Ein Algorithmus zur numerischen Verifikation der äquivarianten Tamagawazahlvermutung für eine Familie von Zahlkörpererweiterungen

Dissertation
zur Erlangung des akademischen Grades eines
Doktors der Naturwissenschaften (Dr. rer. nat.)
am Fachbereich Mathematik
der Universität Kassel

vorgelegt von
Dipl.-Math. Dörthe Janssen
geboren in Jever

Arbeitsgruppe Computational Mathematics
Universität Kassel

Tag der mündlichen Prüfung
21. April 2010

Erstgutachter
Prof. Dr. Werner Bley
Universität Kassel
Zweitgutachter
Prof. Dr. Hans-Georg Rück
Universität Kassel

Dörthe Janssen
Fachbereich Mathematik
Arbeitsgruppe Computational Mathematics
Universität Kassel
Heinrich-Plett-Straße 40
34132 Kassel
djanssen@uni-kassel.de

Danksagung

An erster Stelle möchte ich mich bei meinem Betreuer Prof. Dr. Werner Bley bedanken für die hervorragende Unterstützung während der Entstehung der vorliegenden Arbeit und die vielen konstruktiven Gespräche.
Mein Dank gilt auch meinen Kollegen Thomas Geffers und Oliver Bangert für ihre stetige Diskussionsbereitschaft. Des Weiteren bedanke ich mich bei Anja Panse und Ruben Debeerst für die Korrektur des Manuskripts.
Ein besonderer Dank gilt meinen Eltern, ohne die dies alles nicht möglich gewesen wäre.

Inhaltsverzeichnis

Einleitung

Eines der bemerkenswertesten Resultate der algebraischen Zahlentheorie ist die analytische Klassenzahlformel [Neu92, S. 488]. Sie stellt eine Verbindung her zwischen wichtigen algebraischen und analytischen Invarianten eines Zahlkörpers N, wie zum Beispiel der Klassenzahl und des Regulators, und dem Wert der Dedekindschen Zeta-Funktion an der Stelle 0. Diese Klassenzahlformel führt bis heute zu zahlreichen allgemeineren und feineren Vermutungen. Zu nennen ist die Tamagawazahlvermutung von Bloch und Kato [BK90], die mit den Arbeiten von Fontaine und Perrin-Riou in [FPR94] und [Fon92] eine Neuformulierung und Verallgemeinerung findet. Die äquivariante Tamagawazahlvermutung von Burns und Flach [BF01, Conj. 4], mit der wir uns im Spezialfall des Paares $(h^0(\mathrm{Spec}(N)), \mathbb{Z}[G])$ beschäftigen, ist wiederum eine Verallgemeinerung der Vermutung von Fontaine und Perrin-Riou.

Sei N/K eine galoissche Zahlkörpererweiterung mit Galoisgruppe G und S eine genügend große endliche Menge von Stellen von N. Für einen $\mathbb{C}$-wertigen Charakter χ von G bezeichnen wir die reduzierte Artinsche L-Reihe mit $L_S(N/K, \chi, s)$ und den führenden Koeffizienten in ihrer Taylorreihe bei $s = 0$ mit $L_S^*(N/K, \chi, 0)$. Sei $\mathrm{Irr}(G)$ die Menge der absolut irreduziblen Charaktere von G. Wir setzen

$$\mathcal{L} := (L_S^*(N/K, \overline{\chi}, 0))_{\chi \in \mathrm{Irr}(G)} \in \prod_{\chi \in \mathrm{Irr}(G)} \mathbb{C}^\times \cong \zeta(\mathbb{C}[G])^\times,$$

wobei $\zeta(\mathbb{C}[G])$ das Zentrum von $\mathbb{C}[G]$ bezeichne. Es gilt sogar $\mathcal{L} \in \zeta(\mathbb{R}[G])^\times$. Sei nun $K_0(\mathbb{Z}[G], \mathbb{R})$ die relative K-Gruppe. Diese sitzt in einer exakten Sequenz

$$K_1(\mathbb{Z}[G]) \longrightarrow K_1(\mathbb{R}[G]) \xrightarrow{\partial^1_{\mathbb{Z}[G],\mathbb{R}}} K_0(\mathbb{Z}[G], \mathbb{R}) \xrightarrow{\partial^0_{\mathbb{Z}[G],\mathbb{R}}} K_0(\mathbb{Z}[G]) \longrightarrow K_0(\mathbb{R}[G]).$$

Sei $\hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}}$ der von Burns und Flach in [BF01] definierte kanonische Homomorphismus

$$\hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}} : \zeta(\mathbb{R}[G])^\times \to K_0(\mathbb{Z}[G], \mathbb{R}).$$

Seien nun U_S die S-Einheiten von N, Y_S die freie abelsche Gruppe über S und X_S der Kern der Augmentationsabbildung

$$\begin{cases} Y_S & \to & \mathbb{Z} \\ \sum_{v \in S} \lambda_v v & \mapsto & \sum_{v \in S} \lambda_v \end{cases},$$

dann heißt eine exakte Sequenz

$$0 \to U_S \to A_S \to B_S \to X_S \to 0,$$

Tate-Sequenz, wenn sie eine vorgegebene Klasse in $\mathrm{Ext}^2_G(X_S, U_S)$ repräsentiert. Mit Hilfe dieser Sequenz konstruiert man zur Erweiterung N/K ein Element $R\Omega(N/K)$ in der relativen K-Gruppe. Wir definieren

$$T\Omega := R\Omega(N/K) - \hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}}(\mathcal{L}).$$

Die äquivariante Tamagawazahlvermutung für das Paar $(h^0(\mathrm{Spec}(N)), \mathbb{Z}[G])$ lautet nun $T\Omega = 0$. Burns zeigt in [Bur01], dass dies äquivalent zur gelifteten Wurzelzahlvermutung von Gruenberg, Ritter und Weiss ist ([GRW99, S. 69]) und dass $T\Omega \in K_0(\mathbb{Z}[G], \mathbb{Q})$ äquivalent zur Stark-Vermutung bei $s = 0$ ([Tat84, Ch. I, Conj. 5.1]) ist und $T\Omega$ genau dann in der Torsionsuntergruppe von $K_0(\mathbb{Z}[G], \mathbb{Q})$ liegt, wenn die „Strong-Stark-Conjecture“ ([Chi83, Conj. 2.2]) gilt. Des weiteren impliziert $T\Omega = 0$ Chinburgs Ω_3-Vermutung ([Chi85, Conj. 3.1]).

Gegenstand dieser Arbeit ist ein Algorithmus, der für jedes Fallbeispiel N/Kdie äquivariante Tamagawazahlvermutung für das Paar $(h^0(\mathrm{Spec}(N)), \mathbb{Z}[G])$ numerisch verifiziert, falls es eine Stelle v_0 von N gibt mit $G_{v_0} = G$. Ist zudem $K = \mathbb{Q}$ und gilt für jeden irreduziblen Charakter χ der Gruppe wenigstens eine der beiden Eigenschaften:

(1) Der Charakter χ ist abelsch.

(2) Es gilt $\chi(G) \subseteq \mathbb{Q}$ und χ ist eine Linearkombination von induzierten trivialen Charakteren mit ganzen Koeffizienten.

Dann liefert der Algorithmus einen Beweis.
Da die Berechnung der L-Werte durch die Arbeiten von Dockchitser ([Dok04]) abgedeckt ist und Bley und Wilson in [BW09] Algorithmen entwickelt haben, mit denen man in den relativen K-Gruppe $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ rechnen kann, lag die größte Schwierigkeit in der algorithmischen Berechnung der Tate-Sequenz bzw. eines Repräsentanten in der Gruppe $\mathrm{Ext}^2_G(X_S, U_S)$.
Zunächst haben wir versucht die Ergebnisse von Navilarekallu in [Nav06] algorithmisch umzusetzen. Er beweist in dieser Arbeit die äquivariante Tamagawazahlvermutung für eine einzige A_4-Erweiterungen und benutzt dabei zur Konstruktion der Tate-Sequenz eine Idee von Chinburg. Nach dieser Idee konstruiert man zu jeder Stelle $v \in S$ mit $v \neq v_0$ eine exakte Sequenz

$$0 \to X_v(-2) \to A_v \to B_v \to \mathbb{Z} \to 0,$$

von $\mathbb{Z}[G_v]$-Moduln, in der A_v und B_v frei sind und einen G_v-Homomorphismus $f : X_v(-2) \to U_S$, der gewissen lokalen Bedingungen genügt. Sei $(\alpha_1, \ldots, \alpha_r)$ ein Erzeugendensystem von $X_v(-2)$, dann sind S-Einheiten $u_1, \ldots, u_r$ zu finden, so dass f durch die Zuordnung $\alpha_i \mapsto u_i, i = 1, \ldots, r$ gegeben ist. Leider stellte sich heraus, dass die Bedingungen an die S-Einheiten, die Navilarekallu in seiner Arbeit angibt, nicht ausreichend sind, um die lokalen Vorgaben an die Abbildung f zu erfüllen. Die lokalen Vorgaben bestehen darin, dass für eine weitere Stelle $w \in S$ die Abbildung

$$X_v(-2) \to U_S \to N_w^\times$$

die lokale Fundamentalklasse bzw. die triviale Klasse in $\mathrm{Ext}^2_{G_v \cap G_w}(\mathbb{Z}, N_w^\times)$ repräsentieren soll. Folgende Probleme mussten gelöst werden

(1) Wie berechnet man lokale Fundamentalklassen?

(2) Wie kodiert man die lokalen Bedingungen in ein Gleichungssystem für die S-Einheiten?

(3) Wie gewährleistet man, dass die Abbildung f ein G_v-Homomorphismus ist?

Zur Berechnung der lokalen Fundamentalklasse haben wir für höchstens zahm verzweigte, d.h. unverzweigte oder zahm verzweigte, Erweiterungen wieder eine Idee von Chinburg ([Chi85]) aufgegriffen, die auf den Arbeiten von Serre ([Ser]) beruht. Für

beliebige lokale Erweiterungen wurde von Debeerst ([Deb11]) ein Algorithmus zur Berechnung der lokalen Fundamentalklasse entwickelt. Dieser basiert ebenfalls auf der Arbeit von Serre. Im Fall einer höchstens zahm verzweigten Erweiterung ist dieser allerdings langsamer, als der von uns implementiere Algorithmus. Zur Lösung der Fragestellung (2) verweisen wir auf den Abschnitt 3.2.2. Die Fragestellung (3) konnten wir durch die Entwicklung eines Algorithmus lösen der ein $\mathbb{Z}$-Erzeugendensystem von $\mathrm{Hom}_{\mathbb{Z}[G_v]}(A, B)$ berechnet, wenn A und B endlich erzeugte $\mathbb{Z}[G_v]$-Moduln sind und A zudem $\mathbb{Z}$-frei ist. Als unbeabsichtigten Zusatz konnten wir mit diesem Algorithmus den bestehenden Algorithmus zur Berechnung von $\mathbb{Q}[G]$-linearen Schnitten verallgemeinern und zwar durch einen Algorithmus der nicht nur $\mathbb{Q}[G]$-lineare Schnitte berechnet, sondern auch $\mathbb{Z}[G]$-lineare Schnitte, sofern sie existieren.
Implementiert haben wir bislang einen Algorithmus in das Computeralgebrasystem MAGMA, der die Vermutung für A_4-Erweiterungen numerisch verifiziert. Eine Implementierung für beliebige Gruppen ist noch mit erheblichem Zeitaufwand verbunden.

Diese Arbeit ist wie folgt aufgebaut.
Im ersten Kapitel stellen wir einige Grundlagen aus der analytischen Zahlentheorie, der algebraischen K-Theorie und der homologischen Algebra zusammen. Des Weiteren definieren wir Tates kanonische Klasse. Im zweiten Kapitel gehen wir noch mal auf die Problemstellung dieser Arbeit ein, formulieren die Vermutung und sagen etwas zum aktuellen Forschungsstand. Im dritten Kapitel kommen wir zur algorithmischen Umsetzung. Dabei beschäftigen wir uns erst mit der lokalen Fundamentalklasse und anschließend mit der Konstruktion von Tates kanonischer Klasse. Die Theorie, die wir dabei benutzt haben, stellen wir jeweils voran. Im dritten Abschnitt von Kapitel 3 gehen wir darauf ein, wie wir die Algorithmen von Bley und Wilson aus [BW09] benutzt haben, um die Vermutung numerisch zu verifizieren, und zeigen, dass unser Algorithmus unter gewissen Voraussetzungen die Vermutung beweist. Im vierten Abschnitt stellen wir ausführlich ausgewählte Algorithmen vor, die wir implementiert haben. Unter anderem den Algorithmus zur Berechnung eines $\mathbb{Z}$-Erzeugendensystems der G_v-Homomorphismen, den Algorithmus zur Berechnung von $\mathbb{Z}[G]$-linearen Schnitten sowie einen Algorithmus der zu einem Kozykel den Repräsentanten in der Ext-Gruppe berechnet. Im letzten Kapitel stellen wir die Beispiele zusammen, für die wir die Vermutung numerisch verifiziert haben.

Kapitel 1

Grundlagen

Wir setzen in dieser Arbeit Kenntnisse über Darstellungstheorie voraus, wie sie etwa in [CR81, §9] zu finden sind.

1.1 Artinsche L-Reihen

Wir definieren in diesem Abschnitt die Artinschen L-Reihen und fassen ihre wichtigsten Eigenschaften zusammen. Mehr Details und Beweise der einzelnen Aussagen können im Buch [Neu92, Kap. VII, §10] von Neukirch nachgelesen werden, sofern wir nichts anderes schreiben.
Sei N/K eine galoissche Zahlkörpererweiterung mit Galoisgruppe G und χ ein Charakter von G. Sei V ein endlich-dimensionaler $\mathbb{C}$-Vektorraum und $T_\chi : G \to \mathrm{Aut}_{\mathbb{C}}(V)$ eine Darstellung von G zum Charakter χ. Sei nun $\mathfrak{p}$ ein Primideal von K und $\mathfrak{P}$ ein über $\mathfrak{p}$ liegendes Primideal von N. Mit $G_{\mathfrak{P}}$ bezeichnen wir die Zerlegungsgruppe von $\mathfrak{P}$ und mit $I_{\mathfrak{P}}$ die Trägheitsgruppe von $\mathfrak{P}$. Sei $\sigma_{\mathfrak{P}} \in G$ ein Lift des Frobeniusautomorphismus. Dann ist $\sigma_{\mathfrak{P}}$ ein Endomorphismus auf $V^{I_{\mathfrak{P}}}$ via

$$\sigma_{\mathfrak{P}}(v) := \left(T_\chi(\sigma_{\mathfrak{P}})\right)(v).$$

Das charakteristische Polynom

$$\det(1 - \sigma_{\mathfrak{P}} X \mid V^{I_{\mathfrak{P}}}) \in \mathbb{C}[X]$$

ist unabhängig von der gewählten Stelle $\mathfrak{P}$ über $\mathfrak{p}$. Wir bezeichnen die Normabbildung von N/K mit $\mathrm{N}_{N/K}$.

Definition 1.1.1. *Die Bezeichnungen seien wie oben und zusätzlich sei $\mathcal{O}_K$ der Ganzheitsring von K. Für $s \in \mathbb{C}$ mit $Re(s) > 1$ heißt die Reihe*

$$L(N/K, \chi, s) := \prod_{\mathfrak{p} \leq \mathcal{O}_K} \det\left(1 - \sigma_{\mathfrak{P}} \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-s} \mid V^{I_{\mathfrak{P}}}\right)^{-1}$$

Artinsche L-Reihe zum Charakter χ.

Die Schreibweise der Artinschen L-Reihe lässt vermuten, dass sie nicht von der Darstellung sondern vom Charakter abhängt und dies ist in der Tat so (siehe [Neu92]).

Eigenschaften

(1) Die Artinsche L-Reihe konvergiert absolut und gleichmäßig in der Halbebene $\mathrm{Re}(s) > 1$.

(2) Ist χ der Einscharakter, dann gilt

$$L(N/K, \chi, s) = \zeta_K(s),$$

wobei ζ_K die Zetafunktion zum Zahlkörper K bezeichnet.

(3) Sind χ_1 und χ_2 zwei Charaktere von G, so ist

$$L(N/K, \chi_1 + \chi_2, s) = L(N/K, \chi_1, s) \cdot L(N/K, \chi_2, s).$$

(4) Die Artinsche L-Reihe besitzt eine meromorphe Fortsetzung auf $\mathbb{C}$ und genügt einer Funktionalgleichung ([Neu92, Kap.VII, §12, Th. (12.6)]).

Definition 1.1.2. *Sei S eine endliche Menge von Primidealen von K. Die reduzierte Artinsche L-Reihe zu χ ist definiert durch*

$$L_S(N/K, \chi, s) := \prod_{\mathfrak{p} \notin S} \det\left(1 - \sigma_{\mathfrak{P}} \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-s} \mid V^{I_{\mathfrak{P}}}\right)^{-1}.$$

Den führenden Koeffizienten in der Taylorreihenentwicklung bei $s = 0$ bezeichnen wir mit $L_S^*(N/K, \chi, 0)$.

1.2 Algebraische K-Theorie

In diesem Abschnitt wiederholen wir die hier relevanten Definitionen und Eigenschaften der algebraischen K-Theorie wie sie zum Beispiel in [Swa68] und [CR81] zu finden sind. Sei im Folgenden A ein Ring mit 1. Sofern nichts anderes gesagt wird, verstehen wir unter einem A-Modul einen Links-A-Modul. Mit $\mathcal{P}(A)$ bezeichnen wir die Kategorie der endlich erzeugten projektiven A-Moduln.

1.2.1 Die Grothendieckgruppe $K_0(A)$

Für $P \in \mathcal{P}(A)$ bezeichnen wir mit (P) die Isomorphieklasse von P. Sei $\mathcal{F}$ die freie abelsche Gruppe, die von diesen Isomorphieklassen erzeugt wird. In $\mathcal{F}$ betrachten wir die Untergruppe $\mathcal{R}$, die erzeugt wird von der Menge

$$\{(P) - (P') - (P'') \mid \text{es gibt eine exakte Sequenz } 0 \to P' \to P \to P'' \to 0 \text{ von } A\text{-Moduln}\}$$

und definieren die sogenannte GROTHENDIECKgruppe durch

$$K_0(A) := \mathcal{F}/\mathcal{R}.$$

Die Klasse von (P) in $K_0(A)$ bezeichnen wir mit $[P]$.

1.2.2 Die Whiteheadgruppe $K_1(A)$

Hier betrachten wir Tupel (P, ϕ), wobei $P \in \mathcal{P}(A)$ und ϕ ein Automorphismus von P ist. Unter einem Morphismus $f : (P, \phi) \to (Q, \psi)$ verstehen wir einen A-Modulhomomorphismus $f : P \to Q$ der mit ϕ und ψ verträglich ist, d.h. es gilt $f \circ \phi = \psi \circ f$. Sei $((P, \phi))$ die Isomorphieklasse von (P, ϕ). Wir nennen $0 \to (P', \phi') \to (P, \phi) \to (P'', \phi'') \to 0$ eine kurze exakte Sequenz, wenn $0 \to P' \to P \to P'' \to 0$ eine kurze exakte Sequenz ist. Sei $\mathcal{F}$ die freie abelsche Gruppe, die von den Isomorphieklassen erzeugt wird. Mit $\mathcal{R}$ bezeichnen wir die Untergruppe, die erzeugt wird von den Elementen $((P, \phi)) - ((P', \phi')) - ((P'', \phi''))$, für die es eine kurze exakte Sequenz $0 \to (P', \phi') \to (P, \phi) \to (P'', \phi'') \to 0$ gibt, und den Elementen $((P, \phi \circ \psi)) - ((P, \phi)) - ((P, \psi))$ für alle $P \in \mathcal{P}(A)$ und $\phi, \psi \in \mathrm{Aut}_A(P)$. Wir definieren

$$K_1(A) := \mathcal{F}/\mathcal{R}.$$

Die Klasse von $((P,\phi))$ in $K_1(A)$ bezeichnen wir mit $[P,\phi]$. Die Gruppe $K_1(A)$ heißt WHITEHEADgruppe. Eine vielleicht bekanntere Definition dieser Gruppe ist die folgende: Sei $\mathrm{Gl}_n(A)$ die Gruppe der invertierbaren $n \times n$-Matrizen mit Einträgen in A. Die Einbettung

$$\begin{cases} \mathrm{Gl}_n(A) & \to & \mathrm{Gl}_{n+1}(A) \\ M & \mapsto & \begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix} \end{cases}$$

induziert Einbettungen $\mathrm{Gl}_n(A) \to \mathrm{Gl}_m(A)$ für alle $n, m \in \mathbb{N}$ mit $n < m$. Wir definieren

$$\mathrm{Gl}(A) := \varinjlim_n \mathrm{Gl}_n(A).$$

Nach [CR87, (40.6)] gilt

$$K_1(A) \;\cong\; \mathrm{Gl}(A)/[\mathrm{Gl}(A), \mathrm{Gl}(A)],$$

wobei $[\mathrm{Gl}(A), \mathrm{Gl}(A)]$ die Kommutatoruntergruppe bezeichnet.

1.2.3 Die relative K-Gruppe $K_0(A, f)$

Sei B ein Ring mit 1 und $f : A \to B$ ein Ringhomomorphismus. Vermöge f betrachten wir B als Rechts-A-Modul. Hier betrachten wir Tripel (P, ϕ, Q) mit $P, Q \in \mathcal{P}(A)$ und einem Isomorphismus $\phi : B \otimes_A P \to B \otimes_A Q$ von B-Moduln. Sind $\alpha : P \to P'$ und $\beta : Q \to Q'$ Homomorphismen, dann nennen wir $(\alpha, \beta) : (P, \phi, Q) \to (P', \psi, Q')$ einen Morphismus, wenn das Diagramm

$$\begin{array}{ccc} B \otimes_A P & \xrightarrow{\mathrm{id}\otimes\alpha} & B \otimes_A P' \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \psi} \\ B \otimes_A Q & \xrightarrow{\mathrm{id}\otimes\beta} & B \otimes_A Q' \end{array}$$

kommutiert. Die Isomorphieklasse von (P, ϕ, Q) bezeichnen wir mit $((P, \phi, Q))$. Eine Sequenz $0 \to (P', \phi', Q') \to (P, \phi, Q) \to (P'', \phi'', Q'') \to 0$ heißt exakt, wenn $0 \to P' \to P \to P'' \to 0$ und $0 \to Q' \to Q \to Q'' \to 0$ exakt sind. Die Definition von $K_0(A, f)$ ist analog zu der von $K_1(A)$, d.h. in der freien abelschen Gruppe $\mathcal{F}$, die von den Isomorphieklassen erzeugt wird, betrachten wir die Untergruppe $\mathcal{R}$, die erzeugt wird von den Elementen $((P, \phi, Q)) - ((P', \phi', Q')) - ((P'', \phi'', Q''))$, für die es eine kurze exakte Sequenz $0 \to (P', \phi', Q') \to (P, \phi, Q) \to (P'', \phi'', Q'') \to 0$ gibt, und den

Elementen $((P, \psi \circ \phi, P')) - ((P, \phi, P'')) - ((P'', \psi, P'))$ für alle $P, P', P'' \in \mathcal{P}(A)$, sowie Isomorphismen $\phi : B \otimes_A P \to B \otimes_A P''$ und $\psi : B \otimes_A P'' \to B \otimes_A P'$. Wir definieren

$$K_0(A, f) := \mathcal{F}/\mathcal{R}.$$

Die Gruppe $K_0(A, f)$ heißt relative K-Gruppe. Wie zuvor bezeichnen wir die Klasse von $((P, \phi, Q))$ in $K_0(A, f)$ mit $[P, \phi, Q]$.
Sind R und S Ringe und A bzw. B der Gruppenring $R[G]$ bzw. $S[G]$ für eine endliche Gruppe G und ist $f : R[G] \to S[G]$ induziert von einer natürlichen Inklusion $\iota : R \to S$, dann ist $S[G] \otimes_{R[G]} P \cong S \otimes_R P$ für alle $P \in \mathcal{P}(A)$ und wir schreiben statt $K_0(A, f)$ einfach $K_0(R[G], S)$ und sehen in $[P, \phi, Q]$ den Isomorphismus ϕ als Isomorphismus zwischen $S \otimes_R P$ und $S \otimes_R Q$.

1.2.4 Die exakte Sequenz

Sei wie zuvor $f : A \to B$ ein Ringhomomorphismus. Die folgende Sequenz ist exakt.

$$K_1(A) \xrightarrow{f^*} K_1(B) \xrightarrow{\partial^1_{A,f}} K_0(A, f) \xrightarrow{\partial^0_{A,f}} K_0(A) \xrightarrow{f_*} K_0(B),$$

wobei die Abbildungen auf den Erzeugern wie folgt definiert sind:

$$\begin{aligned} f^*([P, \phi]) &= [B \otimes_A P, \mathrm{id}_B \otimes \phi], \\ \partial^0_{A,f}([P, \phi, Q]) &= [P] - [Q], \\ \partial^1_{A,f}([B^n, \phi]) &= [A^n, \psi, A^n] \text{ mit } \psi : B \otimes_A A^n \xrightarrow{\sim} B^n \xrightarrow{\phi} B^n \xrightarrow{\sim} B \otimes_A A^n, \\ f_*([P]) &= [B \otimes_A P]. \end{aligned}$$

Dabei ist zu beachten, dass nach [CR87, §38B] jedes Element in $K_1(B)$ repräsentiert wird von $[B^n, \phi]$, mit einem geeignetem $n \in \mathbb{N}$. Für einen Beweis der Exaktheit der Sequenz siehe etwa [Swa68, Th. 15.5].

Bemerkung 1. *Ist G eine endliche Gruppe und $A = \mathbb{Z}[G]$ sowie $B = \mathbb{R}[G]$, dann bezeichnen wir für $i = 0, 1$ die Abbildungen $\partial^i_{A,f}$ mit $\partial^i_{\mathbb{Z}[G],\mathbb{R}}$ und für $A = \mathbb{Z}_p[G]$ und $B = \mathbb{Q}_p[G]$ bzw. $B = \mathbb{C}_p[G]$ mit $\partial^i_{\mathbb{Z}_p[G],\mathbb{Q}_p}$ bzw. $\partial^i_{\mathbb{Z}_p[G],\mathbb{C}_p}$. Dabei bezeichnet $\mathbb{C}_p$ die Komplettierung eines algebraischen Abschlusses von $\mathbb{Q}_p$.*

1.2.5 Die reduzierte Norm

Sei A eine zentral einfache K-Algebra. Dann gibt es einen Schiefkörper D über K mit $A \cong \mathrm{M}_n(D)$, wobei $\mathrm{M}_n(D)$ den Ring der $n \times n$-Matrizen mit Einträgen aus D bezeichne. Wir identifizieren im Folgenden A mit $\mathrm{M}_n(D)$. Sei weiterhin E ein Zerfällungskörper zu D, d.h. es gibt ein $m \in \mathbb{N}$ und einen Isomorphismus $h : E \otimes_K D \to \mathrm{M}_m(E)$. Wir definieren die Einbettungen

$$\mu : \left\{ \begin{array}{ccccc} D & \to & E \otimes_K D & \to & \mathrm{M}_m(E) \\ a & \mapsto & 1 \otimes a & \mapsto & h(1 \otimes a) \end{array} \right.$$

und

$$\lambda : \left\{ \begin{array}{ccc} \mathrm{M}_n(D) & \to & \mathrm{M}_{nm}(E) \\ (\alpha_{ij}) & \mapsto & (\mu(\alpha_{ij})) \end{array} \right. .$$

Definition 1.2.1. *Der Homomorphismus*

$$\mathrm{nr}_{A/K}(a) : \left\{ \begin{array}{ccc} A & \to & K \\ a & \mapsto & \det(\lambda(a)) \end{array} \right.$$

heißt reduzierte Normabbildung.

Diese lässt sich wegen $\mathrm{Gl}_r(A) \cong \mathrm{Gl}_{rn}(D)$ für alle $r \in \mathbb{N}$ vermöge λ auf $K_1(A)$ fortsetzen ([CR81, Ex. 7.3], [CR87, (45.3)]). Die Fortsetzung bezeichnen wir ebenfalls mit $\mathrm{nr}_{A/K}$ und nennen sie reduzierte Normabbildung.
Ist A eine halbeinfache K-Algebra, dann induziert die reduzierte Normabbildung über die Wedderburnzerlegung von A eine reduzierte Normabbildung auf $K_1(A)$. Sei dazu $A = \bigoplus_{i=1}^r A_i$ die Wedderburnzerlegung von A. Jedes A_i ist eine zentral einfache Algebra über ihrem Zentrum K_i und für das Zentrum $\zeta(A)$ von A gilt $\zeta(A) \cong \bigoplus_{i=1}^r K_i$. Nach [CR87, (38.29)] ist

$$K_1(A) \cong \bigoplus_{i=1}^{r} K_1(A_i).$$

Für $M \in \mathrm{Gl}(A)$ sei $M_1 \oplus \ldots \oplus M_r$ die von der Wedderburnzerlegung induzierte Zerlegung.

Definition 1.2.2. *Der Homomorphismus*

$$\mathrm{nr}_A : \left\{ \begin{array}{ccc} K_1(A) & \to & \zeta(A)^\times \cong \bigoplus_{i=1}^{r} K_i^\times \\ M & \mapsto & (\mathrm{nr}_{A_i/K_i}(M_i))_{i=1,\ldots,r} \end{array} \right.$$

heißt reduzierte Normabbildung von $K_1(A)$.

Im Spezialfall lässt sich die reduzierte Norm nr_A über Determinantenfunktionen beschreiben, die zu Charakteren assoziiert werden. Sei dazu G eine endliche Gruppe, e der Exponent von G und K eine endliche Erweiterung von $\mathbb{Q}$, die eine primitive e-te Einheitswurzel enthält. Wir betrachten den Fall $A = K[G]$. Sei $\mathrm{Irr}(G)$ die Menge der absolut irreduziblen Charaktere von G.

Satz 1.2.3. *Mit den obigen Voraussetzungen und Bezeichnungen gilt*

1) $\zeta(K[G]) \cong \bigoplus_{\chi \in \mathrm{Irr}(G)} K.$

2) $K[G] \cong \bigoplus_{\chi \in \mathrm{Irr}(G)} \mathrm{M}_{\chi(1)}(K).$

Beweis. Die Aussage *1)* folgt aus [Lor97, §33, Satz 15] in Verbindung mit [Lor97, §33, Satz 2]. Die Aussage *2)* folgt aus [Lor97, §33, Satz 15] mit [Lor97, §33, F12]. □

Für einen Charakter $\chi \in \mathrm{Irr}(G)$ sei $T_\chi : G \to \mathrm{Gl}_{\chi(1)}(K)$ eine zugehörige Darstellung. Die lineare Fortsetzung von T_χ auf $K[G]$ bezeichnen wir ebenfalls mit T_χ.

Lemma 1.2.4. *Der von den Darstellungen T_χ induzierte K-Algebrenhomomorphismus*

$$T : \begin{cases} K[G] & \to & \bigoplus_{\chi \in \mathrm{Irr}(G)} \mathrm{M}_{\chi(1)}(K) \\ \lambda & \mapsto & \left(T_\chi(\lambda)\right)_{\chi \in \mathrm{Irr}(G)} \end{cases}$$

ist ein Isomorphismus.

Beweis. Für jedes $\chi \in \mathrm{Irr}(G)$ ist die Abbildung $T_\chi : K[G] \to \mathrm{M}_{\chi(1)}(K)$ surjektiv. Dies folgt aus [Lor97, §33, F12 u. F5]. Die Bijektivität von T folgt nun aus

$$\dim_K K[G] = |G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = \dim_K \left(\bigoplus_{\chi \in \mathrm{Irr}(G)} \mathrm{M}_{\chi(1)}(K) \right),$$

wobei das zweite Gleichheitszeichen nach [Lor97, §33, F12] gilt. □

Zu jedem $\chi \in \mathrm{Irr}(G)$ definieren wir nun den Homomorphismus

$$\mathrm{Det}_\chi : \begin{cases} K[G] & \to & K^\times \\ \lambda & \mapsto & \det\left(T_\chi(\lambda)\right). \end{cases}$$

Abkürzend setzen wir $A_\chi := \mathrm{M}_{\chi(1)}(K)$. Für alle $\lambda = (\lambda_\chi)_{\chi\in\mathrm{Irr}(G)} \in \bigoplus_{\chi\in\mathrm{Irr}(G)} A_\chi$ gilt somit

$$\mathrm{nr}_{A_\chi/K}(\lambda_\chi) = \mathrm{Det}_\chi(\lambda).$$

Sei nun $S = (s_{ij}) \in \mathrm{Gl}_n(K[G])$ ein Repräsentant von $\theta \in K_1(K[G])$ und $T_\chi(S) := (T_\chi(s_{ij}))_{i,j} \in \mathrm{Gl}_{n\chi(1)}(K)$. Mit $\mathrm{Det}_\chi(\theta) := \det(T_\chi(S))$ gilt

$$\mathrm{nr}_{K[G]}(\theta) = (\mathrm{Det}_\chi(\theta))_{\chi\in\mathrm{Irr}(G)} \in \bigoplus_{\chi\in\mathrm{Irr}(G)} K$$

1.2.6 Der Homomorphismus $\hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}}$

Sei G eine endliche Gruppe.
Wir definieren hier den von Burns und Flach in [BF01, 4.2] eingeführten kanonischen Homomorphismus $\hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}} : \zeta(\mathbb{R}[G])^\times \to K_0(\mathbb{Z}[G],\mathbb{R})$. Er ist eine Fortsetzung des Homomorphismus $\delta^1_{\mathbb{Z}[G],\mathbb{R}} \circ \mathrm{nr}^{-1}_{\mathbb{R}[G]} : \mathrm{im}(\mathrm{nr}_{\mathbb{R}[G]}) \to K_0(\mathbb{Z}[G],\mathbb{R})$ und für die Formulierung der Vermutung von zentraler Bedeutung. Die Idee der Fortsetzung ist grob gesprochen, die folgende.
Elemente $x \in \zeta(\mathbb{R}[G])^\times$ die nicht im Bild der reduzierten Norm liegen, werden mittels einem (nicht eindeutigem) $\lambda \in \zeta(\mathbb{Q}[G])^\times$ in das Bild „geschiftet“ und diese Nichteindeutigkeit durch eine „lokale Differenz“ relativiert.
Sei $\zeta(\mathbb{R}[G])^{\times+}$ das Bild der reduzierten Normabbildung $\mathrm{nr}_{\mathbb{R}[G]} : K_1(\mathbb{R}[G]) \to \zeta(\mathbb{R}[G])^\times$. Nach ([Bre04, Prop. 2.2]) ist $\mathrm{nr}_{\mathbb{R}[G]}$ injektiv. Der kanonische Homomorphismus

$$\delta^1_{\mathbb{Z}[G],\mathbb{R}} : \left\{ \begin{array}{ccc} \zeta(\mathbb{R}[G])^{\times+} & \to & K_0(\mathbb{Z}[G],\mathbb{R})^\times \\ \lambda & \mapsto & \partial^1_{\mathbb{Z}[G],\mathbb{R}} \circ \mathrm{nr}^{-1}_{\mathbb{R}[G]}(\lambda) \end{array} \right. .$$

ist also wohldefiniert. Nach [Bre04, Lemma 2.3] kann man das Bild der Abbildung $\mathrm{nr}_{\mathbb{R}[G]} : K_1(\mathbb{R}[G]) \to \zeta(\mathbb{R}[G])^\times \subset \zeta(\mathbb{C}[G])^\times \cong \prod_{\chi\in\mathrm{Irr}_{\mathbb{C}}(G)} \mathbb{C}^\times$ wie folgt beschreiben

$$\left\{ (\alpha_\chi) \in \prod_{\chi\in\mathrm{Irr}_{\mathbb{C}}(G)} \mathbb{C}^\times \;\middle|\; \begin{array}{l} \alpha_{\bar{\chi}} = \bar{\alpha_\chi} \text{ für alle } \chi \in \mathrm{Irr}_{\mathbb{C}}(G) \text{ und } \alpha_\chi > 0 \text{ für alle} \\ \text{symplektischen } \chi \in \mathrm{Irr}_{\mathbb{C}}(G) \end{array} \right\}.$$

Nach dem schwachen Approximationssatz gibt es also zu jedem $x \in \zeta(\mathbb{R}[G])^\times$, welches nicht im Bild der reduzierten Normabbildung liegt ein $\lambda \in \zeta(\mathbb{Q}[G])^\times$, so dass $\lambda x \in \zeta(\mathbb{R}[G])^{\times+}$ gilt.

Um die „lokale Differenz“ zu beschreiben müssen wir etwas ausholen. Nach [CR87, (40.19),(49.12)] haben wir für $K_0(\mathbb{Z}[G],\mathbb{Q})$ die folgende kanonische Zerlegung

$$\mathrm{K}_0(\mathbb{Z}[G],\mathbb{Q}) \cong \bigoplus_{p \text{ prim}} \mathrm{K}_0(\mathbb{Z}_p[G],\mathbb{Q}_p)$$

via

$$[P,\phi,Q] \mapsto \left([P\otimes_{\mathbb{Z}}\mathbb{Z}_p, \phi\otimes_{\mathbb{Q}}\mathbb{Q}_p, Q\otimes_{\mathbb{Z}}\mathbb{Z}_p]\right)_p .$$

Vermöge dieser Zerlegung sehen wir $K_0(\mathbb{Z}_p[G],\mathbb{Q}_p)$ in $K_0(\mathbb{Z}[G],\mathbb{Q})$ eingebettet.
Für eine Primzahl p ist die reduzierte Normabbildung

$$\mathrm{nr}_{\mathbb{Q}_p[G]} : K_1(\mathbb{Q}_p[G]) \to \zeta(\mathbb{Q}_p[G])^\times$$

ein Isomorphismus ([Bre04, Prop. 2.2]). Wir definieren

$$\delta_p : \begin{cases} \zeta(\mathbb{Q}_p[G])^\times & \to & K_0(\mathbb{Z}_p[G],\mathbb{Q}_p) \\ \lambda & \mapsto & \partial^1_{\mathbb{Z}_p[G],\mathbb{Q}_p}\circ \mathrm{nr}^{-1}_{\mathbb{Q}_p[G]}(\lambda) \end{cases} .$$

Ist nun λx wie oben, dann setzen wir

$$\hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}}(x) := \delta^1_{\mathbb{Z}[G],\mathbb{R}}(\lambda x) - \sum_{p \text{ prim}} \hat{\delta}_p(\lambda).$$

Dabei ist $\hat{\delta}_p$ als das Kompositum

$$\zeta(\mathbb{Q}[G])^\times \xrightarrow{\subseteq} \zeta(\mathbb{Q}_p[G])^\times \xrightarrow{\delta_p} K_1(\mathbb{Z}_p[G],\mathbb{Q}_p) \xrightarrow{\subseteq} K_1(\mathbb{Z}[G],\mathbb{Q})$$

zu verstehen.

1.3 Homologische Algebra

1.3.1 Ext und Yext

In diesem Abschnitt wiederholen wir die Definitionen und einige Eigenschaften der Gruppen Ext^n und Yext^n, in dem Umfang, wie sie in dieser Arbeit benötigt werden und zeigen, dass sie isomorph sind. Im Folgenden sei R ein Ring und A, B seien R-Moduln. Sei

$$\ldots \xrightarrow{\delta_3} P_2 \xrightarrow{\delta_2} P_1 \xrightarrow{\delta_1} P_0 \xrightarrow{\delta_0} A \to 0 \tag{1.1}$$

eine projektive Auflösung von A. Setzen wir $Q_{n-1} := \ker(\delta_{n-1})$ so ist die Sequenz

$$0 \to Q_{n-1} \stackrel{\iota}{\to} P_{n-1} \stackrel{\delta_{n-1}}{\to} \ldots \to P_0 \stackrel{\delta_0}{\to} A \to 0 \tag{1.2}$$

exakt, wenn ι die Einbettung bezeichnet. Die Abbildung ι induziert einen Gruppenhomomorphismus

$$\iota_* : \begin{cases} \mathrm{Hom}_R(P_{n-1}, B) & \to & \mathrm{Hom}_R(Q_{n-1}, B) \\ \\ g & \mapsto & g \circ \iota \end{cases}$$

und wir definieren $\mathrm{Ext}^n_R(A, B)$ als den Quotienten

$$\mathrm{Ext}^n_R(A, B) := \frac{\mathrm{Hom}_R(Q_{n-1}, B)}{\iota_* \left(\mathrm{Hom}_R(P_{n-1}, B)\right)}.$$

Die Darstellung der Elemente in $\mathrm{Ext}^n_R(A, B)$ ist natürlich abhängig von der gewählten projektiven Auflösung (1.1), aber die Gruppe ist bis auf eindeutige Isomorphie eindeutig. Haben wir einmal eine projektive Auflösung des Moduls A gewählt, dann denken wir uns $\mathrm{Ext}^n_R(A, B)$ immer über diese Auflösung gegeben. Mit $[\phi]$ sei die Klasse von ϕ in $\mathrm{Ext}^n_R(A, B)$ bezeichnet. Einen anderen und üblicheren Zugang zu den Gruppen Ext^n, nämlich als rechte Ableitung des Funktors Hom, und mehr Details finden sich in [HS71].

Um $\mathrm{Yext}^n_R(A, B)$ zu definieren, müssen wir etwas weiter ausholen. Eine exakte Sequenz

$$(E): \qquad 0 \to B \to E_n \to \ldots \to E_1 \to A \to 0$$

von R-Moduln heißt *n-Erweiterung* von A mit B. Auf der Menge dieser n-Erweiterungen definieren wir nun eine Äquivalenzrelation. Zwei n-Erweiterungen (E) und (F) heißen in Relation stehend (in Zeichen $(E) \rightsquigarrow (F)$), wenn es ein kommutatives Diagramm

$$\begin{array}{lccccccccc} (E): & 0 & \longrightarrow & B & \longrightarrow & E_n & \longrightarrow \cdots \longrightarrow & E_1 & \longrightarrow & A & \longrightarrow & 0 \\ & & & \| & & \downarrow & & \downarrow & & \| & & \\ (F): & 0 & \longrightarrow & B & \longrightarrow & F_n & \longrightarrow \cdots \longrightarrow & F_1 & \longrightarrow & A & \longrightarrow & 0 \end{array}$$

gibt. Die n-Erweiterungen (E) und (F) heißen äquivalent, wenn es eine Kette von n-Erweiterungen $(E) = (E_0), (E_1), \ldots, (E_r) = (F)$ gibt, die in Relation stehen (etwa $(E_0) \rightsquigarrow (E_1) \leftsquigarrow (E_2) \leftsquigarrow \ldots \rightsquigarrow (E_r)$). Mit $[(E)]$ bezeichnen wir die Äquivalenzklasse von (E). Wir definieren $\mathrm{Yext}^n_R(A, B)$ als die Menge

$$\mathrm{Yext}^n_R(A, B) := \{\ [(E)] \mid (E) \text{ ist eine } n\text{-Erweiterung von } A \text{ mit } B\}.$$

Die Gruppenstruktur auf $\mathrm{Yext}^n_R(A,B)$ wird durch eine bijektive Abbildung von Ext^n nach Yext^n induziert. Wir geben diese Abbildung nur auf den Repräsentanten an. Einen Beweis der Wohldefiniertheit und Bijektivität findet sich etwa in [HS71, IV.9].
Sei $[\varphi] \in \mathrm{Ext}^n_R(A,B)$. Wir betrachten dazu das kommutative Diagramm

$$
\begin{array}{rccccccccccc}
 & 0 & \longrightarrow & Q_{n-1} & \xrightarrow{\iota} & P_{n-1} & \longrightarrow & P_n & \longrightarrow \cdots \longrightarrow & P_0 & \longrightarrow & A & \longrightarrow 0 \\
 & & & \downarrow{\scriptstyle \varphi} & & \downarrow & & \| & & \| & & \| & \\
(E): & 0 & \longrightarrow & B & \longrightarrow & P & \longrightarrow & P_n & \longrightarrow \cdots \longrightarrow & P_0 & \longrightarrow & A & \longrightarrow 0,
\end{array}
$$

wobei die obere Zeile die Zeile (1.2) aus der projektiven Auflösung von A ist und P der Pushout von ι mit φ, d.h. $P = (P_{n-1} \oplus B)\,/\{(\iota(a), -\varphi(a)) \mid a \in Q_{n-1}\}$. Wir definieren das Bild von $[\varphi]$ in $\mathrm{Yext}^n_R(A,B)$ als die Klasse $[(E)]$. Für die andere Richtung sei $[(E) : 0 \to B \to E_n \to \ldots \to E_1 \to A \to 0] \in \mathrm{Yext}^n_R(A,B)$ vorgegeben. Da die Moduln P_i in (1.1) projektiv sind, können wir R-Modulhomomorphismen $\varphi_0, \ldots, \varphi_n$ finden, so dass

$$
\begin{array}{ccccccccccc}
P_{n+1} & \longrightarrow & P_n & \xrightarrow{\delta_n} & P_{n-1} & \xrightarrow{\delta_{n-1}} & \cdots & \longrightarrow & P_0 & \longrightarrow & A & \longrightarrow 0 \\
 & & \downarrow{\scriptstyle \varphi_n} & & \downarrow{\scriptstyle \varphi_{n-1}} & & & & \downarrow{\scriptstyle \varphi_0} & & \| & \\
0 & \longrightarrow & B & \longrightarrow & E_n & \longrightarrow & \cdots & \longrightarrow & E_1 & \longrightarrow & A & \longrightarrow 0
\end{array}
$$

kommutiert. Wir setzen $Q := \ker(\delta_{n-1}) = \mathrm{im}(\delta_n)$ und bestimmen $\varphi : Q \to B$, so dass $\varphi_n = \varphi \circ \delta_n$. Die Klasse $[\varphi]$ ist dann das Bild von $[(E)]$.
Wir wollen jetzt noch diskutieren, was beim Wechsel des Moduls B in $\mathrm{Yext}^n_R(A,B)$ passiert. Jeder R-Modulhomomorphismus $\varphi : B \to C$ induziert einen Gruppenhomomorphismus

$$\varphi_* : \mathrm{Yext}^n_R(A,B) \longrightarrow \mathrm{Yext}^n_R(A,C)$$

via Pushout. Expliziter: Sei $[(E) : 0 \to B \xrightarrow{\iota} E_n \to \ldots \to E_1 \to A \to 0] \in \mathrm{Yext}^n_R(A,B)$, dann liefert der Pushout P von ι mit φ das kommutative Diagramm

$$
\begin{array}{rccccccccccc}
 & 0 & \longrightarrow & B & \xrightarrow{\iota} & E_n & \longrightarrow & E_{n-1} & \longrightarrow \cdots \longrightarrow & E_1 & \longrightarrow & A & \longrightarrow 0 \\
 & & & \downarrow{\scriptstyle \varphi} & & \downarrow & & \| & & \| & & \| & \\
(E_\varphi): & 0 & \longrightarrow & C & \longrightarrow & P & \longrightarrow & E_{n-1} & \longrightarrow \cdots \longrightarrow & E_1 & \longrightarrow & A & \longrightarrow 0
\end{array}
$$

und wir setzen $\varphi_*([(E)]) = [(E_\varphi)]$.

