Universität Leipzig
Fakultät für Mathematik und Informatik
Mathematisches Institut

Die äquivariante Hauptvermutung der Iwasawa-Theorie für die zyklotomische $\mathbb{Z}_p$-Erweiterung abelscher Zahlkörper

Diplomarbeit
im Studiengang Diplom-Mathematik

Leipzig, 19. Juni 2004

vorgelegt von Malte Witte,
geboren am 23. Juli 1977

Die klassische Hauptvermutung der Iwasawa-Theorie für Dirichlet-Charaktere beschreibt einen Zusammenhang zwischen gewissen Moduln über dem pro-endlichen Gruppenring $\mathbb{Z}_p[\![\mathrm{G}(K_\infty/K)]\!]$ der zyklotomischen Erweiterung K_∞/K eines Zahlkörpers K und p-adischen L-Funktionen zu Dirichlet-Charakteren.

Die äquivariante Hauptvermutung behauptet einen entsprechenden Zusammenhang auch über dem größeren Ring $\mathbb{Z}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$. Ziel der vorliegenden Arbeit ist die konkrete Formulierung und der Beweis einer solchen Aussage für abelsche Zahlkörper, einschließlich des problematischen Falls, dass p die Ordnung von $\mathrm{G}(K/\mathbb{Q})$ teilt.

Inhaltsverzeichnis

Einleitung **1**

1 Charakteristische Ideale perfekter Torsionskomplexe **5**

1.1 Endlich erzeugte projektive Moduln 5
1.2 Cartier-Divisoren und fortsetzbare Homomorphismen 6
1.3 Lokale Charakterisierung von Cartier-Divisoren 8
1.4 Determinanten von projektiven Moduln 9
1.5 Perfekte Torsionskomplexe 12
1.6 Azyklische Komplexe 14
1.7 Konstruktion charakteristischer Ideale 16
1.8 Ergänzungen 19
1.9 Der Zusammenhang mit dem charakteristischen Polynom 21

2 Zyklotomische $\mathbb{Z}_p$-Erweiterungen und pro-endliche Gruppenringe **23**

2.1 Abelsche Zahlkörper und Charaktere 23
2.2 Zyklotomische $\mathbb{Z}_p$-Erweiterungen 26
2.3 Der pro-endliche Gruppenring von $\mathrm{G}(K_\infty/\mathbb{Q})$ 29
2.4 Kompakte $\mathbb{Z}_p$-Algebren 31
2.5 Die universelle Eigenschaft des pro-endlichen Gruppenrings 33
2.6 Zerlegung nach Charakteren 35
2.7 Regularität und Cohen-Macauley-Eigenschaft 39
2.8 Charaktere und Primideale 39
2.9 Cartier-Divisoren des pro-endlichen Gruppenrings 40
2.10 Die Operation der stetigen Charaktere 42

3 Stickelberger-Elemente und p-adische L-Funktionen **45**

3.1 Stickelberger-Elemente 45
3.2 Der Nenner des Stickelberger-Elements 47
3.3 Die äquivariante L-Funktion 51
3.4 Zerlegung nach Charakteren 53

4 Das Theorem von Ferrero-Washington **59**

4.1 Die μ-Invariante von K. Iwasawa 59
4.2 Das Theorem von Ferrero-Washington 60
4.3 Vorbereitungen 61
4.4 Iwasawa-Potenzreihen 62
4.5 Relationen der Koeffizienten $B_n(a)$ 64
4.6 Ein Kriterium für das Verschwinden modulo π 66

4.7 Eine weitere Umformulierung 68
4.8 Abschluss des Beweises 70
4.9 Eine Konsequenz für die äquivariante L-Funktion 70

5 Kohomologie von $\mathbb{Z}_p$-Erweiterungen **73**
5.1 Moduln mit stetiger Galois-Operation 73
5.2 Stetige Galois-Kohomologie 74
5.3 Exaktheit von $C^n(G, \cdot)$ 76
5.4 Endliche kohomologische Dimension 77
5.5 Tensorprodukte und Koeffizientenerweiterungen 78
5.6 Eingeschränkte Verzweigung 81
5.7 Induzierte Moduln 83

6 Die äquivariante Hauptvermutung **87**
6.1 Formulierung der äquivarianten Hauptvermutung 87
6.2 Kohomologie von $\mathbb{Z}_p(\varepsilon_{cycl})$ 88
6.3 Torsion und μ-Invariante 92
6.4 Euler-Faktoren 95
6.5 Die Hauptvermutung für Dirichlet-Charaktere 99
6.6 Zerlegung unter Charakteren 101
6.7 Abschluss des Beweises 103

Literaturverzeichnis **I**

Symbolverzeichnis **V**

Einleitung

In der Iwasawa-Theorie beschäftigt man sich mit dem asymptotischen Verhalten der Einheiten- und Klassengruppen der Zwischenkörper von $\mathbb{Z}_p$-Erweiterungen eines Zahlkörpers K, also Erweiterungen, deren Galoisgruppe isomorph zu $\mathbb{Z}_p$ ist. Die zyklotomische $\mathbb{Z}_p$-Erweiterung K_∞/K von K ist dabei von besonderer Bedeutung. Ist $\zeta_p \in K$, so erhält man sie durch Adjunktion aller p^n-ten Einheitswurzeln ζ_{p^n}. Die Quelle der Inspiration für die Iwasawa-Theorie ist die erstaunliche Analogie der Situation über K_∞ zu der Theorie algebraischer Kurven über endlichen Körpern.

K. Iwasawa nahm den klassischen Satz von Weil (siehe [NSW00], Kap. XI, § 6) über den Zusammenhang zwischen dem Tate-Modul der Jakobi-Varietät und der ζ-Funktion von Kurven über endlichen Körpern zum Anlass, einen vergleichbaren Zusammenhang auch für den projektiven Limes der Klassengruppen

$$X = \varprojlim_n Cl(K_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

aller Zwischenkörper K_n der zyklotomischen Erweiterung K_∞/K und den p-adischen L-Funktionen zu Dirichlet-Charakteren zu vermuten.

X ist in natürlicher Weise ein Modul über dem pro-endlichen Gruppenring

$$\Lambda = \mathbb{Z}_p[\![\mathrm{G}(K_\infty/K)]\!] \cong \mathbb{Z}_p[\![T]\!].$$

Ist χ ein ungerader Dirichlet-Charakter und vom Teichmüller-Charakter verschieden, so ist die p-adische L-Funktion durch eine Potenzreihe in einer endlichen Erweiterung von $\mathbb{Z}_p[\![T]\!]$ gegeben. Die Hauptvermutung der Iwasawa-Theorie für Dirichlet-Charaktere besagt, dass diese Potenzreihe bis auf eine Einheit mit dem charakteristischen Polynom des geeignet definierten χ-Eigenraums von X übereinstimmt.

In dieser Form wurde die Hauptvermutung von B. Mazur und A. Wiles für abelsche Zahlkörper bewiesen (siehe [MW86]), in leicht abgeschwächter Form von A. Wiles auch für total reelle Zahlkörper (siehe [Wil90]).

Die Idee der äquivarianten Hauptvermutung ist es nun, die Aussagen der Hauptvermutung für jeden einzelnen ungeraden Charakter von $\mathrm{G}(K/\mathbb{Q})$ zu einem vergleichbaren Zusammenhang zwischen einem Objekt X' über dem größeren Ring

$$\Omega = \mathbb{Z}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$$

und einer geeignet definierten äquivarianten p-adischen L-Funktion zusammenzufügen. Die äquivariante L-Funktion sollte dabei im Wesentlichen mit dem Limes der Stickelberger-Elemente der Zwischenkörper K_n übereinstimmen.

Ziel der vorliegenden Arbeit ist es, diese Aussage für die zyklotomische Erweiterung von abelschen Zahlkörpern zu formulieren und im Beweis auf die Hauptvermutung für Charaktere zurückzuführen. Die wesentlichen Ideen des vorgestellten Beweises gehen auf D. Burns und C. Greither zurück, die in [BG03] bereits ein fast identisches Resultat erzielt haben.

Als Ausgangspunkt wählen wir jedoch nicht die klassische Form, sondern die kohomologische Interpretation der Hauptvermutung, wie sie kürzlich von A. Huber und G. Kings im Zuge ihres Beweises der Tamagawa-Zahl-Vermutung von Bloch und Kato formuliert und bewiesen wurde (siehe [HK03]). In dieser Formulierung wird X durch das alternierende Produkt der charakteristischen Polynome von gewissen étalen Kohomologiegruppen ersetzt.

Ist p kein Teiler der Ordnung der Galoisgruppe $\mathrm{G}(K/\mathbb{Q})$, so lässt sich aus diesem Ergebnis auf fast triviale Weise eine äquivariante Version gewinnen. In diesem Fall zerfällt Ω durch Zerlegung nach Charakteren in ein endliches direktes Produkt von Kopien der Iwasawa-Algebra Λ und die äquivariante Hauptvermutung ist äquivalent zur Gültigkeit der Hauptvermutung für Dirichlet-Charaktere auf jedem einzelnen Faktor.

Teilt jedoch p die Gruppenordnung, so ist die Zerlegung nach Charakteren keine direkte Zerlegung mehr, sondern mit Informationsverlust verbunden. Zusätzliche Schwierigkeiten entstehen dadurch, dass nun die Kohomologiegruppen über Ω keine endliche projektive Auflösung mehr besitzen. Letzteres ist aber eine wesentliche Voraussetzung für die Existenz eines verallgemeinerten charakteristischen Polynoms in Form der Determinante von Knudsen und Mumford (siehe [KM76]).

Die eigentliche Aufgabe besteht deshalb darin, diese Probleme zu überwinden und die äquivariante Hauptvermutung so zu formulieren, dass die Teilbarkeitsbeschränkungen verschwinden. Dies wird dadurch erreicht, dass statt der Kohomologie-Gruppen direkt der entsprechende Koketten-Komplex in der abgeleiteten Kategorie verwendet wird. Wir zeigen, dass die Determinanten-Konstruktion von Knudsen und Mumford diesem Komplex einen invertierbaren Ω-Untermodul des Quotientenrings von Ω zuordnet. Die äquivariante Hauptvermutung ist nun die Aussage, dass dieser Modul von der äquivarianten p-adischen L-Funktion erzeugt wird. Aus technischen Gründen müssen wir allerdings dabei die Euler-Faktoren zu einer endlichen Menge von Primstellen schlechter Reduktion entfernen. Außerdem schließen wir den Fall $p = 2$ von unseren Betrachtungen aus.

Der Schlüssel zum Beweis dieser Aussage ist das Theorem von Ferrero-Washington über das Verschwinden der μ-Invariante von Iwasawa. Wir folgern daraus, dass der Träger des Koketten-Komplexes keine der Singularitäten von Ω enthält. Dieses Zusatzwissen reicht aus, um den Informationsverlust beim Zerlegen nach Charakteren auszugleichen.

Überblick

Die Arbeit ist wie folgt gegliedert: Kapitel 1 behandelt die Konstruktion des charakteristischen Ideals eines perfekten Komplexes über kommutativen Ringen. Dieser Teil der Arbeit ist relativ technisch und kann beim ersten Lesen übersprungen werden.

In Kapitel 2 stellen wir einige elementare Ergebnisse über zyklotomische $\mathbb{Z}_p$-Erweiterungen und pro-endliche Gruppenringe zusammen. Kapitel 3 stellt dar, wie sich aus den Stickelberger-Elementen die äquivariante L-Funktion konstruieren lässt und in Kapitel 4 geben wir den Beweis des Theorems von Ferrero-Washington wieder.

Kapitel 5 beschäftigt sich mit den Eigenschaften von Koketten-Komplexen der stetigen Galois-Kohomologie, die wir anstelle von étaler Kohomologie verwenden. Mit einem solchen Koketten-Komplex werden wir in Kapitel 6 die äquivariante Hauptvermutung formulieren und anschließend beweisen.

1 Charakteristische Ideale perfekter Torsionskomplexe

In diesem Kapitel werden wir eine weit reichende Verallgemeinerung des Begriffs des charakteristischen Polynoms darstellen. Die Konstruktion geht auf den Determinanten-Funktor von F. Knudsen und D. Mumford [KM76] (siehe auch P. Deligne, [Del87]) zurück. Dieser ordnet jedem perfekten Komplex einen invertierbaren Modul, aufgefasst als ein Objekt einer Picard-Kategorie, zu.

Beschränkt man sich allerdings auf solche Komplexe, die über dem totalen Quotientenring azyklisch werden, kann man die entsprechenden Determinanten der Komplexe auf natürliche Weise als invertierbare Untermoduln des Quotientenrings, also als Cartier-Divisoren, auffassen.

Dies ist auch die Voraussetzung, unter der wir die Theorie hier entwickeln wollen. Außerdem beschränken wir uns auf den Fall kommutativer Ringe, d.h. affiner Schemata. Es sollte jedoch möglich sein, die Ergebnisse auch auf allgemeinere Schemata auszudehnen.

1.1 Endlich erzeugte projektive Moduln

Wir erinnern an folgende Charakterisierung endlich erzeugter projektiver Moduln.

Satz 1.1.1. *Sei R ein kommutativer Ring (nicht notwendig noethersch) und P ein R-Modul. Dann sind nachstehende Aussagen äquivalent:*

(i) *P ist ein endlich erzeugter projektiver Modul.*

(ii) *Es gibt endlich viele Elemente $f_1, \ldots, f_n \in R$, die zusammen das (1)-Ideal von R erzeugen, so dass für alle $i = 1, \ldots, n$ der $R[f_i^{-1}]$-Modul $P[f_i^{-1}]$ frei von endlichem Rang ist.*

(iii) *P ist endlich erzeugt, für alle $\mathfrak{p} \in \operatorname{Spec} R$ ist $P_\mathfrak{p}$ frei vom endlichen Rang $\operatorname{rk}_P(\mathfrak{p})$ und die Funktion $\mathfrak{p} \mapsto \operatorname{rk}_P(\mathfrak{p})$ ist lokal konstant auf $\operatorname{Spec} R$.*

(iv) *P ist ein direkter Summand eines endlich erzeugten freien Moduls.*

Beweis. Siehe [Bou89b], Ch. II, Sec 2, Thm. 1. Für die letzte Äquivalenz siehe [Eis99], Thm. A3.1. □

Für beliebige Moduln definieren wir:

Definition 1.1.2. Sei $\phi : R \longrightarrow S$ ein Ringhomomorphismus. Ist M ein R-Modul, so nennen wir den S-Modul

$$\phi_* M = M \otimes_R S$$

die *Koeffizientenerweiterung* von M via ϕ.

Man prüft leicht nach, dass die Koeffizientenerweiterung eines endlich erzeugten, projektiven Moduls selbst wieder endlich erzeugt und projektiv ist. ϕ_* ist also ein Funktor von der Kategorie der endlich erzeugten, projektiven R-Moduln in die entsprechende Kategorie der S-Moduln.

Auf der Kategorie der endlich erzeugten projektiven Moduln ist außerdem wie folgt eine kontravariante Auto-Äquivalenz gegeben:

Definition 1.1.3. Wir schreiben

$$\check{P} \stackrel{\text{def}}{=} \operatorname{Hom}_R(P, R)$$

für das *Dual* eines projektiven Moduls. Ist $f : P \longrightarrow P'$ ein Homomorphismus projektiver Moduln, so heißt die induzierte Abbildung $f^* : \check{P}' \longrightarrow \check{P}$ *duale Abbildung.* Ist P frei mit Basis $e_1, \ldots, e_n$, dann heißt die Basis $\check{e}_1, \ldots, \check{e}_n$ von $\check{P}$ mit

$$\check{e}_i(e_j) = \begin{cases} 1 & \text{für } i = j, \\ 0 & \text{sonst,} \end{cases}$$

duale Basis zu $e_1, \ldots, e_n$.

Die folgenden Eigenschaften des Duals sind hinreichend bekannt:

Lemma 1.1.4.

(i) Das Dual $\check{P}$ eines endlich erzeugten projektiven Moduls ist ein endlich erzeugter und projektiver Modul vom gleichen Rang.

(ii) Das doppelte Dual $\check{\check{P}}$ ist kanonisch isomorph zu P.

(iii) Das Dual einer exakten Sequenz projektiver Moduln ist wieder exakt.

(iv) Sei $\phi : R \longrightarrow S$ ein Ring-Homomorphismus. Dann ist der S-Modul $\phi_*\check{P}$ kanonisch isomorph zum Dual von ϕ_*P über S.

1.2 Cartier-Divisoren und fortsetzbare Homomorphismen

Im Folgenden sei R ein kommutativer Ring mit 1. Mit $Q(R)$ bezeichnen wir den (totalen) *Quotientenring* von R, also die Lokalisierung von R an der multiplikativ abgeschlossenen Menge der Nichtnullteiler. Wir erinnern daran, dass der natürliche Homomorphismus

$$\eta : R \longrightarrow Q(R)$$

stets injektiv ist.

Definition 1.2.1. Ein endlich erzeugter projektiver Modul mit konstantem Rang 1 heißt *invertierbar*. Ein invertierbarer R-Untermodul I von $Q(R)$ mit $\eta_*(I) = Q(R)$ heißt *Cartier-Divisor* (oder *gebrochenes invertierbares Ideal*). Die Menge der Cartier-Divisoren bezeichnen wir mit $\mathfrak{C}(R)$.

Bemerkung 1.2.2. Mit dieser Definition des Cartier-Divisors folgen wir [Eis99], Sec. 11.3. Ist R noethersch und reduziert, (d.h. es existieren keine nilpotenten Elemente), so stimmt der Begriff mit der in der algebraischen Geometrie üblichen Definition als invertierbare Unter-Garbe der Garbe der totalen Quotientenringe $\mathcal{K}$ des affinen Schemas $\operatorname{Spec} R$ (siehe [Har77], Ch. II, Sec. 6) überein, denn [Eis99], Ex. 3.15(a) zeigt, dass man $\mathcal{K}$ mit der zu $Q(R)$ assoziierten quasi-kohärenten Garbe identifizieren kann. Für nicht reduzierte R ist letzteres im Allgemeinen nicht mehr möglich (Ein Gegenbeispiel lässt sich mit Hilfe von [Eis99], Ex. 3.15(c) konstruieren).

Bemerkung 1.2.3. Die Bedingung $\eta_*(I) = Q(R)$ ist für noethersche Ringe R überflüssig (siehe [Eis99], Theorem 11.6.(b)).

Lemma 1.2.4.

(i) Die Menge $\mathfrak{C}(R)$ wird mit der Multiplikation

$$(I, J) \mapsto IJ \subset Q(R)$$

zu einer abelschen Gruppe. $R \subset Q(R)$ ist das neutrale Element und das Inverse von $I \in \mathfrak{C}(R)$ ist gegeben durch

$$I^{-1} = \{s \in Q(R) \,|\, sI \subset R\}.$$

(ii) Ist $I \subset Q(R)$ ein beliebiger R-Untermodul, dann gilt genau dann $I \in \mathfrak{C}(R)$, wenn es einen R-Untermodul $J \subset Q(R)$ gibt, so dass $IJ = R$.

(iii) Seien $I, J \in \mathfrak{C}(R)$. Dann ist

$$I \otimes_R J \longrightarrow IJ, \;\; a \otimes b \mapsto ab$$

ein Isomorphismus.

Beweis. Siehe [Bou89b], Kap. II, § 5.6. □

Wir möchten $\mathfrak{C}(\cdot)$ als einen Funktor von der Kategorie der kommutativen Ringe in die Kategorie der abelschen Gruppen auffassen. Dazu schränken wir die Morphismen der Kategorie der noetherschen reduzierten Ringe auf solche Homomorphismen ein, die folgende zusätzliche Bedingung erfüllen:

Definition 1.2.5. Wir nennen einen Ringhomomorphismus $\phi : R \longrightarrow S$ *fortsetzbar*, wenn es eine (stets eindeutig bestimmte) Fortsetzung von ϕ zu einem Homomorphismus $Q(R) \longrightarrow Q(S)$ gibt.

Aus der Definition des Quotientenrings folgt leicht, dass eine solche Fortsetzung genau dann existiert, wenn ϕ alle Nichtnullteiler von R in Nichtnullteiler von S abbildet. Die Fortsetzung wollen wir wieder ϕ nennen.

Lemma 1.2.6. *Sei $\phi : R \longrightarrow S$ fortsetzbar. Dann ist durch $I \mapsto \phi(I)S \subset Q(S)$ ein Gruppenhomomorphismus $\mathfrak{C}(\phi) : \mathfrak{C}(R) \longrightarrow \mathfrak{C}(S)$ gegeben.*

Beweis. Sicher gilt $\phi(R)S = S$ und $\phi(IJ)S = (\phi(I)S)(\phi(J)S)$ für alle R-Untermoduln I und J von $Q(R)$. Für $I \in \mathfrak{C}(R)$ gilt somit

$$S = \phi(R)S = \phi(I)\phi(I^{-1})S = (\phi(I)S)(\phi(I^{-1})S).$$

Mit Lemma 1.2.4 folgt $\phi(I)S \in \mathfrak{C}(S)$. □

Eine wichtige Klasse von fortsetzbaren Homomorphismen bilden die *flachen* Ringhomomorphismen (d.h. mit der von $R \longrightarrow S$ induzierten R-Algebren-Struktur ist S ein flacher R-Modul):

Lemma 1.2.7. *Alle flachen Ringhomomorphismen sind fortsetzbar. Insbesondere trifft dies auf Lokalisierungen zu.*

Beweis. Siehe [Eis99], Cor. 6.3 und beachte, dass Lokalisierungen flach sind ([Eis99], Prop. 2.5). □

Bemerkung 1.2.8. Ist $f : R \longrightarrow S$ ein fortsetzbarer Homomorphismus zwischen noetherschen, reduzierten Ringen und sind $U \subset R$, $V \subset S$ beliebige multiplikativ abgeschlossene Mengen mit $f(U) \subset V$, so ist nach [Eis99], Ex. 3.15(a) auch der Homomorphismus $f : R[U^{-1}] \longrightarrow R[V^{-1}]$ fortsetzbar. Man beachte, dass dies für nicht reduzierte Ringe im Allgemeinen nicht gilt.

1.3 Lokale Charakterisierung von Cartier-Divisoren

In diesem Abschnitt sei R noethersch. Es zeigt sich, dass ein Cartier-Divisor $I \in \mathfrak{C}(R)$ schon durch die Lokalisierungen an allen zu Nichtnullteilern $r \in R$ assoziierten Primidealen eindeutig festgelegt ist:

Definition 1.3.1. Sei r ein Nichtnullteiler von R. Wir nennen ein Primideal $\mathfrak{p} \in \operatorname{Spec} R$ *zu r assoziiert*, wenn es zu $R/(r)$ assoziiert ist. Das heißt, es ist der *Annullator* eines Elements a von $R/(r)$:

$$\mathfrak{p} = \{x \in R \,|\, xa = 0\}.$$

Satz 1.3.2. *Sei R noethersch und seien $I, J \in \mathfrak{C}(R)$. Es gilt $I = J$ genau dann, wenn für alle zu Nichtnullteilern assoziierte Primideale $\mathfrak{p}$ auch $\mathfrak{C}(\imath_\mathfrak{p})(I) = \mathfrak{C}(\imath_\mathfrak{p})(J)$ gilt. Dabei bezeichnet $\imath_\mathfrak{p}$ den natürlichen Homomorphismus $R \longrightarrow R_\mathfrak{p}$ beziehungsweise die Fortsetzung zu $Q(R) \longrightarrow Q(R_\mathfrak{p})$.*

Beweis. Trivialerweise gilt $\mathfrak{C}(\imath_\mathfrak{p})(I) = \mathfrak{C}(\imath_\mathfrak{p})(J)$, wenn $I = J$. Für die Gegenrichtung reicht es zu zeigen, dass $IJ^{-1} \subset R$ und $I^{-1}J \subset R$, falls $\mathfrak{C}(\imath_\mathfrak{p})(IJ^{-1}) = \mathfrak{C}(\imath_\mathfrak{p})(I^{-1}J) = R_\mathfrak{p}$ für alle zu Nichtnullteilern assoziierten Primideale $\mathfrak{p}$. Dies lässt sich wiederum auf folgende Aussage reduzieren: Wenn $x \in Q(R)$ und $\imath_\mathfrak{p}(x) \in R_\mathfrak{p}$ für jedes der $\mathfrak{p}$ erfüllt ist, so liegt x bereits in R.

Wir folgen dem Argument von [Eis99] (Prop. 11.3): Sei $x \stackrel{def}{=} \frac{a}{r}$ mit $a, r \in R$, r ein Nichtnullteiler. Angenommen, x liegt nicht in R. Dann liegt a nicht in dem von r erzeugten Ideal, denn sonst könnte man den Bruch $\frac{a}{r}$ um r kürzen.

Nun gilt $a \in rR$ genau dann, wenn $\imath_\mathfrak{p}(a) \in \imath_\mathfrak{p}(r)R_\mathfrak{p}$ für alle zu r assoziierten Primideale $\mathfrak{p}$ gilt (siehe [Eis99], Cor. 3.5(b)). Im Umkehrschluss folgt, dass es ein zu r assoziiertes Primideal $\mathfrak{p}$ gibt, so dass $\imath_\mathfrak{p}(a) \notin \imath_\mathfrak{p}(r)R_\mathfrak{p}$. Das heißt aber

$$\imath_\mathfrak{p}(x) = \frac{\imath_\mathfrak{p}(a)}{\imath_\mathfrak{p}(r)} \notin R_\mathfrak{p} = \mathfrak{C}(\imath_\mathfrak{p})(R).$$

Somit ist die Aussage bewiesen. □

Wir erinnern an folgende Definitionen der kommutativen Algebra (siehe [Eis99], Kap. 17 und 18):

Definition 1.3.3. Sei R ein noetherscher Ring und $\mathfrak{p}$ ein Primideal von R. Wir schreiben $\operatorname{codim} \mathfrak{p} \overset{\text{def}}{=} \dim R_\mathfrak{p}$ für die *Kodimension* von $\mathfrak{p}$.

(i) Eine Folge $x_1, \ldots, x_n$ von Elementen in $\mathfrak{p}$ heißt *reguläre Folge*, wenn für jedes $i = 1, \ldots, n$ das Element x_i ein Nichtnullteiler von $R/(x_1, \ldots, x_{i-1})$ ist.

(ii) R ist ein *Cohen-Macauley-Ring*, wenn in jedem maximalen Ideal $\mathfrak{m}$ eine reguläre Folge der Länge $\operatorname{codim} \mathfrak{m}$ existiert.

Wenn R ein Cohen-Macauley-Ring ist, so lässt sich die Bedingung, zu einem Nichtnullteiler assoziiert zu sein, wie folgt ausdrücken:

Lemma 1.3.4. *Sei R ein Cohen-Macauley-Ring. Ein Primideal $\mathfrak{p}$ von R ist genau dann zu einem Nichtnullteiler assoziiert, wenn gilt*

$$\operatorname{codim} \mathfrak{p} = 1.$$

Beweis. [Eis99], Beweis von Theorem 18.15. □

1.4 Determinanten von projektiven Moduln

Sei P ein endlich erzeugter, projektiver R-Modul. Nach Satz 1.1.1.(ii) gibt es Elemente $f_1, \ldots, f_d$, die zusammen das (1)-Ideal von R erzeugen, so dass $P[f_i^{-1}]$ ein freier $R[f_i^{-1}]$-Modul vom Rang r_i ist.

Definition 1.4.1. Die *Determinante* $\det_R P$ von P ist der durch

$$(\det_R P)[f_i^{-1}] = \bigwedge^{r_i} P[f_i^{-1}], \qquad 1 \leq i \leq n,$$

eindeutig bestimmte R-Untermodul der äußeren Algebra $\bigwedge_R(P)$ von P.

Bemerkung 1.4.2. Siehe [Bou89a], Kap. III, § 7 für die Definition und Eigenschaften der äußeren Algebra eines Moduls.

Bemerkung 1.4.3. Ist der Rang von P konstant, so ist die Determinante gleich der höchsten äußeren Potenz von P. Beachte nun, dass der Rang eines endlich erzeugten, projektiven Moduls eine lokal-konstante Funktion $\operatorname{Spec} R \longrightarrow \mathbb{Z}$ ist. Insbesondere kann man $\operatorname{Spec} R$ in endlich viele Komponenten zerlegen, so dass der Rang auf jeder Komponente konstant ist. Diese Zerlegung entspricht einer Darstellung

$$R = \prod_{i=1}^{n} R_i$$

von R (siehe [Har77], Kap. II, Ex. 2.19), so dass $\det_R P$ auf jedem Faktor R_i jeweils durch die höchste äußere Potenz gegeben ist.

Lemma 1.4.4. *Die Determinante $\det_R P$ ist ein endlich erzeugter, invertierbarer R-Modul.*

Beweis. Der $P[f_i^{-1}]$-Modul $(\det_R P)[f_i^{-1}]$ ist die höchste äußere Potenz des freien $P[f_i^{-1}]$-Moduls $P[f_i^{-1}]$, also frei vom Rang 1. Wähle einen Erzeuger a_i. Nach Multiplikation mit einer geeigneten Potenz von f_i können wir o.B.d.A. annehmen, dass a_i ein Urbild b_i in R besitzt. Dann wird $\det_R P$ von $b_1, \ldots, b_n$ erzeugt (siehe [Eis99], Ex. 2.19). Nach Satz 1.1.1.(ii) ist $\det_R P$ also endlich erzeugt und projektiv vom Rang 1, also invertierbar. □

Ist $f : P_1 \longrightarrow P_2$ ein Isomorphismus von endlich erzeugten, projektiven Moduln, so induziert der Isomorphismus

$$\wedge(f) : \bigwedge\nolimits_R(P_1) \longrightarrow \bigwedge\nolimits_R(P_2), \qquad a_1 \wedge \ldots \wedge a_k \longrightarrow f(a_1) \wedge \ldots \wedge f(a_k)$$

der äußeren Algebren einen Isomorphismus der Determinanten. Ferner gilt:

Lemma 1.4.5. *Es existieren folgende natürliche Isomorphismen:*

(i) Für einen Ring-Homomorphismus $\phi : R \longrightarrow S$ zweier noetherscher reduzierter Ringe ist

$$\mathbf{b}(\phi) : \phi_*(\det_R P) \longrightarrow \det_S \phi_*(P)$$

lokal durch

$$\mathbf{b}(\phi)((e_1 \wedge \cdots \wedge e_n) \otimes s) = s((e_1 \otimes 1) \wedge \cdots \wedge (e_n \otimes 1))$$

gegeben ($e_1, \ldots, e_n$ bezeichne eine lokale Basis von P).

(ii) Für einen projektiven R-Modul P ist

$$\mathbf{r} : \det_R(P) \otimes_R \det_R(\check{P}) \longrightarrow R$$

lokal durch

$$\mathbf{r}(e_1 \wedge \cdots \wedge e_n \otimes \check{e}_n \wedge \cdots \wedge \check{e}_1) = 1$$

gegeben (dabei sei $\check{e}_1, \ldots, \check{e}_n$ die duale Basis zu $e_1, \ldots, e_n$).

(iii) Für zwei endlich erzeugte projektive Moduln P' und P'' ist

$$\mathbf{c} : \det_R(P') \otimes_R \det_R(P'') \longrightarrow \det_R(P'') \otimes_R \det_R(P')$$

lokal durch

$$\mathbf{c}(e'_1 \wedge \cdots \wedge e'_{r_i} \otimes e''_1 \wedge \cdots \wedge e''_{s_i}) = (-1)^{r_i s_i} e''_1 \wedge \cdots \wedge e''_{r_i} \otimes e'_1 \wedge \cdots \wedge e'_{s_i}$$

für Basen $e'_1, \ldots, e'_{r_i}$ von $P'[f_i^{-1}]$ und $e''_1, \ldots, e''_{s_i}$ von $P''[f_i^{-1}]$ gegeben, wobei die Zerlegung der Einheit $(f_1, \ldots, f_d) = (1)$ so fein gewählt werde, dass beide Moduln frei sind.

(iv) Sei

$$0 \longrightarrow P' \xrightarrow{f} P \xrightarrow{g} P'' \longrightarrow 0$$

eine kurze exakte Sequenz von endlich erzeugten projektiven R-Moduln und h ein Schnitt von g. Dann ist lokal durch

$$\mathbf{s}(f,g)(e'_1 \wedge \cdots \wedge e'_n \otimes e''_1 \wedge \cdots e''_m) = f(e'_1) \wedge \cdots \wedge f(e'_n) \wedge h(e''_1) \wedge \cdots \wedge h(e''_m)$$

ein Isomorphismus

$$\mathbf{s}(f,g) : \det_R(P') \otimes_R \det_R(P'') \longrightarrow \det_R(P)$$

gegeben (dabei sei $e'_1, \ldots, e'_n$ eine lokale Basis von P', $e''_1, \ldots, e''_m$ eine lokale Basis von P''). Dieser Isomorphismus ist von der Wahl von h unabhängig.

Zum Beweis. Diese Isomorphismen existieren bereits auf der äußeren Algebra, siehe [Bou89a], Kap. III, § 7. Die Unabhängigkeit von der Wahl des Schnittes in (iv) sieht man wie folgt: O.B.d.A. seien P', P'' und P frei. Sei $e'_1, \ldots, e'_n$ eine Basis von P', $e''_1, \ldots, e''_m$ eine Basis von P''. Dann ist $f(e'_1), \ldots, f(e'_n), h(e''_1), \ldots, h(e''_m)$ eine Basis von P und die Matrix zur Abbildung $f \oplus h : P' \oplus P'' \longrightarrow P$ ist die Einheitsmatrix. Ist nun h' ein weiterer Schnitt zu g, so liegt die Differenz $h(e''_i) - h'(e''_i)$ im Kern von g, d.h. die Matrix M zu $f \oplus h'$ in derselben Basis hat obere Dreiecksgestalt und die Einträge auf der Hauptdiagonalen sind gleich 1. Also ist die Determinante von M gleich 1. Nun gilt

$$f(e'_1) \wedge \ldots \wedge f(e'_n) \wedge h'(e''_1) \wedge \ldots \wedge h'(e''_m) = (\det M) f(e'_1) \wedge \ldots \wedge f(e'_n) \wedge h(e''_1) \wedge \ldots \wedge h(e''_m)$$

und somit die Behauptung. □

Der Isomorphismus **r** und das Vorzeichen in der Definition von **c** sind so gewählt, dass wir im folgenden Lemma stets Kommutativität erhalten:

Lemma 1.4.6. *(i) Betrachte folgendes kommutatives Diagramm von endlich erzeugten projektiven R-Moduln mit exakten Zeilen und Spalten*

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & P_{11} \arrow[r, "r_{11}"] \arrow[d, "d_{11}"'] & P_{12} \arrow[r, "r_{12}"] \arrow[d, "d_{12}"'] & P_{13} \arrow[r] \arrow[d, "d_{13}"'] & 0 \\
0 \arrow[r] & P_{21} \arrow[r, "r_{21}"] \arrow[d, "d_{21}"'] & P_{22} \arrow[r, "r_{22}"] \arrow[d, "d_{22}"'] & P_{23} \arrow[r] \arrow[d, "d_{23}"'] & 0 \\
0 \arrow[r] & P_{31} \arrow[r, "r_{31}"] \arrow[d] & P_{32} \arrow[r, "r_{32}"] \arrow[d] & P_{33} \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Dann ist folgendes Diagramm kommutativ:

$$\begin{tikzcd}
& \det_R P_{11} \otimes_R \det_R P_{31} \otimes_R \det_R P_{13} \otimes_R \det_R P_{33} \arrow[dl, "\mathbf{s}(d_{11},d_{21})\otimes\mathbf{s}(d_{13},d_{23})"'] \arrow[dddd, "id\otimes c\otimes id"] \\
\det_R P_{21} \otimes_R \det_R P_{23} \arrow[d, "\mathbf{s}(r_{21},r_{22})"'] & \\
\det_R P_{22} & \\
\det_R P_{12} \otimes_R \det_R P_{32} \arrow[u, "\mathbf{s}(d_{12},d_{22})"] & \\
& \det_R P_{11} \otimes_R \det_R P_{13} \otimes_R \det_R P_{31} \otimes_R \det_R P_{33} \arrow[ul, "\mathbf{s}(r_{11},r_{12})\otimes\mathbf{s}(r_{31},r_{32})"']
\end{tikzcd}$$

(ii) *Für eine kurze exakte Sequenz*

$$0 \longrightarrow P' \xrightarrow{f} P \xrightarrow{g} P'' \longrightarrow 0$$

erhalten wir ein kommutatives Viereck:

$$\begin{tikzcd}
\det_R P' \otimes_R \det_R P'' \otimes_R \det_R \check{P}'' \otimes_R \det_R \check{P}' \arrow[r, "\mathbf{s}(f,g)\otimes\mathbf{s}(g^*,f^*)"] \arrow[d, "id\otimes\mathbf{r}_{P''}\otimes id"'] & \det_R P \otimes_R \det_R \check{P} \arrow[d, "\mathbf{r}_P"] \\
\det_R P' \otimes_R \det_R \check{P}' \arrow[r, "\mathbf{r}_{P'}"] & R
\end{tikzcd}$$

(iii) *Die Isomorphismen* $\mathbf{s}, \mathbf{r}, \mathbf{c}$ *kommutieren mit* $\mathbf{b}(\phi)$.

Zum Beweis. Die Behauptungen lassen sich lokal auf einer Basis leicht nachprüfen. In (i) sollte man zunächst Basen der Ecken P_{11}, P_{13}, P_{31}, P_{33} und dann Schnitte

$$u : P_{31} \longrightarrow P_{21}, \qquad v : P_{13} \longrightarrow P_{12}, \qquad w : P_{33} \longrightarrow P_{22}$$

wählen. □

Bemerkung 1.4.7. In [KM76] ist das Vorzeichen Teil der Definition eines invertierbaren Moduls, d.h. ein invertierbarer Modul ist ein endlich erzeugter, projektiver Modul vom Rang 1 zusammen mit einer lokal konstanten Funktion $\operatorname{Spec} R \longrightarrow \mathbb{Z}$. Dies ist notwendig, um die Kategorie der invertierbaren Moduln als Picard-Kategorie auffassen zu können. Diese Struktur ist aber für uns nicht von Interesse.

1.5 Perfekte Torsionskomplexe

Wir betrachten nun Komplexe von R-Moduln. Für die grundlegenden Definitionen verweisen wir auf [GM96]. Insbesondere betrifft dies die Begriffe *abgeleitete Kategorie*, *abgeleiteter Funktor* und *ausgezeichnetes Dreieck*. Für den Kegel und die Translation benutzen wir dieselbe Vorzeichenkonvention wie in [GM96], Kap. III, § 3.1:

Definition 1.5.1.

(i) Sei $f : K^\bullet \longrightarrow L^\bullet$ ein Homomorphismus von Komplexen. Dann bezeichnet $Cone^\bullet(f)$ den *Kegel* von f, d.h.

$$Cone^n(f) \stackrel{def}{=} K^{n+1} \oplus L^n$$

wobei das Differential durch

$$\partial^n(a,b) \stackrel{def}{=} (-\partial_K^{n+1}(a), f^{n+1}(a) + \partial_L^n(b))$$

für $(a,b) \in K^{n+1} \oplus L^n$ gegeben ist.

(ii) Ist $K^\bullet$ ein Komplex und $k \in \mathbb{Z}$, dann bezeichnet $K^\bullet[k]$ die *Translation* von $K^\bullet$ um k, d.h. $K^n[k] \stackrel{def}{=} K^{n+k}$ und für das Differential gilt $\partial^n[k] \stackrel{def}{=} (-1)^k \partial^{n+k}$.

Definition 1.5.2. Sei $K^\bullet$ ein nach oben beschränkter Komplex von R-Moduln und M ein R-Modul. Mit

$$K^\bullet \otimes_R^{\mathbb{L}} M$$

bezeichnen wir das *links-abgeleitete Tensorprodukt* von $K^\bullet$ und M. Ist $\phi : R \longrightarrow S$ ein Ring-Homomorphismus, so nennen wir den Komplex von S-Moduln

$$\mathbf{L}\phi_* K^\bullet \stackrel{def}{=} K^\bullet \otimes_R^{\mathbb{L}} S$$

als (links-abgeleitete) *Koeffizientenerweiterung* von $K^\bullet$ via ϕ. Die Einbettung von R in den Quotientenkörper werden wir stets mit $\eta : R \longrightarrow Q(R)$ bezeichnen.

Definition 1.5.3. Ein Komplex $P^\bullet$ von R-Moduln heißt *strikt perfekt*, wenn alle P^n endlich erzeugt und projektiv sind und $P^n = 0$ für fast alle n gilt.

Ein Komplex $K^\bullet$ von R Moduln heißt *perfekt*, wenn es einen strikt perfekten Komplex $P^\bullet$ gibt, so dass $P^\bullet$ quasi-isomorph zu $K^\bullet$ ist, d.h. es gibt einen Homomorphismus von Komplexen $f : P^\bullet \to K^\bullet$, der auf der Kohomologie Isomorphismen induziert.

Wir nennen $K^\bullet$ *Torsionskomplex*, wenn der Komplex $\mathbf{L}\eta_* K^\bullet$ azyklisch ist, d.h. alle Kohomologie-Gruppen trivial sind.

Perfekte Komplexe lassen sich wie folgt charakterisieren:

Lemma 1.5.4. *Sei R ein noetherscher Ring. Ein Komplex $K^\bullet$ von R-Moduln ist genau dann perfekt, wenn folgende zwei Bedingungen erfüllt sind:*

(i) Alle Kohomologiemoduln sind endlich erzeugt über R.

(ii) Es gibt ein r, so dass für alle endlich erzeugten R-Moduln M und alle n mit $|n| > r$ gilt:

$$\mathrm{H}^n(K^\bullet \otimes_R^{\mathbb{L}} M) = 0.$$

Beweis. Siehe [FK88], Kapitel I, § 8. Beachte dabei, dass die zweite Bedingung für $M = R$ impliziert, dass $K^\bullet$ beidseitig beschränkt ist. Also existiert $K^\bullet \otimes_R^{\mathbb{L}} M$ für beliebige M. □

Wir folgen [KM76] und erweitern die Konstruktion der Determinante aus dem letzten Abschnitt auf strikt perfekte Komplexe:

Definition 1.5.5. Sei $P^\bullet$ ein strikt perfekter Komplex von R-Moduln. Die *Determinante* von $P^\bullet$ ist durch

$$\det_R P^\bullet \stackrel{def}{=} \bigotimes_{n=-\infty}^{\infty} (\det_R P^{2n} \otimes_R \det_R \check{P}^{2n+1})$$

gegeben.

Da $P^\bullet$ strikt perfekt ist, sind fast alle Faktoren des unendlichen Tensorprodukts trivial. Also ist $\det_R P^\bullet$ wieder ein invertierbarer R-Modul.

Für eine exakte Sequenz strikt perfekter Torsionskomplexe

$$0 \longrightarrow P_1^\bullet \xrightarrow{f} P_2^\bullet \xrightarrow{g} P_3^\bullet \longrightarrow 0$$

konstruieren wir wie folgt einen Isomorphismus

$$\mathbf{s}(f,g) : \det_R P_1^\bullet \otimes_R \det_R P_3^\bullet \longrightarrow \det_R P_2^\bullet$$

von Determinanten von Komplexen: Durch iterierte Anwendung des Isomorphismus $\mathbf{c}$ erhalten wir eine Abbildung

$$\det_R P_1^\bullet \otimes_R \det_R P_3^\bullet \longrightarrow \bigotimes_{n=-\infty}^{\infty} \det_R P_1^{2n} \otimes_R \det_R P_3^{2n} \otimes_R \det_R \check{P}_3^{2n+1} \otimes_R \det_R \check{P}_1^{2n+1}.$$

Die Zusammensetzung mit

$$\cdots \otimes \mathbf{s}(f^{2n}, g^{2n}) \otimes \mathbf{s}(g^{2n+1*}, f^{2n+1*}) \otimes \mathbf{s}(f^{2n+2}, g^{2n+2}) \otimes \cdots$$

liefert den Isomorphismus $\mathbf{s}(f,g)$.

Für Ringhomomorphismen $\phi : R \longrightarrow S$ erhalten wir wie in Lemma 1.4.5 einen Isomorphismus

$$\mathbf{b}(\phi) : \phi_*(\det_R P^\bullet) \longrightarrow \det_S \mathbf{L}\phi_*(P^\bullet).$$

Die Isomorphismen $\mathbf{c}$ und $\mathbf{r}$ werden wir auf dieser Ebene im Folgenden nicht benötigen.

1.6 Azyklische Komplexe

Sei S ein noetherscher und reduzierter Ring und $P^\bullet$ ein azyklischer strikt perfekter Komplex von S-Moduln (später wollen wir $S = Q(R)$ wählen). Ziel ist es, einen Isomorphismus $\lambda : \det_S P^\bullet \longrightarrow S$ zu konstruieren.

Lemma 1.6.1.

(i) *Sei $P^\bullet$ ein strikt perfekter, azyklischer Komplex von S-Moduln. Für jedes n erhalten wir kurze exakte Sequenzen endlich erzeugter projektiver S-Moduln*

$$0 \longrightarrow \operatorname{Ker} \partial^n \xrightarrow{i^n} P^n \xrightarrow{\partial^n} \operatorname{Im} \partial^n \longrightarrow 0$$

und

$$0 \longrightarrow (\operatorname{Im} \partial^n)\check{} \xrightarrow{\partial^{n*}} \check{P}^n \xrightarrow{i^{n*}} (\operatorname{Ker} \partial^n)\check{} \longrightarrow 0.$$

Dabei bezeichne ∂ das Differential von $P^\bullet$ und i die natürliche Inklusion.

(ii) Sei

$$0 \longrightarrow P_1^\bullet \xrightarrow{f} P_2^\bullet \xrightarrow{g} P_3^\bullet \longrightarrow 0$$

ein exaktes Tripel von strikt perfekten, azyklischen Komplexen von S-Moduln. Wir bezeichnen die Differentiale mit ∂_i, $i = 1, 2, 3$. Dann sind für alle n folgende 9-Diagramme exakt:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \operatorname{Ker}\partial_1^n \arrow[r] \arrow[d] & \operatorname{Ker}\partial_2^n \arrow[r] \arrow[d] & \operatorname{Ker}\partial_3^n \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & P_1^n \arrow[r] \arrow[d] & P_2^n \arrow[r] \arrow[d] & P_3^n \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \operatorname{Im}\partial_1^n \arrow[r] \arrow[d] & \operatorname{Im}\partial_2^n \arrow[r] \arrow[d] & \operatorname{Im}\partial_3^n \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Dasselbe gilt auch für die entsprechenden dualen 9-Diagramme.

Beweis. Zu (i): Da $P^\bullet$ nach Voraussetzung azyklisch ist, können wir den Komplex in kurze exakte Sequenzen endlich erzeugter Moduln zerlegen. Es bleibt zu zeigen, dass $\operatorname{Im}\partial^n = \operatorname{Ker}\partial^{n+1}$ für alle n projektiv ist. Für hinreichend große n gilt $\operatorname{Im}\partial^n = P^{n+1} = 0$, da strikt perfekte Komplexe nach Definition beschränkt sind. Insbesondere ist $\operatorname{Im}\partial^n$ projektiv und es existiert ein Schnitt $\operatorname{Im}\partial^n \longrightarrow P^n$. Also ist auch $\operatorname{Ker}\partial^n$ ein direkter Summand von P^n und deshalb ebenfalls projektiv. Per Induktion folgt die Exaktheit der ersten Sequenz in (i) für alle n. Nach Lemma 1.1.4 ist damit auch die zweite Sequenz exakt.

Zu (ii): Dies folgt wieder per Induktion: Für genügend großes n ist die Sequenz der Bilder wegen $P_i^{n+1} = \operatorname{Im}\partial_i^n = 0$ nach Voraussetzung exakt. Nach dem 9-Lemma folgt dies dann auch für die Sequenz der Kerne, die gleichzeitig die Sequenz der Bilder im Diagramm für $n-1$ ist. □

Definition 1.6.2. Wir definieren $\lambda = \lambda_{P^\bullet} : \det_S P^\bullet \longrightarrow S$ als die Zusammensetzung der folgenden Isomorphismen

$$\begin{tikzcd}
\cdots \det_S P^{2n} \otimes_S \det_S \check{P}^{2n+1} \otimes_S \det_S P^{2n+2} \cdots \arrow[d, "\cdots \mathbf{s}^{-1}(i^{2n},\partial^{2n}) \otimes \mathbf{s}^{-1}(\partial^{2n+1*}, i^{2n+1*}) \otimes \mathbf{s}^{-1}(i^{2n+2},\partial^{2n+2}) \cdots"'] \\
\cdots \det_S \operatorname{Im}\partial^{2n}) \otimes_S (\det_S(\operatorname{Im}\partial^{2n+1}\check{)} \otimes_S \det_S(\operatorname{Ker}\partial^{2n+1}\check{)}) \otimes_S (\det_S \operatorname{Ker}\partial^{2n+2} \cdots \arrow[d, "\cdots id \otimes \mathbf{c} \otimes id \cdots"'] \\
\cdots (\det_S \operatorname{Im}\partial^{2n} \otimes_S \det_S(\operatorname{Ker}\partial^{2n+1}\check{)}) \otimes_S (\det_S(\operatorname{Im}\partial^{2n+1}\check{)} \otimes_S \det_S \operatorname{Ker}\partial^{2n+2}) \cdots \arrow[d, "\cdots \mathbf{r} \otimes \mathbf{r} \circ \mathbf{c} \cdots"'] \\
S
\end{tikzcd}$$

(beachte dabei, dass $\operatorname{Ker} \partial^{n+1} = \operatorname{Im} \partial^n$).

Lemma 1.6.3.

(i) Sei $\phi : S \longrightarrow T$ ein Ring-Homomorphismus und $P^\bullet$ ein azyklischer strikt perfekter Komplex über S. Dann ist $\mathbf{L}\phi_* P^\bullet$ ein azyklischer und strikt perfekter Komplex über T und folgendes Diagramm kommutiert:

$$\begin{tikzcd}
\mathbf{L}\phi_*(\det_S P^\bullet) \arrow[r, "\mathbf{b}(\phi)"] \arrow[d, "\phi_*(\lambda)"'] & \det_T(\mathbf{L}\phi_* P^\bullet) \arrow[d, "\lambda"] \\
\phi_*(S) \arrow[r, "\cong"] & T
\end{tikzcd}$$

(ii) Sei

$$0 \longrightarrow P_1^\bullet \xrightarrow{f} P_2^\bullet \xrightarrow{g} P_3^\bullet \longrightarrow 0$$

ein exaktes Tripel von strikt perfekten, azyklischen Komplexen von S-Moduln. Dann kommutiert folgendes Diagramm:

$$\begin{tikzcd}
\det_S(P_1^\bullet) \otimes_S \det_S(P_3^\bullet) \arrow[r, "\mathbf{s}(f,g)"] \arrow[d, "\lambda_{P_1^\bullet} \otimes \lambda_{P_3^\bullet}"'] & \det_S(P_2^\bullet) \arrow[d, "\lambda_{P_2^\bullet}"] \\
S \otimes_S S \arrow[r, "a \otimes b \mapsto ab"] & S
\end{tikzcd}$$

Zum Beweis. Zu (i): Der Funktor ϕ_* bildet endlich erzeugte projektive S-Moduln in endlich erzeugte projektive T-Moduln ab und ist exakt auf strikt perfekten Komplexen. Die Kommutativität folgt nach Lemma 1.4.6.(iii).

