Algorithms for Tamagawa Number Conjectures

DISSERTATION

zur Erlangung des akademischen Grades eines
Doktors der Naturwissenschaften (Dr. rer. nat.)

im Fachbereich Mathematik
und Naturwissenschaften
der Universität Kassel

vorgelegt von
Ruben Pieter Hubert Debeerst
aus Lingen (Ems)

im Februar 2011

Tag der Disputation
13. Mai 2011

Erstgutachter
Prof. Dr. Werner Bley
Universität Kassel

Zweitgutachter
Prof. Dr. Cornelius Greither
Universität der Bundeswehr München

Ruben Pieter Hubert Debeerst
Institut für Mathematik
Fachbereich Mathematik und Naturwissenschaften
Universität Kassel
Heinrich Plett Str. 40
34132 Kassel

debeerst@mathematik.uni-kassel.de

Danksagung

Zuerst möchte ich mich ganz besonders bei Prof. Dr. Werner Bley für seine hervorragende Betreuung bei meiner Promotion bedanken. Die regelmäßigen Treffen und die vielen hilfreichen Diskussionen waren eine große Unterstützung bei der Entstehung dieser Arbeit.

Herrn Prof. Dr. Cornelius Greither danke ich für die Übernahme des Zweitgutachtens und sein Interesse an dieser Arbeit. Darüber hinaus möchte ich mich bei Dr. Manuel Breuning für seine Einladung an das King's College in London bedanken. Unsere Erörterungen gaben bei der Entwicklung der Algorithmen für die Vermutung an der Stelle 1 wichtige Impulse. Auch den Mitarbeitern und Professoren am Institut für Mathematik der Universität Kassel gilt mein Dank für die gute Atmosphäre bei der täglichen Arbeit.

In den Phasen, in denen es mit der Arbeit mal nicht so gut voran ging, konnte ich immer auf die Unterstützung und Aufmunterung meiner Familie und insbesondere meiner Frau Janine zählen. Dafür danke ich Euch ganz besonders.

Ruben Debeerst
Kassel, im Mai 2011

Zusammenfassung

Ein bekanntes Resultat für einen Zahlkörper K ist die *Klassenzahlformel*. Sie stellt einen analytischen Term – das Residuum der Dedekindschen Zetafunktion $\zeta_K(s)$ bei $s = 1$ – in Relation zu verschiedenen algebraischen Invarianten, darunter die absolute Diskriminante, den Regulator und die Klassenzahl von K. Eine weitere Formulierung der Klassenzahlformel verwendet den führenden Koeffizienten der Laurentreihenentwicklung von $\zeta_K(s)$ bei $s = 0$. Zusätzlich hängen beide Formulierungen durch die Funktionalgleichung von $\zeta_K(s)$ zusammen, welche $\zeta_K(1-s)$ und $\zeta_K(s)$ in Relation setzt.[1]

Dieser Zusammenhang wird in verschiedenen Vermutungen verallgemeinert und verfeinert. Eine dieser Vermutungen ist die *äquivariante Tamagawazahlvermutung* von Burns und Flach [BF01]. Galoiserweiterungen $L|K$ von Zahlkörpern, mit denen wir uns in dieser Arbeit im Besonderen beschäftigen, bilden einen Spezialfall dieser sehr allgemeinen Vermutung, und zwar den Spezialfall des so genannten Tate-Motivs. Flach gibt in [Fla04] einen Überblick über diese Tamagawazahlvermutungen und verwandte Resultate, für den wichtigen Spezialfall von Zahlkörpererweiterungen existieren jedoch auch explizite Formulierungen [BlB03, BrB07].

Im Fall einer Galoiserweiterung $L|K$ von Zahlkörpern betrachten wir die *vollständige Artinsche L-Reihe* $\Lambda_{L|K}(\chi, s)$ zu einem Charakter χ der Galoisgruppe $G = \mathrm{Gal}(L|K)$ und die äquivariante Artinsche L-Reihe $\Lambda_{L|K}(s) = \big(\Lambda_{L|K}(\chi, s)\big)_\chi$, welche alle Charaktere vereint. Die äquivariante Tamagawazahlvermutung bei $s = 0$ stellt eine Verbindung zwischen dem führenden Koeffizienten $\zeta^*_{L|K}(0)$ der Laurentreihenentwicklung von $\Lambda_{L|K}(s)$ bei $s = 0$ und algebraischen Invarianten der Erweiterung $L|K$ her. Diese Invarianten werden unter anderem von *Tates kanonischer Klasse* abgeleitet, welche Tate in [Tat66] definiert.

In der äquivarianten Tamagawazahlvermutung bei $s = 1$ wird gleichermaßen eine Relation zwischen dem führenden Koeffizienten $\zeta^*_{L|K}(1)$ der Reihenentwicklung von $\Lambda_{L|K}(s)$ bei $s = 1$ und algebraischen Invarianten, die auf der *globalen Fundamentalklasse* der Kohomologiegruppe $\hat{H}^2(G, C_L)$ basieren, vermutet. Hierbei bezeichnet C_L die Idelklassengruppe von L.