Lemma 1.3.1. *Ist*

$$\begin{array}{lccccccccccccc} (E): & 0 \longrightarrow & B & \xrightarrow{\beta} & B_n & \xrightarrow{\beta_n} & B_{n-1} & \xrightarrow{\beta_{n-1}} & \cdots & \longrightarrow & B_1 & \xrightarrow{\beta_1} & A & \longrightarrow 0 \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi_n} & & \downarrow{\scriptstyle \varphi_{n-1}} & & & & \downarrow{\scriptstyle \varphi_1} & & \| & \\ (F): & 0 \longrightarrow & C & \xrightarrow{\gamma} & C_n & \xrightarrow{\gamma_n} & C_{n-1} & \xrightarrow{\gamma_{n-1}} & \cdots & \longrightarrow & C_1 & \xrightarrow{\gamma_1} & A & \longrightarrow 0 \end{array} \tag{1.3}$$

ein kommutatives Diagramm von R-Moduln, dann ist $\varphi_*([(E)]) = [(F)]$.

Beweis. Per Definition wird $\varphi_*([(E)])$ repräsentiert von

$$0 \to C \xrightarrow{\iota} P \xrightarrow{\tau} B_{n-1} \xrightarrow{\beta_{n-1}} \ldots \to B_1 \xrightarrow{\beta_1} A \to 0$$

mit $P := (C \oplus B_n) / \{(-\varphi(b), \beta(b)) \mid b \in B\}$, $\iota(c) = \overline{(c,0)}$ und $\tau\left(\overline{(c,b)}\right) = \beta_n(b)$.
Um die Behauptung zu zeigen, genügt es zu zeigen, dass

$$\begin{array}{lccccccccccccc} 0 \longrightarrow & C & \xrightarrow{\iota} & P & \xrightarrow{\tau} & B_{n-1} & \xrightarrow{\beta_{n-1}} & \cdots & \longrightarrow & B_1 & \xrightarrow{\beta_1} & A & \longrightarrow 0 \\ & \| & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \varphi_{n-1}} & & & & \downarrow{\scriptstyle \varphi_1} & & \| & \\ 0 \longrightarrow & C & \xrightarrow{\gamma} & C_n & \xrightarrow{\gamma_n} & C_{n-1} & \xrightarrow{\gamma_{n-1}} & \cdots & \longrightarrow & C_1 & \xrightarrow{\gamma_1} & A & \longrightarrow 0 \end{array}$$

mit $\psi(\overline{(c,b)}) = \gamma(c) + \varphi_n(b)$, ein kommutatives Diagramm ist.
Zuerst zeigen wir die Wohldefiniertheit der Abbildung $\psi : P \to C_n$. Für alle $b \in B$ gilt

$$\psi(\overline{(-\varphi(b), \beta(b))}) = -\gamma(\varphi(b)) + \varphi_n(\beta(b)) = 0,$$

wobei letzteres Gleichheitszeichen gilt, da das Diagramm (1.3) kommutiert.
Wir zeigen nur die Kommutativität von

$$\begin{array}{ccc} P & \xrightarrow{\tau} & B_{n-1} \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \varphi_{n-1}} \\ C_n & \xrightarrow{\gamma_n} & C_{n-1}, \end{array}$$

der Rest ist dann klar. Sei $\overline{(c,b)} \in P$, dann gilt

$$\begin{aligned} \varphi_{n-1}(\tau(\overline{(c,b)})) &= \varphi_{n-1}(\beta_n(b)) = \gamma_n(\varphi_n(b)) \quad \text{und} \\ \gamma_n(\psi(\overline{(c,b)})) &= \gamma_n(\gamma(c) + \varphi_n(b)) = \underbrace{\gamma_n(\gamma(c))}_{=0} + \gamma_n(\varphi_n(b)). \end{aligned}$$

Damit ist der Beweis abgeschlossen. □

Bemerkung 2. *Ist* $R = \mathbb{Z}[G]$, *dann schreiben wir statt* $\mathrm{Ext}^n_{\mathbb{Z}[G]}(A,B)$ *(bzw.* $\mathrm{Yext}^n_{\mathbb{Z}[G]}(A,B)$*) einfach* $\mathrm{Ext}^n_G(A,B)$ *(bzw.* $\mathrm{Yext}^n_G(A,B)$*).*

1.3.2 Tate-Kohomologie

Die folgenden Definitionen haben wir aus [Neu69, Teil I, §2] entnommen.
Sei G eine endliche Gruppe und A ein G-Modul. Wir definieren $\mathscr{C}^n(G,A) := \mathscr{C}^{-n-1}(G,A) := \{y : G^n \to A\}$ für $n \geq 1$ und $\mathscr{C}^0(G,A) := \mathscr{C}^{-1}(G,A) := A$. Wir werden jetzt Abbildungen $\partial_A^n : \mathscr{C}^{n-1}(G,A) \to \mathscr{C}^n(G,A)$ definieren, so dass

$$\ldots \to \mathscr{C}^{n-2}(G,A) \xrightarrow{\partial_A^{n-1}} \mathscr{C}^{n-1}(G,A) \xrightarrow{\partial_A^n} \mathscr{C}^n(G,A) \xrightarrow{\partial_A^{n+1}} \mathscr{C}^{n+1}(G,A) \to \ldots$$

ein Komplex ist, d.h. für alle $n \in \mathbb{Z}$ gilt $\partial_A^{n+1} \circ \partial_A^n = 0$. Wir definieren

$$\begin{aligned}
\partial_A^0(a) &= N_G(a) := \sum_{g\in G} ga, \\
\partial_A^1(a) &= \begin{cases} G & \to & A \\ g & \mapsto & ga - a, \end{cases} \\
\partial_A^{-1}(y) &= \sum_{g\in G} (g^{-1}y(g) - y(g)), \\
\partial_A^n(y) &= \begin{cases} G^n & \to & A \\ (g_1,\ldots,g_n) & \mapsto & g_1 y(g_2,\ldots,g_n) + (-1)^n y(g_1,\ldots,g_{n-1}) \\ & & + \sum_{i=1}^{n-1}(-1)^i y(g_1,\ldots,g_{i-1},g_ig_{i+1},g_{i+2},\ldots,g_n) \quad \text{für } n \geq 1, \end{cases} \\
\partial_A^{-n-1}(y) &= \begin{cases} G^n & \to & A \\ (g_1,\ldots,g_n) & \mapsto & \sum_{g\in G}[g^{-1}y(g,g_1,\ldots,g_n) + (-1)^{n+1} y(g_1,\ldots,g_n,g) \\ & & + \sum_{i=1}^{n}(-1)^i y(g_1,\ldots,g_{i-1},g_ig,g^{-1},g_{i+1},\ldots,g_n)] \quad \text{für } n \geq 0. \end{cases}
\end{aligned}$$

Wir setzen

$$\mathscr{Z}^n(G,A) := \ker(\partial_A^{n+1}) \quad \text{und} \quad \mathscr{B}^n(G,A) := \operatorname{im}(\partial_A^n).$$

Die Elemente aus $\mathscr{Z}^n(G,A)$ heißen *n-Kozykel* und die Elemente aus $\mathscr{B}^n(G,A)$ heißen *n-Koränder*. Die Faktorgruppe

$$\mathrm{H}^n(G,A) := \mathscr{Z}^n(G,A)/\mathscr{B}^n(G,A)$$

heißt n-te *Kohomologiegruppe* mit Werten in A oder auch Kohomologiegruppe der Dimension n.

1.3.3 Der Verbindungshomomorphismus und die exakte Kohomologiesequenz

Sei

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

eine exakte Sequenz von G-Moduln. Dann gibt es zu jedem $n \in \mathbb{Z}$ einen kanonischen Homomorphismus

$$\delta_n : \mathrm{H}^n(G, C) \to \mathrm{H}^{n+1}(G, A)$$

und die hieraus entstehende Sequenz

$$\cdots \longrightarrow \mathrm{H}^n(G, A) \longrightarrow \mathrm{H}^n(G, B) \longrightarrow \mathrm{H}^n(G, C) \xrightarrow{\delta_n} \mathrm{H}^{n+1}(G, A) \longrightarrow \cdots \tag{1.4}$$

ist exakt. Der Homomorphismus δ_n heißt *Verbindungshomomorphismus* und die Sequenz (1.4) heißt *exakte Kohomologiesequenz*.
Wir gehen noch kurz darauf ein, wie man den Verbindungshomomorphismus konstruiert, da wir dies an späterer Stelle in dieser expliziten Form brauchen. Wir betrachten dazu das kommutative Diagramm mit exakten Zeilen

$$\begin{array}{ccccccccc}
 & & \mathscr{C}^n(G,A)/\mathscr{B}^n(G,A) & \xrightarrow{\alpha} & \mathscr{C}^n(G,B)/\mathscr{B}^n(G,B) & \xrightarrow{\beta} & \mathscr{C}^n(G,C)/\mathscr{B}^n(G,C) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \partial_A^{n+1}} & & \downarrow{\scriptstyle \partial_B^{n+1}} & & \downarrow{\scriptstyle \partial_C^{n+1}} & & \\
0 & \longrightarrow & \mathscr{Z}^{n+1}(G,A) & \xrightarrow{\alpha} & \mathscr{Z}^{n+1}(G,B) & \xrightarrow{\beta} & \mathscr{Z}^{n+1}(G,C), & &
\end{array}$$

wobei die Abbildungen als die induzierten Abbildungen zu verstehen sind. Es gilt

$$\ker\left(\partial_C^{n+1}\right) = \mathrm{H}^n(G, C) \text{ und } \operatorname{coker}\left(\partial_A^{n+1}\right) = \mathrm{H}^{n+1}(G, A).$$

Das Schlangenlemma liefert uns dann den Verbindungshomomorphismus $\delta_n : \mathrm{H}^n(G, C) \to \mathrm{H}^{n+1}(G, A)$. Dem Beweis des Schlangenlemmas folgend konstruiert man δ_n wie folgt. Sei $[y] \in \mathrm{H}^n(G, C)$ mit $y \in \mathscr{C}^n(G, C)$. Finde $[y'] \in \mathscr{C}^n(G, B)/\mathscr{B}^n(G, B)$ mit $\beta(y') = y$ und berechne $\partial_B^{n+1}(y')$. Bestimme $y'' \in \mathscr{Z}^{n+1}(G, A)$ mit $\alpha(y'') = y'$ und setze

$$\delta_n([y]) := [y''].$$

Definition 1.3.2. *Ein G-Modul A heißt kohomologisch trivial, wenn $\mathrm{H}^i(H, A) = 0$ für alle $i \in \mathbb{Z}$ und alle Untergruppen H von G gilt.*

Bemerkungen 1.3.3. *(1) Die Eigenschaft eines Moduls kohomologisch trivial zu sein, wird meist in folgender Situation benutzt. Sei*

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

eine exakte Sequenz von G-Moduln. Ist der Modul B kohomologisch trivial, dann impliziert die exakte Kohomologiesequenz, dass $\mathrm{H}^i(G,A) \cong \mathrm{H}^{i-1}(G,C)$ für alle $i \in \mathbb{Z}$ gilt. Ist der Modul A bzw. C kohomologisch trivial, dann gilt mit dem selben Argument $\mathrm{H}^i(G,C) \cong \mathrm{H}^i(G,B)$ bzw. $\mathrm{H}^i(G,A) \cong \mathrm{H}^i(G,B)$ für alle $i \in \mathbb{Z}$.

(2) Ist A ein endlich erzeugter $\mathbb{Z}$-freier $\mathbb{Z}[G]$-Modul, dann gilt

$$A \text{ ist kohomologisch trivial } \Leftrightarrow \text{ } A \text{ ist } \mathbb{Z}[G]\text{-projektiv.}$$

Einen Beweis dieser Aussage findet sich in [Nak57, Th.1].

(3) Ein G-Modul A mit eindeutiger und uneingeschränkter Division ist kohomologisch trivial ([Neu69, Kor. (3.17)]), dabei heißt A von eindeutiger und uneingeschränkter Division, wenn die Gleichung $nx = a$ für jede natürliche Zahl n und jedes $a \in A$ eine eindeutige Lösung $x \in A$ besitzt. Insbesondere ist also jeder Körper F kohomologisch trivial.

1.3.4 Die Invariantenabbildung

Sei N/K eine Galoiserweiterung lokaler Körper mit Galoisgruppe G. Wir werden in diesem Abschnitt die sogenannte Invariantenabbildung

$$\mathrm{inv}_{N/K} : \mathrm{H}^2(G, N^\times) \tilde{\to} \frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z}$$

definieren. In der Klassenkörpertheorie ist diese Abbildung von zentraler Bedeutung. Wir folgen hier den Ausführungen in [Neu69].
Sei zunächst N/K als unverzweigt vorausgesetzt. Die Invariantenabbildung ist in diesem Fall definiert als das Kompositum von drei Isomorphismen

$$\mathrm{inv}_{N/K} : \mathrm{H}^2(G, N^\times) \xrightarrow{\overline{v}} \mathrm{H}^2(G, \mathbb{Z}) \xrightarrow{\partial_1^{-1}} \mathrm{H}^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\varphi} \frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z},$$

die wir im Folgenden definieren.
Definition von $\overline{v}$:

Sei v die normierte Bewertung auf N und sei U_N die Einheitengruppe des Bewertungsringes von N. Wir betrachten U_N und $N^\times$ als G-Moduln mit der natürlichen G-Wirkung. Zusammen mit $\mathbb{Z}$ als G-Modul mit trivialer Wirkung sitzen diese Moduln in der exakten Sequenz

$$1 \longrightarrow U_N \longrightarrow N^\times \xrightarrow{v} \mathbb{Z} \longrightarrow 0.$$

Da der Modul U_N kohomologisch trivial ist ([Neu69, Teil II, Satz (4.3)]) induziert v einen Isomorphismus

$$\overline{v} : \mathrm{H}^2(G, N^\times) \to \mathrm{H}^2(G, \mathbb{Z}).$$

Definition von ∂_1^{-1}:
Wir betrachten die exakte Sequenz

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

von G-Moduln, wobei $\mathbb{Q}, \mathbb{Z}$ und $\mathbb{Q}/\mathbb{Z}$ mit der trivialen G-Wirkung ausgestattet seien. Nach Bemerkung 1.3.3 ist $\mathbb{Q}$ kohomologisch trivial und somit ist der Verbindungshomomorphismus

$$\partial_1 : \mathrm{H}^1(G, \mathbb{Q}/\mathbb{Z}) \to \mathrm{H}^2(G, \mathbb{Z})$$

ein Isomorphismus.
Definition von φ:
Direktes Berechnen der 1-Kozykel und 1-Koränder zeigt

$$\mathrm{H}^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z}).$$

Da wir die Erweiterung N/K als unverzweigt vorausgesetzt haben, ist G zyklisch mit dem Frobeniusautomorphismus $\varphi_{N/K}$ als kanonischen Erzeuger. Für alle $\chi \in \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z})$ ist also $\chi(G) \subseteq \frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z}$ eine zyklische Untergruppe deren Ordnung ein Teiler von $|G|$ ist. Da es in $\mathbb{Q}/\mathbb{Z}$ zu jedem $n \in \mathbb{N}$ genau eine Untergruppe der Ordnung n gibt, nämlich die von $\frac{1}{n} + \mathbb{Z}$ erzeugte, ist $|\mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z})| = |\frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z}|$. Der Homomorphismus

$$\varphi : \begin{cases} \mathrm{H}^1(G, \mathbb{Q}/\mathbb{Z}) & \to & \frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z} \\ \chi & \mapsto & \chi(\varphi_{N/K}), \end{cases}$$

ist demnach wohldefiniert und ein Isomorphismus.

Für unverzweigte Erweiterungen N/K ist damit die Invariantenabbildung definiert.
Sei nun N/K nicht notwendig unverzweigt. Der Schlüssel zur Definition von $\mathrm{inv}_{N/K}$ ist der

Satz 1.3.4. *Sei L/K die unverzweigte Erweiterung mit $[L:K] = [N:K]$. Dann gibt es einen kanonischen Isomorphismus*

$$\alpha : \mathrm{H}^2(G, N^\times) \xrightarrow{\sim} \mathrm{H}^2(\mathrm{Gal}(L/K), L^\times).$$

Beweis. [Neu69, Teil II, Satz (5.2)] □

Wir definieren

$$\mathrm{inv}_{N/K} = \mathrm{inv}_{L/K} \circ \alpha.$$

Insgesamt haben wir damit die Invariantenabbildung für lokale Erweiterungen definiert.

Definition 1.3.5. *Das eindeutig bestimmte Element $\gamma \in \mathrm{H}^2(G, N/K)$ mit $\mathrm{inv}_{N/K}(\gamma) = \frac{1}{[N:K]} + \mathbb{Z}$ heißt lokale Fundamentalklasse.*

Sei nun N/K eine normale Zahlkörpererweiterung mit Galoisgruppe G. Für eine Stelle $\mathfrak{p}$ von N sei $N_\mathfrak{p}$ die Komplettierung von N nach $\mathfrak{p}$. Für das Bild von $a \in N$ in $N_\mathfrak{p}$ schreiben wir a. Sei C_N die Idelklassengruppe von N, d.h. C_N ist die Faktorgruppe $J_N/\iota(N^\times)$, wobei $J_N := \{(a_\mathfrak{p})_\mathfrak{p} \in \prod_\mathfrak{p} N_\mathfrak{p} \mid a_\mathfrak{p} \in U_{N_\mathfrak{p}} \text{ für fast alle } \mathfrak{p}\}$ die Idelgruppe ist und $\iota : N^\times \to J_N$ die Diagonaleinbettung. Auch hier definiert man eine Invariantenabbildung

$$\mathrm{inv}_{N/K} : \mathrm{H}^2(G, C_N) \xrightarrow{\sim} \frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z}.$$

Definition 1.3.6. *Das Element $\alpha \in \mathrm{H}^2(G, C_N)$ mit $\mathrm{inv}_{N/K}(\alpha) = \frac{1}{[N:K]} + \mathbb{Z}$ heißt globale Fundamentalklasse.*

Da wir nur bei der Definition von Tates kanonischer Klasse die globale Fundamentalklasse benötigen (aber keine weiteren Eigenschaften von ihr) und die Definition der Invariantenabbildung im globalen Fall relativ kompliziert ist, verzichten wir in dieser Arbeit darauf und verweisen stattdessen auf [Neu69, Teil III].

1.3.5 Die Isomorphie $\mathrm{Yext}^2_G(\mathbb{Z}, C) \cong \mathrm{H}^2(G, C)$

Sei G eine endliche Gruppe und C ein G-Modul. Wir stellen hier einen konstruktiven Beweis der Isomorphie $\mathrm{Yext}^2_G(\mathbb{Z}, C) \cong \mathrm{H}^2(G, C)$ vor, da wir dies später benötigen und uns kein Literaturhinweis für diesen konstruktiven Beweis bekannt ist.

Satz 1.3.7. *Es gibt einen Isomorphismus*

$$\Psi : \mathrm{Yext}^2_G(\mathbb{Z}, C) \xrightarrow{\sim} \mathrm{H}^2(G, C).$$

Beweis. Sei $[E : 0 \to C \xrightarrow{\iota} A \xrightarrow{\phi} B \xrightarrow{\varepsilon} \mathbb{Z} \to 0] \in \mathrm{Yext}^2_G(\mathbb{Z}, C)$. Die Sequenz zerfällt in die beiden kurzen exakten Sequenzen

$$0 \longrightarrow \ker(\varepsilon) \longrightarrow B \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0 \qquad \text{und} \qquad 0 \longrightarrow C \longrightarrow A \xrightarrow{\phi} \mathrm{im}(\phi) \longrightarrow 0.$$

Die erste Sequenz induziert den Verbindungshomomorphismus

$$\delta_0 : \mathrm{H}^0(G, \mathbb{Z}) \to \mathrm{H}^1(G, \ker(\varepsilon))$$

und die zweite

$$\delta_1 : \mathrm{H}^1(G, \ker(\varepsilon)) \to \mathrm{H}^2(G, C).$$

Wir definieren die Abbildung $\Psi : \mathrm{Yext}^2_G(\mathbb{Z}, C) \to \mathrm{H}^2(G, C)$ als $\Psi([E]) := [\delta_1(\delta_0(1 + |G|\mathbb{Z}))]$. Die Wohldefiniertheit sehen wir wie folgt. Ist

$$\begin{array}{lccccccccc} E_1 : & 0 & \longrightarrow & C & \longrightarrow & B & \longrightarrow & A & \xrightarrow{\varphi} & \mathbb{Z} & \longrightarrow & 0 \\ & & & \| & & \downarrow & & \downarrow & & \| & & \\ E_2 : & 0 & \longrightarrow & C & \longrightarrow & B' & \longrightarrow & A' & \xrightarrow{\varphi'} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

ein kommutatives Diagramm mit exakten Zeilen und setzen wir $\kappa := \ker(\varphi)$ und $\kappa' := \ker(\varphi')$, dann sind auch

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C & \longrightarrow & B & \longrightarrow & \kappa & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & C & \longrightarrow & B' & \longrightarrow & \kappa' & \longrightarrow & 0 \end{array} \qquad \begin{array}{ccccccccc} 0 & \longrightarrow & \kappa & \longrightarrow & A & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & \kappa' & \longrightarrow & A' & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

kommutative Diagramme mit exakten Zeilen. Aus [Neu69, I. Satz 3.5] folgt, dass

$$\begin{array}{ccccc} \mathrm{H}^0(G, \mathbb{Z}) & \xrightarrow{\delta_0} & \mathrm{H}^1(G, \kappa) & \xrightarrow{\delta_1} & \mathrm{H}^2(G, C) \\ \| & & \downarrow & & \| \\ \mathrm{H}^0(G, \mathbb{Z}) & \xrightarrow{\delta_0} & \mathrm{H}^1(G, \kappa') & \xrightarrow{\delta_1} & \mathrm{H}^2(G, C) \end{array}$$

kommutativ ist. Dies zeigt die Wohldefiniertheit.
Sei nun $[c] = \gamma \in \mathrm{H}^2(G, C)$. Wir definieren zunächst wie in [NSW08, Ch.III, §1] den $\mathbb{Z}$-Modul $C(\gamma) := C \oplus \bigoplus_{g \neq 1} \mathbb{Z} b_g$ mit formalen Symbolen b_g. Wir setzen $b_1 := c(1, 1)$ und definieren auf $C(\gamma)$ eine G-Wirkung durch

$$g b_h := b_{gh} - b_g + c(g, h).$$

Wir erhalten damit eine exakte Sequenz

$$E_\gamma : \quad 0 \to C \xrightarrow{\iota} C(\gamma) \xrightarrow{\psi} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0,$$

wobei ι die Inklusion, ε die Augmentation und $\psi(b_g) = g - 1$ für $g \neq 1$, $\psi(c) = 0$ für $c \in C$, ist. Wir definieren

$$\Phi : \left\{ \begin{array}{ccc} \mathrm{H}^2(G, C) & \to & \mathrm{Yext}^2_G(\mathbb{Z}, C) \\ \gamma & \mapsto & [E_\gamma]. \end{array} \right.$$

Um die Wohldefiniertheit zu zeigen, zeigen wir dass $C(\gamma)$ bis auf Isomorphie nicht vom Repräsentanten abhängt. Sei also $[c] = [c']$, d.h. es gibt einen 1-Korand $y \in \mathscr{B}^1(G, C)$ mit $c = c' + y$. Sei $C(c) := C \oplus \bigoplus_{g \neq 1} \mathbb{Z} b_g$ der G-Modul mit der von c induzierten G-Wirkung und $C(c') := C \oplus \bigoplus_{g \neq 1} \mathbb{Z} b'_g$ entsprechend definiert. Man rechnet nun ohne Mühe nach, dass

$$\left\{ \begin{array}{ccc} C(c) & \to & C(c') \\ c + \sum\limits_{g \neq 1} \lambda_g b_g & \mapsto & c + \sum\limits_{g \neq 1} \lambda_g b'_g - \sum\limits_{g \neq 1} \lambda_g y(g), \end{array} \right.$$

ein Isomorphismus von G-Moduln ist.
Wir zeigen nun, dass die Abbildungen invers zueinander sind.
Sei $[E : 0 \to C \to A \xrightarrow{\phi} B \xrightarrow{\varepsilon} \mathbb{Z} \to 0] \in \mathrm{Yext}^2_G(\mathbb{Z}, C)$. Wir berechnen zunächst einen Repräsentanten von $\Phi([E])$. Das Element $\delta_0(1 + |G|\mathbb{Z}) \in \mathrm{H}^1(G, \ker(\varepsilon))$ wird nach Definition von δ_0 repräsentiert von

$$\partial^1_B(b) : \left\{ \begin{array}{ccc} G & \to & \ker(\varepsilon) \\ g & \mapsto & gb - b, \end{array} \right.$$

wobei $\varepsilon(b) = 1$ ist. Sei nun $y \in \mathscr{C}^1(G, A)$ mit

$$\phi(y(g)) = gb - b \quad \text{für alle } g \in G,$$

dann wird $\gamma := \Phi([E]) = \delta_1(\delta_0(1 + |G|\mathbb{Z})) \in \mathrm{H}^2(G, C)$ repräsentiert von

$$\partial^2_A(y) : \left\{ \begin{array}{ccc} G \times G & \to & C \\ (g, h) & \mapsto & gy(h) - y(gh) + y(g). \end{array} \right.$$

Wir berechnen nun einen Repräsentanten von $\Phi(\gamma)$. Wir setzen $B' := \bigoplus_{g \neq 1} \mathbb{Z} b_g$ und $C(\gamma) := C \oplus B'$ mit G-Wirkung

$$g b_h := b_{gh} - b_g + gy(h) - y(gh) + y(g).$$

und $b_1 := y(1)$. Daraus ergibt sich als Repräsentant von $\Phi(\gamma)$ die exakte Sequenz

$$0 \longrightarrow C \longrightarrow C(\gamma) \xrightarrow{\psi} \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0, \tag{1.5}$$

mit $\psi(c) = 0$, falls $c \in C$, und $\psi(b_g) = g - 1$.
Die Sequenzen E und (1.5) repräsentieren in $\mathrm{Yext}^2_G(\mathbb{Z}, C)$ das gleiche Element, denn das Diagramm

$$\begin{array}{ccccccccc}
0 & \longrightarrow & C & \longrightarrow & C(\gamma) & \xrightarrow{\psi} & \mathbb{Z}[G] & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle \phi_2} & & \downarrow{\scriptstyle \phi_1} & & \| & & \\
0 & \longrightarrow & C & \longrightarrow & A & \xrightarrow{\phi} & B & \xrightarrow{\varphi} & \mathbb{Z} & \longrightarrow & 0,
\end{array}$$

mit

$$\begin{aligned}
\phi_1(1) &= b, \\
\phi_2\left(c + \sum_{g \neq 1} \lambda_g b_g\right) &= c + \sum_{g \neq 1} \lambda_g y(g),
\end{aligned}$$

ist kommutativ. Dies zeigt $\Phi \circ \Psi = \mathrm{id}$. Sei nun $[c] = \gamma \in \mathrm{H}^2(G, C)$. Wir betrachten dazu die übliche Sequenz

$$0 \to C \to C(\gamma) \xrightarrow{\psi} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0,$$

die $\Phi(\gamma)$ repräsentiert, und konstruieren dazu $\delta_1(\delta_0(1 + |G|\mathbb{Z}))$. Die Klasse $\delta_0(1 + |G|\mathbb{Z})$ wird repräsentiert von

$$\partial^1_{\mathbb{Z}[G]}(1) : \left\{ \begin{array}{ccc} G & \to & \mathbb{Z}[G] \\ g & \mapsto & g - 1 \end{array} \right. .$$

Mit

$$y : \left\{ \begin{array}{ccc} G & \to & C(\gamma) \\ g & \mapsto & b_g \end{array} \right.$$

gilt $\psi(y(g)) = g - 1$ für alle $g \in G$ und demzufolge wird $\delta_1(\delta_0(1 + |G|\mathbb{Z}))$ repräsentiert von

$$\partial^2_{C(\gamma)}(y) : \left\{ \begin{array}{ccc} G \times G & \to & C \\ (g, h) & \mapsto & gy(h) - y(gh) + y(g) \end{array} \right. .$$

Dies ist aber gerade der 2-Kozykel c. Damit ist auch $\Psi \circ \Phi = \mathrm{id}$ gezeigt.
Wir zeigen nun noch, dass Φ ein Gruppenhomomorphismus ist. Die Homomorphieeigenschaft von Ψ ergibt sich dann aus dem bereits Gezeigtem. Da wir die Gruppenstruktur auf $\mathrm{Yext}^2_G(\mathbb{Z}, C)$ über die Gruppenstruktur von $\mathrm{Ext}^2_G(\mathbb{Z}, C)$ definiert haben, betrachten

wir Φ als Abbildung von $\mathrm{H}^2(G,C)$ nach $\mathrm{Ext}^2_G(\mathbb{Z},C)$. Die Gruppe G werde erzeugt von $\{g_1,\ldots,g_r\}$. Wir wählen die Sequenz

$$0 \to Q \to \mathbb{Z}[G]^r \xrightarrow{\phi} \mathbb{Z}[G] \to \mathbb{Z} \to 0,$$

mit $\phi((\sum_{g\in G}\lambda_g^{(1)}g,\ldots,\sum_{g\in G}\lambda_g^{(r)}g)) = \sum_{g\in G}\lambda_g^{(1)}g(g_1-1)+\ldots+\sum_{g\in G}\lambda_g^{(r)}g(g_r-1)$, zur Berechnung von $\mathrm{Ext}^2_G(\mathbb{Z},C)$. Sei nun $[c]=\gamma\in\mathrm{H}^2(G,C)$ und

$$0 \longrightarrow C \longrightarrow C(\gamma) \xrightarrow{\psi} \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$$

die Sequenz, die das Bild von γ in $\mathrm{Yext}^2_G(\mathbb{Z},C)$ repräsentiert. Mit

$$\phi_\gamma : \left\{ \begin{array}{ccc} \mathbb{Z}[G]^r & \to & C(\gamma) \\ (\sum\limits_{g\in G}\lambda_g^{(1)}g,\ldots,\sum\limits_{g\in G}\lambda_g^{(r)}g) & \mapsto & \sum\limits_{g\in G}\lambda_g^{(1)}gb_{g_1}+\ldots+\sum\limits_{g\in G}\lambda_g^{(r)}gb_{g_r} \end{array} \right.$$

und $f_\gamma := \phi_\gamma|_Q$ ist das Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Q & \longrightarrow & \mathbb{Z}[G]^r & \xrightarrow{\phi} & \mathbb{Z}[G] & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_\gamma} & & \downarrow{\scriptstyle \phi_\gamma} & & \| & & \| & & \\ 0 & \longrightarrow & C & \longrightarrow & C(\gamma) & \xrightarrow{\psi} & \mathbb{Z}[G] & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

kommutativ. In $\mathrm{Ext}^2_G(\mathbb{Z},C)$ wird also $\Phi(\gamma)$ repräsentiert von f_γ.
Da f_γ die Einschränkung von ϕ_γ ist, ist für $q=(\sum_{g\in G}\lambda_g^{(1)}g,\ldots,\sum_{g\in G}\lambda_g^{(r)}g)\in Q$ das Element $\phi_\gamma(q)\in C$, d.h. es gibt ein nur von q abhängiges $\mu_q\in\mathbb{Z}$ mit $\sum_{g\in G}\lambda_g^{(1)}gb_{g_1}+\ldots+\sum_{g\in G}\lambda_g^{(r)}gb_{g_r}=\mu c(1,1)$, also $f_\gamma(q)=\mu_q c(1,1)$. Seien nun $[c]=\gamma,[c_1]=\gamma_1\in\mathrm{H}^2(G,C)$. Dann gilt für alle $q\in Q$

$$f_\gamma(q)+f_{\gamma_1}(q)=\mu_q c(1,1)+\mu_q c'(1,1)=\mu_q(c(1,1)+c'(1,1))=f_{\gamma+\gamma_1}.$$

Es gilt also

$$\Phi(\gamma)+\Phi(\gamma_1)=[f_\gamma]+[f_{\gamma_1}]=[f_{\gamma+\gamma_1}]=\Phi(\gamma+\gamma_1).$$

□

Bemerkung 3. *Ist $\alpha\in\mathrm{H}^2(G,N^\times)$ die lokale Fundamentalklasse bzw. ihr Inverses, dann nennen wir das Bild von α unter den angegebenen Isomorphismen $H^2(G,N^\times)\cong\mathrm{Ext}^2_G(\mathbb{Z},N^\times)\cong\mathrm{Yext}^2_G(\mathbb{Z},N^\times)$ ebenfalls die lokale Fundamentalklasse bzw. ihr Inverses.*

1.4 Tates kanonische Klasse

Sei N/K eine endliche galoissche Zahlkörpererweiterung mit Galoisgruppe G und S eine endliche Menge von Stellen von N mit den Eigenschaften

1) S enthält die unendlichen Stellen,
2) S enthält die über K verzweigten Stellen,
3) G wirkt auf S und
4) die endlichen Stellen in S erzeugen die Idealklassengruppe.

Definition 1.4.1. *Wir nennen eine endliche Stellenmenge S mit den Eigenschaften 1) - 4) zulässig für N/K. Ist aus dem Kontext klar erkennbar, welche Körpererweiterung gemeint ist, dann nennen wir S nur zulässig.*

Für $v \in S$ bezeichnen wir die Komplettierung von N bei v mit N_v und die Einheitengruppe des Bewertungsringes von N_v mit U_{N_v}. Wir definieren folgende G-Moduln:

Definition 1.4.2.

Y_S *sei die freie abelsche Gruppe über S mit G-Wirkung*

$$g\left(\sum_{v\in S}\lambda_v v\right) := \sum_{v\in S}\lambda_v(gv) = \sum_{v\in S}\lambda_{g^{-1}v}v.$$

X_S *sei der Kern der Augmentation $\varepsilon : Y_S \to \mathbb{Z}, \sum \lambda_v v \mapsto \sum \lambda_v$.*

J_S *sei die Gruppe der S-Idele, d.h.*

$$J_S = \prod_{v\in S} N_v^\times \times \prod_{v\notin S} U_{N_v}$$

U_S *seien die S-Einheiten, also $U_S = \{a \in N^\times \mid v(a) = 0 \text{ f.a. } v \notin S\}$ mit der offensichtlichen G-Wirkung.*

C_S *sei die S-Idelklassengruppe, d.h. mit der Diagonaleinbettung $\iota : U_S \to J_S, a \mapsto (a)_v$ ist $C_S = J_S/\iota(U_S)$.*

Wir haben also zwei exakte Sequenzen

$$(U)_S : \quad 0 \to U_S \to J_S \to C_S \to 0$$

$$(X)_S: \quad 0 \to X_S \to Y_S \to \mathbb{Z} \to 0$$

von G-Moduln. In [Tat66] vergleicht Tate die Galoiskohomologie dieser beiden Sequenzen und zeigt, dass es Gruppenisomorphismen $\alpha_i^r, i = 1, 2, 3, r \in \mathbb{N}$ gibt, so dass

$$\begin{array}{ccccccccc}
\cdots \longrightarrow & \mathrm{H}^r(G, X_S) & \longrightarrow & \mathrm{H}^r(G, Y_S) & \longrightarrow & \mathrm{H}^r(G, \mathbb{Z}) & \longrightarrow & \mathrm{H}^{r+1}(G, X_S) & \longrightarrow \cdots \\
& \downarrow{\scriptstyle \alpha_3^r} & & \downarrow{\scriptstyle \alpha_2^r} & & \downarrow{\scriptstyle \alpha_1^r} & & \downarrow{\scriptstyle \alpha_3^{r+1}} & \\
\cdots \longrightarrow & \mathrm{H}^{r+2}(G, U_S) & \longrightarrow & \mathrm{H}^{r+2}(G, J_S) & \longrightarrow & \mathrm{H}^{r+2}(G, C_S) & \longrightarrow & \mathrm{H}^{r+3}(G, U_S) & \longrightarrow \cdots
\end{array}$$

kommutativ ist. Dazu gibt er Elemente

$$\begin{aligned}
\alpha_1 &\in \mathrm{H}^2(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, C_S)), \\
\alpha_2 &\in \mathrm{H}^2(G, \mathrm{Hom}_{\mathbb{Z}}(Y_S, J_S)) \quad \text{und} \\
\alpha_3 &\in \mathrm{H}^2(G, \mathrm{Hom}_{\mathbb{Z}}(X_S, U_S))
\end{aligned}$$

an, die dann via Cupprodukt (vgl. [Neu69, Teil I, §5]) die Isomorphismen liefern.
Wir bemerken an dieser Stelle, dass für einen $\mathbb{Z}$-freien G-Modul M und einen G-Modul N nach [Bro94, Ch. III, Prop. (2.2)] gilt

$$\mathrm{H}^2(G, \mathrm{Hom}_{\mathbb{Z}}(M, N)) \cong \mathrm{Ext}_G^2(M, N),$$

wobei die G-Wirkung auf $\mathrm{Hom}_{\mathbb{Z}}(M, N)$ gegeben ist mit $g\alpha : M \to N, m \mapsto g\alpha(g^{-1}m)$.
Definition von α_1:
Sei C die Idelklassengruppe und $Cl_S(N)$ die S-Klassengruppe, d.h. $Cl_S(N)$ ist die Klassengruppe $Cl(N)$ modulo der Untergruppe, die von den Klassen der endlichen Stellen von S erzeugt wird. Zu einer endlichen Stelle v bezeichne $\mathfrak{P}_v$ das zugehörige Primideal.
Der surjektive Homomorphismus

$$\begin{cases}
C & \to & Cl(N) \\
[(a_v)_v] & \mapsto & \left[\prod_{\mathfrak{P}_v \nmid \infty} \mathfrak{P}_v^{v(a_v)}\right]
\end{cases}$$

induziert einen surjektiven Homomorphismus $C \to Cl_S(N)$. Zusammen mit der natürlichen Inklusion $C_S \to C$ erhalten wir eine exakte Sequenz

$$0 \longrightarrow C_S \longrightarrow C \longrightarrow Cl_S(N) \longrightarrow 0.$$

Aus dem Homomorphiesatz folgt $C/C_S \cong Cl_S(N)$. Da nach Eigenschaft 4) an die Stellenmenge S gilt $Cl_S(N) = \{1\}$, ist also $C \cong C_S$. Wir definieren $\alpha_1 \in \mathrm{H}^2(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, C_S))$ als die globale Fundamentalklasse in $\mathrm{H}^2(G, C)$ unter dem Isomorphismus

$$\mathrm{H}^2(G, C) \cong \mathrm{H}^2(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, C_S)).$$

Definition von α_2:
Zunächst zeigen wir den

Satz 1.4.3. *Ist S_0 ein Repräsentantensystem der G-Orbits in S und M ein G-Modul, dann gilt*

$$\bigoplus_{v \in S_0} \mathrm{H}^i(G_v, M) \cong \mathrm{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(Y_S, M)).$$

Beweis. Es ist

$$Y_S = \bigoplus_{v \in S} \mathbb{Z}v = \bigoplus_{v \in S_0} \mathrm{Ind}_{G_v}^G \mathbb{Z}.$$

Definieren wir $Y_v := \mathrm{Ind}_{G_v}^G \mathbb{Z}$ und sei $\{\sigma_1, \ldots, \sigma_n\}$ ein Repräsentantensystem der Rechtsnebenklassen von G/G_v, dann ist

$$\psi : \begin{cases} \mathrm{Ind}_{G_v}^G M = \bigoplus_{i=1}^n \sigma_i M & \longrightarrow \quad \mathrm{Hom}_{\mathbb{Z}}(Y_v, M) \\ \sum_{i=1}^n \sigma_i m_i & \longmapsto \quad \alpha : \begin{cases} Y_v & \to & M \\ \sum_{i=1}^n \sigma_i z_i & \mapsto & \sum_{i=1}^n z_i \sigma_i(m_i) \end{cases} \end{cases}$$

ein Isomorphismus von G-Moduln. Unter Benutzung dieser Tatsache und dass Kohomologie mit Produkten kommutiert, sowie Shapiro's Lemma gilt also

$$\begin{aligned} \mathrm{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(Y_S, M)) \cong \bigoplus_{v \in S_0} \mathrm{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(Y_v, M)) &\cong \bigoplus_{v \in S_0} \mathrm{H}^i(G, \mathrm{Ind}_{G_v}^G M)) \\ &\cong \bigoplus_{v \in S_0} \mathrm{H}^i(G_v, M). \end{aligned}$$

□

Sei der Isomorphismus für $i = 2$ und $M = J_S$ mit ϕ bezeichnet und für $v \in S$ sei $i_v : N_v^\times \to J_S$ die natürliche Inklusion. Diese induziert Gruppenhomomorphismen $i_{\star,v} : \mathrm{H}^2(G_v, N_v^\times) \to \mathrm{H}^2(G_v, J_S)$. Mit $\alpha_v \in \mathrm{H}^2(G_v, N_v^\times)$ sei die lokale Fundamentalklasse bezeichnet. Wir definieren

$$\alpha_2 := \phi(\oplus_{v \in S_0} i_{\star,v}(\alpha_v)) \in \mathrm{H}^2(G, \mathrm{Hom}_{\mathbb{Z}}(Y_S, J_S)).$$

Definition 1.4.4. *Die Klasse $\alpha_2 \in \mathrm{H}^2(G, \mathrm{Hom}_{\mathbb{Z}}(Y_S, J_S))$ heißt semi-lokale Fundamentalklasse.*

Definition von α_3:
Sei $\mathrm{Hom}((X)_S, (U)_S)$ die Gruppe aller Tripel (f_3, f_2, f_1), so dass

$$\begin{array}{lccccccc} (X)_S: & 0 & \longrightarrow & X_S & \longrightarrow & Y_S & \longrightarrow & \mathbb{Z} \longrightarrow 0 \\ & & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_1} \\ (U)_S: & 0 & \longrightarrow & U_S & \longrightarrow & J_S & \longrightarrow & C_S \longrightarrow 0 \end{array}$$

kommutiert. Sei $\pi_i((f_3, f_2, f_1)) = f_i$ die Projektion und $\pi_{\star,i}$ die induzierte Abbildung in der Kohomologie. Tate zeigt in [Tat66], dass es genau ein $\alpha \in \mathrm{H}^2(G, \mathrm{Hom}((X)_S, (U)_S))$ gibt mit $\pi_{\star,1}(\alpha) = \alpha_1$ und $\pi_{\star,2}(\alpha) = \alpha_2$. Wir definieren

$$\alpha_3 := \pi_{\star,3}(\alpha) \in \mathrm{H}^2(G, \mathrm{Hom}_G(X_S, U_S)).$$

Definition 1.4.5. *Das Element $\alpha_3 \in \mathrm{H}^2(G, \mathrm{Hom}_{\mathbb{Z}}(X_S, U_S))$ heißt Tates kanonische Klasse.*

Bemerkung 4. *Wie wir schon gesehen haben gilt*

$$\mathrm{H}^2(G, \mathrm{Hom}_{\mathbb{Z}}(X_S, U_S)) \cong \mathrm{Ext}^2_G(X_S, U_S) \cong \mathrm{Yext}^2_G(X_S, U_S).$$

Das Bild der lokalen Fundamentalklasse α_3 unter diesen Isomorphismen nennen wir ebenfalls Tates kanonische Klasse.

Kapitel 2

Problemstellung

Ziel dieser Arbeit war es, einen Algorithmus zu entwickeln, der die äquivariante Tamagawazahlvermutung für Zahlkörper an der Stelle $s = 0$ numerisch verifiziert, nach Möglichkeit beweist, und diesen Algorithmus in ein Computeralgebrasystem zu implementieren. Zum größten Teil ist dies auch gelungen. Ist N/K eine galoissche Zahlkörpererweiterung mit Galoisgruppe G und gibt es eine Stelle v_0 mit $G_{v_0} = G$, dann können wir zeigen, dass es einen Algorithmus gibt, der die Vermutung für jedes Fallbeispiel numerisch verifiziert. Unter zusätzlichen Voraussetzungen an die Charaktere der Gruppe G (vgl. Satz 3.3.5) können wir zeigen, dass es einen Algorithmus gibt, der die Vermutung für jedes Fallbeispiel über $\mathbb{Q}$, welches die Voraussetzungen erfüllt, beweist. In das Computeralgebrasystem MAGMA haben wir jedoch bislang nur einen Algorithmus implementiert, der die Vermutung für höchstens zahm verzweigte A_4-Erweiterungen numerisch verifiziert. Allerdings erfüllen die Charaktere der A_4 die zusätzlichen Voraussetzungen. Dies zeigen wir auch im Kapitel Beispiele. Mit diesem Algorithmus haben wir für 27 Erweiterungen die Vermutung numerisch verifiziert.
Die größte Schwierigkeit bei der Umsetzung lag dabei in der Konstruktion einer sogenannten Tate-Sequenz (siehe Lemma (2.1)). Wir sind dabei nach Ideen von Chinburg ([Chi89]) vorgegangen, die u.a. auch von Navilarekallu in [Nav06] zur Verifikation der Vermutung herangezogen wurden. Schwierig ist die Konstruktion einer Tate-Sequenz nach den Arbeiten von Chinburg unter anderem deswegen, weil lokale Fundamentalklassen (zur Definition der lokalen Fundamentalklasse siehe Abschnitt 1.3.4) berechnet werden müssen. Für höchstens zahm verzweigte Erweiterungen sind wir dabei den Ausführungen von Chinburg in [Chi85] gefolgt, die auf den Arbeiten von Serre [Ser] basieren. Für beliebige Erweiterungen ist die algorithmische

Berechnung von lokalen Fundamentalklassen durch die Arbeit von Debeerst ([Deb11]) abgedeckt. Dieser Algorithmus benutzt ebenfalls die Arbeiten von Serre. Da der von uns implementierte Algorithmus im höchstens zahm verzweigten Fall schneller ist, ist dieser dem anderen vorzuziehen.

Dass es sich bei dem Algorithmus in erster Linie um eine numerische Verifikation handelt, liegt daran, dass wir von gewissen reellen Zahlen zunächst nicht wissen, ob sie algebraisch sind. In bestimmten Fällen können wir dies jedoch zeigen und die algebraischen Zahlen berechnen. Unter diese Fälle fallen auch die A_4-Erweiterungen. Da wir aber die exakte Berechnung dieser Zahlen noch nicht in den Algorithmus implementiert haben, sind unsere Beispiele bisher nur numerische Verifikationen.
Im nächsten Abschnitt werden wir die Vermutung formulieren und im darauf folgenden Abschnitt kurz darauf eingehen, in welchen Fällen die Vermutung bewiesen ist. Auf die algorithmische Umsetzung gehen wir erst im nächsten Kapitel ein.

2.1 Die äquivariante Tamagawazahlvermutung für Zahlkörper an der Stelle $s = 0$

2.1.1 Formulierung der Vermutung

Zu einer endlichen galoisschen Zahlkörpererweiterung N/K assoziiert man zum einen auf algebraischem Wege und zum anderen auf analytischem Wege jeweils ein Element in der relativen K-Gruppe $K_0(\mathbb{Z}[G], \mathbb{R})$. Die Vermutung ist, das diese Elemente gleich sind. Im Folgenden formulieren wir dies genauer.
Sei N/K eine endliche galoissche Zahlkörpererweiterung mit Galoisgruppe G und S eine zulässige Stellenmenge für N/K (vgl. Definition 1.4.1).
Wir bezeichnen mit U_S die S-Einheiten von N und mit X_S den Kern der Augmentation

$$\begin{cases} Y_S & \to & \mathbb{Z} \\ \sum_{v\in S}\lambda_v v & \mapsto & \sum_{v\in S}\lambda_v \end{cases},$$

wobei Y_S der G-Modul $\{\sum_{v\in S}\lambda_v v \mid \lambda_v \in \mathbb{Z}\}$ mit der von G auf S induzierten Wirkung sei und die Wirkung von G auf $\mathbb{Z}$ trivial sei.
Das folgende Resultat wird von Tate in [Tat66, Ch.II, Th. 5.1] gezeigt.