Zu (ii): Dies folgt leicht mit Lemma 1.6.1.(ii) und Lemma 1.4.6.(i), zumindest bis auf das Vorzeichen. Eine genauere Überprüfung zeigt, dass auch das Vorzeichen übereinstimmt. □

1.7 Konstruktion charakteristischer Ideale

Wir werden charakteristische Ideale zunächst nur für strikt perfekte Torsionskomplexe definieren. Später zeigen wir, dass diese Definition allein von der Isomorphieklasse des Komplexes in der abgeleiteten Kategorie abhängt, so dass wir sie auch auf perfekte Torsionskomplexe ausdehnen können.

Lemma 1.7.1. *Sei $P^\bullet$ ein strikt perfekter Torsionskomplex von R-Moduln und bezeichne $\eta : R \longrightarrow Q(R)$ die natürliche Inklusion. Dann ist das Bild D von $\det_R P^\bullet$ unter der Zusammensetzung der Abbildungen*

$$\det_R(P^\bullet) \longrightarrow \eta_* \det_R(P^\bullet) \xrightarrow{\mathbf{b}(\eta)} \det_{Q(R)}(\mathbf{L}\eta_* P^\bullet) \xrightarrow{\lambda} Q(R)$$

ein Cartier-Divisor von R.

Beweis. $\det_R P^\bullet$ ist projektiv, also flach. Jeder Nichtnullteiler von R ist somit ein Nichtnullteiler auf $\det_R P^\bullet$ (siehe [Eis99], Cor. 6.3.). $\eta_*(\det_R(P^\bullet))$ ist aber die Lokalisierung von $\det_R P^\bullet$ an allen Nichtnullteilern von R. Also ist die Abbildung $\det_R(P^\bullet) \longrightarrow \eta_* \det_R(P^\bullet)$ injektiv; $\mathbf{b}(\eta)$ und λ aber sind Isomorphismen. Da $\det_R(P^\bullet)$ ein endlich erzeugter, invertierbarer R-Modul ist, ist D ebenfalls endlich erzeugt und invertierbar. Außerdem gilt $\eta_*(D) = Q(R)$. Nach Definition 1.2.1 ist D also ein Cartier-Divisor. □

Definition 1.7.2. Wir nennen das Inverse des Cartier-Divisors aus Lemma 1.7.1,

$$\operatorname{char} P^\bullet \overset{def}{=} D^{-1} \in \mathfrak{C}(R),$$

das *charakteristische Ideal* von $P^\bullet$.

Bemerkung 1.7.3. In obiger Definition wählen wir D^{-1} statt D, um Übereinstimmung mit dem Begriff des charakteristischen Polynoms für reguläre lokale Ringe der Dimension 2 (siehe Abschnitt 1.9) zu erhalten.

Lemma 1.7.4. *Betrachte eine kurze exakte Sequenz strikt perfekter Torsionskomplexe von R-Moduln:*

$$0 \longrightarrow P_1^\bullet \xrightarrow{f} P_2^\bullet \xrightarrow{g} P_3^\bullet \longrightarrow 0.$$

Dann gilt

$$\operatorname{char}(P_2^\bullet) = \operatorname{char}(P_1^\bullet)\operatorname{char}(P_3^\bullet)$$

in $\mathfrak{C}(R)$.

Beweis. Nach Lemma 1.4.6.(iii) und Lemma 1.6.3.(ii) kommutiert das Diagramm.

$$\begin{tikzcd}
\det_R P_1^\bullet \otimes_R \det_R P_3^\bullet \arrow[r, "\mathbf{s}(f,g)"] \arrow[d] & \det_R P_2^\bullet \arrow[d] \\
\det_{Q(R)}(\mathbf{L}\eta_* P_1^\bullet) \otimes_{Q(R)} \det_{Q(R)}(\mathbf{L}\eta_* P_3^\bullet) \arrow[r, "\mathbf{s}(f,g)"] \arrow[d, "\lambda_{P_1^\bullet} \otimes \lambda_{P_3^\bullet}"'] & \det_{Q(R)}(\mathbf{L}\eta_* P_2^\bullet) \arrow[d, "\lambda_{P_2^\bullet}"'] \\
Q(R) \otimes_{Q(R)} Q(R) \arrow[r, "a \otimes b \mapsto ab"] & Q(R)
\end{tikzcd}$$

Mit Lemma 1.2.4.(iii) folgt das Ergebnis. □

Wir beweisen nun einige Rechenregeln:

Lemma 1.7.5.

(i) Sei $P^\bullet$ ein azyklischer, strikt perfekter Torsionskomplex. Dann gilt

$$\operatorname{char} P^\bullet = (1) \in \mathfrak{C}(R).$$

(ii) Sei $P^\bullet$ ein strikt perfekter Torsionskomplex. Dann gilt

$$\operatorname{char} P^\bullet[1] = (\operatorname{char} P^\bullet)^{-1}.$$

(iii) Seien $P_1^\bullet$ und $P_2^\bullet$ zwei quasi-isomorphe, strikt perfekte Torsionskomplexe. Dann gilt

$$\operatorname{char} P_1^\bullet = \operatorname{char} P_2^\bullet.$$

Beweis. Punkt (i) folgt sofort aus Lemma 1.6.3. Wir beweisen nun (ii) und (iii). Sei $f : P_1^\bullet \longrightarrow P_2^\bullet$ ein Quasi-Isomorphismus. Dann erhalten wir eine exakte Sequenz

$$0 \longrightarrow P_2^\bullet \longrightarrow \mathit{Cone}^\bullet(f) \longrightarrow P_1^\bullet[1] \longrightarrow 0$$

(siehe [GM96], Lemma 3.3.3). $\mathit{Cone}^\bullet(f)$ ist offensichtlich ebenfalls strikt perfekt und, da f ein Quasi-Isomorphismus ist, bereits über R azyklisch. Nach (i) folgt

$$\operatorname{char} \mathit{Cone}^\bullet(f) = R.$$

Lemma 1.7.4 impliziert nun

$$\operatorname{char} P_2^\bullet = (\operatorname{char} P_1^\bullet[1])^{-1}.$$

Das gleiche Argument, angewandt auf die identische Abbildung von $P_1^\bullet$, zeigt

$$\operatorname{char} P_1^\bullet = (\operatorname{char} P_1^\bullet[1])^{-1}.$$

Damit sind beide Aussagen bewiesen. □

Es ist somit klar ersichtlich, dass $\operatorname{char} P^\bullet$ nur von der Isomorphie-Klasse von $P^\bullet$ in der abgeleiteten Kategorie der R-Moduln abhängt. Wir definieren:

Definition 1.7.6. Sei $K^\bullet$ ein perfekter Komplex mit einem strikt perfekten Repräsentanten $P^\bullet$. Dann setzen wir

$$\operatorname{char} K^\bullet \stackrel{def}{=} \operatorname{char} P^\bullet.$$

Lemma 1.7.4 lässt sich entsprechend auf ausgezeichnete Dreiecke (siehe [GM96], Definition 3.3.4) von perfekten Torsions-Moduln in der abgeleiteten Kategorie der R-Moduln ausweiten:

Satz 1.7.7. *Sei*

$$K^\bullet \xrightarrow{u} L^\bullet \xrightarrow{v} M^\bullet \xrightarrow{w} K^\bullet[1]$$

ein ausgezeichnetes Dreieck mit Morphismen u, v, w der abgeleiteten Kategorie. Sind zwei von den drei Komplexen perfekte Torsionskomplexe, so trifft dies auch für den dritten zu und es gilt:

$$\operatorname{char} L^\bullet = \operatorname{char} K^\bullet \operatorname{char} M^\bullet.$$

Beweis. Die langen exakten Kohomologiesequenzen zu den ausgezeichneten Dreiecken

$$K^\bullet \otimes_R^{\mathbb{L}} N \xrightarrow{u} L^\bullet \otimes_R^{\mathbb{L}} N \xrightarrow{v} M^\bullet \otimes_R^{\mathbb{L}} N \xrightarrow{w} K^\bullet \otimes_R^{\mathbb{L}} N[1]$$

für alle endlich erzeugten R-Moduln N zeigen nach Lemma 1.5.4, dass der dritte Komplex perfekt ist; für $N = Q(R)$ folgt entsprechend, dass er ein Torsionskomplex ist.

Da Quasi-Isomorphismen in der abgeleiteten Kategorie zu Isomorphismen werden, können wir o.B.d.A. annehmen, dass die Komplexe K, L, M strikt perfekt sind. Insbesondere sind sie nach oben beschränkte Komplexe projektiver Objekte. Morphismen in der abgeleiteten Kategorie, die von solchen Objekten ausgehen, können (eindeutig bis auf Homotopie) durch gewöhnliche Homomorphismen von Komplexen dargestellt werden (siehe [GM96], Kap. III, § 5). O.B.d.A. seien also u, v, w solche Abbildungen.

Folgendes Dreieck ist nach Definition ebenfalls ausgezeichnet:

$$K^\bullet \xrightarrow{u} L^\bullet \longrightarrow \mathit{Cone}^\bullet(u) \longrightarrow K^\bullet[1].$$

Aus den Axiomen für ausgezeichnete Dreiecke folgt die Existenz eines Quasi-Isomorphismus $\mathit{Cone}^\bullet(u) \cong M^\bullet$ (siehe [GM96], Kap. IV, § 1). Die exakte Sequenz

$$0 \longrightarrow L^\bullet \longrightarrow \mathit{Cone}^\bullet(u) \longrightarrow K^\bullet[1] \longrightarrow 0$$

des Kegels liefert zusammen mit Lemma 1.7.4 die Behauptung. □

Wir betrachten nun Koeffizientenerweiterungen:

Satz 1.7.8. *Sei $\phi : R \longrightarrow S$ fortsetzbar, $K^\bullet$ ein perfekter Torsionskomplex über R. Dann ist $\mathbf{L}\phi_* K^\bullet$ ein perfekter Torsionskomplex über S und es gilt:*

$$\operatorname{char} \mathbf{L}\phi_* K^\bullet = \mathfrak{C}(\phi)(\operatorname{char} K^\bullet).$$

Beweis. Ersetze $K^\bullet$ durch einen strikt perfekten Repräsentanten $P^\bullet$. Dann gilt

$$\mathbf{L}\phi_* K^\bullet = \mathbf{L}\phi_* P^\bullet,$$

also ist $\mathbf{L}\phi_* K^\bullet$ wieder perfekt. Da ϕ fortsetzbar ist, gilt ferner

$$(\mathbf{L}\eta_* \circ \mathbf{L}\phi_*)(K^\bullet) = (\mathbf{L}\phi_* \circ \mathbf{L}\eta_*)(K^\bullet) = \mathbf{L}\phi_*(0) = 0;$$

also ist $\mathbf{L}\phi_* K^\bullet$ ein Torsionskomplex über S. Die Aussage folgt nun leicht mit Lemma 1.6.3.(i). □

1.8 Ergänzungen

Wir betten die Kategorie der R-Moduln in die abgeleitete Kategorie ein, indem wir jeden R-Modul als einen im Grad 0 konzentrierten Komplex betrachten.

Lemma 1.8.1. *Sei $C^\bullet$ ein perfekter Torsionskomplex, so dass die Kohomologie-Moduln $\mathrm{H}^i\, C^\bullet$ selbst wieder perfekt sind (d.h. sie besitzen eine endliche projektive Auflösung). Dann gilt*

$$\operatorname{char} C^\bullet = \prod_{i \in \mathbb{Z}} (\operatorname{char} \mathrm{H}^i\, C^\bullet)^{(-1)^i}.$$

Beweis. Der Komplex ${}_{\tau \geq k}C^\bullet$ sei gegeben durch

$${}_{\tau\geq k}C^i \overset{\mathit{def}}{=} \begin{cases} 0 & \text{für } i < k, \\ \operatorname{Coker} \partial^{k-1} & \text{für } i = k, \\ C^i & \text{für } i > k. \end{cases}$$

Die exakte Sequenz von Komplexen

$$\begin{tikzcd}
\operatorname{Coker}\partial^{k-1} \arrow[r, "="] \arrow[d, "\partial^k"'] & \operatorname{Coker}\partial^{k-1} \arrow[r] \arrow[d, "\partial^k"'] & 0 \arrow[d] \\
\operatorname{Im}\partial^k \arrow[r, hook] \arrow[d] & C^{k+1} \arrow[r, two heads] \arrow[d, "\partial^{k+1}"'] & \operatorname{Coker}\partial^k \arrow[d, "\partial^{k+1}"'] \\
0 \arrow[r] \arrow[d] & C^{k+2} \arrow[r, "="] \arrow[d, "\partial^{k+2}"'] & C^{k+2} \arrow[d, "\partial^{k+2}"'] \\
\vdots & \vdots & \vdots
\end{tikzcd}$$

und der Quasi-Isomorphismus des linken Komplexes zu $(\mathrm{H}^k\, C^\bullet)[-k]$ liefert ein ausgezeichnetes Dreieck

$$(\mathrm{H}^k\, C^\bullet)[-k] \longrightarrow {}_{\tau\geq k}C^\bullet \longrightarrow {}_{\tau\geq k+1}C^\bullet \longrightarrow (\mathrm{H}^k\, C^\bullet)[-k+1].$$

Nach Voraussetzung ist $\mathrm{H}^k\, C^\bullet$ perfekt und ein Torsionsmodul. Ferner ist ${}_{\tau\geq k}C^\bullet$ für genügend kleine k quasi-isomorph zu $C^\bullet$. Induktives Anwenden von Satz 1.7.7 zeigt, dass ${}_{\tau\geq k}C^\bullet$ für jedes k ein perfekter Torsionskomplex ist und dass gilt:

$$\operatorname{char} C^\bullet = \operatorname{char}({}_{\tau\geq k+1}C^\bullet) \prod_{i=-\infty}^{k} (\operatorname{char} \mathrm{H}^i\, C^\bullet)^{(-1)^i}.$$

Da ${}_{\tau\geq k+1}C^\bullet$ für große k azyklisch ist, folgt die Behauptung. □

Lemma 1.8.2. *Sei a ein Nichtnullteiler von R. Dann ist $R/(a)$ ein perfekter Torsionskomplex und es gilt*

$$\operatorname{char}\big(R/(a)\big) = (a) \in \mathfrak{C}(R).$$

Beweis. $R/(a)$ ist quasi-isomorph zu dem Komplex in den Graden -1 und 0

$$P^\bullet : \quad Re \xrightarrow{\partial} Rf, \qquad \partial e = af$$

(mit freien Erzeugenden e und f). Nach Koeffizientenerweiterung mit $Q(R)$ ist a invertierbar, ∂ also ein Isomorphismus und der Komplex $\mathbf{L}\eta_*(P^\bullet)$ azyklisch. Wir wollen nun die in Abschnitt 1.6 konstruierte Abbildung λ ausführen. Wähle die Basis ∂e von $\operatorname{Im}\partial$. Der erste Schritt der Konstruktion von λ besteht aus der Anwendung von

$$\begin{aligned}&\mathbf{s}^{-1}(\partial^*, 0) \otimes \mathbf{s}^{-1}(id, 0) :\\ &\det\nolimits_{Q(R)} Q(R)\check{e} \otimes_{Q(R)} \det\nolimits_{Q(R)} Q(R)f \longrightarrow \det\nolimits_{Q(R)}(\operatorname{Im}\partial)\check{} \otimes_{Q(R)} \det\nolimits_{Q(R)} \operatorname{Im}\partial.\end{aligned}$$

Nach Definition (siehe Lemma 1.4.5.(iv)) gilt

$$\mathbf{s}(\partial^*, 0) \otimes \mathbf{s}(id, 0)((\partial e)\check{} \otimes \partial e) = \partial^*(\partial e)\check{} \otimes \partial e = \check{e} \otimes \partial e.$$

Die Abbildung

$$\mathbf{c} : (\operatorname{Im} \partial)\check{} \otimes 0 \longrightarrow 0 \otimes (\operatorname{Im} \partial)\check{}$$

im zweiten Schritt ist die Identität. Im letzten Schritt bildet der Isomorphismus

$$\mathbf{r} \circ \mathbf{c} : \det(\operatorname{Im} \partial)\check{} \otimes \det \operatorname{Im} \partial \longrightarrow Q(R)$$

den Erzeuger $(\partial e)\check{} \otimes \partial e$ auf -1 ab (siehe Lemma 1.4.5, Punkte (ii) und (iii)). Wir erhalten insgesamt

$$\lambda(\check{e} \otimes \partial e) = -1.$$

Das Bild von

$$\det_R P^\bullet = R(\check{e} \otimes f) = R(\check{e} \otimes a^{-1}\partial e) \subset Q(R)(\check{e} \otimes \partial e) = \det_{Q(R)}(\mathbf{L}\eta_* P^\bullet)$$

unter λ ist also $(a^{-1}) \in \mathfrak{C}(R)$, d.h. es gilt wie behauptet

$$\operatorname{char} R/(a) = (a).$$

□

1.9 Der Zusammenhang mit dem charakteristischen Polynom

Wir betrachten in diesem Abschnitt reguläre Ringe der Dimension 2.

Definition 1.9.1. Sei R ein regulärer lokaler Ring der Dimension 2. Wir nennen einen Homomorphismus $f : M \longrightarrow N$ von endlich erzeugten R-Moduln *Pseudo-Isomorphismus*, wenn für jedes Primideal $\mathfrak{p}$ der Kodimension 1

$$f_\mathfrak{p} : M_\mathfrak{p} \longrightarrow N_\mathfrak{p}$$

ein Isomorphismus ist.

Die endlich erzeugten R-Moduln lassen sich bis auf Pseudo-Isomorphie wie folgt klassifizieren:

Theorem 1.9.2 (Strukturtheorem). *Sei R ein regulärer lokaler Ring der Dimension 2 und sei M ein endlich erzeugter R-Modul. Dann existieren endlich viele Primideale $\mathfrak{p}_i$ der Kodimension 1 ($1 \leq i \leq k$), eine ganze Zahl $r \geq 0$, positive ganze Zahlen n_i und ein Pseudo-Isomorphismus*

$$f : M \longrightarrow R^r \oplus \bigoplus_{i=1}^{k} R/\mathfrak{p}_i^{n_i}.$$

Die Primideale $\mathfrak{p}_i$ und die Zahlen r, n_i sind durch M eindeutig bestimmt.

Beweis. Siehe [NSW00], Theorem 5.1.10. □

Nun sind alle regulären lokalen Ringe R faktoriell (siehe [Eis99], Theorem 19.19). Insbesondere ist R nullteilerfrei und jedes Primideal der Kodimension 1 ist ein Hauptideal. Das Produkt

$$\prod_{i=1}^{k} \mathfrak{p}_i^{n_i}$$

über die Primideale $\mathfrak{p}_i$ mit Vielfachheiten n_i aus Theorem 1.9.2 ist somit ebenfalls ein Hauptideal und der Erzeuger f dieses Ideals ist bis auf eine Einheit aus $R^\times$ eindeutig bestimmt. Dieser Erzeuger wird auch als *charakteristisches Polynom* von M bezeichnet. Es besteht nun folgender Zusammenhang zu den charakteristischen Idealen:

Lemma 1.9.3. *Sei R ein lokaler regulärer Ring der Dimension* 2 *und M ein endlich erzeugter Torsionsmodul. Dann gilt mit der Notation aus Theorem 1.9.2:*

$$\operatorname{char} M = \prod_{i=1}^{k} \mathfrak{p}_{\mathfrak{i}}{}^{n_i}.$$

Beweis. Jeder endlich erzeugte Modul über einem regulären lokalen Ring besitzt eine endliche Auflösung mit freien, endlich erzeugten Moduln (siehe [Eis99], Cor. 19.6.), d.h. er ist perfekt. Nach Satz 1.7.7 folgt aus dem Strukturtheorem und Lemma 1.8.2

$$\operatorname{char}(M)\operatorname{char}(\operatorname{Coker} f) = \operatorname{char}(\operatorname{Ker} f)\prod_{i=1}^{k} \mathfrak{p}_i^{n_i}.$$

Da f ein Pseudo-Isomorphismus ist, gilt

$$(\operatorname{Coker} f)_{\mathfrak{p}} = (\operatorname{Ker} f)_{\mathfrak{p}} = 0$$

für alle Primideale $\mathfrak{p}$ der Kodimension 1. Bezeichne

$$\imath_{\mathfrak{p}} : R \longrightarrow R_{\mathfrak{p}}$$

die entsprechende Lokalisierungsabbildung. Dann gilt nach Satz 1.7.8:

$$\mathfrak{C}(\imath_{\mathfrak{p}})(\operatorname{char}(\operatorname{Ker} f)) = \operatorname{char} \imath_{\mathfrak{p}*}(\operatorname{Ker} f) = \operatorname{char} 0 = R_{\mathfrak{p}}$$

für alle Primideale $\mathfrak{p}$ der Kodimension 1. Nach Satz 1.3.2 folgt $\operatorname{char}(\operatorname{Ker} f) = R$ (beachte, dass jeder reguläre Ring ein Cohen-Macauley-Ring ist, siehe [Eis99], § 18.2). Entsprechend folgt auch $\operatorname{char}(\operatorname{Coker} f) = R$, also die Behauptung. □

2 Zyklotomische $\mathbb{Z}_p$-Erweiterungen und pro-endliche Gruppenringe

In diesem Kapitel werden wir einige elementare Eigenschaften von zyklotomischen $\mathbb{Z}_p$-Erweiterungen K_∞/K und des pro-endlichen Gruppenrings $\mathbb{Z}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$ zusammenstellen. Eine ausführliche Betrachtung pro-endlicher Gruppenringe findet sich in [NSW00], Kapitel V, § 2. Die Theorie der $\mathbb{Z}_p$-Erweiterungen wird in [Was97] behandelt.

2.1 Abelsche Zahlkörper und Charaktere

Ein Körper K heißt *abelscher Zahlkörper*, wenn die Erweiterung $K/\mathbb{Q}$ des Körpers $\mathbb{Q}$ der rationalen Zahlen eine endliche Galois-Erweiterung mit abelscher Galoisgruppe $\mathrm{G}(K/\mathbb{Q})$ ist. Ist ζ_N eine primitive N-te Einheitswurzel, so ist der *Kreisteilungskörper* $\mathbb{Q}(\zeta_N)$ ein abelscher Zahlkörper. In der Tat können wir wie folgt einen Isomorphismus

$$rec : \mathrm{G}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/(N))^\times$$

festlegen: Ist l eine Primzahl, die N nicht teilt, so identifizieren wir die Restklasse von l modulo N mit dem *geometrischen Frobenius* $\mathcal{F}_l \in \mathrm{G}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, d.h. den durch

$$\mathcal{F}_l({\zeta_N}^l) = \zeta_N$$

eindeutig festgelegten Automorphismus von $\mathbb{Q}(\zeta_N)$.

Bemerkung 2.1.1. In vielen Standard-Werken der Iwasawa-Theorie, wie etwa [Was97], wird l mit dem arithmetischen Frobenius, also dem Inversen des geometrischen Frobenius identifiziert. Wir folgen mit unserer Normierung [HK03].

Wir werden die Notation des geometrischen Frobenius zweckentfremden, um mit

$$\mathcal{F}_{-1} \in \mathrm{G}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$$

die *komplexe Konjugation* zu bezeichnen. Unter der obigen Identifikation ist sie das Bild von $-1 \in (\mathbb{Z}/(N))^\times$ (vergleiche die Operation auf Einheitswurzeln).

Ist A eine abelsche Gruppe endlicher Ordnung, so bezeichnen wir mit $\widehat{A}$ die *Charaktergruppe von* A, d.h. die Gruppe der multiplikativen Homomorphismen von A nach $\mathbb{C}^\times$. Mit

$$\mathbb{1} : A \longrightarrow \mathbb{C}^\times, \qquad a \mapsto 1$$

bezeichnen wir den *trivialen Charakter*.

Ein *Dirichlet-Charakter* ist ein Charakter

$$\chi : (\mathbb{Z}/(N))^\times \longrightarrow \mathbb{C}^\times.$$

Der *Führer von* χ ist die kleinste Zahl f, so dass χ durch $(\mathbb{Z}/(f))^\times$ faktorisiert. Der Dirichlet-Charakter χ heißt *primitiv*, falls $f = N$. Je nachdem, ob $\chi(-1) = -1$ oder $\chi(-1) = 1$ bezeichnet man χ als *ungeraden* bzw. *geraden* Charakter.

Ist p eine fest gewählte, ungerade Primzahl, so heißt χ *von erster Art*, wenn $f = d$ oder $f = dp$ mit $(d,p) = 1$ und *von zweiter Art*, wenn $f = p^{n+1}$ oder $\chi = \mathbb{1}$ (d.h. $\mathbb{1}$ ist von erster und von zweiter Art). Gemäß der Zerlegung

$$(\mathbb{Z}/(dp^{n+1}))^\times = (\mathbb{Z}/(dp))^\times \times \mathbb{Z}/(p^n)$$

lassen sich alle Dirichlet-Charaktere eindeutig als Produkt $\theta\tau$ mit θ von erster Art und τ von zweiter Art (relativ zu p) darstellen.

Oft ist es bequem, χ durch

$$\chi(a) \overset{\text{def}}{=} \begin{cases} \chi(a + N\mathbb{Z}) & \text{für } (a,N) = 1, \\ 0 & \text{für } (a,N) > 1, \end{cases}$$

zu einer Funktion $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$ fortzusetzen.

Mittels *rec* können wir χ als ein Element von $\widehat{\mathrm{G}}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ auffassen. Der Fixkörper K_χ des Kerns von χ heißt der *zu* χ *assoziierte Körper*. Die Charaktergruppe von

$$\mathrm{G}(K_\chi/\mathbb{Q}) = \mathrm{G}(\mathbb{Q}(\zeta_N)/\mathbb{Q})/\operatorname{Ker}\chi$$

ist in natürlicher Weise zu der von χ erzeugten Untergruppe von $\widehat{\mathrm{G}}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ isomorph. Allgemeiner ist jeder Teilkörper eines Kreisteilungskörpers auf diese Art zu einer Gruppe von Dirichlet-Charakteren assoziiert (siehe [Was97], Kapitel 3).

Der Satz von Kronecker und Weber zeigt, dass man auf diese Weise bereits die Gesamtheit aller abelschen Zahlkörper beschrieben hat:

Theorem 2.1.2 (Kronecker, Weber). *Für jeden abelschen Zahlkörper K gibt es eine natürliche Zahl n, so dass $K \subset \mathbb{Q}(\zeta_n)$. Wählt man n minimal, so entspricht die Menge der in $K/\mathbb{Q}$ verzweigten Primzahlen genau den Primteilern von n.*

Beweis. Ein elementarer Beweis findet sich in [Was97], Kap. 14; für die letzte Aussage siehe [Was97], Theorem 1 im §3 des Anhangs. Das Theorem folgt anderseits auch leicht aus den allgemeineren Aussagen der Klassenkörpertheorie (siehe [Tat67], § 5.7). □

Die Isomorphismen *rec* sind kompatibel mit den natürlichen Projektionen

$$\mathrm{G}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \longrightarrow \mathrm{G}(\mathbb{Q}(\zeta_M)/\mathbb{Q})$$

für $M \mid N$. Durch Übergang zum projektiven Limes erhalten wir eine Beschreibung der Galoisgruppe der maximalen abelschen Erweiterung. Sei

$$\mathbb{Q}^{ab} \overset{\text{def}}{=} \bigcup_N \mathbb{Q}(\zeta_N).$$

Dann gilt

$$rec : \mathrm{G}(\mathbb{Q}^{ab}/\mathbb{Q}) \cong \prod_{l \text{ prim}} \mathbb{Z}_l^\times.$$

Die Dirichlet-Charaktere ermöglichen auch eine Beschreibung der wichtigsten arithmetischen Eigenschaften des assoziierten Körpers:

Theorem 2.1.3. *Sei X eine Gruppe von Dirichlet-Charakteren und K der zu X assoziierte Körper. Für eine Primzahl p sei*

$$Y \overset{\text{def}}{=} \{\chi \in X \mid \chi(p) \neq 0\}, \qquad Z \overset{\text{def}}{=} \{\chi \in X \mid \chi(p) = 1\}.$$

Dann entsprechen die Gruppenordnungen

$$\sharp(X/Y), \qquad \sharp(Y/Z), \qquad \sharp Z$$

dem Verzweigungsindex von p in K, dem Restklassenkörpergrad, bzw. der Anzahl der Stellen von K über p.

Beweis. siehe [Was97], Theorem 3.7. □

Mit dem Begriff *Stellen* bezeichnen wir Äquivalenzklassen von Bewertungen eines Zahlkörpers K: Zwei Bewertungen sind äquivalent, wenn sie dieselbe Topologie auf K induzieren. Die *endlichen Stellen* entsprechen den Primidealen des *Ganzheitsrings* $\mathcal{O}_K$ von K. Die *archimedischen Stellen* entsprechen den reellen Einbettungen $K \longrightarrow \mathbb{R}$ bzw. den Paaren von zueinander konjugierten komplexen Einbettungen $K \longrightarrow \mathbb{C}$ (siehe [Cas67]).

Wir werden häufig in der Situation sein, uns auf solche Erweiterungen einschränken zu müssen, die außerhalb einer vorgegebenen endlichen Menge S von Stellen von $\mathbb{Q}$ unverzweigt sind. S enthalte dabei stets die archimedische Stelle ∞ von $\mathbb{Q}$.

Mit

$$\mathrm{G}_S \overset{\text{def}}{=} \mathrm{G}_S(\mathbb{Q})$$

bezeichnen wir die Galois-Gruppe der maximalen außerhalb S unverzweigten Erweiterung von $\mathbb{Q}$. Der maximale abelsche Quotient G_S^{ab} von G_S beschreibt die maximale abelsche außerhalb S unverzweigte Erweiterung. Mit dem Theorem von Kronecker und Weber folgt wieder leicht

$$\mathrm{G}_S^{ab} = \prod_{l \in S \setminus \{\infty\}} \mathbb{Z}_l^\times.$$

Beachte, dass für $l \notin S$ der geometrische Frobenius $\mathcal{F}_l$ ein wohlbestimmtes Element von G_S^{ab} und allen Faktorgruppen von G_S^{ab} ist.

Sei $p \in S \setminus \{\infty\}$ eine fixierte endliche Stelle. Wir bezeichnen mit $\mathbb{Q}_n$ den eindeutig bestimmten Teilkörper von $\mathbb{Q}(\zeta_{p^{n+1}})$, dessen Galoisgruppe $\Gamma_n \overset{\text{def}}{=} \mathrm{G}(\mathbb{Q}_n/\mathbb{Q})$ zyklisch vom Rang p^n ist und setzen

$$\mathbb{Q}_\infty \overset{\text{def}}{=} \bigcup_n \mathbb{Q}_n, \qquad \Gamma \overset{\text{def}}{=} \varprojlim_n \Gamma_n \cong \mathbb{Z}_p.$$

Die Gruppen Γ und Γ_n werden wir stets als multiplikative Gruppen behandeln.

Bezeichne $\mathcal{O}_p$ den Bewertungsring eines Erweiterungskörpers vom endlichen Grad über $\mathbb{Q}_p$. Die stetigen Gruppenhomomorphismen aus $\mathrm{Hom}_{cts}(\mathrm{G}_S, \mathcal{O}_p^\times)$ werden wir *stetige Charaktere* nennen. Ist $K/\mathbb{Q}$ eine außerhalb S unverzweigte Galois-Erweiterung (nicht notwendig vom endlichen Grad), so fassen wir $\mathrm{Hom}_{cts}(\mathrm{G}(K/\mathbb{Q}), \mathcal{O}_p^\times)$ stets als Untergruppe von $\mathrm{Hom}_{cts}(\mathrm{G}_S, \mathcal{O}_p^\times)$ auf.

Die Einheitengruppe $\mathcal{O}_p^\times$ kann kanonisch in die endliche Torsionsgruppe μ der Einheitswurzeln in $\mathcal{O}_p$ und einen endlich erzeugten freien $\mathbb{Z}_p$-Modul $M \subset \mathcal{O}_p^\times$ zerlegt werden. Wir erhalten Isomorphismen

$$\begin{aligned}\mathrm{Hom}_{cts}(\mathrm{G}_S, \mathcal{O}_p^\times) &= \mathrm{Hom}_{cts}(\mathrm{G}_S, \mu) \times \mathrm{Hom}_{cts}(\mathrm{G}_S, M)\\ &= \mathrm{Hom}_{cts}(\mathrm{G}_S^{ab}, \mu) \times \mathrm{Hom}_{cts}(\Gamma, M).\end{aligned}$$

Dementsprechend besitzt jeder Charakter $\chi \in \mathrm{Hom}_{cts}(\mathrm{G}_S, \mathcal{O}_p^\times)$ eine eindeutige Darstellung

$$\chi = \theta\chi_\infty$$

mit einem Charakter $\theta \in \mathrm{Hom}_{cts}(\mathrm{G}_S, \mu)$ *von endlicher Ordnung*, und einem Charakter $\chi_\infty \in \mathrm{Hom}_{cts}(\mathrm{G}_S, M)$ *von unendlicher Ordnung*.

Die Gruppe

$$\mathrm{Hom}_{cts}(\mathrm{G}_S, \mu) \cong \prod_{l \in S\setminus\{\infty\}} \mathrm{Hom}_{cts}(\mathbb{Z}_l^\times, \mu)$$

hat offensichtlich endliche Ordnung. Durch die Wahl einer Einbettung $\mu \hookrightarrow \mathbb{C}^\times$ können wir $\mathrm{Hom}_{cts}(\mathrm{G}_S, \mu)$ mit einer Gruppe von Dirichlet-Charakteren identifizieren. Die zu Untergruppen von $\mathrm{Hom}_{cts}(\mathrm{G}_S, \mu)$ assoziierten Körper hängen dabei nicht von der Wahl dieser Einbettung ab (der Kern ändert sich nicht) und sind über $\mathbb{Q}$ außerhalb von S unverzweigt. Indem man $\mathcal{O}_p$ genügend groß wählt, kann man auf diese Art jede außerhalb von S unverzweigte endliche Erweiterung von $\mathbb{Q}$ gewinnen.

Der *zyklotomische Charakter* $\varepsilon_{cycl} \in \mathrm{Hom}_{cts}(\mathrm{G}_S, \mathbb{Z}_p^\times)$ wird im Folgenden eine besonders wichtige Rolle spielen. Er ist durch die Relation

$$\zeta_{p^n}^{\varepsilon_{cycl}(g)} = g(\zeta_{p^n})$$

für alle $g \in \mathrm{G}_S$ und alle natürlichen Zahlen n eindeutig festgelegt. Nach obiger Zerlegung gilt

$$\varepsilon_{cycl} = \varepsilon\varepsilon_\infty$$

mit $\varepsilon \in \mathrm{Hom}_{cts}(\mathrm{G}_S, \mu_{p-1})$ und $\varepsilon_\infty \in \mathrm{Hom}_{cts}(\mathrm{G}_S, 1 + p\mathbb{Z}_p)$. Der Charakter ε ist im Wesentlichen der Teichmüller-Charakter: Für $g \in \mathrm{G}_S$ ist $\varepsilon(g) \in \mu_{p-1}$ die eindeutig bestimmte Einheitswurzel, für die gilt:

$$\varepsilon(g) \equiv \varepsilon_{cycl}(g) \mod p.$$

Der Fixkörper des Kerns von ε_∞ ist $\mathbb{Q}_\infty$.

Bemerkung 2.1.4. Wir verweisen auf [Was97] für eine detailliertere Betrachtung der vorgestellten Begriffe.

2.2 Zyklotomische $\mathbb{Z}_p$-Erweiterungen

Wir geben nun die allgemeine Definition der zyklotomischen $\mathbb{Z}_p$-Erweiterung:

Definition 2.2.1. Sei K ein Zahlkörper und $K_\infty \overset{def}{=} K\mathbb{Q}_\infty$. Dann heißt K_∞/K *zyklotomische $\mathbb{Z}_p$-Erweiterung* von K.

Sei K_∞/K die zyklotomische $\mathbb{Z}_p$-Erweiterung eines abelschen Zahlkörpers K. Wir interessieren uns für die Galoisgruppe $\mathrm{G}(K_\infty/\mathbb{Q})$. Zunächst stellen wir fest, dass sich $\mathrm{G}(K_\infty/\mathbb{Q})$ wie folgt zerlegen lässt:

Lemma 2.2.2. *Sei K_∞/K die zyklotomische $\mathbb{Z}_p$-Erweiterung eines abelschen Zahlkörpers K. Dann ist $\Gamma = \mathrm{G}(\mathbb{Q}_\infty/\mathbb{Q})$ auf natürliche Weise ein direkter Summand von endlichem Index von $\mathrm{G}(K_\infty/\mathbb{Q})$.*

Beweis. Mit dem Theorem von Kronecker und Weber (siehe Theorem 2.1.2) sieht man leicht, dass wie folgt ein Schnitt

$$\mathrm{G}(\mathbb{Q}_\infty/\mathbb{Q}) \longrightarrow \mathrm{G}(\mathbb{Q}^{ab}/\mathbb{Q})$$

gegeben ist: Einem Element $\sigma \in \mathrm{G}(\mathbb{Q}_\infty/\mathbb{Q})$ wird der durch

$$\bar{\sigma}(\zeta_{p^n}) = \zeta_{p^n}^{\varepsilon_\infty(\sigma)} \qquad \bar{\sigma}(\zeta_{l^n}) = \zeta_{l^n} \qquad \text{für } l \neq p \text{ prim und alle } n > 0$$

eindeutig bestimmte Automorphismus $\bar{\sigma} \in \mathrm{G}(\mathbb{Q}^{ab}/\mathbb{Q})$ zugeordnet. Da $\mathbb{Q}_\infty$ in K_∞ enthalten ist, ist $\mathrm{G}(\mathbb{Q}_\infty/\mathbb{Q})$ auch ein direkter Summand der Faktorgruppe $\mathrm{G}(K_\infty/\mathbb{Q})$ von $\mathrm{G}(\mathbb{Q}^{ab}/\mathbb{Q})$.

Die Endlichkeit des Indexes von $\mathrm{G}(\mathbb{Q}_\infty/\mathbb{Q})$ in $\mathrm{G}(K_\infty/\mathbb{Q})$ ist äquivalent zu der Endlichkeit der Erweiterung $K_\infty/\mathbb{Q}_\infty$. Mit klassischer Galois-Theorie folgt:

$$\mathrm{G}(K_\infty/\mathbb{Q}_\infty) = \mathrm{G}(K/K \cap \mathbb{Q}_\infty).$$

Letztere Galoisgruppe ist aber sicher von endlicher Ordnung.

Es ist aus der Konstruktion offensichtlich, dass für zwei abelsche Zahlkörper $K \subset L$ die so definierten Zerlegungen mit der Projektionsabbildung

$$\mathrm{G}(L_\infty/\mathbb{Q}) \longrightarrow \mathrm{G}(K_\infty/\mathbb{Q})$$

verträglich sind, d.h. die Zerlegung ist funktoriell in K. □

Insbesondere können wir K stets durch den Fixkörper

$$K_0 \overset{\text{def}}{=} K_\infty^\Gamma$$

ersetzen, wobei wir Γ mit dem kanonischen Schnitt aus Lemma 2.2.2 in $\mathrm{G}(K_\infty/\mathbb{Q})$ einbetten. Es genügt also, von vornherein nur die zyklotomischen Erweiterungen K_∞/K_0 von solchen abelschen Zahlkörpern K_0 zu betrachten, für die zusätzlich $K_0 \cap \mathbb{Q}_\infty = \mathbb{Q}$ gilt. Aus dem Theorem von Kronecker und Weber folgt leicht, dass letztere Bedingung genau dann erfüllt ist, wenn K_0 ein Teilkörper von $\mathbb{Q}(\zeta_{Np})$ ist, wobei N eine zu p teilerfremde natürlichen Zahl bezeichnet. Entsprechend bezeichnen wir mit K_n den Körper

$$K_n \overset{\text{def}}{=} \mathbb{Q}_n K_0 = K_\infty^{\Gamma^{p^n}}.$$

Für die Galoisgruppe von $K_0/\mathbb{Q}$ schreiben wir abkürzend

$$\Delta \overset{\text{def}}{=} \mathrm{G}(K_0/\mathbb{Q}).$$

Nach Lemma 2.2.2 gilt

$$\mathrm{G}(K_\infty/\mathbb{Q}) = \Gamma \times \Delta, \qquad \mathrm{G}(K_n/\mathbb{Q}) = \Gamma_n \times \Delta.$$

Bemerkung 2.2.3. Im Allgemeinen gilt nicht $K_0 \subset K$. Für ein Gegenbeispiel siehe [Was97], Ex. 13.4. Erst für genügend große n erhalten wir $K_n = \mathbb{Q}_n K$.

Von folgendem Ergebnis über die Verzweigungen der zyklotomischen $\mathbb{Z}_p$-Erweiterung K_∞/K_0 werden wir später häufig Gebrauch machen.

Satz 2.2.4.

(i) *Alle über p liegenden Stellen von K_0 sind in K_∞/K_0 voll verzweigt. Alle anderen Stellen (einschließlich der archimedischen Stellen) sind in K_∞/K_0 unverzweigt.*

(ii) *Über jeder endlichen Stelle von K_0 liegen nur endlich viele Stellen von K_∞.*

Beweis. Zu (i): In [NSW00], Prop. 11.1.1, wird gezeigt, dass nicht nur die zyklotomische, sondern jede $\mathbb{Z}_p$-Erweiterung außerhalb der Stellen über p unverzweigt ist. Wir zeigen, dass K_∞/K_0 über p voll verzweigt. Die Idee dabei ist, alles auf den hinlänglich bekannten Fall $K_0 = \mathbb{Q}$ zu reduzieren.

Nach Konstruktion gilt $K_0 \subset \mathbb{Q}(\zeta_{Np})$ mit p und N teilerfremd. Aus Theorem 2.1.3 folgt leicht, dass der Verzweigungsindex von p in $\mathbb{Q}(\zeta_{Np})/\mathbb{Q}$ gleich $p-1$ ist. Also ist der Verzweigungsindex e_0 von p in $K_0/\mathbb{Q}$ ein Teiler von $p-1$. Zu einer gegebenen Stelle v_0 von K_0 über p wähle man nun eine Stelle v_n von K_n über v_0 und eine Stelle v_n' von $\mathbb{Q}_n$ zwischen v_n und p. Nach der Multiplikativität der Verzweigungsindices (siehe [Leu96], § 20.6) gilt dann

$$e(v_n|v_0)e(v_0|p) = e(v_n|v_n')e(v_n'|v_0).$$

Da $\mathbb{Q}_n/\mathbb{Q}$, wieder nach Theorem 2.1.3, über p voll verzweigt ist, gilt $e(v_n'|v_0) = p^n$. Nun ist $e_0 = e(v_0|p)$ aber teilerfremd zu p, das heißt, p^n teilt $e(v_n|v_0)$. Weil der Grad der Körpererweiterung K_n/K_0 gleich p^n ist, gilt $p^n = e(v_n|v_0)$, d.h. K_n/K_0 ist über v_0 voll verzweigt. Da dies für alle n und alle v_0 über p gilt, folgt die Behauptung.

Zu (ii): Sei v_0 zunächst eine Stelle von K_0 über p. Dann ist für jedes n die Erweiterung K_n/K_0 in v_0 voll verzweigt, d.h. es gibt genau eine Stelle von K_n über v_0. Da n beliebig war, gilt dies auch für K_∞.

Wir betrachten nun die unverzweigten Stellen. Da $K_\infty/\mathbb{Q}_\infty$ eine endliche Galois-Erweiterung ist, dürfen wir o.B.d.A. K_∞/K_0 durch $\mathbb{Q}_\infty/\mathbb{Q}$ ersetzen (siehe [Was97], Anhang 2). Durch Adjunktion der p-ten Einheitswurzel erhalten wir

$$\mathbb{Q}(\zeta_{p^\infty}) = \mathbb{Q}_\infty(\zeta_p) = \bigcup_n \mathbb{Q}(\zeta_{p^{n+1}}).$$

Es reicht zu zeigen, für jede Primzahl $l \neq p$ ist die Anzahl d_n der Stellen von $\mathbb{Q}(\zeta_{p^{n+1}})$ über l für große n konstant. Dies ist der Fall, weil der lokale Körper $\mathbb{Q}_l$ nur endlich viele Einheitswurzeln enthält. Etwas formaler kann man wie folgt argumentieren:

Sei f_n der Grad der Restklassenkörper-Erweiterung von $\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}$ an der Stelle l. Die Erweiterung $\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}$ hat den Grad $(p-1)p^n$ und l ist unverzweigt. Nach Theorem 2.1.3 gilt darum

$$d_n f_n = (p-1)p^n.$$

Andererseits ist nach dem zyklotomischen Reziprozitätsgesetz (siehe [Was97], Theorem 2.13) f_n die kleinste positive ganze Zahl mit

$$l^{f_n} \equiv 1 \mod p^{n+1}.$$

Sei $f_n = k_n f_0 + r_n$ mit $0 \leq r_n < f_0$. Dann gilt

$$l^{r_n} \equiv l^{k_n f_0 + r_n} \equiv l^{f_n} \equiv 1 \mod p.$$

Da f_0 die kleinste positive ganze Zahl mit dieser Eigenschaft ist, folgt $r_n = 0$. Wir schreiben

$$l^{f_0} = 1 + p^m a$$

mit a teilerfremd zu p. Dann gilt für $n \geq m$

$$l^{f_n} = l^{k_n f_0} \equiv 1 + p^m k_n a \mod p^{m+1}.$$

Infolgedessen gilt $k_n = p^{n-m+1}$ (wieder wegen der Minimalität) und somit

$$d_n = \frac{p^{m-1}(p-1)}{f_0}.$$

Insbesondere ist d_n für $n \geq m$ konstant. □

2.3 Der pro-endliche Gruppenring von $\mathrm{G}(K_\infty/\mathbb{Q})$

Sei $\mathcal{O}_p$ der Bewertungsring eines Erweiterungskörpers endlichen Grades von $\mathbb{Q}_p$. Betrachte den *Gruppenring* $\mathcal{O}_p[\mathrm{G}(K_n/\mathbb{Q})]$, d.h. die von $\mathrm{G}(K_n/\mathbb{Q})$ frei erzeugte $\mathcal{O}_p$-Algebra. Wenn $m \geq n \geq 0$, dann induziert die Projektion

$$\pi_{m,n} : \mathrm{G}(K_m/\mathbb{Q}) \longrightarrow \mathrm{G}(K_n/\mathbb{Q})$$

den natürlichen Homomorphismus

$$\mathcal{O}_p[\mathrm{G}(K_m/\mathbb{Q})] \longrightarrow \mathcal{O}_p[\mathrm{G}(K_n/\mathbb{Q})], \qquad \sum_{\sigma \in \mathrm{G}(K_m/\mathbb{Q})} a_\sigma \sigma \mapsto \sum_{\sigma \in \mathrm{G}(K_m/\mathbb{Q})} a_\sigma \pi_{m,n}(\sigma)$$

($a_\sigma \in \mathcal{O}_p$). Durch Übergang zum projektiven Limes des so definierten inversen Systems erhalten wir den pro-endlichen Gruppenring von $\mathrm{G}(K_\infty/\mathbb{Q})$:

Definition 2.3.1. Der *pro-endliche Gruppenring* von $\mathrm{G}(K_\infty/\mathbb{Q})$ mit Koeffizienten aus $\mathcal{O}_p$ ist durch

$$\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!] = \varprojlim_n \mathcal{O}_p[\mathrm{G}(K_n/\mathbb{Q})]$$

gegeben.

Für $\Gamma = \mathrm{G}(\mathbb{Q}_\infty/\mathbb{Q})$ ist

$$\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$$

die in der klassischen Formulierung der Hauptvermutung betrachtete *Iwasawa-Algebra*. Durch die Wahl eines Erzeugers von Γ kann man Λ mit einem Potenzreihenring identifizieren. Allgemeiner gilt dies auch für $\mathcal{O}_p[\![\Gamma]\!]$:

Sei π ein Erzeuger des maximalen Ideals von $\mathcal{O}_p$. Wähle ferner einen *topologischen Erzeuger* γ von $\Gamma \cong \mathbb{Z}_p$; d.h. die zyklische Untergruppe, die von γ erzeugt wird, ist dicht in der pro-endlichen Topologie von Γ. Mit $\mathcal{O}_p[\![T]\!]$ bezeichnen wir den Potenzreihenring in einer Unbestimmten T über $\mathcal{O}_p$.

Definition 2.3.2. Ein Polynom $P(T) \in \mathcal{O}_p[T] \subset \mathcal{O}_p[\![T]\!]$ heißt *ausgezeichnet*, wenn es die Form

$$P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$$

mit $n > 0$ und $a_i \in (\pi)$, $0 \leq i < n$ hat.

Satz 2.3.3.

(i) Es gilt

$$\mathcal{O}_p[\![T]\!] = \varprojlim_n \mathcal{O}_p[T]/((T+1)^{p^n} - 1)$$

und durch die Zuordnung $T \mapsto \gamma - 1$ wird ein Isomorphismus

$$\mathcal{O}_p[\![T]\!] \longrightarrow \mathcal{O}_p[\![\Gamma]\!]$$

induziert. Insbesondere ist $\mathcal{O}_p[\![\Gamma]\!]$ noethersch.

(ii) $\mathcal{O}_p[\![\Gamma]\!]$ ist ein regulärer lokaler Ring der Dimension 2. Die Primideale von $\mathcal{O}_p[\![\Gamma]\!]$ sind 0, $(\pi, \gamma - 1)$, (π) und $(P(\gamma - 1))$, für alle irreduziblen, ausgezeichneten Polynome $P(T) \in \mathcal{O}_p[T]$. Das einzige maximale Ideal ist $(\pi, \gamma - 1)$.

