für die reine und angewandte Mathematik* 214/215 (1964), S. 328–339 (zit. auf S. 54).

[KM85] Nicholas Katz und Barry Mazur. *Arithmetic Moduli of Elliptic Curves*. Annals of Mathematics Studies 108. Princeton: Princeton University Press, 1985 (zit. auf S. 36).

[KMS00] David Kazhdan, Barry Mazur und Claus-Günther Schmidt. „Relative modular symbols and Rankin-Selberg convolutions“. In: *Journal für die reine und angewandte Mathematik* 519 (2000), S. 97–141 (zit. auf S. 116).

[KS06] Masaki Kashiwara und Pierre Schapira. *Categories and Sheaves*. Grundlehren der mathematischen Wissenschaften. A Series of Comprehensive Studies in Mathematics 332. Berlin, Heidelberg: Springer-Verlag, 2006 (zit. auf S. 3).

[KS13] Hendrik Kasten und Claus-Günther Schmidt. „The critical values of Rankin-Selberg convolutions“. In: *International Journal of Number Theory* 9.1 (2013), S. 205–256 (zit. auf S. 116).

[Lan76] Serge Lang. *Introduction to Modular Forms*. Grundlehren der mathematischen Wissenschaften. A Series of Comprehensive Studies in Mathematics 222. Berlin, Heidelberg: Springer-Verlag, 1976 (zit. auf S. 44, 47, 54).

[Man73] Yuri Manin. „Periods of parabolic forms and p-adic Hecke series“. In: *Mathematics of the USSR. Sbornik* 134.3 (1973), S. 371–393 (zit. auf S. 75).

[Man74] Yuri Manin. „The values of p-adic Hecke series at integer points of the critical strip“. In: *Mathematics of the USSR. Sbornik* 135.4 (1974), S. 631–637 (zit. auf S. 75).

[Maz72] Barry Mazur. „Rational points of abelian varieties with values in towers of number fields“. In: *Inventiones mathematicae* 18 (1972), S. 183–266 (zit. auf S. 110).

[Maz89] Barry Mazur. „Deforming Galois Representations“. In: *MSRI Publications* 16 (1989): *Galois Groups over* $\mathbb{Q}$, S. 385–437 (zit. auf S. 97).

[Miy89] Toshitsune Miyake. *Modular Forms*. Berlin, Heidelberg: Springer-Verlag, 1989 (zit. auf S. 48).

[MR87] John C. McConnell und James Christopher Robson. *Noncommutative Noetherian Rings*. Pure and Applied Mathematics. A Wiley-Interscience publication. Chichester, New York: John Wiley & Sons, 1987 (zit. auf S. 21).

[MS74] Barry Mazur und H. P. F. Swinnerton-Dyer. „Arithmetic of Weil Curves“. In: *Inventiones mathematicae* 25 (1974), S. 1–61 (zit. auf S. 66, 75).

[MT90] Barry Mazur und Jaqcues Tilouine. „Représentations Galoisiennes, Différentielles de Kähler et ‚Conjectures Principales‘“. In: *Publications Mathématiques de l'I.H.E.S.* 71 (1990), S. 65–103 (zit. auf S. 104, 114).

[MTT86] Barry Mazur, John Tate und Jeremy Teitelbaum. „On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer“. In: *Inventiones mathematicae* 84 (1986), S. 1–48 (zit. auf S. 75).

[MW84] Barry Mazur und Andrew Wiles. „Class fields of abelian extensions of $\mathbb{Q}$“. In: *Inventiones mathematicae* 79 (1984), S. 179–330 (zit. auf S. 109).

[Neu07] Jürgen Neukirch. *Algebraische Zahlentheorie.* Berlin, Heidelberg, New York: Springer-Verlag, 2007 (zit. auf S. 9, 103, 108).

[NSW00] Jürgen Neukirch, Alexander Schmidt und Kay Wingberg. *Cohomology of Number Fields.* Grundlehren der mathematischen Wissenschaften. A Series of Comprehensive Studies in Mathematics 323. Berlin, Heidelberg: Springer-Verlag, 2000 (zit. auf S. 10 f., 13, 110).

[Och06] Tadashi Ochiai. „p-adic L-functions for Galois deformations and Iwasawa Main Conjecture“. In: *Trends in Mathematics* 9.1 (2006), S. 65–74 (zit. auf S. 107, 113).

[Pan97] Alexei A. Panchishkin. „Non-Archimedian Mellin Transform and p-Adic L-Functions“. In: *Vietnam Journal of Mathematics* 25.3 (1997), S. 179–202 (zit. auf S. 56).

[Ros94] Jonathan Rosenberg. *Algebraic K-Theory and Its Applications.* Graduate Texts in Mathematics 147. New York: Springer-Verlag, 1994 (zit. auf S. 14, 17–19).