Diese beiden oben genannten Fälle der äquivarianten Tamagawazahlvermutung sind voneinander unabhängig und werden im Folgenden mit $\mathrm{ETNC}(L|K, 0)$ und $\mathrm{ETNC}(L|K, 1)$ bezeichnet.[2]

[1] Siehe etwa [Neu92, Kap. VII, § 5, p. 488 und Satz (5.11)].

[2] Die Bezeichnung stammt vom englischen Begriff *Equivariant Tamagawa Number Conjecture*.

Aus der Funktionalgleichung der Artinschen L-Reihe, die $\Lambda_{L|K}(1-s)$ und $\Lambda_{L|K}(s)$ assoziiert, ergibt sich ein Zusammenhang der beiden führenden Koeffizienten $\zeta^*_{L|K}(0)$ und $\zeta^*_{L|K}(1)$. Ebenso steht Tates kanonische Klasse per Definition über lokale Fundamentalklassen mit der globalen Fundamentalklasse in Beziehung. Diese beiden Abhängigkeiten geben Anlass zu einer Kompatibilitätsvermutung $\mathrm{ETNC}^{\mathrm{loc}}(L|K,1)$. Sie prognostiziert einen Zusammenhang zwischen Epsilonfaktoren, die in der Funktionalgleichung von $\Lambda_{L|K}(s)$ auftauchen, und lokalen Fundamentalklassen und wird auch *Epsilonkonstantenvermutung* genannt. Diese Kompatibilitätsvermutung gilt genau dann, wenn die beiden Vermutungen $\mathrm{ETNC}(L|K,0)$ und $\mathrm{ETNC}(L|K,1)$ zueinander äquivalent sind [BrB07, Thm. 5.2].

Zusammenfassend ergibt sich das folgende Diagramm, in dem waagerechte Pfeile bekannte Zusammenhänge und senkrechte Pfeile vermutete Beziehungen kennzeichnen:

$$\begin{tikzcd}
\zeta^*_{L|K}(0) \arrow[rr, leftrightarrow, "\text{Funktional-}", "\text{gleichung}"'] & & \zeta^*_{L|K}(1) \\
\mathrm{ETNC}(L|K,0) \arrow[u, dashed] \arrow[d, dashed] & \mathrm{ETNC}^{\mathrm{loc}}(L|K,1) \arrow[l] \arrow[r] \arrow[u, dashed] \arrow[d, dashed] & \mathrm{ETNC}(L|K,1) \arrow[u, dashed] \arrow[d, dashed] \\
\text{Tates kanonische Klasse} \arrow[rr, leftrightarrow, "\text{lokale Funda-}", "\text{mentalklassen}"'] & & \text{Globale Fundamentalklasse}
\end{tikzcd}$$

Breuning studiert in [Bre04b] den lokalen Charakter von $\mathrm{ETNC}^{\mathrm{loc}}(L|K,1)$ im Detail und formuliert eine *lokale Epsilonkonstantenvermutung* $\mathrm{ETNC}^{\mathrm{loc}}(E|F,1)$ für lokale Erweiterungen $E|F$ über $\mathbb{Q}_p$. Außerdem zeigt er, dass die Gültigkeit der lokalen Vermutung für alle nicht-archimedischen Komplettierungen $L_w|K_v$ die globale Vermutung $\mathrm{ETNC}^{\mathrm{loc}}(L|K,1)$ impliziert.

Die äquivarianten Tamagawazahlvermutungen sind bereits für einige Fälle bewiesen. So ist beispielsweise bekannt, dass $\mathrm{ETNC}(L|K,0)$ und $\mathrm{ETNC}(L|K,1)$ für alle Erweiterungen gelten, in denen L abelsch über $\mathbb{Q}$ ist [BG03]. Weiterhin sind $\mathrm{ETNC}^{\mathrm{loc}}(L|K,1)$ für abelsche Erweiterungen $L|\mathbb{Q}$ und beide Epsilonkonstantenvermutungen für zahm verzweigte Erweiterungen gültig [BlB03, Bre04b, BF06]. Darüber hinaus implizieren die äquivarianten Tamagawazahlvermutungen Chinburgs Vermutungen aus [Chi85], und nach Burns [Bur01] ist $\mathrm{ETNC}(L|K,0)$ äquivalent zur gelifteten Wurzelzahlvermutung von Gruenberg, Ritter und Weiss [GRW99].

Einige dieser Vermutungen wurden bereits algorithmisch untersucht. Ein Algorithmus zum Beweis der *lokalen Epsilonkonstantenvermutung* wird von Bley und Breuning in [BlBr08] vorgestellt. Dieser wurde bisher jedoch nicht implementiert, da für einige Teilprobleme – unter anderem für die Berechnung lokaler Fundamentalklassen – noch kein effizienter Algorithmus bekannt ist. Unter Verwendung eines lokal-global Prinzips, kann dieser Algorithmus auch zum Beweis der *globalen Epsilonkonstantenvermutung* herangezogen werden.