Beweis. Siehe [Was97], Theorem 7.1 und Satz 13.9. Die Regularität von $\mathcal{O}_p[\![\Gamma]\!]$ folgt, da die minimale Anzahl der Elemente, die das maximale Ideal $(\pi, \gamma - 1)$ erzeugen, mit der Dimension des Ringes übereinstimmt (siehe [Eis99], §16.3, S. 242). □

Bemerkung 2.3.4. Beachte, dass die Identifikation $\Lambda \cong \mathbb{Z}_p[\![T]\!]$ von der Wahl eines Erzeugers abhängt, d.h. nicht kanonisch ist. Unsere Philosophie im Folgenden ist es, deshalb weitgehend auf diese Identifikation zu verzichten und alle Ergebnisse in der Sprache der pro-endlichen Gruppenringe zu formulieren.

Die Ringe $\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$ sind endliche Erweiterungen von Λ:

Lemma 2.3.5. *Es gilt*

$$\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!] = \Lambda \otimes_{\mathbb{Z}_p} \mathcal{O}_p[\Delta].$$

Der Ring $\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$ ist somit noethersch und eine freie endliche Algebra über Λ. Insbesondere ist der natürliche Ringhomomorphismus

$$\Lambda \longrightarrow \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$$

injektiv.

Beweis. Das Problem besteht darin, zu zeigen, dass in der gegebenen Situation Tensorprodukt und projektiver Limes vertauschen. Im Abschnitt 2.4 werden wir diese Frage noch allgemeiner behandeln.

Die Projektionen

$$\Lambda \longrightarrow \mathbb{Z}_p[\Gamma_n]$$

induzieren Ringhomomorphismen

$$\phi_n : \Lambda \otimes_{\mathbb{Z}_p} \mathcal{O}_p[\Delta] \longrightarrow \mathbb{Z}_p[\Gamma_n] \otimes_{\mathbb{Z}_p} \mathcal{O}_p[\Delta] = \mathcal{O}_p[\Gamma_n \times \Delta],$$

die mit den $\pi_{m,n}$ kompatibel sind. Durch Übergang zum projektiven Limes erhält man einen Homomorphismus von Ringen

$$\phi : \Lambda \otimes_{\mathbb{Z}_p} \mathcal{O}_p[\Delta] \longrightarrow \mathcal{O}_p[\![\Gamma \times \Delta]\!].$$

Andererseits wird $\mathcal{O}_p[\Delta]$ als $\mathcal{O}_p$-Modul von den Elementen von Δ frei erzeugt und $\mathcal{O}_p$ ist seinerseits ein freier $\mathbb{Z}_p$-Modul vom Rang r. Durch die Wahl einer $\mathbb{Z}_p$-Basis von $\mathcal{O}_p[\Delta]$ lässt sich ϕ in Isomorphismen

$$\Lambda \otimes_{\mathbb{Z}_p} \mathcal{O}_p[\Delta] \cong \Lambda^{r+\sharp\Delta} \cong \varprojlim_n \mathbb{Z}_p[\Gamma_n]^{r+\sharp\Delta} \cong \varprojlim_n \mathbb{Z}_p[\Gamma_n] \otimes_{\mathbb{Z}_p} \mathcal{O}_p[\Delta]$$

von Λ-Moduln faktorisieren.

Die anderen Behauptungen ergeben sich daraus sofort. Beachte, dass endliche Erweiterungen von noetherschen Ringen wieder noethersch sind (siehe [Bou89b], Kap. III, § 2, Folgerung 3 zu Theorem 2). □

2.4 Kompakte $\mathbb{Z}_p$-Algebren

Die $\mathbb{Z}_p$-Algebren $\mathcal{O}_p/(p^n)[\mathrm{G}(K_n/\mathbb{Q})]$ sind von endlicher Kardinalität. Betrachtet man sie als topologische Ringe mit der diskreten (und gleichzeitig kompakten) Topologie (d.h. alle Teilmengen sind zugleich offen und abgeschlossen), so induziert der Isomorphismus

$$\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!] = \varprojlim_n \mathcal{O}_p/(p^n)[\mathrm{G}(K_n/\mathbb{Q})]$$

eine kompakte Topologie (d.h. eine Hausdorff-Topologie, die dem Überdeckungsaxiom genügt) auf dem pro-endlichen Gruppenring.

In diesem Abschnitt werden wir uns allgemein mit kompakten $\mathbb{Z}_p$-Algebren beschäftigen. Wir beschränken uns dabei auf den kommutativen Fall, obwohl es keine großen Probleme bereitet, die Ergebnisse auf nicht-kommutative Algebren auszudehnen. Die vorgestellten Ideen stammen größtenteils aus [NSW00], Kapitel 5. In [Bru66] wird allgemeiner der Fall pseudo-kompakter Algebren behandelt.

Wir stellen zunächst fest, dass jede kompakte $\mathbb{Z}_p$-Algebra A projektiver Limes von kompakten A-Algebren endlicher Kardinalität ist:

Lemma 2.4.1. *Sei A eine kompakte $\mathbb{Z}_p$-Algebra. Für jedes offene Ideal $\mathfrak{I}$ ist $A/\mathfrak{I}$ eine kompakte und diskrete A-Algebra von endlicher Kardinalität und es gilt*

$$A = \varprojlim A/\mathfrak{I},$$

wobei $\mathfrak{I}$ die offenen Ideale von A durchläuft.

Zum Beweis. Nach [NSW00], Satz 5.2.4 ist A als topologische Gruppe pro-endlich. (Das Pontryagin-Dual von A ist ein diskreter Torsionsmodul über $\mathbb{Z}_p$.) Also gilt

$$A = \varprojlim A/U$$

in der Kategorie der topologischen Gruppen, wobei U die offenen Untergruppen von A durchläuft. Diese sind automatisch von endlichem Index in A. Nun zeigt man wie im Beweis von [NSW00], Satz 1.1.3, dass jede offene Untergruppe U von A ein offenes Ideal $\mathfrak{I}$ enthält. (Man betrachte $\mathfrak{I} = \{u \in U \mid Au \subset U\}$.) □

Wir betrachten nun A-Moduln von endlicher Präsentation.

Definition 2.4.2. Ein A-Modul M heißt *von endlicher Präsentation*, wenn es eine exakte Sequenz

$$F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} M \longrightarrow 0$$

mit endlich erzeugten freien A-Moduln F_0 und F_1 gibt.

Bemerkung 2.4.3. Über noetherschen Ringen ist jeder endlich erzeugte Modul bereits von endlicher Präsentation. Insbesondere trifft dies auf den pro-endlichen Gruppenring $\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$ zu (siehe [Bou89b], Kap. I, § 2, Lemma 8).

Wir erhalten folgendes Ergebnis über das Vertauschen von projektivem Limes und Tensorprodukt:

Lemma 2.4.4. *Sei M ein A-Modul von endlicher Präsentation und N_i, $i \in I$ ein gerichtetes inverses System von A-Moduln endlicher Kardinalität. Dann gibt es einen natürlichen Isomorphismus*

$$M \otimes_A \varprojlim_{i\in I} N_i = \varprojlim_{i\in I}(M \otimes_A N_i).$$

Beweis. Sei M zunächst ein beliebiger A-Modul. Die Projektionen

$$\varprojlim_{i\in I} N_i \longrightarrow N_i$$

induzieren natürliche Homomorphismen

$$M \otimes_A \varprojlim_{i\in I} N_i \longrightarrow M \otimes_A N_i.$$

Der Übergang zum projektiven Limes liefert einen natürlichen Homomorphismus

$$\Phi : M \otimes_A \varprojlim_{i\in I} N_i \longrightarrow \varprojlim_{i\in I} M \otimes_A N_i, \qquad m \otimes (n_i)_{i\in I} \mapsto (m \otimes n_i)_{i\in I}.$$

Für den freien, endlich erzeugten Modul A^k faktorisiert Φ durch die Kette von Isomorphismen

$$A^k \otimes_A \varprojlim N_i \cong (\varprojlim N_i)^k \cong \varprojlim N_i^k \cong \varprojlim(A^k \otimes_A N_i),$$

ist also selbst ein Isomorphismus.

Betrachte nun eine freie endliche Präsentation

$$F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0.$$

Die Moduln $F_1 \otimes_A N_i$, $F_0 \otimes_A N_i$ sind offensichtlich von endlicher Kardinalität. Somit gilt dies auch für $M \otimes_A N_i$. Da das Tensorprodukt rechtsexakt ist und der projektive Limes auf endlichen Gruppen exakt ist, erhalten wir ein kommutatives Diagramm mit exakten Zeilen

$$\begin{tikzcd}
F_1 \otimes_A \varprojlim N_i \arrow[r] \arrow[d, "\cong"'] & F_0 \otimes_A \varprojlim N_i \arrow[r] \arrow[d, "\cong"'] & M \otimes_A \varprojlim N_i \arrow[r] \arrow[d, "\Phi"'] & 0 \\
\varprojlim(F_1 \otimes_A N_i) \arrow[r] & \varprojlim(F_0 \otimes_A N_i) \arrow[r] & \varprojlim(M \otimes_A N_i) \arrow[r] & 0
\end{tikzcd}$$

Nach dem 5-Lemma (siehe [Eis99], Ex. A3.11) ist Φ also auch für M ein Isomorphismus. □

Lemma 2.4.4 erlaubt es uns, Moduln endlicher Präsentation als kompakte Moduln aufzufassen.

Folgerung 2.4.5. *Jeder A-Modul M von endlicher Präsentation besitzt eine kanonische pro-endliche (und damit auch kompakte) Topologie. Jeder Homomorphismus zwischen Moduln endlicher Präsentation ist für diese Topologie stetig.*

Beweis. Nach Lemma 2.4.4 und Lemma 2.4.1 gilt

$$M = M \otimes_A A = M \otimes_A \varprojlim A/\mathfrak{I}A = \varprojlim M \otimes_A A/\mathfrak{I}A = \varprojlim M/\mathfrak{I}M,$$

wobei der projektive Limes über das inverse System der offenen Ideale $\mathfrak{I}$ von A gebildet wird. Da M von endlicher Präsentation ist, ist $M/\mathfrak{I}M$ von endlicher Kardinalität. Wir statten $M/\mathfrak{I}M$ mit der diskreten Topologie und M mit der davon erzeugten Limes-Topologie aus.

Sei $f : M \longrightarrow N$ ein Homomorphismus von A-Moduln endlicher Präsentation. Das kommutative Diagramm

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\Phi"'] & N \arrow[d, "\Phi"'] \\ \varprojlim M/\mathfrak{I}M \arrow[r, "\varprojlim f_{\mathfrak{I}}"] & \varprojlim N/\mathfrak{I}N \end{tikzcd}$$

zeigt, dass f stetig ist. □

Diese Topologie wird in Kapitel 5 eine wichtige Rolle spielen.

2.5 Die universelle Eigenschaft des pro-endlichen Gruppenrings

Sei B eine kompakte $\mathbb{Z}_p$-Algebra. Wir werden häufig in der Situation sein, einen gegebenen Homomorphismus $\mathrm{G}(K_\infty/\mathbb{Q}) \longrightarrow B^\times$ zu einem Ringhomomorphismus $\mathbb{Z}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!] \longrightarrow B$ fortsetzen zu wollen. In diesem Abschnitt werden wir das nötige Werkzeug dazu bereitstellen.

Wir beschränken uns dabei nicht auf $\mathbb{Z}_p$ und $\mathrm{G}(K_\infty/\mathbb{Q})$, sondern betrachten allgemeiner den pro-endlichen Gruppenring

$$A[\![G]\!] \overset{\mathit{def}}{=} \varprojlim_U A[G/U] = \varprojlim_{\mathfrak{I},U} (A/\mathfrak{I})[G/U]$$

für eine kompakte $\mathbb{Z}_p$-Algebra A und eine kommutative pro-endliche Gruppe G, wobei U und $\mathfrak{I}$ die offenen Untergruppen von G, respektive die offenen Ideale von A durchlaufen. $A[\![G]\!]$ ist damit selbst wieder eine kompakte $\mathbb{Z}_p$-Algebra. Wir beweisen zunächst folgendes vorbereitendes Lemma:

Lemma 2.5.1. *Sei A eine kompakte $\mathbb{Z}_p$-Algebra. Dann ist die Einheitengruppe $A^\times \subset A$ abgeschlossen in der Topologie von A und es gilt*

$$A^\times = \varprojlim (A/\mathfrak{I})^\times,$$

wobei $\mathfrak{I}$ die offenen Ideale von A durchläuft. Insbesondere ist $A^\times$ eine pro-endliche Gruppe.

Beweis. Die Elemente von $\varprojlim(A/\mathfrak{I})$ sind die Tupel $(a_{\mathfrak{I}})$ von Elementen $a_{\mathfrak{I}} \in A/\mathfrak{I}$, die unter den Übergangsabbildungen des inversen Systems kompatibel sind. Klar gilt damit:

$$A^\times \subset \varprojlim(A/\mathfrak{I})^\times \subset \varprojlim A/\mathfrak{I}.$$

Außerdem ist $\varprojlim(A/\mathfrak{I})^\times$ in A abgeschlossen, denn

$$\varprojlim(A/\mathfrak{I})^\times = \bigcap \phi_{\mathfrak{I}}^{-1}((A/\mathfrak{I})^\times)$$

ist der Schnitt über die Urbilder unter $\phi_{\mathfrak{I}} : A \longrightarrow A/\mathfrak{I}$ der offenen und abgeschlossenen Einheitengruppen $(A/\mathfrak{I})^\times$. Sei nun

$$u = (u_{\mathfrak{I}}) \in \varprojlim(A/\mathfrak{I})^\times.$$

Dann gibt es für jedes $\mathfrak{I}$ ein Element $v_{\mathfrak{I}} \in (A/\mathfrak{I})^\times$ mit $u_{\mathfrak{I}} v_{\mathfrak{I}} = 1$. Die Elemente $v_{\mathfrak{I}}$ sind nach der Eindeutigkeit des Inversen notwendig unter den Übergangsabbildungen des inversen Systems kompatibel, definieren also ein Inverses von u in A. Deshalb gilt $A^\times = \varprojlim(A/\mathfrak{I})^\times$. □

Weiterhin erhält man für jeden stetigen Homomorphismus $\phi : A \longrightarrow B$ von kompakten $\mathbb{Z}_p$-Algebren durch Einschränkung einen stetigen Homomorphismus $\phi^\times : A^\times \longrightarrow B^\times$ zwischen den Einheitengruppen. Das heißt, $A \mapsto A^\times$ ist ein Funktor von der Kategorie der kompakten $\mathbb{Z}_p$-Algebren in die Kategorie der pro-endlichen Gruppen.

Wir können nun die universelle Eigenschaft der Gruppenringe (siehe [Bou89a], Kap. II, § 2.6) in einer pro-endlichen Version formulieren.

Satz 2.5.2. *Sei A eine kompakte $\mathbb{Z}_p$-Algebra und G eine abelsche pro-endliche Gruppe. Dann besitzt $A[\![G]\!]$ nachstehende universelle Eigenschaft:*

(i) $A[\![G]\!]$ ist eine kompakte A-Algebra und es gibt einen stetigen Homomorphismus

$$G \xrightarrow{j} A[\![G]\!]^\times.$$

(ii) Für jede kompakte A-Algebra B und jeden stetigen Homomorphismus

$$G \xrightarrow{j'} B^\times$$

gibt es genau einen stetigen Homomorphismus von A-Algebren $\phi : A[\![G]\!] \longrightarrow B$, so dass folgendes Diagramm kommutiert:

$$\begin{tikzcd} G \arrow[r, "j"] \arrow[dr, "j'"'] & A[\![G]\!]^\times \arrow[d, "\phi^\times"] \\ & B^\times \end{tikzcd}$$

Beweis. Für jede offene Untergruppe U von G ist G/U endlich und trägt die diskrete Topologie, d.h. jede Teilmenge ist offen und abgeschlossen. Deshalb ist die natürliche

Abbildung $G/U \longrightarrow A[G/U]^\times$ automatisch stetig. Den Homomorphismus j erhält man durch Übergang zum projektiven Limes auf beiden Seiten.

Sei nun $\psi : A \longrightarrow B$ ein stetiger Homomorphismus kompakter $\mathbb{Z}_p$-Algebren und Υ die Menge der offenen Ideale von B. Nach Lemma 2.4.1 gilt

$$B = \varprojlim_{\mathfrak{I} \in \Upsilon} B/\mathfrak{I}$$

mit kompakten B-Algebren $B/\mathfrak{I}$ endlicher Kardinalität. Der Kern $U_{\mathfrak{I}}$ der Zusammensetzung der stetigen Homomorphismen

$$G \xrightarrow{j'} B^\times \longrightarrow (B/\mathfrak{I})^\times$$

ist offen, da 1 in $(B/\mathfrak{I})^\times$ offen ist. Wir erhalten einen Homomorphismus endlicher Gruppen

$$j'_{\mathfrak{I}} : G/U_{\mathfrak{I}} \longrightarrow (B/\mathfrak{I})^\times.$$

Die Konstruktion zeigt weiterhin, dass die Abbildungen $j'_{\mathfrak{I}}$ mit den Übergangs-Homomorphismen des projektiven Systems kommutieren.

Dem Gruppen-Homomorphismus $j'_{\mathfrak{I}}$ entspricht nach der universellen Eigenschaft abstrakter Gruppenringe (siehe [Bou89a] Kap II, §2.6) ein eindeutig bestimmter Homomorphismus

$$\phi_{\mathfrak{I}} : (A/\psi^{-1}(\mathfrak{I}))[G/U_{\mathfrak{I}}] \longrightarrow B/\mathfrak{I}$$

zwischen A-Algebren endlicher Kardinalität. Dieser Homomorphismus ist damit aber automatisch stetig.

Aus dieser universellen Eigenschaft folgt außerdem, dass auch die $\phi_{\mathfrak{I}}$ mit den Übergangs-Homomorphismen kommutieren. Wir können also zum projektiven Limes übergehen. Der gesuchte Homomorphismus ϕ ist dann durch die stetige Abbildung

$$A[\![G]\!] \longrightarrow \varprojlim_{\mathfrak{I}} (A/\psi^{-1}(\mathfrak{I}))[G/U_{\mathfrak{I}}] \xrightarrow{\varprojlim \phi_{\mathfrak{I}}} B$$

gegeben. Die Aussagen über Kommutativität und Eindeutigkeit folgen aus den entsprechenden Aussagen auf endlichem Level. □

2.6 Zerlegung nach Charakteren

Sei K_∞/K_0 die zyklotomische $\mathbb{Z}_p$-Erweiterung von K_0, mit $K_0 \cap \mathbb{Q}_\infty = \mathbb{Q}$ und

$$\Gamma \times \Delta = \mathrm{G}(\mathbb{Q}_\infty/\mathbb{Q}) \times \mathrm{G}(K_0/\mathbb{Q}) = \mathrm{G}(K_\infty/\mathbb{Q})$$

(siehe Abschnitt 2.2). Mit

$$p_\Gamma : \mathrm{G}(K_\infty/\mathbb{Q}) \longrightarrow \Gamma, \qquad p_\Delta : \mathrm{G}(K_\infty/\mathbb{Q}) \longrightarrow \Delta$$

bezeichnen wir die natürlichen Projektionen.

Wir wählen ferner einen Körper von endlichem Grad über $\mathbb{Q}_p$, dessen Bewertungsring $\mathcal{O}_p$ alle Werte der Charaktere aus $\widehat{\Delta}$ enthält und identifizieren $\widehat{\Delta}$ mit $\mathrm{Hom}(\Delta, \mathcal{O}_p^\times)$ (siehe Abschnitt 2.1). Die Gruppe $\mathrm{Hom}(\Delta, \mathcal{O}_p^\times)$ können wir wiederum mittels

$$\mathrm{Hom}(\Delta, \mathcal{O}_p^\times) \longrightarrow \mathrm{Hom}_{cts}(\mathrm{G}(K_\infty/\mathbb{Q}), \mathcal{O}_p^\times), \qquad \theta \mapsto \theta \circ p_\Delta$$

als eine Untergruppe von $\mathrm{Hom}_{cts}(\mathrm{G}(K_\infty/\mathbb{Q}), \mathcal{O}_p^\times)$ auffassen. Den Charakter $\theta \circ p_\Delta$ werden wir, unserer Konvention aus Abschnitt 2.1 folgend, ebenfalls mit θ bezeichnen.

Ziel dieses Abschnittes ist es, den pro-endlichen Gruppenring $\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$ unter den Charakteren von Δ zu zerlegen. Ist p kein Teiler der Gruppenordnung $\sharp\Delta$, so lässt sich jedes Element $w \in \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$ als eine Summe

$$\sum_{\theta \in \widehat{\Delta}} w_\theta e_\theta$$

darstellen. Dabei bezeichnet

$$e_\theta = \frac{1}{\sharp\Delta} \sum_{\sigma \in \Delta} \theta(\sigma)\sigma^{-1}$$

die *Idempotente* zu θ und die Elemente $w_\theta \in \mathcal{O}_p[\![\Gamma]\!]$ sind durch w und θ eindeutig bestimmt (siehe [Was97], § 6.3).

Teilt aber p die Gruppenordnung $\sharp\Delta$, so ist eine Zerlegung des Gruppenrings unter Charakteren im eigentlichen Sinne nicht möglich: In diesem Fall ist $\sharp\Delta$ in $\mathcal{O}_p[\![\Gamma \times \Delta]\!]$ nicht invertierbar und deshalb e_θ kein Element von $\mathcal{O}_p[\![\Gamma \times \Delta]\!]$.

Stattdessen arbeiten wir mit der von θ induzierten Abbildung:

Definition 2.6.1. Sei $\theta \in \widehat{\Delta}$. Dann nennen wir

$$p_\theta : \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!] \longrightarrow \mathcal{O}_p[\![\Gamma]\!], \qquad \sigma \mapsto \theta(\sigma)p_\Gamma(\sigma), \qquad \sigma \in \mathrm{G}(K_\infty/\mathbb{Q})$$

die *Projektion zu* θ.

Das folgende Resultat ist nur wenig schwächer als obige direkte Zerlegung:

Satz 2.6.2. *Sei*

$$\phi_{K_0} \overset{def}{=} \prod_{\theta \in \widehat{\Delta}} p_\theta : \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!] \longrightarrow \prod_{\theta \in \widehat{\Delta}} \mathcal{O}_p[\![\Gamma]\!].$$

Dann gilt:

(i) Der Ring-Homomorphismus ϕ_{K_0} ist fortsetzbar, d.h. er bildet Nichtnullteiler in Nichtnullteiler ab. Außerdem ist ϕ_{K_0} injektiv und endlich.

(ii) ϕ_{K_0} induziert einen Isomorphismus

$$\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!][(\sharp\Delta)^{-1}] \longrightarrow \prod_{\theta \in \widehat{\Delta}} \mathcal{O}_p[\![\Gamma]\!][(\sharp\Delta)^{-1}].$$

Insbesondere ist ϕ_{K_0} selbst schon ein Isomorphismus, wenn p die Ordnung von Δ nicht teilt.

(iii) Sei $L_0 \subset K_0$, $\psi : \mathrm{G}(K_\infty/\mathbb{Q}) \longrightarrow \mathrm{G}(L_\infty/\mathbb{Q})$ die natürliche Projektion und $\Delta_0 \overset{def}{=} \mathrm{G}(L_0/\mathbb{Q})$. Dann ist folgendes Diagramm kommutativ

$$\begin{tikzcd}
\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!] \arrow[r, "\phi_{K_0}"] \arrow[d, "\psi"'] & \prod_{\theta \in \widehat{\Delta}} \mathcal{O}_p[\![\Gamma]\!] \arrow[d, "\overline{\psi}"'] \\
\mathcal{O}_p[\![\mathrm{G}(L_\infty/\mathbb{Q})]\!] \arrow[r, "\phi_{L_0}"] & \prod_{\theta \in \widehat{\Delta}_0} \mathcal{O}_p[\![\Gamma]\!]
\end{tikzcd}$$

und ψ ist fortsetzbar. Dabei bezeichnet $\overline{\psi}$ die Projektion auf die Komponenten zu Charakteren $\theta \in \widehat{\Delta}_0 \subset \widehat{\Delta}$.

Beweis. Wir schreiben zur Abkürzung

$$\begin{aligned} \Omega &\stackrel{\text{def}}{=} \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!], \\ \overline{\Omega} &\stackrel{\text{def}}{=} \prod_{\theta \in \widehat{\Delta}} \mathcal{O}_p[\![\Gamma]\!], \\ A &\stackrel{\text{def}}{=} \mathcal{O}_p[\![\Gamma]\!][(\sharp\Delta)^{-1}]. \end{aligned}$$

Zunächst halten wir fest, dass $\sharp\Delta$ jeweils ein Nichtnullteiler in $\mathcal{O}_p[\![\Gamma]\!]$, Ω und $\overline{\Omega}$ ist. Dies ist leicht einsehbar, denn nach Lemma 2.3.5 ist Ω frei über Λ und dasselbe gilt offensichtlich auch für $\overline{\Omega}$ und $\mathcal{O}_p[\![\Gamma]\!]$. Λ ist aber regulär und lokal, also nullteilerfrei.

Die zweite Aussage folgt direkt durch Zerlegung nach Charakteren im Sinne von [Was97], § 6.3. Durch

$$\begin{aligned} p'_\theta &: \Omega[(\sharp\Delta)^{-1}] \longrightarrow A, & \frac{w}{(\sharp\Delta)^i} &\mapsto \frac{p_\theta(w)}{(\sharp\Delta)^i} \\ \phi'_{K_0} &: \Omega[(\sharp\Delta)^{-1}] \longrightarrow \overline{\Omega}[(\sharp\Delta)^{-1}], & \frac{w}{(\sharp\Delta)^i} &\mapsto \frac{\phi(w)}{(\sharp\Delta)^i} \end{aligned}$$

können p_θ und ϕ_{K_0} fortgesetzt werden. Nun sind

$$\begin{aligned} \Omega[(\sharp\Delta)^{-1}] &= A[\Delta] \\ \overline{\Omega}[(\sharp\Delta)^{-1}] &= \prod_{\theta \in \widehat{\Delta}} A \end{aligned}$$

beides freie A-Algebren vom gleichen Rang $\sharp\Delta$ und man sieht leicht, dass es sich bei ϕ'_{K_0} und p'_θ um A-Algebren-Homomorphismen handelt. Es reicht also zu zeigen, dass ϕ'_{K_0} surjektiv ist.

Für jedes $\theta \in \widehat{\Delta}$ ist die Idempotente e_θ ein Element von $A[\Delta]$ und es gilt

$$p'_\tau(e_\theta) = (\sharp\Delta)^{-1} \sum_{\sigma \in \Delta} \tau^{-1}\theta(\sigma) = \begin{cases} 1 & \text{falls } \tau = \theta, \\ 0 & \text{sonst.} \end{cases}$$

Also ist

$$\sum_{\theta \in \widehat{\Delta}} a_\theta e_\theta \in A[\Delta]$$

ein Urbild von

$$(a_\theta)_{\theta \in \widehat{\Delta}} \in \prod_{\theta \in \widehat{\Delta}} A$$

unter ϕ'_{K_0} und somit ϕ'_{K_0} ein Isomorphismus.

Die erste Aussage des Lemmas lässt sich wie folgt aus der zweiten ableiten. Offensichtlich ist $\overline{\Omega}$ als Modul über Ω endlich erzeugt, mit anderen Worten, ϕ_{K_0} ist ein endlicher Homomorphismus. Das Diagramm

$$\begin{tikzcd} \Omega \arrow[r, "\phi_{K_0}"] \arrow[d, hook, "\imath"'] & \overline{\Omega} \arrow[d, hook, "\jmath"] \\ \Omega[(\sharp\Delta)^{-1}] \arrow[r, "\phi'_{K_0}", "\cong"'] & \overline{\Omega}[(\sharp\Delta)^{-1}] \end{tikzcd}$$

kommutiert und die Lokalisierungsabbildungen $\imath$ und $\jmath$ sind injektiv, da an einem Nichtnullteiler lokalisiert wird. Ferner sind $\imath$ und $\jmath$ nach Lemma 1.2.7 fortsetzbar. Also ist auch ϕ_{K_0} injektiv und bildet ebenfalls Nichtnullteiler in Nichtnullteiler ab. (Beachte jedoch, dass ϕ_{K_0} im Allgemeinen nicht flach ist.)

Die dritte Aussage folgt durch Nachrechnen: Sei $\sigma \in \mathrm{G}(K_\infty/\mathbb{Q})$. Dann gilt:

$$(\phi_{L_0} \circ \psi)(\sigma) = \big((\theta \circ \psi)(\sigma)(p_\Gamma \circ \psi)(\sigma)\big)_{\theta \in \widehat{\Delta}_0} = \overline{\psi}\big(\big(\theta(\sigma)p_\Gamma(\sigma)\big)_{\theta \in \widehat{\Delta}}\big) = (\overline{\psi} \circ \phi_{K_0})(\sigma),$$

da die Einbettung $\widehat{\Delta}_0 \subset \widehat{\Delta}$ den Charakter θ auf $\theta \circ \psi$ abbildet und da $p_\Gamma = p_\Gamma \circ \psi$. Mit der universellen Eigenschaft (siehe Satz 2.5.2) folgt $\phi_{L_0} \circ \psi = \overline{\psi} \circ \phi_{K_0}$. Die Abbildung $\overline{\psi}$ ist trivialerweise fortsetzbar. Somit bildet auch $\overline{\psi} \circ \phi_{K_0} = \phi_{L_0} \circ \psi$ Nichtnullteiler in Nichtnullteiler ab. Da ϕ_{L_0} injektiv ist und somit Nullteiler in Nullteiler abbildet, muss ψ ebenfalls fortsetzbar sein. □

Wir können in gleicher Weise noch weiter nach den Charakteren von endlicher Ordnung auf Γ zerlegen. Sei $\mathcal{O}_{K_v}$ der Bewertungsring zu einem Körper K_v endlichen Grades über $\mathbb{Q}_p$, der $\mathcal{O}_p$ enthält und $\tau : \Gamma \longrightarrow \mathcal{O}_{K_v}$ ein Charakter endlicher Ordnung Nach Satz 2.5.2 erhalten wir eine Abbildung

$$\tau : \mathcal{O}_p[\![\Gamma]\!] \longrightarrow \mathcal{O}_{K_v}.$$

Um alle Charaktere endlicher Ordnung betrachten zu können, variieren wir über die Bewertungsringe $\mathcal{O}_{K_v}$ aller Körper K_v von endlichem Grad über $\mathbb{Q}_p$.

Lemma 2.6.3. *Ein Element $f \in \mathcal{O}_p[\![\Gamma]\!]$ ist eindeutig durch seine Werte $\tau(f) \in \mathcal{O}_{K_v}$ für alle Charaktere endlicher Ordnung $\tau : \Gamma \longrightarrow \mathcal{O}_{K_v}$ und alle Körper K_v von endlichem Grad über $\mathbb{Q}_p$ bestimmt.*

Beweis. Sei $\tau(f) = 0$ für alle Charaktere τ. Es reicht zu zeigen, dass dies bereits $f = 0$ impliziert. Nach Definition gibt es eine eindeutige Darstellung $f = (f_n)_{n \in \mathbb{N}}$ mit Elementen $f_n \in \mathcal{O}_p[\Gamma_n]$, die kompatibel unter den Übergangsabbildungen des inversen Systems sind. Nach unserer Voraussetzung haben wir $\tau(f_n) = \tau(f) = 0$ für alle Charaktere τ von Γ_n. Enthält K_v alle Werte der Charaktere in $\widehat{\Gamma}_n$, dann ist

$$\mathcal{O}_p[\Gamma_n] \longrightarrow \prod_{\tau \in \widehat{\Gamma}_n} \mathcal{O}_{K_v} \qquad a \mapsto (\tau(a))_{\tau \in \widehat{\Gamma}_n}$$

wieder injektiv (vgl. die Argumentation in Satz 2.6.2). Also gilt $f_n = 0$ für alle n und somit $f = 0$. □

Bemerkung 2.6.4. Sei U die multiplikativ abgeschlossene Menge der Nichtnullteiler in $\mathcal{O}_p[\![\Gamma]\!]$, die von keinem Charakter τ endlicher Ordnung in die Null abgebildet werden. Dann gilt die Aussage des Lemmas auch für die Elemente im Unterring $\mathcal{O}_p[\![\Gamma]\!][U^{-1}]$ des totalen Quotientenrings $Q(\mathcal{O}_p[\![\Gamma]\!])$: man betrachte jeweils die Fortsetzung von τ auf diesen Ring. τ ist jedoch nicht im Sinne von Definition 1.2.5 fortsetzbar.

2.7 Regularität und Cohen-Macauley-Eigenschaft

Ist p ein Teiler der Ordnung von Δ, so kann man leicht zeigen, dass $\mathcal{O}_p[\![\Gamma \times \Delta]\!]$ im Gegensatz zu Λ kein regulärer Ring ist. Wir zeigen nun, dass $\mathcal{O}_p[\![\Gamma \times \Delta]\!]$ zumindest noch ein Cohen-Macauley-Ring ist (vgl. Definition 1.3.3).

Satz 2.7.1. $\mathcal{O}_p[\![\Gamma \times \Delta]\!]$ *ist ein Cohen-Macauley-Ring der Dimension* 2.

Beweis. Sei γ ein topologischer Erzeuger von Γ. Dann ist

$$p, \gamma - 1 \in \Lambda$$

eine reguläre Folge für das maximale Ideal von Λ und $\dim \Lambda = 2$ (siehe Satz 2.3.3). Weiterhin ist $\mathcal{O}_p[\![\Gamma \times \Delta]\!]$ eine endliche, freie Λ-Algebra (siehe Lemma 2.3.5). Also sind die Homomorphismen

$$\mathcal{O}_p[\![\Gamma \times \Delta]\!] \xrightarrow{\cdot p} \mathcal{O}_p[\![\Gamma \times \Delta]\!]$$
$$\mathcal{O}_p[\![\Gamma \times \Delta]\!]/(p) \xrightarrow{\cdot(\gamma-1)} \mathcal{O}_p[\![\Gamma \times \Delta]\!]/(p)$$

injektiv. Aus dem Lying-Over-Lemma folgt, dass p und $\gamma - 1$ in jedem maximalen Ideal von $\mathcal{O}_p[\![\Gamma \times \Delta]\!]$ enthalten sind (siehe [Eis99], Cor. 4.17). Auf der anderen Seite erhalten endliche Erweiterungen die Dimension (siehe [Eis99], Prop. 9.2); also gilt $\dim \mathcal{O}_p[\![\Gamma \times \Delta]\!] = 2$.

Die Dimension eines Ringes ist gerade das Maximum der Kodimensionen aller maximalen Ideale. Andererseits ist die Länge einer regulären Folge in einem Primideal höchstens gleich der Kodimension des Primideals (siehe [Eis99], Prop. 18.2). Dies zeigt, dass jedes maximale Ideal $\mathfrak{m}$ von $\mathcal{O}_p[\![\Gamma \times \Delta]\!]$ eine reguläre Folge der Länge $\operatorname{codim} \mathfrak{m} = 2$ enthält. Nach Definition 1.3.3 ist $\mathcal{O}_p[\![\Gamma \times \Delta]\!]$ also ein Cohen-Macauley-Ring. □

2.8 Charaktere und Primideale

In diesem Abschnitt wollen wir uns mit dem Zusammenhang zwischen Primidealen und Charakteren beschäftigen. Wir setzen zur Abkürzung $\Omega \overset{def}{=} \mathcal{O}_p[\![\Gamma \times \Delta]\!]$. Nach Lemma 2.3.5 können wir $\mathcal{O}_p[\![\Gamma]\!]$ als einen Unterring von Ω auffassen.

Lemma 2.8.1. *Sei* $\mathfrak{P}$ *ein Primideal von* Ω *und* $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_p[\![\Gamma]\!]$. *Dann gibt es einen Charakter* $\chi \in \widehat{\Delta}$ *mit* $p_\chi(\mathfrak{P}) = \mathfrak{p}$. *Gilt* $\sharp\Delta \notin \mathfrak{P}$, *so induziert* p_χ *einen Isomorphismus*

$$p_{\chi_\mathfrak{p}} : \Omega_\mathfrak{P} \longrightarrow \Lambda_\mathfrak{p}.$$

Beweis. Wegen $p_\theta(a) = a$ für $a \in \mathcal{O}_p[\![\Gamma]\!]$ gilt $\mathfrak{p} \subset p_\theta(\mathfrak{P})$ für alle Charaktere $\theta \in \widehat{\Delta}$. Sei nun

$$\overline{\Omega} = \prod_{\theta \in \widehat{\Delta}} \mathcal{O}_p[\![\Gamma]\!], \qquad \phi = \prod_{\theta \in \widehat{\Delta}} p_\theta.$$

Nach Satz 2.6.2.(i) ist $\phi : \Omega \longrightarrow \overline{\Omega}$ injektiv. Dem Lying-Over-Lemma (siehe [Eis99], Prop. 4.15) zufolge gibt es ein Primideal $\overline{\mathfrak{P}}$ von $\overline{\Omega}$ mit $\phi^{-1}(\overline{\mathfrak{P}}) = \mathfrak{P}$. $\overline{\mathfrak{P}}$ hat die Gestalt

$$\overline{\mathfrak{P}} = \mathfrak{p}' \times \prod_{\substack{\theta \in \widehat{\Delta} \\ \theta \neq \chi}} \mathcal{O}_p[\![\Gamma]\!]$$

für einen Charakter $\chi \in \widehat{\Delta}$ und ein Primideal $\mathfrak{p}'$ von $\mathcal{O}_p[\![\Gamma]\!]$. Die Einschränkung von ϕ auf $\mathcal{O}_p[\![\Gamma]\!]$ ist die Diagonalabbildung

$$\begin{aligned} \mathcal{O}_p[\![\Gamma]\!] &\longrightarrow \prod_{\theta \in \widehat{\Delta}} \mathcal{O}_p[\![\Gamma]\!], \\ a &\mapsto (a, \dots, a). \end{aligned}$$

Wegen $\phi^{-1}(\overline{\mathfrak{P}}) \cap \mathcal{O}_p[\![\Gamma]\!] = \mathfrak{p}$ folgt $\mathfrak{p}' = \mathfrak{p}$ und somit $p_\chi(\mathfrak{P}) \subset \mathfrak{p}$. Damit ist der erste Teil des Lemmas bewiesen.

Ist $\sharp\Delta \notin \mathfrak{P}$, dann ist nach Satz 2.6.2.(ii)

$$\phi_{\overline{\mathfrak{P}}} : \Omega_{\mathfrak{P}} \longrightarrow \overline{\Omega}_{\overline{\mathfrak{P}}}$$

ein Isomorphismus. Andererseits induziert die Projektion auf die Komponente von $\overline{\Omega}$ zum Charakter χ einen Isomorphismus

$$\overline{\Omega}_{\overline{\mathfrak{P}}} \cong \mathcal{O}_p[\![\Gamma]\!]_{\mathfrak{p}}.$$

Die Zusammensetzung dieser Isomorphismen ist gerade $p_{\theta_{\mathfrak{p}}}$. Dies beweist den zweiten Teil des Lemmas. □

2.9 Cartier-Divisoren des pro-endlichen Gruppenrings

Die Gruppe der Cartier-Divisoren von $\Omega \stackrel{def}{=} \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$ hat eine relativ einfache Struktur:

Lemma 2.9.1. *Sei $\mathcal{O}_p$ der Bewertungsring eines beliebigen Erweiterungskörpers endlichen Grades von $\mathbb{Q}_p$ und $\Omega \stackrel{def}{=} \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$. Dann gilt:*

$$\mathfrak{C}(\Omega) = Q(\Omega)^\times / \Omega^\times.$$

Beweis. Ω ist eine endliche Erweiterung des lokalen Ringes Λ. Folglich besitzt Ω selbst nur endlich viele maximale Ideale, mit anderen Worten, Ω ist semilokal.

Endlich erzeugte projektive Moduln mit konstantem Rang über einem semilokalen Ring sind bereits frei (siehe [Bou89b], Ch. II, Sec. 2, Prop. 5). Insbesondere ist jeder invertierbare R-Untermodul I von $Q(\Omega)$ frei vom Rang 1.

Offensichtlich erzeugt jede Einheit von $Q(\Omega)$ einen freien Ω-Modul vom Rang 1. Sei umgekehrt $x \stackrel{def}{=} \frac{r}{s} \in Q(\Omega)$ ($r, s \in \Omega$, s Nichtnullteiler) ein Erzeuger von I. Da I ein freier Ω-Modul ist, ist auch r ein Nichtnullteiler und somit x eine Einheit in $Q(\Omega)$. Also ist die Abbildung

$$Q(\Omega)^\times \longrightarrow \mathfrak{C}(\Omega) \qquad x \mapsto x\Omega$$

surjektiv.

Sei nun $x\Omega = y\Omega$ mit $x, y \in Q(\Omega)^\times$. Dann gilt $x = uy$ und $y = vx = uvy$ mit $u, v \in \Omega$, also $y(uv - 1) = 0$. Da y eine Einheit von $Q(\Omega)$ ist, folgt $u, v \in \Omega^\times$ und somit

$$Q(\Omega)^\times / \Omega^\times = \mathfrak{C}(\Omega).$$

□

Bemerkung 2.9.2. Satz 2.7.1 zufolge ist Ω ein Cohen-Macauley-Ring. Nach Lemma 1.3.4 und Satz 1.3.2 wird also jeder Cartier-Divisor $D \in \mathfrak{C}(\Omega)$ durch seine Bilder in den Lokalisierungen $\mathfrak{C}(\Omega_\mathfrak{p})$ vollständig bestimmt (wobei $\mathfrak{p}$ die Primideale der Kodimension 1 durchläuft).

Folgendes Lemma zeigt, dass wir den Ring $\mathcal{O}_p$ beliebig vergrößern können. Insbesondere dürfen wir später stets annehmen, dass $\mathcal{O}_p$ die Werte aller Charaktere aus $\widehat{\Delta} = \widehat{\mathrm{G}}(K_0/\mathbb{Q})$ enthält.

Lemma 2.9.3. *Seien $\mathcal{O}_E$ und $\mathcal{O}_F$ die Bewertungsringe von Körpern $E \subset F$ von endlichem Grad über $\mathbb{Q}_p$. Dann gilt:*

$$\mathfrak{C}(\mathcal{O}_E[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]) \subset \mathfrak{C}(\mathcal{O}_F[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]).$$

Beweis. Setze zur Abkürzung

$$\Omega_E = \mathcal{O}_E[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!], \qquad \Omega_F = \mathcal{O}_F[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!].$$

Nach Lemma 2.3.5 gilt

$$\Omega_F = \Lambda \otimes_{\mathbb{Z}_p} \mathcal{O}_F[\Delta] = \Lambda \otimes_{\mathbb{Z}_p} \mathcal{O}_E[\Delta] \otimes_{\mathcal{O}_E} \mathcal{O}_F = \Omega_E \otimes_{\mathcal{O}_E} \mathcal{O}_F.$$

Nun ist $\Omega_E \otimes_{\mathcal{O}_E} \mathcal{O}_F$ eine freie endliche Ω_E-Algebra, d.h.

$$\Omega_E \longrightarrow \Omega_F$$

ist ein injektiver und nach Lemma 1.2.7 fortsetzbarer Ring-Homomorphismus, induziert also einen injektiven Homomorphismus der Quotientenringe. Wir erhalten nach Lemma 2.9.1 ein kommutatives Diagramm mit exakten Zeilen

$$\begin{tikzcd}
0 \arrow[r] & \Omega_E^\times \arrow[r] \arrow[d, hook] & Q(\Omega_E)^\times \arrow[r] \arrow[d, hook] & \mathfrak{C}(\Omega_E) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \Omega_F^\times \arrow[r] & Q(\Omega_F)^\times \arrow[r] & \mathfrak{C}(\Omega_F) \arrow[r] & 0
\end{tikzcd}$$

Für die Injektivität der rechten Abbildung reicht es dem Diagramm zufolge, folgende Inklusion zu beweisen:

$$Q(\Omega_E)^\times \cap \Omega_F^\times \subset \Omega_E^\times.$$

Für beliebige Ringe $R, S \subset T$ gilt $(R \cap S)^\times = R^\times \cap S^\times$. Infolgedessen können wir in obiger Inklusion die Einheitengruppen durch die Ringe ersetzen.

Indem wir bei Bedarf zu einer endlichen Erweiterung von F übergehen, dürfen wir o.B.d.A. annehmen, dass F/E eine Galois-Erweiterung ist. Sei $G \overset{def}{=} \mathrm{G}(F/E)$. Dann wird $\Omega_E \otimes_{\mathcal{O}_E} \mathcal{O}_F$ durch die Operation von G auf $\mathcal{O}_F$ zu einem G-Modul. Da G durch Automorphismen operiert, lässt sich die Operation auf den Quotientenring fortsetzen. Die Elemente von $Q(\Omega_E)$ sind unter dieser Operation invariant.

Somit genügt es, folgende Gleichheit zu zeigen:

$$(\Omega_E \otimes_{\mathcal{O}_E} \mathcal{O}_F)^G = \Omega_E.$$

Die Relation $\mathcal{O}_F^G = \mathcal{O}_E$ ist äquivalent zu der Exaktheit folgender Sequenz:

$$\begin{aligned} 0 \longrightarrow \mathcal{O}_E \longrightarrow \mathcal{O}_F \longrightarrow &\bigoplus_{g\in G} \mathcal{O}_F, \\ a \longmapsto &\ (ga-a)_{g\in G}. \end{aligned}$$

Nun ist Ω_E frei über $\mathcal{O}_E[\![\Gamma]\!]$ (vgl. Lemma 2.3.5) und $\mathcal{O}_E[\![\Gamma]\!] \cong \mathcal{O}_E[\![T]\!]$ flach über $\mathcal{O}_E$ (siehe [Eis99], Theorem 7.2). Also ist der Funktor $\cdot \otimes_{\mathcal{O}_E} \Omega_E$ exakt und wir erhalten eine exakte Sequenz:

$$\begin{aligned} 0 \longrightarrow \Omega_E \longrightarrow \Omega_F \longrightarrow &\bigoplus_{g\in G} \Omega_F, \\ a \longmapsto &\ (ga-a)_{g\in G} \end{aligned}$$

woraus wiederum $\Omega_F^G = \Omega_E$ folgt. Damit ist alles bewiesen. □

2.10 Die Operation der stetigen Charaktere

In diesem Abschnitt werden wir eine Operation der Gruppe $\mathrm{Hom}_{cts}(\mathrm{G}(K_\infty/\mathbb{Q}), \mathcal{O}_p^\times)$ der stetigen Charaktere auf dem pro-endlichen Gruppenring $\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$ definieren. Der Einfachheit halber nehmen wir an, dass $\mathcal{O}_p$ die Werte aller Charaktere aus $\widehat{\Delta}$ enthält.

Mit der kanonischen Zerlegung $\mathrm{G}(K_\infty/\mathbb{Q}) = \Gamma \times \Delta$ aus Lemma 2.2.2 erhalten wir

$$\mathrm{Hom}_{cts}(\mathrm{G}(K_\infty/\mathbb{Q}), \mathcal{O}_p^\times) = \mathrm{Hom}_{cts}(\Gamma, \mathcal{O}_p^\times) \times \widehat{\Delta}.$$

Die Untergruppe $\mathrm{Hom}_{cts}(\Gamma, \mathcal{O}_p^\times)$ besteht aus den Charakteren unendlicher Ordnung und den Dirichlet-Charakteren von zweiter Art in $\mathrm{Hom}_{cts}(\mathrm{G}(K_\infty/\mathbb{Q}), \mathcal{O}_p^\times)$ (siehe Abschnitt 2.1), während $\widehat{\Delta}$ nur Charaktere von endlicher Ordnung und erster Art enthält.

Definition 2.10.1. Sei $\chi \in \mathrm{Hom}_{cts}(\mathrm{G}(K_\infty/\mathbb{Q}), \mathcal{O}_p^\times)$. Dann nennen wir den im Sinne von Satz 2.5.2 eindeutig bestimmten Automorphismus

$$\begin{aligned} Tw_\chi : \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!] &\longrightarrow \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!] \\ \sigma &\mapsto \chi(\sigma)\sigma, \qquad \sigma \in \mathrm{G}(K_\infty/\mathbb{Q}) \end{aligned}$$

die *Verdrehung um* χ.

Bemerkung 2.10.2. Ist $L_0 \subset K_0$ und

$$\chi \in \mathrm{Hom}_{cts}(\mathrm{G}(L_\infty/\mathbb{Q}), \mathcal{O}_p^\times) \subset \mathrm{Hom}_{cts}(\mathrm{G}(K_\infty/\mathbb{Q}), \mathcal{O}_p^\times),$$

so vertauscht Tw_χ mit der Projektionsabbildung

$$\psi : \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!] \longrightarrow \mathcal{O}_p[\![\mathrm{G}(L_\infty/\mathbb{Q})]\!].$$

Dies ist eine einfache Konsequenz der universellen Eigenschaft (siehe Satz 2.5.2). Insbesondere gilt dies für alle Charaktere aus $\mathrm{Hom}_{cts}(\Gamma, \mathcal{O}_p^\times)$.

Ist $\chi \in \mathrm{Hom}_{cts}(\mathrm{G}(K_\infty/\mathbb{Q}), \mathcal{O}_p^\times) \setminus \mathrm{Hom}_{cts}(\mathrm{G}(L_\infty/\mathbb{Q}), \mathcal{O}_p^\times)$, so induziert Tw_χ keinen Automorphismus von $\mathcal{O}_p[\![\mathrm{G}(L_\infty/\mathbb{Q})]\!]$. Um eine Verdrehung um χ ausführen zu können, muss man deshalb von L_0 zu einem größeren Körper übergehen. Dieses technische Problem wird uns in den folgenden Kapiteln des Öfteren begegnen.