Lemma 2.1.1. *Es gibt eine exakte Sequenz*

$$0 \to U_S \to A_S \to B_S \to X_S \to 0 \tag{2.1}$$

die Tates kanonische Klasse $\alpha_3(S) \in \mathrm{Yext}^2_G(X_S, U_S)$ *repräsentiert und in der* A_S *und* B_S *endlich erzeugt und kohomologisch trivial sind.*

Wir nennen so eine Sequenz *Tate-Sequenz*. Man kann zeigen, dass der Komplex $C^\bullet : A_S \to B_S$ perfekt ist, d.h. es gibt einen beschränkten Komplex $P^\bullet$ von endlich erzeugten projektiven $\mathbb{Z}[G]$-Moduln der quasi isomorph zu $C^\bullet$ ist. Mit Hilfe des Komplexes $P^\bullet$ konstruiert man zur Sequenz (2.1) ein Element in der relativen K-Gruppe $K_0(\mathbb{Z}[G], \mathbb{R})$, die sogenannte *Euler Charakteristik* (vgl. [BB07, 4], [Bur01, §2 insbesondere Th. 2.1.2] und [BB05, 5]). Wir führen diese Konstruktion nur in unserem Spezialfall durch. Für den allgemeinen Fall verweisen wir auf [Bur01, 1.2] und [BF01].
Aus unserer späteren Konstruktion der Tate-Sequenz, erhalten wir ein Diagramm

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & \kappa & = & \kappa & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \to & X(-2) & \to & F^0 & \xrightarrow{\alpha} & F^1 & \to & X_S & \to & 0 \\
 & & \downarrow f & & \downarrow & & \| & & \| & & \\
0 & \to & U_S & \to & A_S & \to & B_S & \to & X_S & \to & 0 \\
 & & \downarrow & & \downarrow & & & & & & \\
 & & 0 & & 0 & & & & & &
\end{array} \tag{2.2}$$

mit exakten Zeilen, wobei die untere Zeile die Sequenz (2.1) ist und die $\mathbb{Z}[G]$-Moduln F^0, F^1 und κ projektiv sind. Zu einem $\mathbb{Z}[G]$-Modul M definieren wir den $\mathbb{R}[G]$-Modul $M_\mathbb{R} := M \otimes_\mathbb{Z} \mathbb{R}$. Sei nun W das Bild der Abbildung $\alpha : F^0 \to F^1$ und seien $s_1 : X_{S,\mathbb{R}} \oplus W_\mathbb{R} \to F^1_\mathbb{R}, s_2 : X(-2)_\mathbb{R} \oplus W_\mathbb{R} \to F^0_\mathbb{R}$ sowie $s_3 : \kappa_\mathbb{R} \oplus U_{S,\mathbb{R}} \to X(-2)_\mathbb{R}$ Isomorphismen[1], die von Schnitten der exakten Sequenzen

$$\begin{aligned}
0 \to W_\mathbb{R} \to F^1_\mathbb{R} \to X_{S,\mathbb{R}} \to 0, \\
0 \to X(-2)_\mathbb{R} \to F^0_\mathbb{R} \to W_\mathbb{R} \to 0 \quad \text{und} \\
0 \to \kappa_\mathbb{R} \to X(-2)_\mathbb{R} \to U_{S,\mathbb{R}} \to 0
\end{aligned}$$

[1]Da $\mathbb{R}[G]$ halbeinfach ist, sind alle $\mathbb{R}[G]$-Moduln projektiv, demnach existieren diese Schnitte.

induziert werden. Die Dirichletsche Regulatorabbildung

$$\lambda_S : \begin{cases} U_S & \to & X_{S,\mathbb{R}} \\ u & \mapsto & -\sum_{v\in S} \log|u|_v \, v \end{cases}$$

induziert einen Isomorphismus $U_{S,\mathbb{R}} \cong X_{S,\mathbb{R}}$, den wir ebenfalls mit λ_S bezeichnen. Sei nun θ das Kompositum der Isomorphismen

$$\kappa_{\mathbb{R}} \oplus F^1_{\mathbb{R}} \overset{(\mathrm{id},s_1^{-1})}{\longrightarrow} \kappa_{\mathbb{R}} \oplus X_{S,\mathbb{R}} \oplus W_{\mathbb{R}} \overset{(\mathrm{id},\lambda_S,\mathrm{id})}{\longrightarrow} \kappa_{\mathbb{R}} \oplus U_{S,\mathbb{R}} \oplus W_{\mathbb{R}} \overset{(s_3,\mathrm{id})}{\longrightarrow} X(-2)_{\mathbb{R}} \oplus W_{\mathbb{R}} \overset{s_2}{\to} F^0_{\mathbb{R}},$$

dann ist $[\kappa\oplus F^1, \theta, F^0] \in K_0(\mathbb{Z}[G], \mathbb{R})$. Damit ist die algebraische Seite der Konstruktion abgeschlossen.
Sei $\mathrm{Irr}(G)$ die Menge der irreduziblen $\mathbb{C}$-wertigen Charaktere von G und $S(K)$ die Menge der Stellen von K unter den Stellen von S. Zu einem Charakter $\chi \in \mathrm{Irr}(G)$ definieren wir die reduzierte Artinsche L-Reihe

$$L_S(N/K, \chi, s) := \prod_{\mathfrak{p}\notin S(K)} \det\left(1 - \mathrm{Frob}_{\mathfrak{P}} N_{K/\mathbb{Q}}(\mathfrak{p})^{-1} | V^{I_{\mathfrak{P}}}\right)^{-1},$$

wobei $\mathfrak{P}$ jeweils eine gewählt Stelle über $\mathfrak{p}$ sei. Mit $L^*_S(N/K, \chi, 0)$ sei der führende Koeffizient in der Taylorreihenentwicklung um $s = 0$ von $L_S(N/K, \chi, s)$ bezeichnet. Wir setzen

$$\mathcal{L} := \left(L^*_S(N/K, \overline{\chi}, 0)\right)_{\chi\in\mathrm{Irr}(G)} \in \zeta(\mathbb{C}[G])^\times.$$

Nach [Bur01, Th. 2.1.2] liegt $\mathcal{L}$ bereits in der multiplikativen Gruppe des Zentrums von $\mathbb{R}[G]$. Sei nun $\hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}} : \zeta\left(\mathbb{R}[G]\right)^\times \to K_0(\mathbb{Z}[G], \mathbb{R})$ der Homomorphismus aus Abschnitt 1.2.6. Wir definieren

$$T\Omega(N/K, 0) := [\kappa \oplus F^1, \theta, F^0] - \hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}}(\mathcal{L}).$$

Nach [Bur01, Th. 2.1.2 (i)] bzw. [BF01, Lemma 5] hängt $T\Omega(N/K, 0)$ nur von der Erweiterung N/K ab.

Vermutung 2.1.1. *(1)* $T\Omega(N/K, 0) \in K_0(\mathbb{Z}[G], \mathbb{Q})$.

(2) $T\Omega(N/K, 0) = 0$ *in* $K_0(\mathbb{Z}[G], \mathbb{R})$.

Bemerkungen 2.1.2. *(1) Die Vermutung 2.1.1 (1) werden wir als Rationalitätsvermutung bezeichnen und die Vermutung 2.1.1 (2) bezeichnen wir kurz mit* $ETNC(0)$.

(2) *ETNC*(0) *ist die Tamagawazahlvermutung von Burns und Flach ([BF01, Conj. 4 (iii) u. (iv)]) für das Paar* $(h^0(\mathrm{Spec}(N)), \mathbb{Z}[G])$ *([Bur03, Th. 2.4.1]).*

(3) *In [Bur01] zeigt Burns folgende Zusammenhänge der Vermutung 2.1.1 zu anderen wichtigen Vermutungen der Zahlentheorie.*

   (a) *Die Rationalitätsvermutung ist äquivalent zur Stark-Vermutung bei* $s = 0$*, in der Formulierung von Tate in [Tat84, Ch. I, Conj. 5.1] ([Bur01, Th.2.2.4]).*

   (b) *Falls* $T\Omega(N/K, 0)$ *in* $K_0(\mathbb{Z}[G], \mathbb{Q})$ *gilt, so liegt* $T\Omega(N/K, 0)$ *genau dann in der Torsionsuntergruppe von* $K_0(\mathbb{Z}[G], \mathbb{Q})$*, wenn die „Strong-Stark-Conjecture“ in der Formulierung von Chinburg in [Chi83, Conj. 2.2] wahr ist ([Bur01, Th. 2.2.4]).*

   (c) *ETNC*(0) *ist genau dann wahr, wenn die geliftete Wurzelzahlvermutung von Gruenberg, Ritter und Weiss ([GRW99, S. 69]) wahr ist ([Bur01, Th. 2.3.3]).*

2.2 Forschungsstand

Für eine Primzahl p sei $T\Omega_p$ das Bild von $T\Omega$ in der p-ten Komponente unter der Isomorphie

$$K_0(\mathbb{Z}[G], \mathbb{Q}) \cong \bigoplus_q K_0(\mathbb{Z}_q[G], \mathbb{Q}_q).$$

Unter der Voraussetzung, dass die Rationalitätsvermutung gilt, gilt offensichtlich $T\Omega = 0 \Leftrightarrow T\Omega_p = 0$ für alle p. Für die äquivariante Tamagawazahlvermutung für Zahlkörper an der Stelle $s = 0$ ist bislang folgendes bekannt

(1) Für $N/\mathbb{Q}$ abelsch ist $T\Omega_p = 0$ für alle $p \neq 2$ bewiesen von Burns und Greither ([BG03]). Mit anderen Methoden wurde dies auch von Ritter und Weiss in [RW02] bewiesen. Schließlich zeigt Flach in [Fla04] $T\Omega_p = 0$ auch für $p = 2$.

(2) Für unendlich viele Quaternionenerweiterungen $N/\mathbb{Q}$ ist $T\Omega = 0$ von Burns und Flach in [BF01] bewiesen.

(3) Sei $K/\mathbb{Q}$ eine imaginär-quadratische Erweiterung und p eine Primzahl die in K zerfällt und die kein Teiler der Klassenzahl von K ist. Sei nun L/K eine abelsche Erweiterung. Bley beweist in [Ble06] $T\Omega_p = 0$ für diese p und das Paar $(h^0(\mathrm{Spec}(L)), \mathbb{Z}[\mathrm{Gal}(L/K)])$.

(4) Navilarekallu beweist in [Nav06] $T\Omega = 0$ für eine A_4-Erweiterung.

Zur Rationalitätsvermutung gibt es bislang folgende Resultate.

(1) Für $G = \{1\}$ ist dies die bekannte analytische Klassenzahlformel ([Tat84, Chap. I, 1.2 Cor.]).

(2) Formuliert man die Rationalitätsvermutung charakterweise (dies tun wir im Beweis zu Satz 3.3.5), dann gilt die Rationalitätsvermutung für Charaktere, die sich als Summen von induzierten trivialen Charakteren mit ganzen Koeffizienten schreiben lassen.

(3) Aus der Theorie der zyklotomischen Einheiten folgt die Rationalitätsvermutung für $N/\mathbb{Q}$ abelsch.

(4) Sei $K/\mathbb{Q}$ eine imaginär-quadratische Erweiterung. Ist N/K abelsch, dann zeigt man mit elliptischen Einheiten die Rationalitätsvermutung.

Die entscheidenden Argumente für die Aussagen (2) - (4) gibt Tate in seinem Buch [Tat84], allerdings formuliert er die Aussagen nicht als eigenständige Sätze. Im Satz 3.3.5 haben wir (2) und (3) detailiert bewiesen.

Kapitel 3

Algorithmische Umsetzung

Im ersten Abschnitt stellen wir einen Algorithmus vor, der einen Repräsentanten der lokalen Fundamentalklasse in der Ext-Gruppe berechnet. Für höchstens zahm verzweigte Erweiterungen sind wir dabei nach Ideen von Chinburg in [Chi85] vorgegangen, welche auf Arbeiten von Serre in [Ser] aufbauen. Für wild verzweigte Erweiterungen benutzen wir einen Algorithmus von Debeerst ([Deb11]), der ebenfalls auf den Arbeiten von Serre beruht.
Im zweiten Abschnitt stellen wir einen Algorithmus vor, der einen Repräsentanten f von Tates kanonischer Klasse (vgl. Definition 1.4.5) in $\mathrm{Ext}^2_G(X_S, U_S)$ berechnet. Sei $f \in \mathrm{Hom}_G(X(-2), U_S)$ und ist $\alpha_1, \ldots, \alpha_r$ ein Erzeugendensystem von X_S, dann müssen S-Einheiten $u_1, \ldots, u_r$ so bestimmt werden, dass die Zuordnung $\alpha_i \mapsto u_i$ die Abbildung f induziert, wobei die Einheiten noch gewissen lokalen Bedingungen genügen müssen. Diese Konstruktion geht auf Chinburg zurück ([Chi89]). Besondere Schwierigkeiten lagen dabei in den Punkten

(1) Wie garantiert man das f ein $\mathbb{Z}[G]$-Homomorphismus ist?

(2) Wie kodiert man die Bedingungen an die S-Einheiten in ein lineares Gleichungssystem.

Alle Fragen konnten zufriedenstellend beantwortet werden. (1) wird mit dem Algorithmus 3.4.11 gelöst. Dieser berechnet zu einem $\mathbb{Z}$-freien und endlich erzeugten $\mathbb{Z}[G]$-Modul A und einem endlich erzeugten $\mathbb{Z}[G]$-Modul B ein $\mathbb{Z}$-Erzeugendensystem von $\mathrm{Hom}_{\mathbb{Z}[G]}(A, B)$. Mit Hilfe dieses Algorithmus konnten wir einen bestehenden Algorithmus zur Berechnung von $\mathbb{Q}[G]$-linearen Schnitten (vgl. etwa [BB08, 4.2.4]) verallgemei-

nern. Der Algorithmus 3.4.12 berechnet zu einer kurzen exakten Sequenz

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

von $\mathbb{Z}[G]$-Moduln, in der C projektiv ist, einen $\mathbb{Z}[G]$-linearen Schnitt $s : C \to B$.

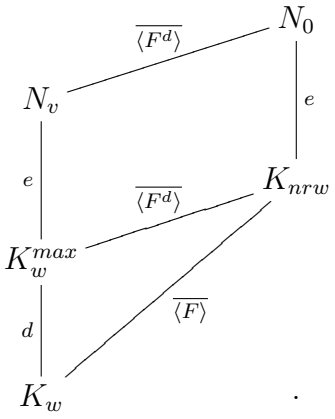
Im letzten Abschnitt zeigen wir dann, wie wir die Algorithmen von Bley und Wilson ([BW09]) zur numerischen Verifikation der Vermutung heranziehen und dass es unter gewissen Voraussetzungen an die Charaktere der Galoisgruppe der Erweiterung einen Algorithmus gibt, der die Vermutung beweist.

Die Namen der Algorithmen entsprechen den Namen in der Implementierung.

3.1 Die lokale Fundamentalklasse

Sei N/K eine endliche galoissche Zahlkörpererweiterung mit Galoisgruppe G, v sei eine endliche normierte Stelle bzw. Bewertung von N und w eine Stelle von K unter v. Die zugehörige lokale Erweiterung bezeichnen wir mit N_v/K_w und ihre Galoisgruppe mit G_v. Um die Idee von Chinburg zur Konstruktion von Tates kanonischer Klasse nutzen zu können (siehe nächsten Abschnitt), müssen wir die lokale Fundamentalklasse als Element in $\mathrm{Ext}^2_{G_v}(\mathbb{Z}, N_v^\times)$ berechnen. Dafür benutzen wir im wild verzweigten Fall Resultate von Serre in [Ser] und für höchstens zahm verzweigte Erweiterungen Resultate von Chinburg in [Chi85]. Zwar kann man die Ergebnisse von Serre auch auf höchstens zahm verzweigte Erweiterungen anwenden, aber vom algorithmischen Standpunkt aus ist für höchstens zahm verzweigte Erweiterungen die Methode von Chinburg für unsere Belange vorzuziehen. Sei K_w^{max} die maximal unverzweigte Teilerweiterung von N_v/K_w mit den Graden $e := [N_v : K_w^{max}]$ und $d := [K_w^{max} : K_w]$. Die maximal unverzweigte Erweiterung von K_w bezeichnen wir mit K_{nrw}. Es ist dann $N_0 := N_v K_{nrw}$ die maximal unverzweigte Erweiterung von N_v. Mit F bezeichnen wir den Frobeniusautomorphismus von K_{nrw}/K_w. Der Frobeniusautomorphismus auf K_{nrw}/K_w^{max} ist dann F^d. Seine Fortsetzung auf N_0/N_v bezeichnen wir ebenfalls mit F^d. Wir betrachten also folgende

Situation:



Definieren wir $N_{nrv} := K_{nrw} \otimes_{K_w} N_v$, dann wird N_{nrv} in natürlicher Weise zu einem $(\mathrm{Gal}(K_{nrw}/K_w) \times G_v)$-Modul. Das Element $F \times 1$ wirkt auf K_{nrw} wie der Frobeniusautomorphismus und trivial auf N_v. Für $\sigma \in G_v$ wirkt $1 \times \sigma$ trivial auf K_{nrw} und wie σ auf N_v. Für unsere Berechnungen ist die folgende Beschreibung des Moduls N_{nrv} günstiger.

$$\alpha \otimes \beta \mapsto (F^{d-1}(\alpha)\beta, F^{d-2}(\alpha)\beta, \ldots, F(\alpha)\beta, \alpha\beta)$$

induziert einen Isomorphismus von K_w-Algebren

$$K_{nrw} \otimes_{K_w} N_v \cong \bigoplus_{i=1}^{d} N_0.$$

Die $(\mathrm{Gal}(K_{nrw}/K_w) \times G_v)$-Wirkung auf $\bigoplus_{i=1}^{d} N_0$ ist wie folgt gegeben:
1.Fall: Wirkung von $(F^j \times \sigma)$ mit $F^j = \sigma$ auf K_w^{max}
Dann ist

$$(F^j \times \sigma)(x_1, \ldots, x_d) = (\tau(x_1), \ldots, \tau(x_d)),$$

wobei $\tau \in \mathrm{Gal}(N_0/K_w)$ ist mit $\tau|_{K_{nrw}} = F^j$ und $\tau|_{N_v} = \sigma$.
2.Fall: Wirkung von $(F \times 1)$
Es ist

$$(F \times 1)(x_1, \ldots, x_d) = (F^d(x_d), x_1, \ldots, x_{d-1}).$$

3.Fall: Wirkung von $(1 \times \sigma)$

Sei F^i eine Fortsetzung von $\sigma|_{K_w^{max}}$. Dann ist $(1 \times \sigma) = (F^{-i} \times 1)(F^i \times \sigma)$ und aus dem ersten Fall ergibt sich

$$(1 \times \sigma)(x_1, \ldots, x_d) = (F^{-i} \times 1)(\tau(x_1), \ldots, \tau(x_d))$$

mit $\tau|_{K_{nrw}} = F^i$ und $\tau|_{N_v} = \sigma$. Der Rest entspricht dann dem 2. Fall.

Sei nun α_v die lokale Fundamentalklasse in $\mathrm{Yext}^2_{G_v}(\mathbb{Z}, N_v^\times)$ und $\omega : N_{nrv}^\times \to \mathbb{Z}$, $(x_1, \ldots, x_d) \mapsto \sum_{i=1}^d v(x_i)$. Nach Serre [Ser, XIII, §2, Ex. 2] gilt: Die Sequenz

$$0 \longrightarrow N_v^\times \longrightarrow N_{nrv}^\times \xrightarrow{(F-1)\times 1} N_{nrv}^\times \xrightarrow{\omega} \mathbb{Z} \longrightarrow 0 \tag{3.1}$$

repräsentiert $-\alpha_v \in \mathrm{Yext}^2_{G_v}(\mathbb{Z}, N_v^\times)$. Führt man nun die Konstruktion im Beweis zu $\mathrm{Yext}^2_{G_v}(\mathbb{Z}, N_v^\times) \cong \mathrm{H}^2(G_v, N_v^\times)$ (vgl. 1.3.5) mit dem Startwert -1 durch, erhält man einen Kozykel, der die lokale Fundamentalklasse repräsentiert.
Es gibt ein kohomologisch triviales Gitter $X \subset N_v^\times$, so dass $N_v^\times/X$ endlich erzeugt ist ([BB08, 4.2.3]). Nach 1.3.3 gilt

$$\mathrm{H}^2(G_v, N_v^\times) \cong \mathrm{H}^2(G_v, N_v^\times/X).$$

Diese Tatsache ermöglicht erst die algorithmische Umsetzung. Ist die Erweiterung N_v/K_w höchstens zahm verzweigt, dann können wir $X = U_{N_v}^{(1)}$ wählen (vgl. [BB03, Prop. 4.3]), wobei $U_{N_v}^{(1)}$ die Einseinheiten von N_v bezeichnen. Für die Wahl eines geeigneten Gitters im wild verzweigten Fall verweisen wir auf [BB08, 4.2.1]. Einen Algorithmus zur Berechnung des Kozykels findet sich in der Arbeit von Debeerst [Deb11]. Dieser wurde auch in MAGMA implementiert. Der Algorithmus 3.4.13 berechnet dann zum Kozykel einen Repräsentanten in $\mathrm{Ext}^2_{G_v}(\mathbb{Z}, N_v^\times/X)$ unter dem Isomorphismus $\mathrm{H}^2(G_v, N_v^\times/X) \cong \mathrm{Ext}^2_{G_v}(\mathbb{Z}, N_v^\times/X)$. Expliziter bedeutet dies: Die Gruppe G_v werde erzeugt von den Elementen $g_1, \ldots, g_r$. Dann wird die exakte Sequenz [1]

$$0 \longrightarrow X_v(-2) \longrightarrow \mathbb{Z}[G_v]^r \xrightarrow{\delta} \mathbb{Z}[G_v] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

mit $\delta(x_1, \ldots, x_r) = \sum_{i=1}^r x_i(g_i - 1)$ und $\varepsilon(\sum_{g \in G_v} \lambda_g g) = \sum_{g \in G_v} \lambda_g$ berechnet, sowie eine Abbildung $f_v : X_v(-2) \to N_v^\times/X$, die die lokale Fundamentalklasse in $\mathrm{Ext}^2_{G_v}(\mathbb{Z}, N_v^\times/X)$ repräsentiert.

[1] Die Bezeichnung $X_v(-2)$ für den Kern von δ hat in dieser Arbeit keine besondere Bedeutung. Sie wurde lediglich von Chinburg ([Chi85]) übernommen.

Für höchstens zahm verzweigte Erweiterungen gibt Chinburg in [Chi85, VI] eine andere Möglichkeit an, um einen Repräsentanten der lokalen Fundamentalklasse in $\mathrm{Ext}^2_{G_v}(\mathbb{Z}, N_v^\times/U_{N_v}^{(1)})$ zu berechnen. Dabei benutzt er ebenfalls die Sequenz (3.1). Wir gehen im Folgenden näher auf diese Konstruktion ein.
Sei also N_v/K_w höchstens zahm verzweigt. Die Galoisgruppe G_v wird dann von zwei Elementen erzeugt. Als Erzeuger können wir einen Erzeuger von $\mathrm{Gal}(N_v/K_w^{max})$ wählen, den wir mit a bezeichnen und ein Element $b \in G_v$, welches in $\mathrm{Gal}(K_w^{max}/K_w)$ den geometrischen Frobeniusautomorphismus induziert[2] und von maximaler Ordnung ist. Zur Berechnung der Elemente in $\mathrm{Ext}^2_{G_v}(\mathbb{Z}, N_v^\times)$ benutzen wir die exakte Sequenz

$$0 \longrightarrow X_v(-2) \longrightarrow \mathbb{Z}[G_v]^2 \xrightarrow{\delta} \mathbb{Z}[G_v] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0 \tag{3.2}$$

mit ε als die Augmentation, also $\varepsilon(\sum_{g\in G_v} \lambda_g g) = \sum_{g\in G_v} \lambda_g$ und $\delta((x,y)) = x(a-1) + y(b-1)$, sowie $X_v(-2) := \ker(\delta)$. Wir definieren $N_v^{(1)} := N_v^\times/U_{N_v}^{(1)}$. Wie schon erwähnt induziert dann die Projektion $N_v^\times \to N_v^{(1)}$ einen Isomorphismus

$$h : \mathrm{Ext}^2_{G_v}\left(\mathbb{Z}, N_v^\times\right) \to \mathrm{Ext}^2_{G_v}\left(\mathbb{Z}, N_v^{(1)}\right).$$

Bezeichnen wir die lokale Fundamentalklasse in $\mathrm{Ext}^2_{G_v}(\mathbb{Z}, N_v^\times)$ mit α_{N_v/K_w}, dann genügt es demnach $h(\alpha_{N_v/K_w})$ zu berechnen. Chinburg gibt in [Chi85] eine Abbildung $f_3 : X_v(-2) \to N_v^{(1)}$ an, die $-h(\alpha_{N_v/K_w})$ repräsentiert, wenn wir $\mathrm{Ext}^2_{G_v}(\mathbb{Z}, N_v)$ bzgl. der Sequenz (3.2) berechnen. Bevor wir die Abbildung f_3 angeben, stellen wir zwei Lemmata voran, die wir zur Berechnung der Abbildung benötigen. Obwohl man den Beweis des ersten Lemmas in [Lor97, §25, F5] und den Beweis des zweiten Lemma in [Chi85, Lemma 6.4] finden kann, geben wir sie hier an, weil sie die Algorithmen zur Berechnung dieser Elemente liefern.

Lemma 3.1.1. *Es gibt ein Primelement $\Pi_0 \in N_v$ mit*

1) $N_v = K_w^{max}(\Pi_0)$

2) $\Pi_0^e \in K_w^{max}$.

Beweis. Sei Π bzw. π ein Primelement von N_v bzw. K_w^{max}. Dann gilt

$$\Pi^e = u\pi$$

[2] d.h. das Inverse des Frobeniusautomorphismus

mit einer Einheit $u \in N_v$. Sei nun q die Anzahl der Elemente des Restklassenkörpers $\overline{K_w^{max}}$ von K_w^{max}. Da die Erweiterung rein verzweigt ist, ist $\overline{K_w^{max}} = \overline{N_v}$ und die $(q-1)$-ten Einheitswurzeln von K_w^{max} bilden ein vollständiges Repräsentantensystem von $\overline{N_v}^{\times}$. Es gibt also eine $(q-1)$-te Einheitswurzel ζ von K_w^{max} und eine Einseinheit u_1 von N_v mit

$$u = \zeta u_1.$$

Aufgrund der zahmen Verzweigung hat das Polynom $f := X^e - u_1 \bmod \Pi$ eine einfache Nullstelle bei 1 mod Π. Ist nun c ein Lift dieser Nullstelle, dann gilt $u_1 = c^e$. Setzt man $\Pi_0 := c^{-1}\Pi$, so gilt

$$\Pi_0^e = u_1^{-1} u\pi = \zeta\pi \ \in K_w^{max}$$

und $N_v = K_w^{max}(\Pi_0)$. □

Damit ergibt sich für die Berechnung von Π_0 folgender Algorithmus.

Algorithmus 3.1.2. *(*`pGoodUniformizingElement`*)*

Input: *Eine rein und zahm verzweigte Erweiterung N_v/K_w^{max} vom Grad e.*

Output: *Ein Primelement $\Pi_0 \in N_v$ mit $N_v = K_w^{max}(\Pi_0)$ und $\Pi_0^e \in K_w^{max}$.*

(1) Berechne ein Primelement $\Pi \in N_v$. Ist $\Pi^e \in K_w^{max}$ dann gib Π aus.

(2) Berechne ein Primelement $\pi \in K_w^{max}$.

(3) Berechne die endliche Menge T der Einheitswurzeln von N_v (z.B. mit dem Algorithmus 4.9.9 in [Coh93]).

(4) Setze $u := \Pi^e/\pi$ und suche $t \in T$, so dass $u_1 := u/t$ eine Einseinheit ist.

(5) Berechne eine Nullstelle c von $X^e - u_1$ und gib $\Pi_0 := \Pi/c$ aus.

Lemma 3.1.3. *Seien a und b wie oben gewählt, d.h. a ist ein Erzeuger von $\mathrm{Gal}(N_v/K_w^{max})$ und b^{-1} induziert auf K_w^{max}/K_w den Frobeniusautomorphismus. Mit q sei die Anzahl der Elemente des Restklassenkörpers von K_w^{max} bezeichnet. Es gibt dann ein Primelement $\pi \in N_v$, so dass $u := \pi^{a-1}$ eine e-te primitive Einheitswurzel in N_v ist und eine Einheitswurzel $u_1 \in N_v$, mit zu q teilerfremder Ordnung, so dass $\pi^{b-1} \equiv u_1 \bmod U_{N_v}^{(1)}$ gilt.*
Insbesondere sind $u, u_1 \in K_w^{max}$.

Beweis. Nach Lemma 3.1.1 können wir ein $\pi \in N_v$ wählen mit $\pi^e \in K_w^{max}$ und $N_v = K_w^{max}(\pi)$. Dann ist $u := \pi^{a-1}$ eine e-te primitive Einheitswurzel. Wegen $v(\pi^{b-1}) = 1$, ist π^{b-1} eine Einheit. Bezeichnen wir mit $\mu(N_v)$ die Einheitswurzeln von N_v mit zu q teilerfremder Ordnung, dann ist $U_{N_v}/U_{N_v}^{(1)} \cong \mu(N_v)$. Es gibt also ein $u_1 \in \mu(N_v)$ mit $\pi^{b-1} \equiv u_1 \bmod U_{N_v}^{(1)}$.
Da die Ordnungen von u und u_1 teilerfremd zu q sind und die Erweiterung N_v/K_w^{max} rein verzweigt ist, sind $u, u_1 \in K_w^{max}$. □

Die algorithmische Berechnung von u ist mit dem Algorithmus 3.1.2 klar, wenn man einen Erzeuger a von $\mathrm{Gal}(N_v/K_w^{max})$ berechnet hat. In unserer Implementierung heißt der Algorithmus zur Berechnung von u `ComputeU`. Die Berechnung von u_1 erfolgt mit dem

Algorithmus 3.1.4. *(`ComputeU1`)*

Input: *Eine höchstens zahm verzweigte endliche Galoiserweiterung N_v/K_w lokaler Körper.*

Output: *Das Element u_1 aus dem Lemma 3.1.3.*

(1) Berechne die maximal unverzweigte Teilerweiterung K_w^{max}.

(2) Berechne mit dem Algorithmus 3.1.2 das Primelement π.

(3) Berechne die Einheitswurzeln T von N_v.

(4) Berechne einen Lift b vom geometrischen Frobeniusautomorphismus.

(5) Suche $t \in T$ mit $\pi^{b-1} \cdot t^{-1} \in U_{N_v}^{(1)}$.

(6) Setze $u_1 := t$ und gib u_1 aus.

Wir führen nun noch eine Reihe von Bezeichnungen und Abbildungen ein. Seien $U_{N_0}^{(1)}$ die Einseinheiten von N_0 und $N_{nrw}^{(1)} := \bigoplus_{i=1}^{d} N_0^{\times}/U_{N_0}^{(1)}$. Die Abbildung $\tau^{(1)} : N_v^{(1)} \to N_{nrw}^{(1)}$ sei die Diagonaleinbettung und $\omega^{(1)} : N_{nrw}^{(1)} \to \mathbb{Z}$ sei induziert von der Summe der Bewertungen, d.h. $(\overline{x_1}, \ldots, \overline{x_d}) \mapsto \sum_{i=1}^{d} v(x_i)$. Seien u und u_1 wie im Lemma 3.1.3 und γ bzw. γ_1 seien $(q^d - 1)$-te Wurzeln aus u bzw. u_1. Dann sind γ, γ_1 Einheitswurzeln in K_{nrw} und es gilt der

Satz 3.1.5. *Das Diagramm*

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & X_v(-2) & \longrightarrow & \mathbb{Z}[G_v]^2 & \xrightarrow{\delta} & \mathbb{Z}[G_v] & \xrightarrow{\varepsilon} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_1} & & \| & & \\ 1 & \longrightarrow & N_v^{(1)} & \xrightarrow{\tau^{(1)}} & N_{nrv}^{(1)} & \xrightarrow{(F-1)\times 1} & N_{nrv}^{(1)} & \xrightarrow{\omega^{(1)}} & \mathbb{Z} & \longrightarrow & 0 \end{array} \tag{3.3}$$

hat exakte Zeilen, ist kommutativ und f_3 repräsentiert $-h(\alpha_{N_v/K_w})$, wenn wir die vertikalen Abbildungen wie folgt wählen

$$\begin{aligned} f_1(1) &:= (\pi, 1, \ldots, 1), \\ f_2(1,0) &:= (\pi^b\gamma_1, \gamma_1, \ldots, \gamma_1), \\ f_2(0,1) &:= (\gamma, \ldots, \gamma), \\ f_3 &:= f_2|_{X(-2)}. \end{aligned}$$

Beweis. [Chi85, Lemma 6.3, Cor. 6.1] □

Die Elemente γ und γ_1 können natürlich in der unverzweigten Erweiterung vom Grad (q^d-1) von K_{nrw} berechnet werden, aber im Allgemeinen wird ein kleinerer Grad genügen. Das folgende Lemma gibt Auskunft darüber, wie wir den Grad der Erweiterung wählen müssen.

Lemma 3.1.6. *Sei u' eine primitive n-te Einheitswurzel in K_w^{max} und γ' eine Nullstelle von $X^{q^d-1}-u'$ in einem geeigneten Erweiterungskörper L von K_w^{max}. Sei weiter q die Anzahl der Element des Restklassenkörpers von K_w. Mit $m := \mathrm{ord}(q^d \bmod n(q^d-1))$ und L definiert als die unverzweigte Erweiterung von K_w^{max} vom Grad m gilt $\gamma' \in L$.*

Beweis. Wegen $u'^n = 1$ und $(\gamma')^{q^d-1} = u'$ ist γ' eine Nullstelle von $X^{n(q^d-1)}-1$. Wir nehmen an, dass γ' die maximal mögliche Ordnung hat, also $n(q^d-1)$. Die Behauptung folgt nun direkt aus

$$[K_w^{max}(\gamma') : K_w^{max}] = \mathrm{ord}(q^d \bmod n(q^d-1)) = m.$$

□

Sind m, m_1 zu γ und γ_1 bestimmt wie im Lemma, dann wählen wir die Erweiterung in der wir γ und γ_1 berechnen, als die unverzweigte Erweiterung von K_w^{max} vom Grad $\mathrm{kgV}(m, m_1)$. Die lokale Fundamentalklasse in $\mathrm{Ext}^2_{G_v}(\mathbb{Z}, N_v^\times)$ kann man also für höchstens zahm verzweigte Erweiterungen N_v/K_w mit folgendem Algorithmus berechnen.

Algorithmus 3.1.7.

Input: *Eine höchstens zahm verzweigte endliche Galoiserweiterung N_v/K_w lokaler Körper.*

Output: *Ein Repräsentant der lokalen Fundamentalklasse in* $\mathrm{Ext}^2_{G_v}(\mathbb{Z}, N_v^\times)$.

(1) Berechne mit dem Algorithmus 3.4.4[3] *die exakte Sequenz*

$$0 \longrightarrow X_v(-2) \longrightarrow \mathbb{Z}[G_v]^2 \longrightarrow \mathbb{Z}[G_v] \longrightarrow \mathbb{Z} \longrightarrow 0. \tag{3.4}$$

(2) Berechne die Elemente γ und γ_1.

(3) Berechne für ein Erzeugendensystem $\alpha_1, \ldots, \alpha_r$ von $X_v(-2)$ die Bilder $f_3(\alpha_i), i = 1, \ldots, r$.

(4) Gib die Abbildung f_3 und die Sequenz (3.4) aus.

Der Algorithmus ist in dieser Form noch nicht implementiert. Für die von uns getesteten A_4-Erweiterungen und zyklischen Erweiterungen haben wir Erzeuger des Moduls $X_v(-2)$, als $\mathbb{Z}$-Linearkombinationen von a und b, sowie die Bilder unter f_3, als $\mathbb{Z}[G]$-Linearkombinationen in π, γ und γ_1 per Hand berechnet und an die Programme übergeben. In Kapitel 4 sind diese Rechnungen ausgeführt.
Um den Rechenaufwand insgesamt zu verringern, was insbesondere noch kommende Rechnungen betrifft, sollte das Erzeugendensystem von $X_v(-2)$ klein sein. Einen naiven Algorithmus zur Berechnung eines $\mathbb{Z}[G_v]$-Erzeugendensystemes liefert der Algorithmus 3.4.7. Für die von uns getesteten Beispiele genügte diese naive Herangehensweise. Im Anhang von [Ble03] findet man einen Algorithmus von D. Kusnezow der auf nicht naivem Wege ein kleines Erzeugendensystem von $\mathbb{Z}[G_v]$-Gittern berechnet, wenn G_v abelsch ist.

3.2 Tates kanonische Klasse

3.2.1 Chinburgs Idee

Wir stellen hier Chinburgs Idee aus [Chi89] zur Konstruktion von Tates kanonischer Klasse vor, die wir algorithmisch umgesetzt haben.

[3] Dieser wird in Abschnitt 3.4 beschrieben.

Sei N/K eine galoissche Zahlkörpererweiterung mit Galoisgruppe G. Für eine Stelle w von N bezeichnen wir die Komplettierung nach w von N mit N_w. Sei S eine zulässige Stellenmenge für N/K (vgl. Def. 1.4.1). Wir stellen an die Erweiterung die folgende Voraussetzung:

„Es gibt ein $v_0 \in S$ mit $G_{v_0} = G$“.

Dies ist eine wirkliche Einschränkung an die Erweiterung bzw. Anwendbarkeit des Algorithmus. Zunächst einmal kommen nur noch Galoiserweiterungen N/K mit auflösbarer Galoisgruppe in Frage und nicht jede Galoiserweiterung muss diese Bedingung erfüllen. Leider können wir keine Aussage darüber treffen, wie dicht die Menge der Galoiserweiterungen mit dieser Eigenschaft und vorgegebener Galoisgruppe in der Menge aller Galoiserweiterungen zu gegebener Gruppe liegt.

Mit U_S bezeichnen wir die S-Einheiten von N und mit J_S die S-Idele (vgl. Def. 1.4.2). Sei S_0 ein Repräsentantensystem der G-Orbits der Stellen in S. Für $v \in S_0 \setminus \{v_0\}$ sei $S(v)$ ein Repräsentantensystem der G_v-Orbits in S mit $S_0 \subseteq S(v)$. Sei $w \in S(v)$. Wir betrachten folgende Situation

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \underline{X_v(-2)} & \longrightarrow & \underline{A_v} & \longrightarrow & \underline{B_v} & \longrightarrow & \mathbb{Z} \longrightarrow 0 \\ & & \downarrow{\scriptstyle \underline{f_v}} & & & & & & \\ & & U_S & & & & & & \\ & & \downarrow{\scriptstyle \pi_w} & & & & & & \\ & & N_w^\times/U_{N_w}^{(1)} & & & & & & \end{array} \qquad (*)$$

wobei die obere Zeile eine exakte Sequenz von $\mathbb{Z}[G_v]$-Moduln ist, in der $\underline{A_v}$ und $\underline{B_v}$ frei sind, $\underline{f_v}$ ein $\mathbb{Z}[G_v]$-Modulhomomorphismus ist und π_w von der natürlichen Inklusion $N \hookrightarrow N_w$ induziert sei. Chinburgs Idee besteht nun darin zu jedem $v \in S$ mit $v \neq v_0$ die Abbildung $\underline{f_v} \in \mathrm{Hom}_{\mathbb{Z}[G_v]}(\underline{X_v(-2)}, U_S)$ so zu konstruieren, dass für jedes $w \in S(v)$ die Abbildung $\pi_w \circ \underline{f_v}$ gewissen lokalen Bedingungen genügt. Induzieren wir nun die Sequenz und die Abbildung nach G, dann repräsentiert $\mathrm{Ind}_{G_v}^G(\underline{f_v})$ ein Element in $\mathrm{Ext}_G^2(\mathrm{Ind}_{G_v}^G(\mathbb{Z}), U_S)$. Zur Abkürzung setzen wir

$$Y_v := \mathrm{Ind}_{G_v}^G(\mathbb{Z}).$$

Bevor wir expliziter auf die Konstruktion eingehen, betrachten wir die injektive Abbildung

$$\begin{aligned} \iota : \mathrm{H}^2(G_v, U_S) \cong \mathrm{Ext}^2_G(Y_v, U_S) \hookrightarrow \mathrm{Ext}^2_G(Y_v, J_S) &\cong \mathrm{H}^2(G_v, J_S) \\ &\cong \bigoplus_{w \in S(v)} \mathrm{H}^2(G_v \cap G_w, N_w^\times). \end{aligned} \tag{3.5}$$

Erläuterungen

(1) Die Isomorphien $\mathrm{H}^2(G_v, U_S) \cong \mathrm{Ext}^2_G(Y_v, U_S)$ und $\mathrm{Ext}^2_G(Y_v, J_S) \cong \mathrm{H}^2(G_v, J_S)$ folgen aus dem

Lemma 3.2.1. *Mit den Bezeichnungen von oben gilt: Ist M ein G_v-Modul, dann ist*

$$\mathrm{Ext}^2_G(Y_v, M) \cong \mathrm{H}^2(G_v, U_S).$$

Beweis. Da Y_v ein $\mathbb{Z}$-freier Modul ist gilt zunächst nach [Bro94, Ch. III, Prop. (2.2)]

$$\mathrm{Ext}^2_G(Y_v, M) \cong \mathrm{H}^2(G, \mathrm{Hom}_{\mathbb{Z}}(Y_v, M)).$$

Sei nun $\{\sigma_1, \ldots, \sigma_n\}$ ein Repräsentantensystem der Rechtsnebenklassen von G/G_v. Dann ist $\mathrm{Ind}^G_{G_v}(M) = \bigoplus_{i=1}^n \sigma_i M$ und die Abbildung

$$\begin{cases} \bigoplus_{i=1}^n \sigma_i M & \to \quad \mathrm{Hom}_{\mathbb{Z}}(Y_v, M) \\ \sum_{i=1}^n \sigma_i m_i & \mapsto \begin{cases} Y_v & \to \quad M \\ \sum_{i=1}^n \sigma_i z_i & \mapsto \quad \sum_{i=1}^n \sigma_i z_i m_i \end{cases} \end{cases}$$

ist ein Isomorphismus von G-Moduln. Wenden wir jetzt noch Shapiros Lemma an [Neu69, Teil I, §4, Satz (4.19)], dann folgt die Behauptung. □

(2) Die Injektivität von $\mathrm{Ext}^2_G(Y_v, U_S) \hookrightarrow \mathrm{Ext}^2_G(Y_v, J_S)$ sieht man wie folgt ein. Nach (1) ist $\mathrm{Ext}^2_G(Y_v, U_S) \cong \mathrm{H}^2(G_v, U_S)$ und $\mathrm{Ext}^2_G(Y_v, J_S) \cong \mathrm{H}^2(G_v, J_S)$. Sei nun C die Idelklassengruppe und C_S die S-Idelklassengruppen. In Abschnitt 1.4 haben wir gesehen, dass $C \cong C_S$ gilt. Aus der exakten Sequenz

$$0 \longrightarrow U_S \longrightarrow J_S \longrightarrow C \longrightarrow 0$$

erhalten wir die unendliche exakte Sequenz

$$\ldots \to \mathrm{H}^1(G_v, J_S) \to \mathrm{H}^1(G_v, C) \to \mathrm{H}^2(G_v, U_S) \to \mathrm{H}^2(G_v, J_S) \to \mathrm{H}^2(G_v, C) \to \ldots$$

Da $\mathrm{H}^1(G_v, C)$ trivial ist, ist $\mathrm{H}^2(G_v, U_S) \to \mathrm{H}^2(G_v, J_S)$ injektiv und somit auch $\mathrm{Ext}^2_G(Y_v, U_S) \to \mathrm{Ext}^2_G(Y_v, J_S)$.

(3) Die letzte Isomorphie folgt aus [Neu69, Teil III, §3, Satz (3.2)] und Shapiros Lemma.

Sei nun

$$\mathrm{inv}(G_v \cap G_w, w) : \mathrm{H}^2(G_v \cap G_w, N_w^\times) \to \frac{1}{|G_v \cap G_w|}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$$

die Invariantenabbildung von $\mathrm{H}^2(G_v \cap G_w, N_w^\times)$ (vgl. Abschnitt 1.3.4). Nach [AT68, Ch.7, §3, Th.8] besteht das Bild der Abbildung ι aus allen $\beta \in \bigoplus_{w \in S(v)} \mathrm{H}^2(G_v \cap G_w, N_w^\times)$ mit

$$\sum_{w \in S(v)} \mathrm{inv}(G_v \cap G_w, w)(\beta) = 0 \text{ in } \mathbb{Q}/\mathbb{Z}. \tag{3.6}$$

Für eine Stelle $u \in S(v)$ bezeichnen wir mit ι_u das Kompositum

$$\mathrm{Ext}^2_G(Y_v, U_S) \to \bigoplus_{w \in S(v)} \mathrm{H}^2(G_v \cap G_w, N_w^\times) \to \mathrm{H}^2(G_v \cap G_u, N_u^\times).$$

Wir kommen nun zurück zur Konstruktion. Sei

$$0 \longrightarrow X_v(-2) \longrightarrow A_v \longrightarrow B_v \longrightarrow Y_v \longrightarrow 0 \tag{3.7}$$

die induzierte Sequenz (*) und $f_v \in \mathrm{Hom}_G(X_v(-2), U_S)$ ein Repräsentant der eindeutig bestimmten Klasse $\beta_v \in \mathrm{Ext}^2_G(Y_v, U_S)$ mit

$$\mathrm{inv}(G_v \cap G_w, w)(\iota_w(\beta_v)) = \begin{cases} \frac{1}{|G_v|} & \text{für } w = v, \\ -\frac{1}{|G_v|} & \text{für } w = v_0, \\ 0 & \text{sonst.} \end{cases}$$

Summieren wir die Sequenzen (3.7) über alle $v \in S_0 \setminus \{v_0\}$ und setzen $X(-2) := \bigoplus_{v \in S_0 \setminus \{v_0\}} X_v(-2)$, dann erhalten wir eine exakte Sequenz von G-Moduln

$$0 \longrightarrow X(-2) \longrightarrow \bigoplus_{v \in S_0 \setminus \{v_0\}} A_v \longrightarrow \bigoplus_{v \in S_0 \setminus \{v_0\}} B_v \longrightarrow \bigoplus_{v \in S_0 \setminus \{v_0\}} Y_v \longrightarrow 0.$$

Wir identifizieren die freie abelsche Gruppe $Y_S = \{\sum_{v\in S} \lambda_v v \mid \lambda_v \in \mathbb{Z}\}$ mit $\oplus_{v\in S_0} Y_v$ und Y_{v_0} mit $\mathbb{Z}v_0$. Der Kern der Augmentation $\varepsilon : Y_S \to \mathbb{Z}, \sum \lambda_v v \mapsto \sum \lambda_v$ ist dann X_S. Sei nun

$$\Delta : \bigoplus_{v\in S_0\setminus\{v_0\}} Y_v \to X_S$$

wie folgt definiert: Für $y \in Y_v$ und $v \in S_0 \setminus \{v_0\}$ sei $\Delta(y)$ dasjenige Element in Y_S, dessen Komponente bei v gerade y ist und bei v_0 gerade $-\varepsilon(y)v_0$ und sonst 0. Dann ist Δ ein Isomorphismus.
Mit $f := \bigoplus_{v\in S_0\setminus\{v_0\}} f_v$ erhalten wir das kommutative Diagramm von $\mathbb{Z}[G]$-Moduln

$$\begin{array}{ccccccccc}
0 & \longrightarrow & X(-2) & \xrightarrow{\iota} & \bigoplus_{v\in S_0\setminus\{v_0\}} A_v & \longrightarrow & \bigoplus_{v\in S_0\setminus\{v_0\}} B_v & \longrightarrow & X_S \longrightarrow 0 \\
 & & \downarrow{\scriptstyle f} & & \downarrow & & \| & & \| \\
1 & \longrightarrow & U_S & \longrightarrow & P & \longrightarrow & \bigoplus_{v\in S_0\setminus\{v_0\}} B_v & \longrightarrow & X_S \longrightarrow 0,
\end{array}$$

wobei P den Pushout von f und ι bezeichnet. Von großer Bedeutung ist der folgende

Satz 3.2.2. *Die Abbildung $f = \bigoplus_{v\in S_0\setminus\{v_0\}} f_v \in \mathrm{Hom}_G(X(-2), U_S)$ repräsentiert Tates kanonische Klasse in $\mathrm{Ext}^2_G(X_S, U_S)$.*

Beweis. [Chi89, III.2, Prop. 3.2.1] □

3.2.2 Ein Algorithmus zur Berechnung von Tates kanonischer Klasse

Der Algorithmus zur Berechnung von Tates kanonischer Klasse ist für den gesamten Algorithmus von zentraler Bedeutung.
Wir übernehmen die Bezeichnungen aus dem vorherigen Abschnitt.
Da es zunächst genügt die Abbildung $\underline{f_v}$ und die mit dieser Abbildung verbundene Sequenz zu berechnen, verzichten wir zur Vereinfachung im Folgenden auf die „unterstrichene“ Notation der beiden Moduln und der Abbildung. Wir gliedern die Beschreibung des Algorithmus in die folgenden Schritte:

Schritt 1: Berechnung der Stellenmenge S.