Die äquivariante Tamagawazahlvermutung bei $s = 0$ wird von Janssen in [Jan10] studiert. Sie verwendet eine Konstruktion von Chinburg [Chi89], um Tates kanonische Klasse zu berechnen, und entwickelt einen Algorithmus, welcher $\mathrm{ETNC}(L|K, 0)$ numerisch verifizieren kann. In einigen Fällen kann der Algorithmus sogar so modifiziert werden, dass er einen Beweis liefert. Allerdings ist Chinburgs Konstruktion nur in Erweiterungen $L|K$ anwendbar, in denen eine Stelle von K existiert, die in L unzerlegt ist. Diese Voraussetzung ist eine sehr starke Einschränkung an die Erweiterung $L|K$.

Um die äquivarianten Tamagawazahlvermutungen algorithmisch zu untersuchen, ist es also von zentraler Bedeutung effiziente Methoden zur Berechnung der drei Fundamentalklassen zu kennen. Nach einer Einführung verschiedener für die gesamte Arbeit wichtiger Begriffe und Notationen (Kapitel 1), beschäftigen wir uns im ersten Teil der vorliegenden Arbeit im wesentlichen mit der Herleitung solcher Algorithmen (Kapitel 2 bis 4). Anschließend verwenden wir diese im zweiten Teil für rechnerische Untersuchungen der Tamagawazahlvermutungen (Kapitel 5 und 6).

In Kapitel 2 beschäftigen wir uns mit der Kohomologiegruppe $\hat{H}^2(G, E^\times)$ einer lokalen Galoiserweiterung $E|F$ über $\mathbb{Q}_p$ mit Gruppe G. Wir geben einen endlich erzeugten Modul E^f an, der einen kohomologischen Isomorphismus $\hat{H}^2(G, E^\times) \simeq \hat{H}^2\big(G, E^f\big)$ liefert. Dadurch können wir die Methoden von Holt [Hol06] verwenden, um die Gruppe $\hat{H}^2(G, E^f)$ explizit zu berechnen (siehe Abschnitt 2.3).

Für eine unverzweigte Galoiserweiterung $E|F$ kann die lokale Fundamentalklasse in dieser Gruppe direkt angegeben werden. Bei allgemeinen Erweiterungen werden wir die explizite Berechnung von $\hat{H}^2(G, E^f)$ nutzen und direkt aus der Definition der lokalen Fundamentalklasse eine Konstruktion herleiten. Dies führt zu Algorithmus 2.5, welcher jedoch für Erweiterungen vom Grad $[E : \mathbb{Q}_p] > 10$ nicht sehr effizient ist.

In Abschnitt 2.2.2 wird ein leistungsfähigerer Algorithmus für die Berechnung lokaler Fundamentalklassen beschrieben, der auf der Theorie von Serre [Ser79, Kap. XI, § 2] basiert. Insbesondere verzichtet dieser Ansatz vollständig auf die Berechnung von Kohomologiegruppen. Stattdessen wird die lokale Fundamentalklasse in Proposition 2.14 als Kozykel konstruiert. Der darauf basierende Algorithmus ist für die gesamte Arbeit bedeutend.

Als erste Anwendung ermöglicht dieser neue Algorithmus Berechnungen in der *relativen Brauergruppe* $\mathrm{Br}(L|K)$ einer galloisschen Zahlkörpererweiterung $L|K$. Sie wird über den Isomorphismus $\mathrm{Br}(L|K) \simeq \hat{H}^2\big(\mathrm{Gal}(L|K), L^\times\big)$ durch Kozykel mit Werten in $L^\times$ und lokal über

$$\mathrm{Br}(L|K) \simeq \bigoplus_v \hat{H}^2\big(\mathrm{Gal}(L_w|K_v), L_w^\times\big) \simeq \bigoplus_v \frac{1}{[L_w : K_v]}\mathbb{Z}/\mathbb{Z}$$

durch Invarianten (rationale Zahlen) beschrieben, wobei v alle Stellen von K durchläuft. Durch die Kenntnis der lokalen Fundamentalklassen können wir diese lokalen Invarianten explizit berechnen (Algorithmus 2.23) und ebenso einen globalen Kozykel aus lokalen Bedingungen konstruieren (Algorithmus 2.27). In beiden Fällen ist dabei die Einschränkung auf eine endliche Stellenmenge von K die größte Herausforderung.

In Kapitel 3 wenden wir uns der Kohomologiegruppe $\hat{H}^2(G, C_L)$ für eine Galoiserweiterung $L|K$ von Zahlkörpern mit Gruppe G zu. Für algorithmische Fragestellungen sind wir zunächst wieder daran interessiert, einen endlich erzeugten Modul C_L^f zu konstruieren, der einen Isomorphismus $\hat{H}^2(G, C_L^f) \simeq \hat{H}^2(G, C_L)$ liefert. Chinburg beweist in [Chi85] die Existenz eines solchen Moduls, und wir werden in Proposition 3.3 die Konstruktivität seines Beweises zeigen.