Setze

$$\Omega \overset{def}{=} \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!], \qquad \overline{\Omega} \overset{def}{=} \prod_{\theta\in\widehat{\Delta}} \mathcal{O}_p[\![\Gamma]\!].$$

Wir definieren wie folgt eine $\mathrm{Hom}_{cts}(\mathrm{G}(K_\infty/\mathbb{Q}), \mathcal{O}_p^\times)$-Operation auf Ω und $\overline{\Omega}$:

$$\begin{aligned} \mathrm{Hom}_{cts}(\mathrm{G}(K_\infty/\mathbb{Q}), \mathcal{O}_p^\times) \times \Omega &\longrightarrow \Omega, & (\chi, a) &\mapsto Tw_\chi(a), \\ \mathrm{Hom}_{cts}(\Gamma, \mathcal{O}_p^\times) \times \overline{\Omega} &\longrightarrow \overline{\Omega}, & \big(\tau, (a_\alpha)_{\alpha\in\widehat{\Delta}}\big) &\mapsto \big(Tw_\tau(a_\alpha)\big)_{\alpha\in\widehat{\Delta}}, \\ \widehat{\Delta} \times \overline{\Omega} &\longrightarrow \overline{\Omega}, & \big(\theta, (a_\alpha)_{\alpha\in\widehat{\Delta}}\big) &\mapsto (a_{\alpha\theta})_{\alpha\in\widehat{\Delta}}. \end{aligned}$$

Lemma 2.10.3. *Die Abbildung*

$$\phi : \Omega \longrightarrow \overline{\Omega}, \qquad a \mapsto \big(p_\alpha(a)\big)_{\alpha\in\widehat{\Delta}}$$

aus Satz 2.6.2 ist $\mathrm{Hom}_{cts}(\mathrm{G}(K_\infty/\mathbb{Q}), \mathcal{O}_p^\times)$*-äquivariant.*

Beweis. Sei $\theta \in \widehat{\Delta}$, $\tau \in \mathrm{Hom}_{cts}(\Gamma, \mathcal{O}_p^\times)$ und

$$a \overset{def}{=} \sum_{\sigma\in\Delta} a_\sigma \sigma \in \Omega, \quad a_\sigma \in \mathcal{O}_p[\![\Gamma]\!].$$

Dann gilt

$$Tw_{\theta\tau}(a) = \sum_{\sigma\in\Delta} Tw_\tau(a_\sigma)\theta(\sigma)\sigma$$

und somit

$$p_\alpha(Tw_{\theta\tau}(a)) = Tw_\tau\Big(\sum_{\sigma\in\Delta}(a_\sigma)\alpha\theta(\sigma)\Big) = Tw_\tau(p_{\alpha\theta}(a)),$$

womit alles gezeigt ist. □

Bemerkung 2.10.4. Wir erhalten auch eine Operation von $\mathrm{Hom}_{cts}(\mathrm{G}(K_\infty/\mathbb{Q}), \mathcal{O}_p^\times)$ auf $\mathfrak{C}(\Omega)$: Für jeden stetigen Charakter $\chi \in \mathrm{Hom}_{cts}(\mathrm{G}(K_\infty/\mathbb{Q}), \mathcal{O}_p^\times)$ ist der Automorphismus Tw_χ trivialerweise fortsetzbar, induziert also nach Lemma 1.2.6 einen Automorphismus

$$Tw_\chi : \mathfrak{C}(\Omega) \longrightarrow \mathfrak{C}(\Omega).$$

3 Stickelberger-Elemente und p-adische L-Funktionen

In [Was97], Kapitel 7, wird eine Konstruktion von K. Iwasawa beschrieben, die die Stickelberger-Elemente der Zwischenkörper einer zyklotomischen $\mathbb{Z}_p$-Erweiterung durch Zerlegung nach Charakteren mit p-adischen L-Funktionen in Verbindung bringt. Wir adaptieren diese Konstruktion leicht, um ein Element des pro-endlichen Gruppenrings $\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$ zu erhalten, welches wir als äquivariante L-Funktion bezeichnen. Zerlegt man dieses Element unter ungeraden Charakteren, so erhält man die den p-adischen L-Funktionen entsprechenden Iwasawa-Potenzreihen.

Das Material dieses Kapitels ist im Wesentlichen wohlbekannt. In [BG03], Sec. 5.2, und [Rub00] werden ähnliche Betrachtungen angestellt. Im Vergleich zu diesen Darstellungen wurden hier lediglich einige Details ergänzt.

3.1 Stickelberger-Elemente

Zunächst betrachten wir nur die Kreisteilungskörper $\mathbb{Q}(\zeta_N)$. Wir zweckentfremden die Notation des geometrischen Frobenius und bezeichnen mit $\mathcal{F}_a \in \mathrm{G}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, für $a \in \mathbb{Z}$, $(N, a) = 1$, das durch

$$\mathcal{F}_a(\zeta_N^a) = \zeta_N$$

eindeutig bestimmte Elemente der Galoisgruppe. Nach unserer Normierung des Isomorphismus *rec* ist $\mathit{rec}(\mathcal{F}_a)$ die Restklasse von a modulo N (siehe Abschnitt 2.1). Klar gilt $\mathcal{F}_{ab} = \mathcal{F}_a\mathcal{F}_b$ für $a, b \in \mathbb{Z}$, $(a, N) = (b, N) = 1$, insbesondere also

$$\mathcal{F}_a = \begin{cases} \prod\limits_{\substack{l \mid a \\ l \text{ prim}}} \mathcal{F}_l & \text{für } a > 0, \\ \mathcal{F}_{-1} \prod\limits_{\substack{l \mid a \\ l \text{ prim}}} \mathcal{F}_l = \prod\limits_{\substack{l \mid N-a \\ l \text{ prim}}} \mathcal{F}_l & \text{für } a < 0, \end{cases}$$

wobei $\mathcal{F}_l$ den geometrischen Frobenius zu l und $\mathcal{F}_{-1}$ die komplexe Konjugation bezeichnet (siehe Abschnitt 2.1). Wir benutzen ferner folgende Schreibweise:

Notation 3.1.1.

$$e_+ \overset{\mathit{def}}{=} \frac{1 + \mathcal{F}_{-1}}{2} \qquad , e_- \overset{\mathit{def}}{=} \frac{1 - \mathcal{F}_{-1}}{2}.$$

Da wir stets voraussetzen, dass p eine ungerade Primzahl bezeichnet, ist der in e_+ und e_- auftauchende Nenner eine Einheit in allen Erweiterungen von $\mathbb{Z}_p$. Es gilt ferner

$$e_-^2 = e_-, \qquad e_+^2 = e_+, \qquad e_-e_+ = 0, \qquad e_- + e_+ = 1,$$

d.h. die beiden Elemente bilden ein System zueinander orthogonaler Idempotenten.

Definition 3.1.2. Wir nennen

$$\xi_N \overset{def}{=} e_- \sum_{\substack{0 \leqslant a < N \\ (a,N)=1}} \frac{a}{N} \mathcal{F}_a = \sum_{\substack{0 \leqslant a < N \\ (a,N)=1}} \left(\frac{a}{N} - \frac{1}{2} \right) \mathcal{F}_a \in \mathbb{Q}_p[\mathrm{G}(\mathbb{Q}(\zeta_N)/\mathbb{Q})]$$

das *Stickelberger-Element* von $\mathbb{Q}(\zeta_N)$.

Bemerkung 3.1.3. ξ_N stimmt mit dem ungeraden Anteil des in [Was97], Kapitel 6, definierten Stickelberger-Elements überein. Wir folgen mit unserer Definition [BG03], § 5.2 und [Rub00].

Es gilt folgende Distributionsrelation:

Lemma 3.1.4. *Sei n ein Teiler von N und $\psi : \mathrm{G}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \longrightarrow \mathrm{G}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ die natürliche Projektion, bzw. die davon induzierte Abbildung der Gruppenringe über $\mathbb{Q}_p$. Dann gilt:*

$$\psi(\xi_N) = \xi_n \prod_{\substack{l \mid N \ prim \\ l \nmid n}} (1 - \mathcal{F}_l).$$

Beweis. Durch Induktion über die Primteiler von $\frac{N}{n}$ und ihre Vielfachheiten können wir die Aussage auf die folgenden zwei Fälle reduzieren:

Fall 1: Es gelte $N = nl$ mit l prim und $l \mid n$. Dann folgt

$$\begin{aligned}
\psi(\xi_N) &= \sum_{\substack{0 \leqslant a < N \\ (a,N)=1}} \left(\frac{a}{N} - \frac{1}{2} \right) \psi(\mathcal{F}_a) \\
&= \sum_{b=0}^{n-1} \sum_{\substack{0 \leqslant c < l \\ (b+cn,nl)=1}} \left(\frac{b+cn}{nl} - \frac{1}{2} \right) \mathcal{F}_b \\
&= \sum_{\substack{0 \leqslant b < n \\ (b,n)=1}} \left(\sum_{c=0}^{l-1} \left(\frac{b+cn}{nl} - \frac{1}{2} \right) \right) \mathcal{F}_b,
\end{aligned}$$

denn $(b+cn, nl) = (b,n)(b+cn, l)$ und $(b,n) = 1$ impliziert nach unserer Voraussetzung $(b+cn, l) = 1$. Nun gilt

$$\sum_{c=0}^{l-1} \left(\frac{b+cn}{nl} - \frac{1}{2} \right) = \frac{b}{n} + \frac{l-1}{2} - \frac{l}{2} = \frac{b}{n} - \frac{1}{2}$$

und somit $\psi(\xi_N) = \xi_n$, wie behauptet.

Fall 2: Es gelte $N = nl$ mit l prim und $l \nmid n$. Dann gilt

$$\begin{aligned}
\psi(\xi_N) &= \sum_{\substack{0\leqslant b<n \\ (b,n)=1}} \sum_{\substack{0\leqslant c<l \\ (b+cn,l)=1}} \left(\frac{b+cn}{nl} - \frac{1}{2}\right)\mathcal{F}_b \\
&= \sum_{\substack{0\leqslant b<n \\ (b,n)=1}} \sum_{c=0}^{l-1} \left(\frac{b+cn}{nl} - \frac{1}{2}\right)\mathcal{F}_b - \sum_{\substack{0\leqslant b<n \\ (b,n)=1}} \sum_{\substack{0\leqslant c<l \\ (b+cn,l)=l}} \left(\frac{b+cn}{nl} - \frac{1}{2}\right)\mathcal{F}_b \\
&= \xi_n - \sum_{\substack{0\leqslant a<nl \\ (a,nl)=l}} \left(\frac{a}{nl} - \frac{1}{2}\right)\mathcal{F}_a \\
&= \xi_n - \sum_{\substack{0\leqslant b<n \\ (b,n)=1}} \left(\frac{bl}{nl} - \frac{1}{2}\right)\mathcal{F}_b\mathcal{F}_l \\
&= \xi_n(1-\mathcal{F}_l),
\end{aligned}$$

wie behauptet. □

Betrachte nun die zyklotomische $\mathbb{Z}_p$-Erweiterung von $K_0 = \mathbb{Q}(\zeta_{Np})$ für $p \nmid N$. Es gilt $K_n = \mathbb{Q}(\zeta_{Np^{n+1}})$. Dementsprechend werden wir K_∞ mit $\mathbb{Q}(\zeta_{Np^\infty})$ bezeichnen.

Folgerung 3.1.5. *Die Stickelberger-Elemente $\xi_{Np^{n+1}}$ definieren ein Element*

$$\xi_{Np^\infty} \in \mathbb{Q}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})]\!] \overset{def}{=} \varprojlim_n \mathbb{Q}_p[\mathrm{G}(\mathbb{Q}(\zeta_{Np^{n+1}})/\mathbb{Q})].$$

Beweis. Lemma 3.1.4 zeigt, dass die betrachteten Stickelberger-Elemente unter den Übergangsabbildungen kompatibel sind, denn alle Np^{n+1} haben dieselben Primteiler. □

Bemerkung 3.1.6. Beachte, dass $\mathbb{Q}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})]\!]$ keine kompakte $\mathbb{Z}_p$-Algebra ist. Insbesondere kann Satz 2.5.2 (die universelle Eigenschaft) nicht angewandt werden. Es existiert zum Beispiel keine Fortsetzung von $Tw_{\varepsilon_\infty^{-1}}$ zu einem Endomorphismus von $\mathbb{Q}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})]\!]$. Ein solcher würde die Einheit $1-\varepsilon_\infty(\gamma)\gamma^{-1}$ (für einen Erzeuger γ von Γ, vgl. Abschnitt 3.2) auf $(1-\gamma^{-1})$ abbilden. Man überzeugt sich nun leicht, dass $(1-\gamma^{-1})$ in $\mathbb{Q}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})]\!]$ ein Nullteiler ist.

Diese Bemerkung bezieht sich jedoch nicht auf die von einem stetigen Homomorphismus $G \longrightarrow H$ pro-endlicher Gruppen induzierte Abbildung $\mathbb{Q}_p[\![G]\!] \longrightarrow \mathbb{Q}_p[\![H]\!]$.

3.2 Der Nenner des Stickelberger-Elements

In diesem Abschnitt sei N eine zu p teilerfremde Zahl. Wir betrachten die zyklotomische $\mathbb{Z}_p$-Erweiterung von $K_0 = \mathbb{Q}(\zeta_{Np})$ und setzen $\Delta = \mathrm{G}(\mathbb{Q}(\zeta_{Np})/\mathbb{Q})$. Es wird sich herausstellen, dass das Stickelberger-Element ξ_{Np^∞} als ein Element des Quotientenrings von $\mathbb{Z}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})]\!]$ aufgefasst werden kann.

Wir erinnern an den zyklotomischen Charakter

$$\varepsilon_{cycl} : \mathrm{G}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbb{Z}_p^\times, \qquad \sigma(\zeta_{p^n}) = \zeta_{p^n}^{\varepsilon_{cycl}(\sigma)} \text{ für } \sigma \in \mathrm{G}(\overline{\mathbb{Q}}/\mathbb{Q})$$

aus Abschnitt 2.1. Der Charakter ε_{cycl} faktorisiert durch $G(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})$; es gilt also

$$\varepsilon_{cycl} \in \mathrm{Hom}_{cts}(\Gamma \times \Delta, \mathbb{Z}_p^\times).$$

Die $\widehat{\Delta}$-Komponente von ε_{cycl} ist gerade ε, die $\mathrm{Hom}_{cts}(\Gamma, \mathbb{Z}_p^\times)$-Komponente ist ε_∞.

Das folgende Element der Iwasawa-Algebra wird die Rolle eines Nenners des Stickelberger-Elements übernehmen:

Notation 3.2.1. Sei γ ein topologischer Erzeuger von Γ. Setze

$$h_\gamma \stackrel{def}{=} 1 - \varepsilon_\infty(\gamma)\gamma^{-1} \in \Lambda.$$

Das Element h_γ hängt nur unwesentlich von der Wahl des topologischen Erzeugers γ ab:

Lemma 3.2.2. *Seien μ und γ topologische Erzeuger von Γ. Dann gilt $h_\gamma = h_\mu u$ mit $u \in \Lambda^\times$.*

Beweis. Da γ ein topologischer Erzeuger von $\Gamma \cong \mathbb{Z}_p$ ist, gibt es ein $a \in \mathbb{Z}_p$ mit $\mu = \gamma^a$. Ferner gilt $\mathbb{Z}_p[\Gamma_n] = \Lambda/(\gamma^{p^n} - 1)$. Für jedes $n \geq 0$ existieren eindeutige $a_n \in \mathbb{Z}, b_n \in \mathbb{Z}_p$ mit $0 \leq a_n < p^n$ und

$$a = b_n p^n + a_n.$$

Setze

$$u_n \stackrel{def}{=} \sum_{k=0}^{p^n-1} b_n \gamma^{-k} + \sum_{k=0}^{a_n-1} \gamma^{-k}.$$

Dann gilt

$$(1-\gamma^{-1})u_n = b_n(1-\gamma^{-p^n}) + (1-\gamma^{-a_n}) \equiv 1 - \mu^{-1} \mod (\gamma^{p^n} - 1).$$

Mit $c \stackrel{def}{=} \frac{a_n - a_{n-1}}{p^{n-1}}$ folgt:

$$\begin{aligned}
u_n &= \sum_{k=0}^{p^{n-1}-1} \sum_{l=0}^{p-1} b_n \gamma^{-(k+lp^{n+1})} + \sum_{k=0}^{p^{n-1}-1} \sum_{l=0}^{c-1} \gamma^{-(k+lp^{n-1})} + \sum_{k=0}^{a_{n-1}-1} \gamma^{-(k+cp^{n-1})} \\
&\equiv \sum_{k=0}^{p^{n-1}-1} \sum_{l=0}^{p-1} b_n \gamma^{-k} + \sum_{k=0}^{p^{n-1}-1} \sum_{l=0}^{c-1} \gamma^{-k} + \sum_{k=0}^{a_{n-1}-1} \gamma^{-k} \\
&\equiv (b_n p + c) \left(\sum_{k=0}^{p^{n-1}-1} \gamma^{-k} \right) + \sum_{k=0}^{a_{n-1}-1} \gamma^{-k} \\
&\equiv u_{n-1} \mod (\gamma^{p^{n-1}} - 1).
\end{aligned}$$

Also konvergieren die u_n gegen ein Element $u \in \Lambda$, das $(1-\gamma^{-1})u = 1 - \mu^{-1}$ erfüllt. Analog existiert ein Element $v \in \Lambda$ mit $(1-\mu^{-1})v = 1 - \gamma^{-1}$. Da Λ lokal und regulär, also nullteilerfrei ist, gilt $u = v^{-1} \in \Lambda^\times$. Die Aussage des Lemmas folgt nach Anwendung von $Tw_{\varepsilon_\infty^{-1}}$ (siehe Definition 2.10.1), denn der Automorphismus $Tw_{\varepsilon_\infty^{-1}}$ bildet Einheiten auf Einheiten ab. □

Die Inklusionen

$$\mathbb{Z}_p[\mathrm{G}(\mathbb{Q}(\zeta_{Np^{n+1}})/\mathbb{Q})] \subset \mathbb{Q}_p[\mathrm{G}(\mathbb{Q}(\zeta_{Np^{n+1}})/\mathbb{Q})]$$

induzieren eine injektive Abbildung

$$\mathbb{Z}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})]\!] \longrightarrow \mathbb{Q}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})]\!].$$

Also können wir h_γ als ein Element von $\mathbb{Q}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})]\!]$ auffassen.

Lemma 3.2.3. *h_γ ist eine Einheit in $\mathbb{Q}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})]\!]$.*

Beweis. Wir bezeichnen das Bild von γ in $\mathrm{G}(\mathbb{Q}(\zeta_{Np^{n+1}})/\mathbb{Q}) = \Gamma_n \times \Delta$ ebenfalls mit γ. In $\mathbb{Q}_p[\mathrm{G}(\mathbb{Q}(\zeta_{Np^{n+1}})/\mathbb{Q})]$ gilt $\gamma^{p^n} = 1$ und somit

$$\frac{h_\gamma}{1-\varepsilon_\infty(\gamma)^{p^n}} \left(\sum_{k=0}^{p^n-1} \varepsilon_\infty(\gamma)^k \gamma^{-k} \right) = \frac{1-\varepsilon_\infty(\gamma^{p^n})\gamma^{-p^n}}{1-\varepsilon_\infty(\gamma)^{p^n}} = 1.$$

Man beachte, dass $1 \neq \varepsilon_\infty(\gamma) \in 1 + p\mathbb{Z}_p$, d.h. $\varepsilon_\infty(\gamma)$ ist keine Einheitswurzel. Somit ist der Nenner stets wohldefiniert. Nun zeigt man wieder leicht, dass die Elemente

$$\frac{1}{1-\varepsilon_\infty(\gamma)^{p^n}} \left(\sum_{k=0}^{p^n-1} \varepsilon_\infty(\gamma)^k \gamma^{-k} \right) \in \mathbb{Q}_p[\mathrm{G}(K_n/\mathbb{Q})]$$

unter den Übergangsabbildungen kompatibel sind und somit ein Inverses von h_γ in $\mathbb{Q}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})]\!]$ definieren. □

Wir erhalten also eine Injektion

$$\mathbb{Z}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})]\!][h_\gamma^{-1}] \longrightarrow \mathbb{Q}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})]\!].$$

(Beachte, dass nach Lemma 3.2.2 der Ring $\mathbb{Z}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})]\!][h_\gamma^{-1}]$ nicht von der speziellen Wahl des Erzeugers γ abhängt.) Weiter unten werden wir zeigen, dass ξ_{Np^∞} ein Urbild unter dieser Abbildung hat. Zunächst beweisen wir ein vorbereitendes Lemma:

Lemma 3.2.4. *Sei $(N,p) = 1$. Dann ist $\mathcal{F}_{1+Np}^{-1} \in \mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})$ ein topologischer Erzeuger von $\Gamma \subset \mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})$.*

Beweis. Nach Definition (siehe Abschnitt 2.1) wirkt $\mathcal{F}_{1+Np}^{-1}$ wie folgt auf einer primitiven Np-ten Einheitswurzel:

$$\mathcal{F}_{1+Np}^{-1}\zeta_{Np} = \zeta_{Np}^{1+Np} = \zeta_{Np}.$$

Mit anderen Worten, die Δ-Komponente von $\mathcal{F}_{1+Np}^{-1}$ ist trivial, also $\mathcal{F}_{1+Np}^{-1} \in \Gamma$. Andererseits wird $\mathcal{F}_{1+Np}^{-1}$ unter

$$rec : \Gamma \longrightarrow 1 + p\mathbb{Z}_p$$

auf $(1+Np)^{-1}$ abgebildet (siehe Abschnitt 2.1), also auf einen Erzeuger von $1+p\mathbb{Z}_p$. □

Definition 3.2.5. Sei $y \in \mathbb{Q}$. Dann bezeichne $[y] \in \mathbb{Z}$ den *ganzen Anteil* von y, d.h. die nächstkleinere ganze Zahl. Der *gebrochene Anteil* von y ist gegeben durch $\{y\} \overset{def}{=} y - [y]$, ist also die eindeutig bestimmte Zahl $z \in \mathbb{Q}$ mit $0 \leq z < 1$ und $y - z \in \mathbb{Z}$.

Lemma 3.2.6. *Sei γ ein beliebiger Erzeuger von Γ. Dann gilt*

$$h_\gamma \xi_{Np^\infty} \in \mathbb{Z}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})]\!],$$

insbesondere also

$$\xi_{Np^\infty} \in Q(\mathbb{Z}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})]\!]).$$

Für die spezielle Wahl $\gamma = \mathcal{F}_{1+Np}^{-1}$ folgt

$$h_\gamma \xi_{Np^\infty} \equiv \sum_{\substack{0 \leqslant a < Np^{n+1} \\ (a,Np)=1}} \left(\frac{Np}{2} - \left[\frac{(1+Np)a}{Np^{n+1}} \right] \right) \mathcal{F}_{a(1+Np)} \mod (\gamma^n - 1)$$

für alle $n \geq 0$.

Beweis. Es ist klar, dass wir nur die letzte Aussage beweisen müssen, denn nach Lemma 3.2.2 dürfen wir den Erzeuger frei wählen. Man beachte außerdem, dass h_γ ein Nichtnullteiler von Λ und somit auch von $\mathbb{Z}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})]\!]$ ist (siehe Lemma 2.3.5 und Lemma 1.2.7).

Sei also $\gamma = \mathcal{F}_{1+Np}^{-1}$. Nach unserer Normierung der Reziprozitätsabbildung erhalten wir $\varepsilon_\infty(\mathcal{F}_{1+Np}^{-1}) = 1 + Np$. Es gilt folgende Gleichung in $\mathbb{Q}_p[\Gamma_n \times \Delta]$:

$$\begin{aligned}
h_\gamma \xi_{Np^{n+1}} &= (1 - (1+Np)\mathcal{F}_{1+Np}) \left(\sum \left(\left\{ \frac{a}{Np^{n+1}} \right\} - \frac{1}{2} \right) \mathcal{F}_a \right) \\
&= \sum \left(\left\{ \frac{a}{Np^{n+1}} \right\} - \frac{1}{2} \right) \mathcal{F}_a - (1+Np) \sum \left(\left\{ \frac{a}{Np^{n+1}} \right\} - \frac{1}{2} \right) \mathcal{F}_{a(1+Np)} \\
&= \sum \left(\left\{ \frac{(1+Np)a}{Np^{n+1}} \right\} - \frac{1}{2} \right) \mathcal{F}_{a(1+Np)} - (1+Np) \sum \left(\left\{ \frac{a}{Np^{n+1}} \right\} - \frac{1}{2} \right) \mathcal{F}_{a(1+Np)} \\
&= \sum \left(\left\{ \frac{(1+Np)a}{Np^{n+1}} \right\} - (1+Np) \left\{ \frac{a}{Np^{n+1}} \right\} + \frac{Np}{2} \right) \mathcal{F}_{a(1+Np)}
\end{aligned}$$

wobei sich alle Summen über $0 \leq a < Np^{n+1}$ mit $(a, Np) = 1$ erstrecken. In der vorletzten Zeile wurde in der ersten Summe a durch $a(1 + Np)$ substituiert. Dies entspricht einer Permutation der Summanden.

Nun gilt für ganze Zahlen a mit $0 \leq a < Np^{n+1}$:

$$\left[\frac{(1+Np)a}{Np^{n+1}} \right] + \left\{ \frac{(1+Np)a}{Np^{n+1}} \right\} = \frac{(1+Np)a}{Np^{n+1}} = (1+Np) \left\{ \frac{a}{Np^{n+1}} \right\}.$$

Mit dieser Relation können wir obige Gleichung zu

$$h_\gamma \xi_{Np^{n+1}} = \sum_{\substack{0 \leqslant a < Np^{n+1} \\ (a,Np)=1}} \left(\frac{Np}{2} - \left[\frac{(1+Np)a}{Np^{n+1}} \right] \right) \mathcal{F}_{a(1+Np)}$$

umformen. Da $p \neq 2$ vorausgesetzt war, liegen alle Koeffizienten in $\mathbb{Z}_p$, d.h. es gilt

$$h_\gamma \xi_{Np^{n+1}} \in \mathbb{Z}_p[\Gamma_n \times \Delta].$$

Da die Abbildungen $\mathbb{Z}_p[\mathrm{G}(\mathbb{Q}(\zeta_{Np^{n+1}})/\mathbb{Q})] \longrightarrow \mathbb{Q}_p[\mathrm{G}(\mathbb{Q}(\zeta_{Np^{n+1}})/\mathbb{Q})]$ injektiv sind und mit den Übergangsabbildungen des projektiven Systems kommutieren, definieren die Elemente $h_\gamma \xi_{Np^{n+1}}$ ein Urbild von $h_\gamma \xi_{Np^\infty}$ in $\mathbb{Z}_p[\![\Gamma \times \Delta]\!]$, für das gilt:

$$h_\gamma \xi_{Np^\infty} \equiv \sum_{\substack{0 \leqslant a < Np^{n+1} \\ (a,Np)=1}} \left(\frac{Np}{2} - \left[\frac{(1+Np)a}{Np^{n+1}} \right] \right) \mathcal{F}_{a(1+Np)} \mod (\gamma^n - 1)$$

(beachte, dass $\mathbb{Z}_p[\![\Gamma \times \Delta]\!]/(\gamma^n - 1) = \mathbb{Z}_p[\Gamma_n \times \Delta]$). □

Sei d ein Teiler von N. Nach Satz 2.6.2.(iii) ist die natürliche Projektion

$$\psi : \mathbb{Z}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})]\!] \longrightarrow \mathbb{Z}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{dp^\infty})/\mathbb{Q})]\!]$$

fortsetzbar. Lemma 3.1.4 impliziert nun:

Folgerung 3.2.7. *Sei d ein Teiler von N. Ferner bezeichne*

$$\psi : Q(\mathbb{Z}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q})]\!]) \longrightarrow Q(\mathbb{Z}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{dp^\infty})/\mathbb{Q})]\!])$$

die von der natürlichen Projektion induzierte Abbildung. Dann gilt:

$$\psi(\xi_{Np^\infty}) = \xi_{dp^\infty} \prod_{\substack{l \mid N \ prim \\ l \nmid d}} (1 - \mathcal{F}_l).$$

Beweis. Die Einschränkung von ψ auf Γ ist die Identität (siehe Lemma 2.2.2). Insbesondere wird h_γ auf h_γ abgebildet. Nach Lemma 3.1.4 folgt durch Übergang zum projektiven Limes

$$\psi(h_\gamma \xi_{Np^\infty}) = h_\gamma \xi_{dp^\infty} \prod_{\substack{l \mid N \text{ prim} \\ l \nmid d}} (1 - \mathcal{F}_l) \in \mathbb{Z}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{dp^\infty})/\mathbb{Q})]\!]$$

und somit die Aussage für $Q(\mathbb{Z}_p[\![\mathrm{G}(\mathbb{Q}(\zeta_{dp^\infty})/\mathbb{Q})]\!])$. □

3.3 Die äquivariante L-Funktion

Sei S eine endliche Menge von Stellen von $\mathbb{Q}$, die p und ∞ enthält und sei $K_0/\mathbb{Q}$ außerhalb S unverzweigt. Ist $L_0 \subset K_0$, so bezeichnen wir mit

$$\psi_{K_\infty/L_\infty} : \mathrm{G}(K_\infty/\mathbb{Q}) \longrightarrow \mathrm{G}(L_\infty/\mathbb{Q})$$

die natürliche Projektion, bzw. den entsprechenden Homomorphismus der pro-endlichen Gruppenringe. Nach Satz 2.6.2.(iii) ist ψ_{K_∞/L_∞} zu einem Homomorphismus

$$\psi_{K_\infty/L_\infty} : Q(\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]) \longrightarrow Q(\mathcal{O}_p[\![\mathrm{G}(L_\infty/\mathbb{Q})]\!])$$

fortsetzbar. Mit G_S bezeichnen wir die Galoisgruppe der maximalen, außerhalb S unverzweigten Erweiterung von $\mathbb{Q}$ (siehe Abschnitt 2.1).

Lemma 3.3.1. *Sei $K_0/\mathbb{Q}$ außerhalb S unverzweigt und $\chi : \mathrm{G}_S \longrightarrow \mathcal{O}_p^\times$ ein stetiger Charakter. Dann existiert eine natürliche Zahl N, die folgende Bedingungen erfüllt:*

(i) Die Menge der Primteiler von Np stimmt mit $S \setminus \{\infty\}$ überein,

(ii) $K_0 \subset \mathbb{Q}(\zeta_{Np})$,

(iii) $\chi \in \mathrm{Hom}_{cts}(\mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q}), \mathcal{O}_p^\times)$,

(iv) $(N, p) = 1$.

Beweis. Nach dem Satz von Kronecker und Weber (siehe Theorem 2.1.2) und der Diskussion in Abschnitt 2.1 existiert ein N, dass die ersten drei Bedingungen erfüllt. Ferner hatten wir vorausgesetzt, dass $\mathbb{Q}_n \cap K_0 = \mathbb{Q}$ für alle $n \geq 0$ (siehe Abschnitt 2.2). Folglich können wir N so wählen, dass auch die vierte Bedingung erfüllt ist. □

Definition 3.3.2. Sei $\chi : \mathrm{G}_S \longrightarrow \mathcal{O}_p^\times$ ein stetiger Charakter und $K_0/\mathbb{Q}$ außerhalb S unverzweigt. Wähle ein N, das den Bedingungen von Lemma 3.3.1 genügt. Dann nennen wir

$$\mathcal{L}_{p,S}(K_\infty, \chi) \overset{def}{=} \psi_{\mathbb{Q}(\zeta_{Np^\infty})/K_\infty}(Tw_\chi(e_+ - \xi_{Np^\infty})) \in Q(\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!])$$

äquivariante L-Funktion zu K_∞ und S am Charakter χ.

Lemma 3.3.3.

(i) $\mathcal{L}_{p,S}(K_\infty, \chi)$ hängt nicht von der speziellen Wahl von N ab.

(ii) Sei L_0 ein Teilkörper von K_0. Dann gilt:

$$\psi_{K_\infty/L_\infty}(\mathcal{L}_{p,S}(K_\infty, \chi)) = \mathcal{L}_{p,S}(L_\infty, \chi).$$

(iii) Sei T eine weitere endliche Menge von Stellen, die S enthält. Dann gilt:

$$\mathcal{L}_{p,T}(K_\infty, \chi) = \mathcal{L}_{p,S}(K_\infty, \chi) \prod_{l \in T \setminus S} (1 - Tw_\chi(e_- \mathcal{F}_l)).$$

Beweis. Zu (i): Sei d die minimale Zahl, die die Bedingungen von Lemma 3.3.1 erfüllt. Dann gilt $d \mid N$. Außerdem stimmt die Menge der Primteiler von d mit der von N überein und Tw_χ vertauscht nach Bemerkung 2.10.2 mit $\psi_{\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q}(\zeta_{dp^\infty})}$. Also gilt

$$\begin{aligned} &\psi_{\mathbb{Q}(\zeta_{Np^\infty})/K_\infty}(Tw_\chi(e_+ - \xi_{Np^\infty})) = \\ &\quad = (\psi_{\mathbb{Q}(\zeta_{dp^\infty})/K_\infty} \circ Tw_\chi \circ \psi_{\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q}(\zeta_{dp^\infty})})(e_+ - \xi_{Np^\infty}) \\ &\quad = \psi_{\mathbb{Q}(\zeta_{dp^\infty})/K_\infty}(Tw_\chi(e_+ - \xi_{dp^\infty})) \end{aligned}$$

nach Folgerung 3.2.7.

Zu (ii): Ist K_0 in $\mathbb{Q}(\zeta_{Np})$ enthalten, so auch L_0. Da L_0 ein Teilkörper von K_0 ist, enthält S bereits alle in $L_0/\mathbb{Q}$ verzweigten Stellen. Damit erfüllt N auch für L_0 die Bedingungen von Lemma 3.3.1 und es gilt:

$$\mathcal{L}_{p,S}(L_\infty, \chi) = \psi_{\mathbb{Q}(\zeta_{Np^\infty})/L_\infty}(Tw_\chi(e_+ - \xi_{Np^\infty})) = \psi_{K_\infty/L_\infty}(\mathcal{L}_{p,S}(K_\infty, \chi)).$$

Zu (iii): Sei

$$M \overset{\text{def}}{=} N \prod_{l \in T \setminus S} l.$$

Dann erfüllt M die Bedingungen von Lemma 3.3.1 für K_0, T und den Charakter $\chi \in \mathrm{Hom}_{cts}(\mathrm{G}_S, \mathcal{O}_p^\times) \subset \mathrm{Hom}_{cts}(\mathrm{G}_T, \mathcal{O}_p^\times)$. Nach Folgerung 3.2.7 gilt:

$$\begin{aligned}\mathcal{L}_{p,T}(K_\infty, \chi) &= \psi_{\mathbb{Q}(\zeta_{Mp^\infty})/K_\infty}\big(Tw_\chi(e_+ - \xi_{Mp^\infty})\big) \\ &= \psi_{\mathbb{Q}(\zeta_{Np^\infty})/K_\infty}\Big(Tw_\chi\Big(e_+ - \xi_{Np^\infty} \prod_{l \in T \setminus S} (1 - \mathcal{F}_l)\Big)\Big).\end{aligned}$$

Beachte nun, dass e_+ und e_- ein System zueinander orthogonaler Idempotenten bilden und dass $\xi_{Np^\infty} = e_- \xi_{Np^\infty}$. Also gilt:

$$\begin{aligned}&e_+ - \xi_{Np^\infty} \prod_{l \in T \setminus S} (1 - \mathcal{F}_l) = \\ &\quad = (e_+ - e_- \xi_{Np^\infty}) \prod_{l \in T \setminus S} \big(e_+ + e_-(1 - \mathcal{F}_l)\big) = (e_+ - \xi_{Np^\infty}) \prod_{l \in T \setminus S} (1 - e_- \mathcal{F}_l),\end{aligned}$$

woraus die Behauptung folgt. □

Bemerkung 3.3.4. Formal korrekt müssten wir

$$1 - \psi_{\mathbb{Q}(\zeta_{Np^\infty})/K_\infty}\big(Tw_\chi(e_- \mathcal{F}_l)\big)$$

statt $1 - Tw_\chi(e_- \mathcal{F}_l)$ schreiben (siehe Bemerkung 2.10.2). Wir hoffen jedoch, dass unsere Schreibweise nicht zu Missverständnissen führen wird.

3.4 Zerlegung nach Charakteren

In diesem Abschnitt werden wir zeigen, wie die Bilder der äquivarianten L-Funktion unter den Projektionen p_θ (für $\theta \in \widehat{\Delta}$, siehe Definition 2.6.1) mit den p-adischen L-Funktionen zu Dirichlet-Charakteren zusammenhängen. Folgendes Lemma ist wohlbekannt:

Lemma 3.4.1. *Sei $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$ ein primitiver Dirichlet-Charakter. Dann ist die L-Funktion zu χ für $s > 1$ durch*

$$L(\chi, s) \overset{\text{def}}{=} \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

definiert und auf ganz $\mathbb{C}$ meromorph fortsetzbar. Die Funktionswerte $L(\chi, 1 - r)$ für ganzzahlige $r > 0$ liegen in dem Erweiterungskörper $\mathbb{Q}(\{\chi(a) \,|\, a \in \mathbb{Z}\})$ von endlichem Grad über $\mathbb{Q}$.

Beweis. Siehe [Brü95], Satz 2.4.1, Satz 2.4.2 und [Was97], Theorem 4.2. □

Bemerkung 3.4.2. Ist F ein endlicher Erweiterungskörper von $\mathbb{Q}_p$ mit Bewertungsring $\mathcal{O}_p$ und (für beliebiges S) $\chi : \mathrm{G}_S \longrightarrow \mathcal{O}_p^\times$ ein Charakter endlicher Ordnung, so können wir χ in der in Abschnitt 2.1 beschriebenen Weise mit einem Dirichlet-Charakter mit Werten in $\mathbb{C}$ identifizieren, indem wir eine Einbettung $\varrho : F \longrightarrow \mathbb{C}$ wählen. Andererseits existiert nach Lemma 3.4.1 ein Urbild von $L(\varrho \circ \chi, 1-r)$ (für $r > 0$ ganzzahlig) unter ϱ. Das Urbild $\varrho^{-1}(L(\varrho\circ\chi, 1-r))$ hängt offensichtlich nicht von ϱ ab. Wir werden deshalb die Identifikation ϱ in Zukunft nicht mehr gesondert kennzeichnen.

Lemma 3.4.3. *Seien $m > 0$, $k \geq 0$, N ganze Zahlen mit $(N,p) = 1$ und χ ein Dirichlet-Charakter mit Führer Np^k und Werten in dem Erweiterungskörper F von endlichem Grad über $\mathbb{Q}_p$. Dann gilt:*

$$\lim_{n\to\infty} \frac{1}{Np^{n+1}} \sum_{\substack{0\leqslant a<Np^{n+1}\\ (a,Np)=1}} \chi\varepsilon^m(a)a^m = -m(1-\chi\varepsilon^m(p)p^{m-1})L(\chi\varepsilon^m, 1-m)$$

in F, wobei wir $\chi\varepsilon^m$ als primitiven Dirichlet-Charakter auffassen.

Beweis. Dies ist genau [Was97], Lemma 7.11, verknüpft mit Theorem 4.2. Beachte dabei, dass der Teichmüller-Charakter ω in [Was97] für $(a,p) = 1$ wie folgt mit ε zusammenhängt:

$$\varepsilon(\mathcal{F}_a) = \varepsilon(a) = \omega^{-1}(a).$$

□

Wir wollen den Zusammenhang mit den in [HK03] verwendeten Elementen der Iwasawa-Algebra herstellen.

Definition 3.4.4. Sei $r > 0$ und χ ein primitiver Dirichlet-Charakter mit $\chi(-1) = (-1)^r$. Dann sei $\mathcal{L}_p(\chi, 1-r) \in Q(\mathcal{O}_p[\![\Gamma]\!])$ das nach Lemma 2.6.3 und Bemerkung 2.6.4 durch folgende Bedingung eindeutig charakterisierte Element: Sei $\tau : \Gamma \longrightarrow \mathcal{O}_p^\times$ ein Charakter endlicher Ordnung (mit $\mathcal{O}_p$ genügend groß). Dann gelte

$$\tau(\mathcal{L}_p(\chi, 1-r)) = (1 - \chi\tau(p)p^{r-1})L(\chi\tau, 1-r).$$

Bemerkung 3.4.5. Die Elemente $\mathcal{L}_p(\chi, 1-r)$ stimmen leider nicht ganz mit den in [HK03] verwendeten Elementen gleichen Namens überein, siehe Abschnitt 6.5.

Folgender Satz ist eine direkte Konsequenz von [Was97], Theorem 7.10. Da die unterschiedliche Normierung der Reziprozitäts-Abbildung leicht zu Verwechselungen führen kann, geben wir hier den Beweis, adaptiert auf unsere Notation, vollständig wieder.

Satz 3.4.6. *Sei $(N,p) = 1$ und $\theta : \mathrm{G}(\mathbb{Q}(\zeta_{Np})/\mathbb{Q}) \longrightarrow \mathcal{O}_p^\times$ ein Charakter mit Führer N oder Np. Die Menge S bestehe aus den Primteilern von Np und der archimedischen Stelle. Sei weiterhin $r > 0$ ganzzahlig. Dann gilt*

$$p_\theta(\mathcal{L}_{p,S}(\mathbb{Q}(\zeta_{Np^\infty}), \varepsilon_{cycl}^{1-r})) = \begin{cases} \mathcal{L}_p(\theta, 1-r) & \textit{für } \theta(-1) = (-1)^r, \\ 1 & \textit{für } \theta(-1) = (-1)^{r-1}. \end{cases}$$

Beweis. Die Zahl N erfüllt die Bedingungen von Lemma 3.3.1 für $K_0 = \mathbb{Q}(\zeta_{Np})$, S und θ. Es gilt deshalb

$$\mathcal{L}_{p,S}(\mathbb{Q}(\zeta_{Np^\infty}), \varepsilon_{cycl}^{1-r}) = Tw_{\varepsilon_{cycl}^{1-r}}(e_+ - \xi_{Np^\infty}).$$

Bezeichne

$$p_\Gamma : \mathrm{G}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q}) \longrightarrow \Gamma$$

die natürliche Projektion. Dann gilt $p_\theta(\mathcal{F}_{-1}) = 1$. Außerdem gilt nach der Definition des zyklotomischen Charakters (siehe Abschnitt 2.1) $\varepsilon_{cycl}(\mathcal{F}_a^{-1}) = a \in \mathbb{Z}_p$ für $a \in \mathbb{Z}$, $(a, Np) = 1$. Wir erhalten somit:

$$(p_\theta \circ Tw_{\varepsilon_{cycl}^{1-r}})(e_+) = \frac{1 + \theta\varepsilon_{cycl}^{1-r}(\mathcal{F}_{-1})}{2} = \begin{cases} 1 & \text{für } \theta(-1) = (-1)^{r-1}, \\ 0 & \text{für } \theta(-1) = (-1)^r. \end{cases}$$

Für e_- gelten die entgegengesetzten Vorzeichen. Da $\xi_{Np^\infty} = e_-\xi_{Np^\infty}$, folgt

$$p_\theta(\mathcal{L}_{p,S}(\mathbb{Q}(\zeta_{Np^\infty}), \varepsilon_{cycl}^{1-r})) = 1$$

für $\theta(-1) = (-1)^{r-1}$.

Sei nun $\theta(-1) = (-1)^r$. Wir zerlegen ε_{cycl} in ε_∞ und ε. Wähle $\gamma = \mathcal{F}_{1+Np}^{-1}$ als topologischen Erzeuger von Γ. Nach Lemma 3.2.6 gilt:

$$p_{\varepsilon^{1-r}\theta}(e_+ - h_\gamma \xi_{Np^\infty}) \equiv \sum_{a \in A_n} \left(\left[\frac{(1+Np)a}{Np^{n+1}} \right] - \frac{Np}{2} \right) \varepsilon^{1-r}\theta(a(1+Np)) p_\Gamma(\mathcal{F}_{a(1+Np)}) \mod (\gamma^n - 1),$$

wobei sich die Summe über die Elemente a der Menge

$$A_n \overset{\text{def}}{=} \{0 \le a < Np^{n+1} \mid (a, Np) = 1\}$$

erstreckt. Für $a \in A_n$ schreiben wir:

$$\begin{aligned} b_n(a) &\overset{\text{def}}{=} \left[\frac{(1+Np)a}{Np^{n+1}} \right] \\ c_n(a) &\overset{\text{def}}{=} (1+Np)a - Np^{n+1} b_n(a) = Np^{n+1} \left\{ \frac{(1+Np)a}{Np^{n+1}} \right\}. \end{aligned}$$

Die Abbildung $c_n : A_n \longrightarrow A_n$ ist gerade die Multiplikation der Restklassen modulo Np^{n+1} mit $(1 + Np)$, gesehen als eine Permutation der Repräsentanten-Menge A_n.

Sei τ ein Charakter endlicher Ordnung von Γ. Für genügend große n gilt $\tau(\gamma)^{p^n} = 1$ und somit

$$(\tau \circ Tw_{\varepsilon_\infty^{1-r}})(\gamma^{p^n}) = \varepsilon_\infty(\mathcal{F}_{1+Np}^{-1})^{p^n(1-r)} = (1+Np)^{p^n(1-r)} \equiv 1 \mod p^n,$$

d.h. die Abbildung $\tau \circ Tw_{\varepsilon_\infty^{1-r}} : \Gamma \longrightarrow (\mathcal{O}_p/p^n\mathcal{O}_p)^\times$ faktorisiert durch Γ_n. Nach der universellen Eigenschaft der pro-endlichen Gruppenringe (siehe Satz 2.5.2) gilt also:

$$\begin{aligned}
&(\tau \circ p_\theta \circ Tw_{\varepsilon_{cycl}^{1-r}})(e_+ - h_\gamma \xi_{Np^\infty}) \equiv \\
&\quad \equiv \sum_{a \in A_n} \left(b_n(a) - \frac{Np}{2} \right) \varepsilon_{cycl}(\mathcal{F}_{a(1+Np)})^{1-r} \theta\tau(\mathcal{F}_{a(1+Np)}) \\
&\quad \equiv \sum_{a \in A_n} \left(b_n(a) - \frac{Np}{2} \right) (a(1+Np))^{r-1} \theta\tau(a(1+Np)) \\
&\quad \equiv \sum_{a \in A_n} \left(b_n(a) - \frac{Np}{2} \right) (c_n(a) + Np^{n+1} b_n(a))^{r-1} \theta\tau(c_n(a) + Np^{n+1} b_n(a)) \\
&\quad \equiv \sum_{a \in A_n} \left(b_n(a) - \frac{Np}{2} \right) c_n(a)^{r-1} \theta\tau(c_n(a)) \mod p^{n+1}.
\end{aligned}$$

Wir verwenden dabei, dass θ ein Charakter mit Führer N oder Np und τ stets ein gerader Charakter mit Führer p^k für ein festes k ist. Daher gilt auch für n hinreichend groß:

$$\begin{aligned}
\sum_{a \in A_n} \theta\tau(a) a^{r-1} &\equiv \frac{1}{2} \Big(\sum_{a \in A_n} \theta\tau(a) a^{r-1} + \sum_{b \in A_n} \theta\tau(Np^{n+1} - b)(Np^{n+1} - b)^{r-1} \Big) \\
&\equiv \frac{1}{2} \Big(\sum_{a \in A_n} \theta(a) a^{r-1} + \theta(-1)(-1)^{r-1} \sum_{b \in A_n} \theta\tau(b) b^{r-1} \Big) \equiv 0 \mod p^{n+1}.
\end{aligned}$$

Somit können wir den Term $-\frac{Np}{2}$ streichen:

$$\Big(\tau \circ p_\theta \circ Tw_{\varepsilon_{cycl}^{1-r}} \Big)(e_+ - h_\gamma \xi_{Np^\infty}) \equiv \sum_{a \in A_n} b_n(a) c_n(a)^{r-1} \theta\tau(c_n(a)) \mod p^{n+1}.$$

Nun gilt:

$$\begin{aligned}
\Big(\tau \circ p_\theta \circ Tw_{\varepsilon_{cycl}^{1-r}} \Big)(h_\gamma) &= \Big(\tau \circ Tw_{\varepsilon_\infty^{1-r}} \circ p_{\varepsilon^{1-r}\theta} \Big)(1 - \varepsilon_\infty(\gamma)\gamma^{-1}) = \\
&= 1 - \varepsilon_\infty^r(\gamma)\tau(\gamma)^{-1} = 1 - (1+Np)^r \tau(1+Np).
\end{aligned}$$

Wir erhalten folgende Kongruenz:

$$\begin{aligned}
&\Big(\tau \circ Tw_{\varepsilon_\infty^{1-r}} \Big)(h_\gamma) \sum_{a \in A_n} a^r \theta\tau(a) \equiv \big(1 - (1+Np)^r \tau(1+Np) \big) \sum_{a \in A_n} a^r \theta\tau(a) \\
&\quad \equiv \sum_{a \in A_n} a^r \theta\tau(a) - \sum_{a \in A_n} (a(1+Np))^r \theta\tau(a(1+Np)) \\
&\quad \equiv \sum_{a \in A_n} a^r \theta\tau(a) - \sum_{a \in A_n} \big(c_n(a) + Np^{n+1} b_n(a) \big)^r \theta\tau(c_n(a)) \\
&\quad \equiv \sum_{a \in A_n} a^r \theta\tau(a) - \sum_{a \in A_n} \big(c_n(a)^r + rNp^{n+1} b_n(a) c_n(a)^{r-1} \big) \theta\tau(c_n(a)) \\
&\quad \equiv \sum_{a \in A_n} a^r \theta\tau(a) - \sum_{a \in A_n} c_n(a)^r \theta\tau(c_n(a)) - \sum_{a \in A_n} rNp^{n+1} b_n(a) c_n(a)^{r-1} \theta\tau(c_n(a)) \\
&\quad \equiv -rNp^{n+1} \sum_{a \in A_n} b_n(a) c_n(a)^{r-1} \theta\tau(c_n(a)) \mod p^{(n+1)^2}.
\end{aligned}$$

Es gilt also:

$$r\Big(\tau\circ Tw_{\varepsilon_\infty^{1-r}}\circ p_{\varepsilon^{1-r}\theta}\Big)(e_+ - h_\gamma\xi_{Np^\infty}) \equiv \Big(\tau\circ Tw_{\varepsilon_\infty^{1-r}}\Big)(h_\gamma)\sum_{a\in A_n}\frac{a^r}{Np^{n+1}}\theta\tau(a) \mod p^{(n+1)}.$$

Lemma 3.4.3, angewandt auf den geraden Charakter $\chi = \theta\tau\varepsilon^{-r}$ und $m = r$, liefert nun das Ergebnis. □

Folgerung 3.4.7. *Sei S eine endliche Menge von Stellen, die p und ∞ enthält. Sei ferner $K_0/\mathbb{Q}$ außerhalb S unverzweigt. Der Bewertungsring $\mathcal{O}_p$ enthalte die Werte der Charaktere aus $\widehat{\Delta}$. Ist $\theta \in \widehat{\Delta}$ und $r > 0$ eine positive ganze Zahl, so gilt*

$$p_\theta(\mathcal{L}_{p,S}(K_\infty, \varepsilon_{cycl}^{1-r})) = \begin{cases} \mathcal{L}_p(\theta, 1-r)\prod\limits_{l\in S\setminus T}(1 - l^{r-1}p_\theta(\mathcal{F}_l)) & \textit{für } \theta(-1) = (-1)^r,\\ 1 & \textit{für } \theta(-1) = (-1)^{r-1}, \end{cases}$$

mit

$$T \overset{\text{def}}{=} \{\infty, p\} \cup \{\textit{Primteiler des Führers von } \theta\}.$$

Beweis. Sei d oder dp mit $(d,p) = 1$ der Führer von θ. Wir nutzen die Kommutativitäts-Aussage von Satz 2.6.2 und Lemma 3.3.3. Danach können wir, indem wir eventuell zu einem Teilkörper von K_0 übergehen, annehmen, dass $K_0/\mathbb{Q}$ nur über p, ∞ und den Primteilern von d verzweigt ist. Dann erfüllt d die Bedingungen von Lemma 3.3.1 für T, K_0 und θ. Wir wenden Satz 3.4.6 für θ an. Durch Vergrößern der Menge T zu S erhalten wir nach Lemma 3.3.3 die Euler-Faktoren in der obigen Aussage. □

Wir zeigen nun noch, dass $\mathcal{L}_{p,S}(K_\infty,\chi)$ ein Element in der Gruppe der Cartier-Divisoren $\mathfrak{C}(\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!])$ definiert. Mit diesem Element werden wir uns später eingehend beschäftigen. Zunächst beweisen wir ein vorbereitendes Lemma:

Lemma 3.4.8. *Sei $\mathcal{O}_p$ der Bewertungsring eines beliebigen Erweiterungskörpers endlichen Grades von $\mathbb{Q}_p$ und $l \neq p$ eine Primzahl, die in $K_0/\mathbb{Q}$ nicht verzweigt. Dann ist der Euler-Faktor $1 - e_-\mathcal{F}_l$ ein Nichtnullteiler von $\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$.*

Beweis. Nach Lemma 1.2.7 ist die Erweiterung $\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!] \longrightarrow \mathcal{O}'_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$ für $\mathcal{O}_p \subset \mathcal{O}'_p$ fortsetzbar. Wir dürfen deshalb annehmen, dass $\mathcal{O}_p$ die Werte der Charaktere aus $\widehat{\Delta}$ enthält. Nach Satz 2.6.2.(i) reicht es zu zeigen, dass für jeden Charakter $\theta \in \widehat{\Delta}$ das Element $1 - p_\theta(e_-\mathcal{F}_l) \in \mathcal{O}_p[\![\Gamma]\!]$ ein Nichtnullteiler ist. Nun gilt aber sicher

$$p_\theta(\mathcal{F}_l) = \theta(l)p_\Gamma(\mathcal{F}_l) \neq 1.$$

Da $\mathcal{O}_p[\![\Gamma]\!]$ ein regulärer lokaler Ring (siehe Satz 2.3.3), also nullteilerfrei ist, folgt die Behauptung. □

Folgerung 3.4.9. *Sei $\chi : \mathrm{G}_S \longrightarrow \mathcal{O}_p^\times$ ein stetiger Charakter. Dann ist $\mathcal{L}_{p,S}(K_\infty,\chi)$ eine Einheit von $Q(\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!])$. Insbesondere erzeugt $\mathcal{L}_{p,S}(K_\infty,\chi)$ einen Cartier-Divisor von $\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$.*

Beweis. Nach Satz 2.6.2.(iii) dürfen wir annehmen, dass $K_0 = \mathbb{Q}(\zeta_{Np})$ für ein N, das den Bedingungen von Lemma 3.3.1 genügt. Da alle Verdrehungen um Charaktere Einheiten in Einheiten abbilden, können wir o.B.d.A. $\chi = \varepsilon_{cycl}^{-2}$ wählen.