Schritt 2: Zu jedem $v \in S_0$ mit $v \neq v_0$ berechnen wir eine exakte Sequenz

$$0 \to X_v(-2) \to A_v \to B_v \to \mathbb{Z} \to 0 \tag{3.8}$$

von $\mathbb{Z}[G_v]$-Moduln und einen $\mathbb{Z}[G_v]$-Modulhomomorphismus $f_v : X_v(-2) \to U_S$ mit der Eigenschaft: Ist $S(v)$ ein Repräsentantensystem der G_v-Orbits der Stellen in S mit $S_0 \subseteq S$ und ist $w \in S(v)$ mit $w \neq v_0$, sowie

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X_w(-2) & \longrightarrow & A_w & \longrightarrow & B_w & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_w} & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & X_v(-2) & \longrightarrow & A_v & \longrightarrow & B_v & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \end{array} \tag{3.9}$$

ein kommutatives Diagramm von $G_v \cap G_w$-Moduln mit exakten Zeilen, dann repräsentiert $\pi_w \circ f_v \circ \varphi_w$ eine vorgegebene Klasse in $\mathrm{H}^2(G_v \cap G_w, N_w^\times) \cong \mathrm{Ext}^2_{G_v \cap G_w}(\mathbb{Z}, N_w^\times)$. Genauer soll gelten, dass für $w = v$ die Abbildung $\pi_v \circ f_v$ die lokale Fundamentalklasse in $\mathrm{H}^2(G_v, N_v^\times)$ repräsentiert und für $w \neq v$ repräsentiert $\pi_w \circ f_v \circ \varphi_w$ die triviale Klasse in $\mathrm{H}^2(G_v \cap G_w, N_w^\times)$. Wegen der Gleichheit (3.6) repräsentiert $\pi_{v_0} \circ f_v \circ \varphi_{v_0}$ dann automatisch das Inverse der lokalen Fundamentalklasse in $\mathrm{H}^2(G, N_{v_0}^\times)$.

Schritt 3: Berechnung der Sequenz

$$0 \longrightarrow X(-2) \longrightarrow \bigoplus_{v \in S_0 \setminus \{v_0\}} A_v \longrightarrow \bigoplus_{v \in S_0 \setminus \{v_0\}} B_v \longrightarrow X_S \longrightarrow 0$$

und der Abbildung $f = \bigoplus_{v \in S_0 \setminus \{v_0\}} f_v$.

Zu Schritt 1:

Wir gehen davon aus, dass die Erweiterung N/K durch ein primitives Element und dem Minimalpolynom dieses Elementes gegeben ist. Weiterhin gehen wir davon aus, dass die Galoisgruppe G der Erweiterung bereits berechnet ist[4] und die Erweiterung

[4]Die Berechnung der Galoisgruppe ist im Allgemeinen ein großes Problem. Der in Magma imple-

die Voraussetzung

„Es gibt eine Stelle v_0 mit $G_{v_0} = G$.“,

erfüllt. Dies lässt sich algorithmisch testen, denn ist die Galoisgruppe nicht abelsch (und uns interessieren nur diese Fälle) und ist v_0 unverzweigt, dann ist G_{v_0} zyklisch, also von G verschieden. Wir brauchen v_0 demnach nur unter den endlich vielen verzweigten Stellen suchen.
Die komplexen Nullstellen des Minimalpolynomes, und damit die unendlichen Stellen, lassen sich mit dem Algorithmus 3.6.6 in [Coh93] berechnen. Zur Berechnung der verzweigten Stellen verweisen wir auf den Algorithmus 4.8.21 in [Coh93] und Algorithmus 2.3.22 in [Coh00]. Ersterer berechnet die Differente eines Zahlkörpers und der zweite eine Primfaktorzerlegung der Differente. Um die Stellenmenge jetzt noch groß genug zu machen, kann man den Algorithmus 6.5.9 in [Coh93] zur Berechnung der Klassengruppe und den Algorithmus 7.4.6 in [Coh00] zur Berechnung der S-Klassengruppe heranziehen.

Zu Schritt 2:
Sei $v \in S_0$ und $S(v)$ ein Repräsentantensystem der G_v-Orbits mit $S_0 \subseteq S(v)$. Sei weiterhin

$$0 \longrightarrow X_v(-2) \longrightarrow A_v \longrightarrow B_v \longrightarrow \mathbb{Z} \longrightarrow 0,$$

die exakte Sequenz (3.8) von G_v-Moduln in der A_v und B_v frei seien. Ist G_v trivial, dann wählen wir als Sequenz

$$0 \to 0 \to 0 \to \mathbb{Z} \to \mathbb{Z} \to 0.$$

Der Modul $X_v(-2)$ werde über $\mathbb{Z}[G]$ erzeugt von den Elementen $\alpha_1, \ldots, \alpha_r$. Die Sequenz können wir mit dem Algorithmus 3.4.4 berechnen und die Erzeuger mit dem Algorithmus 3.4.5 bzw. 3.4.7. Sei weiterhin

$$U_S = \langle \varepsilon_1 \rangle \times \langle \varepsilon_2 \rangle \times \ldots \times \langle \varepsilon_s \rangle,$$

wobei ε_1 die Torsionsuntergruppe der Ordnung t erzeuge. Diese Zerlegung kann man mit dem Algorithmus 7.4.8 [Coh00] berechnen.

mentierte Algorithmus basiert auf den Methoden von R. Stauduhar [Sta73], die von J. Klüners und K. Geißler in [GK], [Gei03] erweitert wurden.

Wir wollen S-Einheiten $u_1, \ldots, u_r$ bestimmen, so dass

$$f_v : \begin{cases} X_v(-2) & \to \quad U_S \\ \sum_{i=1}^{r} \lambda_i \alpha_i & \mapsto \quad \prod_{i=1}^{r} u_i^{\lambda_i}, \quad \lambda_i \in \mathbb{Z}[G_v], \end{cases}$$

ein $\mathbb{Z}[G_v]$-Modulhomomorphismus ist und gewissen lokalen Vorgaben genügt. Wir machen den Ansatz

$$u_i = \prod_{j=1}^{s} \varepsilon_j^{x_j^{(i)}} \quad \text{mit } x_j^{(i)} \in \mathbb{Z}, i = 1, \ldots, r.$$

Wohldefiniertheit und damit $\mathbb{Z}[G_v]$-Linearität bekommen wir erfüllt, indem wir garantieren, dass aus $\sum_{i=1}^{r} \lambda_i \alpha_i = 0$ mit $\lambda_i \in \mathbb{Z}[G_v]$ immer auch $\prod_{i=1}^{r} u_i^{\lambda_i} = 1$ folgt. Wie man diese Bedingung in einer lineares Gleichungssystem umwandelt wird im Algorithmus 3.4.11 beschrieben und wir gehen hier nicht noch einmal darauf ein.
Wir beschränken uns hier auf den Fall, dass die Erweiterung N/K für alle $v \in S$ mit $v \neq v_0$ höchstens zahm verzweigt ist. Auf den wilden Fall gehen wir später kurz ein. Zu einer Stelle w bezeichnen wir das zugehörige Primideal mit $\mathfrak{P}_w$. Wie wir schon erwähnt haben, genügt es im höchstens zahm verzweigten Fall mod $1 + \mathfrak{P}_w$ zu rechnen. Wir haben der Allgemeinheit wegen alles mod $1 + \mathfrak{P}_w^{\eta}, \eta \in \mathbb{N}_{\geq 1}$, beschrieben.
Wir beschreiben jetzt in Abhängigkeit davon, ob v eine endliche oder unendliche Stelle ist, wie man zu einem linearen Gleichungssystem gelangt, dessen Lösungsmenge die gewünschten Potenzen der S-Einheiten liefert.

Der Fall: v ist eine endliche Stelle

Für $w \in S(v)$ unterscheiden wir die drei Fälle

1. w ist eine endliche Stelle mit $G_v \cap G_w = G_v$.
2. w ist eine endliche Stelle mit $G_v \cap G_w = H, H \neq G_v$.
3. w ist eine unendliche Stelle mit $G_v \cap G_w = C_2$.

Ist w eine Stelle mit $G_w = C_1$, dann ist nichts zu tun.
1. Fall
In diesem Fall sind die obere und untere Zeile in (3.9) identisch und damit $\varphi_w = \mathrm{id}$. Seien nun $\hat{c}_{w,1}, \ldots, \hat{c}_{w,r} \in N_w^{\times}$, so dass $\pi_w(f_v(\alpha_i)) = \hat{c}_{w,i}, i = 1, \ldots, r$ im Fall $w = v$ die lokale Fundamentalklasse in $\mathrm{Ext}^2_{G_v}(X_v(-2), N_v^{\times}/U_{N_v}^{(1)})$ repräsentiert und im Fall $w \neq v$

die triviale Klasse in $\mathrm{Ext}^2_{G_v}(X_v(-2), N_w^\times/U_{N_w}^{(1)})$ repräsentiert. Im ersten Fall berechnen wir die Elemente $\hat{c}_{w,1},\ldots,\hat{c}_{w,r}$ mit dem Algorithmus 3.1.7 und im zweiten Fall wählen wir $\hat{c}_{w,i}=1, i=1,\ldots,r$. Mit dieser festen Wahl der lokalen Elemente können wir nicht garantieren, dass unser Algorithmus immer eine Lösung berechnet, da wir uns auf einen Repräsentanten festgelegt haben. In unseren Beispielen, mit einer Ausnahme, hat der Algorithmus eine Lösung berechnet. Bei der Ausnahme war offensichtlich wie man die Werte $\hat{c}_{w,i}$ ändern musste. Der Algorithmus ist bislang auch nur in dieser Weise implementiert. Wir werden am Ende noch einmal auf dieses Problem eingehen und schildern, wie man vorgehen muss, damit der Algorithmus immer eine Lösung berechnet.
Abkürzend setzen wir $\hat{c}_i := \hat{c}_{w,i}, i=1,\ldots,r$. Seien $c_1,\ldots,c_r \in N$ mit

$$w(\hat{c}_i) = w(c_i) \quad \text{und} \quad w(\hat{c}_i - c_i) \geq n \text{ für ein } n \in \mathbb{N}_{\geq \eta}.$$

Die S-Einheiten $u_1,\ldots,u_r$ müssen dann der Bedingung

$$u_i \equiv c_i \bmod 1+\mathfrak{P}_w^\eta$$

genügen. Sei $(\mathcal{O}_N/\mathfrak{P}_w^\eta)^\times = \prod_{i=1}^d \langle\omega_i\rangle$ und $e_j = w(\varepsilon_j), e^{(i)} = w(c_i), j=1,\ldots,s, i=1,\ldots,r$, sowie $\pi \in N$ mit $w(\pi)=1$. Seien weiterhin $m_k^{(i)}, a_{kj} \in \mathbb{Z}, k=1,\ldots,d, i=1,\ldots,r$, so dass

$$\begin{aligned} c_i\pi^{-e^{(i)}} &\equiv \prod_{k=1}^d \omega_k^{m_k^{(i)}} \bmod \mathfrak{P}_w^\eta, \\ \varepsilon_j\pi^{-e_j} &\equiv \prod_{k=1}^d \omega_k^{a_{kj}} \bmod \mathfrak{P}_w^\eta. \end{aligned}$$

Die Zerlegung von $(\mathcal{O}_N/\mathfrak{P}_w^\eta)^\times$ kann man mit dem Algorithmus 4.2.17 aus [Coh00] berechnen und der Algorithmus 4.2.18 aus [Coh00] löst das diskrete Logarithmusproblem in $(\mathcal{O}_N/\mathfrak{P}_w^\eta)^\times$. Zu lösen ist dann das lineare Gleichungssystem

$$\sum_{j=1}^s a_{kj}x_j^{(i)} - \mathrm{ord}(\omega_k)y_k^{(i)} = m_k^{(i)}, \quad k=1,\ldots,d, i=1,\ldots,r, \tag{3.10}$$

$$\sum_{j=1}^s e_j x_j^{(i)} = e^{(i)}, \quad i=1,\ldots,r, \tag{3.11}$$

in den Unbestimmten $x_j^{(i)}, y_k^{(i)}, i=1,\ldots,r, k=1,\ldots,d, j=1,\ldots,s$, denn ist $(x_1^{(1)},\ldots,x_s^{(1)},x_1^{(2)},\ldots,x_s^{(2)},\ldots,x_1^{(r)},\ldots,x_s^{(r)},y_1^{(1)},\ldots,y_d^{(r)})$ eine Lösung, dann gilt mit

$$u_i = \prod_{j=1}^s \varepsilon_j^{x_j^{(i)}}$$

gerade

$$\begin{aligned} u_i\pi^{-e^{(i)}} &= \prod_{j=1}^{s} \varepsilon_j^{x_j^{(i)}} \pi^{-e^{(i)}} = \prod_{j=1}^{s} \left(\varepsilon_j \pi^{-e_j}\right)^{x_j^{(i)}} \\ &\equiv \prod_{j=1}^{s}\prod_{k=1}^{d} \omega_k^{a_{kj}x_j^{(i)}} \equiv \prod_{k=1}^{d} \omega_k^{\sum_{j=1}^{s} a_{kj}x_j^{(i)}} \equiv \prod_{k=1}^{d} \omega_k^{m_k^{(i)}} \equiv c_i\pi^{-e^{(i)}} \bmod \mathfrak{P}_w^{\eta}. \end{aligned}$$

Also gilt

$$u_i \equiv c_i \bmod 1 + \mathfrak{P}_w^{\eta}.$$

2. Fall

Sei

$$0 \longrightarrow X_w(-2) \longrightarrow A_w \longrightarrow B_w \longrightarrow \mathbb{Z} \longrightarrow 0,$$

die mit dem Algorithmus 3.4.4 berechnete exakte Sequenz von H-Moduln. Wie im Algorithmus 3.4.8 beschrieben berechnen wir Abbildungen φ und φ_w, so dass das Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X_w(-2) & \longrightarrow & A_w & \longrightarrow & B_w & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_w} & & \downarrow{\scriptstyle \varphi} & & \downarrow & & \| & & \\ 0 & \longrightarrow & X_v(-2) & \longrightarrow & A_v & \longrightarrow & B_v & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

kommutiert. Der Modul $X_w(-2)$ werde erzeugt von den Elementen $\beta_1, \ldots, \beta_m$. Um das Verwenden von noch mehr Indizes zu vermeiden, beschränken wir uns darauf, zu zeigen, was für einen gewählten Erzeuger β_k von $X_w(-2)$ zu tun ist. Sei

$$\varphi_w(\beta_k) = \sum_{i=1}^{r} \left(\sum_{g\in G} \lambda_g^{(i)} g \right) \alpha_i \quad \text{mit } \lambda_g^{(i)} \in \mathbb{Z}, i = 1, \ldots, r.$$

Die S-Einheiten $u_1, \ldots, u_s$ müssen dann der Bedingung

$$\prod_{i=1}^{r} \left(\prod_{g\in G} g(u_i)^{\lambda_g^{(i)}} \right) \equiv 1 \bmod 1 + \mathfrak{P}_w^{\eta}$$

genügen. Für alle $g \in G$ und $i = 1, \ldots, s$ berechnen wir ganze Zahlen $e_j(g,i), j = 1, \ldots, s$ mit

$$g(\varepsilon_i) = \prod_{j=1}^{s} \varepsilon_j^{e_j(g,i)}.$$

Sei $w(\varepsilon_j) = e_j$ und $(\mathcal{O}_N/\mathfrak{P}_w^{\eta})^{\times} = \prod_{n=1}^{d} \langle \omega_n \rangle$. Ist $\pi \in N$ mit $w(\pi) = 1$, dann bestimmen wir wie eben natürliche Zahlen $a_{nj}, n = 1, \ldots, d, j = 1, \ldots, s$ mit

$$\varepsilon_j \pi^{-e_j} \equiv \prod_{n=1}^{d} \omega_n^{a_{nj}} \bmod \mathfrak{P}_w^{\eta}.$$

Ist nun $(x_1^{(1)},\dots,x_s^{(1)},x_1^{(2)},\dots,x_s^{(2)},\dots,x_1^{(r)},\dots,x_s^{(r)},y_1,\dots,y_d)$ eine Lösung des linearen Gleichungssystemes

$$\sum_{j=1}^{s}\sum_{i=1}^{r}\left(\sum_{l=1}^{s}\sum_{g\in G}a_{nl}\lambda_g^{(i)}e_l(g,j)\right)x_j^{(i)}-\mathrm{ord}(\omega_n)y_n \;=\; 0,\quad n=1,\dots,d, \tag{3.12}$$

$$\sum_{j=1}^{s}\sum_{i=1}^{r}\left(\sum_{\iota=1}^{s}\sum_{g\in G}e_\iota\lambda_g^{(i)}e_\iota(g,j)\right)x_j^{(i)} \;=\; 0, \tag{3.13}$$

dann gilt

$$\begin{aligned}
\prod_{i=1}^{r}\prod_{g\in G}g(u_i)^{\lambda_g^{(i)}} &= \prod_{i=1}^{r}\prod_{g\in G}\prod_{j=1}^{s}g(\varepsilon_j)^{\lambda_g^{(i)}x_j^{(i)}}=\prod_{i=1}^{r}\prod_{g\in G}\prod_{j=1}^{s}\prod_{l=1}^{s}\varepsilon_l^{e_l(g,j)\lambda_g^{(i)}x_j^{(i)}}\\
&= \pi^0\prod_{l=1}^{s}\varepsilon_l^{\sum_{j=1}^{s}\sum_{i=1}^{r}x_j^{(i)}\sum_{g\in G}\lambda_g^{(i)}e_l(g,j)}\\
&= \pi^{-\sum_{\iota=1}^{s}e_\iota\left(\sum_{j=1}^{s}\sum_{i=1}^{r}x_j^{(i)}\sum_{g\in G}\lambda_g^{(i)}e_\iota(g,j)\right)}\cdot\prod_{l=1}^{s}\varepsilon_l^{\sum_{j=1}^{s}\sum_{i=1}^{r}x_j^{(i)}\sum_{g\in G}\lambda_g^{(i)}e_l(g,j)}\\
&= \prod_{l=1}^{s}\left(\varepsilon_l\pi^{-e_l}\right)^{\sum_{j=1}^{s}\sum_{i=1}^{r}x_j^{(i)}\sum_{g\in G}\lambda_g^{(i)}e_l(g,j)}\equiv\prod_{l=1}^{s}\prod_{n=1}^{d}\omega_n^{a_{nl}\sum_{j=1}^{s}\sum_{i=1}^{r}x_j^{(i)}\sum_{g\in G}\lambda_g^{(i)}e_l(g,j)}\\
&\equiv \prod_{n=1}^{d}\omega_n^{\sum_{l=1}^{s}a_{nl}\sum_{j=1}^{s}\sum_{i=1}^{r}x_j^{(i)}\sum_{g\in G}\lambda_g^{(i)}e_l(g,j)}\equiv\prod_{n=1}^{d}\omega_n^{0}\equiv 1 \bmod \mathfrak{P}_w^{\eta}.
\end{aligned}$$

Insgesamt gilt also

$$f_v\left(\varphi_w\left(\beta_k\right)\right)\equiv 1 \bmod 1+\mathfrak{P}_w^{\eta}.$$

3. Fall

Sei σ ein Erzeuger von C_2. Wie vorhin bestimmen wir eine Abbildung $\varphi:\mathbb{Z}[C_2]\to A_v$, so dass das Diagramm

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\sigma+1} & \mathbb{Z}[C_2] & \xrightarrow{\sigma-1} & \mathbb{Z}[C_2] & \longrightarrow & \mathbb{Z} & \longrightarrow & 0\\
 & & \downarrow{\scriptstyle\varphi_w} & & \downarrow{\scriptstyle\varphi} & & \downarrow & & \| & & \\
0 & \longrightarrow & X_v(-2) & \longrightarrow & A_v & \longrightarrow & B_v & \longrightarrow & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

kommutiert. Die Abbildung $f_v:X_v(-2)\to U_S$ bzw. die S-Einheiten $u_1,\dots,u_r$ müssen dann so bestimmt werden, dass $f_v(\varphi_w(1))$ die triviale Klasse in

$$\mathrm{Ext}^2_{C_2}(\mathbb{Z},N_w^{\times}/U_{N_w}^{(1)})\cong\mathrm{H}^2(C_2,\mathbb{C}^{\times})\cong\mathrm{H}^0(C_2,\mathbb{C}^{\times})=\left(\mathbb{C}^{\times}\right)^{C_2}/\mathrm{N}_{C_2}(\mathbb{C}^{\times})=\mathbb{R}^{\times}/\mathbb{R}_{>0}$$

repräsentiert. Für eine komplexe Zahl $z = x + iy$ bedeutet dabei $\mathrm{N}_{C_2}(z) = x^2 + y^2$. Wir gehen dabei folgendermaßen vor. Sei $x + A$ der affine Lösungsraum der S-Einheiten für die Bedingungen aus den endlichen Stellen. Sei nun $\varphi_w(1) = \sum_{i=1}^{r} \left(\sum_{g \in G} \lambda_g^{(i)} g \right) \alpha_i$ mit $\lambda_g^{(i)} \in \mathbb{Z}$, dann wenden wir salopp gesprochen, auf $x + A$ die entsprechende G-Wirkung an und bestimmen in diesem Raum ein Element, dass unter der Einbettung w größer als Null ist. Das machen wir jetzt expliziter.
Sei nun $x + \sum_{k=1}^{l} a_k x(k)$ mit $x = (x_1^{(1)}, \ldots, x_s^{(1)}, x_1^{(2)}, \ldots, x_s^{(r)})$, $x(k) = (x_1^{(1)}(k), \ldots, x_s^{(1)}(k), x_1^{(2)}(k), \ldots, x_s^{(r)}(k))$ und $a_k \in \mathbb{Z}$, der Lösungsraum von $x + A$, d.h. mit

$$u_i := \prod_{j=1}^{s} \varepsilon_j^{x_j^{(i)} + \sum_{k=1}^{l} a_k x_j^{(i)}(k)},$$

erfüllen $u_1, \ldots, u_r$ die Linearitätsbedingung und die Bedingungen aus den vorherigen Fällen. Sei $\varphi_w(1) = \sum_{i=1}^{r} \left(\sum_{g \in G} \lambda_g^{(i)} g \right) \alpha_i$, dann bestimmen wir zu $x, x(k), k = 1, \ldots, l$, Elemente $\overline{x} = (\overline{x_1^{(1)}}, \ldots, \overline{x_s^{(1)}}, \overline{x_1^{(2)}}, \ldots, \overline{x_s^{(r)}})$ und $\overline{x(k)} = (\overline{x_1^{(1)}(k)}, \ldots, \overline{x_s^{(1)}(k)}, \overline{x_1^{(2)}(k)}, \ldots, \overline{x_s^{(r)}(k)}), k = 1, \ldots, l$, so dass

$$\begin{aligned}
\prod_{g \in G} g \left(\prod_{j=1}^{s} \varepsilon_j^{x_j^{(i)}} \right)^{\lambda_g^{(i)}} &= \prod_{j=1}^{s} \varepsilon_j^{\overline{x_j^{(i)}}}, \quad i = 1, \ldots, r \quad \text{und} \\
\prod_{g \in G} g \left(\prod_{j=1}^{s} \varepsilon_j^{x_j^{(i)}(k)} \right)^{\lambda_g^{(i)}} &= \prod_{j=1}^{s} \varepsilon_j^{\overline{x_j^{(i)}(k)}}, \quad i = 1, \ldots, r, k = 1, \ldots, l,
\end{aligned}$$

gilt. Dies ist die Anwendung der G-Wirkung auf $x + A$. Dann ist

$$\prod_{g \in G} g(u_i)^{\lambda_g^{(i)}} = \prod_{g \in G} g \left(\prod_{j=1}^{s} \varepsilon_j^{x_j^{(i)} + \sum_{k=1}^{l} a_k x_j^{(i)}(k)} \right)^{\lambda_g^{(i)}} = \prod_{j=1}^{s} \varepsilon_j^{\overline{x_j^{(i)}} + \sum_{k=1}^{l} a_k \overline{x_j^{(i)}(k)}}$$

und somit

$$\begin{aligned}
f_v\left(\varphi_w(1)\right) &= \prod_{i=1}^{r} \prod_{g \in G} g(u_i)^{\lambda_g^{(i)}} = \prod_{i=1}^{r} \prod_{j=1}^{s} \varepsilon_j^{\overline{x_j^{(i)}} + \sum_{k=1}^{l} a_k \overline{x_j^{(i)}(k)}} \\
&= \prod_{j=1}^{s} \varepsilon_j^{\sum_{i=1}^{r} \overline{x_j^{(i)}} + \sum_{k=1}^{l} a_k \sum_{i=1}^{r} \overline{x_j^{(i)}(k)}} \\
&= \prod_{j=1}^{s} \varepsilon_j^{\sum_{i=1}^{r} \overline{x_j^{(i)}}} \cdot \prod_{k=1}^{l} \left(\prod_{j=1}^{s} \varepsilon_j^{\sum_{i=1}^{r} \overline{x_j^{(i)}(k)}} \right)^{a_k}.
\end{aligned}$$

Da $f_v \circ \varphi_w$ insbesondere ein C_2-Modulhomomorphismus ist, liegt $f_v(\varphi_w(1))$ im Fixkörper $F := N^{C_2}$ und damit ebenso die Elemente

$$\prod_{j=1}^{s} \varepsilon_j^{\sum_{i=1}^{r} \overline{x_j^{(i)}}} \text{ und } \prod_{j=1}^{s} \varepsilon_j^{\sum_{i=1}^{r} \overline{x_j^{(i)}(k)}},\ k = 1, \ldots, r.$$

Sei nun

$$\chi_F : \begin{cases} F & \to & \{0,1\} \\ x & \mapsto & \begin{cases} 1, & \text{falls } w(x) \leq 0, \\ 0, & \text{falls } w(x) > 0. \end{cases} \end{cases}$$

Wir unterscheiden zwei Fälle. Sei im ersten Fall $w\left(\prod_{j=1}^{s} \varepsilon_j^{\sum_{i=1}^{r} \overline{x_j^{(i)}}}\right) > 0$, dann muss $w\left(\prod_{k=1}^{l}\left(\prod_{j=1}^{s} \varepsilon_j^{\sum_{i=1}^{r} \overline{x_j^{(i)}(k)}}\right)^{a_k}\right) > 0$ gelten. Für jede Lösung $(a_1, \ldots, a_k, y)$ des linearen Gleichungssystems

$$\sum_{k=1}^{l} \chi_F\left(\prod_{j=1}^{s} \varepsilon_j^{\sum_{i=1}^{r} \overline{x_j^{(i)}(k)}}\right) a_k - 2y = 0$$

gilt die Ungleichung

$$w\left(\prod_{j=1}^{s} \varepsilon_j^{\sum_{i=1}^{r} \overline{x_j^{(i)}}} \cdot \prod_{k=1}^{l}\left(\prod_{j=1}^{s} \varepsilon_j^{\sum_{i=1}^{r} \overline{x_j^{(i)}(k)}}\right)^{a_k}\right) > 0.$$

Sei nun $w\left(\prod_{j=1}^{s} \varepsilon_j^{\sum_{i=1}^{r} \overline{x_j^{(i)}}}\right) < 0$. Dann gilt für jede Lösung $(a_1, \ldots, a_k, y)$ des linearen Gleichungssytemes

$$\sum_{k=1}^{l} \chi_F\left(\prod_{j=1}^{s} \varepsilon_j^{\sum_{i=1}^{r} \overline{x_j^{(i)}(k)}}\right) a_k - 2y = 1$$

die Ungleichung

$$w\left(\prod_{j=1}^{s} \varepsilon_j^{\sum_{i=1}^{r} \overline{x_j^{(i)}}} \cdot \prod_{k=1}^{l}\left(\prod_{j=1}^{s} \varepsilon_j^{\sum_{i=1}^{r} \overline{x_j^{(i)}(k)}}\right)^{a_k}\right) < 0.$$

Der Fall: v ist komplex unendlich

Sei $G_v = C_2 = \langle \sigma \rangle$. Wir wählen als Sequenz

$$0 \to \mathbb{Z} \overset{\sigma+1}{\to} \mathbb{Z}[C_2] \overset{\sigma-1}{\to} \mathbb{Z}[C_2] \overset{\varepsilon}{\to} \mathbb{Z} \to 0.$$

Da $\mathbb{Z}$ von einem Element erzeugt wird, muß nur eine S-Einheit u bestimmt werden, so dass $f_v : \mathbb{Z} \to U_S, 1 \mapsto u$ gewissen Bedingungen genügt. Für $w \in S(v)$ müssen wir die Einheit u so bestimmen, dass $\pi_v \circ f_v$ die lokale Fundamentalklasse in $\mathrm{Ext}^2_{C_2}(\mathbb{Z}, N_v^\times)$ repräsentiert und $\pi_w \circ f_v$ die triviale Klasse in $\mathrm{Ext}^2_{C_2}(\mathbb{Z}, N_w^\times)$. Notwendige und hinreichende Bedingung dafür, dass f_v ein $\mathbb{Z}[C_2]$-Modulhomomorphismus ist, ist $u \in F := N^{C_2}$. Wir bestimmen u also gleich in $U_{S,F}$. Sei dafür

$$U_{S,F} = \langle \delta_1 \rangle \times \ldots \times \langle \delta_m \rangle,$$

wobei δ_1 die Torsionsuntergruppe der Ordnung t_F erzeuge. Sei zunächst $w \in S(v)$ eine unendliche Stelle mit $G_w = G_v$. Die Einheit u muss den Bedingungen

$$v(u) < 0 \quad \text{und} \quad w(u) > 0$$

genügen. Wir machen wieder den Ansatz

$$u = \prod_{j=1}^{m} \delta_j^{x_j}$$

und definieren Abbildungen $\chi_{F,v}$ und $\chi_{F,w}$ analog zur Abbildung χ_F aus dem vorherigen Abschnitt. Das zu lösende lineare Gleichungssystem ist dann

$$\begin{aligned} \sum_{j=1}^{\nu} \chi_{F,v}(\delta_j) x_j - 2y &= 1 \\ \sum_{j=1}^{\nu} \chi_{F,w}(\delta_j) x_j - 2z &= 0 \end{aligned}$$

in den Unbestimmten $x_1, \ldots, x_\nu, y, z$.
Sei nun w eine endliche Stelle mit $G_w = G_v$. Die Einheit u muss die Bedingungen

$$v(u) < 0 \quad \text{und} \quad u \equiv 1 \bmod 1 + \mathfrak{P}_w^\eta,$$

erfüllen. Das zu lösende lineare Gleichungssystem erhalten wir für die erste Bedingung wie eben und für die zweite Bedingung wie im zuerst beschriebenen Fall mit $i = 1$ und $c_1 = 1$.

Zu Schritt 3:
Die induzierten Moduln kann man mit dem Algorithmus 3.4.9 berechnen. Die Abbildungen zu induzieren und die Sequenzen zu addieren ist einfache lineare Algebra. Sei

$$0 \longrightarrow X(-2) \longrightarrow \mathbb{Z}[G]^n \longrightarrow \mathbb{Z}[G]^m \longrightarrow Y \longrightarrow 0,$$

die so entstandene Sequenz.
Der Modul Y ist isomorph zu X_S und wird durch diesen ersetzt.

Wir zeigen nun, wie man den Algorithmus modifizieren muss, damit immer eine Lösung berechnet wird, falls es ein $v_0 \in G$ gibt mit $G_{v_0} = G$.
Sei die Erweiterung zunächst an allen Stellen $\neq v_0$ höchstens zahm verzweigt. Wir betrachten die Situation

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X_v(-2) & \xrightarrow{\tau} & A_v & \longrightarrow & B_v & \longrightarrow & \mathbb{Z} \longrightarrow 0 \\ & & \downarrow{\scriptstyle f_v} & \swarrow{\scriptstyle f} & & & & & \\ & & U_S & & & & & & \\ & & \downarrow{\scriptstyle \pi_w} & & & & & & \\ & & N_w^\times/U_{N_w}^{(1)}. & & & & & & \end{array}$$

Wir haben uns Elemente $\hat{c}_{w,i} \in N_w^\times, i = 1, \ldots, r$ vorgegeben, so dass $\pi_w \circ f_v$ eine vorgegebene Klasse in $\mathrm{Ext}^2_{G_v \cap G_w}(\mathbb{Z}, N_w^\times/U_{N_w}^{(1)})$ repräsentiert. Seien wie oben $\alpha_1, \ldots, \alpha_r$ Erzeuger von $X_v(-2)$, dann repräsentiert $(\pi_w \circ f_v) + (f \circ \tau)$ dieselbe Klasse. Dies haben wir bislang nicht berücksichtigt und holen es an dieser Stelle nach.
Die Grundidee ist dabei folgende. Bislang haben wir $Ax = b$ gelöst. Nun müssen wir $Ax \in b + B$ lösen.
Da der Modul A_v endlich erzeugt und frei ist und der Modul $N_w^\times/U_{N_w}^{(1)}$ endlich erzeugt, können wir mit dem Algorithmus 3.4.11 ein $\mathbb{Z}$-Erzeugendensystem von $\mathrm{Hom}_{\mathbb{Z}[G_v]}(A_v, N_w^\times/U_{N_w}^{(1)})$ bestimmen. Genauer gilt: Sei $v_1, \ldots, v_n$ ein „geliftetes“ Erzeugendensystem von $N_w^\times/U_{N_w}^{(1)}$ in $N^\times$ und $\sum_{l=1}^t a_l x(l)$ mit $x(l) = (x_1^{(1)}(l), \ldots, x_n^{(1)}(l), x_1^{(2)}(l), \ldots, x_n^{(r)}(l)), a_l \in \mathbb{Z}$, das $\mathbb{Z}$-Erzeugendensystem von $\mathrm{Hom}_{\mathbb{Z}[G_v]}(A_v, N_w^\times/U_{N_w}^{(1)})$, d.h. die Zuordnung $\alpha_i \mapsto \prod_{j=1}^n v_j^{\sum_{l=1}^t a_l x_j^{(i)}(l)}$, $i = 1, \ldots, r$ vermittelt einen $\mathbb{Z}[G_v]$-Homomorphismus von A_v nach $N^\times$. Haben wir bislang im Fall einer endlichen Stelle v und gleichen Zerlegungsgruppen von v und w für ein i die Kongruenz

$$u_i \equiv c_i \bmod 1 + \mathfrak{P}_w,$$

gelöst, so hätte man auch

$$u_i \equiv c_i \prod_{l=1}^t \left(\prod_{j=1}^n v_j^{x_j^{(i)}(l)} \right)^{a_l} \bmod 1 + \mathfrak{P}_w$$

lösen können. Wir erinnern kurz daran, welches Gleichungssystem im oberen Fall zu lösen war. Sei ω ein Erzeuger von $(U_N/\mathfrak{P}_w)^\times$ und $\pi \in N_w$ mit $w(\pi) = 1$. Sei weiterhin $\varepsilon_j \pi^{-w(\varepsilon_j)} \equiv \omega^{s_j}$ und $c_i \pi^{-w(c_i)} \equiv \omega^m$. Zu lösen war dann das lineare Gleichungssystem

$$\begin{aligned} \sum_{j=1}^{s} s_j x_j - \mathrm{ord}(\omega) y &= m, \\ \sum_{j=1}^{s} w(\varepsilon_j) x_j &= w(c_i). \end{aligned}$$

Sei nun $c_l := \prod_{j=1}^{n} v_j^{x_j^{(i)}(l)}$ und $c_l \pi^{-w(c_l)} = m_l$, dann gilt

$$c_i \prod_{l=1}^{t} c_l^{a_l} \pi^{-w(c_i c_1 \ldots c_t)} \equiv \omega^{m + \sum_{l=1}^{t} a_l m_l} \bmod \mathfrak{P}_w.$$

Zu lösen ist demnach das Gleichungssystem

$$\begin{aligned} \sum_{j=1}^{s} s_j x_j - \mathrm{ord}(\omega) y &= m + \sum_{l=1}^{t} a_l m_l, \\ \sum_{j=1}^{s} w(\varepsilon_j) x_j &= w(c_i) + \sum_{l=1}^{t} a_l w(c_l), \end{aligned}$$

in den Unbestimmten $x_j, j = 1, \ldots, s, a_l, l = 1, \ldots, t$, denn mit

$$u_i = \prod_{j=1}^{s} \varepsilon_j^{x_j}$$

gilt

$$\begin{aligned} u_i \pi^{-w(c_i) - \sum_{l=1}^{t} a_l w(c_l)} &= \prod_{j=1}^{s} \varepsilon_j^{x_j} \pi^{-w(c_i) - \sum_{l=1}^{t} a_l w(c_l)} = \prod_{j=1}^{s} \varepsilon_j^{x_j} \pi^{-\sum_{p=1}^{s} w(\varepsilon_p) x_p} \\ &= \prod_{j=1}^{s} \left(\varepsilon_j \pi^{-w(\varepsilon_j)} \right)^{x_j} \equiv \prod_{j=1}^{s} \omega^{s_j x_j} \equiv \omega^{\sum_{j=1}^{s} s_j x_j} \equiv \omega^{m + \sum_{l=1}^{t} a_l m_l} \\ &\equiv c_i \prod_{l=1}^{t} c_l^{a_l} \pi^{-w(c_i) - \sum_{l=1}^{t} a_l w(c_l)} \bmod \mathfrak{P}_w \end{aligned}$$

und somit

$$u_i \equiv c_i \prod_{l=1}^{t} c_l^{a_l} \bmod 1 + \mathfrak{P}_w.$$

Sind die Zerlegungsgruppen von v und w verschieden und sind beides endliche Stellen, dann ändert sich die rechte Seite des Gleichungssystemes (3.12) analog.

Für die unendlichen Stellen ist nichts weiter zu beachten, da die Bedingung $w(u) > 0$ notwendig und hinreichend ist.
Wir gehen jetzt noch kurz darauf ein, was zu tun ist, wenn w eine wild verzweigte Stelle ist. Wie schon erwähnt, gibt es dann einen kohomologisch trivialen Modul X_w, so dass es genügt die lokalen Elemente mod X_w zu bestimmen. Des Weiteren gibt es ein $\eta \in \mathbb{N}$ mit $U_{N_w}^{(\eta)} \subseteq X_w$ ([BB08, 4.2.3]). Also gilt $U_{N_w}/U_{N_w}^{(\eta)} \twoheadrightarrow U_{N_w}/X_w$. Nun ist

$$\begin{aligned} U_{N_w}/U_{N_w}^{(\eta)} &\overset{\iota}{\cong} (\mathcal{O}_N/\mathfrak{P}_w^{\eta})^{\times} \quad \text{und} \\ U_{N_w}/X_w &\cong \frac{U_{N_w}/U_{N_w}^{(\eta)}}{X_w/U_{N_w}^{(\eta)}} \cong \frac{(\mathcal{O}_N/\mathfrak{P}_w^{\eta})^{\times}}{\iota\left(X_w/U_{N_w}^{(\eta)}\right)}. \end{aligned}$$

Wie man den Modul X_w berechnet, wird in [Ble03, Rem. 3.6] beschrieben. Eine Zerlegung

$$\frac{(\mathcal{O}_N/\mathfrak{P}_w^{\eta})^{\times}}{\iota\left(X_w/U_{N_w}^{(\eta)}\right)} = \prod_{i=1}^{t} \langle \omega_i \rangle$$

kann dann mit den Algorithmen 4.2.17 (berechnet $\left(\mathcal{O}_N/\mathfrak{P}_w^{(\eta)}\right)^{\times}$), 4.1.18 (löst das diskrete Logarithmenproblem) und 4.1.7 (berechnet den Quotienten zweier Gruppen) aus [Coh00] berechnet werden.
Insgesamt haben wir bewiesen

Satz 3.2.3. *Ist N/K eine galoissche Zahlkörpererweiterung mit Galoisgruppe G und gibt es ein $v_0 \in G$ mit $G_{v_0} = G$, dann gibt es einen Algorithmus der einen Repräsentanten von Tates kanonischer Klasse berechnet.*

3.3 Ein Algorithmus zur numerischen Verifikation der Vermutung

Im letzten Abschnitt haben wir einen Algorithmus vorgestellt, der zu einer galoisschen Zahlkörpererweiterung N/K mit Galoisgruppe G einen Repräsentanten von Tates kanonischer Klasse berechnet, falls es ein $v_0 \in G$ gibt mit $G_{v_0} = G$.
In diesem Abschnitt erläutern wir, wie wir die Algorithmen von Bley und Wilson in [BW09] zur numerischen Verifikation von ETNC(0) heranziehen. Des Weiteren werden wir zeigen, dass es unter zusätzlichen Voraussetzungen an die Charaktere von G einen

Algorithmus gibt, der die Vermutung für jedes Fallbeispiel über $\mathbb{Q}$, welches die Voraussetzungen erfüllt, beweist. Dies ist der Hauptsatz des Abschnittes. Dieser ist bislang jedoch nicht implementiert.
Um die Algorithmen von Bley und Wilson anwenden zu können müssen wir uns zuerst mit der Rationalitätsvermutung beschäftigen. Bevor wir dies tun, erinnern wir an die Definition von $T\Omega$.
Mit dem Algorithmus aus dem letzten Abschnitt haben eine exakte Sequenz

$$0 \longrightarrow X(-2) \xrightarrow{\iota} F^0 \xrightarrow{\alpha} F^1 \xrightarrow{\beta} X_S \longrightarrow 0,$$

von $\mathbb{Z}[G]$-Moduln berechnet und eine Abbildung $f \in \mathrm{Hom}_G(X(-2), U_S)$ die Tates kanonische Klasse repräsentiert. Wir können ohne Einschränkung annehmen, dass die Abbildung f surjektiv ist, denn ist f nicht surjektiv, dann addieren wir zu den Moduln $X(-2)$ und F^0 einen genügend großen Modul $\mathbb{Z}[G]^l$. Wir setzen $\kappa := \ker(f)$ und erhalten das Diagramm

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & \kappa & = & \kappa & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & X(-2) & \xrightarrow{\iota} & F^0 & \xrightarrow{\alpha} & F^1 & \longrightarrow & X_S & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f} & & \downarrow & & \| & & \| & & \\
0 & \longrightarrow & U_S & \longrightarrow & P & \longrightarrow & F^1 & \longrightarrow & X_S & \longrightarrow & 0, \\
 & & \downarrow & & \downarrow & & & & & & \\
 & & 0 & & 0 & & & & & &
\end{array} \tag{3.14}$$

wobei P der Pushout von f mit ι ist. Dies ist gerade das Diagramm (2.2). Um dies einzusehen, müssen wir uns davon überzeugen, dass die Moduln F^0, F^1 und κ projektiv sind. Für die Moduln F^0 und F^1 ist dies klar, weil sie als freie Moduln konstruiert sind. Der Modul κ ist $\mathbb{Z}$-frei, da er Untermodul des $\mathbb{Z}$-freien Moduls $X(-2)$ ist. Wir betrachten nun die exakte Sequenz

$$0 \longrightarrow \kappa \longrightarrow F^0 \longrightarrow P \longrightarrow 0. \tag{3.15}$$

Da die untere Zeile im Diagramm Tates kanonische Klasse repräsentiert, ist der Modul P kohomologisch trivial. Der Modul F^0 ist als freier Modul ebenfalls kohomologisch

trivial. Aus der exakten Kohomologiesequenz zur Sequenz (3.15) folgt, dass auch κ kohomologisch trivial ist, also nach Bemerkung 1.3.3 projektiv.
Wir setzen $W := \ker(F^1 \to X_S)$. Seien $s_1 : X_{S,\mathbb{R}} \oplus W_{\mathbb{R}} \to F^1_{\mathbb{R}}$, $s_2 : X(-2)_{\mathbb{R}} \oplus W_{\mathbb{R}} \to F^0_{\mathbb{R}}$ und $s_3 : \kappa_{\mathbb{R}} \oplus U_{S,\mathbb{R}} \to X(-2)_{\mathbb{R}}$ Isomorphismen, die von Schnitten der exakten Sequenzen

$$\begin{aligned} 0 \to W_{\mathbb{R}} \to F^1_{\mathbb{R}} \to X_{S,\mathbb{R}} \to 0, \\ 0 \to X(-2)_{\mathbb{R}} \to F^0_{\mathbb{R}} \to W_{\mathbb{R}} \to 0 \quad \text{und} \\ 0 \to \kappa_{\mathbb{R}} \to X(-2)_{\mathbb{R}} \to U_{S,\mathbb{R}} \to 0 \end{aligned}$$

induziert werden. Sei weiter

$$\lambda_S : \begin{cases} U_{S,\mathbb{R}} & \to & X_{S,\mathbb{R}} \\ u & \mapsto & -\sum_{v \in S} \log(|u|_v) v, \end{cases}$$

der von der Dirichletschen Regulatorabbildung induzierte Isomorphismus und θ das Kompositum

$$\kappa_{\mathbb{R}} \oplus F^1_{\mathbb{R}} \xrightarrow{(\mathrm{id}, s_1^{-1})} \kappa_{\mathbb{R}} \oplus X_{S,\mathbb{R}} \oplus W_{\mathbb{R}} \xrightarrow{(\mathrm{id}, \lambda_S, \mathrm{id})} \kappa_{\mathbb{R}} \oplus U_{S,\mathbb{R}} \oplus W_{\mathbb{R}} \xrightarrow{(s_3, \mathrm{id})} X(-2)_{\mathbb{R}} \oplus W_{\mathbb{R}} \xrightarrow{s_2} F^0_{\mathbb{R}}.$$

Wir definieren $\mathcal{L} := (L^*_S(N/K, \overline{\chi}, 0))_{\chi \in \mathrm{Irr}(G)} \in \zeta(\mathbb{R}[G])^\times$, wobei $L^*_S(N/K, \overline{\chi}, 0)$ der führende Koeffizient in der Taylorreihenentwicklung der reduzierten Artinschen L-Reihe zum Charakter $\overline{\chi}$ sei (vgl. Abschnitt 1.1). Es war

$$T\Omega = [\kappa \oplus F^1, \theta, F^0] - \hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}}(\mathcal{L}),$$

wobei $\hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}}$ der Homomorphismus aus 1.2.6 ist.
Wie man die Schnitte und Isomorphismen berechnet, beschreiben wir im nächsten Abschnitt. Wir bemerken lediglich, dass die Abbildungen aus diesen Algorithmen durch Matrizen mit Einträgen in $\mathbb{Z}$ bzw. $\mathbb{Q}$ repräsentiert werden, mit Ausnahme der Matrix die durch die Regulatorabbildung induziert ist; diese hat Einträge in $\mathbb{R}$.
Wie schon erwähnt benutzen wir zur Verifikation von $T\Omega = 0$ die Algorithmen von Bley und Wilson in [BW09] mit denen man explizit in den Gruppen $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ rechnen kann. Damit wir sie anwenden können, muss $T\Omega$ die Rationalitätsvermutung erfüllen. Auf den folgenden Seiten werden wir zeigen, dass $T\Omega$ die Rationalitätsvermutung erfüllt ist, wenn gilt:

(1) $K = \mathbb{Q}$,

(2) jeder absolut irreduzible Charakter von G erfüllt eine der Bedingungen

(a) χ ist abelsch,

(b) $\chi(G) \subset \mathbb{Q}$ und χ ist ganzzahlige Linearkombination von irreduziblen trivialen Charakteren.