Unter Verwendung der Methoden von Holt können wir dann wieder die Kohomologiegruppe $\hat{H}^2(G, C_L^f)$ berechnen. Basierend auf der Konstruktion lokaler Fundamentalklassen entwickeln wir anschließend einen Algorithmus, der die globale Fundamentalklasse in $\hat{H}^2(G, C_L^f)$ berechnet. Dieser Algorithmus ist der erste Algorithmus seiner Art, aber aus Komplexitätsgründen ist er in der Praxis nur für kleine Erweiterungen (vom Grad kleiner als 20 über $\mathbb{Q}$) anwendbar.

Die Kompatibilität der lokalen und globalen Klassenkörpertheorie spiegelt sich in Tates kanonischer Klasse wieder. In Kapitel 4 wiederholen wir Tates Definition aus [Tat66], welche unter anderem *semi-lokale Fundamentalklassen* verwendet.

Von den Algorithmen für lokale und globale Fundamentalklassen leiten wir dann Algorithmen zur Berechnung der semi-lokalen Fundamentalklasse (Algorithmus 4.6) und für Tates kanonische Klasse (Algorithmus 4.12) ab. Anschließend zeigen wir in Abschnitt 4.5, dass diese Berechnung die Konstruktion von Chinburg aus [Chi89] verallgemeinert.

Als Hauptresultat der ersten drei Kapitel können wir somit explizite Algorithmen zur Berechnung lokaler Fundamentalklassen, globaler Fundamentalklassen und für Tates kanonische Klasse herleiten.

Im zweiten Teil der vorliegenden Arbeit wenden wir diese Algorithmen für Fundamentalklassen auf Tamagawazahlvermutungen an.

In Kapitel 5 wiederholen wir die Formulierungen der globalen und lokalen Epsilonkonstantenvermutung von [BlB03] und [Bre04b]. Breunings lokal-global Prinzip (siehe Satz 5.6) zeigt, dass die globale Vermutung $\mathrm{ETNC}^{\mathrm{loc}}(L|K, 1)$ durch einen algorithmischen Beweis der lokalen Vermutung $\mathrm{ETNC}^{\mathrm{loc}}(E|F, 1)$ für endlich viele lokale Erweiterungen $E|F$ bewiesen werden kann.

Diese endlich vielen lokalen Erweiterungen müssen zunächst durch globale Erweiterungen dargestellt werden. Dazu konstruieren wir Galoiserweiterungen $L|K$ von Zahlkörpern mit Stellen $w|v$, so dass gilt: $L_w \simeq E$ und $K_v \simeq F$. Dabei muss v eine unzerlegte Stelle sein, d.h. w ist die einzige Stelle über v und die

Körpergrade $[L : K]$ und $[E : F]$ sind gleich. Da keine algorithmische Herangehensweise bekannt ist, welche den Grad von K über $\mathbb{Q}$ klein hält, geben wir in Abschnitt 5.3.1 verschiedene Heuristiken an und setzen diese im Anschluss bei lokalen Erweiterungen bis zum Grad 15 ein.

In Abschnitt 5.4 geben wir den Algorithmus von Bley und Breuning [BlBr08] zum Beweis von $\mathrm{ETNC}^{\mathrm{loc}}(E|F, 1)$ wieder. Unter Verwendung der Berechnung lokaler Fundamentalklassen mit den Methoden aus Kapitel 2 kann dieser Algorithmus vollständig implementiert werden. Letztlich können wir folgendes rechnergestütztes Resultat (Satz 5.16 und Korollar 5.20) beweisen:

Die globale Epsilonkonstantenvermutung $\mathrm{ETNC}^{\mathrm{loc}}(L|K, 1)$ *gilt für alle Galoiserweiterungen bei denen L in einer Galoiserweiterung $M|\mathbb{Q}$ vom Grad* ≤ 15 *eingebettet werden kann.*

Zuletzt beschäftigen wir uns in Kapitel 6 mit der äquivarianten Tamagawazahlvermutung bei $s = 1$. Die Formulierung aus [BrB07, § 3] für Galoiserweiterungen $L|K$ von Zahlkörpern basiert auf einen Komplex E_S welcher aus der globalen Fundamentalklasse in $\hat{H}^2(\mathrm{Gal}(L|K), C_L)$ konstruiert wird. Für algorithmische Fragestellungen ist wiederum das Hauptproblem, dass der Komplex E_S nicht aus endlich erzeugten Moduln besteht. Allerdings erlaubt die Konstruktion des endlich erzeugten Moduls C_L^f bei der Berechnung globaler Fundamentalklassen aus Kapitel 3 die Definition eines verwandten Komplexes E_S^f, der aus endlich erzeugten Moduln besteht. Ein wesentliches Resultat beweisen wir im Anschluss in Satz 6.10:

Der Komplex E_S^f ist quasi-isomorph zu E_S und kann ebenfalls zur Beschreibung der Vermutung verwendet werden.