Nach Satz 2.6.2.(i) können wir feststellen, ob $\mathcal{L}_{p,S}(\mathbb{Q}(\zeta_{Np^\infty}), \varepsilon_{cycl}^{-2})$ eine Einheit in $Q(\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!])$ ist, indem wir nach Charakteren θ von $\Delta = \mathrm{G}(\mathbb{Q}(\zeta_{Np})/\mathbb{Q})$ zerlegen. Wir benutzen Folgerung 3.4.7. Nach Lemma 3.4.8 sind alle Euler-Faktoren Einheiten des Quotientenrings. Infolgedessen müssen wir nur $\mathcal{L}_p(\theta, -2)$ für ungerade Charaktere θ betrachten (für gerade Charaktere ist nichts zu zeigen). Es ist aber bekannt, dass für θ ungerade $L(\theta, -2) \neq 0$ gilt (siehe [Brü95], Satz 2.4.2). Offensichtlich ist auch $(1 - \theta(p)p^2) \neq 0$. Nach Definition 3.4.4 folgt somit $\mathcal{L}_p(\theta, -2) \neq 0$, also die Behauptung. $\square$

4 Das Theorem von Ferrero-Washington

In diesem Kapitel geben wir den Beweis von L. C. Washington ([Was97] bzw. [Was89]) des Theorems von Ferrero-Washington wieder. Dabei handelt es sich um eine Umformulierung des Beweises von W. Sinnot (siehe [Sin84]), der wiederum eine wesentliche Vereinfachung des ursprünglichen Beweises von Ferrero und Washington (siehe [FW79]) darstellt.

4.1 Die μ-Invariante von K. Iwasawa

Die Iwasawa-Algebra $\Lambda \cong \mathbb{Z}_p[\![T]\!]$ ist ein regulärer und lokaler Ring der Dimension 2 und die Primideale der Kodimension 1 sind (p) und die von irreduziblen, ausgezeichneten Polynomen

$$P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0, \qquad n > 0, \quad a_i \in (p), \quad 0 \leq i < n,$$

erzeugten Hauptideale (siehe Satz 2.3.3). Ist M ein endlich erzeugter Λ-Modul, so gibt es nach dem Strukturtheorem (siehe Theorem 1.9.2) einen Pseudo-Isomorphismus

$$f : M \longrightarrow \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/(p^{m_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(P_j^{n_j})$$

mit irreduziblen, ausgezeichneten Polynomen P_j.

Definition 4.1.1. Die Zahl

$$\mu(M) \overset{def}{=} \sum_{i=1}^{s} m_i$$

heißt *μ-Invariante* von M.

Das Verschwinden der μ-Invariante kann man wie folgt charakterisieren:

Lemma 4.1.2. *Sei M ein endlich erzeugter Torsionsmodul über Λ. Dann sind folgende Aussagen äquivalent:*

(i) $\mu(M) = 0$

(ii) *M ist über $\mathbb{Z}_p$ endlich erzeugt.*

(iii) $M \otimes_\Lambda \Lambda_{(p)} = 0$.

Beweis. Sei

$$f : M \longrightarrow \bigoplus_{i=1}^{s} \Lambda/(p^{m_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(P_j^{n_j})$$

ein Pseudo-Isomorphismus. Dann gilt nach Definition 1.9.1

$$\mathrm{Ker}(f) \otimes_\Lambda \Lambda_{(p)} = \mathrm{Coker}(f) \otimes_\Lambda \Lambda_{(p)} = 0$$

und somit

$$M \otimes_\Lambda \Lambda_{(p)} \cong \left(\bigoplus_{i=1}^{s} \Lambda/(p^{m_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(P_j^{n_j}) \right) \otimes_\Lambda \Lambda_{(p)} \cong \bigoplus_{i=1}^{s} \Lambda_{(p)}/(p^{m_i}).$$

Die Äquivalenz von (i) und (iii) folgt daraus sofort.

Andererseits ist ein Λ-Homomorphismus f genau dann ein Pseudo-Isomorphismus, wenn der Kern und der Kokern von f endliche Kardinalität haben (siehe [NSW00], Bemerkung 4 nach Definition 5.1.4). Also dürfen wir in (i) und (ii) den Modul M durch

$$M' = \bigoplus_{i=1}^{s} \Lambda/(p^{m_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(P_j^{n_j})$$

ersetzen. Sei

$$P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0,$$

mit $n > 0$ und $a_i \in (p)$, $0 \leq i < n$ ein beliebiges ausgezeichnetes Polynom. Dann gilt $\Lambda/(P) \cong \mathbb{Z}_p^n$ als $\mathbb{Z}_p$-Moduln. Andererseits ist

$$\Lambda/(p^n) \cong \mathbb{Z}/(p^n)[\![T]\!]$$

eindeutig kein endlich erzeugter $\mathbb{Z}_p$-Modul. Damit folgt die Äquivalenz von (i) und (ii). □

Diese Charakterisierung werden wir jedoch erst später benötigen (siehe Kapitel 6).

4.2 Das Theorem von Ferrero-Washington

Sei K_∞/K die zyklotomische $\mathbb{Z}_p$-Erweiterung eines abelschen Zahlkörpers K. Dann ist

$$X \stackrel{\mathit{def}}{=} \varprojlim_n Cl(K_n) \otimes_\mathbb{Z} \mathbb{Z}_p$$

ein Λ-Modul (siehe [Was97], § 13.3). Wir wollen folgendes Theorem beweisen:

Theorem 4.2.1 (Ferrero-Washington).

(i) *Sei K eine abelsche Erweiterung von $\mathbb{Q}$, p eine ungerade Primzahl und K_∞/K die zyklotomische $\mathbb{Z}_p$-Erweiterung von K. Dann gilt $\mu(X) = 0$.*

(ii) *Sei θ ein primitiver, ungerader Dirichlet-Charakter der ersten Art und γ ein topologischer Erzeuger von Γ. Sei ferner $\mathcal{O}_p$ der Bewertungsring eines Erweiterungskörpers endlichen Grades von $\mathbb{Q}_p$, der die Werte von θ enthält. Das maximale Ideal von $\mathcal{O}_p$ werde von π erzeugt. Dann ist π kein Teiler von*

$$h_\gamma \mathcal{L}_p(\theta, 0) \in \mathcal{O}_p[\![\Gamma]\!].$$

Dabei reicht es, die zweite der beiden Aussagen zu zeigen:

Satz 4.2.2. *In Theorem 4.2.1 impliziert Aussage (ii) die Aussage (i).*

Beweis. Siehe [Was97], § 7.5. Der Beweis beruht im Wesentlichen auf der Klassenzahlformel. □

Der Beweis von Theorem 4.2.1 wird uns die nächsten Abschnitte beschäftigen. Im letzten Abschnitt zeigen wir, welche Konsequenz das Theorem von Ferrero-Washington für den Cartier-Divisor hat, der von der äquivarianten L-Funktion erzeugt wird.

4.3 Vorbereitungen

Wir führen in diesem Abschnitt zwei Bezeichnungen ein, die wir später benötigen werden.

Definition 4.3.1. Sei $a \in \mathbb{Z}_p^\times$ und $\alpha \in \mu_{p-1}$ die eindeutig bestimmte $p-1$-te Einheitswurzel mit $a \equiv \alpha \mod p$. Dann setzen wir

$$\langle a \rangle \overset{def}{=} \alpha^{-1} a \in 1 + p\mathbb{Z}_p.$$

Definition 4.3.2. Sei $a \in \mathbb{Z}_p^\times$. Setze

$$\mathrm{i}(a) \overset{def}{=} \frac{\log_p(a)}{\log_p(1+dp)}.$$

Dabei bezeichnet *log_p* den *p-adischen Logarithmus* (siehe [Was97], § 5.1).

Mit der Funktion i hat es folgende Bewandtnis: $(1 + dp)$ ist ein topologischer Erzeuger der multiplikativen Gruppe $1 + p\mathbb{Z}_p$. Ist $a \in \mathbb{Z}_p^\times$, so gilt:

$$(1 + dp)^{\mathrm{i}(a)} = \langle a \rangle\,.$$

Genauer gilt:

Lemma 4.3.3. *Seien $a, b \in \mathbb{Z}_p^\times$. Dann gilt*

(i) $\mathrm{i}(a) \in \mathbb{Z}_p$,

(ii) $\mathrm{i}(ab) = \mathrm{i}(a) + \mathrm{i}(b)$,

(iii) $\mathrm{i}(a) = \mathrm{i}(\langle a \rangle)$,

(iv) $\mathrm{i}(a) \equiv \mathrm{i}(b) \mod p^n$ *genau dann, wenn* $\langle a \rangle \equiv \langle b \rangle \mod p^{n+1}$.

(v) i *induziert einen stetigen Gruppenisomorphismus* $1 + p\mathbb{Z}_p \longrightarrow \mathbb{Z}_p$.

Beweis. Wir verwenden folgende Eigenschaften von *log_p* (siehe [Was97], Satz 5.4 und Lemma 5.5): Seien $a, b \in \mathbb{Z}_p^\times$. Dann gilt:

$$\begin{aligned}
\log_p(a) &\in p\mathbb{Z}_p \\
\log_p(ab) &= \log_p(a) + \log_p(b) \\
\log_p(\langle a \rangle) &= \log_p(a) \\
\left|\log_p(\langle a \rangle)\right|_p &= |\langle a \rangle - 1|_p\,,
\end{aligned}$$

wobei $|x|_p$ den p-adischen Betrag von x bezeichnet. Daraus folgen unmittelbar (ii), (iii) und wegen

$$\left|\log_p(1+dp)\right|_p = |dp|_p = p^{-1}$$

auch (i). Weiter folgt

$$\begin{aligned}
& \mathrm{i}(a) \equiv \mathrm{i}(b) && \mod p^n \\
\Longleftrightarrow\quad & \log_p(a) \equiv \log_p(b) && \mod p^{n+1} \\
\Longleftrightarrow\quad & \left|\log_p\left(\frac{a}{b}\right)\right|_p \leq p^{-n-1} && \\
\Longleftrightarrow\quad & \left|\left\langle\frac{a}{b}\right\rangle - 1\right|_p \leq p^{-n-1} && \\
\Longleftrightarrow\quad & \langle a\rangle \equiv \langle b\rangle && \mod p^{n+1}
\end{aligned}$$

und somit (iv). Die Injektivität in (v) ist damit klar und da $\log_p$ stetig ist, trifft dies auch auf i zu. Da $1 + p\mathbb{Z}_p$ kompakt ist, ist das Bild von i abgeschlossen in $\mathbb{Z}_p$. Sei $a \in \mathbb{Z}$. Dann gilt nach (ii)

$$\mathrm{i}\left((1+dp)^a\right) = a\,\mathrm{i}(1+dp) = a.$$

Da $\mathbb{Z}$ in $\mathbb{Z}_p$ dicht ist, folgt die Surjektivität von i. □

4.4 Iwasawa-Potenzreihen

Für der Rest des Kapitels sei θ ein ungerader, primitiver Dirichlet-Charakter mit Führer $f = d$ oder $f = pd$, $(d,p) = 1$, d.h. θ ist ein Charakter der ersten Art (siehe Abschnitt 2.1). $\mathcal{O}_p$ sei der Bewertungsring eines Erweiterungskörpers endlichen Grades von $\mathbb{Q}_p$, der alle Werte von θ enthält. Das maximale Ideal von $\mathcal{O}_p$ werde von π erzeugt.

Das Element

$$\gamma = \mathcal{F}_{1+dp}^{-1} \in \mathrm{G}(\mathbb{Q}(\zeta_{dp^\infty})/\mathbb{Q})$$

ist ein topologischer Erzeuger von Γ, wenn wir Γ in der in Lemma 2.2.2 beschriebenen Weise in $\mathrm{G}(\mathbb{Q}(\zeta_{dp^\infty})/\mathbb{Q})$ einbetten (siehe Lemma 3.2.4). Die Zuordnung $\gamma \mapsto (1+T)$ induziert einen Isomorphismus

$$\varrho : \mathcal{O}_p[\![\Gamma]\!] \longrightarrow \varprojlim_n \mathcal{O}_p[T]/((T+1)^{p^n} - 1) = \mathcal{O}_p[\![T]\!]$$

(siehe Satz 2.3.3). Wir setzen

$$g(T) \stackrel{\text{def}}{=} \varrho(h_\gamma \mathcal{L}_p(\theta, 0)).$$

Ferner schreiben wir abkürzend

$$\omega_n(T) \stackrel{\text{def}}{=} (T+1)^{p^n} - 1.$$

Definition 4.4.1. Für $n \geq 0$ und $a \in \mathbb{Z}$, $(a, dp) = 1$ definieren wir

$$B_n(a) \stackrel{\text{def}}{=} \left[(1 + dp) \left\{ \frac{a}{dp^{n+1}} \right\} \right] - \frac{dp}{2}.$$

Dabei bezeichnen $[y]$ und $\{y\}$ den ganzen, bzw. gebrochenen Anteil von $y \in \mathbb{Q}$ (siehe Definition 3.2.5).

Lemma 4.4.2. *Für alle $n \geq 0$ gilt*

$$g(T) \equiv \sum_{\substack{0 \leqslant a < dp^{n+1} \\ (a,dp)=1}} B_n(a)\theta(a)(1+T)^{-\operatorname{i}(a)-1} \mod \omega_n(T).$$

Beweis. Aus Satz 3.4.6 folgt

$$\mathcal{L}_p(\theta, 0) = p_\theta(\mathcal{L}_{p,S}(\mathbb{Q}(\zeta_{dp^\infty}), \mathbb{1})),$$

wobei die Menge S aus den Primteilern von dp und der archimedischen Stelle besteht und $\mathbb{1}$ den trivialen Charakter bezeichnet. Nun gilt nach Definition 3.3.2

$$p_\theta(h_\gamma \mathcal{L}_{p,S}(\mathbb{Q}(\zeta_{dp^\infty}), \mathbb{1})) = p_\theta(h_\gamma(e_+ - \xi_{dp^\infty})) = -p_\theta(h_\gamma \xi_{dp^\infty}),$$

denn θ ist ungerade, d.h. $p_\theta(e_+) = 0$. Mit Lemma 3.2.6 folgt

$$p_\theta(h_\gamma \xi_{dp^\infty}) \equiv \sum_{\substack{0 \leqslant a < dp^{n+1} \\ (a,dp)=1}} B_n(a) p_\theta(\mathcal{F}_{a(1+dp)}) \mod (\gamma^n - 1).$$

Nach Definition (siehe Abschnitt 2.6) gilt $p_\theta(\mathcal{F}_{a(1+dp)}) = \theta(\mathcal{F}_{a(1+dp)}) p_\Gamma(\mathcal{F}_{a(1+dp)})$. Unserer Konvention zufolge (siehe Abschnitt 2.1) identifizieren wir $\mathcal{F}_{a(1+dp)}$ mittels *rec* mit $a(1 + dp)$ und erhalten

$$\theta(\mathcal{F}_{a(1+dp)}) = \theta(a + adp) = \theta(a),$$

denn der Führer von θ teilt adp. Andererseits ist

$$p_\Gamma(\mathcal{F}^{-1}_{a(1+dp)})\zeta_{p^{n+1}} = \zeta_{p^{n+1}}^{a(1+dp)} = \zeta_{p^{n+1}}^{\langle a \rangle (1+dp)} = \zeta_{p^{n+1}}^{(1+dp)^{\operatorname{i}(a)+1}} = \gamma^{\operatorname{i}(a)+1} \zeta_{p^{n+1}}$$

für alle $n \in \mathbb{N}$ und somit $p_\Gamma(\mathcal{F}_{a(1+dp)}) = \gamma^{-\operatorname{i}(a)-1}$. Die Identifikation $\gamma \mapsto (T + 1)$ liefert nun das Ergebnis. $\square$

Bemerkung 4.4.3. Das $\operatorname{i}(a)$ in [Was89] unterscheidet sich zu dem hier und in [Was97] benutzten durch ein Vorzeichen. Diese unterschiedliche Konvention wurde jedoch in [Was97] bei dem für g auf Seite 381 angegebenen Ausdruck unterschlagen.

4.5 Relationen der Koeffizienten $B_n(a)$

Im Folgenden werden wir einige einfache Rechengesetze für ganze Anteile brauchen, die wir hier zusammenstellen:

Lemma 4.5.1. *Sei $a, b \in \mathbb{Q}$ und $k \in \mathbb{Z}$. Dann gilt:*

(i) $[-a] = \begin{cases} -a & \textit{falls } a \textit{ ganz,} \\ -1 - [a] & \textit{sonst.} \end{cases}$

(ii) $[a + b] = [a] + [b] + [\{a\} + \{b\}]$,

(iii) $\left[\frac{a}{k}\right] = \left[\frac{[a]}{k}\right]$.

Beweis. Zu (i): Es gilt

$$[-a] + \{-a\} = -a = -([a] + \{a\}),$$

also

$$[-a] + [a] = -(\{a\} + \{-a\}).$$

Für $a \in \mathbb{Z}$ verschwindet die rechte Seite, für $a \notin \mathbb{Z}$ ist $0 < \{a\} + \{-a\} < 2$. Da die linke Seite ganz ist, folgt $\{a\} + \{-a\} = 1$.
Zu (ii): Es gilt

$$\begin{aligned} [a + b] + \{a + b\} &= a + b = [a] + \{a\} + [b] + \{b\} \\ &= [a] + [b] + [\{a\} + \{b\}] + \{\{a\} + \{b\}\}\,. \end{aligned}$$

Die Behauptung folgt wegen $\{\{a\} + \{b\}\} = \{a + b\}$.
Zu (iii): Es gilt

$$\left[\frac{a}{k}\right] = \left[\frac{[a] + \{a\}}{k}\right] = \left[\frac{[a]}{k}\right] + \left[\left\{\frac{[a]}{k}\right\} + \frac{\{a\}}{k}\right]$$

nach (ii). Nun gilt $\left\{\frac{[a]}{k}\right\} \le \frac{k-1}{k}$ und $\frac{\{a\}}{k} < \frac{1}{k}$, also

$$\left[\left\{\frac{[a]}{k}\right\} + \frac{\{a\}}{k}\right] = 0.$$

□

Daraus können wir folgende Eigenschaften von $B_n(a)$ ableiten:

Lemma 4.5.2. *Sei $n \ge 0$ und $a, b \in \mathbb{Z}$ mit $(a, dp) = (b, dp) = 1$. Dann gilt*

(i) $B_n(a) = B_n(b)$ *für* $a \equiv b \mod dp^{n+1}$,

(ii) $B_n(-a) = -B_n(a)$,

(iii) $\sum_{k=0}^{p-1} B_{n+1}(a + kdp^{n+1}) = B_n(a)$.

Beweis. (i) ist offensichtlich. Sei in (ii) deshalb o.B.d.A. $0 \leq a < dp^{n+1}$. Mit Hilfe der Regeln (i) und (ii) aus Lemma 4.5.1 folgt

$$\begin{aligned} B_n(-a) = B_n(dp^{n+1} - a) &= \left[\Big(1 + dp\Big)\Big(1 - \frac{a}{dp^{n+1}}\Big)\right] - \frac{dp}{2} \\ &= (1 + dp) + \left[-\frac{(1+dp)a}{dp^{n+1}}\right] - \frac{dp}{2} = \frac{dp}{2} - \left[\frac{(1+dp)a}{dp^{n+1}}\right] = -B_n(a) \end{aligned}$$

und damit (i). Beachte dabei, dass $\frac{(1+dp)a}{dp^{n+1}} \notin \mathbb{Z}$, weil nach Voraussetzung $(a, dp) = 1$.

Wir beweisen nun (iii). Zunächst stellen wir fest, dass

$$\sum_{k=0}^{p-1} B_{n+1}(a + kdp^{n+1}) = \sum_{k=0}^{p-1} B_{n+1}(b + kdp^{n+1})$$

für $a \equiv b \mod dp^{n+1}$: Für jede ganze Zahl k mit $0 \leq k < p$ gibt es genau eine ganze Zahl k' mit $0 \leq k' < p$, so dass $a + kdp^{n+1} \equiv b + k'dp^{n+1} \mod dp^{n+2}$. Nach (i) sind also beide Summen gleich.

Die rechte Seite von (iii) hängt nach (i) ebenfalls nur von der Restklasse von a modulo dp^{n+1} ab. Deshalb können wir o.B.d.A. annehmen, dass $0 \leq a < dp^{n+1}$. Für $z \overset{\mathrm{def}}{=} \frac{a}{dp^{n+1}}$ ist also $0 \leq z < 1$. Es gilt

$$\begin{aligned} \left[\frac{(1+dp)(z+k)}{p}\right] &= \left[\frac{[(1+dp)z + (1+dp)k]}{p}\right] = \left[\frac{[(1+dp)z] + (1+dp)k}{p}\right] \\ &= \left[\frac{(1+dp)z}{p}\right] + \left[\frac{k}{p} + kd\right] + \left[\left\{\frac{[(1+dp)z]}{p}\right\} + \left\{\frac{k}{p} + kd\right\}\right] \\ &= \left[\frac{(1+dp)z}{p}\right] + kd + \left[\frac{c}{p} + \frac{k}{p}\right] \end{aligned}$$

mit

$$c \overset{\mathrm{def}}{=} p\left\{\frac{[(1+dp)z]}{p}\right\} = [(1+dp)z] - p\left[\frac{(1+dp)z}{p}\right].$$

Nun gilt $c < p$ und somit

$$\left[\frac{c+k}{p}\right] = \begin{cases} 0 & \text{wenn } k < p - c, \\ 1 & \text{wenn } k \geq p - c. \end{cases}$$

Daher folgt

$$\begin{aligned} \sum_{k=0}^{p-1} B_{n+1}(a + kdp^{n+1}) &= -\frac{dp^2}{2} + \sum_{k=0}^{p-1}\left[\frac{(1+dp)(a + kdp^{n+1})}{dp^{n+2}}\right] \\ &= -\frac{dp^2}{2} + \sum_{k=0}^{p-1}\left[\frac{(1+dp)(z+k)}{p}\right] \\ &= -\frac{dp^2}{2} + \sum_{k=0}^{p-1}\left(\left[\frac{(1+dp)z}{p}\right] + \frac{dpk}{p} + \left[\frac{c+k}{p}\right]\right) \end{aligned}$$

$$
\begin{aligned}
&= -\frac{dp^2}{2} + p\left[\frac{(1+dp)z}{p}\right] + \frac{dp(p-1)}{2} + c \\
&= -\frac{dp}{2} + [(1+dp)z] = B_n(a)
\end{aligned}
$$

und somit (iii). □

Schließlich betrachten wir noch folgende Relation:

Lemma 4.5.3. *Sei $(1+dp)dp < dp^{n+1}$. Für $0 \leq a < dp^{n+1}$, $(dp, a) = 1$ sei $(1+dp)a \equiv x_a \mod dp^{n+1}$ mit $0 \leq x_a < dp^{n+1}$. Dann gilt*

$$
B_n(a-dp) - B_n(a) = \begin{cases} dp & \text{wenn } a < dp, \\ -1 & \text{wenn } a > dp \text{ und } x_a < (1+dp)dp, \\ 0 & \text{sonst.} \end{cases}
$$

Beweis. Sei zunächst $a < dp$. Dann gilt mit (ii) von Lemma 4.5.2:

$$
\begin{aligned}
B_n(a-dp) - B_n(a) &= -B_n(dp-a) - B_n(a) \\
&= dp - \left[\frac{(1+dp)(dp-a)}{dp^{n+1}}\right] - \left[\frac{(1+dp)a}{dp^{n+1}}\right] = dp,
\end{aligned}
$$

denn die Argumente von $[\cdot]$ sind jeweils kleiner als 1.

Sei nun $a > dp$. Dann gilt mit (ii) von Lemma 4.5.1:

$$
\begin{aligned}
B_n(a-dp) - B_n(a) &= \left[\frac{(1+dp)(a-dp)}{dp^{n+1}}\right] - \left[\frac{(1+dp)a}{dp^{n+1}}\right] \\
= \left[\frac{(1+dp)a}{dp^{n+1}}\right] + \left[-\frac{(1+dp)dp}{dp^{n+1}}\right] &+ \left[\left\{\frac{(1+dp)a}{dp^{n+1}}\right\} + \left\{-\frac{(1+dp)dp}{dp^{n+1}}\right\}\right] - \left[\frac{(1+dp)a}{dp^{n+1}}\right] \\
&= -1 - \left[\frac{(1+dp)dp}{dp^{n+1}}\right] + \left[\frac{x_a}{dp^{n+1}} + \left(1 - \frac{(1+dp)dp}{dp^{n+1}}\right)\right] \\
&= -1 + \left[1 + \frac{x_a - (1+dp)dp}{dp^{n+1}}\right],
\end{aligned}
$$

woraus sich die beiden übrigen Fälle ergeben. □

4.6 Ein Kriterium für das Verschwinden modulo π

Die Aussage des folgenden Lemmas ist zwar beinahe trivial, aber entscheidend für das weitere Vorgehen:

Lemma 4.6.1. *Sei $f(T) \in \mathcal{O}_p[\![T]\!]$. Dann gibt es genau ein Polynom*

$$
f_n(T) = \sum_{k=0}^{p^n-1} a_{k,n}(T+1)^k \in \mathcal{O}_p[T]
$$

mit $f(T) \equiv f_n(T) \mod \omega_n(T)$. Insbesondere gilt $f(T) \equiv 0 \mod \pi$ genau dann, wenn für alle k und n

$$
a_{k,n} \equiv 0 \mod \pi
$$

erfüllt ist.

Beweis. Dies folgt direkt aus dem fundamentalen Isomorphismus

$$\mathcal{O}_p[\![T]\!] \cong \varprojlim_n \mathcal{O}_p[T]/(\omega_n(T))$$

(siehe Satz 2.3.3), denn die Polynome in $(1+T)$ vom Grad kleiner als p^n bilden ein vollständiges Repräsentantensystem von $\mathcal{O}_p[T]/(\omega_n(T))$. $\square$

Beachte dabei, dass die Anordnung der Koeffizienten für die Teilbarkeit durch π keine Rolle spielt. Dies werden wir wie folgt ausnutzen:

Lemma 4.6.2. *Sei $g(T)$ wie in Abschnitt 4.4. Wir nehmen an, dass $g(T) \equiv 0 \mod \pi$. Dann gilt für alle $n \geq 0$ und alle $b \in \mathbb{Z}$:*

$$\sum_{a \in M_b} B_n(a)\theta(a) \equiv 0 \mod \pi,$$

wobei sich die Summe über die Elemente der Menge

$$M_b \overset{\text{def}}{=} \{0 \leq a < dp^{n+1} \mid (a, dp) = 1, \quad \langle a \rangle \equiv b \mod p^{n+1}\}.$$

erstreckt.

Beweis. Nach Lemma 4.4.2 gilt

$$g(T) \equiv \sum_{k=0}^{p^n-1} \Big(\sum_{a \in N_k} B_n(a)\theta(a) \Big) (1+T)^k \mod \omega_n(T)$$

für

$$N_k \overset{\text{def}}{=} \{0 \leq a < dp^{n+1} \mid (a, dp) = 1, \quad -\mathrm{i}(a) - 1 \equiv k \mod p^n\}.$$

Auf die Aussage des Lemmas kommen wir, indem wir die Koeffizienten umordnen: O.B.d.A. gelte $b \in 1 + p\mathbb{Z}$, denn ansonsten ist $M_b = \emptyset$. Nun gibt es nach Lemma 4.3.3.(v) ein k mit $0 \leq k < p^{n+1}$, so dass $-\mathrm{i}(b) - 1 \equiv k \mod p^n$ und nach Lemma 4.3.3.(iv) gilt

$$\begin{aligned} N_k &= \{0 \leq a < dp^{n+1} \mid (a, dp) = 1, \quad \mathrm{i}(a) \equiv \mathrm{i}(b) \mod p^n\} \\ &= \{0 \leq a < dp^{n+1} \mid (a, dp) = 1, \quad \langle a \rangle \equiv b \mod p^{n+1}\} = M_b \end{aligned}$$

Für $g(T) \equiv 0 \mod \pi$ folgt also

$$\sum_{a \in M_b} B_n(a)\theta(a) \equiv 0 \mod \pi$$

nach Lemma 4.6.1. $\square$

4.7 Eine weitere Umformulierung

Die Idee ist nun, mit den Koeffizienten $B_n(a)$ neue Potenzreihen in $\mathcal{O}_p[\![T]\!]$ zu bilden, die sich leichter handhaben lassen. Wir betrachten die folgenden Polynome:

Definition 4.7.1. Sei $\alpha \in \mu_{p-1}$. Setze

$$\tilde{g}_\alpha^n(T) \overset{def}{\equiv} \sum_{\substack{0\leqslant a<dp^{n+1}\\ a\equiv\alpha \bmod p}} B_n(a)\theta(a)(1+T)^{(1+dp)a}.$$

Bemerkung 4.7.2. Beachte, dass nach Konvention $\theta(a) = 0$, falls $d \mid a$. Zusammen mit $a \equiv \alpha \mod p$ erspart dies die Bedingung $(a, dp) = 1$.

Lemma 4.7.3. *Die Folge der $\tilde{g}_\alpha^n$ definiert ein Element $\tilde{g}_\alpha \in \mathcal{O}_p[\![T]\!]$.*

Beweis. Wir müssen zeigen, dass für alle $n \geq 0$ gilt:

$$\tilde{g}_\alpha^{n+1}(T) \equiv \tilde{g}_\alpha^n(T) \mod \omega_n(T).$$

Dies folgt leicht mit Lemma 4.5.2, Punkt (iii):

$$\begin{aligned}
&\sum_{\substack{0\leqslant b<dp^{n+2}\\ b\equiv\alpha \bmod p}} B_n(b)\theta(b)(1+T)^{(1+dp)b} \equiv \\
&\equiv \sum_{\substack{0\leqslant a<dp^{n+1}\\ a\equiv\alpha \bmod p}} \sum_{k=0}^{p-1} B_n(a+kdp^{n+1})\theta(a+kdp^{n+1})(1+T)^{(1+dp)(a+kdp^{n+1})} \\
&\equiv \sum_{\substack{0\leqslant a<dp^{n+1}\\ a\equiv\alpha \bmod p}} B_n(a)\theta(a)(1+T)^{(1+dp)a} \mod \omega_n(T).
\end{aligned}$$

Beachte dabei, dass $(1+T)^a \equiv (1+T)^b \mod \omega_n(T)$ für $a \equiv b \mod p^n$ und dass der Führer von θ gleich d oder dp ist. □

Aus Lemma 4.5.2 und Lemma 4.5.3 ergeben sich nun folgende Eigenschaften:

Lemma 4.7.4. *Es gilt $\tilde{g}_{-\alpha}((1+T)^{-1}-1) = \tilde{g}_\alpha(T)$.*

Beweis. Es reicht, dies modulo $\omega_n(T)$ zu überprüfen. Benutze dazu Lemma 4.5.2, Punkt (ii) und beachte, dass θ ein ungerader Charakter ist. Es gilt

$$\begin{aligned}
&\sum_{\substack{0\leqslant a<dp^{n+1}\\ a\equiv-\alpha \bmod p}} B_n(a)\theta(a)\big(1+\big((1+T)^{-1}-1\big)\big)^{(1+dp)a} \equiv \\
&\equiv \sum_{\substack{0\leqslant a<dp^{n+1}\\ a\equiv-\alpha \bmod p}} B_n(a)\theta(a)(1+T)^{-(1+dp)a} \\
&\equiv \sum_{\substack{0\leqslant b<dp^{n+1}\\ b\equiv\alpha \bmod p}} B_n(-b)\theta(-b)(1+T)^{(1+dp)b} \\
&\equiv \sum_{\substack{0\leqslant b<dp^{n+1}\\ b\equiv\alpha \bmod p}} B_n(b)\theta(b)(1+T)^{(1+dp)b} \mod \omega_n(T)
\end{aligned}$$

und somit die Behauptung. □

Lemma 4.7.5. *Es gilt*

$$\tilde{g}_\alpha(T) = \sum_{\substack{0 \leqslant a < dp \\ a \equiv \alpha \bmod p}} \frac{(1+dp)\theta(a)(1+T)^{a(1+dp)}}{(1+T)^{dp(1+dp)}-1} - \sum_{\substack{0 \leqslant a < dp(1+dp) \\ a \equiv \alpha \bmod p}} \frac{\theta(a)(1+T)^a}{(1+T)^{dp(1+dp)}-1}$$

und somit $\tilde{g}_\alpha(T) \in Q(\mathcal{O}_p[T])$.

Beweis. Mit Lemma 4.5.3 gilt für hinreichend großes n:

$$\begin{aligned}
&((1+T)^{dp(dp+1)}-1)\tilde{g}_\alpha^n(T) \equiv \\
&\equiv \sum_{\substack{0 \leqslant b < dp^{n+1} \\ b \equiv \alpha \bmod p}} B_n(b)\theta(b)(1+T)^{(b+dp)(1+dp)} - \sum_{\substack{0 \leqslant a < dp^{n+1} \\ a \equiv \alpha \bmod p}} B_n(a)\theta(a)(1+T)^{a(1+dp)} \\
&\equiv \sum_{\substack{0 \leqslant a < dp^{n+1} \\ a \equiv \alpha \bmod p}} B_n(a-dp)\theta(a-dp)(1+T)^{a(1+dp)} - \sum_{\substack{0 \leqslant a < dp^{n+1} \\ a \equiv \alpha \bmod p}} B_n(a)\theta(a)(1+T)^{a(1+dp)} \\
&\equiv \sum_{\substack{0 \leqslant a < dp^{n+1} \\ a \equiv \alpha \bmod p}} \big(B_n(a-dp) - B_n(a)\big)\theta(a)(1+T)^{a(1+dp)} \\
&\equiv (1+dp) \sum_{\substack{0 \leqslant a < dp \\ a \equiv \alpha \bmod p}} \theta(a)(1+T)^{a(1+dp)} - \sum_{\substack{0 \leqslant a < dp^{n+1} \\ x_a < (1+dp)dp \\ a \equiv \alpha \bmod p}} \theta(a)(1+T)^{a(dp+1)} \\
&\equiv (1+dp) \sum_{\substack{0 \leqslant a < dp \\ a \equiv \alpha \bmod p}} \theta(a)(1+T)^{a(1+dp)} - \sum_{\substack{0 \leqslant x < dp(dp+1) \\ x \equiv \alpha \bmod p}} \theta(x)(1+T)^{x} \mod \omega_n(T),
\end{aligned}$$

wobei $0 \leq x_a < dp^{n+1}$ jeweils als Repräsentant der Restklasse von $(1+dp)a$ modulo dp^{n+1} gewählt wird. Beachte dabei, dass $a \equiv x_a \mod p$ und $\theta(a) = \theta(x_a)$. □

Das Kriterium aus Lemma 4.6.2 können wir nun wie folgt formulieren:

Lemma 4.7.6. *Sei* $g(T) \equiv 0 \mod \pi$. *Dann gilt:*

$$\sum_{\alpha \in \mu_{p-1}} \tilde{g}_\alpha((1+T)^{\alpha^{-1}}-1) \equiv 0 \mod \pi.$$

Beweis. Es ist

$$\begin{aligned}
\sum_{\alpha \in \mu_{p-1}} \tilde{g}_\alpha((1+T)^{\alpha^{-1}}-1) &\equiv \sum_{\alpha \in \mu_{p-1}} \sum_{\substack{0 \leqslant a < dp^{n+1} \\ a \equiv \alpha \bmod p}} B_n(a)\theta(a)(1+T)^{(1+dp)\alpha^{-1}a} \\
&\equiv \sum_{0 \leqslant b < p^{n+1}} \sum_{a \in M_b} B_n(a)\theta(a)(1+T)^{(1+dp)b} \mod \omega_n(T)
\end{aligned}$$

mit

$$M_b = \{0 \leq a < dp^{n+1} \mid (a, dp) = 1, \quad \langle a \rangle \equiv b \mod p^{n+1}\}.$$

Die Behauptung folgt nun direkt aus Lemma 4.6.2. □

4.8 Abschluss des Beweises

Der Beweis von Theorem 4.2.1 kann mit Hilfe des folgenden rein algebraischen Argumentes schnell zu Ende geführt werden:

Lemma 4.8.1 (W. Sinnot). *Für jede $p-1$-te Einheitswurzel α sei*

$$F_\alpha(T) \in \mathcal{O}_p[\![T]\!] \cap Q(\mathcal{O}_p[T]).$$

Angenommen

$$\sum_{\alpha \in \mu_{p-1}} F_\alpha((1+T)^\alpha - 1) \in \pi \mathcal{O}_p[\![T]\!]$$

Dann gibt es Konstanten $c_\alpha \in \mathcal{O}_p$, so dass

$$F_\alpha(T) + F_{-\alpha}((1+T)^{-1} - 1) \equiv c_\alpha \mod \pi \mathcal{O}_p[\![T]\!].$$

Beweis. Siehe [Was97], Lemma 16.9. □

Beweis von Theorem 4.2.1. Wir nehmen an,

$$\sum_{\alpha \in \mu_{p-1}} \tilde{g}_\alpha((1+T)^{\alpha^{-1}} - 1) \equiv 0 \mod \pi.$$

Nach Lemma 4.7.6 reicht es, diese Annahme zum Widerspruch zu führen. Wende Sinnotts Lemma mit $F_\alpha(T) = \frac{1}{2}\tilde{g}_{\alpha^{-1}}(T)$ an. Nach den in Lemma 4.7.4 beschriebenen Symmetrieeigenschaften folgt

$$\tilde{g}_\alpha(T) = \frac{1}{2}(\tilde{g}_\alpha(T) + \tilde{g}_{-\alpha}((1+T)^{-1} - 1)) \equiv c_\alpha \mod \pi \mathcal{O}_p[\![T]\!].$$

Das kann aber mit Hilfe der Formel für $\tilde{g}_\alpha(T)$ aus Lemma 4.7.5 leicht zum Widerspruch geführt werden: Für $\alpha = 1$ berechnet sich danach der Koeffizient von $(1+T)$ in $((1+T)^{dp(dp+1)} - 1)\tilde{g}_1(T)$ zu

$$-\theta(1) = -1 \not\equiv 0 \mod \pi.$$

Andererseits hat $((1+T)^{dp(dp+1)} - 1)c_1$ als Polynom in $(1+T)$ keinen linearen Term. Also gilt

$$((1+T)^{dp(dp+1)} - 1)\tilde{g}_1(T) \not\equiv ((1+T)^{dp(dp+1)} - 1)c_1 \mod \pi,$$

im Widerspruch zu unserer Annahme. □

4.9 Eine Konsequenz für die äquivariante L-Funktion

Für die äquivariante L-Funktion hat Theorem 4.2.1 folgende Konsequenz:

Folgerung 4.9.1. *Sei S eine endliche Menge von Stellen von $\mathbb{Q}$, die p, ∞ und die in $K_0/\mathbb{Q}$ verzweigten Stellen enthält; $\mathcal{O}_p$ der Bewertungsring eines beliebigen Körpers vom endlichen Grad über $\mathbb{Q}_p$ und $\mathbb{1} : \mathrm{G}_S \longrightarrow \mathcal{O}_p^\times$ der triviale Charakter. Bezeichne ferner*

$$D \in \mathfrak{C}(\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!])$$

den von der äquivarianten L-Funktion $\mathcal{L}_{p,S}(K_\infty, \mathbb{1})$ erzeugten Cartier-Divisor. Ist $\mathfrak{P}$ ein Primideal von $\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$ mit $p \in \mathfrak{P}$, dann gilt

$$\mathfrak{C}(\imath_{\mathfrak{P}})(D) = (1) \in \mathfrak{C}(\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]_{\mathfrak{P}})$$

für die natürliche Lokalisierungsabbildung $\imath_{\mathfrak{P}} : \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!] \longrightarrow \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]_{\mathfrak{P}}$.

Beweis. Sei γ ein topologischer Erzeuger von Γ und $h_\gamma \stackrel{\text{def}}{=} 1 - \varepsilon_\infty(\gamma)\gamma^{-1} \in \Lambda$. Mit Lemma 3.2.6 folgt $h_\gamma \mathcal{L}_{p,S}(K_\infty, \mathbb{1}) \in \mathbb{Z}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$, d.h. wir können $\mathcal{L}_{p,S}(K_\infty, \mathbb{1})$ als

$$\mathcal{L}_{p,S}(K_\infty, \mathbb{1}) = \frac{h_\gamma \mathcal{L}_{p,S}(K_\infty, \mathbb{1})}{h_\gamma}$$

darstellen. Nach Konstruktion von $\mathfrak{C}(\imath_{\mathfrak{P}})$ (siehe Lemma 1.2.6), reicht es zu zeigen, dass

$$\imath_{\mathfrak{P}}(h_\gamma), \imath_{\mathfrak{P}}(h_\gamma \mathcal{L}_{p,S}(K_\infty, \mathbb{1})) \in \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]_{\mathfrak{P}}^\times,$$

d.h. dass beide Elemente nicht in $\mathfrak{P}$ liegen. Wir nehmen zunächst an, dass $\mathcal{O}_p$ die Werte aller Charaktere von $\Delta = \mathrm{G}(K_0/\mathbb{Q})$ enthält und können somit Lemma 2.8.1 anwenden. Danach gibt es einen Charakter $\theta \in \widehat{\Delta}$ mit

$$p_\theta(\mathfrak{P}) = (\pi) \subset \mathcal{O}_p[\![\Gamma]\!],$$

wobei π einen Erzeuger des maximalen Ideals von $\mathcal{O}_p$ bezeichnet. (Beachte, dass Satz 2.3.3 zufolge (π) das einzige Ideal von $\mathcal{O}_p[\![\Gamma]\!]$ der Kodimension 1 ist, welches p enthält.)

Nun ist

$$p_\theta(h_\gamma) = h_\gamma = P(1-\gamma)$$

mit $P(T) = 1 - \varepsilon_\infty(\gamma)(1+T)^{-1} \in \mathbb{Z}_p[\![T]\!]$, also ganz sicher nicht durch π teilbar. Nach Folgerung 3.4.7 gilt ferner

$$p_\theta(h_\gamma \mathcal{L}_{p,S}(K_\infty, \mathbb{1})) = h_\gamma \mathcal{L}_p(\theta, 0) \prod_{l \in S \setminus S'} (1 - p_\theta(\mathcal{F}_l)),$$

mit

$$S' \stackrel{\text{def}}{=} \{\infty\} \cup \{\text{Primteiler von } fp\},$$

im Fall, dass θ ein ungerader Charakter mit Führer f ist. Nach dem Theorem von Ferrero-Washington (siehe Theorem 4.2.1) ist π kein Teiler von $\mathcal{L}_p(\theta, 0)$. Andererseits gilt

$$1 - p_\theta(\mathcal{F}_l) = Q(\gamma - 1)$$

mit $Q(T) = 1 - \theta(l)(1+T)^{-\mathrm{i}(l)} \in \mathbb{Z}_p[\![T]\!]$. Mit Lemma 4.6.1 folgt daher leicht, dass auch $1 - p_\theta(\mathcal{F}_l)$ nicht durch π teilbar ist. Im Fall, dass θ ein gerader Charakter ist, gilt

$$p_\theta(h_\gamma \mathcal{L}_{p,S}(K_\infty, \mathbb{1})) = h_\gamma.$$

Es ist also nichts weiter zu zeigen.

Enthält $\mathcal{O}_p$ nicht alle Werte der Charaktere aus $\widehat{\Delta}$, so wähle einen Bewertungsring $\mathcal{O}'_p$, welcher die Werte enthält. Nach dem Lying-Over-Lemma (siehe [Eis99], Satz 4.15) gibt es ein Primideal $\mathfrak{P}'$ von $\mathcal{O}'_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$ mit $\mathfrak{P}' \cap \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!] = \mathfrak{P}$ und $\operatorname{codim} \mathfrak{P}' = 1$. Da h_γ und $h_\gamma \mathcal{L}_{p,S}(K_\infty, \mathbb{1})$ nicht in $\mathfrak{P}'$ liegen, sind sie auch nicht in $\mathfrak{P}$ enthalten. $\square$

5 Kohomologie von $\mathbb{Z}_p$-Erweiterungen

A. Huber und G. Kings betrachten in ihrer Formulierung der Hauptvermutung der Iwasawa-Theorie für Dirichlet-Charaktere Kohomologie-Gruppen der Form

$$H \stackrel{def}{=} \varprojlim_n \mathrm{H}^k_{\text{ét}}(\operatorname{Spec} \mathcal{O}_{K_n}[p^{-1}], \mathcal{F}).$$

Dabei bezeichnet $\mathrm{H}^k_{\text{ét}}(\operatorname{Spec} \mathcal{O}_{K_n}[N^{-1}], \mathcal{F})$ die étale Kohomologiegruppe einer konstruierbaren $\mathbb{Z}_p$-Garbe $\mathcal{F}$ über dem Schema $\operatorname{Spec} \mathcal{O}_{K_n}[N^{-1}]$.

Die Gruppe H trägt in natürlicher Weise die Struktur eines $\mathbb{Z}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$-Moduls. Teilt p die Ordnung von $\mathrm{G}(K_\infty/\mathbb{Q})$, so ist $\mathbb{Z}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$ kein regulärer Ring. H besitzt dann im Allgemeinen keine endliche projektive Auflösung. Also existiert auch kein charakteristisches Ideal im Sinne von Definition 1.7.6.

Stattdessen soll der entsprechende Komplex in der abgeleiteten Kategorie betrachtet werden. Die Entwicklung des Formalismus einer „abgeleiteten“ Kategorie von étalen $\mathbb{Z}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$-Garben, die für die Konstruktion dieses Komplexes notwendig wäre, ist jedoch technisch recht aufwendig (siehe [Eke90]).

Wir umgehen einen Teil dieses Aufwandes, indem wir étale Kohomologie durch stetige Galois-Kohomologie ersetzen, also den Komplex stetiger Koketten mit Werten in kompakten Galois-Moduln betrachten. In diesem Kapitel erläutern wir diese Konstruktion und untersuchen ihre Eigenschaften.

5.1 Moduln mit stetiger Galois-Operation

Sei Ω eine kompakte und noethersche $\mathbb{Z}_p$-Algebra und G eine pro-endliche Gruppe (nicht notwendig abelsch). Wir führen Bezeichnungen für folgende Kategorien ein:

Notation 5.1.1.

G-Cpt	Kategorie der kompakten Räume mit stetiger G-Operation. Die Morphismen sind stetige G-äquivariante Abbildungen.
$Mod(\Omega)$	Kategorie der Ω-Moduln.
$Mod_{f.g.}(\Omega)$	Unterkategorie von $Mod(\Omega)$ der endlich erzeugten Ω-Moduln.
$Der(\Omega)$	abgeleitete Kategorie der Kategorie $Mod(\Omega)$.