Darüber hinaus wird der Beweis zeigen, dass wir in diesem Fall exakt rechnen können und der Algorithmus einen Beweis für ETNC(0) liefert.
Wir zeigen nun, dass es zum Beweis der Rationalitätsvermutung genügt zu zeigen, dass gewisse Quotienten Einheiten im Zentrum von $\mathbb{Q}[G]$ sind.
Sei $A \in \mathrm{Gl}_d(\mathbb{R}[G])$ eine Koordinatenmatrix von θ bzgl. $\mathbb{R}[G]$-Basen. Wir erinnern an das Diagramm

$$\begin{array}{ccccccccc} & & & & \zeta(\mathbb{R}[G])^\times & & & & \\ & & & & \uparrow{\scriptstyle \mathrm{nr}_{\mathbb{R}[G]}} & \searrow^{\hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}}} & & & \\ K_1(\mathbb{Z}[G]) & \longrightarrow & K_1(\mathbb{R}[G]) & \xrightarrow{\partial^1_{\mathbb{Z}[G],\mathbb{R}}} & K_0(\mathbb{Z}[G],\mathbb{R}) & \longrightarrow & K_0(\mathbb{Z}[G]) & \longrightarrow & K_0(\mathbb{R}[G]), \end{array} \tag{3.16}$$

wobei $\partial^1_{\mathbb{Z}[G],\mathbb{R}}([\mathbb{R}[G]^n, \varphi]) = [\mathbb{Z}[G]^n, \varphi, \mathbb{Z}[G]^n]$ war und

$$\hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}} \circ \mathrm{nr}_{\mathbb{R}[G]} = \partial^1_{\mathbb{Z}[G],\mathbb{R}}$$

gilt.
In den nächsten beiden Lemmata wird sich zeigen, dass die Betrachtung des Quotienten

$$\mathrm{nr}_{\mathbb{R}[G]}(A)/\mathcal{L}$$

genügt.

Lemma 3.3.1. *Sei $\xi \in \zeta(\mathbb{R}[G])^\times$. Dann gilt*

$$\hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}}(\xi) \in K_0(\mathbb{Z}[G],\mathbb{Q}) \iff \xi \in \zeta(\mathbb{Q}[G])^\times.$$

Beweis. [Ble, Lemma 2.4] □

Satz 3.3.2. *Sei $(v_1 \otimes 1, \ldots, v_d \otimes 1)$ bzw. $(w_1 \otimes 1, \ldots, w_d \otimes 1)$ eine $\mathbb{Q}[G]$-Basis von $(\kappa \oplus F^1)_{\mathbb{Q}}$ bzw. $F^0_{\mathbb{Q}}$, wobei $v_i \in \kappa \oplus F^1, w_i \in F^0$ für $i = 1, \ldots, d$ gelte und sei $A \in \mathrm{Gl}_d(\mathbb{R}[G])$ die Koordinatenmatrix von θ bzgl. dieser Basen. Es gilt*

$$\mathrm{nr}_{\mathbb{R}[G]}(A)/\mathcal{L} \in \zeta(\mathbb{Q}[G])^\times \iff T\Omega \in K_0(\mathbb{Z}[G],\mathbb{Q}).$$

Beweis. Wir setzen $X := \mathbb{Z}[G]v_1 \oplus \ldots \oplus \mathbb{Z}[G]v_d$ und $Y := \mathbb{Z}[G]w_1 \oplus \ldots \oplus \mathbb{Z}[G]w_d$. Dann gilt

$$\begin{aligned}[X, A, Y] &- [\kappa \oplus F^1, \theta, F^0] \\ &= [\kappa \oplus F^1, A, F^0] - [\kappa \oplus F^1, \mathrm{id}, X] - [Y, \mathrm{id}, F^0] - [\kappa \oplus F^1, \theta, F^0] \\ &= [\kappa \oplus F^1, \theta^{-1} \circ A, \kappa \oplus F^1] - [\kappa \oplus F^1, \mathrm{id}, X] - [Y, \mathrm{id}, F^0] \in K_0(\mathbb{Z}[G], \mathbb{Q}).\end{aligned}$$

Damit gilt

$$\begin{aligned}T\Omega \in K_0(\mathbb{Z}[G], \mathbb{Q}) &\iff [X, A, Y] - \hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}}(\mathcal{L}) \in K_0(\mathbb{Z}[G], \mathbb{Q}) \\ &\iff \partial^1_{\mathbb{Z}[G],\mathbb{R}}([\mathbb{R}[G]^d, A]) - \hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}}(\mathcal{L}) \in K_0(\mathbb{Z}[G], \mathbb{Q}) \\ &\iff \hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}}(\mathrm{nr}_{\mathbb{R}[G]}(A)/\mathcal{L}) \in K_0(\mathbb{Z}[G], \mathbb{Q}) \\ &\iff \mathrm{nr}_{\mathbb{R}[G]}(A)/\mathcal{L} \in \zeta(\mathbb{Q}[G])^\times.\end{aligned}$$

□

Wir werden jetzt zeigen, dass unter den oben genannten Voraussetzungen an die Charaktere von G die Rationalitätsvermutung gilt, also $T\Omega \in K_0(\mathbb{Z}[G], \mathbb{Q})$ und wir in diesem Fall das Element $\mathrm{nr}_{\mathbb{R}[G]}(A)/\mathcal{L}$ exakt berechnen können. Bevor wir dazu kommen, erinnern wir an den Induktionssatz von Artin.

Satz 3.3.3. *Sei G eine endliche Gruppe und χ ein absolut irreduzibler Charakter von G mit $\chi(G) \subseteq \mathbb{Q}$. Für eine Untergruppe H von G sei 1_H der triviale Charakter auf H. Es gibt dann eine natürliche Zahl m und ganze Zahlen n_H mit*

$$m\chi = \sum_{H \leq G} n_H \mathrm{Ind}_H^G(1_H).$$

Beweis. [Tat84, Ch. II, Prop. 1.2] □

Um den Beweis des Hauptsatzes aus diesem Kapitel übersichtlicher zu halten, beweisen wir an dieser Stelle folgendes

Lemma 3.3.4. *Für eine Untergruppe H von G sei $e_H := \frac{1}{|H|} \sum_{h \in H} h$ und $F := N^H$. Die Stellenmenge von F unter den Stellen in S bezeichnen wir ebenfalls mit S und die S-Einheiten von F mit $U_{F,S}$. Es gilt*

(1) $e_H U_{S,\mathbb{C}} = U_{F,S,\mathbb{C}}$.

(2) $e_H X_{S,\mathbb{C}} \cong X_{F,S,\mathbb{C}}$.

Beweis. Zu *(1)*: Es gilt $U_S^H = U_{F,S}$ und mit $t_H := \sum_{h\in H} h$ gilt $\mathrm{H}^0(H, U_S) = U_S^H/t_H U_S$. Diese Gruppe ist nach [Neu69, Teil I, Satz (3.16)] endlich. Betrachten wir nun die exakte Sequenz

$$0 \to t_H U_S \to U_S^H \to U_S^H/t_H U_S \to 0,$$

und beachten, dass tensorieren mit $\mathbb{C}$ Exaktheit erhält, dann folgt die Behauptung.
Zu *(2)*: Der Isomorphismus ist induziert vom Isomorphismus

$$\begin{cases} e_H(Y_S \otimes \mathbb{C}) & \to & Y_{F,S} \otimes \mathbb{C} \\ e_H w & \mapsto & v_w, \end{cases}$$

wobei v_w die Stelle von F unter w bezeichnet. □

Kommen wir nun zum Herzstück des Abschnittes.

Satz 3.3.5. *Sei $K = \mathbb{Q}$ und $A \in \mathrm{Gl}_d(\mathbb{R}[G])$ ein Repräsentant der Abbildung θ^{-1}. Für jeden absolut irreduziblen Charakter χ von G gelte eine der beiden folgenden Eigenschaften:*

1. *$\chi(G) \subseteq \mathbb{Q}$ und der Induktionssatz von Artin gilt mit $m = 1$,*
2. *χ ist abelsch.*

Dann gilt

$$\mathrm{nr}_{\mathbb{R}[G]}(A)/\mathcal{L} \in \zeta(\mathbb{Q}[G])^\times$$

und dieser Quotient läßt sich exakt berechnen.

Beweis. Die Abbildung θ^{-1} war definiert als ein Kompositum von Isomorphismen

$$F_{\mathbb{R}}^0 \to X(-2)_{\mathbb{R}} \oplus W_{\mathbb{R}} \to \kappa_{\mathbb{R}} \oplus U_{S,\mathbb{R}} \oplus W_{\mathbb{R}} \to \kappa_{\mathbb{R}} \oplus X_{S,\mathbb{R}} \oplus W_{\mathbb{R}} \to \kappa_{\mathbb{R}} \oplus F_{\mathbb{R}}^1,$$

die von Schnitten und der Regulatorabbildung induziert waren. Da $\mathbb{R}[G]^d \cong F_{\mathbb{R}}^0 \cong \kappa_{\mathbb{R}} \oplus F_{\mathbb{R}}^1$ gilt, können wir ohne Einschränkung annehmen, dass die Matrix A bzgl. der kanonischen Basis die Abbildung θ^{-1} repräsentiert. Genauer: Sei $e_1, \ldots, e_d$ die kanonische Basis von $\mathbb{R}[G]^d$ und für $k = 1, \ldots, d$ sei $\theta^{-1}(e_k) = \sum_{l=1}^d \alpha_{kl} e_l$ mit $\alpha_{kl} \in \mathbb{R}[G]$. Für ein beliebiges Element $\sum_{k=1}^d x_k e_k$ in $\mathbb{R}[G]^d$ gilt dann

$$\theta^{-1}\left(\sum_{k=1}^d x_k e_k\right) = \sum_{k=1}^d x_k \sum_{l=1}^d \alpha_{kl} e_l = \sum_{l=1}^d \sum_{k=1}^d x_k \alpha_{kl} e_l.$$

Repräsentieren wir $\mathbb{R}[G]^d$ durch Zeilenvektoren, dann repräsentiert $A := (\alpha_{kl})_{1\leq k,l\leq d}$ die Abbildung θ^{-1} durch Multiplikation von rechts.
Wie wir im Abschnitt 1.2.5 gesehen haben, genügt es $\mathrm{Det}_\chi(A)$ für jeden Charakter $\chi \in \mathrm{Irr}(G)$ zu berechnen. Wir unterscheiden dabei 2 Fälle.
1. Fall:
Sei $\chi \in \mathrm{Irr}(G)$ mit $\chi(G) \subseteq \mathbb{Q}$ und

$$\chi = \sum_{H\leq G} n_H \mathrm{ind}_H^G(1_H) \quad \text{mit } n_H \in \mathbb{Z}.$$

Dann gilt

$$\begin{aligned} \mathrm{Det}_\chi(A) &= \prod_{H\leq G} \mathrm{Det}_{\mathrm{ind}_H^G(1_H)}(A)^{n_H} \quad \text{und} \\ L_S^*(N/\mathbb{Q}, \overline{\chi}, 0) &= \prod_{H\leq G} \zeta_{N^H,S}^*(0)^{n_H}, \end{aligned}$$

wobei ζ_{N^H} die Zetafunktion zum Zahlkörper N^H bezeichnet und die S- und $*$-Notation analog zu der bei $L_S^*(N/\mathbb{Q}, \overline{\chi}, 0)$ zu verstehen ist. Also gilt

$$\frac{\mathrm{Det}_\chi(A)}{L_S^*(N/\mathbb{Q}, \overline{\chi}, 0)} = \prod_{H\leq G} \left(\frac{\mathrm{Det}_{\mathrm{ind}_H^G(1_H)}(A)}{\zeta_{N^H,S}^*(0)} \right)^{n_H}.$$

Es genügt also für jede Untergruppe H den Quotienten

$$\frac{\mathrm{Det}_{\mathrm{ind}_H^G(1_H)}(A)}{\zeta_{N^H,S}^*(0)}$$

zu berechnen.
Für $H \leq G$ sei $e_H := \frac{1}{|H|}\sum_{h\in H} h$. Die Matrix A induziert einen $\mathbb{C}$-Vektorraumisomorphismus

$$e_H\mathbb{C}[G]^d \xrightarrow{\varphi} e_H\mathbb{C}[G]^d.$$

Wir werden jetzt zeigen, dass

$$\mathrm{Det}_{\mathrm{ind}_H^G(1_H)}(A) = \det_{\mathbb{C}}(\varphi) \tag{3.17}$$

gilt.
Es gilt

$$\mathrm{Det}_{\mathrm{ind}_H^G(1_H)}(A) = \det(T(\alpha_{kl}))_{1\leq k,l\leq d},$$

wobei $T : G \to \mathrm{Gl}_r(\mathbb{C})$ mit $r := |G/H|$ eine Darstellung zum Charakter $\mathrm{ind}_H^G(1_H)$ ist bzw. seine Fortsetzung auf $\mathbb{C}[G]$. Wir berechnen jetzt die Darstellung T. Nach Definition wird T von der regulären Darstellung auf H induziert. Sei also $G = \bigcup_{i=1}^{r} Hg_i$ eine disjunkte Zerlegung von G in Nebenklassen. Für jedes $g \in G$ definieren wir die Permutation

$$\pi_g : \left\{ \begin{array}{ccccc} \{1,\ldots,r\} & \to & \{1,\ldots,r\} & & \\ i & \mapsto & j, & \text{falls } Hg_ig = Hg_j. \end{array} \right.$$

Für jedes $g \in G$ ist dann

$$T(g) = (\varepsilon_{ij})_{1\le i,j\le r} \text{ mit } \varepsilon_{ij} = \left\{ \begin{array}{ll} 1, & \text{falls } \pi_g(i) = j \\ 0, & \text{sonst.} \end{array} \right.$$

Sei nun $\alpha_{kl} = \sum_{g\in G} a_{kl,g}g$, dann gilt $T(\alpha_{kl}) = \sum_{g\in G} a_{kl,g}T(g)$, also

$$T(\alpha_{kl}) = (\delta_{ij}^{(k,l)})_{1\le i,j\le r} \text{ mit } \delta_{ij}^{(k,l)} = \sum_{g\in G,\pi_g(i)=j} a_{kl,g} = \sum_{g\in g_i^{-1}Hg_j} a_{kl,g}.$$

Insgesamt erhalten wir

$$\mathrm{Det}_{\mathrm{ind}_H^G(1_H)}(A) = \det_{\mathbb{C}}\left(\left(\delta_{ij}^{(k,l)}\right)_{1\le i,j\le r}\right)_{1\le k,l\le d}.$$

Wir berechnen jetzt $\det_{\mathbb{C}}(\varphi)$ bzgl. der $\mathbb{C}$-Basis

$$e_Hg_1e_1,\ldots,e_Hg_re_1,\ldots,e_Hg_1e_d,\ldots,e_Hg_re_d.$$

Das Bild von $e_Hg_ie_k$ unter φ wird repräsentiert von $(0,\ldots,0,e_Hg_i,0,\ldots,0)A$, wobei der Eintrag e_Hg_i an k-ter Stelle steht. Wir rechnen

$$\begin{aligned} (0,\ldots,0,e_Hg_i,0,\ldots,0)A &= (e_Hg_i\alpha_{kl})_{1\le l\le d} = (e_Hg_i\sum_{g\in G} a_{kl,g}g)_{1\le l\le d} \\ &= (\sum_{g\in G} a_{kl,g}e_Hg_ig)_{1\le l\le d} = (\sum_{g\in G} a_{kl,g}e_Hg_{\pi_g(i)})_{1\le l\le d} \\ &= (\sum_{j=1}^{r}\sum_{g\in G,\pi_g(i)=j} a_{kl,g}e_Hg_j)_{1\le l\le d} \\ &= (\sum_{j=1}^{r}(\sum_{g\in g_i^{-1}Hg_j} a_{kl,g})e_Hg_j)_{1\le l\le d}. \end{aligned}$$

Damit erhalten wir

$$\begin{aligned}\varphi(e_H g_i e_k) &= \sum_{j=1}^{r}\Big(\sum_{g\in g_i^{-1}Hg_j} a_{k1,g}\Big)e_H g_j e_1 + \ldots + \sum_{j=1}^{r}\Big(\sum_{g\in g_i^{-1}Hg_j} a_{kd,g}\Big)e_H g_j e_d \\ &= \sum_{g\in g_i^{-1}Hg_1} a_{k1,g} e_H g_1 e_1 + \ldots + \sum_{g\in g_i^{-1}Hg_r} a_{k1,g} e_H g_r e_1 + \ldots \\ &\quad + \sum_{g\in g_i^{-1}Hg_1} a_{kd,g} e_H g_1 e_d + \ldots + \sum_{g\in g_i^{-1}Hg_r} a_{kd,g} e_H g_r e_d.\end{aligned}$$

Die Darstellungsmatrix von φ ist also gleich der Matrix $((\delta_{ij}^{(k,l)})_{1\le i,j\le r})_{1\le k,l\le d}$ und somit ist (3.17) gezeigt.
Es genügt also $\det_{\mathbb{C}}(\varphi)$ zu berechnen. Da φ das Kompositum von

$$\begin{aligned}(e_H\mathbb{C}[G])^d &\to e_H F^0_{\mathbb{C}} \to e_H X(-2)_{\mathbb{C}} \oplus e_H W_{\mathbb{C}} \to e_H\kappa_{\mathbb{C}} \oplus e_H U_{S,\mathbb{C}} \oplus e_H W_{\mathbb{C}} \\ &\to e_H\kappa_{\mathbb{C}} \oplus e_H X_{S,\mathbb{C}} \oplus e_H W_{\mathbb{C}} \to e_H\kappa_{\mathbb{C}} \oplus e_H F^1_{\mathbb{C}} \to (e_H\mathbb{C}[G])^d\end{aligned}$$

ist und bis auf die von der Dirichletschen Regulatorabbildung induzierte Abbildung

$$\lambda_H : e_H U_{S,\mathbb{C}} \to e_H X_{S,\mathbb{C}},$$

alle anderen Abbildungen über $\mathbb{Q}$ definiert sind, genügt es die Abbildung λ_H zu betrachten.
Wir setzen $F := K^H$. Die Stellenmenge von F bzw. $\mathbb{Q}$ unter den Stellen in S bezeichnen wir mit $S(F)$ bzw. $S(\mathbb{Q})$. In zweifelsfreien Fällen, wie zum Beispiel $U_{F,S(F),\mathbb{C}}$, verzichten wir auf die Nennung des Körpers bei der Stellenmenge und schreiben kurz S. Wir betrachten nun die von der Regulatorabbildung von F induzierte Abbildung

$$\lambda_F : U_{F,S,\mathbb{C}} \longrightarrow X_{F,S,\mathbb{C}}.$$

Mit Lemma 3.3.4 zeigen wir nun, dass es genügt die Determinante von λ_F zu berechnen. Dazu betrachten wir das nicht-kommutative Diagramm

$$\begin{array}{ccc} e_H U_{S,\mathbb{C}} & \xrightarrow{\lambda_H} & e_H X_{S,\mathbb{C}} \\ \downarrow{\scriptstyle \mathrm{id}} & & \uparrow{\scriptstyle \alpha} \\ U_{F,S,\mathbb{C}} & \xrightarrow{\lambda_F} & X_{F,S,\mathbb{C}}. \end{array}$$

Die Abbildung α ist dabei wie folgt definiert: Sei w eine Stelle von F und $v(w)$ eine Stelle von N über w, dann ist

$$\alpha(w) = e_H v(w).$$

Wir werden jetzt zeigen, dass

$$\lambda_H = [N:F]^{\dim_{\mathbb{C}}(U_{F,S,\mathbb{C}})}\ \alpha \circ \lambda_F$$

gilt. Sei $e_H u \in e_H U_{S,\mathbb{C}}$, dann ist

$$\lambda_H(e_H u) = -\sum_{v\in S} \log |e_H u|_v\, v \quad \text{und} \quad \alpha(\lambda_F(e_H u)) = -\sum_{w\in S(F)} \log |e_H u|_w\, e_H v(w).$$

Es gilt

$$\begin{aligned}\sum_{v\in S} \log |e_H u|_v\, v &= \sum_{v\in S} \log |e_H u|_v\, e_H v = \sum_{w\in S(F)} \left(\sum_{v|w} \log |e_H u|_v\right) e_H v(w)\\ &= \sum_{w\in S(F)} \left(\log\left(\prod_{v|w} |e_H u|_v\right)\right) e_H e(w)\end{aligned}$$

Wir müssen also nur den Unterschied zwischen $\log\left(\prod_{v|w} |e_H u|_v\right)$ und $\log |e_H u|_w$ bestimmen.
Zunächst nehmen wir an, dass w eine endliche Stelle über der Primzahl p ist. Mit $\mathfrak{P}_v$ bzw. $\mathfrak{p}_w$ bezeichnen wir das Primideal zu v bzw. w, mit $e_{N/F}$ den Verzweigungsindex und mit $f_{N/\mathbb{Q}}, f_{N/F}, f_{F/\mathbb{Q}}$ die entsprechenden Restklassengrade. Damit gilt

$$\begin{aligned}\log\left(\prod_{v|w} |e_H u|_v\right) &= \log\left(\prod_{v|w} \mathrm{N}_{N/\mathbb{Q}}\left(\mathfrak{P}_v\right)^{-v(e_H u)}\right) = \log\left(\prod_{v|w} p^{-f_{N/\mathbb{Q}} v(e_H u)}\right)\\ &= \log\left(\prod_{v|w} p^{-f_{N/F} f_{F/\mathbb{Q}} e_{N/F} w(e_H u)}\right) = \log\left(p^{-[N:F] f_{F/\mathbb{Q}} w(e_H u)}\right)\\ &= -[N:F] f_{F/\mathbb{Q}} w(e_H u) \log(p)\end{aligned}$$

und

$$\log |e_H u|_w = \log\left(\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p}_w)^{-w(e_H u)}\right) = \log\left(p^{-f_{F/\mathbb{Q}} w(e_H u)}\right) = -f_{F/\mathbb{Q}} w(e_H u) \log(p).$$

Für jede endliche Stelle w von F bekommen wir also den Faktor $[N:F]$.
Sei nun w eine unendliche Stelle. Sind w und v reelle Einbettungen, dann gilt

$$\log\left(\prod_{v|w} |e_H u|_v\right) = \log\left(\prod_{v|w} |v(e_H u)|\right) = \log\left(\prod_{v|w} |w(e_H u)|\right) = [N:F] \log |w(e_H u)|$$

und $\log|e_H u|_w = \log|w(e_H u)|$, d.h. auch in diesem Fall ist der Unterschied der Faktor $[N:F]$. Seien nun beides komplexe Einbettungen, dann gilt

$$\begin{aligned}\log\left(\prod_{v|w}|e_H u|_v\right) &= \log\left(\prod_{v|w}|v(e_H u)|^2\right) = \log\left(\prod_{v|w}|w(e_H u)|^2\right)\\ &= \log|w(e_H u)|^{2[N:F]} = 2[N:F]\log|w(e_H u)|,\end{aligned}$$

sowie $\log|e_H u|_w = 2\log|w(e_H u)|$. Im letzten Fall sei w eine reelle Einbettung und v eine komplexe Einbettung. Dann ist

$$\begin{aligned}\log\left(\prod_{v|w}|e_H u|_v\right) &= \log\left(\prod_{v|w}|v(e_H u)|^2\right) = \log\left(\prod_{v|w}|w(e_H u)|^2\right)\\ &= \log|w(e_H u)|^{[N:F]} = [N:F]\log|w(e_H u)|\end{aligned}$$

und $\log|e_H u|_w = \log|w(e_H u)|$.
In jedem dieser Fälle haben wir demnach den Faktor $[N:F]$ hinzubekommen. Insgesamt ergibt sich somit

$$\lambda_H = [N:F]^{\dim_{\mathbb{C}}(U_{F,S,\mathbb{C}})}\,\alpha\circ\lambda_F.$$

Sei nun $\xi_1,\ldots,\xi_r$ ein System von Fundamentaleinheiten von F, dann ist $\{\xi_i\otimes 1 \mid i=1,\ldots,r\}$ eine $\mathbb{C}$-Basis von $U_{F,S,\mathbb{C}}$. Sei $v_0\in S(F)$. Dann ist $\{(v-v_0)\otimes 1 \mid v\in S(F)\backslash\{v_0\}\}$ eine Basis von $X_{F,S,\mathbb{C}}$. Mit dieser Wahl gilt

$$\det_{\mathbb{C}}(\lambda_F) = \pm R_{F,S},$$

wobei $R_{F,S}$ den S-Regulator von F bezeichne (vgl. [Tat84, Ch.I, §2]). Sei nun e die Ordnung der Gruppe der Einheitswurzeln von F und h_S die S-Klassenzahl von F. Nach [Tat84, Ch.I, Cor. 2.2] gilt

$$\zeta^*_{F,S}(0) = -\frac{h_S\cdot R_{F,S}}{e}.$$

Damit haben wir gezeigt, dass bis auf einen rationalen Faktor, entstanden durch Basiswechsel und dem Übergang von λ_H zu λ_F, gilt

$$\frac{\mathrm{Det}_{\mathrm{ind}_H^G(1_H)}(A)}{\zeta^*_{F,S}(0)} = \pm\frac{e}{h_S}\in\mathbb{Q}.$$

2. Fall:
Sei nun χ abelsch, d.h. $\chi : G \to \mathbb{C}^\times$ ist ein Homomorphismus. Ohne Einschränkung sei χ nicht der triviale Charakter (das ist mit dem obigen Fall schon abgehandelt). Wir setzen $H := \ker(\chi), F := N^H$ und $e_\chi := \frac{1}{|G|}\sum_{g\in G}\chi(g^{-1})g$. Wie eben können wir uns auf die Berechnung der Determinante von

$$\lambda : e_\chi U_{S,\mathbb{C}} \to e_\chi X_{S,\mathbb{C}}$$

beschränken, denn alle anderen Abbildungen sind über $\mathbb{Q}(\chi) := \mathbb{Q}(\{\chi(g) \mid g \in G\})$ definiert. Wir wollen dies noch weiter einschränken. Sei dazu $\overline{g}$ die Restklasse von g in G/H. Es gilt

$$\begin{aligned} e_\chi &= \frac{1}{|G|}\sum_{g\in G}\chi(g^{-1})g = \frac{1}{|G|}\sum_{\overline{g}\in G/H}\sum_{h\in H}\chi((gh)^{-1})gh \\ &= \frac{1}{|G|}\sum_{\overline{g}\in G/H}\chi(g^{-1})g\sum_{h\in H}h. \end{aligned}$$

Mit $e_{\overline{\chi}} := \frac{1}{|G/H|}\sum_{\overline{g}\in G/H}\chi(g^{-1})g$ und $e_H := \frac{1}{|H|}\sum_{h\in H}h$ gilt also

$$e_\chi = e_{\overline{\chi}}\, e_H.$$

Mit Lemma 3.3.4 erhalten wir das nicht-kommutative Diagramm

$$\begin{array}{ccc} e_\chi U_{S,\mathbb{C}} = e_{\overline{\chi}}\, e_H U_{S,\mathbb{C}} & = & e_{\overline{\chi}} U_{F,S,\mathbb{C}} \\ \downarrow{\scriptstyle \lambda} & & \downarrow{\scriptstyle \lambda_F} \\ e_\chi X_{S,\mathbb{C}} = e_{\overline{\chi}}\, e_H X_{S,\mathbb{C}} & \cong & e_{\overline{\chi}} X_{F,S,\mathbb{C}}. \end{array}$$

Wie eben genügt es die Determinante von

$$\lambda_F : e_{\overline{\chi}} U_{F,S,\mathbb{C}} \to e_{\overline{\chi}} X_{F,S,\mathbb{C}}$$

zu berechnen, wobei λ_F wie im vorherigen Fall definiert ist.
Wir führen noch weitere Bezeichnungen ein. Für die endlichen Stellen einer Stellenmenge T schreiben wir T_f und für die unendlichen T_∞. Die Galoisgruppe von $F/\mathbb{Q}$ bezeichnen wir mit $\hat{G}$. Da $\hat{G} \cong G/H$ und $H = \ker(\chi)$ gilt, induziert χ einen Charakter auf $\hat{G}$. Diesen bezeichnen wir mit $\hat{\chi}$.

Zu $p \in S(\mathbb{Q})$ betrachten wir

$$\begin{array}{ccc} F & & w_p \\ | & & | \\ F^{G_{w_p}} & & v_p \\ | & & | \\ \mathbb{Q} & & p. \end{array}$$

Ist v_p eine endliche Stelle, dann sei $\mathfrak{p}_{v_p}$ das Primideal zu v_p. Wir wählen nun zu jedem $p \in S(\mathbb{Q})$ das kleinste $n_{w_p} \in \mathbb{N}$ mit der Eigenschaft:

$$\mathfrak{p}_{v_p}^{n_{w_p}} \quad \text{ist ein Hauptideal.}$$

Sei $\pi_{w_p} \in F^{G_{w_p}}$ ein Erzeuger dieses Hauptideales.
Wir bestimmen jetzt eine $\mathbb{C}$-Basis von $e_{\hat{\chi}} U_{F,S,\mathbb{C}}$. Sind $\varepsilon_1, \ldots, \varepsilon_{\#S_\infty(F)-1}$ Fundamentaleinheiten von F, dann ist

$$\{\varepsilon_1, \ldots, \varepsilon_{\#S_\infty(F)-1}\} \cup \{\pi_{w_p}^g \mid p \in S_f(\mathbb{Q}), \bar{g} \in \hat{G}/G_{w_p}\}$$

eine $\mathbb{Q}$-Basis von $U_{F,S,\mathbb{Q}}$. Wegen $e_{\hat{\chi}} \pi_{w_p}^g = \hat{\chi}(g) e_{\hat{\chi}} \pi_{w_p}$ ist $\{e_{\hat{\chi}} \pi_{w_p}^g, e_{\hat{\chi}} \pi_{w_p}\}$ linear abhängig über $\mathbb{C}$. Ein Erzeugendensystem von $e_{\hat{\chi}} U_{F,S_f,\mathbb{C}}$ ist also

$$\{e_{\hat{\chi}} \pi_{w_p} \mid p \in S_f(\mathbb{Q})\}.$$

Wir berechnen $e_{\hat{\chi}} \pi_{w_p}$. Es gilt

$$\begin{aligned} e_{\hat{\chi}} \pi_{w_p} &= \frac{1}{|\hat{G}|} \sum_{g \in \hat{G}} \hat{\chi}(g^{-1}) g \pi_{w_p} = \frac{1}{|\hat{G}|} \sum_{\bar{g} \in \hat{G}/G_{w_p}} \left(\sum_{h \in G_{w_p}} \hat{\chi}((gh)^{-1}) gh \pi_{w_p} \right) \\ &= \frac{1}{|\hat{G}|} \sum_{\bar{g} \in \hat{G}/G_{w_p}} \hat{\chi}(g^{-1}) \left(\sum_{h \in G_{w_p}} \hat{\chi}(h^{-1}) \right) g \pi_{w_p}. \end{aligned}$$

Für $\hat{\chi}|_{G_{w_p}} = 1$ ist $\sum_{h \in G_{w_p}} \hat{\chi}(h^{-1}) = |G_{w_p}|$ und für $\hat{\chi}|_{G_{w_p}} \neq 1$ folgt aus der Allgemeinen Orthogonalitätsrelation $\sum_{h \in G_{w_p}} \hat{\chi}(h^{-1}) = 0$. Es ist also

$$e_{\hat{\chi}} \pi_{w_p} = \begin{cases} \dfrac{1}{|\hat{G}|} \displaystyle\sum_{\bar{g} \in \hat{G}/G_{w_p}} |G_{w_p}| \hat{\chi}(g^{-1}) g \pi_{w_p} & , \text{falls } \hat{\chi}|_{G_{w_p}} = 1 \\ 0 & , \text{sonst.} \end{cases}$$

Aus der Existenz einer Minkowski Einheit ([Was97, Lemma 5.27]) schließen wir

$$\dim_{\mathbb{C}} e_\chi U_{S_\infty,F,\mathbb{C}} = \begin{cases} 1, & \text{falls } F \text{ total reell,} \\ 0 & \text{sonst.} \end{cases}$$

Dies zeigt:
Ist $F/\mathbb{Q}$ rein imaginär, dann ist

$$\{e_{\hat{\chi}}\pi_{w_p} \mid p \in S_f(\mathbb{Q}), \hat{\chi}|_{G_{w_p}} = 1\}$$

eine $\mathbb{C}$-Basis von $e_{\hat{\chi}}U_{F,S_f,\mathbb{C}} = e_{\hat{\chi}}U_{F,S,\mathbb{C}}$. Nun fehlt uns noch ein geeigneter Erzeuger von $e_{\hat{\chi}}U_{F,S_\infty(F),\mathbb{C}}$ für den Fall, dass $F/\mathbb{Q}$ total reell ist. Die Idee zur „richtigen“ Wahl des Erzeugers, holen wir uns aus der L-Reihe. Sei dazu $f(\hat{\chi})$ der Führer von $\hat{\chi}$ und ζ eine $f(\hat{\chi})$-te primitive Einheitswurzel. Mit H' bezeichnen wir die Galoisgruppe von $\mathbb{Q}(\zeta)/F$. Wir haben also die Situation:

$$\begin{array}{c} \mathbb{Q}(\zeta) \\ \Big| {\scriptstyle H'} \\ F \\ \Big| {\scriptstyle \hat{G}} \\ \mathbb{Q} \end{array}$$

Die Galoisgruppe der zyklotomischen Erweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ bezeichnen wir mit $\mathcal{G}$ und sehen $\hat{\chi}$ via Inflation als Charakter von $\mathcal{G}$ bzw. $(\mathbb{Z}/f(\hat{\chi})\mathbb{Z})^\times$.
Ist $F/\mathbb{Q}$ total reell, dann ist $\hat{\chi}(-1) = 1$ und nach [Was97, Th. 4.9] gilt

$$L^*(F/\mathbb{Q},\hat{\chi},1) = -\frac{\tau(\hat{\chi})}{f(\hat{\chi})}\sum_{a=1}^{f(\hat{\chi})}\overline{\hat{\chi}}(a)\log|1-\zeta^a|\,,$$

wobei $\tau(\hat{\chi}) := \sum_{a=1}^{f(\hat{\chi})}\hat{\chi}(a)\zeta^a$ eine Gauss-Summe. Unter Benutzung der Funktionalgleichung im ersten Schritt berechnen wir

$$\begin{aligned} L^*(F/\mathbb{Q},\hat{\chi},0) &= -\frac{1}{2}\sum_{a=1}^{f(\hat{\chi})}\hat{\chi}(a)\log|1-\zeta^a| = -\frac{1}{2}\sum_{g\in\mathcal{G}}\hat{\chi}(g)\log|1-\zeta^g| \\ &= -\frac{1}{2}\sum_{g\in\hat{G}}\hat{\chi}(g)\sum_{h\in H'}\overline{\hat{\chi}}(h)\log\left|1-\zeta^{gh}\right| = -\frac{1}{2}\sum_{g\in\hat{G}}\hat{\chi}(g)\sum_{h\in H'}\log\left|1-\zeta^{gh}\right| \\ &= -\frac{1}{2}\sum_{g\in\hat{G}}\hat{\chi}(g)\log\left|\left(\mathrm{N}_{\mathbb{Q}(\zeta)/F}(1-\zeta)\right)^g\right|. \end{aligned}$$

Wir setzen $\xi := \mathrm{N}_{\mathbb{Q}(\zeta)/F}(1-\zeta)$ und wählen als $\mathbb{C}$-Basis von $e_{\hat{\chi}}U_{F,S,\mathbb{C}}$ im Fall, dass $F/\mathbb{Q}$ total reell ist

$$\{e_{\hat{\chi}}\xi\} \cup \{e_{\hat{\chi}}\pi_{w_p} \mid p \in S_f(\mathbb{Q}), \hat{\chi}|_{G_{w_p}} = 1\}.$$

Wir berechnen jetzt die Bilder der Basisvektoren unter dem Regulator

$$\lambda_F : \begin{cases} e_{\hat{\chi}}U_{F,S,\mathbb{C}} & \to & e_{\hat{\chi}}X_{F,S,\mathbb{C}} \\ e_{\hat{\chi}}u & \mapsto & -e_{\hat{\chi}} \sum\limits_{w\in S(F)} \log|u|_w \, w \end{cases}$$

Sei w_∞ eine unendliche Stelle von F. Zu jeder Primzahl $q \in S_f(\mathbb{Q})$ wählen wir eine Stelle w_q von F über q und bezeichnen diese Menge von Stellen mit M. Es gilt

$$\begin{aligned} \lambda_F(e_{\hat{\chi}}\pi_{w_p}) &= -e_{\hat{\chi}} \sum_{z\in S(F)} \log\left|\pi_{w_p}\right|_z z = -e_{\hat{\chi}} \sum_{z\in S_\infty(F)} \log\left|\pi_{w_p}\right|_z z - e_{\hat{\chi}} \sum_{z\in S_f(F)} \log\left|\pi_{w_p}\right|_z z \\ &= -\delta \sum_{g\in\hat{G}} \log\left|\pi_{w_p}\right|_{gw_\infty} e_{\hat{\chi}} g w_\infty - \sum_{w_q\in M} \sum_{\bar{g}\in\hat{G}/G_{w_q}} \log\left|\pi_{w_p}\right|_{gw_q} e_{\hat{\chi}} g w_q, \end{aligned}$$

wobei

$$\delta = \begin{cases} 1 & \text{,falls } F/\mathbb{Q} \text{ total reell,} \\ 0 & \text{,falls } F/\mathbb{Q} \text{ rein imaginär.} \end{cases}$$

Da $\log\left|\pi_{w_p}\right|_{gw_q} = 0$ für $p \neq q$ und $\log\left|\pi_{w_p}\right|_{gw_p} = 0$ für $g \neq \mathrm{id}$, ist

$$\lambda_F(e_{\hat{\chi}}) = -\delta \sum_{g\in\hat{G}} \log\left|\pi_{w_p}\right|_{gw_\infty} e_{\hat{\chi}} g w_\infty - \log\left|\pi_{w_p}\right|_{w_p} e_{\hat{\chi}} w_p.$$

Sei nun $\mathfrak{P}_{w_p}$ das Primideal zu w_p, $f_{F/\mathbb{Q}}(w_p)$ der Restklassengrad und $e_{F/\mathbb{Q}}(w_p)$ der Verzweigungsindex. Wir erinnern daran, dass $(\pi_{w_p}) = \mathfrak{p}_{v_p}^{n_{w_p}}$ war, wobei $\mathfrak{p}_{v_p}$ das Primideal von $F^{G_{w_p}}$ unter $\mathfrak{P}_{w_p}$ ist. Damit ist

$$\begin{aligned} \lambda_F(e_{\hat{\chi}}\pi_{w_p}) &= -\delta \sum_{g\in\hat{G}} \log\left|\pi_{w_p}\right|_{gw_\infty} e_{\hat{\chi}} g w_\infty - \log\left(\mathrm{N}_{F/\mathbb{Q}}\left(\mathfrak{P}_{w_p}\right)^{-w_p(\pi_{w_p})}\right) e_{\hat{\chi}} w_p \\ &= -\delta \sum_{g\in\hat{G}} \log\left|\pi_{w_p}\right|_{gw_\infty} e_{\hat{\chi}} g w_\infty - \log\left(p^{-f_{F/\mathbb{Q}}(w_p) w_p(\pi_{w_p})}\right) e_{\hat{\chi}} w_p \\ &= -\delta \sum_{g\in\hat{G}} \log\left|\pi_{w_p}\right|_{gw_\infty} e_{\hat{\chi}} g w_\infty - \log\left(p^{-\frac{f_{F/\mathbb{Q}}(w_p)}{e_{F/\mathbb{Q}}(w_p)} v_p(\pi_{w_p})}\right) e_{\hat{\chi}} w_p \\ &= -\delta \sum_{g\in\hat{G}} \log\left|\pi_{w_p}\right|_{gw_\infty} e_{\hat{\chi}} g w_\infty - \log\left(p^{-\frac{f_{F/\mathbb{Q}}(w_p)}{e_{F/\mathbb{Q}}(w_p)} n_{w_p}}\right) e_{\hat{\chi}} w_p \\ &= -\delta \sum_{g\in\hat{G}} \log\left|\pi_{w_p}\right|_{gw_\infty} e_{\hat{\chi}} g w_\infty + \frac{f_{F/\mathbb{Q}}(w_p)}{e_{F/\mathbb{Q}}(w_p)} n_{w_p} \log(p)\, e_{\hat{\chi}} w_p. \end{aligned}$$

Für $F/\mathbb{Q}$ total reell berechnen wir jetzt noch das Bild von $e_{\hat{\chi}}\xi$. Es ist

$$\begin{aligned}\lambda_F(e_{\hat{\chi}}\xi) &= -e_{\hat{\chi}} \sum_{z\in S(F)} \log|\xi|_z \, z = -e_{\hat{\chi}} \sum_{z\in S_\infty(F)} \log|\xi|_z \, z = -\sum_{g\in\hat{G}} \log|\xi|_{gw_\infty} \, e_{\hat{\chi}} g w_\infty \\ &= -\sum_{g\in\hat{G}} \log\left|\xi^{g^{-1}}\right|_{w_\infty} \hat{\chi}(g) e_{\hat{\chi}} w_\infty.\end{aligned}$$

Als $\mathbb{C}$-Basis von $e_{\hat{\chi}} X_{F,S,\mathbb{C}}$ wählen wir

$$\begin{cases} \{e_{\hat{\chi}} w_\infty\} \cup \{e_{\hat{\chi}} \pi_{w_p} \mid p \in S_f(\mathbb{Q}) \text{ mit } \hat{\chi}|_{G_{w_p}} = 1\} & \text{, falls } F/\mathbb{Q} \text{ total reell ist,} \\ \{e_{\hat{\chi}} \pi_{w_p} \mid p \in S_f(\mathbb{Q}) \text{ mit } \hat{\chi}|_{G_{w_p}} = 1\} & \text{, falls } F/\mathbb{Q} \text{ rein imaginär ist.} \end{cases}$$

Die Darstellungsmatrix von λ_F bzgl. der gewählten Basen ist also (im Fall $F/\mathbb{Q}$ rein imaginär ist die erste Zeile und Spalte zu streichen)

$$\begin{pmatrix} -\sum_{g\in\hat{G}} \log\left|\xi^{g^{-1}}\right|_{w_\infty} \hat{\chi}(g) & 0 & \dots & 0 \\ -\sum_{g\in\hat{G}} \log\left|\pi_{w_p}\right|_{gw_\infty} \hat{\chi}(g) & \frac{n_{w_p} f_{F/\mathbb{Q}}(w_p)\log(p)}{e_{F/\mathbb{Q}}(w_p)} & 0 & \vdots \\ \vdots & 0 & \ddots & \vdots \\ -\sum_{g\in\hat{G}} \log\left|\pi_{w_p}\right|_{gw_\infty} \hat{\chi}(g) & 0 & 0 & \frac{n_{w_p} f_{F/\mathbb{Q}}(w_p)\log(p)}{e_{F/\mathbb{Q}}(w_p)} \end{pmatrix}.$$

Hierbei werden bei den endlichen Stellen zeilenweise die $p \in S_f(\mathbb{Q})$ mit $\hat{\chi}|_{G_{w_p}} = 1$ durchlaufen. Damit ergibt sich

$$\mathrm{Det}_{\hat{\chi}}(\lambda_F) = \begin{cases} -\sum_{g\in\hat{G}} \log\left|\xi^{g^{-1}}\right|_{w_\infty} \hat{\chi}(g) \prod_{p\in S_f(\mathbb{Q}),\hat{\chi}|_{G_w}=1} \frac{n_{w_p} f_{F/\mathbb{Q}}(w_p)\log(p)}{e_{F/\mathbb{Q}}(w_p)} & \text{, falls } F/\mathbb{Q} \text{ total reell,} \\ \prod_{p\in S_f(\mathbb{Q}),\hat{\chi}|_{G_w}=1} \frac{n_{w_p} f_{F/\mathbb{Q}}(w_p)\log(p)}{e_{F/\mathbb{Q}}(w_p)} & \text{, falls } F/\mathbb{Q} \text{ rein imaginär.} \end{cases}$$

Wir berechnen jetzt $L_S^*(F/\mathbb{Q},\overline{\hat{\chi}},0)$. Sei zunächst $F/\mathbb{Q}$ total reell. In diesem Fall haben wir schon gesehen, dass

$$L^*(F/\mathbb{Q},\overline{\hat{\chi}},0) = -\frac{1}{2}\sum_{g\in\hat{G}} \overline{\hat{\chi}}(g)\log|\xi^g|$$

ist. Also gilt

$$\begin{aligned}L_S^*(F/\mathbb{Q},\overline{\hat{\chi}},0) &= -\frac{1}{2}\sum_{g\in\hat{G}} \overline{\hat{\chi}}(g)\log|\xi^g| \prod_{p\in S_f(\mathbb{Q}),\hat{\chi}(p)=1} \overline{\hat{\chi}}(p)\log(p) \prod_{p\in S_f(\mathbb{Q}),\hat{\chi}(p)\neq 1} (1-\overline{\hat{\chi}}(p)) \\ &= -\frac{1}{2}\sum_{g\in\hat{G}} \overline{\hat{\chi}}(g)\log|\xi^g| \prod_{p\in S_f(\mathbb{Q}),\hat{\chi}(p)=1} \log(p) \prod_{p\in S_f(\mathbb{Q}),\hat{\chi}(p)\neq 1} (1-\overline{\hat{\chi}}(p))\end{aligned}$$

Ist $F/\mathbb{Q}$ rein imaginär, dann gilt nach [Was97, Th. 4.9]

$$L(F/\mathbb{Q},\hat{\chi},1)=\pi i\frac{\tau(\hat{\chi})}{f(\hat{\chi})}\sum_{a=1}^{f(\hat{\chi})}\overline{\hat{\chi}}(a)a.$$

Aus

$$L(F/\mathbb{Q},\hat{\chi},1)=\frac{\tau(\hat{\chi})\pi}{if(\hat{\chi})}L(F/\mathbb{Q},\overline{\hat{\chi}},0)$$

(siehe [Was97, S.35]) folgt

$$L(F/\mathbb{Q},\overline{\hat{\chi}},0)=-\sum_{a=1}^{f(\hat{\chi})}\overline{\hat{\chi}}(a)a=-\sum_{g\in\mathcal{G}}\overline{\hat{\chi}}(g)g.$$

Für $F/\mathbb{Q}$ rein imaginär ist also

$$L_S^*(F/\mathbb{Q},\overline{\hat{\chi}},0)=-\sum_{g\in\hat{G}}\overline{\hat{\chi}}(g)g\prod_{p\in S_f(\mathbb{Q}),\hat{\chi}(p)=1}\log(p)\prod_{p\in S_f(\mathbb{Q}),\hat{\chi}(p)\neq 1}(1-\overline{\hat{\chi}}(p)).$$

Damit ergibt sich insgesamt im Fall $F/\mathbb{Q}$ rein imaginär

$$\begin{aligned}\frac{\mathrm{Det}_{\hat{\chi}}(\lambda_F)}{L_S^*(F/\mathbb{Q},\overline{\hat{\chi}},0)} &= \frac{\displaystyle\prod_{p\in S_f(\mathbb{Q}),\hat{\chi}|_{G_{w_p}}=1}\frac{n_{w_p}f_{F/\mathbb{Q}}(w_p)\log(p)}{e_{F/\mathbb{Q}}(w_p)}}{\displaystyle-\sum_{g\in\mathcal{G}}\overline{\hat{\chi}}(g)g\prod_{p\in S_f(\mathbb{Q}),\chi(p)=1}\log(p)\prod_{p\in S_f(\mathbb{Q}),\chi(p)\neq 1}(1-\overline{\hat{\chi}}(p))}\\ &= -\frac{1}{\displaystyle\sum_{g\in\mathcal{G}}\overline{\hat{\chi}}(g)g}\prod_{p\in S_f(\mathbb{Q}),\hat{\chi}(p)=1}\frac{n_{w_p}f_{F/\mathbb{Q}}(w_p)}{e_{F/\mathbb{Q}}(w_p)}\prod_{p\in S_f(\mathbb{Q}),\hat{\chi}(p)\neq 1}\frac{1}{(1-\overline{\hat{\chi}}(p))}.\end{aligned}$$

Und für $F/\mathbb{Q}$ total reell ist

$$\begin{aligned}\frac{\mathrm{Det}_{\hat{\chi}}(\lambda_F)}{L_S^*(F/\mathbb{Q},\overline{\hat{\chi}},0)} &= \frac{\displaystyle-\sum_{g\in\hat{G}}\log\left|\xi^{g^{-1}}\right|_{w_\infty}\hat{\chi}(g)\prod_{p\in S_f(\mathbb{Q}),\hat{\chi}|_{G_{w_p}}=1}\frac{n_{w_p}f_{F/\mathbb{Q}}(w_p)\log(p)}{e_{F/\mathbb{Q}}(w_p)}}{\displaystyle-\tfrac{1}{2}\sum_{g\in\hat{G}}\log|\xi^g|\,\hat{\chi}(g^{-1})\prod_{p\in S_f(\mathbb{Q}),\hat{\chi}(p)=1}\log(p)\prod_{p\in S_f(\mathbb{Q}),\hat{\chi}(p)\neq 1}(1-\overline{\hat{\chi}}(p))}.\\ &= 2\prod_{p\in S_f(\mathbb{Q}),\hat{\chi}(p)=1}\frac{n_{w_p}f_{F/\mathbb{Q}}(w_p)}{e_{F/\mathbb{Q}}(w_p)}\prod_{p\in S_f(\mathbb{Q}),\hat{\chi}(p)\neq 1}\frac{1}{(1-\overline{\hat{\chi}}(p))}\end{aligned}$$

□

Bemerkung 5. *Die Voraussetzung im obigen Satz an die absolut irreduziblen Charaktere von G, ist eine echte Voraussetzung. So erfüllt zum Beispiel die Quaternionengruppe Q_8 diese Voraussetzung nicht.*

Wenn wir nicht wissen, dass $T\Omega$ die Rationalitätsvermutung erfüllt, dann nehmen wir dies einfach an. Mit Hilfe des folgenden Lemmas (siehe etwas [Ble]) können wir zumindest in Abhängigkeit der Genauigkeit der Rechnungen unsere Annahme unterstützen.