Der Komplex E_S^f und die Methoden zur Berechnung globaler Fundamentalklassen aus Kapitel 3 werden anschließend verwendet, um einen Algorithmus für die numerische Verifikation von $\mathrm{ETNC}(L|\mathbb{Q}, 1)$ zu beschreiben. Abschließend zeigen wir in Satz 6.15, dass dieser Algorithmus einen Beweis der äquivarianten Tamagawazahlvermutung liefert, sofern alle Charaktere von G rational oder abelsch sind.

Contents

List of algorithms

List of tables

List of Symbols

Introduction

A well know result for a number field K is the *class number formula.* It relates an analytic term — the residue at $s = 1$ of the Dedekind zeta-function associated to K — to various algebraic terms, for example the absolute discriminant, the regulator and the class number of K. There also exists a similar formulation using the leading term of the $\zeta_K(s)$ at $s = 0$, and both formulations are connected by the functional equation of $\zeta_K(s)$ which relates the values $\zeta_K(1-s)$ and $\zeta_K(s)$.[3]

In the past, various conjectures have been established which can be considered as generalization of these facts. One of these generalization is the *equivariant Tamagawa number conjecture* of Burns and Flach [BF01]. Galois extensions $L|K$ of number fields, which are considered in this thesis, make up a special case in this conjecture, namely the case for the so-called Tate motive. For a summary of these conjectures and related results we refer to [Fla04], but for the important case of number field extensions there are also explicit reformulations of these conjectures [BlB03, BrB07].

In the case of a Galois extension $L|K$ of number fields we consider the completed Artin L-function $\Lambda_{L|K}(\chi, s)$ associated to the characters χ of the Galois group $G = \mathrm{Gal}(L|K)$ and the equivariant Artin L-function $\Lambda_{L|K}(s) = \big(\Lambda_{L|K}(\chi, s)\big)_\chi$ which combines the functions for all characters. The equivariant Tamagawa number conjecture at $s = 0$ relates the leading term $\zeta_{L|K} * (0)$ in the Laurent series expansion at $s = 0$ of the function $\Lambda_{L|K}(s)$ to algebraic terms associated to L and K. These algebraic invariants are constructed from *Tate's canonical class* which is defined by Tate in [Tat66].

Similarly, the equivariant Tamagawa number conjecture at $s = 1$ relates the leading term $\zeta^*_{L|K}(1)$ of the series expansion at $s = 1$ to algebraic invariants which are based on the *global fundamental class* of the Tate cohomology group $\hat{H}^2(G, C_L)$, where C_L denotes the idèle class group of L.

Those two independet cases of the equivariant Tamagawa number conjecture are denoted by $\mathrm{ETNC}(L|K, 0)$ and $\mathrm{ETNC}(L|K, 1)$ respectively.

The two leading terms $\zeta^*_{L|K}(0)$ and $\zeta^*_{L|K}(1)$ are connected by a functional equation which relates $\Lambda_{L|K}(s)$ and $\Lambda_{L|K}(1-s)$. Moreover, by definition of *Tate's canonical class*, this class is related to the *global fundamental class* through *local fundamental classes.* From these relations one therefore obtains a compatibility conjecture $\mathrm{ETNC}^{\mathrm{loc}}(L|K, 1)$. It predicts a relation between epsilon factors from the functional equation and local fundamental classes and is therefore also called

[3] For example see [Neu92, Chp. VII, § 5, p. 488 and Thm. (5.11)].

epsilon constant conjecture. By [BrB07, Thm. 5.2] the compatibility conjecture is valid if and only if $\mathrm{ETNC}(L|K,0)$ and $\mathrm{ETNC}(L|K,1)$ are equivalent.

To summarize, we have the following diagram in which horizontal arrows indicate known relations and vertical arrows are relations predicted by the conjectures:

$$
\begin{tikzcd}
\zeta^*_{L|K}(0) \arrow[rr, leftrightarrow, "\text{functional}", "\text{equation}"'] & {} & \zeta^*_{L|K}(1) \\
\mathrm{ETNC}(L|K,0) \arrow[u, dashed] \arrow[d, dashed] & \mathrm{ETNC}^{\mathrm{loc}}(L|K,1) \arrow[l] \arrow[r] \arrow[u, dashed] \arrow[d, dashed] & \mathrm{ETNC}(L|K,1) \arrow[u, dashed] \arrow[d, dashed] \\
\text{Tate's canonical class} \arrow[rr, leftrightarrow, "\text{local fundamental}", "\text{classes}"'] & {} & \text{Global fundamental class}
\end{tikzcd}
$$

In [Bre04b] Breuning studies the local nature of $\mathrm{ETNC}^{\mathrm{loc}}(L|K,1)$ in more detail and establishes a *local epsilon constant conjecture* $\mathrm{ETNC}^{\mathrm{loc}}(E|F,1)$ for local number fields $E|F$. He also shows that the validity of $\mathrm{ETNC}^{\mathrm{loc}}(L_w|K_v,1)$ for all non-archimedian completions $L_w|K_v$ implies the validity of $\mathrm{ETNC}^{\mathrm{loc}}(L|K,1)$.