Wir erinnern daran, dass auf jedem Modul der Kategorie $Mod_{f.g.}(\Omega)$ eine kanonische kompakte Topologie gegeben ist, für die alle Homomorphismen stetig sind (siehe Folgerung 2.4.5 und Bemerkung 2.4.3). Bei Bedarf können wir deshalb die Objekte von $Mod_{f.g.}(\Omega)$ als topologische Moduln auffassen. Dies ist dann interessant, wenn wir auf Ω-Moduln zusätzlich eine stetige G-Operation betrachten wollen:

Definition 5.1.2. Die Objekte der Kategorie $G\text{-}Mod_{f.g.}(\Omega)$ seinen endlich erzeugte Ω-Moduln mit ihrer kompakten Topologie, zusammen mit einer stetigen G-Operation durch Ω-Homomorphismen. Die Morphismen sind stetige, G-äquivariante Ω-Homomorphismen.

Lemma 5.1.3. *$G\text{-}Mod_{f.g.}(\Omega)$, $Mod_{f.g.}(\Omega)$ und $Mod(\Omega)$ sind abelsche Kategorien. Ferner sind sie Ω-*linear*: Ist C eine der drei Kategorien und sind X, Y Objekte von C, so trägt die Morphismen-Menge $\mathrm{Hom}_C(X,Y)$ die Struktur eines Ω-Moduls und die Komposition von Morphismen ist bilinear.*

Zum Beweis. Für die Axiome additiver und abelscher Kategorien siehe [GM96], Kap. II, §5. Dass $Mod(\Omega)$ und $Mod_{f.g.}(\Omega)$ (für Ω noethersch) abelsch und Ω-linear sind, ist eine bekannte Tatsache. Der Fall $G\text{-}Mod_{f.g.}(\Omega)$ lässt sich andererseits leicht darauf zurückführen. So sind $\mathrm{Ker}\, f$ und $\mathrm{Coker}\, f$ eines stetigen G-äquivarianten Ω-Homomorphismus $f : M \longrightarrow N$ gerade der Kern bzw. Kokern in der Kategorie $Mod_{f.g.}(\Omega)$, ausgestattet mit ihrer kompakten Topologie und der induzierten G-Operation. Die Stetigkeit dieser Operation folgt aus der Kompaktheit der betrachteten Moduln. Die Isomorphie von Bild und Kobild in $G\text{-}Mod_{f.g.}(\Omega)$ ist dann eine direkte Konsequenz der entsprechenden Isomorphie in $Mod_{f.g.}(\Omega)$. □

Bemerkung 5.1.4. $G\text{-}Mod_{f.g.}(\Omega)$ ist eine Unter-Kategorie der Kategorie der kompakten $\Omega[\![G]\!]$-Links-Moduln. Letztere ist auch dann noch abelsch, wenn Ω nicht noethersch ist (siehe [NSW00], Kap. V, § 2). Die in Abschnitt 5.2 bis Abschnitt 5.5 vorgestellten Ergebnisse dürften sich ohne weiteres auf Moduln dieser Kategorie ausdehnen lassen, wobei man in Abschnitt 5.5 das gewöhnliche Tensorprodukt durch das komplettierte Tensorprodukt ersetzen muss.

Die Idee ist jedoch, dass, falls $G = \pi_1(X, \bar{x})$ die étale Fundamentalgruppe eines Schemas X bezeichnet, auf dem p invertierbar ist, $G\text{-}Mod_{f.g.}(\Omega)$ äquivalent zu der geeignet definierten Kategorie glatter und konstruierbarer Ω-Garben sein sollte. Ist Ω eine endliche Erweiterung von $\mathbb{Z}_p$, so ist dies eine wohlbekannte Tatsache (siehe [KW01], Anhang A).

5.2 Stetige Galois-Kohomologie

Die Kategorie $G\text{-}Mod_{f.g.}(\Omega)$ ist zwar abelsch, hat aber nicht genügend injektive Objekte. Die Konstruktion von rechts-abgeleiteten Funktoren ist deshalb nicht ohne weiteres möglich. Stattdessen ordnen wir jedem Modul in $G\text{-}Mod_{f.g.}(\Omega)$ direkt den Koketten-Komplex der stetigen Galois-Kohomologie in der abgeleiteten Kategorie der Ω-Moduln zu. Stetige Galois-Kohomologie wurde von J. Tate in [Tat76] eingeführt. Wir folgen hier größtenteils der Darstellung in [NSW00], Kap. II, §3.

Sei M ein Modul in $G\text{-}Mod_{f.g.}(\Omega)$ und $n \geq 0$. Setze

$$C^n(G,M) \stackrel{def}{=} \mathrm{Hom}_{G\text{-}Cpt}(G^{n+1}, M).$$

Mit der Operation

$$\Omega \times C^n(G,M) \to C^n(G,M), \quad (a,x) \mapsto ax, \qquad (ax)(v) \stackrel{def}{=} a(x(v)), \quad v \in G^{n+1}$$

wird $C^n(G,M)$ zu einem Ω-Modul. Einem G-$Mod_{f.g.}(\Omega)$-Morphismus $f : M \longrightarrow N$ wird die Ω-lineare *induzierte Abbildung*

$$f_*^n : C^n(G,M) \longrightarrow C^n(G,N), \qquad x \mapsto f \circ x$$

zugeordnet. Wir erhalten somit einen Funktor

$$C^n(G,\cdot) : G\text{-}Mod_{f.g.}(\Omega) \longrightarrow Mod(\Omega).$$

Für alle $n \geq 0$ ist dieser Funktor Ω-*linear*, d.h. für Moduln X, Y der Kategorie G-$Mod_{f.g.}(\Omega)$ ist die Abbildung

$$\mathrm{Hom}_{G\text{-}Mod_{f.g.}(\Omega)}(X,Y) \longrightarrow \mathrm{Hom}_{Mod(\Omega)}(C^n(G,X), C^n(G,Y)), \qquad f \mapsto f_*$$

ein Ω-Homomorphismus.

Sei $n \geq 0$ und M ein Modul aus G-$Mod_{f.g.}(\Omega)$. Setze

$$\partial^n : C^n(G,M) \longrightarrow C^{n+1}(G,M) \qquad x \mapsto \partial^n x.$$

Dabei ist $\partial^n x$ auf dem Tupel $(v_0, \ldots, v_{n+1}) \in G^{n+2}$ durch

$$\partial^n x(v_0, \ldots, v_{n+1}) \overset{\text{def}}{=} \sum_{i=0}^{n+1} (-1)^i x(v_0, \ldots, \widehat{v_i}, \ldots, v_{n+1})$$

gegeben. (Mit $\widehat{v_i}$ deuten wir an, dass im Tupel $(v_0, \ldots, \widehat{v_i}, \ldots, v_{n+1})$ das Element v_i ausgelassen wurde.)

Man prüft schnell nach, dass die Abbildungen ∂^n ebenfalls Ω-linear sind und als natürliche Transformationen der Funktoren $C^n(G,\cdot)$ aufgefasst werden können, d.h. ∂^n kommutiert mit den induzierten Abbildungen. Ferner gilt $\partial^{n+1} \circ \partial^n = 0$, d.h.

$$C^0(G,M) \xrightarrow{\partial^0} C^1(G,M) \xrightarrow{\partial^1} C^2(G,M) \xrightarrow{\partial^2} \cdots$$

ist ein Komplex. Wir fassen ihn als ein Objekt der abgeleiteten Kategorie von $Mod(\Omega)$ auf und erhalten somit einen Funktor

$$C^\bullet(G,\cdot) : G\text{-}Mod_{f.g.}(\Omega) \longrightarrow Der(\Omega).$$

Definition 5.2.1. Sei M ein Modul in G-$Mod_{f.g.}(\Omega)$. Dann heißt $C^\bullet(G,M)$ *stetiger (homogener) Koketten-Komplex* (mit Ω-Modul-Struktur). Der Kohomologie-Modul

$$\mathrm{H}^n(G,M) \overset{\text{def}}{=} \mathrm{H}^n\, C^\bullet(G,M)$$

heißt *n-te stetige Galois-Kohomologie.*

Es gilt $\mathrm{H}^0(G,M) = M^G$, denn auf der einen Seite ist jeder Kozykel $c \in \operatorname{Ker} \partial^0$ konstant und G-äquivariant, kann also mit einem Element von M^G identifiziert werden; auf der anderen Seite ist jede konstante Funktion $G \longrightarrow M$ stetig (da M kompakt, also ein Hausdorff-Raum ist) und genau dann G-äquivariant, wenn der Wert der Funktion in M^G liegt.

Ist M ein endlicher Modul in G-$Mod_{f.g.}(\Omega)$, so ist stetige Galois-Kohomologie mit Werten in M gleich der üblichen Galois-Kohomologie (siehe [NSW00], Kap. II, § 3), denn die kompakte Topologie eines endlichen Moduls ist diskret.

5.3 Exaktheit von $C^n(G,\cdot)$

Stetige Galois-Kohomologie kann allgemeiner für jeden topologischen G-Modul definiert werden. Eine lange exakte Kohomologie-Sequenz existiert jedoch nur unter einschränkenden Bedingungen (wesentlich ist dabei die Existenz eines stetigen Schnitts). Folgendes Lemma zeigt, dass diese Bedingungen für die von uns betrachteten Moduln stets erfüllt sind:

Lemma 5.3.1. *Für alle $n \geq 0$ ist $C^n(G,\cdot)$ ein exakter Funktor.*

Beweis. Betrachte eine kurze exakte Sequenz in $G\text{-}Mod_{f.g.}(\Omega)$:

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0.$$

Es ist leicht zu sehen, dass $f_*^n : C^n(G,M') \longrightarrow C^n(G,M)$ injektiv ist und dass $\operatorname{Im} f_*^n \subset \operatorname{Ker} g_*^n$ gilt. Wir zeigen $\operatorname{Ker} g_*^n \subset \operatorname{Im} f_*^n$: Sei $v \in G^{n+1}$ und $x \in \operatorname{Ker} g_*^n$. Dann ist $g \circ x(v) = 0$, d.h. $x(v) \in \operatorname{Ker} g = \operatorname{Im} f$. Da $\operatorname{Ker} g$ abgeschlossen ist, ist die Einschränkung $x : G^{n+1} \longrightarrow \operatorname{Im} f$ stetig. Aus der Kompaktheit der Moduln und der Injektivität von f folgt, dass die Einschränkung $f : M' \longrightarrow \operatorname{Im} f$ ein Homöomorphismus ist. Setze $y \stackrel{def}{=} f^{-1} \circ x$. Die Abbildung $y : G^{n+1} \longrightarrow M'$ ist offensichtlich stetig. Weil f G-äquivariant ist, trifft dies auch auf f^{-1} und somit auf y zu. Darum gilt $y \in C^n(G,M')$. Nun ist y ein Urbild von x unter f_*^n, also $\operatorname{Im} f_*^n = \operatorname{Ker} g_*^n$.

Wir zeigen nun die Surjektivität von g_*^n. Da die Moduln M und M'' als Gruppen pro-endlich sind, existiert eine stetige Abbildung (nicht notwendig ein Homomorphismus) $s : M'' \longrightarrow N$ mit $g \circ s = id$ (siehe [Ser64], Kap. I, Satz 1). Sei $x \in C^n(G,M'')$ und $v \stackrel{def}{=} (v_0,\ldots,v_n) \in G^{n+1}$. Setze

$$y(v) \stackrel{def}{=} v_0 s(x(v_0^{-1}v)).$$

$y : G^{n+1} \longrightarrow M$ ist als Zusammensetzung der stetigen Abbildungen

$$\begin{array}{ccccccc}
G^{n+1} & \longrightarrow & G \times G^{n+1} & \longrightarrow & G \times G^{n+1} & \longrightarrow & G \times M & \longrightarrow & M \\
v & \longmapsto & (v_0, v) & & (v_0,u) & \longmapsto & (v_0, s \circ x(u)) & & \\
 & & (v_0,v) & \longmapsto & (v_0, v_0^{-1}v) & & (v_0,m) & \longmapsto & v_0 m
\end{array}$$

stetig und offensichtlich G-äquivariant. Also gilt $y \in C^n(G,M)$. Nach Konstruktion ist y ein Urbild von x. Somit ist alles bewiesen. □

Aus diesem Lemma folgt leicht, dass man einer kurzen exakten Sequenz von Moduln aus $G\text{-}Mod_{f.g.}(\Omega)$ kanonisch ein ausgezeichnetes Dreieck in $Der(\Omega)$ zuordnen kann:

Folgerung 5.3.2. *Jede kurze exakte Sequenz in $G\text{-}Mod_{f.g.}(\Omega)$*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

induziert ein ausgezeichnetes Dreieck

$$C^\bullet(G,M') \xrightarrow{f_*} C^\bullet(G,M) \xrightarrow{g_*} C^\bullet(G,M'') \xrightarrow{\delta} C^\bullet(G,M')[1]$$

in $Der(\Omega)$.

Beweis. Nach Lemma 5.3.1 erhalten wir ein exaktes Tripel von Komplexen

$$0 \longrightarrow C^\bullet(G, M') \xrightarrow{f_*} C^\bullet(G, M) \xrightarrow{g_*} C^\bullet(G, M'') \longrightarrow 0.$$

Es ist bekannt, dass jedes solches Tripel kanonisch zu einem ausgezeichneten Dreieck vervollständigt werden kann (siehe [GM96], Prop. 3.3.5). □

Jedes ausgezeichnete Dreieck in $Der(\Omega)$ gibt nun wiederum Anlass zu einer langen exakten Kohomologie-Sequenz (siehe [GM96], Theorem 3.3.6).

5.4 Endliche kohomologische Dimension

Definition 5.4.1. Sei G eine pro-endliche Gruppe. Die *kohomologische Dimension* von G ist die kleinste ganze Zahl k, so dass für alle $n > k$ und alle Moduln M in $G\text{-}Mod_{f.g.}(\Omega)$ gilt:

$$\mathrm{H}^n(G, M) = 0.$$

Wir zeigen in diesem Abschnitt, dass man für Gruppen G endlicher kohomologischer Dimension den Komplex $C^\bullet(G, M)$ durch einen beidseitig beschränkten Komplex ersetzen kann.

Für $n \geq 0$ sei

$$Z^n(G, \cdot) = \operatorname{Ker} C^n(G, \cdot) \xrightarrow{\partial^n} C^{n+1}(G, \cdot).$$

Der Funktor $Z^n(G, \cdot)$ ist ebenfalls Ω-linear, im Allgemeinen jedoch nur links-exakt.

Lemma 5.4.2. *G habe kohomologische Dimension k. Dann ist der Funktor $Z^k(G, \cdot)$ exakt und für jeden Modul M aus $G\text{-}Mod_{f.g.}(\Omega)$ ist der natürliche Homomorphismus von Komplexen*

$$\begin{tikzcd}
\cdots \arrow[r, "\partial^{k-2}"] & C^{k-1}(G,M) \arrow[r, "\partial^{k-1}"] \arrow[d, "="'] & Z^k(G,M) \arrow[r] \arrow[d, hook] & 0 \arrow[r] \arrow[d, hook] & \cdots \\
\cdots \arrow[r, "\partial^{k-2}"] & C^{k-1}(G,M) \arrow[r, "\partial^{k-1}"] & C^k(G,M) \arrow[r, "\partial^k"] & C^{k+1}(G,M) \arrow[r, "\partial^{k+1}"] & \cdots
\end{tikzcd}$$

ein Quasi-Isomorphismus.

Beweis. Nach Voraussetzung gilt $\mathrm{H}^n(G, M) = 0$ für $n > k$, also induziert obiger Komplex-Homomorphismus einen Isomorphismus auf der Kohomologie und ist somit ein Quasi-Isomorphismus.

Andererseits gilt danach auch $Z^{k+1}(G, M) = \operatorname{Im} \partial^k$. Für eine kurze exakte Sequenz in $G\text{-}Mod_{f.g.}(\Omega)$

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

erhalten wir ein kommutatives Diagramm mit exakten Zeilen und Spalten

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & Z^k(G,M') \arrow[r, "f_*^k"] \arrow[d] & Z^k(G,M) \arrow[r, "g_*^k"] \arrow[d] & Z^k(G,M'') \arrow[d] & \\
0 \arrow[r] & C^k(G,M') \arrow[r, "f_*^k"] \arrow[d, "\partial^k"'] & C^k(G,M) \arrow[r, "g_*^k"] \arrow[d, "\partial^k"'] & C^k(G,M'') \arrow[r] \arrow[d, "\partial^k"'] & 0 \\
0 \arrow[r] & Z^{k+1}(G,M') \arrow[r, "f_*^{k+1}"] \arrow[d] & Z^{k+1}(G,M) \arrow[r, "g_*^{k+1}"] \arrow[d] & Z^{k+1}(G,M'') \arrow[d] & \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Eine Diagramm-Jagd oder das Schlangen-Lemma zeigen nun, dass

$$g_*^k : Z^k(G,M) \longrightarrow Z^k(G,M'')$$

surjektiv ist. □

5.5 Tensorprodukte und Koeffizientenerweiterungen

In diesem Abschnitt definieren wir zunächst ein Tensorprodukt

$$G\text{-}Mod_{f.g.}(\Omega) \times Mod_{f.g.}(\Omega) \longrightarrow G\text{-}Mod_{f.g.}(\Omega)$$

und zeigen dann, dass das Tensorprodukt mit dem Funktor $C^\bullet(G,\cdot)$ vertauscht. Insbesondere trifft dies auf die Koeffizientenerweiterung eines Moduls (siehe Definition 1.1.2) mittels eines endlichen Ringhomomorphismus zu.

Für Moduln M aus $G\text{-}Mod_{f.g.}(\Omega)$ und N aus $Mod_{f.g.}(\Omega)$ statten wir den Modul $M \otimes_\Omega N$ (das Tensorprodukt in $Mod_{f.g.}(\Omega)$) mit der G-Operation

$$G \times (M \otimes_\Omega N) \longrightarrow M \otimes_\Omega N \qquad (g, m \otimes n) \mapsto (gm) \otimes n$$

und seiner kompakten Topologie aus. Man sieht leicht, dass die vom Tensorprodukt induzierten Homomorphismen für diese Operation G-äquivariant sind.

Nicht ganz offensichtlich ist die Stetigkeit der so definierten G-Operation: Wir nehmen zunächst an, $N = \Omega^n$ ist frei. Dann ist der natürliche Isomorphismus

$$M \otimes_\Omega \Omega^n \xrightarrow{\cong} M^n, \qquad m \otimes (n_i)_{i=1}^n \mapsto (n_i m)_{i=1}^n$$

G-äquivariant (und stetig), also muss die oben definierte Operation auf $M \otimes_\Omega \Omega^n$ stetig sein. Für allgemeines N zeigt die Wahl einer endlichen freien Präsentation

$$F_1 \xrightarrow{f} F_0 \longrightarrow N \longrightarrow 0,$$

dass die Operation auf $M \otimes_\Omega N \cong \mathrm{Coker}(id \otimes f)$ ebenfalls stetig sein muss: $id \otimes f$ ist offensichtlich G-äquivariant. Da nach Lemma 5.1.3 G-$Mod_{f.g.}(\Omega)$ eine abelsche Kategorie ist, ist $\mathrm{Coker}(id \otimes f)$ ein Objekt von G-$Mod_{f.g.}(\Omega)$.

Wir erhalten also einen rechtsexakten Bifunktor

$$G\text{-}Mod_{f.g.}(\Omega) \times Mod_{f.g.}(\Omega) \longrightarrow G\text{-}Mod_{f.g.}(\Omega) \qquad (M,N) \mapsto M \otimes_\Omega N.$$

Da $Mod_{f.g.}(\Omega)$ genügend projektive Objekte besitzt, existieren die (klassischen) linksabgeleiteten Funktoren

$$\mathrm{Tor}_i^\Omega(M,\cdot) : Mod_{f.g.}(\Omega) \longrightarrow G\text{-}Mod_{f.g.}(\Omega).$$

Ist $P^\bullet$ eine projektive Auflösung des Moduls N aus $Mod_{f.g.}(\Omega)$, so ist

$$\mathrm{Tor}_i^\Omega(M,N) = \mathrm{H}^{-i}(M \otimes_\Omega P^\bullet).$$

Als Ω-Moduln stimmen die $\mathrm{Tor}_i^\Omega(M,N)$ offensichtlich mit den Linksableitungen des gewöhnlichen Tensorprodukts überein. Sie tragen nun aber zusätzlich eine stetige G-Operation.

Wir untersuchen das Vertauschen mit den Funktoren $C^n(G,\cdot)$.

Lemma 5.5.1. *Sei M ein Modul aus G-$Mod_{f.g.}(\Omega)$, N ein Modul aus $Mod_{f.g.}(\Omega)$. Dann gilt:*

(i) Für alle natürlichen Zahlen $k, i \geq 0$ existiert ein natürlicher Isomorphismus von Bifunktoren

$$\alpha_i^k : \mathrm{Tor}_i^\Omega(C^k(G,M),N) \longrightarrow C^k(G,\mathrm{Tor}_i^\Omega(M,N))$$

und es gilt $\partial^k \circ \alpha_i^k = \alpha_i^{k+1} \circ \mathrm{Tor}_i^\Omega(\partial^k)$.

(ii) Ist M als Ω-Modul flach, so sind auch die Ω-Moduln $C^k(G,M)$ flach.

(iii) Hat G endliche kohomologische Dimension d, so gelten die Aussagen (i) und (ii) auch für $Z^d(G,M)$ anstelle von $C^d(G,M)$.

Beweis. Zu (i): Für jedes $n \in N$ ist die Abbildung

$$\bar{n} : M \mapsto M \otimes_\Omega N \qquad m \mapsto m \otimes n$$

ein G-äquivarianter Ω-Homomorphismus. Die Abbildung

$$C^k(G,M) \times N \longrightarrow C^k(G, M \otimes_\Omega N) \qquad (x,n) \mapsto \bar{n}_*^k(x)$$

ist Ω-bilinear. (Die Linearität in x ist klar, die Linearität in n folgt sofort aus der Ω-Linearität des Funktors $C^k(G,\cdot)$.) Somit induziert sie einen Ω-Homomorphismus

$$\alpha_0^k : C^k(G,M) \otimes_\Omega N \longrightarrow C^k(G, M \otimes_\Omega N).$$

Man prüft schnell nach, dass α_0^k eine funktorielle Transformation ist und mit den Differentialen ∂^k vertauscht.

Betrachte nun zunächst freie Moduln Ω^r. Beachte, dass $C^k(G, \cdot)$ als Ω-linearer Funktor mit endlichen direkten Summen vertauscht. Es gibt daher natürliche Isomorphismen

$$C^k(G, M) \otimes_\Omega \Omega^r \cong (C^k(G, M))^r \cong C^k(G, M^r) \cong C^k(G, M \otimes_\Omega \Omega^r).$$

Man überzeugt sich leicht, dass die Zusammensetzung dieser Isomorphismen gleich α_0^k ist.

Sei nun $F^\bullet$ eine freie Auflösung von N. Wir erhalten nach dem eben Gezeigten einen Isomorphismus von Komplexen

$$\alpha^k : C^k(G, M) \otimes_\Omega F^\bullet \longrightarrow C^k(G, M \otimes_\Omega F^\bullet).$$

Da der Funktor $C^k(G, \cdot)$ exakt ist, wird durch Übergang zur Kohomologie der Komplexe ein Isomorphismus

$$\begin{aligned} \alpha_i^k : \operatorname{Tor}_i^\Omega(C^k(G, M), N) = \\ = \mathrm{H}^{-i}(C^k(G, M) \otimes_\Omega F^\bullet) \xrightarrow{\cong} \mathrm{H}^{-i}(C^k(G, M \otimes_\Omega F^\bullet)) = \\ = C^k(G, \mathrm{H}^{-i}(M \otimes_\Omega F^\bullet)) = C^k(G, \operatorname{Tor}_i^\Omega(M, N)) \end{aligned}$$

induziert. Dieser Isomorphismus erfüllt offensichtlich die oben angeführten Bedingungen.

Zu (ii): Ein Ω-Modul M ist flach genau dann, wenn für alle endlich erzeugten Ω-Moduln N und alle $i > 0$ gilt: $\operatorname{Tor}_i^\Omega(M, N) = 0$ (siehe [Eis99],Prop. 6.1). Mit (i) folgt daraus sofort die Behauptung.

Zu (iii): Die Ergebnisse von Lemma 5.4.2 zeigen, dass sich die Argumente aus (i) und (ii) direkt übertragen lassen. □

Wir wollen nun zeigen, dass $C^\bullet(G, \cdot)$ mit dem abgeleiteten Tensorprodukt $\otimes_\Omega^\mathbb{L}$ und mit Koeffizentenerweiterungen vertauscht. Wir beschränken uns dabei auf den für uns wichtigen Spezialfall.

Sei Ω' eine weitere kompakte und noethersche $\mathbb{Z}_p$-Algebra und $\phi : \Omega \longrightarrow \Omega'$ ein endlicher und stetiger Ring-Homomorphismus. Als Koeffizientenerweiterung eines Moduls M aus $G\text{-}Mod_{f.g.}(\Omega)$ mittels ϕ bezeichnen wir den Modul

$$\phi_* M \stackrel{\mathit{def}}{=} M \otimes_\Omega \Omega'$$

aus $G\text{-}Mod_{f.g.}(\Omega')$. Entsprechend bezeichnen wir den links-abgeleiteten Funktor der Koeffizientenerweiterung von Ω-Moduln (siehe auch Abschnitt 1.5):

$$\mathbf{L}\phi_* : Der(\Omega) \longrightarrow Der(\Omega') \qquad C^\bullet \mapsto C^\bullet \otimes_\Omega^\mathbb{L} \Omega'.$$

Satz 5.5.2. *Sei G von endlicher kohomologischer Dimension. P sei ein Modul aus $G\text{-}Mod_{f.g.}(\Omega)$, der als Ω-Modul flach ist.*

(i) Sei M ein endlich erzeugter Ω-Modul. Dann gilt

$$C^\bullet(G, P) \otimes_\Omega^\mathbb{L} M = C^\bullet(G, P \otimes_\Omega M).$$

(ii) Sei $\phi : \Omega \longrightarrow \Omega'$ ein stetiger und endlicher Ring-Homomorphismus. Dann gilt

$$\mathbf{L}\phi_* C^\bullet(G, P) = C^\bullet(G, \phi_* P).$$

Beweis. Um das abgeleitete Tensorprodukt zu berechnen, müssen wir $C^\bullet(G, P)$ durch einen quasi-isomorphen, nach oben beschränkten Komplex von flachen Ω-Moduln ersetzen. Da G von endlicher kohomologischer Dimension ist, liefert Lemma 5.4.2 einen solchen. Alles andere folgt aus Lemma 5.5.1. □

Bemerkung 5.5.3. Als Modell für die Ergebnisse dieses Abschnitts diente [Kat93], Prop. 4.17 (der dort gegebene Beweis ist jedoch nicht ganz korrekt) und [Har77], Kap. III, § 12. Die Methoden gehen ursprünglich auf A. Grothendieck zurück.

5.6 Eingeschränkte Verzweigung

Im Folgenden wollen wir die Betrachtung allgemeiner pro-endlichen Gruppen auf die für uns interessanten Fälle spezialisieren. Sei K ein abelscher Zahlkörper. Wir führen folgende Bezeichnungen ein:

Notation 5.6.1.

p	eine ungerade Primzahl.
S	eine endliche Menge von Stellen von K, die alle über p liegenden Stellen und die archimedischen Stellen enthält.
K_S	die maximale außerhalb S unverzweigte Erweiterung von K.

Ferner bezeichnen wir mit

$$\mathrm{G}_S(K) \overset{def}{=} \mathrm{G}(K_S/K)$$

die (pro-endliche) Galois-Gruppe der maximalen außerhalb von S unverzweigten Erweiterung K_S/K. Ist $K = \mathbb{Q}$ so schreiben wir abkürzend

$$\mathrm{G}_S \overset{def}{=} \mathrm{G}_S(\mathbb{Q}).$$

Die pro-endlichen Gruppen $\mathrm{G}_S(K)$ haben folgende wichtige zusätzliche Eigenschaft:

Satz 5.6.2. *Sei M ein Modul von endlicher Kardinalität in $\mathrm{G}_S(K)$-$Mod_{f.g.}(\Omega)$. Dann sind die Kohomologie-Moduln $\mathrm{H}^n(\mathrm{G}_S(K), M)$ für alle $n \geq 0$ endlich und trivial für $n > 2$.*

Beweis. Da M ein endlicher Ω-Modul ist und Ω eine $\mathbb{Z}_p$-Algebra, ist die Ordnung von M eine Potenz von p und wir hatten vorausgesetzt, dass $p \in S$. Der Satz folgt nun aus [NSW00], Satz 8.3.17 und Theorem 8.3.19. □

Für den folgenden Satz müssen wir zusätzlich fordern, dass Ω als projektiver Limes über ein durch $\mathbb{N}$ (mit der natürlichen Ordnung) indiziertes inverses System

$$\cdots \longrightarrow \Omega_2 \longrightarrow \Omega_1 \longrightarrow \Omega_0$$

von kompakten $\mathbb{Z}_p$-Algebren endlicher Kardinalität Ω_i dargestellt werden kann. Eine genaue Analyse des Beweises würde jedoch wahrscheinlich zeigen, dass diese Voraussetzung unnötig ist.

Satz 5.6.3. *Für $i \in \mathbb{N}$ sei Ω_i eine kompakte $\mathbb{Z}_p$-Algebra endlicher Kardinalität,*

$$\Omega \overset{def}{=} \varprojlim_{i \in \mathbb{N}} \Omega_i,$$

und M ein Modul in $\mathrm{G}_S(K)$-$Mod_{f.g.}(\Omega)$. Dann gilt für alle $n \geq 0$:

$$\mathrm{H}^n(\mathrm{G}_S(K), M) = \varprojlim_{i \in \mathbb{N}} \mathrm{H}^n(\mathrm{G}_S(K), M \otimes_\Omega \Omega_i).$$

Zum Beweis. Nach Lemma 2.4.4 gilt

$$M = \varprojlim_{i \in \mathbb{N}} M \otimes_\Omega \Omega_i$$

und da M über Ω endlich erzeugt ist, ist $M \otimes_\Omega \Omega_i$ für alle $i \in \mathbb{N}$ von endlicher Kardinalität. Mit Satz 5.6.2 folgt aus [NSW00], Cor. 2.3.5 obige Gleichheit in der Kategorie abelscher Gruppen. Man prüft jedoch leicht nach, dass die dabei verwendete Identifikation ein Ω-Homomorphismus ist. □

Wir setzen nun voraus, dass Ω eine endliche Erweiterung der Iwasawa-Algebra Λ ist. Dann erfüllt Ω die Voraussetzung von Satz 5.6.3: Mit Λ (siehe Satz 2.3.3) ist auch Ω noethersch. Da Ω als Λ-Modul endlich erzeugt ist, hat $\Omega \otimes_\Lambda \mathbb{Z}/(p^i)[\Gamma_i]$ endliche Kardinalität und nach Lemma 2.4.4 gilt:

$$\Omega = \varprojlim_{i \in \mathbb{N}} \Omega \otimes_\Lambda \mathbb{Z}/(p^i)[\Gamma_i].$$

Satz 5.6.4. *Sei Ω eine endliche Erweiterung von Λ. Dann sind die Kohomologie-Moduln $\mathrm{H}^n(\mathrm{G}_S(K), M)$ für jeden Modul M aus $\mathrm{G}_S(K)$-$Mod_{f.g.}(\Omega)$ über Ω endlich erzeugt.*

Beweis. Es reicht zu zeigen, dass $\mathrm{H}^n(\mathrm{G}_S(K), M)$ über Λ endlich erzeugt ist. Für $n = 0$ folgt dies sofort, da M über Ω und somit über Λ endlich erzeugt ist und $\mathrm{H}^0(\mathrm{G}_S(K), M) = M^{\mathrm{G}_S(K)}$ ein Untermodul von M ist. Sei also $n = 1$ oder $n = 2$.

Nach Satz 5.6.3 ist $\mathrm{H}^n(\mathrm{G}_S(K), M)$ projektiver Limes von Λ-Moduln endlicher Kardinalität. Mit der entsprechenden pro-endlichen Topologie ist $\mathrm{H}^n(\mathrm{G}_S(K), M)$ kompakt.

Sei $k \cong \mathbb{Z}/(p)$ der Restklassenkörper von Λ. Nach dem topologischen Nakayama-Lemma (siehe [Was97], Lemma 13.6) ist ein kompakter Λ-Modul N endlich erzeugt, wenn $N \otimes_\Lambda k$ endlich ist. Wir müssen uns also von der Endlichkeit des Moduls $\mathrm{H}^n(\mathrm{G}_S(K), M) \otimes_\Lambda k$ überzeugen. Da M als Λ-Modul endlich erzeugt ist, sind andererseits die Moduln $\mathrm{Tor}_i^\Lambda(M, k)$ für alle $i \geq 0$ endlich (ersetze M durch eine Auflösung mit endlich erzeugten, freien Λ-Moduln). Nach Satz 5.6.2 wissen wir damit, dass $\mathrm{H}^n(\mathrm{G}_S(K), \mathrm{Tor}_i^\Lambda(M, k))$ endlich ist.

Da Λ ein lokaler regulärer Ring der Dimension 2 ist (siehe Satz 2.3.3), besitzt jeder endlich erzeugte Modul über Λ eine freie Auflösung der Länge 2 (siehe [Eis99], Cor. 19.3 und Cor. 19.6), d.h. es gibt einen Komplex $F^\bullet$ bestehend aus endlich erzeugten, freien Λ-Moduln, so dass $F^{-i} = 0$ für $i > 2$ und die Sequenz

$$0 \longrightarrow F^{-2} \longrightarrow F^{-1} \longrightarrow F^0 \longrightarrow k \longrightarrow 0$$

exakt ist.

Betrachte den Doppelkomplex $C^\bullet(\mathrm{G}_S(K), M) \otimes_\Lambda F^\bullet$. Dieser liefert uns nach Lemma 5.5.1 Spektralsequenzen

$$\begin{aligned}\mathrm{Tor}^\Lambda_{-i}(\mathrm{H}^j(\mathrm{G}_S(K), M), k) &\Rightarrow \mathrm{H}^{i+j}(C^\bullet(\mathrm{G}_S(K), M) \otimes^{\mathbb{L}}_\Lambda k)\\ \mathrm{H}^j(\mathrm{G}_S(K), \mathrm{Tor}^\Lambda_{-i}(M, k)) &\Rightarrow \mathrm{H}^{i+j}(C^\bullet(\mathrm{G}_S(K), M) \otimes^{\mathbb{L}}_\Lambda k)\end{aligned}$$

(siehe [GM96], Kap. III, § 7.9). Beide Spektralsequenzen degenerieren bereits im nächsten Schritt und alle Einträge außerhalb eines 3×3-Quadrats sind trivial. Da die Anfangsterme $\mathrm{H}^j(\mathrm{G}_S(K), \mathrm{Tor}^\Lambda_{-i}(M, k))$ der zweiten Spektralsequenz endliche Moduln sind, folgt sofort dasselbe für die Endterme $\mathrm{H}^{i+j}(C^\bullet(\mathrm{G}_S(K), M) \otimes^{\mathbb{L}}_\Lambda k)$.

Die erste Spektralsequenz liefert einen Isomorphismus

$$\mathrm{H}^2(\mathrm{G}_S(K), M) \otimes_\Lambda k = \mathrm{H}^2(C^\bullet(\mathrm{G}_S(K), M) \otimes^{\mathbb{L}}_\Lambda k).$$

Daher ist $\mathrm{H}^2(\mathrm{G}_S(K), M)$ nach dem topologischen Nakayama-Lemma endlich erzeugt, woraus wiederum die Endlichkeit aller Moduln $\mathrm{Tor}^\Lambda_i(\mathrm{H}^2(\mathrm{G}_S(K), M), k)$ folgt.

Betrachte nun das Differential

$$d : \mathrm{Tor}^\Lambda_2(\mathrm{H}^2(\mathrm{G}_S(K), M), k) \longrightarrow \mathrm{H}^1(\mathrm{G}_S(K), M) \otimes_\Lambda k.$$

Mit $\mathrm{Tor}^\Lambda_2(\mathrm{H}^2(\mathrm{G}_S(K), M), k)$ ist auch $\mathrm{Im}\, d$ endlich.

Die graduierten Stücke, die zum Endterm $\mathrm{H}^1(C^\bullet(\mathrm{G}_S, M) \otimes^{\mathbb{L}}_\Lambda k)$ beitragen, sind $\mathrm{Tor}^\Lambda_1(\mathrm{H}^2(\mathrm{G}_S(K), M), N)$ und $\mathrm{Coker}\, d$. Also ist $\mathrm{Coker}\, d$ endlich. Damit muss aber bereits $\mathrm{H}^1(\mathrm{G}_S, M) \otimes_\Lambda k$ endlich sein. Dies galt es noch zu zeigen. □

Folgerung 5.6.5. *Sei P in $\mathrm{G}_S(K)$-$Mod_{f.g.}(\Omega)$ flach als Ω-Modul. Dann ist der Komplex $C^\bullet(\mathrm{G}_S(K), P)$ perfekt.*

Beweis. Dies folgt sofort aus aus Satz 5.6.4 und Lemma 1.5.4. □

5.7 Induzierte Moduln

In diesem Abschnitt beschäftigen wir uns wieder mit den im Kapitel 2 eingeführten pro-endlichen Gruppenringen einer zyklotomischen $\mathbb{Z}_p$-Erweiterung K_∞/K_0 mit $K_0 \cap \mathbb{Q}_\infty = \mathbb{Q}$. Sei $\mathcal{O}_p$ der Bewertungsring eines Erweiterungskörpers endlichen Grades von $\mathbb{Q}_p$. Wir setzen zur Abkürzung

$$\Omega \stackrel{def}{=} \mathcal{O}_p[\![\mathrm{G}(K_\infty/K_0)]\!].$$

Die endliche Menge $S = S_{\mathbb{Q}}$ von Stellen von $\mathbb{Q}$ enthalte p, die unendliche Stelle von $\mathbb{Q}$ und alle in $K_0/\mathbb{Q}$ verzweigten Stellen. Die Menge der über S liegenden Stellen von K_n bezeichnen wir mit S_{K_n} oder ebenfalls mit S, falls der zugehörige Körper klar ersichtlich ist.

Da nach Satz 2.2.4.(i) $K_n/\mathbb{Q}$ außerhalb von S unverzweigt ist, ist auf der einen Seite K_n in der maximalen außerhalb S unverzweigten Erweiterung von $\mathbb{Q}$ enthalten, auf der anderen Seite ist nach der Multiplikativität der Verzweigungsindices aber auch jede außerhalb S unverzweigte Erweiterung von K_n bereits über $\mathbb{Q}$ außerhalb S

unverzweigt. Mit anderen Worten, $\mathrm{G}_S(K_n)$ ist eine offene Untergruppe von G_S und es gilt

$$\mathrm{G}_S \,/\, \mathrm{G}_S(K_n) = \mathrm{G}(K_n/\mathbb{Q}).$$

Insbesondere ist jeder Modul M in G_S-$\mathit{Mod}_{f.g.}(\mathcal{O}_p)$ in natürlicher Weise auch ein Modul in $\mathrm{G}_S(K_n)$-$\mathit{Mod}_{f.g.}(\mathcal{O}_p)$.

Wir erinnern an folgende Konstruktion der Gruppen-Kohomologie (siehe [NSW00], Kap. II, § 3):

Definition 5.7.1. Sei G eine pro-endliche Gruppe, $H \subset G$ eine offene Untergruppe und M ein kompakter G-Modul. Dann lässt sich die *Normabbildung*

$$N_{G/H} : M^H \longrightarrow M^G \qquad m \mapsto \sum_{\sigma \in G/H} \sigma m$$

für alle k eindeutig zu funktoriellen Homomorphismen

$$\mathit{cor} : \mathrm{H}^k(H, M) \longrightarrow \mathrm{H}^k(G, M),$$

den *Korestriktionsabbildungen*, fortsetzen.

Auf $\mathrm{H}^k(\mathrm{G}_S(K_n), M)$ ist wie folgt eine Operation von $\mathrm{G}(K_n/\mathbb{Q})$ definiert: Sei σ die Restklasse in $\mathrm{G}(K_n/\mathbb{Q})$ von $g \in \mathrm{G}_S$. Das Bild eines Kozykels $c : \mathrm{G}_S(K_n)^{k+1} \longrightarrow M$ unter σ wird durch

$$\sigma c(x) \overset{\mathit{def}}{=} g c(g^{-1} x g), \qquad x \in \mathrm{G}_S(K_n)^{k+1}$$

gegeben. Die Kohomologieklasse von σc ist dann von der speziellen Wahl von g unabhängig (siehe [NSW00], Satz 1.6.2). Auf $M^{\mathrm{G}_S(K_n)} = \mathrm{H}^0(\mathrm{G}_S(K_n), M)$ ist dies gerade die von G_S induzierte Operation.

Diese Operation ist mit den Korestriktionsabbildungen

$$\mathit{cor} : \mathrm{H}^k(\mathrm{G}_S(K_{n+1}), M) \longrightarrow \mathrm{H}^k(\mathrm{G}_S(K_n), M)$$

und den Zusammenhangshomomorphismen kompatibel (siehe [NSW00], Satz 1.5.4). Der projektive Limes

$$\varprojlim_n \mathrm{H}^k(\mathrm{G}_S(K_n), M)$$

über die Korestriktionsabbildungen trägt auf diese Weise die Struktur eines Ω-Moduls. Ziel ist es, diesen Modul als Kohomologie-Modul eines Objektes in G_S-$\mathit{Mod}_{f.g.}(\Omega)$ zu interpretieren.

Sei M ein Modul in G_S-$\mathit{Mod}_{f.g.}(\mathcal{O}_p)$. Wir statten den Modul

$$\mathrm{Ind}_{K_n}(M) \overset{\mathit{def}}{=} M \otimes_{\mathcal{O}_p} \mathcal{O}_p[\mathrm{G}(K_n/\mathbb{Q})] = \Big\{ \sum_{\sigma \in \mathrm{G}(K_n/\mathbb{Q})} m_\sigma \otimes \sigma \;\Big|\; m_\sigma \in M \Big\}$$

mit der stetigen G_S-Operation

$$\begin{aligned} &\mathrm{G}_S \times \mathrm{Ind}_{K_n}(M) \longrightarrow \mathrm{Ind}_{K_n}(M) \\ &\Big(g, \sum_\sigma m_\sigma \otimes \sigma\Big) \mapsto \sum_\sigma g m_\sigma \otimes \Psi_{K_n}(g^{-1})\sigma = \sum_{\sigma'} g m_{(\Psi_{K_n}(g)\sigma')} \otimes \sigma' \end{aligned}$$

aus. Dabei bezeichnet $\Psi_{K_n} : \mathrm{G}_S \longrightarrow \mathrm{G}(K_n/\mathbb{Q})$ die natürliche Projektion.

Mittels der Projektion $\Omega \longrightarrow \mathcal{O}_p[\mathrm{G}(K_n/\mathbb{Q})]$ fassen wir $\mathrm{Ind}_{K_n}(M)$ als ein Objekt von $\mathrm{G}_S\text{-}\mathit{Mod}_{f.g.}(\Omega)$ auf. Ind_{K_n} ist in offensichtlicher Weise ein Funktor und die Projektion $\pi_{m,n} : \mathcal{O}_p[\mathrm{G}(K_m/\mathbb{Q})] \longrightarrow \mathcal{O}_p[\mathrm{G}(K_n/\mathbb{Q})]$ (für $m \geq n > 0$) induziert einen natürlichen Morphismus

$$\begin{aligned} \mathrm{Ind}_{K_m}(M) &\longrightarrow \mathrm{Ind}_{K_n}(M) \\ \sum_{\sigma \in \mathrm{G}(K_m/\mathbb{Q})} a_\sigma \otimes \sigma &\mapsto \sum_{\tau \in \mathrm{G}(K_n/\mathbb{Q})} \Big(\sum_{\pi_{m,n}(\sigma)=\tau} a_\sigma \Big) \otimes \tau \end{aligned}$$

von Moduln in $\mathrm{G}_S\text{-}\mathit{Mod}_{f.g.}(\Omega)$.

Definition 5.7.2. Sei S eine endliche Menge von Stellen von $\mathbb{Q}$ mit $p, \infty \in S$ und sei $K_0/\mathbb{Q}$ außerhalb S unverzweigt. Dann heißt

$$\mathrm{Ind}_{K_\infty}(M) \stackrel{def}{=} \varprojlim_n \mathrm{Ind}_{K_n}(M) = \varprojlim_n \mathrm{Ind}_{K_n}(M/p^n M).$$

der *von M (kompakt) induzierte Modul* in $\mathrm{G}_S\text{-}\mathit{Mod}_{f.g.}(\Omega)$.

Als Ω-Modul ist $\mathrm{Ind}_{K_\infty}(M)$ isomorph zu $M \otimes_{\mathcal{O}_p} \Omega$ und G_S operiert auf $\mathrm{Ind}_{K_\infty}(M)$ durch

$$g(m \otimes \omega) = gm \otimes \Psi_{K_\infty}(g^{-1})\omega$$

für $g \in \mathrm{G}_S$, $m \in M$ und $\omega \in \Omega$, also in gleicher Weise wie auf $\mathrm{Ind}_{K_n}(M)$.

Satz 5.7.3. *Sei M ein Modul in $\mathrm{G}_S\text{-}\mathit{Mod}_{f.g.}(\mathcal{O}_p)$. Dann gibt es einen natürlichen Isomorphismus von Ω-Moduln:*

$$\mathrm{H}^k(\mathrm{G}_S, \mathrm{Ind}_{K_\infty}(M)) \cong \varprojlim_n \mathrm{H}^k(\mathrm{G}_S(K_n), M).$$

Zum Beweis. Die Moduln M/p^n sind endlich, also gleichzeitig kompakt und diskret. Nach dem Lemma von Shapiro für diskrete Moduln (siehe [NSW00], Satz 1.6.3) induziert die Abbildung

$$\mathrm{Ind}_{K_n}(M/p^n M) \longrightarrow M/p^n M, \qquad \sum_{\sigma \in \mathrm{G}(K_n/\mathbb{Q})} m_\sigma \otimes \sigma \mapsto m_1$$

einen natürlichen Isomorphismus

$$sh : \mathrm{H}^k(\mathrm{G}_S, \mathrm{Ind}_{K_n}(M/p^n)) \mapsto \mathrm{H}^k(\mathrm{G}_S(K_n), M/p^n)$$

und [NSW00], Satz 1.6.4 zeigt, dass $sh \circ \pi_{m,n_*} = cor \circ sh$. Die Aussage folgt nun durch Übergang zum projektiven Limes. □

Bemerkung 5.7.4. Analoge Betrachtungen im Fall lokaler Körper wurden bereits von Pierre Colmez durchgeführt, siehe [Col98], Satz II.1.1.

Wir beweisen nun noch zwei wichtige Eigenschaften von induzierten Moduln.

Lemma 5.7.5. *Sei M ein Modul in $\mathrm{G}_S\text{-}\mathit{Mod}_{f.g.}(\mathcal{O}_p)$. Dann gilt*

$$\mathrm{H}^0(\mathrm{G}_S, \mathrm{Ind}_{K_\infty}(M)) = 0.$$

Beweis. Es gilt nach Satz 5.7.3 und Satz 5.6.3

$$\begin{aligned}\mathrm{H}^0(\mathrm{G}_S, \mathrm{Ind}_{K_\infty}(M)) &= \varprojlim_n \mathrm{H}^0(\mathrm{G}_S(K_n), M)\\ &= \varprojlim_{n,k} \mathrm{H}^0(\mathrm{G}_S(K_n), M/p^kM) = \varprojlim_k \mathrm{H}^0(\mathrm{G}_S, \mathrm{Ind}_{K_\infty}(M/p^kM)).\end{aligned}$$

Insbesondere genügt es, die Aussage für die endlichen Moduln M/p^kM zu beweisen. Sei deshalb von nun an M endlich. Die aufsteigende Kette von Untermoduln

$$M^{\mathrm{G}_S(K_0)} \subseteq M^{\mathrm{G}_S(K_1)} \subseteq \cdots \subseteq M^{\mathrm{G}_S(K_n)} \subseteq \cdots$$

wird stationär, d.h. es gibt eine natürliche Zahl N, so dass für $n \geq N$ und alle $a \geq 0$ gilt:

$$M^{\mathrm{G}_S(K_{n+a})} = M^{\mathrm{G}_S(K_n)} = (M^{\mathrm{G}_S(K_{n+a})})^{\mathrm{G}(K_{n+a}/K_n)},$$

d.h. $\mathrm{G}(K_{n+a}/K_n)$ operiert trivial auf $M^{\mathrm{G}_S(K_{n+a})}$. Also ist die Normabbildung

$$N_{\mathrm{G}(K_{n+a}/K_n)} : M^{\mathrm{G}_S(K_{n+a})} \longrightarrow M^{\mathrm{G}_S(K_n)}$$

gleich der Multiplikation mit $p^a = \sharp\, \mathrm{G}(K_{n+a}/K_n)$. Ist nun a so groß, dass $p^aM = 0$, dann ist $N_{\mathrm{G}(K_{n+a}/K_n)}$ gleich der Nullabbildung, d.h. für den projektiven Limes bezüglich der Normabbildungen muss gelten:

$$\varprojlim_n \mathrm{H}^0(\mathrm{G}_S(K_n), M) = 0.$$

□

Lemma 5.7.6. *Sei $K_0 \subset L_0$ und $L_0/\mathbb{Q}$ außerhalb S unverzweigt. Bezeichne*

$$\psi_* : \mathrm{G}_S\text{-}Mod_{f.g.}(\mathcal{O}_p[\![\mathrm{G}(L_\infty/\mathbb{Q})]\!]) \longrightarrow \mathrm{G}_S\text{-}Mod_{f.g.}(\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!])$$

die von der natürlichen Projektion $\psi : \mathrm{G}(L_\infty/\mathbb{Q}) \longrightarrow \mathrm{G}(K_\infty/\mathbb{Q})$ induzierte Koeffizientenerweiterung. Dann gilt für jeden Modul M in $\mathrm{G}_S\text{-}Mod_{f.g.}(\mathcal{O}_p)$:

$$\psi_* \mathrm{Ind}_{L_\infty}(M) = \mathrm{Ind}_{K_\infty}(M).$$

Beweis. Sei $m \in M$, $l \in \Omega' \stackrel{def}{=} \mathcal{O}_p[\![\mathrm{G}(L_\infty/\mathbb{Q})]\!]$ und $k \in \Omega \stackrel{def}{=} \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$. Wir müssen zeigen, dass der Isomorphismus von Ω-Moduln

$$\begin{aligned} f : \psi_* \mathrm{Ind}_{L_\infty}(M) = M \otimes_{\mathcal{O}_p} \Omega' \otimes_{\Omega'} \Omega &\longrightarrow M \otimes_{\mathcal{O}_p} \Omega = \mathrm{Ind}_{K_\infty}(M)\\ m \otimes l \otimes k &\mapsto m \otimes \psi(l)k \end{aligned}$$

G_S-äquivariant ist. Bezeichne $\Psi_F : \mathrm{G}_S \longrightarrow \mathrm{G}(F/\mathbb{Q})$ (mit $F = L_\infty, K_\infty$) die natürliche Abbildung. Die Operation von $g \in \mathrm{G}_S$ auf $\psi_* \mathrm{Ind}_{L\infty}(M)$ ist durch

$$g(m \otimes l \otimes k) = gm \otimes \Psi_{L_\infty}(g^{-1})l \otimes k$$

gegeben (vgl. Abschnitt 5.5). Wegen $\psi \circ \Psi_{L_\infty} = \Psi_{K_\infty}$ folgt

$$f(gm \otimes \Psi_{L_\infty}(g^{-1})l \otimes k) = gm \otimes \Psi_{K_\infty}(g^{-1})\psi(l)k = gf(m \otimes l \otimes k),$$

also die Behauptung. □

Bemerkung 5.7.7. Man zeigt in gleicher Weise leicht, dass Ind_{K_∞} mit endlichen Erweiterungen des Ringes $\mathcal{O}_p$ vertauscht.