Lemma 3.3.6. *Sei $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$ und sei $\alpha = (\alpha_\chi)_{\chi \in \mathrm{Irr}(G)} \in \prod_{\chi \in \mathrm{Irr}(G)} \mathbb{C} \cong \zeta(\mathbb{C}[G])^\times$. Dann gilt*

$$\alpha \in \zeta(F[G])^\times \iff \alpha_{\sigma\circ\chi} = \sigma(\alpha_\chi)$$

für alle $\chi \in \mathrm{Irr}(G)$ und alle $\sigma \in \mathrm{Aut}(\mathbb{C}/F)$.

Insbesondere gilt für $F = \mathbb{Q}$

$$\alpha \in \zeta(\mathbb{Q}[G]) \iff \alpha_\chi \in \mathbb{Q}(\chi) \text{ und } \alpha_{\sigma\circ\chi} = \sigma(\alpha_\chi)$$

für alle $\chi \in \mathrm{Irr}(G)$ und alle $\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$.
Dies können wir effektiv testen, wenn wir eine gute Approximation der komplexen Zahlen α_χ und eine Abschätzung für die Nenner haben.
Zur Berechnung der L-Werte benutzen wir den Algorithmus von Dokchitser [Dok04] der auch in MAGMA implementiert ist. Für die Berechnung des führenden Koeffizienten der Taylorreihenentwicklung um $s = 0$ der reduzierten Artinschen-L-Reihen benutzen wir den von Bley in MAGMA implementierten Algorithmus.
Jetzt erläutern wir kurz, wie wir den Algorithmus von Bley und Wilson in [BW09] zur Verifikation verwenden. Dafür geben wir eines der Hauptresultate dieses Artikels wieder.
Im Folgenden sei N entweder eine endliche galoissche Körpererweiterung von $\mathbb{Q}$ (dies bezeichnen wir als globalen Fall) oder eine endliche galoissche Erweiterung von $\mathbb{Q}_p$ für eine Primzahl p (dies bezeichnen wir als lokalen Fall). Sei weiter $\mathcal{O}_N$ der Ring der ganzen Zahlen von N. Ist L endliche direkte Summe von solchen Körpern, also $L = N_1 \oplus \ldots \oplus N_r$, dann sei $\mathcal{O}_L$ die maximale Ordnung $\mathcal{O}_{N_1} \oplus \ldots \oplus \mathcal{O}_{N_r}$ von L. Mit $I(L)$ bezeichnen wir die Gruppe der gebrochenen Ideale von $\mathcal{O}_L$, also ist $I(L) \cong I(N_1) \oplus \ldots \oplus I(N_r)$. Sei $\mathcal{A}$ eine $\mathcal{O}_N$-Ordnung in einer halbeinfachen N-Algebra A und sei $\mathcal{M}$ eine Maximalordnung in A die $\mathcal{A}$ enthält. Sei $\mathfrak{f}$ ein volles zweiseitiges Ideal von $\mathcal{M}$, das in $\mathcal{A}$ enthalten ist. Sei weiter C das Zentrum von A und $\mathfrak{g} := \mathcal{O}_C \cap \mathfrak{f}$. Für ein Primideal $\mathfrak{p} \leq \mathcal{O}_N$ und einen $\mathcal{O}_N$-Modul M setzen wir $M_\mathfrak{p} := M \otimes_{\mathcal{O}_N} \mathcal{O}_{N_\mathfrak{p}}$.

Wir betrachten das Diagramm mit exakter Zeile

$$\begin{array}{ccccccccc} & & & & C^\times & & & & \\ & & \nearrow & & \uparrow{\scriptstyle \mathrm{nr}_A} & & & & \\ K_1(\mathcal{A}) & \xrightarrow{f^*} & K_1(A) & \xrightarrow{\partial^1_{\mathcal{A}}} & K_0(\mathcal{A},N) & \xrightarrow{\partial^0_{\mathcal{A}}} & K_0(\mathcal{A}) & \longrightarrow & K_0(A) \end{array}$$

mit $f^*([\mathcal{A}^n,\varphi]) = [A\otimes\mathcal{A}^n, \mathrm{id}_A\otimes\varphi], \partial^1_{\mathcal{A}}([A^n,\varphi]) = [\mathcal{A}^n,\varphi,\mathcal{A}^n]$ und $\partial^0_{\mathcal{A}}([P,\varphi,Q]) = [P]-[Q]$. Im lokalen Fall induziert $\mathrm{nr}_A \circ (\partial^1_{\mathcal{A}})^{-1}$ einen Isomorphismus zwischen $\partial^1_{\mathcal{A}}(K_1(\mathcal{A}))$ und $C^\times/\mathrm{nr}_A(f^*(K_1(\mathcal{A})))$. Diesen bezeichnen wir mit $\overline{\mathrm{n}}_{\mathcal{A}}$.

Lemma 3.3.7. *(1) Die reduzierte Norm von $\mathcal{A}$ induziert einen Homomorphismus*

$$\mu : K_1(\mathcal{A}/\mathfrak{f}) \to (\mathcal{O}_C/\mathfrak{g})^\times.$$

(2) Es gibt einen kanonischen Isomorphismus

$$K_0(\mathcal{A},N)_{tors} \to \mathrm{cok}(\mu).$$

Im lokalen Fall ist er von der Abbildung $\overline{\mathrm{n}}_{\mathcal{A}}$ induziert.

Beweis. [BW09, Th. 2.6] □

Sei nun N wieder global. Seien $e_1,\ldots,e_r$ die primitiven Idempotenten von C. Wir setzen $A_i := Ae_i$, dann gilt

$$A = A_1 \oplus \ldots \oplus A_r,$$

mit den unzerlegbaren Idealen A_i von A. Jedes A_i ist eine N-Algebra mit Einselement e_i und Zentrum $Z(A_i) =: N_i$ sind endliche Erweiterungen von N. Die Wedderburnzerlegung von A induziert Zerlegungen $C = N_1 \oplus \ldots \oplus N_r$ und $\mathcal{O}_C = \mathcal{O}_{N_1} \oplus \ldots \oplus \mathcal{O}_{N_r}$. Für ein Primideal $\mathfrak{p} \leq \mathcal{O}_N$ gilt

$$C_{\mathfrak{p}} \cong \bigoplus_{i=1}^{r} \bigoplus_{\mathfrak{P}} N_{i,\mathfrak{P}}, \tag{3.18}$$

wobei $\mathfrak{P}$ über alle Primideale von $\mathcal{O}_N$ läuft, die $\mathfrak{p}$ teilen. Dieser Isomorphismus induziert einen Isomorphismus $I(C_{\mathfrak{p}}) \cong \bigoplus_{i=1}^r \bigoplus_{\mathfrak{P}} I(N_{i,\mathfrak{P}})$. Sei nun $\mathfrak{g}_{i,p}$ der $\mathfrak{p}$-Anteil von $\mathfrak{g}_i$. Dann gilt $(\mathcal{O}_{C,\mathfrak{p}}/\mathfrak{g}_{\mathfrak{p}})^\times \cong \bigoplus_{i=1}^r (\mathcal{O}_{N_i}/\mathfrak{g}_{i,\mathfrak{p}})^\times$.

Lemma 3.3.8. *Sei $\mathcal{A} = \mathcal{O}_N[G]$ für eine endliche Gruppe G. Für jedes Paar $(i, \mathfrak{P})$ wie in (3.18) wählen wir ein Element $\pi_{i,\mathfrak{P}} \in \mathcal{O}_N$, welches in $N_{i,\mathfrak{P}}$ eine Uniformisierende ist und kongruent zu 1 modulo $\mathfrak{g}_{\mathfrak{P}'}$ für jedes andere Primideal $\mathfrak{P}'$ über $\mathfrak{p}$ in N_i/N. Dann gibt es einen Isomorphismen*

$$K_0(\mathcal{A}_\mathfrak{p}, N_\mathfrak{p}) \xrightarrow{\overline{\mathrm{n}}_{\mathcal{A}_\mathfrak{p}}} C_\mathfrak{p}^\times/\mathrm{nr}(\mathcal{A}_\mathfrak{p}^\times) \xrightarrow{\overline{\varphi}} I(C_\mathfrak{p}) \times \mathrm{cok}(\mu_\mathfrak{p}),$$

wobei $\overline{\mathrm{n}}_{\mathcal{A}_\mathfrak{p}}$ von $\mathrm{nr}_{A_\mathfrak{p}} \circ (\partial^1_{A_\mathfrak{p},N_\mathfrak{p}})^{-1}$ induziert ist und die Abbildung $\overline{\varphi}$ induziert ist von

$$\varphi : \begin{cases} C_\mathfrak{p}^\times & \to \quad I(C_\mathfrak{p}) \times (\mathcal{O}_{C,\mathfrak{p}}/\mathfrak{g}_\mathfrak{p})^\times \\ \nu = (\nu_1, \ldots, \nu_r) & \mapsto \quad \left(\left(\prod_\mathfrak{P} \mathfrak{P}^{v_\mathfrak{P}(\nu_i)}\right)_i, (\overline{\mu_1}, \ldots, \overline{\mu_r})\right), \end{cases}$$

mit $\mu_i := \prod_\mathfrak{P} \pi_{i,\mathfrak{P}}^{-v_\mathfrak{P}(\nu_i)}$.

Sei nun $[P, \varphi, Q] \in K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$. Nach [Ble, Rem. 2.6 a)] können wir ohne Einschränkung annehmen, dass P und Q frei sind. Sei $(v_1, \ldots, v_d)$ bzw. $(w_1, \ldots, w_d)$ eine $\mathbb{Z}_p[G]$-Basis von P bzw. Q und $S \in \mathrm{Gl}_d(\mathbb{Q}_p[G])$ die Koordinatenmatrix von φ bzgl. dieser Basen. Sei nun $\mathrm{nr}_{\mathbb{Q}_p[G]}(S) = \eta = (\overline{\eta}_1, \ldots, \overline{\eta}_r)$. Dann repräsentiert η das Bild von $[P, \varphi, Q]$ unter der Abbildung $\overline{n}_{\mathbb{Z}[G]}$. Insbesondere gilt

$$[P, \varphi, Q] = 0 \iff \begin{cases} v_\mathfrak{P}(\eta_i) = 0, & \text{für alle } i \in \{1, \ldots, r\} \text{ und } \mathfrak{P}|p \\ \text{und} & \\ (\overline{\eta_1}, \ldots, \overline{\eta_r}) \in \mathrm{im}(\mu_p), & \end{cases} \tag{3.19}$$

wobei $\overline{\eta_i}$ das Bild von η_i unter der Projektion $\mathcal{O}_{N_i,p} \to (\mathcal{O}_{N_i}/\mathfrak{g}_{i,p})^\times$ bezeichnet.

Bemerkung 6. *Ist p kein Teiler der Ordnung von G, dann ist die Torsionsuntergruppe von $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ trivial (siehe [Bre04, Prop. 2.6]). In (3.19) ist für diese p die zweite Bedingung also immer erfüllt.*

Im nächsten Satz zeigen wir, warum und wie wir die Programme von Bley und Wilson auf $T\Omega = [\kappa \oplus F^1, \theta, F^0] - \hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}}(\mathcal{L})$ anwenden können. Sei dazu $T\Omega_p$ das Bild von $T\Omega$ unter der Abbildung

$$K_0(\mathbb{Z}[G], \mathbb{Q}) \cong \bigoplus_q K_0(\mathbb{Z}_q[G], \mathbb{Q}_q) \to K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$$

und $j : \mathbb{R} \to \mathbb{C}_p$ eine Einbettung, wobei $\mathbb{C}_p$ die Komplettierung eines algebraischen Abschlusses von $\mathbb{Q}_p$ sei. Weiter sei

$$\tau_p : \zeta(\mathbb{Q}[G])^\times \hookrightarrow \zeta(\mathbb{Q}_p[G])^\times.$$

Satz 3.3.9. *Sei $(v_1, \ldots, v_d)$ eine $\mathbb{Z}_p[G]$-Basis von $(\kappa \oplus F^1) \otimes \mathbb{Z}_p$ und $(w_1, \ldots, w_d)$ eine $\mathbb{Z}_p[G]$-Basis von $F^1 \otimes \mathbb{Z}_p$. Sei A ein Repräsentant von θ bzgl. dieser Basis. Es gelte*

$$\eta := \mathrm{nr}_{\mathbb{R}[G]}(A)/\mathcal{L} \in \zeta(\mathbb{Q}[G])^\times.$$

Dann repräsentiert $\tau_p(\eta)$ das Element $T\Omega_p$.

Beweis. Wir bemerken, dass nach Satz 3.3.2 $T\Omega$ in $K_0(\mathbb{Z}[G], \mathbb{Q})$ liegt.
Sei $\delta_{\mathbb{C}_p} := \partial^1_{\mathbb{Z}_p[G],\mathbb{C}_p} \circ \mathrm{nr}^{-1}_{\mathbb{C}_p[G]} : \zeta(\mathbb{C}_p[G])^\times \to K_0(\mathbb{Z}_p[G], \mathbb{C}_p)$. Diese Abbildung ist wohldefiniert, denn nach [Bre04, Prop. 2.2] ist die reduzierte Normabbildung $\mathrm{nr}_{\mathbb{C}_p[G]}$ ein Isomorphismus. Das Diagramm

$$\begin{array}{ccc} \zeta(\mathbb{R}[G])^\times & \xrightarrow{\ j\ } & \zeta(\mathbb{C}_p[G])^\times \\ \downarrow{\scriptstyle \hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}}} & & \downarrow{\scriptstyle \delta_{\mathbb{C}_p}} \\ K_0(\mathbb{Z}[G], \mathbb{R}) & \xrightarrow{\ j\ } & K_0(\mathbb{Z}_p[G], \mathbb{C}_p) \end{array}$$

ist kommutativ [Bre04, Prop. 2.9], wobei die Abbildungen j von der Einbettung j induziert sind. Weiterhin gilt

$$j(K_0(\mathbb{Z}[G], \mathbb{Q})) \subseteq K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$$

und

$$\begin{aligned} T\Omega_p &= j(T\Omega) = j([\kappa \oplus F^1, \theta, F^0] - \hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}}(\mathcal{L})) = j([\kappa \oplus F^1, \theta, F^0]) - j(\hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}}(\mathcal{L})) \\ &= j([\kappa \oplus F^1, \theta, F^0]) - \delta_{\mathbb{C}_p}(j(\mathcal{L})) = [\mathbb{Z}_p[G]^d, A, \mathbb{Z}_p[G]^d] - \delta_{\mathbb{C}_p}(j(\mathcal{L})). \end{aligned}$$

Nach [CR87, (40.31)] gibt es eine Matrix $A' \in \mathrm{Gl}_d(\mathbb{C}_p[G])$ mit $\mathrm{nr}_{\mathbb{C}_p[G]}(A') = j(\mathcal{L})$. Also gilt

$$\begin{aligned} j(T\Omega) &= [\mathbb{Z}_p[G]^d, A, \mathbb{Z}_p[G]^d] - \delta_{\mathbb{C}_p}(j(\mathcal{L})) = [\mathbb{Z}_p[G]^d, A, \mathbb{Z}_p[G]^d] - [\mathbb{Z}_p[G]^d, A', \mathbb{Z}_p[G]^d] \\ &= [\mathbb{Z}_p[G]^d, (A')^{-1} \circ A, \mathbb{Z}_p[G]^d] \in K_0(\mathbb{Z}_p[G], \mathbb{Q}_p). \end{aligned}$$

Wieder nach [CR87, (40.31)] gibt es eine Matrix $B \in \mathrm{Gl}_d(\mathbb{Q}_p[G])$ mit $\mathrm{nr}_{\mathbb{C}_p[G]}(B) = \mathrm{nr}_{\mathbb{C}_p[G]}\left((A')^{-1} \circ A\right)$. Nach [Bur04, Lemma 2.2] gilt nun

$$j(T\Omega) = [\mathbb{Z}_p[G]^d, B, \mathbb{Z}_p[G]^d].$$

Des Weiteren gilt

$$\mathrm{nr}_{\mathbb{C}_p[G]}(B) = \mathrm{nr}_{\mathbb{C}_p[G]}\left((A')^{-1} \circ A\right) = \frac{\mathrm{nr}_{\mathbb{C}_p[G]}(A)}{j(\mathcal{L})} = \tau_p\left(\frac{\mathrm{nr}_{\mathbb{R}[G]}(A)}{\mathcal{L}}\right).$$

□

Insgesamt ergibt sich daraus folgender Algorithmus.

Algorithmus 3.3.10.

Input: *Das Tripel* $[\kappa \oplus F^1, \theta, F^0]$ *und das Tupel* $\mathcal{L}$.

Output: *Wahr, falls* $T\Omega = 0$ *numerisch verifiziert, sonst falsch.*

(1) Verifikation von $T\Omega = 0$ *in* $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ *für alle Primzahlen* p*, die die Gruppenordnung nicht teilen.*

(a) Berechne eine $\mathbb{R}[G]$*-Basis von* $(\kappa \oplus F^1)_{\mathbb{R}}$ *und* $F^0_{\mathbb{R}}$*, so dass diese Basis für jedes* $p \nmid \#G$ *auch eine* $\mathbb{Z}_p[G]$*-Basis von* $(\kappa \oplus F^1) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ *und* $F^0 \otimes_{\mathbb{Z}} \mathbb{Z}_p$ *darstellt (Vergleiche Bemerkungen unten).*

(b) Berechne einen Repräsentanten $A \in \mathrm{Gl}_d(\mathbb{R}[G])$ *von* θ *bzgl. dieser Basen.*

(c) Berechne $\mathrm{nr}_{\mathbb{R}[G]}(A)/\mathcal{L} = (\eta_1, \ldots, \eta_r)$ *exakt, wenn die Voraussetzungen aus Satz 3.3.5 erfüllt sind, ansonsten runde.*

(d) Für $i = 1, \ldots, r$ *bestimme eine Primfaktorzerlegung von* η_i *im entsprechenden Charakterkörper und teste, ob nur Ideale mit Träger in* $\{q \mid q | \#G\}$ *vorkommen. Ist dies nicht der Fall, dann gib falsch aus.*

(2) Verifikation von $T\Omega = 0$ *in* $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ *für alle Primzahlen* p*, die die Gruppenordnung teilen. Für jedes solches* p *tue folgendes*

(a) Berechne $v_1, \ldots, v_d \in \kappa \oplus F^1$ *und* $w_1, \ldots, w_d \in F^0$*, so dass* $\{v_i \otimes 1 \mid i = 1, \ldots, d\}$ *bzw.* $\{w_i \otimes 1 \mid i = 1, \ldots, d\}$ *eine* $\mathbb{Z}_p[G]$*-Basis (und damit auch* $\mathbb{R}[G]$*-Basis) von* $(\kappa \oplus F^1) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ *bzw.* $F^0 \otimes_{\mathbb{Z}} \mathbb{Z}_p$ *ist (Vergleiche Bemerkungen unten).*

(b) Berechne einen Repräsentanten $A \in \mathrm{Gl}_d(\mathbb{R}[G])$ *von* θ *bzgl. dieser Basen.*

(c) Berechne $\eta := \mathrm{nr}_{\mathbb{R}[G]}(A)/\mathcal{L} = (\eta_1, \ldots, \eta_r)$ *exakt, wenn die Voraussetzungen aus Satz 3.3.5 erfüllt sind, ansonsten runde.*

(d) Lies η *in* $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ *und teste, ob* $\eta = 0$ *gilt. Ist dies nicht der Fall, dann gib falsch aus.*

(3) Gib wahr aus.

Bemerkungen 3.3.11. *(1) Die Existenz solcher Basen folgt aus einem Resultat von Swan ([CR81, Th. 32.11]), welches garantiert, dass unsere Moduln lokal frei sind. Die Berechnung der Basen ist ein nicht triviales Problem. Im Fall $p \nmid \#G$ kann man den Algorithmus von Bley und Johnston in [BJ, 6.4] benutzen. Dort werden unter gewissen Voraussetzungen Basen über Maximalordnungen berechnet und für $p \nmid \#G$ sind dies $\mathbb{Z}_p[G]$-Basen. Die Voraussetzungen sind z.B. im Falle des Gruppenringes $\mathbb{Z}_p[G]$ für Gruppen bis Ordnung 31 erfüllt ([BJ, Prop. 4.6]). Im Fall $p|\#G$ berechnet man $\mathbb{Z}_p[G]$-Basen wie in [BW09, 4.2] beschrieben.*

Bei Gruppen größerer Ordnung kann man wie folgt vorgehen. Sei $(v_1 \otimes 1, \ldots, v_d \otimes 1)$ bzw. $(w_1 \otimes 1, \ldots, w_d \otimes 1)$ eine $\mathbb{Q}[G]$-Basis von $(\kappa \oplus F^1)_{\mathbb{Q}}$ bzw. $F^0_{\mathbb{Q}}$, wobei $v_i \in \kappa \oplus F^1, w_i \in F^0, i = 1, \ldots, d$ gelte. Sei weiter $n := [\mathbb{Z}[G] : \langle v_1, \ldots, v_d \rangle_{\mathbb{Z}[G]}]$ und $m := [\mathbb{Z}[G] : \langle w_1, \ldots, w_d \rangle_{\mathbb{Z}[G]}]$. Für alle $p \nmid nm$ ist dann $(v_1 \otimes 1, \ldots, v_d \otimes 1)$ bzw. $(w_1 \otimes 1, \ldots, w_d \otimes 1)$ auch eine $\mathbb{Z}_p[G]$-Basis von $(\kappa \oplus F^1)_{\mathbb{Z}_p}$ bzw. $F^0_{\mathbb{Z}_p}$. Für die anderen endlich vielen p verfährt man wieder wie in [BW09, 4.2].

(2) Da $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p) \cong K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)_f \oplus K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)_{tors}$ gilt, wobei $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)_f$ die freie Untergruppe und $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)_{tors}$ die Torsionsuntergruppe bezeichne, kann man Schritt (2) (d) in zwei Teile aufteilen. Den „Nulltest“ in der freien Untergruppe macht man wie in (1) (d). In den folgenden Fällen gibt Bley in [Ble, 2.3] expliziete Kongruenzen an, die das Tupel $(\eta_1, \ldots, \eta_r)$ erfüllen muss, damit $\hat{\delta}^1_{\mathbb{Z}[G],\mathbb{R}}(\eta_1, \ldots, \eta_r) = 0$ in $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)_{tors}$ gilt:

(a) G zyklisch von Primzahlordnung $p \neq 2$.

(b) $G = D_{2p}$ mit $p \neq 2$.

(c) $G = A_4$ und $p \in \{2, 3\}$.

Der Nulltest kann in diesen Fällen also auch durch prüfen dieser Kongruenzen erfolgen. Für A_4-Erweiterungen geben wir diese Kongruenzen im Kapitel 4 an.

Für A_4-Erweiterungen über $\mathbb{Q}$ haben wir den Algorithmus zur numerischen Verifikation von $T\Omega$ in MAGMA vollständig implementiert. Dies ist der Algorithmus `NumProofETNC` aus der Datei NumETNC auf der beigefügten CD.

3.4 Algorithmen für $\mathbb{Z}[G]$-Moduln

Sei G eine endliche Gruppe. Wir stellen hier die für diese Arbeit wesentlichen Algorithmen zum rechnen mit $\mathbb{Z}[G]$-Moduln vor, die von uns in MAGMA implementiert wurden. Die MAGMA Implementierung dieser und weiterer Algorithmen ist auf der beiliegenden CD zu finden.
Wir setzen an dieser Stelle Kenntnisse der algorithmischen linearen Algebra voraus, wie das Berechnen von Kernen, der hermiteschen Normalform etc. Solche Algorithmen findet man z.B. in [Coh93, Chap. 2]. Zur Berechnung von ganzzahligen Lösungen von Gleichungen über $\mathbb{Z}$ haben wir den Algorithmus von Matthews implementiert, wie er in [Mat01] beschrieben ist, da die Lösungen aus dem Standardalgorithmus in unseren Anwendungen zu große Einträge haben. Der Algorithmus von Matthews brachte eine signifikante Verbesserung.
Eine endliche Gruppe G denken wir uns über eine Liste der Elemente und eine gespeicherte Multiplikationstabelle gegeben. Ein $\mathbb{Z}$-freier $\mathbb{Z}[G]$-Modul M ist bei uns gegeben durch ein Paar (A, φ), wobei A eine Matrix in hermitescher Normalform ist und die Zeilen der Matrix ein $\mathbb{Z}$-Erzeugendensystem des Moduls bilden und φ die Gruppenwirkung auf A repräsentiert. Genauer bedeutet dies: Sei $A = (a_{ij})_{1\leq i\leq r, 1\leq j\leq n}$, dann ist

$$\varphi : G \to \mathrm{Gl}_n(\mathbb{Z})$$

ein Gruppenhomomorphismus, so dass

$$g(a_{i1}, \ldots, a_{in}) = (a_{i1}, \ldots, a_{in})\varphi(g)^t$$

gilt.
Zur Vereinfachung unterscheiden wir fortan nicht mehr zwischen dem Modul M und der Matrix A und sprechen einfach von dem Modul A oder dem Modul (A, φ).

Notationen
Mit E_n bezeichnen wir die n-reihige Einheitsmatrix und mit e_i den i-ten kanonischen Einheitsvektor. Die Nullmatrix mit n Zeilen und m Spalten bezeichnen wir mit $O_{n\times m}$. Sind $A_1, \ldots, A_n$ Matrizen, dann bezeichnen wir mit $\mathrm{diag}(A_1, \ldots, A_n)$ die Matrix mit den Matrizen $A_1, \ldots, A_n$ auf der Hauptdiagonalen und sonst Nullen.

Um eine Übersicht in den Algorithmen zu gewährleisten, ist die Beschreibung einzelner

Schritte in größeren Algorithmen weniger detailliert. Die Namen in den Klammern entsprechen den Namen der Algorithmen in der Implementierung.
Als erstes geben wir einen Algorithmus an, der das Paar (A, φ) zum Gruppenring $\mathbb{Z}[G]$ berechnet.

Algorithmus 3.4.1. `InitZG`

Input: *Eine endliche Gruppe* $G = [g_1, \ldots, g_n]$.

Output: *Ein Paar* (A, φ)*, welches den Gruppenring* $\mathbb{Z}[G]$ *repräsentiert.*

(1) Setze $A := E_n$*. Die* j*-te Zeile von* A *repräsentiert* g_j*.*

(2) (Bestimme φ*). Für* $g \in G$ *tue folgendes*

(a) Für $j \in \{1, \ldots, n\}$ *tue folgendes*

- *Bestimme* $k \in \{1, \ldots, n\}$ *mit* $gg_j = g_k$*.*
- *Setze die* j*-te Spalte in* $\varphi(g)$ *als* e_k*.*

(3) Gib (A, φ) *aus.*

Seien (A, φ) und (B, ψ) zwei $\mathbb{Z}$-freie $\mathbb{Z}[G]$-Moduln und $f : A \to B$ eine Matrix mit Einträgen in $\mathbb{Z}$ die eine $\mathbb{Z}[G]$-lineare Abbildung von repräsentiert. Mit dem folgenden Algorithmus kann man $\ker(f)$ und die Inklusion $\ker(f) \hookrightarrow B$ berechnen.

Algorithmus 3.4.2. `MapToKernel`

Input: *Zwei* $\mathbb{Z}$*-freie* $\mathbb{Z}[G]$*-Moduln* (A, φ) *und* (B, ψ)*, eine Matrix* f *mit Einträgen in* $\mathbb{Z}$*, die eine* $\mathbb{Z}[G]$*-lineare Abbildung von* A *nach* B *repräsentiert.*

Output: *Der* $\mathbb{Z}[G]$*-Modul* $\ker(f)$ *und die Inklusion* $\iota : \ker(f) \to A$*.*

(1) Berechne den Kern der Matrix f*. Sei etwa* $(v_1, \ldots, v_l)$ *eine Basis von* $\ker(f)$*, wobei die* v_i *Zeilenvektoren sind.*

(2) Setze $T := \begin{pmatrix} v_1 A \\ \vdots \\ v_l A \end{pmatrix}$ *und* $\iota := (v_1, \ldots, v_l)^t$

(3) Gib (T, φ) *und* ι *aus.*

Es folgt ein Algorithmus der die direkte Summe zweier $\mathbb{Z}$-freier $\mathbb{Z}[G]$-Moduln berechnet.

Algorithmus 3.4.3. `ZGModuleDirectSum`

Input: *Zwei $\mathbb{Z}$-freie Moduln (A, φ) und (B, ψ).*

Output: *Der Modul $(A \oplus B, \varphi \oplus \psi)$.*

(1) Setze $A \oplus B := \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$.

(2) Für alle $g \in G$ tue folgendes

(a) Setze $(\varphi \oplus \psi) := \begin{pmatrix} \varphi(g) & 0 \\ 0 & \psi(g) \end{pmatrix}$.

(3) Gib $(A \oplus B, \varphi \oplus \psi)$ aus.

Wir wollen jetzt zu einer endlichen Gruppe G die Sequenz

$$0 \longrightarrow X(-2) \xrightarrow{\iota} \mathbb{Z}[G]^r \xrightarrow{f} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0 \tag{3.20}$$

berechnen. Dabei ist ε die Augmentation, $X(-2)$ der Kern von f, r die Anzahl von Erzeugern von G und f die Abbildung $(\lambda_1, \ldots, \lambda_r) \mapsto \lambda_1(g_1 - 1) + \ldots + \lambda_r(g_r - 1)$, wobei $g_1, \ldots, g_r$ die Gruppe G erzeugen.

Algorithmus 3.4.4. `InitSequenz`

Input: *Eine endliche Gruppe $G = [g_1, \ldots, g_n]$.*

Output: *$((X(-2), \varphi_1), \iota, (\mathbb{Z}[G]^r, \varphi_2), f, (\mathbb{Z}[G], \varphi_3), \varepsilon, (\mathbb{Z}, \varphi_4))$, so dass $0 \to X(-2) \xrightarrow{\iota} \mathbb{Z}[G]^r \xrightarrow{f} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0$ eine exakte Sequenz von $\mathbb{Z}[G]$-Moduln ist.*

(1) Initiiere $(\mathbb{Z}, \varphi_4)$ durch $\mathbb{Z} = E_1$ und $\varphi_4 = E_1$.

(2) Berechne $(\mathbb{Z}[G], \varphi_3)$ mit dem Algorithmus 3.4.1.

(3) Setze $\varepsilon := \underbrace{(1, \ldots, 1)^t}_{|G|-\text{mal}}$.

(4) Berechne Erzeuger $[g_1, \ldots, g_r]$ von G.

(5) Berechne $(\mathbb{Z}[G]^r, \varphi_2)$ mit dem Algorithmus 3.4.3.

(6) (Berechne f). Setze $f := (\underbrace{-E_n, \ldots, -E_n}_{r-mal})$.

(a) *Für* $s \in [s_1, \ldots, s_r]$ *tue folgendes*

i. *Bestimme* $k \in \{1, \ldots, n\}$ *mit* $g_j s_i = g_k$.

ii. *Setze* $f[k, j + n(j-1)] = 1$.

(7) *Berechne* $(\ker(f), \varphi_1)$ *mit dem Algorithmus 3.4.2.*

(8) *Gib* $((X(-2), \varphi_1), \iota, (\mathbb{Z}[G]^r, \varphi_2), f, (\mathbb{Z}[G], \varphi_3), \varepsilon, (\mathbb{Z}, \varphi_4))$ *aus.*

Wir wenden uns jetzt der Aufgabe zu, eine Gleichung mit Koeffizienten aus $\mathbb{Z}[G]$ zu lösen. Sei dazu $G = \{g_1, \ldots, g_r\}$. Zu gegebenen $\alpha_1, \ldots, \alpha_n, \beta \in \mathbb{Z}[G]$ berechnen wir $x_1, \ldots, x_n \in \mathbb{Z}[G]$ mit $\sum_{i=1}^n x_i \alpha_i = \beta$, falls β eine $\mathbb{Z}[G]$-Linearkombination der $\alpha_i' s$ ist. Sei $\alpha_i = \sum_{g \in G} \lambda_g^{(i)} g, \beta = \sum_{i=1}^n b_j g_j$ mit $b_j, \lambda_g^{(i)} \in \mathbb{Z}$. Es gilt

$$\sum_{i=1}^{n} \left(\sum_{g \in G} x_g^{(i)} g \right) \left(\sum_{g \in G} \lambda_g^{(i)} g \right) = \sum_{i=1}^{n} \sum_{j=1}^{r} \left(\sum_{gh = g_j} x_g^{(i)} \lambda_h^{(i)} \right) g_j = \sum_{j=1}^{r} \left(\sum_{i=1}^{n} \sum_{gh = g_j} x_g^{(i)} \lambda_h^{(i)} \right) g_j$$

Zu lösen ist demnach das lineare Gleichungssystem

$$\begin{aligned}
\sum_{i=1}^{n} \left(\sum_{gh = g_1} x_g^{(i)} \lambda_h^{(i)} \right) &= b_1 \\
\sum_{i=1}^{n} \left(\sum_{gh = g_2} x_g^{(i)} \lambda_h^{(i)} \right) &= b_2 \\
\vdots \qquad\qquad &\quad \vdots \\
\sum_{i=1}^{n} \left(\sum_{gh = g_r} x_g^{(i)} \lambda_h^{(i)} \right) &= b_r.
\end{aligned}$$

Daraus ergibt sich der

Algorithmus 3.4.5. `TesteAufLinKombi`

Input: *Elemente* $\sum_{g \in G} \lambda_g^{(1)} g, \ldots, \sum_{g \in G} \lambda_g^{(n)} g, \sum_{j=1}^r b_j g_j \in \mathbb{Z}[G]$, *wobei* G *eine endliche Gruppe der Ordnung* r *sei.*

Output: *Eine Matrix* A *und ein Vektor* b, *so dass* $Ax = b$ *genau dann über* $\mathbb{Z}$ *lösbar ist, wenn* $\sum_{j=1}^r b_j g_j$ *eine Links-*$\mathbb{Z}[G]$*-Linearkombination der* $\sum_{g \in G} \lambda_g^{(i)} g$ *ist. Genauer gilt: Ist* $(x_1, \ldots, x_{n \cdot r})$ *eine Lösung von* $Ax = b$, *dann gilt mit* $\mu_i := \sum_{j=1}^r x_{(r(i-1)+j)} g_j$ *für* $i = 1, \ldots, n$ *die Gleichheit* $\sum_{i=1}^n \mu_i \sum_{j=1}^r \lambda_{g_j}^{(i)} g_j = \sum_{j=1}^r b_j g_j$.

(1) Setze $A := O_{r\times n\cdot r}$.

(2) Für $j = 1, \ldots, r$ *tue folgendes*

- *Für* $i = 1, \ldots, r$ *tue folgendes*
  - *Für* $l = 1, \ldots, n$ *tue folgendes*
    - *Setze* $A[i, j + (l-1)r] := \lambda^{(l)}_{g_k}$.

(3) Setze $b := (b_1, \ldots, b_r)^t$.

(4) Gib A *und* b *aus.*

Jetzt können wir auch ohne Probleme Links-$\mathbb{Z}[G]$-Linearkombinationen von Elementen aus $\mathbb{Z}[G]^r$ mit $r \in \mathbb{N}$ berechnen.

Algorithmus 3.4.6. `TesteAufLinKombi`

Input: *Elemente* $a_i = (a_1^{(i)}, \ldots, a_r^{(i)})$ *mit* $a_j^{(i)} \in \mathbb{Z}[G], i = 1, \ldots, n$ *\$ und* $(b_1, \ldots, b_r) \in \mathbb{Z}[G]^r$.

Output: *Matrix* A *und Vektor* b*, so dass* $Ax = b$ *genau dann über* $\mathbb{Z}$ *lösbar ist, wenn* $(b_1, \ldots, b_r)$ *eine Links-*$\mathbb{Z}[G]$*-Linearkombination der* a_i *ist.*

(1) Für $j = 1, \ldots, r$ *tue folgendes*

(a) Zu $a_j^{(i)}$ *und* b_j *berechne mit dem Algorithmus* A_i *und* c_i.

(2) Gib $A := (A_1, \ldots, A_r)^t$ *und* $b := (c_1, \ldots, c_r)^t$ *aus.*

Das Berechnen von Links-$\mathbb{Z}[G]$-Linearkombinationen ist auch möglich, wenn der Modul als Paar (A, φ) gegeben ist. Seien etwa $v_1, \ldots, v_n, w \in A$ gegeben. Wir suchen $\sum_{g\in G} x_g^{(i)} g \in \mathbb{Z}[G], x_g^{(i)}, i = 1, \ldots, n$ mit

$$\sum_{i=1}^{n} \left(\sum_{g\in G} x_g^{(i)} v_i \varphi(g)^t \right) = w.$$

Algorithmus 3.4.7. `TesteAufLinKombiZ`

Input: *$\mathbb{Z}$-freier $\mathbb{Z}[G]$-Modul (A, φ) und Elemente $v_1, \ldots, v_n, w \in A$ die von Zeilenvektoren repräsentiert werden.*

Output: *Matrix B und Vektor b, so dass $Bx = b$ genau dann lösbar ist, wenn w eine Links-$\mathbb{Z}[G]$-Linearkombination von $v_1, \ldots, v_n$ ist. Genauer gilt: Ist $(x_1, \ldots, x_{n \cdot r})$ eine Lösung von $Bx = b$, wobei r die Ordnung von G sei, dann gilt mit $\mu_i := \sum_{j=1}^{r} x_{(r(i-1)+j)} g_j$ für $i = 1, \ldots n$ die Gleichheit $\sum_{i=1}^{n} (v_i \varphi(\mu_i)^t)$.*

(1) Für $j = 1, \ldots, n$ tue folgendes

(a) Für $l = 1, \ldots r$ tue folgendes

- *Setze die $((j-1)r - l)$-te Spalte von B als $v_j \varphi(g_l)^t$.*

(2) Gib B und b aus.

Mit Hilfe der letzten beiden Algorithmen können wir jetzt auf naivem Wege $\mathbb{Z}[G]$-Erzeuger eines $\mathbb{Z}$-freien $\mathbb{Z}[G]$-Moduls bestimmen, indem wir einfach sukzessive testen, ob sich ein Vektor im Erzeugendensystem als Linearkombination der anderen darstellen lässt und wenn ja, diesen Vektor aus dem Erzeugendensystem streichen. Für nachfolgende Rechnungen kann dies von Vorteil sein, weil sich die Anzahl der Erzeuger stark reduzieren kann. Implementiert ist dieser Algorithmus unter dem Namen `ZGGenerators`.

Zu einer endlichen Gruppe G mit Erzeugern $g_1, \ldots, g_s$ betrachten wir nun die exakte Sequenz von $\mathbb{Z}[G]$-Moduln

$$0 \longrightarrow X_G(-2) \xrightarrow{\tau_G} \mathbb{Z}[G]^s \xrightarrow{\delta_G} \mathbb{Z}[G] \xrightarrow{\varepsilon_G} \mathbb{Z} \longrightarrow 0,$$

wobei $\delta_G(x_1, \ldots, x_s) = \sum_{j=1}^{s} x_j(g_j - 1)$ und ε_G die Augmentation sei. Ist nun H eine Untergruppe von G mit den Erzeugern $h_1, \ldots, h_r$ und

$$h_i - 1 = \sum_{j=1}^{s} \alpha_{ji}(g_j - 1) \quad \text{mit } \alpha_{ji} \in \mathbb{Z}[G], i = 1, \ldots, r,$$

dann ist das Diagramm von $\mathbb{Z}[H]$-Moduln

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X_H(-2) & \xrightarrow{\tau_H} & \mathbb{Z}[H]^r & \xrightarrow{\delta_H} & \mathbb{Z}[H] & \xrightarrow{\varepsilon_H} & \mathbb{Z} \longrightarrow 0 \\ & & \downarrow f & & \downarrow \varphi & & \downarrow \iota & & \| \\ 0 & \longrightarrow & X_G(-2) & \xrightarrow{\tau_G} & \mathbb{Z}[G]^s & \xrightarrow{\delta_G} & \mathbb{Z}[G] & \xrightarrow{\varepsilon_G} & \mathbb{Z} \longrightarrow 0, \end{array} \tag{3.21}$$

mit der natürlichen Inklusion ι und $\varphi(x_1,\ldots,x_r) = (\sum_{j=1}^r x_j\alpha_{1j},\ldots,\sum_{j=1}^r x_j\alpha_{sj})$ kommutativ
Der folgende Algorithmus berechnet dieses Diagramm. Wir übernehmen dabei die Bezeichnungen von oben.

Algorithmus 3.4.8. `KommDiag`

Input: *Endliche Gruppe $G = [g'_1,\ldots,g'_n]$ und eine Untergruppe $H = [h'_1,\ldots,h'_m]$.*

Output: *Ein kommutatives Diagramm, wie oben.*

(1) Berechne die Zeilen im Diagramm mit dem Algorithmus 3.4.4.

(2) (Berechne die Abbildung ι) Setze $\iota := O_{n\times m}$.

(a) Für $i = 1,\ldots,r$ tue folgendes

i. Bestimme j mit $g'_j = h'_i$.

ii. Setze $\iota[j,i] := 1$.

(3) (Berechne die Abbildung φ) Berechne mit dem Algorithmus 3.4.5 Elemente $\alpha_{ji} = \sum_{k=1}^n \lambda_k^{(ij)} g_k \in \mathbb{Z}[G]$, so dass $h_i - 1 = \sum_{j=1}^s \alpha_{ji}(g_j - 1)$ für $i = 1,\ldots,r$ gilt. Sei ψ die G-Wirkung auf $\mathbb{Z}[G]$.

(4) Für $i = 1,\ldots,r$ tue folgendes

(a) Für $k = 1,\ldots,n$ tue folgendes

i. Setze die $((i-1)m+k)$-te Spalte in φ als

$$(\lambda_1^{(i1)},\lambda_2^{(i1)},\ldots,\lambda_n^{(i1)},\lambda_1^{(i2)},\ldots,\lambda_n^{(2i)},\ldots,\lambda_1^{(is)},\ldots,\lambda_n^{(is)})\psi(h_k).$$

(5) (Berechne die Abbildung f) Berechne eine Lösung X von $\tau_G \cdot X = \varphi \cdot \tau_H$ und setze $f = X$.

(6) Gib die Sequenzen und die Abbildungen ι, φ und f aus.