The equivariant Tamagawa number conjectures have already been proved for some cases. For example, $\mathrm{ETNC}(L|K,0)$ and $\mathrm{ETNC}(L|K,1)$ are true for extensions in which L is abelian over $\mathbb{Q}$ [BG03], $\mathrm{ETNC}^{\mathrm{loc}}(L|K,1)$ holds for abelian extensions $L|\mathbb{Q}$ [BlB03, BF06], and for tamely ramified extensions the local and global epsilon constant conjecture are valid by [BlB03] and [Bre04b]. Furthermore, the equivariant Tamagawa number conjectures are known to imply Chinburg's conjectures [Chi85], and in [Bur01] Burns proved that $\mathrm{ETNC}(L|K,0)$ is equivalent to the lifted root number conjecture of Gruenberg, Ritter and Weiss [GRW99].

Some of the conjectures were already studied algorithmically. An algorithm to prove the *local epsilon constant conjecture* is presented by Bley and Breuning in [BlBr08] but it is not yet implemented because there are some problems for which no efficient solution was known at that time. One of these problems is the computation of local fundamental classes. Using a local-global principle and some theoretical results for the global case, this algorithm can also be used to prove the *global epsilon constant conjecture*.

The equivariant Tamagawa number conjecture at $s = 0$ is considered algorithmically by Janssen [Jan10]. She uses a construction of Tate's canonical class from Chinburg [Chi89] and presents an algorithm which gives numerical evidence for $\mathrm{ETNC}(L|K,0)$ and also gives a proof for special cases. However, Chinburg's construction of Tate's canonical class is only applicable for extensions $L|K$ in which there is a place of K which is undecomposed in L. This is a strong condition on $L|K$ and it would be pleasing to find a construction which is applicable in the general case.

Outline

To consider equivariant Tamagawa number conjectures algorithmically, it is essential to have methods for the computation of fundamental classes. In the first part of this thesis we will develop different methods for the computation of fundamental classes (Chapters 2 to 4). These algorithms will then be applied to Tamagawa number conjectures (Chapters 5 and 6). But first we will give an introduction to several topics which will be needed throughout this thesis (Chapter 1).

In Chapter 2 we consider the Tate cohomology group $\hat{H}^2(G, E^\times)$ of a local Galois extension $E|F$ of number fields with group G. We specify a finitely generated module E^f for which one has an isomorphism $\hat{H}^2(G, E^\times) \simeq \hat{H}^2\big(G, E^f\big)$ in cohomology. Using methods described by Holt in [Hol06] we can then explicitly compute the group $\hat{H}^2(G, E^f)$, see Algorithm 2.3.

For an unramified extension $E|F$ one can directly specify the local fundamental class in this group. For arbitrary extensions, the explicit computation of cohomology groups also allows the construction of the local fundamental class by using its definition. This leads to Algorithm 2.5 which is, however, not very efficient for extensions $E|F$ in which $[E : \mathbb{Q}_p] > 10$.

In Section 2.2.2 we develop an efficient algorithm for the computation of the local fundamental class in $\hat{H}^2(G, E^f)$, based on the theory of Serre [Ser79, Chp. XI, § 2]. Most importantly, this approach avoids the computation of cohomology groups. Instead, the local fundamental class is directly constructed as a cocycle in Proposition 2.14. This provides a new algorithm which is relevant throughout this thesis.

As a first application it allows computations in the *relative Brauer group* $\mathrm{Br}(L|K)$ for Galois extensions $L|K$ of number fields. It is described by global cocycles $\mathrm{Br}(L|K) \simeq \hat{H}^2\big(\mathrm{Gal}(L|K), L^\times\big)$ or through

$$\mathrm{Br}(L|K) \simeq \bigoplus_v \hat{H}^2\big(\mathrm{Gal}(L_w|K_v), L_w^\times\big) \simeq \bigoplus_v \frac{1}{[L_w : K_v]}\mathbb{Z}/\mathbb{Z}$$

by local invariants (rational numbers), where v ranges over all places of K and w is a place of L above v. The elements in $\mathrm{Br}(L|K)$ can therefore be characterized by invariants at every place v. In Section 2.3 we show how to compute these invariants (Algorithm 2.23) and how to construct a global cocycle which satisfies local conditions (Algorithm 2.27). The main effort in both cases is the restriction to a finite set of places of K.

In Chapter 3 we deal with the cohomology group $\hat{H}^2(G, C_L)$ for a Galois extension $L|K$ of number fields with group G. For algorithmic considerations, we are again interested in the construction of a finitely generated module C_L^f for which there is an isomorphism $\hat{H}^2\big(G, C_L^f\big) \simeq \hat{H}^2(G, C_L)$. Chinburg proves the existence of such a module [Chi85] and an important step is to make his proof constructive, see Proposition 3.3.