6 Die äquivariante Hauptvermutung

In diesem Kapitel werden wir unser Hauptresultat, die äquivariante Hauptvermutung der Iwasawa-Theorie für die zyklotomische $\mathbb{Z}_p$-Erweiterung abelscher Zahlkörper, formulieren und beweisen.

6.1 Formulierung der äquivarianten Hauptvermutung

Sei S eine endliche Menge von Stellen von $\mathbb{Q}$, welche die archimedische Stelle ∞ und die ungerade Primzahl p enthält. $\chi : \mathrm{G}_S \longrightarrow \mathcal{O}_p^\times$ sei ein stetiger Charakter mit Werten im Bewertungsring $\mathcal{O}_p$ eines Erweiterungskörpers endlichen Grades von $\mathbb{Q}_p$.

Mit $\mathcal{O}_p(\chi)$ bezeichnen wir den freien $\mathcal{O}_p$-Modul vom Rang 1 mit der G_S-Operation

$$\begin{aligned} \mathrm{G}_S \times \mathcal{O}_p(\chi) &\longrightarrow \mathcal{O}_p(\chi), \\ (g, m) &\mapsto \chi(g)m. \end{aligned}$$

Dies ist klar ein Modul der Kategorie $\mathrm{G}_S\text{-}\mathit{Mod}_{f.g.}(\mathcal{O}_p)$ (siehe Abschnitt 5.1).

Ein wichtiger Spezialfall ist der Modul $\mathbb{Z}_p(\varepsilon_{cycl})$ aus $\mathrm{G}_S\text{-}\mathit{Mod}_{f.g.}(\mathbb{Z}_p)$. Es gilt

$$\mathbb{Z}_p(\varepsilon_{cycl}) = \varprojlim_n \mu_{p^n},$$

wobei μ_{p^n} den (multiplikativ geschriebenen) $\mathbb{Z}_p$-Modul der p^n-ten Einheitswurzeln mit der natürlichen G_S-Operation bezeichnet. Die Übergangsabbildung $\mu_{p^{n+1}} \longrightarrow \mu_{p^n}$ ist das Erheben in die p-te Potenz.

Sei nun $K/\mathbb{Q}$ eine außerhalb S unverzweigte, endliche und abelsche Erweiterung von $\mathbb{Q}$ und K_∞/K die zyklotomische $\mathbb{Z}_p$-Erweiterung von K. Wir sind nur an K_∞ interessiert, können also o.B.d.A. K durch $K_0 = K_\infty^\Gamma$ ersetzen (siehe Abschnitt 2.2).

Nach Konstruktion (siehe Definition 5.7.2) ist der induzierte Modul $\mathrm{Ind}_{K_\infty} \mathcal{O}_p(\chi)$ ein freier $\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$-Modul vom Rang 1 mit der G_S-Operation

$$\mathrm{G}_S \times \mathrm{Ind}_{K_\infty} \mathcal{O}_p(\chi) \longrightarrow \mathrm{Ind}_{K_\infty} \mathcal{O}_p(\chi), \qquad (g, m) \mapsto \Psi_{K_\infty}(g^{-1})\chi\varepsilon_{cycl}(g)m,$$

wobei $\Psi_{K_\infty} : \mathrm{G}_S \longrightarrow \mathrm{G}(K_\infty/\mathbb{Q})$ die natürliche Projektion bezeichnet.

Wie in Kapitel 3 bezeichne $\mathcal{F}_{-1}$ die komplexe Konjugation und

$$e_+ \overset{def}{=} \frac{1 + \mathcal{F}_{-1}}{2}, \qquad e_- \overset{def}{=} \frac{1 - \mathcal{F}_{-1}}{2}$$

die entsprechenden idempotenten Elemente von $\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$.

Im Laufe dieses Kapitels wird es sich herausstellen, dass der Kokettenkomplex $C^\bullet(\mathrm{G}_S, e_- \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))$ der stetigen Galois-Kohomologie (siehe Kapitel 5) eine sinnvolle Verallgemeinerung des pro-endlichen Limes der Klassengruppen in der klassischen Formulierung der Hauptvermutung darstellt. Insbesondere werden wir zeigen, dass dieser Komplex ein perfekter Torsionskomplex im Sinne von Definition 1.5.3 ist (siehe Satz 6.3.4).

Also können wir die in Kapitel 1 entwickelte Konstruktion des charakteristischen Ideals auf $C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))$ anwenden und erhalten ein Element

$$\operatorname{char} C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) \in \mathfrak{C}(\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!])$$

in der Cartier-Divisor-Gruppe. Das folgende Theorem ist unser Hauptresultat:

Theorem 6.1.1 (Äquivariante Hauptvermutung, [BG03], Theorem 6.1). *Sei p eine ungerade Primzahl und K_∞/K die zyklotomische $\mathbb{Z}_p$-Erweiterung eines abelschen Zahlkörpers K. S sei eine endliche Menge von Stellen von $\mathbb{Q}$, die p, die archimedische Stelle ∞, und alle in $K/\mathbb{Q}$ verzweigten Stellen enthält. $\mathbb{1} : \mathrm{G}(K_\infty/\mathbb{Q}) \longrightarrow \mathbb{Z}_p$ bezeichne den trivialen Charakter. Dann ist die äquivariante L-Funktion $\mathcal{L}_{p,S}(K_\infty, \mathbb{1})$ ein Erzeuger des charakteristischen Ideals*

$$\operatorname{char} C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) \in \mathfrak{C}(\mathbb{Z}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]).$$

Die äquivariante L-Funktion $\mathcal{L}_{p,S}(K_\infty, \mathbb{1})$ hatten wir in Kapitel 3 aus dem Limes von Stickelberger-Elementen konstruiert. Durch Zerlegung nach Charakteren gewinnt man die üblichen p-adischen L-Funktionen zu Dirichlet-Charakteren (siehe Satz 3.4.6).

Durch das Verdrehen mit stetigen Charakteren von G_S (siehe Abschnitt 2.10) erhalten wir folgende Verallgemeinerung:

Folgerung 6.1.2 (Um χ verdrehte Hauptvermutung, [BG03], Theorem 7.1). *Sei $\mathcal{O}_p$ der Bewertungsring eines Erweiterungskörpers endlichen Grades von $\mathbb{Q}_p$ und $\chi : \mathrm{G}_S \longrightarrow \mathcal{O}_p^\times$ ein stetiger Charakter. Dann ist $\mathcal{L}_{p,S}(K_\infty, \chi)$ ein Erzeuger des charakteristischen Ideals*

$$\operatorname{char} C^\bullet(\mathrm{G}_S, Tw_\chi(e_-) \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\chi^{-1}\varepsilon_{cycl})) \in \mathfrak{C}(\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]).$$

Der Beweis beider Aussagen wird uns für den Rest dieses Kapitels beschäftigen.

6.2 Kohomologie von $\mathbb{Z}_p(\varepsilon_{cycl})$

In diesem Abschnitt wollen wir die Kohomologie von $\operatorname{Ind}_{K_\infty}(\mathbb{Z}_p(\varepsilon_{cycl}))$ bestimmen. Dabei folgen wir weitgehend den Beweisen von [BG03], Lemma 3.2 und Satz 5.1. Wir verwenden nachstehende Bezeichnungen (siehe auch [NSW00], Kapitel VIII, § 3):

Definition 6.2.1. Sei L ein Zahlkörper und S eine Menge von Stellen von L, die alle archimedischen Stellen enthält.

(i) $\mathcal{O}_{L,S}^\times$ bezeichne den *Gruppe der S-Einheiten* von L, d.h. $\mathcal{O}_{L,S}^\times$ besteht aus den Elementen von L, die für jede Stelle v von L mit $v \notin S$ im Bewertungsring des lokalen Körpers L_v Einheiten sind.

(ii) Sei I_S die von den Stellen von L außerhalb S frei erzeugte abelsche Gruppe. Betrachte die Abbildung

$$val : L^\times \longrightarrow I_S, \qquad x \mapsto \sum_{v \notin S} val_v(x) v,$$

wobei val_v die additive Bewertung zur Stelle v bezeichnet. Dann heißt

$$Cl_S(L) = I_S / \operatorname{Im} val$$

S-Klassengruppe von L. Mit anderen Worten, $Cl_S(L)$ ist die Faktorgruppe der vollen Klassengruppe $Cl(L)$ modulo der von den endlichen Stellen von S erzeugten Untergruppe.

Für Galois-Erweiterungen $L/\mathbb{Q}$ betrachten wir beide Gruppen mittels der natürlichen Operation als $\mathrm{G}(L/\mathbb{Q})$-Moduln.

Sei $S_\mathbb{Q}$ wieder eine endliche Menge von Stellen von $\mathbb{Q}$ mit $p, \infty \in S$ und S_L die Menge der Stellen eines Zahlkörpers L über den Stellen von $S_\mathbb{Q}$. Wir unterdrücken den Index L, falls klar ersichtlich ist, um welchen Körper es sich handelt.

Bezeichne

$$\mathcal{O}_S^\times \stackrel{def}{=} \bigcup \mathcal{O}_{L,S}^\times$$

die Vereinigung der Gruppen der S_L-Einheiten über alle außerhalb von $S_\mathbb{Q}$ unverzweigten Erweiterungen L von $\mathbb{Q}$. Die Gruppe $\mathcal{O}_S^\times$ ist damit in natürlicher Weise ein diskreter $\mathrm{G}_S(\mathbb{Q})$-Modul.

Sei $L/\mathbb{Q}$ eine endliche Galois-Erweiterung. Wir zerlegen $S_L = S_{L,f} \cup S_{L,\infty}$ in die Menge der endlichen Stellen $S_{L,f}$ und die Menge der archimedischen Stellen $S_{L,\infty}$ in S_L. Ist A eine abelsche Gruppe, so bezeichne $A[S_{L,f}]$ den $\mathrm{G}(L/\mathbb{Q})$-Modul $\bigoplus\limits_{v \in S_{L,f}} Av$ mit der Operation

$$\mathrm{G}(L/\mathbb{Q}) \times A[S_{L,f}] \longrightarrow A[S_{L,f}], \qquad \Big(\sigma, \sum_{v \in S_{L,f}} a_v v\Big) \mapsto \sum_{v \in S_{L,f}} a_v \sigma v.$$

Betrachtet man A als trivialen $\mathrm{G}(L/\mathbb{Q})$-Modul, so ist

$$\varsigma : A[S_{L,f}] \longrightarrow A, \qquad \sum_{v \in S_{L,f}} a_v v \mapsto \sum_{v \in S_{L,f}} a_v$$

offensichtlich ein $\mathrm{G}(L/\mathbb{Q})$-Homomorphismus. Ist L'/L eine endliche Galois-Erweiterung, so ist

$$\alpha_{L'/L} : A[S_{L',f}] \longrightarrow A[S_{L,f}], \qquad \sum_{w \in S_{L',f}} a_w w \mapsto \sum_{v \in S_{L,f}} \sum_{w | v} a_w v$$

ein $\mathrm{G}(L'/\mathbb{Q})$-Homomorphismus und es gilt $\varsigma \circ \alpha_{L'/L} = \varsigma$.

Lemma 6.2.2. *Seien L'/L und $L/\mathbb{Q}$ außerhalb von S unverzweigte, endliche Galois-Erweiterungen. Dann gilt:*

(i) $\mathrm{H}^0(\mathrm{G}_S(L), \mathcal{O}_S^\times) = \mathcal{O}_{L,S}^\times$ *als* $\mathrm{G}(L/\mathbb{Q})$*-Moduln. Die Korestriktionsabbildung ist gleich der Normabbildung*

$$N_{L'/L} : \mathcal{O}_{L',S}^\times \mapsto \mathcal{O}_{L,S}^\times, \qquad u \mapsto \prod_{\sigma \in \mathrm{G}(L'/L)} \sigma u.$$

(ii) $\mathrm{H}^1(\mathrm{G}_S(L), \mathcal{O}_S^\times) = Cl_S(L)$ *als* $\mathrm{G}(L/\mathbb{Q})$*-Moduln. Die Korestriktionsabbildung ist gleich der Normabbildung* $N_{L'/L} : Cl_S(L') \longrightarrow Cl_S(L)$*, d.h. für eine Stelle* $v \notin S_L$ *von* L *und eine Stelle* V *von* L' *über* v *gilt* $N_{L'/L}(V) = f(V|v)v$*, wobei* $f(V|v)$ *den Restklassenkörpergrad der ensprechenden lokalen Erweiterung bezeichnet.*

(iii) Folgendes Diagramm von $\mathrm{G}(L'/\mathbb{Q})$*-Moduln ist kommutativ und die Zeilen sind exakt:*

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^2(\mathrm{G}_S(L'), \mathcal{O}_S^\times) \otimes_{\mathbb{Z}} \mathbb{Z}_p \arrow[r] \arrow[d, "cor"'] & \mathbb{Q}_p/\mathbb{Z}_p[S_{L',f}] \arrow[r, "\varsigma"] \arrow[d, "\alpha_{L'/L}"'] & \mathbb{Q}_p/\mathbb{Z}_p \arrow[r] \arrow[d, "="'] & 0 \\
0 \arrow[r] & \mathrm{H}^2(\mathrm{G}_S(L), \mathcal{O}_S^\times) \otimes_{\mathbb{Z}} \mathbb{Z}_p \arrow[r] & \mathbb{Q}_p/\mathbb{Z}_p[S_{L,f}] \arrow[r, "\varsigma"] & \mathbb{Q}_p/\mathbb{Z}_p \arrow[r] & 0
\end{tikzcd}$$

Zum Beweis. In [NSW00], Satz 8.3.10 wird (i), (ii) und die Exaktheitsaussage von (iii) gezeigt. Die Kommutativität folgt im Wesentlichen aus [NSW00], Satz 8.1.4 und Satz 8.1.10. □

Die Kohomologie von $\mathbb{Z}_p(\varepsilon_{cycl})$ lässt sich nun leicht berechnen.

Lemma 6.2.3 (siehe [BG03], Lemma 3.2). *Sei* $L/\mathbb{Q}$ *eine außerhalb von* S *unverzweigte, endliche Galois-Erweiterung. Dann gilt*

$$\mathrm{H}^1(\mathrm{G}_S(L), \mathbb{Z}_p(\varepsilon_{cycl})) = \mathcal{O}_{L,S}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

und Korestriktionsabbildung ist durch die Normabbildung gegeben. Ist $L'/\mathbb{Q}$ *eine weitere außerhalb* S *unverzweigte, endliche Galois-Erweiterung mit* $L \subset L'$*, so ist folgendes Diagramm von* $\mathbb{Z}_p[\mathrm{G}(L/\mathbb{Q})]$*-Moduln kommutativ und die Zeilen sind exakt.*

$$\begin{tikzcd}
0 \arrow[r] & Cl_S(L') \otimes_{\mathbb{Z}} \mathbb{Z}_p \arrow[r] \arrow[d, "N_{L'/L}"'] & \mathrm{H}^2(\mathrm{G}_S(L'), \mathbb{Z}_p(\varepsilon_{cycl})) \arrow[r] \arrow[d, "cor"'] & \mathbb{Z}_p[S_{L',f}] \arrow[r, "\varsigma"] \arrow[d, "\alpha_{L'/L}"'] & \mathbb{Z}_p \arrow[r] \arrow[d, "="'] & 0 \\
0 \arrow[r] & Cl_S(L) \otimes_{\mathbb{Z}} \mathbb{Z}_p \arrow[r] & \mathrm{H}^2(\mathrm{G}_S(L), \mathbb{Z}_p(\varepsilon_{cycl})) \arrow[r] & \mathbb{Z}_p[S_{L,f}] \arrow[r, "\varsigma"] & \mathbb{Z}_p \arrow[r] & 0
\end{tikzcd}$$

Beweis. Für jede natürliche Zahl n ist die Kummer-Sequenz

$$0 \longrightarrow \mu_{p^n} \longrightarrow \mathcal{O}_S^\times \xrightarrow{p^n} \mathcal{O}_S^\times \longrightarrow 0$$

exakt (siehe [NSW00], Satz 8.3.3). Wir betrachten die dazugehörige lange exakte Kohomologiesequenz. Für ein genügend großes k annulliert p^k den endlichen $\mathbb{Z}_p$-Modul $Cl_S(L) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ und die lange exakte Kohomologiesequenz liefert ein kommutatives Diagramm mit exakten Zeilen

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_{L,S}^\times/(\mathcal{O}_{L,S}^\times)^{p^{k(n+1)}} \arrow[r] \arrow[d] & \mathrm{H}^1(\mathrm{G}_S(L), \mu_{p^{k(n+1)}}) \arrow[r] \arrow[d, "p^k"'] & Cl_S(L) \otimes_{\mathbb{Z}} \mathbb{Z}_p \arrow[r] \arrow[d, "0"'] & 0 \\
0 \arrow[r] & \mathcal{O}_{L,S}^\times/(\mathcal{O}_{L,S}^\times)^{p^{kn}} \arrow[r] & \mathrm{H}^1(\mathrm{G}_S(L), \mu_{p^{kn}}) \arrow[r] & Cl_S(L) \otimes_{\mathbb{Z}} \mathbb{Z}_p \arrow[r] & 0
\end{tikzcd}$$

Durch Übergang zum projektiven Limes erhalten wir den ersten Teil der Aussage.

Setze $H_n \stackrel{def}{=} \mathrm{Ker}(\mathrm{H}^2(\mathrm{G}_S(L), \mathcal{O}_S^\times) \xrightarrow{p^n} \mathrm{H}^2(\mathrm{G}_S(L), \mathcal{O}_S^\times))$. Aus der langen exakten Kohomologiesequenz der Kummersequenz folgt die Exaktheit von

$$0 \longrightarrow Cl_S(L)/p^n\,Cl_S(L) \longrightarrow \mathrm{H}^2(\mathrm{G}_S(L), \mu_{p^n}) \longrightarrow H_n \longrightarrow 0.$$

Andererseits liefert uns Punkt (iii) von Lemma 6.2.2 zusammen mit dem Schlangenlemma eine exakte Sequenz

$$0 \longrightarrow H_n \longrightarrow \left(\frac{1}{p^n}\mathbb{Z}/\mathbb{Z}\right)[S_{L,f}] \xrightarrow{\varsigma} \frac{1}{p^n}\mathbb{Z}/\mathbb{Z} \longrightarrow 0.$$

Die Übergangsabbildung zu den entsprechenden Sequenzen für $n-1$ ist, bis auf die natürliche Projektion $Cl_S(L)/p^n\,Cl_S(L) \longrightarrow Cl_S(L)/p^{n-1}\,Cl_S(L)$, jeweils Multiplikation mit p. Der Übergang zum projektiven Limes bei beiden Sequenzen liefert zusammen mit dem natürlichen Isomorphismus

$$\varprojlim_n \frac{1}{p^n}\mathbb{Z}/\mathbb{Z} = \mathbb{Z}_p$$

die Exaktheit der Zeilen im Diagramm des Lemmas. Die Kommutativität des Diagramms sieht man nun leicht ein. □

Betrachte nun wieder die zyklotomische $\mathbb{Z}_p$-Erweiterung K_∞/K_0. Wir erhalten folgende Beschreibung der Kohomologie von $\mathrm{Ind}_{K_\infty}(\mathbb{Z}_p(\varepsilon_{cycl}))$.

Satz 6.2.4 (siehe [BG03], Satz 3.2). *Der Komplex $C^\bullet(\mathrm{G}_S, \mathrm{Ind}_{K_\infty}\mathbb{Z}_p(\varepsilon_{cycl}))$ ist azyklisch außerhalb der Grade 1 und 2. Ferner gibt es einen kanonischen Isomorphismus von $\mathbb{Z}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$-Moduln*

$$\mathrm{H}^1(\mathrm{G}_S, \mathrm{Ind}_{K_\infty}(\mathbb{Z}_p(\varepsilon_{cycl}))) = \varprojlim_n \mathcal{O}_{K_n,S}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

und für genügend großes $n_0 \in \mathbb{N}$ eine exakte Sequenz von $\mathbb{Z}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$-Moduln

$$0 \longrightarrow \varprojlim_n Cl_S(K_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p \longrightarrow \mathrm{H}^2(\mathrm{G}_S, \mathrm{Ind}_{K_\infty}\mathbb{Z}_p(\varepsilon_{cycl})) \longrightarrow \mathbb{Z}_p[S_{K_{n_0},f}] \xrightarrow{\varsigma} \mathbb{Z}_p \longrightarrow 0.$$

Beweis. Das Verschwinden der Kohomologie außerhalb der Grade 1 und 2 haben wir in Lemma 5.7.5 und Satz 5.6.2 bereits allgemein bewiesen. Für $n \geq n_0$ mit n_0 genügend groß gilt nach Satz 2.2.4 $\sharp S_{K_n,f} = \sharp S_{K_{n_0},f}$. Also ist

$$\alpha_{K_n/K_{n_0}} : \mathbb{Z}_p[S_{K_n,f}] \longrightarrow \mathbb{Z}_p[S_{K_{n_0},f}]$$

ein Isomorphismus von $\mathbb{Z}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$-Moduln.

Alles andere folgt aus Lemma 6.2.3 durch Übergang zum projektiven Limes über die Korestriktionsabbildungen, denn nach Satz 5.6.3 gilt:

$$\mathrm{H}^i(\mathrm{G}_S, \mathrm{Ind}_{K_\infty}(\mathbb{Z}_p(\varepsilon_{cycl}))) = \varprojlim_n \mathrm{H}^i(\mathrm{G}_S(K_n), \mathbb{Z}_p(\varepsilon_{cycl})).$$

□

6.3 Torsion und μ-Invariante

Um die Ergebnisse aus Kapitel 1 anwenden zu können, benötigen wir einen perfekten Torsionskomplex. Der Komplex $C^\bullet(\mathrm{G}_S, \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))$ ist nach Folgerung 5.6.5 perfekt, denn $\mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})$ ist isomorph zu $\Omega \overset{def}{=} \mathbb{Z}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$ als Ω-Modul, insbesondere also frei und somit flach. Jedoch ist er kein Torsionskomplex. Man kann zeigen, dass die erste Kohomologie über dem Quotientenring im Allgemeinen nicht verschwindet.

Genau wie bei der Konstruktion des äquivarianten Stickelberger-Elements im Kapitel 3 müssen wir deshalb den Komplex nach den Idempotenten

$$e_+ \overset{def}{=} \frac{1+\mathcal{F}_{-1}}{2}, \qquad e_- \overset{def}{=} \frac{1-\mathcal{F}_{-1}}{2}$$

zerlegen und den e_+-Anteil entfernen. Wir können diese Zerlegung als Bildung des Tensorprodukts

$$e_- C^\bullet(\mathrm{G}_S, \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) = C^\bullet(\mathrm{G}_S, \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) \otimes^{\mathbb{L}}_{\Omega} e_-\Omega$$

interpretieren. Nach Satz 5.5.2 gilt also

$$e_- C^\bullet(\mathrm{G}_S, \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) = C^\bullet(\mathrm{G}_S, e_- \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))$$

und weil $e_-\Omega$ als direkter Summand von Ω projektiv ist (siehe Satz 1.1.1) gilt auch

$$e_- \mathrm{H}^i(\mathrm{G}_S, \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) = \mathrm{H}^i(\mathrm{G}_S, e_- \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})).$$

Wir werden weiter unten zeigen, dass der so veränderte Komplex bereits über Λ ein perfekter Torsionskomplex ist.

Gleichzeitig erhalten wir noch ein weiteres wichtiges Resultat. Wir möchten durch Zerlegung nach Charakteren die äquivariante Hauptvermutung auf die klassische Hauptvermutung in der Formulierung von [HK03] zurückführen. Doch bei dieser Zerlegung geht die Information über das charakteristische Ideal an den Singularitäten von Ω (d.h. den Primidealen, die $\sharp\, \mathrm{G}(K_0/\mathbb{Q})$ enthalten) verloren.

In diesem Abschnitt werden wir zeigen, dass das charakteristische Ideal des Komplexes $C^\bullet(\mathrm{G}_S, e_- \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))$ an den Singularitäten trivial ist, also gar keine Information enthält. (Diese Beobachtung geht ursprünglich auf D. Burns und C. Greither zurück, siehe [BG03].) Essentieller Bestandteil des Beweises ist eine Anwendung des Theorems von Ferrero-Washington über das Verschwinden der μ-Invariante, welches wir in Kapitel 4 bewiesen haben.

Lemma 6.3.1. $\mathrm{H}^1(\mathrm{G}_S, e_- \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))$ *ist als* $\mathbb{Z}_p$*-Modul endlich erzeugt.*

Beweis. Wir erinnern daran, dass $\mathcal{F}_{-1}$ auf K_n als komplexe Konjugation operiert. Mit K_n^+ bezeichnen wir den maximalen reellen Teilkörper von K_n, d.h. den Teilkörper der unter $\mathcal{F}_{-1}$ invarianten Elemente.

Ist $K_0 = K_0^+$, so gilt auch $K_\infty = K_0\mathbb{Q}_\infty = K_\infty^+$ (jeder der Körper $\mathbb{Q}_n$ ist reell, da der Grad der Erweiterung $\mathbb{Q}_n/\mathbb{Q}$ nicht durch 2 teilbar ist). Also ist $\mathcal{F}_{-1} = id$ in $\mathrm{G}(K_\infty/\mathbb{Q})$, d.h. es gilt $e_- \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}) = 0$. In diesem Fall ist die Aussage deshalb trivial.

Sei nun $K_0 \neq K_0^+$. Der Untermodul der unter $\mathcal{F}_{-1}$ invarianten Elemente von $\mathcal{O}^\times_{K_n,S} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ ist demnach $\mathcal{O}^\times_{K_n^+,S} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Andererseits ist dieser Modul gerade der Kern der Multiplikation mit e_- auf $\mathcal{O}^\times_{K_n,S} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Da e_- idempotent ist, ist $\mathcal{O}^\times_{K_n^+,S} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ ein direkter Summand von $\mathcal{O}^\times_{K_n,S} \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

Weil die Galoisgruppe $\mathrm{G}(K_{n+1}/K_n)$ abelsch ist, vertauscht die Operation von $\mathcal{F}_{-1}$ mit der Normabbildung N_{K_{n+1}/K_n}. Die Zerlegung

$$\mathcal{O}^\times_{K_n,S} \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathcal{O}^\times_{K_n^+,S} \otimes_{\mathbb{Z}} \mathbb{Z}_p \oplus e_-\mathcal{O}^\times_{K_n,S} \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

ist somit mit der Normabbildung verträglich. Insbesondere folgt nach Satz 6.2.4

$$\mathrm{H}^1(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) = \varprojlim_n e_-\mathcal{O}^\times_{K_n,S} \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

Nach dem Einheitensatz von Dirichlet (siehe [Cas67], § 18) gilt

$$\mathcal{O}_{K_n^+,S} \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathbb{Z}_p^{\sharp S_{K_n^+}-1}, \qquad \mathcal{O}_{K_n,S} \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong W_n \times \mathbb{Z}_p^{\sharp S_{K_n}-1}$$

als $\mathbb{Z}_p$-Moduln, wobei $W_n = \mu_{p^{n+1}}$ oder $W_n = 0$, je nachdem, ob K_0 die p-ten Einheitswurzeln enthält oder nicht.

Die archimedischen Stellen von K_n^+ in der Erweiterung K_n/K_n^+ sind vollständig verzweigt, denn diese Erweiterung hat den Grad 2 und alle Einbettungen von K_n^+ nach $\mathbb{C}$ liegen in $\mathbb{R}$, während dies für keine Einbettung von K_n gelten kann: $K_n/\mathbb{Q}$ ist eine Galois-Erweiterung, d.h. alle archimedischen Stellen sind unter der Operation von $\mathrm{G}(K_n/\mathbb{Q})$ zueinander konjugiert (siehe [Tat67], Prop. 1.2). Da eine der archimedischen Stellen nicht reell ist, gilt dies für alle archimedischen Stellen.

Infolgedessen ist $\sharp S_{K_n^+,\infty} = \sharp S_{K_n,\infty}$ und es gilt

$$e_-\mathcal{O}^\times_{K_n,S} \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong W_n \times \mathbb{Z}_p^{a_n}$$

mit $a_n \stackrel{def}{=} \sharp S_{K_n,f} - \sharp S_{K_n^+,f}$. Nach Satz 2.2.4, angewendet auf die zyklotomischen $\mathbb{Z}_p$-Erweiterungen K_∞^+/K_0^+ und K_∞/K_0, ist der Wert von a_n ab einem gewissen n_0 konstant.

Im Fall $W_n = \mu_{p^{n+1}}$ liegt das Bild W_{n+1} unter der Normabbildung ganz in W_n. Genauer gilt für eine Einheitswurzel $\zeta \in W_{n+1}$:

$$N_{K_{n+1}/K_n}\zeta = \prod_{\sigma\in\Gamma_{n+1}/\Gamma_n} \sigma\zeta = \prod_{k=0}^{p-1} \zeta^{1+p^{n+2}k} = \zeta^{p+\frac{p^{n+3}(p-1)}{2}} = \zeta^p.$$

Setze $A_n \stackrel{def}{=} \mathbb{Z}_p^{a_n}$. Wir erhalten in beiden Fällen ein kommutatives Diagramm von $\mathbb{Z}_p$-Moduln mit exakten Zeilen

$$\begin{tikzcd}
0 \arrow[r] & W_m \arrow[r] \arrow[d, "p^{m-n}"'] & e_-\mathcal{O}^\times_{K_m,S} \otimes_{\mathbb{Z}} \mathbb{Z}_p \arrow[r] \arrow[d, "N_{K_m/K_n}"'] & A_m \arrow[r] \arrow[d, "f_{m,n}"'] & 0 \\
0 \arrow[r] & W_n \arrow[r] & e_-\mathcal{O}^\times_{K_n,S} \otimes_{\mathbb{Z}} \mathbb{Z}_p \arrow[r] & A_n \arrow[r] & 0
\end{tikzcd}$$

wobei $f_{m,n}$ die von der Norm induzierte Abbildung bezeichnet.

Da A_n ein freier $\mathbb{Z}_p$-Modul ist, gilt dies auch für das Bild von $f_{m,n}$. Setze für jedes $n \in \mathbb{N}$

$$B_n \overset{def}{=} \bigcap_{m=n}^{\infty} \mathrm{Im}(f_{m,n}).$$

Dann ist B_n ein freier $\mathbb{Z}_p$-Modul vom Rang $b_n \leq a_n$ und $f_{m,n}$ lässt sich auf einen surjektiven Homomorphismus $f_{m,n} : B_m \longrightarrow B_n$ einschränken. Wegen $b_n \leq a_n$ ist ab einer gewissen natürlichen Zahl $n_1 \geq n_0$ auch b_n konstant, d.h. $f_{m,n}$ ist für $m \geq n \geq n_1$ ein Isomorphismus von $\mathbb{Z}_p$-Moduln.

Der Übergang zum projektiven Limes im obigen Diagramm liefert somit einen Isomorphismus von $\mathbb{Z}_p$-Moduln

$$\begin{aligned} &\mathrm{H}^1(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) = \\ &\qquad = \varprojlim_n e_- \mathcal{O}_{K_n,S}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathbb{Z}_p^\delta \times \varprojlim_n A_n = \mathbb{Z}_p^\delta \times \varprojlim_n B_n \cong \mathbb{Z}_p^{\delta + b_{n_1}} \end{aligned}$$

mit $\delta = 1$ oder $\delta = 0$, je nachdem, ob K_0 die p-ten Einheitswurzeln enthält oder nicht. □

Bemerkung 6.3.2. Aus den weitaus allgemeineren Betrachtungen in [NSW00], Kap. XI, insbesondere Theorem 11.3.11, folgt in dem Fall $p \nmid \sharp\, \mathrm{G}(K_0/\mathbb{Q})$, dass

$$\mathrm{H}^1(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) = \mathbb{Z}_p(\varepsilon_{cycl}),$$

falls $\mu_p \subset K_0$. Es sollte möglich sein, dies auch im Fall $p \mid \sharp\, \mathrm{G}(K_0/\mathbb{Q})$ zu zeigen.

Lemma 6.3.3. $\mathrm{H}^2(\mathrm{G}_S, \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))$ *ist als* $\mathbb{Z}_p$*-Modul endlich erzeugt.*

Beweis. Wir betrachten die exakte Sequenz aus Satz 6.2.4:

$$0 \longrightarrow \varprojlim_n Cl_S(K_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p \longrightarrow \mathrm{H}^2(\mathrm{G}_S, \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) \longrightarrow \mathbb{Z}_p[S_{K_{n_0},f}] \xrightarrow{\varsigma} \mathbb{Z}_p \longrightarrow 0.$$

Nach dem Theorem von Ferrero-Washington (Theorem 4.2.1) und Lemma 4.1.2 ist $\varprojlim Cl(K_n)$ über $\mathbb{Z}_p$ endlich erzeugt. Dies ändert sich selbstverständlich nicht, wenn wir $Cl(K_n)$ jeweils durch den Faktormodul $Cl_S(K_n)$ ersetzen. Also ist der erste Term und der dritte Term der obigen exakten Sequenz über $\mathbb{Z}_p$ endlich erzeugt, somit aber automatisch auch der zweite Term. □

Wir beweisen nun das oben angekündigte Resultat:

Satz 6.3.4. $C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))$ *ist ein perfekter Torsionskomplex über* Λ *und über* Ω*. Genauer ist bereits die Lokalisierung*

$$C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) \otimes_\Lambda^{\mathbb{L}} \Lambda_{(p)}$$

an dem Primideal (p) *von* Λ *azyklisch. Also gilt dies auch für*

$$C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) \otimes_\Omega^{\mathbb{L}} \Omega_{\mathfrak{p}},$$

wobei $\mathfrak{p}$ *alle Primideale von* Ω *durchläuft, die* $p \in \mathfrak{p}$ *und* $\operatorname{codim} \mathfrak{p} = 1$ *erfüllen.*

Beweis. Wir zeigen zunächst, dass $C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) \otimes^{\mathbb{L}}_\Lambda \Lambda_{(p)}$ azyklisch ist. Da Lokalisierung flach ist, lässt sich dies auf der Kohomologie überprüfen, d.h. es reicht zu zeigen: Für $i = 1, 2$ gilt

$$\mathrm{H}^i(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) \otimes_\Lambda \Lambda_{(p)} = 0.$$

Dies folgt nach Lemma 4.1.2 sofort daraus, dass beide Kohomologie-Moduln über $\mathbb{Z}_p$ endlich erzeugt sind (siehe Lemma 6.3.1 bzw. Lemma 6.3.3). Wegen $\Lambda_{(p)} \subset Q(\Lambda)$ folgt auch

$$C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) \otimes^{\mathbb{L}}_\Lambda Q(\Lambda) = 0.$$

Die entsprechende Aussage für $\Omega_{\mathfrak{p}}$, mit $p \in \mathfrak{p}$ und $\operatorname{codim} \mathfrak{p} = 1$, ergibt sich nach dem folgenden Lemma 6.3.5, angewandt auf $\Lambda \subset \Omega$, für $U = \Lambda \backslash (p)$ und $V = \Omega \backslash \mathfrak{p}$ (beachte, dass $\mathfrak{p} \cap \Lambda = (p)$). Die Aussage für $Q(\Omega)$ lässt sich analog auf die Aussage für $Q(\Lambda)$ reduzieren, indem man für U und V jeweils die Menge der Nichtnullteiler von Λ bzw. Ω wählt. Beachte dabei, dass Ω frei über Λ ist (siehe Lemma 2.3.5). Insbesondere ist die Einbettung $\Lambda \subset \Omega$ fortsetzbar, bildet also Nichtnullteiler auf Nichtnullteiler ab (siehe Lemma 1.2.7). □

Lemma 6.3.5. *Sei $f : A \longrightarrow B$ ein Ringhomomorphismus. $U \subset A$ und $V \subset B$ seien multiplikativ abgeschlossene Mengen mit $f(U) \subset V$. Ist M ein B-Modul mit $M \otimes_A A[U^{-1}] = 0$, so gilt auch $M \otimes_B B[V^{-1}] = 0$.*

Beweis. $M \otimes_B B[V^{-1}] = 0$ gilt genau dann, wenn für jedes $m \in M$ ein $v_m \in V$ mit $v_m m = 0$ existiert. M wird durch die Operation

$$A \times M \longrightarrow M, \qquad (a, m) \mapsto f(a)m$$

zu einem A-Modul. Nach Voraussetzung existiert ein $u_m \in U$ mit $f(u_m)m = 0$ und es gilt $f(U) \subset V$. Damit ist alles bewiesen. □

6.4 Euler-Faktoren

Sei $K_0/\mathbb{Q}$ außerhalb S unverzweigt und $T \overset{def}{=} S \cup \{l\}$ für eine Stelle $l \notin S$ von $\mathbb{Q}$. Wir werden zeigen, dass sich die charakteristischen Ideale von $C^\bullet(\mathrm{G}_T, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))$ und von $C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))$ genau um den Euler-Faktor $1 - e_-\mathcal{F}_l$ unterscheiden.

Setze $\Omega \overset{def}{=} \mathbb{Z}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$. Die Projektion $\kappa : \mathrm{G}_T \longrightarrow \mathrm{G}_S$ induziert für jeden Modul M aus G_S-$Mod_{f.g.}(\Omega)$ einen Ω-Homomorphismus von Komplexen

$$infl : C^\bullet(\mathrm{G}_S, M) \longrightarrow C^\bullet(\mathrm{G}_T, M), \qquad x \mapsto x \circ \kappa$$

(siehe [NSW00], Kap. I, § 5).

Definition 6.4.1. Wir setzen

$$C^\bullet_l(\mathrm{G}_S, M) \overset{def}{=} Cone^\bullet(infl)[-1].$$

Den i-ten Kohomologie-Modul $\mathrm{H}^i_l(\mathrm{G}_S(K), M)$ des Komplexes $C^\bullet_l(\mathrm{G}_S(K), M)$ nennen wir *i-te relative Kohomologie.*

Bemerkung 6.4.2. Siehe Definition 1.5.1 für unsere Vorzeichenkonvention bezüglich des Kegels $Cone^\bullet(f)$ eines Morphismus f. Wir verschieben den Kegel von *infl* um -1, um in der Notation mit der relativen Kohomologie étaler Garben übereinzustimmen.

Bemerkung 6.4.3. $C_l^\bullet(\mathrm{G}_S(K), M)$ ist in der abgeleiteten Kategorie $Der(\Omega)$ durch die Existenz des ausgezeichneten Dreiecks

$$C_l^\bullet(\mathrm{G}_S, M) \longrightarrow C^\bullet(\mathrm{G}_S, M) \xrightarrow{infl} C^\bullet(\mathrm{G}_T, M) \longrightarrow C_l^\bullet(\mathrm{G}_S, M)[1]$$

bis auf Isomorphie eindeutig bestimmt (siehe [GM96], Kap. IV, § 1).

Wir wollen nun die Kohomologie-Moduln $\mathrm{H}_l^i(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))$ berechnen.

Lemma 6.4.4. *Sei $K/\mathbb{Q}$ außerhalb S unverzweigt.*

(i) Folgendes Diagramm ist kommutativ:

$$\begin{tikzcd}
\mathrm{H}^1(\mathrm{G}_S(K), \mathbb{Z}_p(\varepsilon_{cycl})) \arrow[r, "\cong"] \arrow[d, "infl"'] & \mathcal{O}_{K,S}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p \arrow[d, hook] \\
\mathrm{H}^1(\mathrm{G}_T(K), \mathbb{Z}_p(\varepsilon_{cycl})) \arrow[r, "\cong"] & \mathcal{O}_{K,T}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p
\end{tikzcd}$$

(ii) Folgendes Diagramm ist kommutativ und die Zeilen sind exakt:

$$\begin{tikzcd}
0 \arrow[r] & Cl_S(K) \otimes_{\mathbb{Z}} \mathbb{Z}_p \arrow[r] \arrow[d] & \mathrm{H}^2(\mathrm{G}_S(K), \mathbb{Z}_p(\varepsilon_{cycl})) \arrow[r] \arrow[d, "infl"'] & \mathbb{Z}_p[S_{K,f}] \arrow[r, "\varsigma"] \arrow[d, hook] & \mathbb{Z}_p \arrow[r] \arrow[d, "="'] & 0 \\
0 \arrow[r] & Cl_T(K) \otimes_{\mathbb{Z}} \mathbb{Z}_p \arrow[r] & \mathrm{H}^2(\mathrm{G}_T(K), \mathbb{Z}_p(\varepsilon_{cycl})) \arrow[r] & \mathbb{Z}_p[T_{K,f}] \arrow[r, "\varsigma"] & \mathbb{Z}_p \arrow[r] & 0
\end{tikzcd}$$

Zum Beweis. Die Kommutativität der Diagramme überrascht zwar kaum, ein exakter Beweis ist jedoch recht aufwendig. Die wesentlichen Argumente werden in [NSW00], Kapitel VIII, § 3 beschrieben und können ohne größere Probleme auf die vorliegende Situation übertragen werden. Wir geben hier nur eine kurze Skizze.

Wie im Abschnitt 6.2 benutzt man die Kummer-Sequenz, um die Aussage auf die entsprechende Aussage über die Kohomologie von $\mathcal{O}_S^\times = \mathcal{O}_{K_S,S}^\times$ und $\mathcal{O}_T^\times = \mathcal{O}_{K_T,T}^\times$ (mit den maximal außerhalb S bzw. T unverzweigten Erweiterungen K_S und K_T) zu reduzieren. Die Abbildung $\mathrm{H}^i(\mathrm{G}_S, \mathcal{O}_S^\times) \longrightarrow \mathrm{H}^i(\mathrm{G}_T, \mathcal{O}_T^\times)$ ist jedoch nicht *infl*, sondern die Zusammensetzung

$$\mathrm{H}^i(\mathrm{G}_S, \mathcal{O}_{K_S,S}^\times) \longrightarrow \mathrm{H}^i(\mathrm{G}_S, \mathcal{O}_{K_S,T}^\times) \xrightarrow{infl} \mathrm{H}^i(\mathrm{G}_T, \mathcal{O}_{K_T,T}^\times).$$

Die Kommutativität folgt nun für $i = 0$ auf triviale Weise, für $i > 0$ aus einer genauen Analyse der Berechnung der Kohomologiegruppen von $\mathcal{O}_S^\times$ in [NSW00], Kapitel VIII, § 3 und der Ausdehnung der dortigen Ergebnisse auf die Kohomologie von $\mathcal{O}_{K_S,T}^\times$. Dies beinhaltet wiederum eine Berechnung der Kohomologie der entsprechenden S-Idele-Gruppen und S-Idele-Klassengruppen. □

Lemma 6.4.5. *Es gilt*

$$\mathrm{H}_l^i(\mathrm{G}_S, \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) \cong \begin{cases} 0 & \text{für } i \neq 3, \\ \Omega/(1-\mathcal{F}_l) & \text{für } i = 3. \end{cases}$$

Beweis. Das ausgezeichnete Dreieck aus Bemerkung 6.4.3 für $M = \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})$ induziert nach [GM96], Theorem 3.3.6 eine lange exakte Kohomologiesequenz

$$\mathrm{H}^i_l(\mathrm{G}_S, \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) \longrightarrow \mathrm{H}^i(\mathrm{G}_S, \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) \longrightarrow \mathrm{H}^i(\mathrm{G}_T, \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})).$$

Mit Satz 6.2.4 folgt, da

$$\mathrm{H}^1(\mathrm{G}_S, \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) \xrightarrow{infl} \mathrm{H}^1(\mathrm{G}_T, \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))$$

injektiv ist (siehe [NSW00], Satz 1.6.6), $\mathrm{H}^i_l(\mathrm{G}_S, \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) = 0$ für $i \neq 2, 3$.

Wir behandeln nun die Fälle $i = 2$ und $i = 3$. Sei $R_{K_n} = T_{K_n} \setminus S_{K_n}$ die Menge der Stellen von K_n über l. Für $m \geq n > 0$ bezeichne ferner

$$\beta_{K_m/K_n} : \mathbb{Z}[R_{K_m}] \longrightarrow \mathbb{Z}[R_{K_n}]$$

den folgenden Homomorphismus: Für $v \in R_{K_n}$ und $V \in R_{K_m}$ über v sei $f(V|v)$ der Restklassenkörpergrad der entsprechenden lokalen Erweiterung. Dann ist

$$\beta_{K_m/K_n}(V) = f(V|v)v.$$

(Beachte, dass sich β grundlegend von dem in Abschnitt 6.2 benutzten Übergangshomomorphismus α unterscheidet.)

Außerdem betrachten wir die Abbildung

$$val : \mathcal{O}^\times_{K_n,T} \longrightarrow \mathbb{Z}[R_{K_n}], \qquad u \mapsto \sum_{v \in R_{K_n}} val_v(u)v,$$

wobei $val_v(u)$ die Bewertung zu der Stelle v bezeichnet.