Nun folgt ein Algorithmus zur Berechnung von induzierten Moduln. Sei A ein $\mathbb{Z}$-freier H-Modul und H Untergruppe der endlichen Gruppe G. Es ist $\mathrm{Ind}_H^G(A) = \mathbb{Z}[G]\otimes_{\mathbb{Z}[H]} A$. Sind nun $v_1,\ldots,v_r$ mit $v_i \in \mathbb{Z}^n$ die Zeilen von A und ist $\{l_1,\ldots,l_t\}$ ein Linksvertretersystem von $G \setminus H$, dann ist $\{l_i \otimes v_j \mid i = 1,\ldots,t, j = 1,\ldots,r\}$ eine $\mathbb{Z}$-Basis von

$\mathrm{Ind}_H^G(A)$. Wir können also als Matrix für $\mathrm{Ind}_H^G(A)$ die Matrix

$$\begin{pmatrix} A & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & A \end{pmatrix}$$

wählen, wobei A genau t-mal vorkommt. Das Element $l_i \otimes v_j$ entspricht dann der $(n(i-1)+j)$-ten Zeile in $\mathrm{Ind}_H^G(A)$. Sei $\dot{\varphi}(g) := \varphi(g)$ für $g \in H$ und $\dot{\varphi}(g) := 0$ für $g \notin H$. Dann ist die Gruppenwirkung auf $\mathrm{Ind}_H^G(A)$ gegeben durch den Homomorphismus

$$\psi : \begin{cases} G & \to & \mathrm{Gl}_{tn}(\mathbb{Z}) \\ g & \mapsto & \left(\dot{\varphi}(l_i^{-1} g l_j)\right)_{1 \le i,j, \le t} \end{cases}.$$

Denn sei $g \in G$ mit $gl_i = l_m h$ für ein $h \in H$ und $l_m \in \{l_1, \ldots, l_t\}$, dann gilt

$$g(l_i \otimes v_j) = l_m h \otimes v_j = l_m \otimes h v_j = l_m \otimes (l_m^{-1} g l_i) v_j$$

und

$$\begin{aligned} g(l_i \otimes v_j) &= (\underbrace{0, \ldots, 0}_{n(i-1)-\text{mal}}, \underbrace{v_{j1}, \ldots v_{jn}}_{=v_j}, 0, \ldots, 0) \cdot \begin{pmatrix} \dot{\varphi}(l_1^{-1} g l_1)^t & \dot{\varphi}(l_2^{-1} g l_1)^t & \ldots & \dot{\varphi}(l_t^{-1} g l_1)^t \\ \dot{\varphi}(l_1^{-1} g l_2)^t & \dot{\varphi}(l_2^{-1} g l_2)^t & \ldots & \dot{\varphi}(l_t^{-1} g l_2^t) \\ \vdots & \vdots & \ddots & \vdots \\ \dot{\varphi}(l_1^{-1} g l_t)^t & \dot{\varphi}(l_2^{-1} g l_t)^t & \ldots & \dot{\varphi}(l_t^{-1} g l_t)^t \end{pmatrix} \\ &= (v_j \dot{\varphi}(l_1^{-1} g l_i)^t, \ldots, v_j \dot{\varphi}(l_t^{-1} g l_i)^t) = (\underbrace{0, \ldots, 0}_{n(m-1)-\text{mal}}, v_j \varphi(l_m^{-1} g l_i)^t, 0, \ldots, 0) \\ &= l_m \otimes (l_m^{-1} g l_i) v_j. \end{aligned}$$

Daraus ergibt sich der

Algorithmus 3.4.9. `ModuleInduction`

Input: *Ein $\mathbb{Z}$-freier H-Modul (A, φ) und eine endliche Gruppe G mit $H \le G$.*

Output: *Der Modul $(\mathrm{Ind}_H^G(A), \psi)$.*

(1) Setze $\mathrm{Ind}_H^G(A) := \begin{pmatrix} A & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & A \end{pmatrix}$.

(2) Berechne ein Linksvertretersystem $\{l_1, \ldots, l_t\}$ von $G \setminus H$.

(3) (Berechne φ) Für $g \in G$ tue folgendes

(a) Setze $\psi(g) := \left(\dot{\varphi}(l_i^{-1} g l_j)\right)_{1 \leq i,j, \leq t}$, wobei $\dot{\varphi}(g) = \varphi(g)$, falls $g \in H$ und sonst $\dot{\varphi}(g) = 0$.

(4) Gib $(\mathrm{Ind}_H^G(A), \psi)$ aus.

Als nächstes stellen wir einen Algorithmus vor, der zu einem $\mathbb{Z}$-freien $\mathbb{Z}[G]$-Modul A und einem beliebigen $\mathbb{Z}[G]$-Modul B ein Erzeugendensystem von $\mathrm{Hom}_{\mathbb{Z}[G]}(A, B)$ berechnet. Dieser Algorithmus ist einer der wichtigsten, da er es überhaupt erst möglich gemacht hat, die Tate-Sequenz algorithmisch zu berechnen. Sei also A ein $\mathbb{Z}$-freier $\mathbb{Z}[G]$-Modul und $(\alpha_1, \ldots, \alpha_r)$ ein $\mathbb{Z}[G]$-Erzeugendensystem von A. Weiterhin sei B ein beliebiger $\mathbb{Z}[G]$-Modul und $(v_1, \ldots, v_k)$ ein $\mathbb{Z}$-Erzeugendensystem, wobei $v_1, \ldots, v_t$ die Torsionsuntergruppe erzeugen mit den Ordnungen $t_1, \ldots, t_T$. Wir suchen $b_1, \ldots, b_r \in B$, so dass

$$f : \begin{cases} A & \longrightarrow & B \\ \sum_{i=1}^{r} \lambda_i \alpha_i & \longmapsto & \sum_{i=1}^{r} \lambda_i b_i \quad \text{mit } \lambda_i \in \mathbb{Z}[G], \end{cases}$$

wohldefiniert und damit ein $\mathbb{Z}[G]$-Modulhomomorphismus ist. Wir beweisen zunächst das

Lemma 3.4.10. *Mit den Bezeichnungen von oben gilt: Die Abbildung f ist genau dann wohldefiniert und damit ein $\mathbb{Z}[G]$-Modulhomomorphismus, wenn gilt:*

$$\sum_{i=1}^{r} \lambda_i \alpha_i = 0 \Longrightarrow \sum_{i=1}^{r} \lambda_i b_i = 0.$$

Beweis. Sei $\sum_{i=1}^{r} \lambda_i \alpha_i = \sum_{i=1}^{r} \mu_i \alpha_i$, dann gilt $\sum_{i=1}^{r} (\lambda_i - \mu_i)\alpha_i = 0$. Also gilt nach Voraussetzung $\sum_{i=1}^{r} (\lambda_i - \mu_i) b_i = 0$. Und somit gilt $\sum_{i=1}^{r} \lambda_i b_i = \sum_{i=1}^{r} \mu_i b_i$. □

Wir führen dieses Problem auf das Lösen eines linearen Gleichungssystemes zurück. Sei

$$b_i = \sum_{j=1}^{k} x_j^{(i)} v_j \quad \text{für } i = 1, \ldots, r \text{ und } x_j^{(i)} \in \mathbb{Z}.$$

Für alle $g \in G$ und alle $i = 1, \ldots, k$ schreiben wir

$$g v_i = \sum_{j=1}^{r} e_j(g, i) v_j \quad \text{mit } e_j(g, i) \in \mathbb{Z}.$$

Dann ist

$$gb_i = \sum_{i=1}^{r} x_j^{(i)} \sum_{l=1}^{k} e_l(g,j) v_l.$$

Ist nun

$$\sum_{i=1}^{r} \left(\sum_{g \in G} \lambda_g^{(i)} g \right) \alpha_i = 0 \quad \text{mit } \lambda_g^{(i)} \in \mathbb{Z} \text{ eine Relation der } \alpha_i' s,$$

dann soll gelten

$$\begin{aligned} 0 = \sum_{i=1}^{r} \sum_{g \in G} \lambda_g^{(i)} g b_i &= \sum_{i=1}^{r} \left(\sum_{g \in G} \lambda_g^{(i)} \left(\sum_{j=1}^{k} x_j^{(i)} \sum_{l=1}^{k} e_l(g,j) v_l \right) \right) \\ &= \sum_{l=1}^{k} \left(\sum_{j=1}^{k} \sum_{i=1}^{r} x_j^{(i)} \left(\sum_{g \in G} \lambda_g^{(i)} e_l(g,j) \right) \right) v_l. \end{aligned}$$

Unter Beachtung der Torsion ist also für eine Relation das lineare Gleichungssystem

$$\begin{aligned} \sum_{j=1}^{k} \left(\sum_{i=1}^{r} x_j^{(i)} \left(\sum_{g \in G} \lambda_g^{(i)} e_1(g,j) \right) \right) + t_1 y_1 &= 0 \\ \vdots &= \vdots \\ \sum_{j=1}^{k} \left(\sum_{i=1}^{r} x_j^{(i)} \left(\sum_{g \in G} \lambda_g^{(i)} e_t(g,j) \right) \right) + t_t y_t &= 0 \\ \sum_{j=1}^{k} \left(\sum_{i=1}^{r} x_j^{(i)} \left(\sum_{g \in G} \lambda_g^{(i)} e_{t+1}(g,j) \right) \right) &= 0 \\ \vdots &\vdots \\ \sum_{j=1}^{k} \left(\sum_{i=1}^{r} x_j^{(i)} \left(\sum_{g \in G} \lambda_g^{(i)} e_k(g,j) \right) \right) &= 0 \end{aligned}$$

in den $k \cdot r + t$ Unbestimmten $x_j^{(i)}, y_1, \ldots, y_t$ und mit k-Zeilen, zu lösen. Der Koeffizient bei $x_j^{(i)}$ in der l-ten Zeile ist also $\sum_{g \in G} \lambda_g^{(i)} e_l(g,j)$. Da der Modul A nach Voraussetzung $\mathbb{Z}$-frei ist, liefert uns der Algorithmus 3.4.5 alle Relationen die wir zu beachten haben. Um dies effektiv zu implementieren stellen wir noch folgende Überlegung an. Ist $G = [g_1, \ldots, g_n]$ und ist für $l = 1, \ldots, r$ die Matrix A_l definiert durch

$$A_l := \begin{pmatrix} e_j(g_1,1) & e_j(g_2,1) & \ldots & e_j(g_n,1) \\ e_j(g_1,2) & e_j(g_2,2) & \ldots & e_j(g_n,2) \\ \vdots & \vdots & \ddots & \vdots \\ e_j(g_1,r) & e_j(g_2,r) & \ldots & e_j(g_n,r) \end{pmatrix},$$

dann gilt für das zu lösende Gleichungssystem

$$A_l \cdot \begin{pmatrix} \lambda_{g_1}^{(i)} \\ \lambda_{g_2}^{(i)} \\ \vdots \\ \lambda_{g_n}^{(i)} \end{pmatrix} = \begin{pmatrix} \sum_{m=1}^{n} \lambda_{g_m}^{(i)} e_l(g_m, 1) \\ \sum_{m=1}^{n} \lambda_{g_m}^{(i)} e_l(g_m, 2) \\ \vdots \\ \sum_{m=1}^{n} \lambda_{g_m}^{(i)} e_l(g_m, r) \end{pmatrix} = \begin{pmatrix} \text{Koeffizient vor } x_1^{(i)} \text{ in der } l\text{-ten Zeile} \\ \text{Koeffizient vor } x_2^{(i)} \text{ in der } l\text{-ten Zeile} \\ \vdots \\ \text{Koeffizient vor } x_r^{(i)} \text{ in der } l\text{-ten Zeile} \end{pmatrix}.$$

Algorithmus 3.4.11. `RelationenMatrix`

Input: *$\mathbb{Z}$-freier $\mathbb{Z}[G]$-Modul (A, ϕ), ein $\mathbb{Z}[G]$-Erzeugendensystem $\alpha_1, \ldots, \alpha_r$ von A und ein $\mathbb{Z}[G]$-Modul (B, ψ).*

Output: *Eine Matrix M, dessen homogener Lösungsraum $\mathbb{Z}[G]$-Homomorphismen von A nach B liefert.*

(1) Erstelle eine Liste L mit den $e_l(g, j)$. Ist $G = [g_1, \ldots, g_n]$, dann setze

$$\begin{aligned} L \;:=\; \Big[&[e_1(g_1,1), e_2(g_1,1), e_3(g_1,1), \ldots, e_r(g_1,1)], \\ &[e_1(g_1,2), e_2(g_1,2), e_3(g_1,2), \ldots, e_r(g_1,2)], \\ &\qquad\vdots \\ &[e_1(g_1,r), e_2(g_1,r), e_3(g_1,r), \ldots, e_r(g_1,r)], \\ &[e_1(g_2,1), e_2(g_2,1), e_3(g_2,1), \ldots, e_r(g_2,1)], \\ &\qquad\vdots \\ &[e_1(g_n,r), e_2(g_n,r), e_3(g_n,r), \ldots, e_r(g_n,r)]\Big]. \end{aligned}$$

(2) Für $j = 1, \ldots, r$ definiere Matrizen A_j durch $A_j[i,k] := L[(k-1) \cdot r + i][1, j]$ für $i = 1, \ldots, r$ und $k = 1, \ldots, n$.

(3) Bestimme mit dem Algorithmus 3.4.5 bzw. 3.4.7 ein $\mathbb{Z}$-Erzeugendensystem aller $\mathbb{Z}[G]$-Relationen von $\alpha_1, \ldots, \alpha_r$. Sei s die Länge des Erzeugendensystems.

(4) Repräsentiert $(\lambda_{g_1}^{(1)}, \ldots, \lambda_{g_n}^{(1)}, \lambda_{g_1}^{(2)}, \ldots, \lambda_{g_n}^{(r)})$ die m-te Relation, dann definiere die Matrix M_m durch

$$M_m[i,j] := A_i \cdot (\lambda_{g_1}^{(j)}, \ldots, \lambda_{g_1}^{(j)})^t$$

und $T_m := (t_1, \ldots, t_t, \underbrace{0, \ldots, 0}_{(k-t)\text{-mal}})^t$.

(5) Gib die Matrix

$$\begin{pmatrix} \mathrm{Mat}_1 & T_1 & & \\ \mathrm{Mat}_2 & & T_2 & \\ \vdots & & & \ddots \\ \mathrm{Mat}_s & & & T_s \end{pmatrix}$$

zurück.

Jetzt können wir auch einen Algorithmus angeben der $\mathbb{Z}[G]$-lineare Schnitte berechnet, wenn sie existieren.

Algorithmus 3.4.12. `ZGSection`

Input: *$\mathbb{Z}$-freie $\mathbb{Z}[G]$-Moduln (A, φ) und (B, ψ) sowie eine Matrix f, die eine $\mathbb{Z}[G]$-lineare Abbildung von A nach B repräsentiert.*

Output: *Eine Matrix s, die einen $\mathbb{Z}[G]$-linearen Schnitt zu f repräsentiert, wenn ein solcher existiert.*

(1) Sei A_R die Matrix aus dem Algorithmus 3.4.11.

(2) Setze $M := B^t \cdot f$.

(3) Setze $A_S := \mathrm{diag}(M, \ldots, M)$, wobei die Matrix M so oft auftaucht, wie der $\mathbb{Z}$-Rang von B ist.

(4) Setze $A_G := (A_R, A_S)^t$.

(5) Sei B_i die i-te Zeile von B und r der $\mathbb{Z}$-Rang von B. Setze $b := (\underbrace{0, \ldots, 0}_{\text{Anzahl der Spalten von } A_R}, B_1, \ldots, B_r)^t$.

(6) Sei k der $\mathbb{Z}$-Rang von A und $(x_1^{(1)}, \ldots, x_k^{(1)}, x_1^{(2)}, \ldots, x_k^{(2)}, \ldots, x_1^{(r)}, \ldots, x_k^{(r)})$ eine Lösung von $A_G x = b$, dann setze die i-te Zeile in der Matrix s als $(x_1^{(i)}, \ldots, x_k^{(i)})$.

(7) Gib die Matrix s zurück.

Wir stellen jetzt einen Algorithmus vor, der zu einer gegebenen Klasse $[\gamma] \in \mathrm{H}^2(G, C)$ eine Abbildung f berechnet, welche die Klasse von γ in $\mathrm{Ext}_G^2(\mathbb{Z}, C)$ repräsentiert, wenn wir die Standardsequenz

$$0 \to X(-2) \to \mathbb{Z}[G]^r \xrightarrow{\delta_G} \mathbb{Z}[G] \to \mathbb{Z} \to 0, \tag{3.22}$$

zur Berechnung von $\mathrm{Ext}^2_G(\mathbb{Z}, C)$ heranziehen. Seien $g_1, \ldots, g_r$ Erzeuger der Gruppe G und $G = \{g_1, \ldots, g_r, h_1, \ldots, h_s\}$, wobei $h_1 = \mathrm{id}_G$ sei. Die Abbildung δ_G ist dann gegeben mit $\delta_G(x_1, \ldots, x_r) = \sum_{j=1}^{r} x_j(g_j - 1)$. Im Abschnitt 1.3.5 haben wir schon gesehen, dass die Klasse von γ unter dem Isomorphismus $\mathrm{H}^2(G, C) \cong \mathrm{Yext}^2_G(\mathbb{Z}, C)$ auf die Klasse der Sequenz

$$0 \to C \to C(\gamma) \xrightarrow{\psi} \mathbb{Z}[G] \to \mathbb{Z} \to 0,$$

abgebildet wird. Es war dabei

$$C(\gamma) = C \oplus \bigoplus_{\sigma \in G, \sigma \neq 1} \mathbb{Z} b_\sigma,$$

mit formalen Symbolen b_σ und G-Wirkung $\tau b_\sigma = b_{\tau\sigma} - b_\tau + \gamma(\tau, \sigma)$, wobei $b_{\mathrm{id}} = \gamma(1, 1)$ gesetzt wird. Die Abbildung ψ ist gegeben mit $\psi((c, \sum_{\sigma \neq 1} \lambda_\sigma b_\sigma)) = \sum_{\sigma \neq 1} \lambda_\sigma(\sigma - 1)$. Für nachfolgende Rechnungen schreiben wir jetzt

$$C(\gamma) = C \oplus \bigoplus_{i=1}^{r} \mathbb{Z} b_i \oplus \bigoplus_{j=2}^{s} \mathbb{Z} a_j.$$

Im Abschnitt 1.3.1 haben wir gesehen, dass wir eine Abbildung ϕ konstruieren müssen, so dass das Diagramm

$$\begin{array}{ccccccccc}
0 & \longrightarrow & X(-2) & \longrightarrow & \mathbb{Z}[G]^r & \xrightarrow{\delta_G} & \mathbb{Z}[G] & \longrightarrow & \mathbb{Z} \longrightarrow 0 \\
 & & \downarrow f & & \downarrow \phi & & \| & & \| \\
0 & \longrightarrow & C & \longrightarrow & C(\gamma) & \xrightarrow{\psi} & \mathbb{Z}[G] & \longrightarrow & \mathbb{Z} \longrightarrow 0
\end{array}$$

kommutiert, damit die Abbildung $f = \phi|_{X(-2)}$ die Klasse von γ in $\mathrm{Ext}^2_G(\mathbb{Z}, C)$ repräsentiert. Setzen wir

$$\phi(x_1, \ldots, x_r) = (0, \sum_{i=1}^{r} x_i b_i) \quad \text{und} \quad f = \phi|_{X(-2)},$$

dann kommutiert das Diagramm. Im nachfolgenden Algorithmus übernehmen wir die Bezeichnungen von oben.

Algorithmus 3.4.13. `H2ToExt`

Input: *Kozykel* $\gamma : G \times G \to C$.

Output: *Die Sequenz 3.22,* $\mathbb{Z}[G]$*-Erzeuger* $\alpha_1, \ldots, \alpha_k$ *des Moduls* $X(-2)$ *und Elemente* $c_1, \ldots, c_k$*, so dass* $f : X(-2) \to C, \alpha_i \mapsto c_i \in C$ *die obige Eigenschaft hat.*

(1) Berechne mit dem Algorithmus 3.4.4 die Sequenz 3.22.

(2) Berechne mit dem Algorithmus 3.4.5 $\mathbb{Z}[G]$-Erzeuger $\alpha_1, \ldots, \alpha_k$ des Moduls $X(-2)$. Sei etwa $\alpha_i = (\sum_{n=1}^{r} \varepsilon_1^{(i)}(n) g_n + \sum_{m=1}^{s} \delta_1^{(i)}(m) h_m, \ldots, \sum_{n=1}^{r} \varepsilon_r^{(i)}(n) g_n + \sum_{m=1}^{s} \delta_r^{(i)}(m) h_m), i = 1, \ldots, k$.

(3) Berechne die Elemente $c_1, \ldots, c_k$. Zu g_j sei $g_{j'} = g_j^{-1}$. Berechne für $i = 1, \ldots, k$

$$c_i = \sum_{j=1}^{r} \left(\sum_{n=1}^{r} \varepsilon_j^{(i)}(n) \gamma(g_n, g_j) + \sum_{m=2}^{s} \delta_j^{(i)} \gamma(h_m, g_j) + \varepsilon_j^{(i)}(j') \gamma(1,1) \right).$$

(4) Gebe die Sequenz, die Elemente $\alpha_1, \ldots, \alpha_k$ und $c_1, \ldots, c_k$ zurück.

Bemerkung 7. *Den nicht $\mathbb{Z}$-freien $\mathbb{Z}[G]$-Modul U_S haben wir ebenfalls durch eine Matrix A dargestellt, wobei die erste Zeile e_1 ist und einen Erzeuger der Torsionsuntergruppe repräsentiert. Die Gruppenwirkung wird auch hier durch einen Homomorphismus $\varphi : G \to \mathrm{Gl}_n(\mathbb{Z})$ repräsentiert, wobei bei jeder Anwendung die Torsion zu beachten ist, d.h. im Zeilenvektor ist im ersten Eintrag modulo der Ordnung der Torsion zu rechnen.*
Ist A ein $\mathbb{Z}$-freier $\mathbb{Z}[G]$-Modul und $f : B \to A$ eine $\mathbb{Z}[G]$-lineare Abbildung, wobei B $\mathbb{Z}$-frei ist, dann kann man den Kern von f etwa wie in [Ble03, 3.4] beschrieben, berechnen.

Kapitel 4

Beispiele

Wir stellen hier die absoluten A_4-Erweiterungen zusammen, für die wir die äquivariante Tamagawazahlvermutung mit unserem Algorithmus numerisch verifiziert haben. Getestet haben wir den Algorithmus an einigen zyklischen Erweiterungen.
Bevor wir auf die einzelnen Beispiele eingehen, zeigen wir, dass wir auf A_4-Erweiterungen den Satz 3.3.5 anwenden können.
Wie schon erwähnt, ist der Algorithmus noch nicht allgemein implementiert. Wir zeigen hier auch, an welcher Stelle diese Spezialisierung statt findet und welche Werte wir berechnet, und an den Algorithmus übergeben haben.

Sei ζ_3 eine 3-te primitive Einheitswurzel. Die Charaktertafel der A_4 ist dann

	Id(G)	(1 2)(3 4)	(1 2 3)	(1 3 2)
χ_1	1	1	1	1
χ_2	1	1	ζ_3	ζ_3^2
χ_3	1	1	ζ_3^2	ζ_3
χ_4	3	-1	0	0

Die ersten drei Charaktere sind offenbar abelsch und für χ_4 gilt

$$\chi_4 = \mathrm{Ind}_{C_2}^{A_4} 1_{C_2} - \mathrm{Ind}_{V_4}^{A_4} 1_{V_4},$$

wobei V_4 die Kleinsche Vierergruppe bezeichnet, C_i für $i = 2, 3$ zyklisch der Ordnung i sind und 1_H den trivialen Charakter der Gruppe H bezeichne. Dies zeigt, dass wir Satz 3.3.5 anwenden können.
Die Elemente die wir berechnet haben und an den Algorithmus übergeben haben, sind die Bilder der Abbildung $-f_3$ aus dem Satz 3.1.5 und die Erzeuger des Moduls $X_v(-2)$

aus demselben Satz und zwar in den Fällen $G_v \in \{V_4, C_2, C_3\}$. Die Berechnung der Elemente führen wir etwas genauer aus.
Wir beziehen uns mit unseren Bezeichnungen auf den Abschnitt 3.1 ohne diese nochmals neu einzuführen.
Sei zunächst v eine Stelle mit $G_v = V_4$. Dann sind N_v/K_w^{max} und K_w^{max}/K_w zyklisch der Ordnung 2. Sei a ein Erzeuger von $\mathrm{Gal}(N_v/K_w^{max})$ und b ein Lift vom geometrischen Frobeniusautomorphismus auf K_w^{max}/K_w. Die Gruppe V_4 wird dann erzeugt von a und b. Der Modul $X_v(-2)$ aus der exakten Sequenz

$$0 \to X_v(-2) \to \mathbb{Z}[V_4]^2 \xrightarrow{\delta} \mathbb{Z}[V_4] \xrightarrow{\varepsilon} \mathbb{Z} \to 0,$$

mit ε als Augmentation und $\delta((1,0)) = b-1, \delta((0,1)) = a-1$, wird erzeugt von den Elementen $(1+b,0), (0,1+a)$ und $(-1-ab, 1+ab)$. Wir berechnen nun die Bilder dieser Elemente unter der Abbildung f_2 aus Satz 3.1.5. Es war $f_2((1,0)) = (\pi^b\gamma_1, \gamma_1)$ und $f_2((0,1)) = (\gamma,\gamma)$, wobei π, γ und γ_1 wie im Abschnitt 3.1 seien. Sei nun F der Frobeniusautomorphismus der maximal unverzweigten Erweiterung von K_w. Wir erinnern daran, dass $\gamma, \gamma_1 \in K_w^{max}$ galt. Für die Bilder der Erzeuger von $X_v(-2)$ unter f_2 gilt dann:

$$\begin{aligned}
f_2((1+b,0)) &= (\pi^b\gamma_1,\gamma_1)(\pi^b\gamma_1,\gamma_1)^{(1\times b)} = (\pi^b\gamma_1,\gamma_1)(\pi^{b^2}F^{-1}(\gamma_1), F^{-1}(\gamma_1)^{(F\times 1)} \\
&= (\pi^b\gamma_1,\gamma_1)(F^2(F^{-1}(\gamma_1)), \pi F^{-1}(\gamma_1)) = (\pi^b\gamma_1 F(\gamma_1), \pi F^{-1}(\gamma_1)\gamma_1). \\
f_2((0,1+a)) &= (\gamma,\gamma)(\gamma,\gamma)^{(1\times a)} = (\gamma^2,\gamma^2). \\
f_3((-1-ab,1+ab)) &= (\pi^b\gamma_1,\gamma_1)^{-1}\left((\pi^{ba}\gamma_1,\gamma_1)^{-1}\right)^{(1\times b)}(\gamma,\gamma)(\gamma,\gamma)^{(1\times b)} \\
&= (\pi^b\gamma_1,\gamma_1)^{-1}\left((\pi^{bab}F^{-1}(\gamma_1), F^{-1}(\gamma_1))^{-1}\right)^{(F\times 1)} \\
&\quad \cdot(\gamma,\gamma)(F^{-1}(\gamma), F^{-1}(\gamma))^{(F\times 1)} \\
&= (\pi^b\gamma_1,\gamma_1)^{-1}\left((\pi^a F^{-1}(\gamma_1), F^{-1}(\gamma_1))^{-1}\right)^{(F\times 1)} \\
&\quad \cdot(\gamma,\gamma)(F^{-1}(\gamma), F^{-1}(\gamma))^{(F\times 1)} \\
&= (\pi^b\gamma_1,\gamma_1)^{-1}(F^2(F^{-1}(\gamma_1)), \pi^a F^{-1}(\gamma_1))^{-1} \\
&\quad (\gamma,\gamma)(F^2(F^{-1}(\gamma)), F^{-1}(\gamma)) \\
&= (\pi^b\gamma_1,\gamma_1)^{-1}\left(F(\gamma_1), \pi^a F^{-1}(\gamma_1)\right)^{-1}(\gamma,\gamma)(F(\gamma), F^{-1}(\gamma)) \\
&= \left(\frac{\gamma F(\gamma)}{\pi^b\gamma_1 F(\gamma_1)}, \frac{\gamma F^{-1}(\gamma)}{\gamma_1\pi^a F^{-1}(\gamma_1)}\right).
\end{aligned}$$

Wir haben neben den Erzeugern des Moduls $X_v(-2)$ die Werte $(\pi^b\gamma_1 F(\gamma_1)\gamma_1)^{-1}, \gamma^{-2})$ und $\frac{\pi^b F(\gamma_1)}{\gamma F(\gamma)}$ an das Programm übergeben.

Sei nun G_v zyklisch der Ordnung $n \geq 2$ und v verzweigt[1]. Es ist dann $K_w^{max} = K_w$. Sei weiter a ein Erzeuger von N_w/K_w^{max}. Als Sequenz haben wir die Sequenz

$$0 \to X_v(-2) \to \mathbb{Z}[G_v]^2 \xrightarrow{\delta} \mathbb{Z}[G_v] \xrightarrow{\varepsilon} \mathbb{Z} \to 0,$$

mit ε als Augmentation und $\delta((1,0)) = a - 1 = \delta((0,1))$ gewählt.
Der Modul $X_v(-2)$ wird erzeugt von den Elementen $(1 + a + \ldots + a^{n-1}, 0)$, $(0, 1 + a + \ldots + a^{n-1})$ und $(-1, 1)$. Für die Bilder unter f_2 gilt:

$$\begin{aligned} f_2((1 + a + \ldots + a^{n-1}, 0)) &= (\pi^a \gamma_1)^{(1\times(1+a+\ldots+a^{n-1}))} = (\pi^{1+a+\ldots+a^{n-1}} \gamma_1^n). \\ f_2((0, 1 + a + \ldots + a^{n-1})) &= (\gamma)^{(1\times(1+a+\ldots+a^{n-1}))} = (\gamma^n). \\ f_2((-1, 1)) &= \left(\frac{\gamma}{\pi^a \gamma_1}\right). \end{aligned}$$

Die Tabellen sind wie folgt zu verstehen. Die Nummer des Polynoms bezieht sich auf die Datei `A4Mipos.m`, die auf der beigefügten CD ist. Polynom Nr. 4 ist das 4-te Polynom in dieser Liste. Die getestete A_4-Erweiterung wird von diesem Polynom erzeugt. Die Signatur gibt die Anzahl der reellen und komplexen Einbettungen wieder. Mit d bezeichnen wir die Diskriminante, mit S_f die endlichen Stellen für zulässiges S, mit h die Klassenzahl und die Zeit gibt an, wie lange der Algorithmus zur Verifikation benötigt, hat nachdem die Stellenmenge berechnet wurde. Die Zeitangabe soll nur eine grobe Vorstellung geben.
In der Spalte $\mathcal{Q}_{\text{approx}}$ stehen die berechneten komplexen Zahlen des Quotienten $\left(\text{nr}_{\mathbb{R}[G]}(A)/\mathcal{L}\right)_{\chi_i}$ für $i = 1, 2, 3$, wobei der Zusatz $\mathbb{Z}_p[G]$-Basen für $p \neq 2, 3$ bedeutet, dass $\text{nr}_{\mathbb{R}[G]}(A)$ bzgl. $\mathbb{Z}_p[G]$-Basen für $p \neq 2, 3$ berechnet wurde. Der Zusatz $\mathbb{Z}_2[G]$-Basen bzw. $\mathbb{Z}_3[G]$-Basen ist analog zu verstehen. Da für χ_3 immer das konjugierte zu χ_2 berechnet wurde, haben wir darauf verzichtet dies in die Tabellen aufzunehmen.
Wir geben jetzt genauer an, wie der „Nulltest“ im Falle einer A_4-Erweiterung aussieht. Der Leser kann diesen Test mit den berechneten Zahlen aus den Beispielen dann auch ohne Computeralgebrasystem prüfen. Sei dazu $\left(\text{nr}_{\mathbb{R}[G]}(A)/\mathcal{L}\right) = (\eta_1, \eta_2, \eta_3)$ bzgl. einer $\mathbb{Z}_p[A_4]$-Basis. In (3.21) haben wir gesehen, dass man für den „Nulltest“ die beiden Bedingungen

(1) $v_{\mathfrak{P}}(\eta_i)$ für alle $\mathfrak{P}|p$ und $i = 1, 2, 3$,

[1]Der Fall G_v zyklisch und v unverzweigt tritt bei unseren $A4$-Erweiterungen nicht auf, da wir nur voll zerlegte Stellen zu S dazugenommen haben, wenn die verzweigten Stellen zur Erzeugung der Idealklassengruppe nicht genügten.

(2) $(\overline{\eta_1}, \overline{\eta_2}, \overline{\eta_3}) \in \mathrm{im}(\mu_p)$,

prüfen muss. Ebenso haben wir gesehen, dass im Falle $p \neq 2, 3$ die Torsionsuntergruppe von $K_0(\mathbb{Z}_p[A_4], \mathbb{Q}_p)$ trivial ist. Es genügt dann also die Bedingung (1) zu prüfen. Für $p \in 2, 3$ gibt Bley in [Ble, 2.3] explizite Kongruenzen an, die das Tripel (η_1, η_2, η_3) erfüllen muß, damit $(\overline{\eta_1}, \overline{\eta_2}, \overline{\eta_3}) \in \mathrm{im}(\mu_p)$ gilt. Sei dazu ζ_3 eine dritte primitive Einheitswurzel. Ist $p = 2$ dann gilt

$$(\overline{\eta_1}, \overline{\eta_2}, \overline{\eta_3}) \in \mathrm{im}(\mu_p) \Longleftrightarrow \eta_1 \mathrm{N}_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(\eta_2) \equiv \eta_3 \bmod 4.$$

Und für $p = 3$ gilt

$$(\overline{\eta_1}, \overline{\eta_2}, \overline{\eta_3}) \in \mathrm{im}(\mu_p) \Longleftrightarrow \eta_1 \equiv \eta_2 \bmod 1 - \zeta_3.$$

In der Spalte $\mathcal{Q}_{\mathrm{round}}$ stehen die algebraischen Zahlen, zu denen wir die berechneten gerundet haben (im Algorithmus 3.3.10 ist dies jeweils Schritt (c)) und mit denen im Algorithmus weiter gerechnet wurde. $\zeta_3 \mapsto e^{2\pi i/3}$ gibt die jeweilige Einbettung an.
Ab Polynom Nr. 61 haben wir die Klassenzahl und Klassengruppe mit der Bachkonstante berechnen lassen. Es wurden natürlich nur A_4-Erweiterungen getestet, die der Bedingung

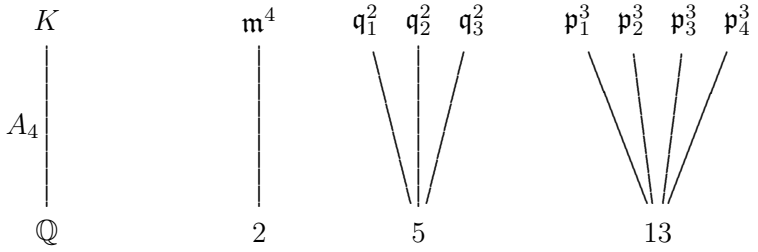
„Es gibt eine Stelle v_0 mit $G_{v_0} = G$“

genügen. Daher sind die Beispiele nicht durchgehend nummeriert.

Polynom Nr. 4

$f(x) = x^{12} - 6x^{11} - 30x^{10} + 182x^9 + 173x^8 - 1432x^7 + 628x^6 + 1472x^5 - 173x^4 - 650x^3 - 238x^2 - 30x - 1$

Signatur	d	S_f	h	Zeit
$(12, 0)$	$2^{18} \cdot 5^6 \cdot 13^8$	$\{2, 5, 13\}$	2	~ 5 min.

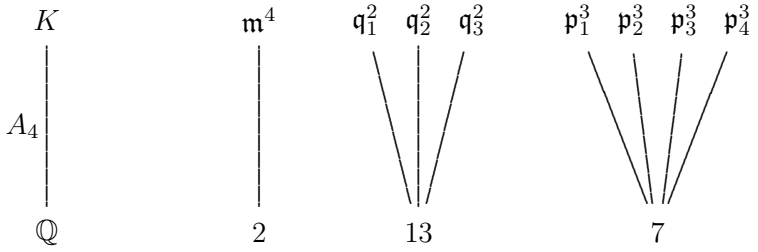


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$1.000000000000000000000000000000$	1
$0.499999999999999999999999999983$	$-\zeta_3$, Genauigkeit: 10^{-29}
$-0.866025403784438646763723170754i$	
$0.999999999999999999999999999961$	1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$-15.000000000000000000000000000000$	-15
$13.500000000000000000000000000000$	$-3\zeta_3 + 12$, Genauigkeit: 10^{-29}
$-2.598076211353315940291169512 26i$	
$72.999999999999999999999999972$	73
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$-424.000000000000000000000000000$	-424
$-16.000000000000000000000000000000$	$32\zeta_3$, Genauigkeit: 10^{-28}
$+27.712812921102036696439141 4641i$	
$-75775.999999999999999999999971$	75776

Polynom Nr. 7

$f(x) = x^{12} + 8x^{11} - 12x^{10} - 194x^9 - 210x^8 + 826x^7 + 1378x^6 - 366x^5 - 1927x^4 - 1424x^3 - 430x^2 - 50x - 1$

Signatur	d	S_f	h	Zeit
$(12, 0)$	$2^{18} \cdot 7^8 \cdot 13^6$	$\{2, 7, 13\}$	2	~ 4 min.

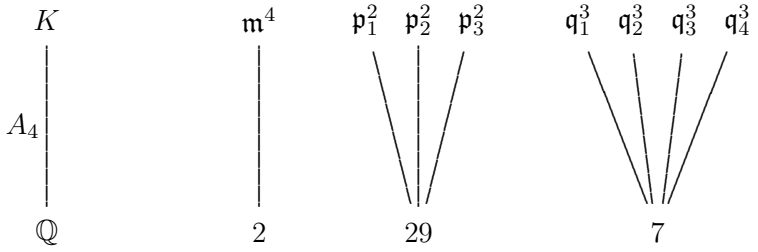


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$-1.000000000000000000000000000000$	-1
$0.500000000000000000000000000000$	$\zeta_3 + 1$, Genauigkeit: 10^{-29}
$+0.866025403784438646763723170751i$	
$-0.999999999999999999999999999983$	-1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$-17.000000000000000000000000000000$	-17
$-2.000000000000000000000000000000$	$-2\zeta_3 - 3$, Genauigkeit: 10^{-29}
$-1.732050807568877293527446341505i$	
$-90.999999999999999999999999999985$	-91
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$-67.000000000000000000000000000000$	-67
$-13.000000000000000000000000000000$	$2\zeta_3 - 12$, Genauigkeit: 10^{-28}
$+1.732050807568877293527446341505i$	
$-53535.999999999999999999999999991$	-53536

Polynom Nr. 17

$f(x) = x^{12} + 10x^{11} - 16x^{10} - 252x^9 + 250x^8 + 1350x^7 - 662x^6 - 2314x^5 + 137x^4 + 1364x^3 + 252x^2 - 196x - 49$

Signatur	d	S_f	h	Zeit
$(12, 0)$	$2^{18} \cdot 7^8 \cdot 29^6$	$\{2, 7, 29\}$	2	~ 8 min.

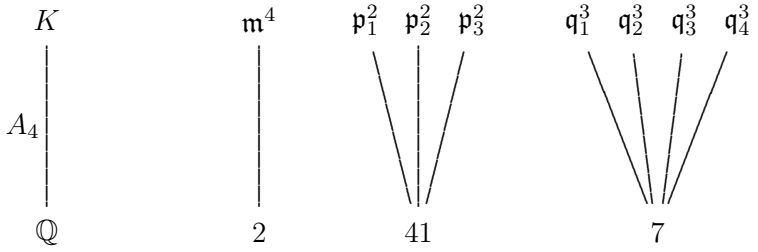


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$ $0.99999999999999999999999999998$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$ 1
$0.49999999999999999999999999998$ $+0.86602540378443864676372317085 6i$	$\zeta_3 + 1$, Genauigkeit: 10^{-27}
$-0.99999999999999999999999999979$	-1
$\mathbb{Z}_2[G]$-Basen $357.00000000000000000000000000$	$\mathbb{Z}_2[G]$-Basen 357
$201.00000000000000000000000027$ $-169.74097914174997476568974147 2i$	$-196\zeta_3 + 103$, Genauigkeit: 10^{-25}
$-37968590.999999999999999999992$	-37968591
$\mathbb{Z}_3[G]$-Basen $954.99999999999999999999999998$	$\mathbb{Z}_3[G]$-Basen 955
$535.00000000000000000000000071$ $-443.40500673763258714302623435i$	$-512\zeta_3 + 279$, Genauigkeit: 10^{-25}
$-563378632.00000000000000000088$	-563378633

Polynom Nr. 25

$f(x) = x^{12} + 2x^{11} - 116x^{10} - 398x^9 + 3315x^8 + 16950x^7 + 7696x^6 - 54388x^5 - 95878x^4 - 64268x^3 - 19770x^2 - 2650x - 125$

Signatur	d	S_f	h	Zeit
$(12, 0)$	$2^{18} \cdot 7^8 \cdot 41^6$	$\{2, 7, 41\}$	2	~ 22 min.

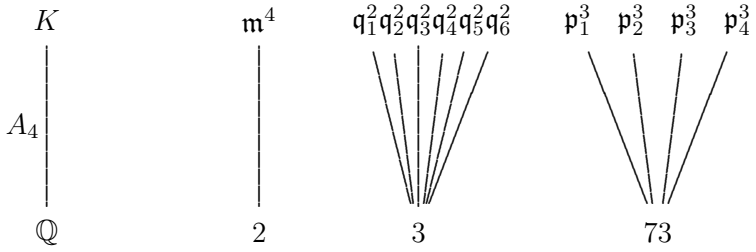


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$-0.99999999999999999999999999998$	-1
$0.99999999999999999999999999978$	1
$-827987638814259433381723079726i \cdot 10^{-30}$	
$-1.00000000000000000000000000002$	-1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$-17541.00000000000000000000000000$	-17541
$-3262.49999999999999999999999992$	$1333\zeta_3 - 2596$, Genauigkeit: 10^{-25}
$+1154.41186324465671613604298661i$	
$184096484307.000000000000000003$	184096484307
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$158156.00000000000000000000000000$	158156
$27231.49999999999999999999999994$	$7011\zeta_3 + 30737$, Genauigkeit: 10^{-22}
$+6071.70410593269935246046314979i$	
$-21047203381132.0000000000000003$	-21047203381132

Polynom Nr. 35

$f(x) = x^{12} - 6x^{11} - 78x^{10} + 364x^9 + 1566x^8 - 5796x^7 - 9968x^6 + 20706x^5 + 34197x^4 + 18x^3 - 14112x^2 - 3726x + 243$

Signatur	d	S_f	h	Zeit
$(12, 0)$	$2^{18} \cdot 3^6 \cdot 73^8$	$\{2, 3, 73\}$	2	~ 4 min.

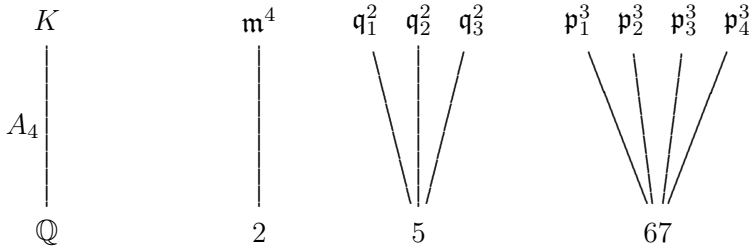


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$1.000000000000000000000000000000$	1
$5.000000000000000000000000000000$	ζ_3, Genauigkeit: 10^{-29}
$+0.866025403784438646763723170755i$	
$0.999999999999999999999999999965$	1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$1.000000000000000000000000000000$	1
$-0.500000000000000000000000000001$	ζ_3, Genauigkeit: 10^{-28}
$-5.448853807017499299706330099 76i$	
$-98.999999999999999999999999965$	99
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$11.000000000000000000000000000$	11
$-14.500000000000000000000000000$	$19\zeta_3 - 5$, Genauigkeit: 10^{-27}
$+16.454482671904334288510740244 4i$	
$89914.999999999999999999999968$	89915

Polynom Nr. 37

$f(x) = x^{12} + 6x^11 - 90x^{10} - 720x^9 + 1146x^8 + 20860x^7 + 34080x^6 - 133642x^5 - 473471x^4 - 364274x^3 + 199808x^2 + 282354x + 62631$

Signatur	d	S_f	h	Zeit
$(12, 0)$	$2^{18} \cdot 5^6 \cdot 67^8$	$\{2, 5, 67\}$	2	~ 4 min.

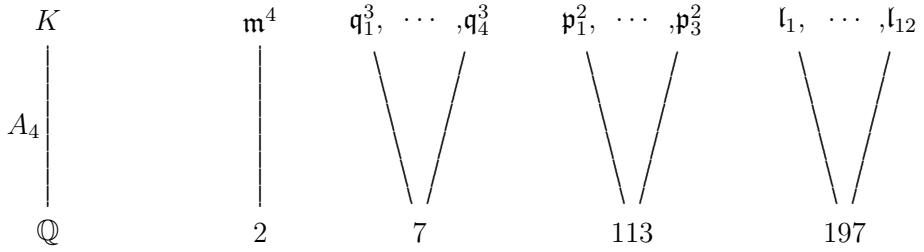


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$-0.99999999999999999999999999998$	-1
$0.99999999999999999999999999997$	1
$+5.954453719383761294524375986 21i \cdot 10^{-30}$	
$-1.00000000000000000000000000001$	-1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$0.99999999999999999999999999998$	1
$-0.50000000000000000000000000014$	$3\zeta_3 + 1$, Genauigkeit: 10^{-28}
$+2.59807621135331594029116951225i$	
$-5.00000000000000000000000000006$	-5
$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$-0.99999999999999999999999999998$	-1
$0.99999999999999999999999999997$	1
$+5.954453719383767612945243759862 1i \cdot 10^{-30}$	
$-1.00000000000000000000000000001$	-1

Polynom Nr. 39

$f(x) = x^{12} + 4x^{11} - 156x^{10} - 224x^9 + 6571x^8 + 9514x^7 - 109330x^6 - 215274x^5 + 609914x^4 + 1724388x^3 + 581644x^2 - 679042x - 8281$

Signatur	d	S_f	h	Zeit
$(12, 0)$	$2^{18} \cdot 7^8 \cdot 113^6$	$\{2, 7, 113, 197\}$	2	~ 14 min.

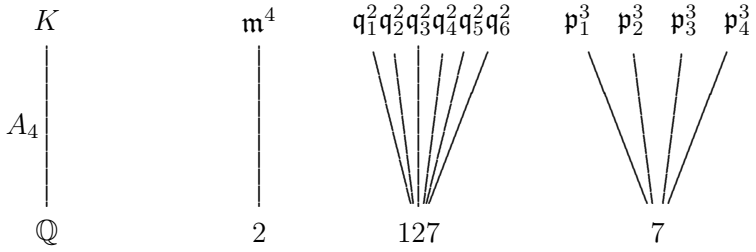


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$-1.000000000000000000000000000000$	-1
$0.999999999999999999999999999998$	1
$+4.710808061552998568378503186 19i \cdot 10^{-30}$	
$-1.000000000000000000000000000002$	-1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$-3.000000000000000000000000000000$	-3
$-2.999999999999999999999999999997$	$-4\zeta_3 - 5$, Genauigkeit: 10^{-28}
$-3.464101615137754587054892683 02i$	
$-7.000000000000000000000000000018$	-7
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$-37.000000000000000000000000000001$	-37
$-33.999999999999999999999999999998$	$-30\zeta_3 - 49$, Genauigkeit: 10^{-27}
$-25.980762113533159402911695122 7i$	
$-129787.000000000000000000000000003$	-129787

Polynom Nr. 41

$f(x) = x^{12} - 2x^{11} - 138x^{10} - 150x^9 + 6517x^8 + 24692x^7 - 70812x^6 - 619026x^5 - 1365066x^4 - 808056x^3 + 1108554x^2 + 1680616x + 575177$

Signatur	d	S_f	h	Zeit
$(12, 0)$	$2^{18} \cdot 7^8 \cdot 127^6$	$\{2, 7, 127\}$	1	~ 5 min.