Using the methods described in [Hol06] one can then compute the cohomology group $\hat{H}^2(G, C_L^f)$. Based on the construction of the local fundamental class we develop Algorithm 3.13 which computes the global fundamental class in $\hat{H}^2(G, C_L^f)$. This is the first algorithm to compute the global fundamental class, but for complexity reasons it is only applicable to small extensions (of degree less than 20 over $\mathbb{Q}$) in practice.

The compatibility of local and global class field theory is expressed in *Tate's canonical class* which is considered in Chapter 4. We recall its definition from [Tat66] which also involves the *semi-local fundamental class*.

From the algorithms for local and global fundamental classes we deduce algorithms which compute the semi-local fundamental class (Algorithm 4.6) and Tate's canonical class (Algorithm 4.12) for arbitrary Galois extensions $L|K$ of number fields. As a last result, we show in Section 4.5 that this computation of Tate's canonical class generalizes the construction described by Chinburg in [Chi89].

As a result of those three chapters, we develop explicit algorithms to compute the local fundamental class, the global fundamental class and Tate's canonical class.

In the second part of this thesis, these algorithms for fundamental classes will be applied to Tamagawa number conjectures.

In Chapter 5 we recall the formulations of the global and local epsilon constant conjecture for number fields from [BlB03] and [Bre04b]. Using Breuning's local-global principle (see Theorem 5.6) one can show that the conjecture $\mathrm{ETNC}^{\mathrm{loc}}(L|K, 1)$ is true if $\mathrm{ETNC}^{\mathrm{loc}}(E|F, 1)$ is true for finitely many local number field extensions $L_w|K_v$, and this can be done computationally.

In a first step, we have to represent those local extensions $E|F$ globally. We need to construct a Galois extension $L|K$ of number fields with places $w|v$ such that $L_w \simeq E$ and $K_v \simeq F$. Moreover, this place v must be undecomposed in L. In other words w must be the only place of L which lies above v and the degrees $[L : K]$ and $[E : F]$ must be equal. We were not able to give an algorithm for such a Since no construction is known which keeps the degree of K small, we will describe several heuristics in Section 5.3.1 and apply them to extensions $E|\mathbb{Q}_p$ up to degree 15.

Using the construction of local fundamental classes from Chapter 2 it is possible to implement the algorithm for the proof of $\mathrm{ETNC}^{\mathrm{loc}}(E|F, 1)$ from [BlBr08]. In Section 5.4 we recall the description of this algorithm. Then we can computationally prove the following result, see Theorem 5.16 and Corollary 5.20:

The global epsilon constant conjecture $\mathrm{ETNC}^{\mathrm{loc}}(L|K,1)$ *is true for all Galois extensions in which* L *can be embedded into a Galois extension* $M|\mathbb{Q}$ *which is of degree at most 15.*

Finally, Chapter 6 deals with the equivariant Tamagawa number conjecture at $s = 1$. We recall the formulation from [BrB07, § 3] for Galois extensions $L|K$ of number fields which is based on a complex E_S constructed from the global fundamental class in $\hat{H}^2(\mathrm{Gal}(L|K), C_L)$.

To consider this conjecture algorithmically, the main challenge is again the fact that E_S consists of modules which are not finitely generated. But the construction of the finitely generated module C_L^f used in the computation of global fundamental classes, allows the definition of a complex E_S^f consisting of finitely generated modules. As a main result we prove in Theorem 6.10:

The complexes E_S *and* E_S^f *are quasi-isomorphic and we can also use the latter complex in the description of the conjecture.*

The complex E_S^f and Algorithm 3.13 for the construction of the global fundamental class are then used in Section 6.4 to describe an algorithm which numerically verifies $\mathrm{ETNC}(L|\mathbb{Q}, 1)$. As a last result we prove in Theorem 6.15 that this algorithm can actually prove of the equivariant Tamagawa number conjecture at $s = 1$ for a single extension $L|\mathbb{Q}$ in the case where every character of G is rational or abelian.

1 Preliminaries

1.1 Tate Cohomology

Let G be a finite group and A a G-module. Then $\hat{H}^q(G,A)$ will denote the *Tate cohomology* groups as defined in [NSW00, Chp. I, § 2] or [Neu69, Chp. I, § 2].

More precisely, in terminology of [NSW00] the group $C^q(G,A)$ of q-cochains, the group $Z^q(G,A) = \ker(\partial_{q+1})$ of q-cocycles, and the group $B^q(G,A) = \operatorname{im}(\partial_q)$ of q-coboundaries are defined using the *cohomological complete standard resolution of* A with *differentials* ∂_q. The *q-th cohomology groups* $\hat{H}^q(G,A) := Z^q(G,A)/B^q(G,A)$ are then called *modified cohomology groups* (or *Tate cohomology groups*). For computational issues we will always use the *inhomogeneous representation*, where $C^0(G,A) = A$ and $C^q(G,A)$ is the group of all functions $y : G^q \to A$ for $q \geq 1$.[1]