Folgendes Diagramm ist damit kommutativ und die Zeilen sind exakt:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}^\times_{K_m,S} \arrow[r] \arrow[d, "N_{K_m/K_n}"'] & \mathcal{O}^\times_{K_m,T} \arrow[r, "val"] \arrow[d, "N_{K_m/K_n}"'] & \mathbb{Z}[R_{K_m}] \arrow[r] \arrow[d, "\beta_{K_m/K_n}"'] & Cl_S(K_m) \arrow[r] \arrow[d, "N_{K_m/K_n}"'] & Cl_T(K_m) \arrow[r] \arrow[d, "N_{K_m/K_n}"'] & 0 \\
0 \arrow[r] & \mathcal{O}^\times_{K_n,S} \arrow[r] & \mathcal{O}^\times_{K_n,T} \arrow[r, "val"] & \mathbb{Z}[R_{K_n}] \arrow[r] & Cl_S(K_n) \arrow[r] & Cl_T(K_n) \arrow[r] & 0
\end{tikzcd}$$

Dies gilt auch noch, wenn man das Diagramm mit $\mathbb{Z}_p$ tensoriert. Nach Satz 2.2.4 gibt es ein n_0, so dass $\sharp R_{K_n}$ für $n \geq n_0$ konstant bleibt. Für $V \in R_{K_m}$, $v \in R_{K_n}$ und $m \geq n \geq n_0$ folgt $f(V|v) = p^{m-n}$, da V unverzweigt über l ist. Mit anderen Worten, β_{K_m/K_n} ist die Multiplikation mit p^{m-n}. Der Übergang zum projektiven Limes liefert

$$\varprojlim_n \mathbb{Z}_p[R_{K_n}] = 0.$$

Man erhält also Isomorphismen

$$\varprojlim_n \mathcal{O}^\times_{K_n,S} \otimes_{\mathbb{Z}} \mathbb{Z}_p = \varprojlim_n \mathcal{O}^\times_{K_n,T} \otimes_{\mathbb{Z}} \mathbb{Z}_p,$$
$$\varprojlim_n Cl_S(K_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p = \varprojlim_n Cl_T(K_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

Da *cor* mit *infl* kommutiert (siehe [NSW00], Satz 1.5.5), können wir auch in Lemma 6.4.4 zum projektiven Limes über die Korestriktionsabbildungen übergehen. Somit gilt:

$$\mathrm{H}^1(\mathrm{G}_S, \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) \xrightarrow[\cong]{infl} \mathrm{H}^1(\mathrm{G}_T, \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))$$

(siehe Satz 5.7.3). Für $n_0 \in \mathbb{N}$ genügend groß ist folgendes Diagramm kommutativ mit exakten Zeilen (siehe Satz 6.2.4):

$$\begin{tikzcd}
0 \arrow[r] & \varprojlim\limits_n Cl_S(K_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p \arrow[r] \arrow[d, "\cong"'] & \mathrm{H}^2(\mathrm{G}_S, \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) \arrow[r] \arrow[d, hook, "infl"'] & \mathbb{Z}_p[S_{K_{n_0},f}] \arrow[r, "\varsigma"] \arrow[d, hook, "j"'] & \mathbb{Z}_p \arrow[r] \arrow[d, "="'] & 0 \\
0 \arrow[r] & \varprojlim\limits_n Cl_T(K_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p \arrow[r] & \mathrm{H}^2(\mathrm{G}_T, \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) \arrow[r] & \mathbb{Z}_p[T_{K_{n_0},f}] \arrow[r, "\varsigma"] & \mathbb{Z}_p \arrow[r] & 0
\end{tikzcd}$$

Folglich ist $\mathrm{H}^2_l(\mathrm{G}_S, \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) = 0$ und

$$\mathrm{H}^3_l(\mathrm{G}_S, \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) \cong \mathrm{Coker}\, j \cong \mathbb{Z}_p[R_{n_0}].$$

Bezeichne $D_l \subset \mathrm{G}(K_\infty/\mathbb{Q})$ die Zerlegungsgruppe von l. Da $K_\infty/\mathbb{Q}$ unverzweigt außerhalb S, also auch in l ist, ist D_l isomorph zur Galoisgruppe der Restklassenkörpererweiterung an der Stelle l. Diese wird von $\mathcal{F}_l$ topologisch erzeugt. Sei nun $v \in R_{n_0}$ eine fest gewählte Stelle. Dann ist die Abbildung

$$\mathrm{G}(K_\infty/\mathbb{Q}) \longrightarrow R_{n_0}, \qquad \sigma \mapsto \sigma v$$

surjektiv, denn die Operation von $\mathrm{G}(K_\infty/\mathbb{Q})$ auf R_{n_0} ist transitiv (siehe [Tat67], Prop. 1.2.(ii)). Nach Definition ist D_l gerade das Urbild von v unter dieser Abbildung (siehe [Was97], Anhang 2 und beachte, dass n_0 beliebig vergrößert werden kann). Wir erhalten somit einen Isomorphismus von Ω-Moduln

$$\Omega/(1-\mathcal{F}_l) = \mathbb{Z}_p[\mathrm{G}(K_\infty/\mathbb{Q})/D_l] \cong \mathbb{Z}_p[R_{n_0}] \cong \mathrm{H}^3_l(\mathrm{G}_S, \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})).$$

□

Wir kommen nun zu dem anfangs angekündigten Ergebnis:

Satz 6.4.6. *Seien $S \subset T$ endliche Mengen von Stellen von $\mathbb{Q}$, welche p und die archimedische Stelle ∞ enthalten. Ferner sei $K_0/\mathbb{Q}$ unverzweigt außerhalb S. Dann gilt*

$$\mathrm{char}\, C^\bullet(\mathrm{G}_T, e_- \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) = \mathrm{char}(C^\bullet(\mathrm{G}_S, e_- \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))) \prod_{l \in T\setminus S} (1 - e_-\mathcal{F}_l).$$

Beweis. Durch Induktion über $\sharp(T \setminus S)$ können wir annehmen, dass $T = S \cup \{l\}$ mit $l \notin S$. Aus Satz 5.5.2 und dem ausgezeichneten Dreieck aus Bemerkung 6.4.3 für $M = \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})$ folgt nach Anwendung des Funktors $\cdot \otimes^{\mathbb{L}}_\Omega e_-\Omega$

$$C^\bullet_l(\mathrm{G}_S, e_- \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) = C^\bullet_l(\mathrm{G}_S, \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) \otimes^{\mathbb{L}}_\Omega e_-\Omega.$$

Der einzige nicht triviale Kohomologie-Modul ist nach Lemma 6.4.5

$$\mathrm{H}^3_l(\mathrm{G}_S, e_- \mathrm{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) = \Omega/(1-\mathcal{F}_l) \otimes_\Omega e_-\Omega = \Omega/(1 - e_-\mathcal{F}_l).$$

(beachte, dass $e_-\Omega$ projektiv und deshalb flach ist). Nun ist $(1 - e_-\mathcal{F}_l)$ ein Nichtnullteiler in Ω (siehe Lemma 3.4.8). Mit Lemma 1.8.1 und Lemma 1.8.2 folgt

$$\operatorname{char} C_l^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) = (1 - e_-\mathcal{F}_l)^{-1}$$

Nach Satz 1.7.7 gilt

$$\begin{aligned}&\operatorname{char}(C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))) = \\ &\qquad = \operatorname{char}(C^\bullet(\mathrm{G}_T, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))) \operatorname{char}(C_l^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))).\end{aligned}$$

Daraus ergibt sich sofort die Behauptung. □

6.5 Die Hauptvermutung für Dirichlet-Charaktere

A. Huber und G. Kings formulieren und beweisen in [HK03] nachfolgende kohomologische Version der Hauptvermutung der Iwasawa-Theorie für Dirichlet-Charaktere (die Notation werden wir weiter unten erläutern):

Theorem 6.5.1 (Hauptvermutung für Dirichlet-Charaktere, [HK03], Theorem 4.2.4). *Sei $p \neq 2$ und θ ein Dirichlet-Charakter mit $\theta(-1) = (-1)^k$. Setze*

$$\Upsilon \overset{def}{=} \mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p[\![\Gamma]\!].$$

Dann ist die p-adische L-Funktion $\tilde{\mathcal{L}}_p(\theta, k)$ ein Erzeuger des Cartier-Divisors

$$\big(\operatorname{char} \mathrm{H}^1_{\mathrm{gl}}(T_p(\theta^{-1})(k))\big)^{-1} \operatorname{char} \mathrm{H}^2_{\mathrm{gl}}(T_p(\theta^{-1})) \in \mathfrak{C}(\Upsilon).$$

Wir wollen dieses Theorem in folgender Form verwenden:

Theorem 6.5.2 (Hauptvermutung für Dirichlet-Charaktere). *Sei p eine ungerade Primzahl. Für einen ungeraden Dirichlet-Charakter θ mit Führer f sei*

$$S(fp) \overset{def}{=} \{\infty\} \cup \{l \,|\, l \text{ Primteiler von } fp\}$$

und $\mathcal{O}_p$ der Bewertungsring eines Erweiterungskörpers endlichen Grades von $\mathbb{Q}_p$, der die Werte von θ enthält, d.h. $\theta : \mathrm{G}_{S(fp)} \longrightarrow \mathcal{O}_p^\times$ ist ein Charakter von endlicher Ordnung. Dann ist die p-adische L-Funktion $\mathcal{L}_p(\theta, 1-k)$ ein Erzeuger des charakteristischen Ideals

$$\operatorname{char} C^\bullet(\mathrm{G}_{S(fp)}, \operatorname{Ind}_{\mathbb{Q}_\infty} \mathcal{O}_p(\theta^{-1}\varepsilon^k_{cycl})) \in \mathfrak{C}(\mathcal{O}_p[\![\Gamma]\!]).$$

Wir werden kurz skizzieren, wie sich Theorem 6.5.1 in Theorem 6.5.2 übersetzen lässt. Dabei müssen wir allerdings eine Annahme über die Euler-Faktoren der verzweigten Primstellen machen, die wir hier nicht beweisen. Im Folgenden verwenden wir ohne weitere Erläuterung die Begriffe der étalen Garbenkohomologie. Eine Einführung in die Theorie étaler Garben findet sich in den Büchern [Tam94] und [Mil80].

In der Notation von Theorem 6.5.1 bezeichnet $\mathcal{O}_F$ den Ganzheitsring eines Zahlkörpers F, der alle Werte des Dirichlet-Charakters θ enthält. Es gilt also

$$\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p = \prod_{v|p} \mathcal{O}_{F_v},$$

wobei v die Stellen von F über p durchläuft und $\mathcal{O}_{F_v}$ der Bewertungsring des lokalen Körpers F_v ist.

Entsprechend ist auch die von A. Huber und G. Kings verwendete p-adische L-Funktion $\tilde{\mathcal{L}}_p(\theta, 1-k)$ ein Element von Υ. Sie ist wie folgt eindeutig charakterisiert: Für jede endliche Erweiterung F'/F und jeden Charakter $\tau : \Gamma \longrightarrow \mathcal{O}_{F'}^{\times}$ endlicher Ordnung gilt:

$$\tau(\tilde{\mathcal{L}}_p(\theta, 1-k)) = (1 - \theta\tau(p)p^{k-1})L(\theta\tau, 1-k) \in \mathcal{O}_{F'} \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

Bemerkung 6.5.3. In [HK03] steht an dieser Stelle $\tau^{-1}(\tilde{\mathcal{L}}_p(\theta, 1-k))$. Dabei handelt es sich jedoch wahrscheinlich um einen Vorzeichenfehler.

Diese L-Funktion hängt wie folgt mit dem von uns definierten Element $\mathcal{L}_p(\theta, 1-k) \in \mathcal{O}_{F_v}[\![\Gamma]\!]$ (siehe Definition 3.4.4) zusammen: Ist $\rho_v : \mathcal{O}_F \longrightarrow \mathcal{O}_{F_v}$ die natürliche Einbettung, so gilt

$$\rho_v(\tilde{\mathcal{L}}_p(\theta, 1-k)) = \mathcal{L}_p(\rho_v \circ \theta, 1-k).$$

Im Wesentlichen ist dies die Projektion auf einen der Faktoren.

$T_p(\theta^{-1})(k)$ bezeichnet einen freien $\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$-Modul vom Rang 1, auf dem die absolute Galoisgruppe $\mathrm{G} \overset{def}{=} \mathrm{G}(\overline{\mathbb{Q}}/\mathbb{Q})$ durch Multiplikation mit $\theta^{-1}\varepsilon_{cycl}^k$ operiert. $T_p(\theta^{-1})(k)$ entspricht in unserer Notation damit dem Modul $(\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p)(\theta^{-1}\varepsilon_{cycl}^k)$ aus $\mathrm{G}\text{-}\mathit{Mod}_{f.g.}(\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p)$.

Ist X ein zusammenhängendes, lokal noethersches Schema, $\bar{x}$ ein geometrischer Punkt, $\pi_1(X, \bar{x})$ die étale Fundamentalgruppe und R eine endliche Erweiterung von $\mathbb{Z}_p$, so ist bekannt, dass die Kategorie $\pi_1(X, \bar{x})\text{-}\mathit{Mod}_{f.g.}(R)$ zu der Kategorie der glatten, konstruierbaren R-Garben auf X äquivalent ist (siehe [KW01], Anhang A). Für uns relevant sind die Schemata $\operatorname{Spec} K$ und $\operatorname{Spec} \mathcal{O}_K[d^{-1}]$, $d \in \mathbb{Z}$ für Zahlkörper K. Es gilt

$$\pi_1(\operatorname{Spec} K, \overline{\eta}) = \mathrm{G}(\overline{\mathbb{Q}}/K), \qquad \pi_1(\operatorname{Spec} \mathcal{O}_K[d^{-1}], \overline{\eta}) = \mathrm{G}_{S(d)}(K)$$

mit

$$S(d) \overset{def}{=} \{\text{archimedische Stellen von } K\} \cup \{\text{Stellen über Primteilern von } d\}$$

(siehe [Mil80], Kap. I, Beispiel 5.2.(a) und (b)).

Sei $j : \operatorname{Spec} \mathbb{Q} \longrightarrow \operatorname{Spec} \mathbb{Z}$. Dann ist nach Definition

$$\mathrm{H}^i_{\mathrm{gl}}(T_p(\theta^{-1})(k)) \overset{def}{=} \varprojlim_n \mathrm{H}^i_{\text{ét}}(\operatorname{Spec} \mathcal{O}_{\mathbb{Q}_n}[p^{-1}], j_* T_p(\theta^{-1})),$$

wobei die étalen Kohomologiegruppen $\mathrm{H}^i_{\text{ét}}(\operatorname{Spec} \mathcal{O}_{\mathbb{Q}_n}[p^{-1}], j_* T_p(\theta^{-1}))$ durch die Operation von $\Gamma_n = \mathrm{G}(\mathbb{Q}_n/\mathbb{Q})$ auf $\operatorname{Spec} \mathcal{O}_{\mathbb{Q}_n}[p^{-1}]$ als $\mathbb{Z}_p[\Gamma_n]$-Moduln aufgefasst werden und der projektive Limes bezüglich der Korestriktionsabbildung gebildet wird. Die Υ-Moduln $\mathrm{H}^i_{\mathrm{gl}}(T_p(\theta^{-1})(k))$ sind für alle i endlich erzeugte Torsions-Moduln und trivial für $i \neq 1, 2$ (siehe [HK03], Prop. 4.2.1). Ferner ist Υ ein endliches direktes Produkt lokaler regulärer Ringe der Dimension 2 (siehe Satz 2.3.3). Also existiert das charakteristische Ideal der Kohomologie-Moduln (siehe Lemma 1.9.3).

Die étale Kohomologie hängt wie folgt mit stetiger Galois-Kohomologie zusammen:

Satz 6.5.4. *Sei R eine endliche Erweiterung von $\mathbb{Z}_p$, $d \in \mathbb{Z}$, $\mathcal{F}$ eine glatte, konstruierbare R-Garbe auf $\mathcal{O}_K[(dp)^{-1}]$ und M der Modul aus $\mathrm{G}(\overline{\mathbb{Q}}/K)$-$Mod_{f.g.}(R)$, der dem Halm von $\mathcal{F}$ im generischen Punkt entspricht. Dann gilt für $r \geq 0$:*

$$\mathrm{H}^r_{\text{ét}}(\operatorname{Spec} \mathcal{O}_K[(dp)^{-1}], \mathcal{F}) = \mathrm{H}^r(\mathrm{G}_{S(dp)}(K), M).$$

Zum Beweis: In [Mil86], Kap. II, Prop. 2.9 wird dies für lokal-konstante, konstruierbare p-Torsions-Garben gezeigt. Das Ergebnis lässt sich nun leicht auf den Fall von glatten, konstruierbaren R-Garben verallgemeinern.

Trotz der oben erwähnten Kategorien-Äquivalenz zwischen glatten, konstruierbaren R-Garben und den Moduln aus $\pi_1(X, \bar{x})$-$Mod_{f.g.}(R)$ ist dieses Ergebnis keineswegs trivial und lässt sich auch nicht ohne weiteres auf allgemeinere Schemata X ausdehnen. □

Beachte, dass $j_* T_p(\theta^{-1})(k)$ nur dann glatt ist, wenn die Operation von G auf $T_p(\theta^{-1})(k)$ durch $\mathrm{G}_{S(p)}$ faktorisiert, d.h. wenn der Führer f von θ ein Vielfaches von p ist. Die relative Kohomologie-Sequenz (siehe [Mil80], Kap. III, Prop. 1.25)

$$\bigoplus_{v \in S(fp) \setminus S(p)} (\mathrm{H}_{\text{ét}})^i_v(X_K, j_* T_p(\theta^{-1})(k)) \longrightarrow \mathrm{H}^i_{\text{ét}}(X_K, j_* T_p(\theta^{-1})(k)) \longrightarrow \mathrm{H}^i_{\text{ét}}(U_K, T_p(\theta^{-1})(k))$$

für $X_K = \operatorname{Spec} \mathcal{O}_K[p^{-1}]$, $U_K = \operatorname{Spec} \mathcal{O}_K[(fp)^{-1}]$, erlaubt es uns, auch im allgemeinen Fall $\mathrm{H}^i_{\text{ét}}(X_K, j_* T_p(\theta^{-1})(k))$ mit Galois-Kohomologie in Verbindung zu bringen.

Sei

$$\mathrm{H}^i_{X \setminus U}(T_p(\chi^{-1})(k)) \stackrel{\mathit{def}}{=} \varprojlim_n \bigoplus_{v \in S_{K_n}(fp) \setminus S_{K_n}(p)} (\mathrm{H}_{\text{ét}})^i_v(j_* T_p(\theta^{-1})(k)).$$

Es liegt nahe, dass das charakteristische Ideal von $\mathrm{H}^i_{X \setminus U}(T_p(\chi^{-1})(k))$ gleich dem Produkt der Euler-Faktoren zu $l \mid f$, $l \neq p$ ist. Nun folgt aber $(1 - \chi(l)\mathcal{F}_l) = 1$ wegen $\chi(l) = 0$. Also sollte gelten:

Vermutung 6.5.5. $\mathrm{H}^i_{X \setminus U}(T_p(\chi^{-1})(k))$ *ist für $i = 2, 3$ endlich und für alle anderen i trivial.*

Diese Vermutung vorausgesetzt, folgt aus der relativen Kohomologie-Sequenz (nach Übergang zum projektiven Limes) mit Satz 1.7.7 und Lemma 1.9.3:

$$\operatorname{char} C^\bullet(\mathrm{G}_S, T_p(\theta^{-1})(k)) = (\operatorname{char} \mathrm{H}^1_{\mathrm{gl}}(T_p(\theta^{-1})(k)))^{-1} \operatorname{char} \mathrm{H}^2_{\mathrm{gl}}(T_p(\theta^{-1})).$$

Anwenden der Projektion

$$\Upsilon \longrightarrow \mathcal{O}_{F_v}[\![\Gamma]\!]$$

für eine beliebige Stelle v von F über p liefert dann Theorem 6.5.2.

6.6 Zerlegung unter Charakteren

Sei wieder K_∞ / K_0 die zyklotomische $\mathbb{Z}_p$-Erweiterung eines abelschen Zahlkörpers K_0 mit $K_0 \cap \mathbb{Q}_\infty = \mathbb{Q}$. Die Menge S enthalte p, ∞ und alle in $K_0/\mathbb{Q}$ verzweigten Stellen, d.h. $\mathrm{G}(K_\infty/\mathbb{Q})$ ist eine Faktorgruppe von G_S.

Setze $\Omega \stackrel{def}{=} \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$. Durch die Verdrehung um χ (siehe Definition 2.10.1)

$$Tw_\chi : \Omega \longrightarrow \Omega$$

wird Ω zu einer Algebra über sich selbst. Zur besseren Orientierung bezeichnen wir diese Algebra mit $Tw_\chi(\Omega)$. Jeden Modul M aus $\mathrm{G}_S\text{-}Mod_{f.g.}(\Omega)$ kann man nun auf zwei verschiedene Weisen nach $\mathrm{G}_S\text{-}Mod_{f.g.}(Tw_\chi(\Omega))$ verpflanzen: zum einen durch die natürliche Identifikation $Tw_\chi(\Omega) = \Omega$ unter Missachtung der Algebren-Struktur (diesen Modul nennen wir weiterhin M), zum anderen durch die Koeffizientenerweiterung $Tw_{\chi*}$ (siehe Definition 1.1.2).

Ist ferner $\theta : \mathrm{G}(K_0/\mathbb{Q}) \longrightarrow \mathcal{O}_p^\times$ ein Charakter des Grundkörpers K_0, so bezeichne $p_\theta : \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!] \longrightarrow \mathcal{O}_p[\![\mathrm{G}(\mathbb{Q}_\infty/\mathbb{Q})]\!]$ die entsprechende Projektion (siehe Abschnitt 2.6).

Lemma 6.6.1. *Es gilt*

$$Tw_{\chi*} \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\varepsilon_{cycl}) = \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\chi^{-1}\varepsilon_{cycl})$$

und

$$p_{\theta*} \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\varepsilon_{cycl}) = \operatorname{Ind}_{\mathbb{Q}_\infty} \mathcal{O}_p(\theta^{-1}\varepsilon_{cycl}).$$

Beweis. Nach Definition (siehe Abschnitt 5.5) ist $Tw_{\chi*} \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\varepsilon_{cycl})$ der freie $Tw_\chi(\Omega)$-Modul

$$\Omega \otimes_\Omega Tw_{\chi*}(\Omega)$$

mit der G_S-Operation

$$\begin{aligned} g(1 \otimes 1) &= (\Psi_{K_\infty}(g^{-1})\varepsilon_{cycl}(g)) \otimes 1 \\ &= 1 \otimes (Tw_\chi(\Psi_{K_\infty}(g^{-1})\varepsilon_{cycl}(g))) \\ &= 1 \otimes (\chi^{-1}\varepsilon_{cycl}(g)\Psi_{K_\infty}(g^{-1})). \end{aligned}$$

Die Abbildung

$$Tw_{\chi*} \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\varepsilon_{cycl}) \longrightarrow \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\chi^{-1}\varepsilon_{cycl}), \qquad a \otimes b \mapsto Tw_\chi(a)b$$

ist damit klar der gesuchte G_S-äquivariante Isomorphismus von $Tw_\chi(\Omega)$-Moduln.

Beachte nun, dass $p_\theta = p_\Gamma \circ Tw_\theta$, wobei

$$p_\Gamma : \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!] \longrightarrow \mathcal{O}_p[\![\mathrm{G}(\mathbb{Q}_\infty/\mathbb{Q})]\!]$$

die natürliche Projektion bezeichnet. Die zweite Aussage des Lemmas folgt somit aus der ersten und Lemma 5.7.6. □

Das folgende Lemma ist eine weitere Umformulierung von Theorem 6.5.2. Es erlaubt nun beliebige Vergrößerung der Ausnahmemenge S und stellt den Zusammenhang zum eingangs betrachteten Komplex $C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))$ her.

Lemma 6.6.2. *Sei* $\theta : \mathrm{G}(K_0/\mathbb{Q}) \longrightarrow \mathcal{O}_p^\times$ *ein ungerader Charakter.* S *sei eine endliche Menge von Stellen von* $\mathbb{Q}$*, die* p*,* ∞ *und die in* $K_0/\mathbb{Q}$ *verzweigten Stellen enthält. Ferner sei*

$$T \stackrel{def}{=} \{p, \infty\} \cup \{\textit{Primteiler des Führers von } \theta\} \subset S.$$

Dann ist $\mathcal{L}_p(\theta, 0) \prod_{l \in S \setminus T} (1 - p_\theta(\mathcal{F}_l))$ *ein Erzeuger von*

$$\mathfrak{C}(p_\theta)\big(\operatorname{char} C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\varepsilon_{cycl}))\big) \in \mathfrak{C}(\Omega).$$

Ist θ *ein gerader Charakter, so gilt*

$$\mathfrak{C}(p_\theta)\big(\operatorname{char} C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\varepsilon_{cycl}))\big) = (1) \in \mathfrak{C}(\Omega).$$

Beweis. Sei $L_0 \overset{def}{=} K_0^{\operatorname{Ker}\theta}$. Die Charaktergruppe von L_0 wird von θ erzeugt. Nach Theorem 2.1.3 sind die endlichen verzweigten Stellen von $L_0/\mathbb{Q}$ genau die Primteiler des Führers f von θ, d.h. $L_0/\mathbb{Q}$ ist außerhalb S unverzweigt. Betrachte die natürliche Projektion $\psi : \mathrm{G}(K_0/\mathbb{Q}) \longrightarrow \mathrm{G}(L_0/\mathbb{Q})$. Wir erhalten ein kommutatives Diagramm

$$\begin{tikzcd}
\mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!] \arrow[r, "\psi"] \arrow[dr, "p_\theta"'] & \mathcal{O}_p[\![\mathrm{G}(L_\infty/\mathbb{Q})]\!] \arrow[d, "p_\theta"] \\
& \mathcal{O}_p[\![\mathrm{G}(\mathbb{Q}_\infty/\mathbb{Q})]\!]
\end{tikzcd}$$

Für ungerade Charaktere θ folgt:

$$\begin{aligned}
&\mathfrak{C}(p_\theta \circ \psi)\big(\operatorname{char} C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\varepsilon_{cycl}))\big) = \\
&= \mathfrak{C}(p_\theta)\big(\operatorname{char} \mathbf{L}\psi_* C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\varepsilon_{cycl}))\big) && \text{nach Satz 1.7.8,} \\
&= \mathfrak{C}(p_\theta)\big(\operatorname{char} C^\bullet(\mathrm{G}_S, \psi_*(e_- \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\varepsilon_{cycl})))\big) && \text{nach Satz 5.5.2,} \\
&= \mathfrak{C}(p_\theta)\big(\operatorname{char} C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{L_\infty} \mathcal{O}_p(\varepsilon_{cycl}))\big) && \text{nach Lemma 5.7.6,} \\
&= \mathfrak{C}(p_\theta)\Big(\operatorname{char}(C^\bullet(\mathrm{G}_T, e_- \operatorname{Ind}_{L_\infty} \mathcal{O}_p(\varepsilon_{cycl}))) \prod_{l \in S \setminus T} (1 - e_- \mathcal{F}_l)\Big) && \text{nach Lemma 6.4.6,} \\
&= \operatorname{char}(C^\bullet(\mathrm{G}_T, p_{\theta *} \operatorname{Ind}_{L_\infty} \mathcal{O}_p(\varepsilon_{cycl}))) \prod_{l \in S \setminus T} (1 - p_\theta(\mathcal{F}_l)) && \text{weil } p_\theta(e_-) = 1, \\
&= \operatorname{char}(C^\bullet(\mathrm{G}_T, \operatorname{Ind}_{\mathbb{Q}_\infty} \mathcal{O}_p(\theta^{-1}\varepsilon_{cycl}))) \prod_{l \in S \setminus T} (1 - p_\theta(\mathcal{F}_l)) && \text{nach Lemma 6.6.1}
\end{aligned}$$

und nach Theorem 6.5.2 ist $\mathcal{L}_p(\theta, 0)$ ein Erzeuger von

$$\operatorname{char} C^\bullet(\mathrm{G}_T, \operatorname{Ind}_{\mathbb{Q}_\infty} \mathcal{O}_p(\theta^{-1}\varepsilon_{cycl})).$$

Für gerade Charaktere θ folgt die Behauptung aus der gleichen Rechnung wegen $p_\theta(e_-) = 0$. $\square$

6.7 Abschluss des Beweises

Wir führen nun den Beweis von Theorem 6.1.1 und von Folgerung 6.1.2 zu Ende.

Beweis von Theorem 6.1.1. Sei $D \in \mathfrak{C}(\mathbb{Z}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!])$ der von der äquivarianten L-Funktion $\mathcal{L}_{p,S}(K_\infty, \mathbb{1})$ erzeugte Cartier-Divisor. Wir wollen zeigen:

$$D = \operatorname{char} C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})).$$

Nach Satz 1.3.2 genügt es zu überprüfen, dass die Lokalisierungen beider Cartier-Divisoren für alle Primideale $\mathfrak{p}$ der Kodimension 1 übereinstimmen.

Wir wissen bereits, dass die Lokalisierungen beider Divisoren für solche $\mathfrak{p}$, die p enthalten, die trivialen Divisoren sind: Für D haben wir dies in Folgerung 4.9.1 bewiesen. Für das charakteristische Ideal von $C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))$ folgt dies aus Satz 6.3.4 und Lemma 1.7.5.(i).

Für alle anderen Primideale $\mathfrak{p}$ der Kodimension 1 folgt die Gleichheit im Wesentlichen aus Folgerung 3.4.7 zusammen mit Theorem 6.5.2. Dabei trifft man noch auf einige kleinere technische Schwierigkeiten, auf die wir im Folgenden eingehen werden.

Im ersten Schritt wollen wir den Ring $\mathbb{Z}_p$ durch den Bewertungsring $\mathcal{O}_p$ eines Erweiterungskörpers endlichen Grades von $\mathbb{Q}_p$ ersetzen, der alle Werte der Charaktere auf $\Delta = \mathrm{G}(K_0/\mathbb{Q})$ enthält (dabei bezeichnet K_0 wie üblich den Fixkörper K_∞^Γ, siehe Abschnitt 2.2). Sei $\Omega \overset{def}{=} \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$ und

$$\kappa : \mathbb{Z}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!] \longrightarrow \Omega$$

die natürliche Inklusion. Nach Lemma 2.9.3 ist der induzierte Homomorphismus

$$\mathfrak{C}(\kappa) : \mathfrak{C}(\mathbb{Z}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]) \longrightarrow \mathfrak{C}(\Omega)$$

injektiv. Andererseits gilt nach Satz 1.7.8, Satz 5.5.2 und Bemerkung 5.7.7

$$\mathfrak{C}(\kappa)\big(\operatorname{char} C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl}))\big) = \operatorname{char} C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\varepsilon_{cycl})).$$

Sei $\imath_\mathfrak{p} : \Omega \longrightarrow \Omega_\mathfrak{p}$ die Lokalisierungsabbildung für ein Primideal $\mathfrak{p}$ von Ω mit $\operatorname{codim} \mathfrak{p} = 1$. Falls $p \in \mathfrak{p}$, so gilt nach Folgerung 4.9.1 immer noch

$$\mathfrak{C}(\imath_\mathfrak{p}) \circ \mathfrak{C}(\kappa)\big(D\big) = \mathfrak{C}(\imath_\mathfrak{p}) \circ \mathfrak{C}(\kappa)\big(\operatorname{char} C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathbb{Z}_p(\varepsilon_{cycl})) = (1) \in \mathfrak{C}(\Omega_\mathfrak{p})\big).$$

Wir können deshalb annehmen, dass $p \notin \mathfrak{p}$. Sei $\mathfrak{q} = \mathfrak{p} \cap \mathcal{O}_p[\![\Gamma]\!]$. Nach Lemma 2.8.1 gibt es einen Charakter θ, so dass folgendes Diagramm kommutiert:

$$\begin{tikzcd} \Omega \arrow[r, "p_\theta"] \arrow[d, "\imath_\mathfrak{p}"'] & \mathcal{O}_p[\![\Gamma]\!] \arrow[d, "\imath_\mathfrak{q}"] \\ \Omega_\mathfrak{p} \arrow[r, "(p_\theta)_\mathfrak{q}", "\cong"'] & \mathcal{O}_p[\![\Gamma]\!]_\mathfrak{q} \end{tikzcd}$$

Somit reicht es zu zeigen, dass $p_\theta(\mathcal{L}_{p,S}(K_\infty, \mathbb{1}))$ für alle Charaktere $\theta \in \widehat{\Delta}$ ein Erzeuger von

$$\mathfrak{C}(p_\theta)\big(\operatorname{char} C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\varepsilon_{cycl}))\big) \in \mathfrak{C}(\mathcal{O}_p[\![\Gamma]\!])$$

ist. Nach Folgerung 3.4.7 gilt

$$p_\theta(\mathcal{L}_{p,S}(K_\infty, \mathbb{1})) = \begin{cases} \mathcal{L}_p(\theta, 0) \prod\limits_{l \in S \setminus T} (1 - p_\theta(\mathcal{F}_l)) & \text{für } \theta(-1) = -1, \\ 1 & \text{für } \theta(-1) = 1, \end{cases}$$

mit

$$T \overset{def}{=} \{p, \infty\} \cup \{\text{Primteiler des Führers von } \theta\} \subset S.$$

Die Behauptung folgt nun direkt aus Lemma 6.6.2. □

Beweis von Folgerung 6.1.2. Sei $\chi : \mathrm{G}_S \longrightarrow \mathcal{O}_p^\times$ ein stetiger Charakter. Wir wollen zeigen, dass $\mathcal{L}_{p,S}(K_\infty, \chi)$ ein Erzeuger des charakteristischen Ideals

$$\operatorname{char} C^\bullet(\mathrm{G}_S,\, Tw_\chi(e_-) \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\chi^{-1}\varepsilon_{cycl}))$$

ist.

Wir betrachten zunächst den Fall, dass χ durch $\mathrm{G}(K_\infty/\mathbb{Q})$ faktorisiert. Damit ist Tw_χ ein Automorphismus von $\Omega \overset{def}{=} \mathcal{O}_p[\![\mathrm{G}(K_\infty/\mathbb{Q})]\!]$. Wir schreiben wieder $Tw_\chi(\Omega)$ für den Ring Ω mit der durch Tw_χ vermittelten Algebren-Struktur, fassen aber $C^\bullet(\mathrm{G}_S,\, Tw_\chi(e_-) \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\chi^{-1}\varepsilon_{cycl}))$ unter Missachtung dieser Algebren-Struktur als Komplex über $Tw_\chi(\Omega)$ auf. Damit sind wir in der Lage, die bereitgestellten Sätze anzuwenden und erhalten

$$\begin{aligned}
&\operatorname{char} C^\bullet(\mathrm{G}_S,\, Tw_\chi(e_-) \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\chi^{-1}\varepsilon_{cycl})) = && \\
&= \operatorname{char} C^\bullet(\mathrm{G}_S,\, Tw_{\chi*}(e_- \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\varepsilon_{cycl}))) && \text{nach Lemma 6.6.1,} \\
&= \operatorname{char} \mathbf{L}\, Tw_{\chi*} C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\varepsilon_{cycl})) && \text{nach Satz 5.5.2,} \\
&= \mathfrak{C}(Tw_\chi)\big(\operatorname{char} C^\bullet(\mathrm{G}_S, e_- \operatorname{Ind}_{K_\infty} \mathcal{O}_p(\varepsilon_{cycl}))\big) && \text{nach Satz 1.7.8,} \\
&= Tw_\chi\big(\mathcal{L}_{p,S}(K_\infty, \mathbb{1})\big)\, Tw_\chi(\Omega) && \text{nach Theorem 6.1.1,} \\
&= \mathcal{L}_{p,S}(K_\infty, \chi)\, Tw_\chi(\Omega) && \text{nach Definition, siehe Abschnitt 3.3.}
\end{aligned}$$

Indem wir nun die Algebren-Struktur wieder vergessen, folgt die Behauptung.

Faktorisiert χ nicht durch $\mathrm{G}(K_\infty/\mathbb{Q})$, so ersetze man K durch einen entsprechenden größeren Körper. Die Aussage folgt nun wegen der Kompatibilität beider Seiten mit Projektionen (siehe Lemma 5.7.6 und Lemma 3.3.3). □

Danksagung

Hiermit möchte ich mich herzlich bei Frau Professor Dr. Annette Huber-Klawitter bedanken, die mir die interessante Aufgabe gestellt hat, das vorliegende Thema zu bearbeiten, und das Entstehen dieser Arbeit mit viel Geduld und gutem Rat begleitet hat. Ich danke ihr insbesondere für die viele Zeit, die sie sich nahm, um auftauchende Probleme zu diskutieren, und für die Anregungen, die ich durch diese Diskussionen erhalten habe. Mein Dank gilt ferner Herrn R. Munck und Herrn B. Friedrich, die das Manuskript mit großer Sorgfalt geprüft haben.

Literaturverzeichnis

[BG03] Burns, David ; Greither, Cornelius: On the Equivariant Tamagawa Number Conjecture for Tate Motives. In: *Invent. Math.* (2003), Nr. 153, S. 303–359

[Bou89a] Bourbaki, Nicolas: *Algebra I.* Springer Verlag, 1989 (Elements of Mathematics)

[Bou89b] Bourbaki, Nicolas: *Commutative Algebra.* Springer Verlag, 1989 (Elements of Mathematics)

[Brü95] Brüdern, Jörg: *Einführung in die analytische Zahlentheorie.* Springer Verlag, 1995

[Bru66] Brumer, Armand: Pseudocompact Algebras, Profinite Groups and Class Formations. In: *Journal of Algebra* (1966), Nr. 4, S. 442–470

[Cas67] Cassels, J.W.S.: Global Fields. In: Cassels, J.W.S. (Hrsg.) ; Fröhlich, A. (Hrsg.): *Algebraic Number Theory* London Mathematical Society, Academic Press, 1967, S. 42–83

[Col98] Colmez, Pierre: Théorie d'Iwasawa des répresentations de de Rham d'un corps local. In: *Annals of Mathematics* (1998), Nr. 148, S. 485–571

[Del87] Deligne, Pierre: Le Déterminant de la Cohomologie. In: *Current Trends in Arithmetical Algebraic Geometry.* American Math. Soc., 1987 (Contemp. Math. 67), S. 93–177

[Eis99] Eisenbud, David: *Commutative Algebra with a View Toward Algebraic Geometry.* 3. New York : Springer Verlag, 1999 (Graduate Texts in Mathematics 150)

[Eke90] Ekedahl, Torsten: On the Adic Formalism. In: *The Grothendieck Festschrift* Bd. II. Boston, MA : Birkhäuser, 1990, S. 197–218

[FK88] Freitag, Eberhard ; Kiehl, Reinhardt: *Etale Cohomology and the Weil Conjecture.* Berlin : Springer Verlag, 1988 (Ergebnisse der Mathematik und ihrer Grenzgebiete (3) 13)

[FW79] Ferrero, B. ; Washington, L.C.: The Iwasawa Invariant μ_p Vanishes for Abelian Number Fields. In: *Ann. of Math.* (1979), Nr. 109, S. 377–395

[GM96] Gelfand, S.I. ; Manin, Yu.I.: *Methods of Homological Algebra.* Berlin Heidelberg : Springer Verlag, 1996

[Har77] HARTSHORNE, Robin: *Algebraic Geometry.* New York : Springer-Verlag, 1977 (Graduate Texts in Mathematics 52)

[HK03] HUBER, Annette ; KINGS, Guido: Bloch-Kato Conjecture and Main Conjecture of Iwasawa Theory for Dirichlet Characters. In: *Duke Mathematical Journal* 119 (2003), Nr. 3, S. 395–464

[Kat93] KATO, Katsuya: Iwasawa Theory and p-adic Hodge theory. In: *Kodai Math. J.* 16 (1993), Nr. 1, S. 1–31

[KM76] KNUDSEN, Finn ; MUMFORD, David: The Projectivity of the Moduli Spaces of Stable Curves I. In: *Math. Scand.* 39 (1976), Nr. 1, S. 19–55

[KW01] KIEHL, Reinhardt ; WEISSAUER, Rainer: *Weil Conjectures, Perverse Sheaves and l'adic Fourier Transform.* Berlin, 2001 (Ergebnisse der Mathematik und ihrer Grenzgebiete (3) 42)

[Leu96] LEUTBECHER, Armin: *Zahlentheorie.* Springer, 1996

[Mil80] MILNE, James S.: *Etale Cohomology.* New Jersey : Princeton University Press, 1980 (Princeton Mathematical Series 33)

[Mil86] MILNE, James S.: *Arithmetic Duality Theorems.* Boston, MA : Academic Press, Inc., 1986 (Perspectives in Mathematics 1)

[MW86] MAZUR, Berry ; WILES, Andrew: Class Fields of Abelian Extensions of $\mathbb{Q}$. In: *Invent. Math.* (1986), Nr. 76, S. 179–330

[NSW00] NEUKIRCH, Jürgen ; SCHMIDT, Alexander ; WINGBERG, Kay: *Cohomology of Number Fields.* Berlin Heidelberg : Springer Verlag, 2000 (Grundlehren der mathematischen Wissenschaften 323)

[Rub00] RUBIN, Karl: *Euler Systems.* New Jersey : Princenton University Press, 2000 (Annals of Mathematics Studies 147)

[Ser64] SERRE, Jean-Pierre: Cohomologie galoisienne. In: *Lecture Notes in Mathematics, No. 5.* Springer, 1964

[Sin84] SINNOTT, W.: On the μ-Invariant of the Γ-Transform of a Rational Function. In: *Invent. Math.* (1984), Nr. 75, S. 273–282

[Tam94] TAMME, Günter: *Introduction to Etale Cohomology.* Berlin Heidelberg : Springer-Verlag, 1994 (Universitext)

[Tat67] TATE, J.T.: Global Class Field Theory. In: CASSELS, J.W.S. (Hrsg.) ; FRÖHLICH, A. (Hrsg.): *Algebraic Number Theory* London Mathematical Society, Academic Press, 1967, S. 162–203

[Tat76] TATE, J.T.: Relations Between K_2 and Galois Cohomology. In: *Invent. Math.* (1976), Nr. 36, S. 257–274

[Was89] WASHINGTON, Lawrence C.: On Sinnot's Proof of the Vanishing of the Iwasawa Invariant μ_p. In: *Algebraic Number Theory – In Honor of K. Iwasawa*. Orlando, FL : Academic Press, 1989 (Advanced Studies in Pure Mathematics 17), S. 457–462

[Was97] WASHINGTON, Lawrence C.: *Introduction to Cyclotomic Fields*. 2. New York : Springer-Verlag, 1997 (Graduate Texts in Mathematics 83)

[Wil90] WILES, Andrew: The Iwasawa Conjecture for Totally Real Fields. In: *Ann. of. Math.* (1990), Nr. 131, S. 97–127

Symbolverzeichnis

(a, b)	größter gemeinsamer Teiler von a und b
$\{y\}$	gebrochener Anteil von y, siehe Seite 50
$[y]$	ganzer Anteil von y, siehe Seite 50
$\langle\cdot\rangle$	Projektion $\mathbb{Z}_p^\times \longrightarrow 1 + p\mathbb{Z}_p$, siehe Seite 61
$A \hookrightarrow B$	Inklusion
$A \twoheadrightarrow B$	Projektion
$M \setminus N$	Komplement der Menge N in M
$\mathbb{1}$	trivialer Charakter, siehe Seite 23
$a \equiv b \bmod c$	a ist kongruent b modulo c
$a \overset{def}{\equiv} b$	a wird durch b definiert
$A \cong B$	A ist isomorph zu B
$\tau_{\geq k} K^\bullet$	Abschneide-Operator, siehe Seite 20
∞	archimedische Stelle von $\mathbb{Q}$
∂	Differential eines Komplexes
$\alpha_{L'/L}$	Übergangsabbildung, siehe Seite 89
χ, θ, τ	Charaktere
Δ	Galoisgruppe $\mathrm{G}(K_0/\mathbb{Q})$, siehe Seite 27
ε_{cycl}	zyklotomischer Charakter, siehe Seite 26
ε_∞	Anteil unendlicher Ordnung von ε_{cycl}, siehe Seite 26
ε	Anteil endlicher Ordnung von ε_{cycl}, siehe Seite 26
η	Einbettung $R \longrightarrow Q(R)$, siehe Seite 13
Γ	die Galoisgruppe $\mathrm{G}(\mathbb{Q}_\infty/\mathbb{Q})$, siehe Seite 25
Γ_n	die Galoisgruppe $\mathrm{G}(\mathbb{Q}_n/\mathbb{Q})$, siehe Seite 25
γ	topologischer Erzeuger von Γ

λ	Isomorphismus $\det_S P^\bullet \longrightarrow S$ für azyklische Komplexe, siehe Seite 14
Λ	Iwasawa-Algebra, siehe Seite 29
ζ_N	primitive N-te Einheitswurzel
$\mu(M)$	μ-Invariante, siehe Seite 59
μ_n	Gruppe der n-ten Einheitswurzeln
$\omega_n(T)$	das Polynom $(T+1)^{p^n} - 1$, siehe Seite 62
$\pi_{m,n}$	Projektion $\mathrm{G}(K_m/\mathbb{Q}) \longrightarrow \mathrm{G}(K_n/\mathbb{Q})$, siehe Seite 29
$\pi_1(X, \bar{x})$	étale Fundamentalgruppe des Schemas X, siehe Seite 74
ψ	Projektion $\mathrm{G}(K_\infty/\mathbb{Q}) \longrightarrow \mathrm{G}(L_\infty/\mathbb{Q})$, siehe Seite 36
Ψ_K	Projektion $\mathrm{G}_S \longrightarrow \mathrm{G}(K/\mathbb{Q})$, siehe Seite 85
ς	Summationsabbildung, siehe Seite 89
ξ_N	Stickelberger-Element, siehe Seite 46
$f \circ g$	Verknüpfung der Abbildungen f und g
$\sharp M$	Kardinalität der Menge M
$K^\bullet$	Komplex, siehe Seite 13
$A^\times$	Einheitengruppe von A
$\check{P}$	Dual eines projektiven Moduls P, siehe Seite 6
$\widehat{A}$	Charaktergruppe, siehe Seite 23
$a \wedge b$	äußeres Produkt von a und b
$\mathbb{Q}^{ab}$	maximale abelsche Erweiterung von $\mathbb{Q}$
G^{ab}	maximaler abelscher Quotient der Gruppe G
M^G	Modul der Invarianten unter der Operation von G auf M
$\mathbf{L}\phi_*$	links-abgeleitete Koeffizientenerweiterung, siehe Seite 13
$A[U^{-1}]$	Lokalisierung an der multiplikativ abgeschlossenen Menge U
$A[G]$	Gruppenring, siehe Seite 29
$A[T]$	Polynomring in der Unbestimmten T
$A[f^{-1}]$	Lokalisierung an den Potenzen von f
$A[S]$	von der G-Menge S über A frei erzeugter G Modul, siehe Seite 89

$A[\![T]\!]$	Potenzreihenring in T
$A[\![G]\!]$	pro-endlicher Gruppenring, siehe Seite 33
$\bigwedge^r A$	r-te äußere Potenz
$\bigwedge_R(M)$	äußere Algebra von M
$A \oplus B$	direkte Summe von A und B
$K^\bullet \otimes_R^{\mathbb{L}} M$	links-abgeleitetes Tensorprodukt, siehe Seite 13
$A \otimes_C B$	Tensorprodukt von A und B über C
$\mathbf{b}(\phi)$	Isomorphismus von Determinanten, siehe Seite 10
$B_n(a)$	Koeffizienten der Potenzreihe $g(T)$, siehe Seite 63
$\mathfrak{C}(A)$	Gruppe der Cartier-Divisoren, siehe Seite 6
$\mathfrak{C}(\phi)$	von ϕ induzierter Homomorphismus der Cartier-Gruppen, siehe Seite 7
$\mathbf{c}$	Isomorphismus von Determinanten, siehe Seite 10
$\mathbb{C}$	komplexe Zahlen
$C^\bullet(G,M)$	stetiger Koketten-Komplex, siehe Seite 75
$C_l^\bullet(G,M)$	Koketten-Komplex der relativen Kohomologie, siehe Seite 95
$char P^\bullet$	charakteristisches Ideal von $P^\bullet$, siehe Seite 17
$Cl_S(K)$	S-Klassengruppe, siehe Seite 88
$\operatorname{codim} \mathfrak{p}$	Kodimension von $\mathfrak{p}$, siehe Seite 9
$\operatorname{Coker} f$	Kokern von f
$Cone^\bullet(f)$	Kegel von f, siehe Seite 13
cor	Korestriktion, siehe Seite 84
G-Cpt	Kategorie der kompakten Räume mit stetiger G-Operation, siehe Seite 73
$Der(\Omega)$	abgeleitete Kategorie der Kategorie $Mod(\Omega)$, siehe Seite 73
$\det_R P$	Determinante, siehe Seite 9
$\dim R$	Krull-Dimension des Rings R
$e(V\|v)$	Verzweigungsindex, siehe Seite 28
e_θ	Idempotente zum Charakter θ, siehe Seite 36

e_+	Idempotente zum (+)-Anteil
e_-	Idempotente zum (-)-Anteil
$\mathcal{F}_l$	geometrischer Frobenius zur Primzahl l, siehe Seite 23
$\mathcal{F}_a$	durch $\mathcal{F}_a(\zeta_N^a) = \zeta_N$ bestimmtes Element der Galoisgruppe, siehe Seite 45
$f(V\|v)$	Restklassenkörpergrad, siehe Seite 90
$\mathcal{F}$	étale Garbe, siehe Seite 101
$\mathcal{F}_{-1}$	komplexe Konjugation, siehe Seite 23
$g(T)$	Potenzreihe zur L-Funktion, siehe Seite 62
$\mathrm{G}_S(K)$	Galois-Gruppe der maximalen außerhalb S unverzweigten Erweiterung von K, siehe Seite 25
$\mathrm{G}(L/K)$	Galoisgruppe der Körpererweiterung L/K
$\mathrm{H}^n\, K^\bullet$	n-te Kohomologiegruppe von $K^\bullet$
h_γ	Nenner des Stickelberger-Elements, siehe Seite 48
$\mathrm{H}^k_{\text{ét}}(X, \mathcal{F})$	étale Garbenkohomologie, siehe Seite 73
$\mathrm{H}^n(G, M)$	stetige Galois-Kohomologie, siehe Seite 75
$\mathrm{H}_l(G, M)$	relative Kohomologie, siehe Seite 95
$\mathrm{Hom}_R(A, B)$	R-Homomorphismen $A \longrightarrow B$
$\mathrm{Hom}_{cts}(A, B)$	stetige Homomorphismen $A \longrightarrow B$
$\mathrm{Hom}(A, B)$	Homomorphismen $A \longrightarrow B$
$\mathrm{Hom}_C(A, B)$	Morphismen $A \longrightarrow B$ der Kategorie C
$\mathfrak{I}$	Ideal
i	die Funktion $\mathrm{i}(a) = \log_p(a)/log_p(1 + dp)$, siehe Seite 61
$\mathrm{Im}\, f$	Bild von f
$\mathrm{Ind}_K(M)$	induzierter Modul, siehe Seite 84
infl	Aufblasung, siehe Seite 95
$K^\bullet[k]$	Translation, siehe Seite 13
$\mathcal{K}$	Garbe der totalen Quotientenringe, siehe Seite 7
K_0	Fixkörper K_∞^Γ, siehe Seite 27

K_∞/K	zyklotomische $\mathbb{Z}_p$ Erweiterung von K, siehe Seite 26
$\operatorname{Ker} f$	Kern von f
$\mathcal{L}_{p,S}(K_\infty, \chi)$	äquivariante L-Funktion, siehe Seite 52
$\mathcal{L}_p(\chi, 1-r)$	p-adische L-Funktion zum Charakter χ, siehe Seite 54
$L(\chi, s)$	komplexe L-Funktion, siehe Seite 53
$\mathfrak{m}$	maximales Ideal
$G\text{-}Mod_{f.g.}(\Omega)$	endlich erzeugte Moduln mit stetiger G-Operation, siehe Seite 74
$Mod_{f.g.}(\Omega)$	Kategorie der endlich erzeugten Ω-Moduln, siehe Seite 73
$Mod(\Omega)$	Kategorie der Ω-Moduln, siehe Seite 73
$\mathbb{N}$	natürliche Zahlen
$N_{G/H}$	Normabbildung, siehe Seite 84
$N_{L/K}$	Normabbildung, siehe Seite 89
$\mathcal{O}_p$	Bewertungsring eines Körpers vom endlichen Grad über $\mathbb{Q}_p$
$\mathcal{O}_{K,S}^\times$	S-Einheiten von K, siehe Seite 88
$\mathcal{O}_S^\times$	S-Einheiten der maximalen außerhalb S unverzweigten Erweiterung von $\mathbb{Q}$, siehe Seite 89
$\mathcal{O}_F$	Ganzheitsring des Körpers F
$\mathfrak{p}, \mathfrak{P}$	Primideale
p	eine ungerade Primzahl
p_Γ	Natürliche Projektion $\mathrm{G}(K_\infty/\mathbb{Q}) \longrightarrow \Gamma$, siehe Seite 35
p_θ	Projektion zum Charakter θ, siehe Seite 36
p_Δ	Natürliche Projektion $\mathrm{G}(K_\infty/\mathbb{Q}) \longrightarrow \Delta$, siehe Seite 35
$Q(R)$	Quotientenring von R
$\mathbb{Q}(\zeta_N)$	N-ter Kreisteilungskörper, siehe Seite 23
$\mathbb{Q}$	rationale Zahlen
$\overline{\mathbb{Q}}$	algebraischer Abschluss von $\mathbb{Q}$
$\mathbb{Q}_p$	Körper der p-adischen Zahlen
$\mathbf{r}$	Isomorphismus von Determinanten, siehe Seite 10
rec	Reziprozitäts-Isomorphismus, siehe Seite 23

$\mathrm{rk}_P(\mathfrak{p})$	Rang eines projektiven Moduls, siehe Seite 5
$\mathbf{s}(f,g)$	Isomorphismus von Determinanten, siehe Seite 10
S_∞	archimedische Stellen in S, siehe Seite 89
S_f	endliche Stellen in S, siehe Seite 89
$\mathrm{Spec}\, R$	Spektrum des Rings R
$\mathrm{Tor}_i^\Omega(M,N)$	Ableitungen des Tensorprodukts, siehe Seite 79
Tw_χ	Verdrehung um χ, siehe Seite 42
val_v	Bewertung zur Stelle v
$\mathbb{Z}$	ganze Zahlen
$Z^n(G,)$	stetige Kozyklen, siehe Seite 77
$\mathbb{Z}_p$	p-adische ganze Zahlen

Erklärung

Ich versichere, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

Diese Arbeit wurde in dieser oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Ort und Datum Unterschrift