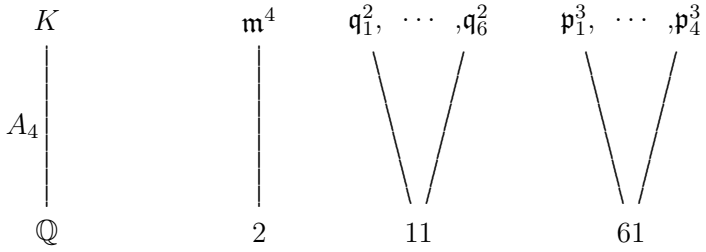


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$-1.000000000000000000000000000000$	-1
$0.499999999999999999999999999991$	$-\zeta_3$, Genauigkeit: 10^{-28}
$-0.866025403784438646763723170776i$	
$-1.000000000000000000000000000003$	-1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$-82798.999999999999999999999999$	-82799
$-6663.500000000000000000000000055$	$-29395\zeta_3 - 21361$,
$-25456.816744243574021619642604 6i$	Genauigkeit: 10^{-23}
$-41187964171237.000000000000011$	-41187964171237
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$-421489.000000000000000000000000$	-421489
$-33922.000000000000000000000028$	$-149636\zeta_3 - 108740$,
$-129588.577320688261347136480380i$	Genauigkeit: 10^{-23}
$-5433389545384784.00000000000014$	-5433389545384784

Polynom Nr. 50

$f(x) = x^{12} + 6x^{11} - 244x^{10} + 1074x^9 + 2363x^8 - 21394x^7 + 16840x^6 + 100568x^5 - 168294x^4 - 74812x^3 + 216938x^2 + 1550x - 57829$

Signatur	d	S_f	h	Zeit
$(12, 0)$	$2^{18} \cdot 11^6 \cdot 61^8$	$\{2, 11, 61\}$	1	~ 13 min.

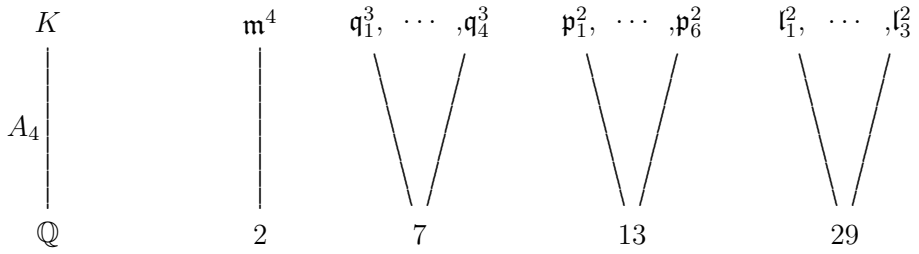


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$0.99999999999999999999999999999$	1
$-0.49999999999999999999999999994$	$-\zeta_3 - 1$, Genauigkeit: 10^{-28}
$-0.86602540378443864676372317076 0i$	
$1.00000000000000000000000000000$	1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$0.99999999999999999999999999999$	1
$-0.49999999999999999999999999994$	$-\zeta_3 - 1$, Genauigkeit: 10^{-28}
$-0.86602540378443864676372317076 0i$	
$93.00000000000000000000000000004$	93
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$49.99999999999999999999999999999$	50
$0.49999999999999999999999999994$	$\zeta_3 + 1$, Genauigkeit: 10^{-28}
$+0.86602540378443864676372317076 0i$	
$18590.00000000000000000000000001$	18590

Polynom Nr. 61

$f(x) = x^{12} - 2x^{11} - 354x^{10} - 1470x^9 + 31142x^8 + 302734x^7 + 792704x^6 - 484864x^5 - 3839975x^4 - 1097230x^3 + 2953552x^2 - 840840x + 42133$

Signatur	d	S_f	h	Zeit
$(12, 0)$	$2^{18} \cdot 7^8 \cdot 13^6 \cdot 29^6$	$\{2, 7, 13, 29\}$	16	$\sim$ 26 min.

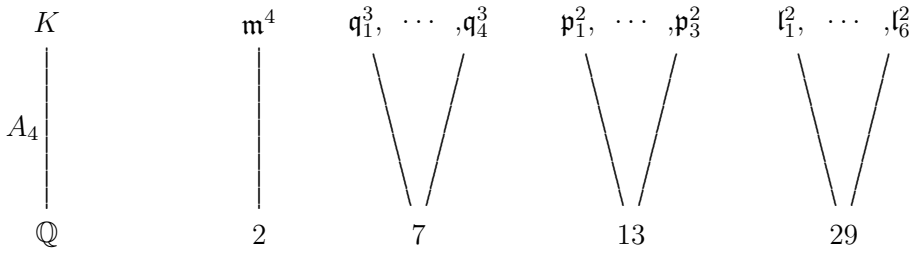


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$ $0.99999999999999999999999999991$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$ 1
$0.50000000000000000000000000125$ $+0.86602540378443864676372317071 8i$	$\zeta_3 + 1$, Genauigkeit: 10^{-27}
$-0.99999999999999999999999999979$	-1
$\mathbb{Z}_2[G]$-Basen $-42906.99999999999999999999999$	$\mathbb{Z}_2[G]$-Basen -42907
$13767.50000000000000000000015$ $+8538.144455910780618443546738 99i$	$9859\zeta_3 + 18697$, Genauigkeit: 10^{-22}
$2832083871019454.99999999999994$	2832083871019455
$\mathbb{Z}_3[G]$-Basen $-1415768.00000000000000000000000$	$\mathbb{Z}_3[G]$-Basen -1415768
$495597.99999999999999999999949$ $-532733.795087189864679410781122i$	$-615148\zeta_3 + 188024$, Genauigkeit: 10^{-21}
$-399069715912807210879.999999991$	$-39906971591280721088 0$

Polynom Nr. 62

$f(x) = x^{12} - 2x^{11} - 258x^{10} - 700x^9 + 22218x^8 + 160104x^7 - 223412x^6 - 6816482x^5 - 33566867x^4 - 80039450x^3 - 98196812x^2 - 52659418x - 4942441$

Signatur	d	S_f	h	Zeit
$(12, 0)$	$2^{18} \cdot 7^8 \cdot 13^6 \cdot 29^6$	$\{2, 7, 13, 29\}$	1	~ 28 min.

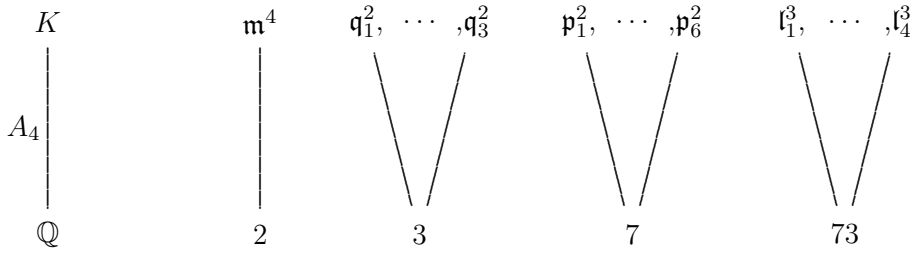


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$ $0.999999999999999999999999999999$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$ 1
$1.000000000000000000000000028$ $+4.055206608997820323134235254 18i \cdot 10^{-30}$	1
$0.999999999999999999999999999940$	1
$\mathbb{Z}_2[G]$-Basen $-55674.999999999999999999999999$	$\mathbb{Z}_2[G]$-Basen -55675
$-135.999999999999999999999999936$ $-122.97560733790287840448690314i$	$-142\zeta_3 - 207$, Genauigkeit: 10^{-24}
$367590159407670346.999999999978$	367590159407670347
$\mathbb{Z}_3[G]$-Basen $2248708.000000000000000000000000$	$\mathbb{Z}_3[G]$-Basen 2248708
$-880.999999999999999999999998844$ $-2249.933999031971604292152798 04i$	$-2598\zeta_3 - 2180$, Genauigkeit: 10^{-23}
$-9464907660817252640655.99999943$	$-946490766081725264065 6$

Polynom Nr. 66

$f(x) = x^{12} - 2x^{11} - 266x^{10} - 968x^9 + 15903x^8 + 116414x^7 + 65338x^6 - 1368358x^5 - 3579014x^4 + 455910x^3 + 12227712x^2 + 15849540x + 6337611$

Signatur	d	S_f	h	Zeit
$(12, 0)$	$2^{18} \cdot 3^6 \cdot 7^6 \cdot 73^8$	$\{2, 3, 7, 73\}$	8	~ 22 min.

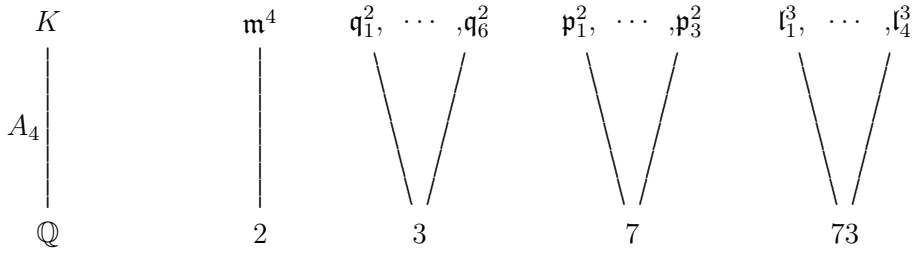


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$0.999999999999999999999999999999$	1
$-0.499999999999999999999999999974$ $+0.866025403784438646763723170771i$	ζ_3, Genauigkeit: 10^{-28}
$-1.000000000000000000000000000003$	1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$36.999999999999999999999999999$	37
$-36.500000000000000000000000064$ $-196.587766659067572815365159760i$	$-227\zeta_3 - 150$, Genauigkeit: 10^{-26}
$-412767205.000000000000000000011$	-412767205
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$-290.000000000000000000000000000$	-290
$379.000000000000000000000000036$ $+1075.603551500272992805441780 7i$	$1242\zeta_3 + 1000$, Genauigkeit: 10^{-25}
$-16464184712.000000000000000000004$	16464184712

Polynom Nr. 67

$f(x) = x^{12} - 220x^{10} + 17058x^8 - 593974x^6 + 9784993x^4 - 72293214x^2 + 190357209$

Signatur	d	S_f	h	Zeit
$(12, 0)$	$2^{18} \cdot 3^6 \cdot 7^6 \cdot 73^8$	$\{2, 3, 7, 73\}$	16	$\sim$ 16 min.

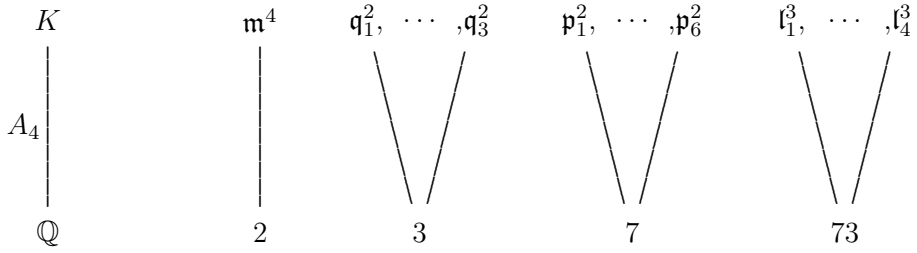


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$0.999999999999999999999999999999$	1
$0.499999999999999999999999999991$	$-\zeta_3$, Genauigkeit: 10^{-28}
$-0.866025403784438646763723170748i$	
$1.000000000000000000000000000008$	1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$0.999999999999999999999999999999$	1
$2.499999999999999999999999999999$	$-11\zeta_3 - 3$, Genauigkeit: 10^{-27}
$-9.526279441628825114400954878 24i$	
$17241449.000000000000000000000014$	17241449
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$10988.000000000000000000000000$	10988
$-103.000000000000000000000000028$	$1062\zeta_3 + 428$, Genauigkeit: 10^{-25}
$+919.718978819073842863074007335i$	
$-179139539445440.000000000000015$	-179139539445440

Polynom Nr. 68

$f(x) = x^{12} - 274x^{10} + 17839x^8 - 286332x^6 + 425007x^4 - 168210x^2 + 39697$

Signatur	d	S_f	h	Zeit
$(12, 0)$	$2^{18} \cdot 3^6 \cdot 7^6 \cdot 73^8$	$\{2, 3, 7, 73\}$	8	~ 14 min.

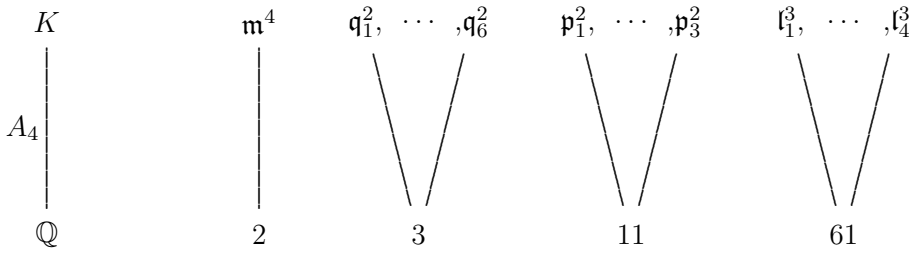


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$0.999999999999999999999999999999$	1
$-1.000000000000000000000000000000$	-1
$+7.686716279034387637856551685 17i \cdot 10^{-30}$	
$1.000000000000000000000000000015$	1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$227.000000000000000000000000000$	227
$126.500000000000000000000000000$	$165\zeta_3 + 209$, Genauigkeit: 10^{-27}
$+142.894191624432376716014323175i$	
$-141096249.000000000000000000022$	-141096249
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$757.999999999999999999999999999$	758
$-111.999999999999999999999999999$	$2022\zeta_3 + 899$, Genauigkeit: 10^{-25}
$+1751.10336645213494375624825127i$	
$137930752450.000000000000000021$	137930752450

Polynom Nr. 70

$f(x) = x^{12} - 8x^{11} - 408x^{10} + 3260x^9 + 7064x^8 - 110988x^7 + 242180x^6 + 211400x^5 - 1225932x^4 + 896560x^3 + 870328x^2 - 1245888x + 344952$

Signatur	d	S_f	h	Zeit
$(12, 0)$	$2^{18} \cdot 3^6 \cdot 11^6 \cdot 61^8$	$\{2, 3, 11, 61\}$	8	$\sim$ 15 min.

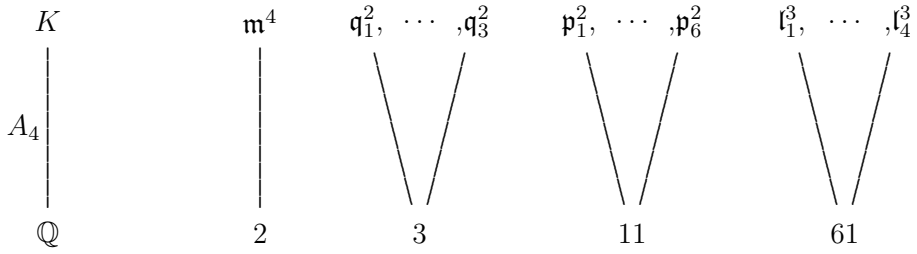


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$-1.000000000000000000000000000000$	-1
$0.499999999999999999999999999991$	$-\zeta_3$, Genauigkeit: 10^{-28}
$-0.866025403784438646763723170776i$	
$-1.000000000000000000000000000003$	-1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$-82798.999999999999999999999999$	-82799
$-6663.500000000000000000000000055$	$-29395\zeta_3 - 21361$, Genauigkeit: 10^{-24}
$-25456.816744243574021619642604 6i$	
$-41187964171237.000000000000011$	-41187964171237
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$-421489.000000000000000000000000$	-421489
$-33922.000000000000000000000028$	$-149636\zeta_3 - 108740$, Genauigkeit: 10^{-23}
$-129588.577320688261347136480380i$	
$-5433389545384784.00000000000014$	-5433389545384784

Polynom Nr. 71

$f(x) = x^{12} - 188x^{10} + 12066x^8 - 331142x^6 + 3805729x^4 - 15471918x^2 + 4052169$

Signatur	d	S_f	h	Zeit
$(12, 0)$	$2^{18} \cdot 3^6 \cdot 11^6 \cdot 61^8$	$\{2, 3, 11, 61\}$	16	$\sim$ 15 min.

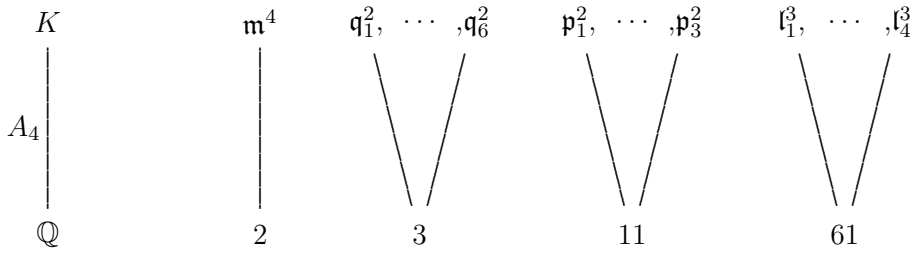


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$1.000000000000000000000000000000$	1
$0.500000000000000000000000000002$	$\zeta_3 + 1$, Genauigkeit: 10^{-29}
$+0.866025403784438646763723170755i$	
$1.000000000000000000000000000013$	1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$-1629.000000000000000000000000000$	-1629
$7.500000000000000000000000000002$	$-5\zeta_3 + 5$, Genauigkeit: 10^{-28}
$-4.330127018922193233818615853 79i$	
$-59875335.000000000000000000079$	-59875335
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$-35332.000000000000000000000000$	-35332
$8.000000000000000000000000000005$	$56\zeta_3 + 36$, Genauigkeit: 10^{-27}
$+48.497422611928564218768497562 3i$	
$7452305707016.00000000000000097$	7452305707016

Polynom Nr. 72

$f(x) = x^{12} + 8x^{11} - 646x^{10} + 6194x^9 + 9311x^8 - 460078x^7 + 2806096x^6 - 6640080x^5 + 2516142x^4 + 11455578x^3 - 8113770x^2 - 3142800x + 1609875$

Signatur	d	S_f	h	Zeit
$(12, 0)$	$2^{18} \cdot 3^6 \cdot 11^6 \cdot 61^8$	$\{2, 3, 11, 61\}$	8	~ 19 min.

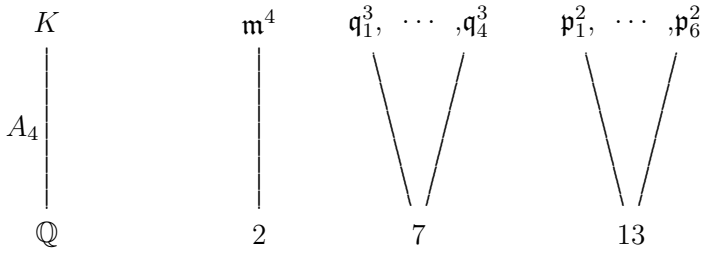


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$1.000000000000000000000000000000$	1
$0.499999999999999999999999999998$	$\zeta_3 + 1$, Genauigkeit: 10^{-29}
$+0.866025403784438646763723170755i$	
$1.000000000000000000000000000003$	1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$-809.000000000000000000000000000$	-809
$1810.000000000000000000000000000$	$666\zeta_3 + 2143$, Genauigkeit: 10^{-26}
$+576.772918920436138744639631728i$	
$144354607113.000000000000000004$	144354607113
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$-48603.999999999999999999999999$	-48604
$113618.000000000000000000000000$	$25264\zeta_3 + 126250$, Genauigkeit: 10^{-24}
$+21879.265801210057971838702186 3i$	
$-3814229326907734208.00000000010$	-3814229326907734208

Polynom Nr. 102

$f(x) = x^{12} - 46x^9 + 434x^8 - 1162x^7 + 1942x^6 - 1246x^5 + 1561x^4 - 356x^3 + 2450x^2 + 1050x + 875$

Signatur	d	S_f	h	Zeit
$(0, 6)$	$2^{18} \cdot 7^8 \cdot 13^6$	$\{2, 7, 13\}$	16	~ 4 min.

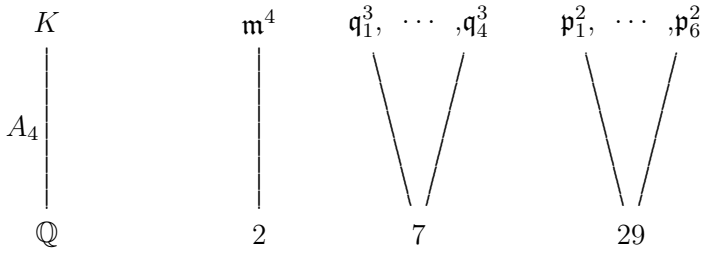


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$-1.000000000000000000000000000000$	-1
$0.999999999999999999999999999994$	1
$+3.731480877898780179538625290 10i \cdot 10^{-30}$	
$1.000000000000000000000000000002$	1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$-1.000000000000000000000000000000$	-1
$0.499999999999999999999999999994$	$\zeta_3 + 1$, Genauigkeit: 10^{-29}
$+0.866025403784438646763723170750i$	
$-1.000000000000000000000000000002$	-1
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$-34.000000000000000000000000000000$	-34
$22.999999999999999999999999999996$	$78\zeta_3 + 62$, Genauigkeit: 10^{-27}
$+67.549981495186214447570407 3183i$	
$104480.000000000000000000000002$	104480

Polynom Nr. 107

$f(x) = x^{12} - 2x^{11} + 62x^{10} + 44x^9 + 1486x^8 - 172x^7 + 2548x^6 + 4216x^5 + 416x^4 - 3544x^3 + 1488x^2 + 1152x + 216$

Signatur	d	S_f	h	Zeit
$(0, 6)$	$2^{18} \cdot 7^8 \cdot 29^6$	$\{2, 7, 29\}$	16	~ 6 min.

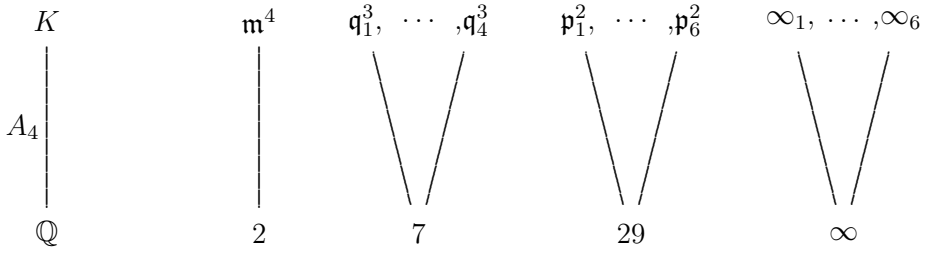


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$ $-0.99999999999999999999999999998$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$ -1
$0.50000000000000000000000000003$ $+0.86602540378443864676372317075 4i$	$\zeta_3 + 1$, Genauigkeit: 10^{-28}
$-1.00000000000000000000000000003$	-1
$\mathbb{Z}_2[G]$-Basen $-0.99999999999999999999999999997$	$\mathbb{Z}_2[G]$-Basen -1
$0.49999999999999999999999999994$ $-2.59807621135331594029116951226i$	$-3\zeta_3 - 1$, Genauigkeit: 10^{-29}
$-43.00000000000000000000000000014$	-43
$\mathbb{Z}_3[G]$-Basen $-1.99999999999999999999999999999$	$\mathbb{Z}_3[G]$-Basen -2
$43.00000000000000000000000000001$ $-1.73205080756887729352744634161i$	$-2\zeta_3 + 42$, Genauigkeit: 10^{-27}
$-290104.00000000000000000000000010$	-290104

Polynom Nr. 108

$f(x) = x^{12} + 94x^9 + 938x^8 + 2562x^7 + 2446x^6 - 4634x^5 - 4319x^4 + 6868x^3 + 7938x^2 - 12474x + 5103$

Signatur	d	S_f	h	Zeit
$(0, 6)$	$2^{18} \cdot 7^8 \cdot 29^6$	$\{2, 7, 29\}$	16	~ 6 min.

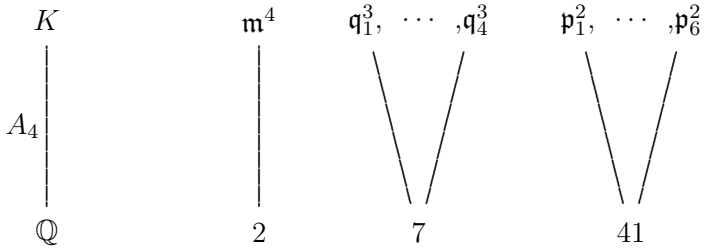


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$ $0.99999999999999999999999999998$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$ 1
$0.50000000000000000000000000000$ $-0.86602540378443864676372317075 7i$	$-\zeta_3$, Genauigkeit: 10^{-29}
$-0.99999999999999999999999999978$	-1
$\mathbb{Z}_2[G]$-Basen $-9803.000000000000000000000000000$	$\mathbb{Z}_2[G]$-Basen -9803
$47.500000000000000000000000009$ $-317.831322318888898336228640366 8i$	$-367\zeta_3 - 136$, Genauigkeit: 10^{-24}
$56226972714704.9999999999999987$	56226972714705
$\mathbb{Z}_3[G]$-Basen $78400.000000000000000000000000$	$\mathbb{Z}_3[G]$-Basen 78400
$-15866.000000000000000000000000000$ $-40952.609294158534728162941298 8i$	$-47288\zeta_3 - 39510$, Genauigkeit: 10^{-24}
$6004779708806403199.99999999986$	6004779708806403200

Polynom Nr. 109

$f(x) = x^{12} + 2x^{11} + 10x^{10} - 202x^9 + 697x^8 - 760x^7 + 14108x^6 - 79504x^5 + 202371x^4 - 290802x^3 + 249282x^2 - 121342x + 26531$

Signatur	d	S_f	h	Zeit
$(0, 6)$	$2^{18} \cdot 7^8 \cdot 41^6$	$\{2, 7, 41\}$	128	~ 5 min.

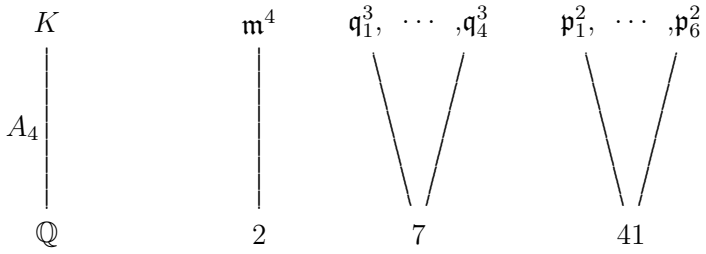


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$-0.99999999999999999999999999998$	-1
$0.49999999999999999999999999984$	$-\zeta_3$, Genauigkeit: 10^{-28}
$-0.86602540378443864676372317076 2i$	
$-1.00000000000000000000000000005$	-1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$40.99999999999999999999999999$	41
$9.49999999999999999999999999994$	$-3\zeta_3 + 8$, Genauigkeit: 10^{-27}
$-2.59807621135331594029116951243i$	
$1128153.00000000000000000000005$	1128153
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$981.99999999999999999999999998$	982
$21.99999999999999999999999984$	$-100\zeta_3 - 28$, Genauigkeit: 10^{-27}
$-86.60254037844386467637231707 57i$	
$150138608.00000000000000000007$	150138608

Polynom Nr. 110

$f(x) = x^{12} + 56x^{10} - 214x^9 + 2114x^8 - 5026x^7 + 19050x^6 - 14238x^5 + 46809x^4 + 148x^3 + 49686x^2 + 7098x + 15379$

Signatur	d	S_f	h	Zeit
$(0, 6)$	$2^{18} \cdot 7^8 \cdot 41^6$	$\{2, 7, 41\}$	16	~ 5 min.

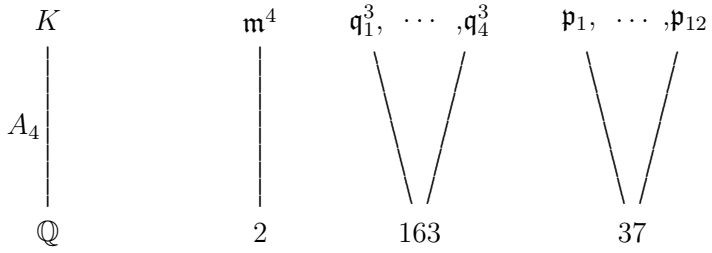


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$0.99999999999999999999999999998$	1
$0.50000000000000000000000000001$	$-\zeta_3$, Genauigkeit: 10^{-29}
$-0.86602540378443864676372317075 4i$	
$0.99999999999999999999999999980$	1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$0.99999999999999999999999999998$	1
$0.50000000000000000000000000001$	ζ_3, Genauigkeit: 10^{-29}
$+0.86602540378443864676372317075 3i$	
$-2.99999999999999999999999999994$	-3
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$-31.99999999999999999999999999999$	-421489
$16.00000000000000000000000000000$	$-60\zeta_3 - 14$, Genauigkeit: 10^{-27}
$-51.96152422706631880582339024 52i$	
$2959.99999999999999999999999994$	2960

Polynom Nr. 114

$f(x) = x^{12} + 6x^{10} + 655x^8 + 2580x^6 + 3903x^4 + 2662x^2 + 625$

Signatur	d	S_f	h	Zeit
$(0, 6)$	$2^{18} \cdot 163^8$	$\{2, 163, 37\}$	64	~ 4 min.

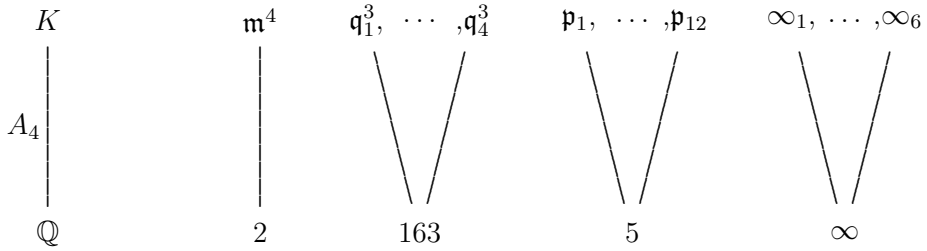


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$-1.000000000000000000000000000000$	1
$-0.500000000000000000000000000002$	$-\zeta_3 - 1$, Genauigkeit: 10^{-29}
$-0.866025403784438646763723170750i$	
$-1.000000000000000000000000000003$	1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$-1.000000000000000000000000000000$	-1
$1.999999999999999999999999999999$	$-2\zeta_3 + 1$, Genauigkeit: 10^{-28}
$-1.732050807568877293527446341 51i$	
$41.000000000000000000000000000012$	41
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$-23.000000000000000000000000000000$	-23
$26.499999999999999999999999999998$	$-47\zeta_3 + 3$, Genauigkeit: 10^{-27}
$-40.703193977868616397894989025 5i$	
$406327.000000000000000000000000012$	406327

Polynom Nr. 115

$f(x) = x^{12} + 34x^{10} + 205x^8 + 72650x^6 + 1170x^4 + 1296x^2 + 729$

Signatur	d	S_f	h	Zeit
$(0, 6)$	$2^{18} \cdot 163^8$	$\{2, 163, 5\}$	128	~ 3 min.

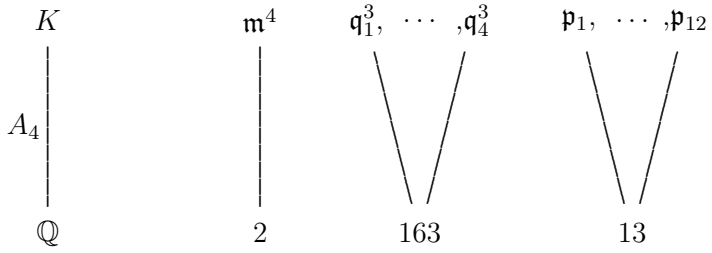


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$-1.000000000000000000000000000$	-1
$0.499999999999999999999999985$	$-\zeta_3$, Genauigkeit: 10^{-27}
$-0.866025403784438646763723170804i$	
$0.999999999999999999999999977$	-1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$-1469.000000000000000000000000$	-1469
$-609.499999999999999999999893$	$3925\zeta_3 + 1353$, Genauigkeit: 10^{-24}
$+3399.149709853921688547613445 35i$	
$2714192044834.9999999999999994$	2714192044835
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$-4190.000000000000000000000000$	-4190
$-1735.999999999999999999999969$	$11194\zeta_3 + 3861$, Genauigkeit: 10^{-24}
$+9694.288369963006211873117173 82i$	
$62962987478749.9999999999999985$	62962987478750

Polynom Nr. 116

$f(x) = x^{12} - 32x^{10} + 450x^8 - 1926x^6 - 12551x^4 + 159414x^2 + 26569$

Signatur	d	S_f	h	Zeit
$(0, 6)$	$2^{18} \cdot 163^8$	$\{2, 163, 13\}$	128	~ 6 min.

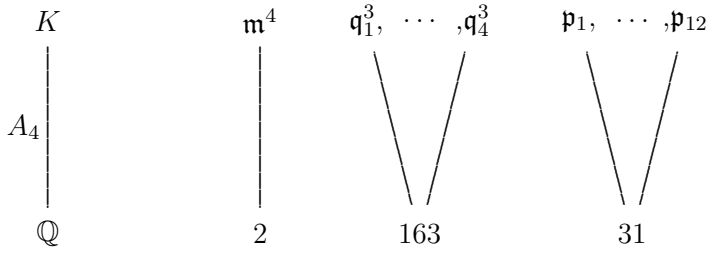


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$ $0.99999999999999999999999999998$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$ 1
$0.49999999999999999999999999916$ $-0.86602540378443864676372317072 7i$	$-\zeta_3$, Genauigkeit: 10^{-28}
$-1.00000000000000000000000000001$	1
$\mathbb{Z}_2[G]$-Basen $2797.00000000000000000000000000$	$\mathbb{Z}_2[G]$-Basen 2797
$854.49999999999999999999999966$ $+352.47233934026652923283533042 2i$	$407\zeta_3 + 1058$, Genauigkeit: 10^{-25}
$127964408523.000000000000000001$	127964408523
$\mathbb{Z}_3[G]$-Basen $8218.99999999999999999999999999$	$\mathbb{Z}_3[G]$-Basen 8219
$2509.99999999999999999999999990$ $+1034.03433211861974423588546566$	$1194\zeta_3 + 3107$, Genauigkeit: 10^{-24}
$3243289135537.00000000000000003$	3243289135537

Polynom Nr. 117

$f(x) = x^{12} - 6x^{11} + 46x^{10} - 166x^9 + 541x^8 - 1736x^7 + 6636x^6 - 9734x^5 + 7038x^4 + 812x^3 + 386x^2 + 28x + 1$

Signatur	d	S_f	h	Zeit
$(0, 6)$	$2^{18} \cdot 163^8$	$\{2, 163, 31\}$	512	~ 5 min.

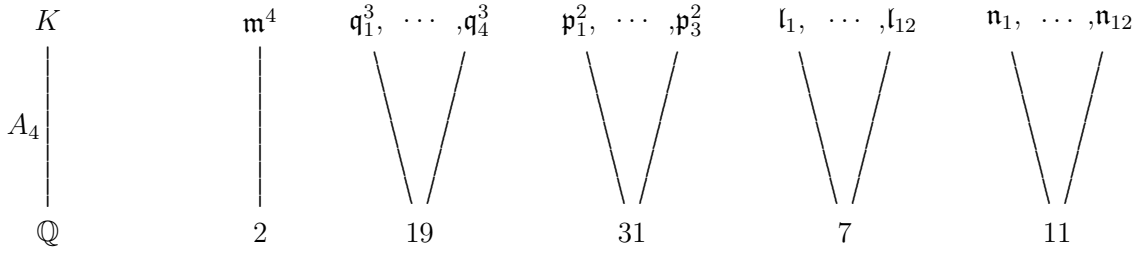


$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$0.999999999999999999999999999999$	1
$-0.499999999999999999999999999992$	ζ_3, Genauigkeit: 10^{-29}
$+0.866025403784438646763723170751i$	
$0.999999999999999999999999999998$	1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$13.000000000000000000000000000$	13
$-30.499999999999999999999999998$	$-\zeta_3 - 31$, Genauigkeit: 10^{-27}
$-866025403784438646763723170560i$	
43379	43379
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$699.999999999999999999999999$	700
$159.999999999999999999999999$	$20\zeta_3 + 170$, Genauigkeit: 10^{-26}
$17.320508075688772935274463413 9i$	
$-728573631.99999999999999999$	-728573632

Polynom Nr. 120

$f(x) = x^{12} - 116x^{10} + 5790x^8 - 94146x^6 - 1555967x^4 + 76076418x^2 + 16999129$

Signatur	d	S_f	h	Zeit
$(0, 6)$	$2^{18} \cdot 19^8 \cdot 31^6$	$\{2, 19, 31, 7, 11\}$	128	~ 63 min.



$\mathcal{Q}_{\text{approx}}$	$\mathcal{Q}_{\text{round}} : \zeta_3 \mapsto e^{2\pi i/3}$
$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$	$\mathbb{Z}_p[G]$-Basen, $p \neq 2, 3$
$1.000000000000000000000000000$	1
$0.500000000000000000000000000185$	$\zeta_3 + 1$, Genauigkeit: 10^{-27}
$-0.866025403784438646763723170693i$	
$0.999999999999999999999999999982$	1
$\mathbb{Z}_2[G]$-Basen	$\mathbb{Z}_2[G]$-Basen
$229.000000000000000000000000000$	229
$261.499999999999999999999999674$	$-2045\zeta_3 - 761$, Genauigkeit: 10^{-24}
$-1771.021950739177032631813884 31i$	
$12470898.999999999999999999999998$	-41187964171237
$\mathbb{Z}_3[G]$-Basen	$\mathbb{Z}_3[G]$-Basen
$35383.999999999999999999999999$	35384
$90350.000000000000000000000222$	$113184\zeta_3 + 146942$, Genauigkeit: 10^{-22}
$+98020.219301937903795305243345 2i$	
$3847557303487.99999999999999993$	3847557303488

Literaturverzeichnis

[AT68] E. Artin und J. Tate, *Class field theory*, W. A. Benjamin, Inc., New York-Amsterdam (1968).

[BB03] W. Bley und D. Burns, *Equivariant epsilon constants, discriminants and étale cohomology*, Proc. London Math. Soc. (3), **Bd. 87** (3), 545–590 (2003).

[BB05] Manuel Breuning und David Burns, *Additivity of Euler characteristics in relative algebraic K-groups*, Homology, Homotopy Appl., **Bd. 7** (3), 11–36 (electronic) (2005).

[BB07] Manuel Breuning und David Burns, *Leading terms of Artin L-functions at $s = 0$ and $s = 1$*, Compos. Math., **Bd. 143** (6), 1427–1464 (2007).

[BB08] Werner Bley und Manuel Breuning, *Exact algorithms for p-adic fields and epsilon constant conjectures*, Illinois J. Math., **Bd. 52** (3), 773–797 (2008).

[BF01] D. Burns und M. Flach, *Tamagawa numbers for motives with (non-commutative) coefficients*, Doc. Math., **Bd. 6**, 501–570 (electronic) (2001).

[BG03] D. Burns und C. Greither, *On the equivariant Tamagawa number conjecture for Tate motives*, Invent. Math., **Bd. 153** (2), 303–359 (2003).

[BJ] Werner Bley und Henri Johnston, *Computing generators of free modules over orders in group algebras II*, preprint 2010, 26 Seiten, erscheint in Math.Comp.

[BK90] Spencer Bloch und Kazuya Kato, *L-functions and Tamagawa numbers of motives*, in *The Grothendieck Festschrift, Vol. I*, Bd. 86 von *Progr. Math.*, S. 333–400, Birkhäuser Boston, Boston, MA (1990).

[Ble] W. Bley, *Numerical evidence for the equivariant Birch and Swinnerton-Dyer conjecture*, preprint 2010, 44 Seiten, erscheint in Exp.Math.

[Ble03] W. Bley, *Numerical evidence for a conjectural generalization of Hilbert's Theorem 132*, LMS J. Comput. Math., **Bd. 6**, 68–88 (electronic) (2003), with an appendix by D. Kusnezow.

[Ble06] W. Bley, *Equivariant Tamagawa number conjecture for abelian extensions of a quadratic imaginary field*, Doc. Math., **Bd. 11**, 73–118 (electronic) (2006).

[Bre04] Breuning, M., *Equivariant epsilon constants for Galois extensions of number fields and p-adic fields*, Dissertation, King's College London (2004), `http://www.mth.kcl.ac.uk/staff/m_breuning.html`.

[Bro94] Kenneth S. Brown, *Cohomology of groups*, Bd. 87 von *Graduate Texts in Mathematics*, Springer-Verlag, New York (1994), corrected reprint of the 1982 original.

[Bur01] D. Burns, *Equivariant Tamagawa numbers and Galois module theory I*, Compositio Math., (129), 203 – 237 (2001).

[Bur03] David Burns, *Equivariant Tamagawa numbers and refined abelian Stark conjectures*, J. Math. Sci. Univ. Tokyo, **Bd. 10** (2), 225–259 (2003).

[Bur04] David Burns, *Equivariant Whitehead torsion and refined Euler characteristics*, in *Number theory*, Bd. 36 von *CRM Proc. Lecture Notes*, S. 35–59, Amer. Math. Soc., Providence, RI (2004).

[BW09] W. Bley und M.J. Wilson, *Computations in relative algebraic K-groups*, LMS Journal of Computation and Mathematics, S. 166 – 194 (2009).

[Chi83] T. Chinburg, *On the Galois structure of algebraic integers and S-units*, Invent. Math., **Bd. 74** (3), 321–349 (1983).

[Chi85] Ted Chinburg, *Exact sequences and Galois module structure*, Ann. of Math. (2), **Bd. 121** (2), 351–376 (1985).

[Chi89] Ted Chinburg, *The analytic theory of multiplicative Galois structure*, Mem. Amer. Math. Soc., **Bd. 77** (395), iv+158 (1989).

[Coh93] Henri Cohen, *A course in computational algebraic number theory*, Bd. 138 von *Graduate Texts in Mathematics*, Springer-Verlag, Berlin (1993).

[Coh00] Henri Cohen, *Advanced topics in computational number theory*, Bd. 193 von *Graduate Texts in Mathematics*, Springer-Verlag, New York (2000).

[CR81] C.W. Curtis und I. Reiner, *Methods of Representation Theory. Vol. I*, John Wiley and Sons (1981).

[CR87] C.W. Curtis und I. Reiner, *Methods of Representation Theory. Vol. II*, John Wiley and Sons (1987).

[Deb11] Debeerst, Ruben, *Algorithms for Tamagawa Number Conjectures*, Dissertation, University of Kassel (2011), to appear.

[Dok04] Tim Dokchitser, *Computing special values of motivic L-functions*, Experiment. Math., **Bd. 13** (2), 137–149 (2004).

[Fla04] Matthias Flach, *The equivariant Tamagawa number conjecture: a survey*, in *Stark's conjectures: recent work and new directions*, Bd. 358 von *Contemp. Math.*, S. 79–125, Amer. Math. Soc., Providence, RI (2004), with an appendix by C. Greither.

[Fon92] Jean-Marc Fontaine, *Valeurs spéciales des fonctions L des motifs*, Astérisque, (206), Exp. No. 751, 4, 205–249 (1992), séminaire Bourbaki, Vol. 1991/92.

[FPR94] Jean-Marc Fontaine und Bernadette Perrin-Riou, *Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L*, in *Motives (Seattle, WA, 1991)*, Bd. 55 von *Proc. Sympos. Pure Math.*, S. 599–706, Amer. Math. Soc., Providence, RI (1994).

[Gei03] Geißler, K., *Berechnung von Galoisgruppen über Zahl- und Funktionenkörpern*, Dissertation, TU Berlin (2003), http://www.math.tu-berlin.de/ kant/publications/diss/geissler.pdf.

[GK] K. Geißler und J. Klüners, *The determination of Galois Groups*, J. Symbolic Comp., (30).

[GRW99] K. W. Gruenberg; J. Ritter und A. Weiss, *A local approach to Chinburg's root number conjecture*, Proc. London Math. Soc. (3), **Bd. 79** (1), 47–80 (1999).

[HS71] Peter John Hilton und Urs Stammbach, *A course in homological algebra*, Springer-Verlag, New York (1971), graduate Texts in Mathematics, Vol. 4.

[Lor97] F. Lorenz, *Einführung in die Algebra II*, Spektrum, Heidelberg Berlin Oxford (1997).

[Mat01] Keith Matthews, *Short solutions of $AX = B$ using a LLL-based Hermite normal form algorithm* (2001), `http://www.numbertheory.org/notes.html`.

[Nak57] Tadasi Nakayama, *On modules of trivial cohomology over a finite group. II. Finitely generated modules*, Nagoya Math. J., **Bd. 12**, 171–176 (1957).

[Nav06] Tejaswi Navilarekallu, *On the equivariant Tamagawa number conjecture for A_4-extensions of number fields*, J. Number Theory, **Bd. 121** (1), 67–89 (2006).

[Neu69] Jürgen Neukirch, *Klassenkörpertheorie*, Bibliographisches Institut, Mannheim (1969), b. I-Hochschulskripten, 713/713a*.

[Neu92] J. Neukirch, *Algebraische Zahlentheorie*, Springer, Berlin Heidelberg New York (1992).

[NSW08] Jürgen Neukirch; Alexander Schmidt und Kay Wingberg, *Cohomology of number fields*, Bd. 323 von *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*, Springer-Verlag, Berlin, zweite Aufl. (2008).

[RW02] Jürgen Ritter und Alfred Weiss, *Toward equivariant Iwasawa theory*, Manuscripta Math., **Bd. 109** (2), 131–146 (2002).

[Ser] Jean-Pierre Serre, *Local fields*, Bd. 67 von *Graduate Texts in Mathematics*.

[Sta73] Richard P. Stauduhar, *The determination of Galois groups*, Math. Comp., **Bd. 27**, 981–996 (1973).

[Swa68] R. G. Swan, *Algebraic K-theory*, Lecture Notes in Mathematics, No. 76, Springer-Verlag, Berlin (1968).

[Tat66] J. Tate, *The cohomology groups of tori in finite Galois extensions of number fields*, Nagoya Math. J., **Bd. 27**, 709–719 (1966).

[Tat84] John Tate, *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$*, Bd. 47 von *Progress in Mathematics*, Birkhäuser Boston Inc., Boston, MA (1984), lecture notes edited by Dominique Bernardi and Norbert Schappacher.

[Was97] Lawrence C. Washington, *Introduction to cyclotomic fields*, Bd. 83 von *Graduate Texts in Mathematics*, Springer-Verlag, New York, zweite Aufl. (1997).

Erklärung

Hiermit versichere ich, dass ich die vorliegende Dissertation selbstständig und ohne unerlaubte Hilfe angefertigt und andere als die in der Dissertation angegebenen Hilfsmittel nicht benutzt habe. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder unveröffentlichten Schriften entnommen sind, habe ich als solche kenntlich gemacht. Kein Teil dieser Arbeit ist in einem anderen Promotions- oder Habilitationsverfahren verwendet worden.

Dörthe Janssen
Kassel, im Februar 2010