[RS11] Kenneth A. Ribet und William A. Stein. *Lectures on Modular Forms and Hecke Operators.* 2011. URL: `http://wstein.org/books/ribet-stein/main.pdf` (zit. auf S. 81).

[RZ00] Luis Ribes und Pavel Zalesskii. *Profinite Groups.* Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics 40. Berlin, Heidelberg: Springer-Verlag, 2000 (zit. auf S. 4 f., 7).

[Sch00] Claus-Günther Schmidt. „Period relations p-adic measures“. In: *Manuscripta Mathematica* 106 (2000), S. 177–201 (zit. auf S. 116).

[Sch11] Peter Schneider. *p-Adic Lie Groups.* Grundlehren der mathematischen Wissenschaften. A Series of Comprehensive Studies in Mathematics 344. Berlin, Heidelberg: Springer-Verlag, 2011 (zit. auf S. 22).

[Sch93] Claus-Günther Schmidt. „Relative modular symbols and p-adic Rankin-Selberg convolutions“. In: *Inventiones mathematicae* 112 (1993), S. 31–76 (zit. auf S. 116).

[Ser67] Jean-Pierre Serre. „Local Class Field Theory“. In: John. W. S. Cassels und Albert Fröhlich. *Algebraic Number Theory.* London: Academic Press, 1967, S. 128–161 (zit. auf S. 102).

[Ser72] Jean-Pierre Serre. „Propriétés galoisiennes des points d'ordre fini des courbes elliptiques“. In: *Inventiones mathematicae* 15 (1972), S. 259–331 (zit. auf S. 112).

[Ser77] Jean-Pierre Serre. *Linear Representations of Finite Groups*. Graduate Texts in Mathematics 42. New York: Springer-Verlag, 1977 (zit. auf S. 28, 62, 103).

[Ser79] Jean-Pierre Serre. *Local Fields*. Graduate Texts in Mathematics 67. New York: Springer-Verlag, 1979 (zit. auf S. 95, 103).

[Shi71] Goro Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Publications of the Mathematical Society of Japan 11. Tokyo: Iwanami Shoten und Princeton University Press, 1971 (zit. auf S. 36, 39, 42 f., 45–47, 49, 51, 80 f.).

[Shi77] Goro Shimura. „On the Periods of Modular Forms“. In: *Mathematische Annalen* 229 (1977), S. 211–221 (zit. auf S. 75).

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics 106. New York: Springer-Verlag, 1986 (zit. auf S. 31, 110, 112).

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics 151. New York: Springer-Verlag, 1994 (zit. auf S. 31, 116).

[Tat67a] John T. Tate. „Fourier Analysis in Number Fields and Hecke's Zeta-Functions“. In: John. W. S. Cassels und Albert Fröhlich. *Algebraic Number Theory*. London: Academic Press, 1967, S. 305–347 (zit. auf S. 34, 74).

[Tat67b] John T. Tate. „Global Class Field Theory“. In: John. W. S. Cassels und Albert Fröhlich. *Algebraic Number Theory*. London: Academic Press, 1967, S. 163–203 (zit. auf S. 34).

[TW95] Richard Taylor und Andrew Wiles. „Ring-theoretic properties of certain Hecke algebras“. In: *Annals of Mathematics* 141.3 (1995), S. 553–572 (zit. auf S. 33, 104, 116).

[Ven03] Otmar Venjakob. „Characteristic Elements in Noncommutative Iwasawa Theory“. Habilitationsschrift. Universität Heidelberg, 2003 (zit. auf S. 22).

[Ven05] Otmar Venjakob. „From classical to non-commutative Iwasawa theory – an introduction to the GL_2 main conjecture“. In: *European Congress of Mathematics: Stockholm, June 27–July 2, 2004*. Hrsg. von Ari Laptev. European Mathematical Society, 2005, S. 861–880 (zit. auf S. 19).

[Was82] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Graduate Texts in Mathematics 83. New York: Springer-Verlag, 1982 (zit. auf S. ix, 8, 11, 59, 61, 63, 65, 108).

[Wei13] Charles Weibel. *The K-book: An Introduction to Algebraic K-theory*. Graduate Studies in Mathematics 145. Providence, Rhode Island: American Mathematical Society, 2013 (zit. auf S. 16).

[Wil88] Andrew Wiles. „On ordinary λ-adic representations associated to modular forms“. In: *Inventiones mathematicae* 94 (1988), S. 529–573 (zit. auf S. 86, 94).

[Wil95] Andrew Wiles. „Modular elliptic curves and Fermat's Last Theorem“. In: *Annals of Mathematics* 141.3 (1995), S. 443–551 (zit. auf S. 33, 104, 116).

[Zag81] Don Bernard Zagier. *Zetafunktionen und quadratische Körper. Eine Einführung in die höhere Zahlentheorie.* Berlin, Heidelberg, New York: Springer-Verlag, 1981 (zit. auf S. 24 f.).

Symbolverzeichnis

Index