Explicitly, the most important cohomology groups for our purposes are those in degrees -1 to 2:

$$\hat{H}^0(G,A) := A^G / \operatorname{N}_G A \quad \text{and} \quad \hat{H}^{-1}(G,A) := {}_{\operatorname{N}_G}A / \operatorname{I}_G A$$

where $\operatorname{N}_G A = \{\operatorname{N}_G a = \sum_{\sigma \in G} \sigma a \mid a \in A\}$ is the norm group, ${}_{\operatorname{N}_G}A = \{a \in A \mid \operatorname{N}_G a = 0\}$ is the group of elements with trivial norm and $\operatorname{I}_G A = \langle \sigma a - a \mid a \in A, \sigma \in G\rangle$. In degree 1, we obtain the 1-cocycles as 1-cochains x with $x(\sigma\tau) = \sigma x(\tau) + x(\sigma)$ for $\sigma, \tau \in G$ and the 1-coboundaries are maps $x(\sigma) = (\partial_1 a)(\sigma) := \sigma a - a$ for $\sigma \in G$ and with $a \in A$. Finally, the 2-cocycles satisfy the relation

$$x(\sigma\tau, \rho) + x(\sigma, \tau) = \sigma x(\tau, \rho) + x(\sigma, \tau\rho) \tag{1.1}$$

for $\sigma, \tau, \rho \in G$ and 2-coboundaries are maps $x(\sigma,\tau) = (\partial_2 y)(\sigma,\tau) := \sigma y(\tau) - y(\sigma\tau) + y(\sigma)$ with arbitrary 1-cochain $y \in C^1(G,A)$.

Remark 1.1. Note that the equations above assume that G acts *from the left* on A, i.e. $\sigma(\tau a) = (\sigma\tau)a$. If G acts *from the right*, we will use the exponent notation to avoid confusion and one has the relation $(a^\tau)^\sigma = a^{\tau\sigma}$. The relation (1.1) for 2-cocycles then becomes (written multiplicatively)

$$x(\rho, \tau\sigma) x(\tau, \sigma) = x(\rho, \tau)^\sigma x(\rho\tau, \sigma). \tag{1.2}$$

This will be important when it comes to implementing algorithms into the computer algebra system Magma [BCP97] because it prefers right-actions: for example the action by the automorphism group of a number field is computed as a right-action.

[1] In [NSW00] these inhomogeneous groups are denoted by the script letters $\mathscr{C}$, $\mathscr{Z}$ and $\mathscr{B}$.

Remark 1.2 (Normalized cocycles). A cochain $f \in C^n(G, A), n \geq 1$, is called *normalized* if $f(\sigma_1, \dots, \sigma_n) = 1$ whenever one of the σ_i is 1. Every class in $\hat{H}^n(G, A)$ can be represented by a (not necessarily unique) normalized cocycle, cf. [NSW00, Chp. I, § 2, Ex. 5].

For example, let g be a 2-cocycle and let A be a division ring. Consider the constant 1-cochain $\lambda : G \to L^\times$, $\sigma \to g(1,1)^{-1}$. Then one can easily check that $f = \partial_2(\lambda)g$ is the normalized cocycle in the class of g in $\hat{H}^2(G, A)$, cf. [Ker07, § 8.1].

For a subgroup H of G, we denote the *restriction* map by $\mathrm{res}^G_H : \hat{H}^n(G, A) \to \hat{H}^n(H, A)$ and (if H is normal) the *inflation* map by $\inf^G_{G/H} : \hat{H}^n(G/H, A^H) \to \hat{H}^n(G, A)$.

Since we will focus on the computation of fundamental classes in Chapters 2 to 4 we will summarize some results from local and global class field theory in the following sections. See [NSW00, Chp. VII, § 1 and Chp. VIII, § 1] for details.

1.1.1 Cohomology of local fields

For a Galois extension $L|K$ of local non-archimedian number fields with group G the cohomology group $H^2(L|K) := \hat{H}^2(G, L^\times)$ has an important role. Below we follow the construction of a *canonical invariant map* for local fields with non-archimedian valuation. It is based on the following invariant map for *unramified extensions.*

Theorem 1.3. *For every unramified Galois extension $L|K$ with group G there is a canonical isomorphism* $\mathrm{inv}_{L|K} : H^2(L|K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ *induced by the valuation of L and the evaluation of characters at the Frobenius automorphism φ of $L|K$.*

Proof. [NSW00, Chp. VII, § 1]. □

Explicitly, the local invariant map is given by

$$\mathrm{inv}_{L|K} : \hat{H}^2(G, L^\times) \xrightarrow{v_L} \hat{H}^2(G, \mathbb{Z}) \xrightarrow{\simeq} \hat{H}^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\simeq} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \qquad (1.3)$$

where the left-hand map is an isomorphism since the unit group $U_L = \ker(v_L)$ is cohomologically trivial, the middle isomorphism is the inverse of the connecting homomorphism obtained from the short exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ (where $\mathbb{Q}$ is cohomologically trivial), and the latter isomorphism sends a character χ to the image of the Frobenius automorphism $\chi(\varphi)$.

Similarly, one obtains an invariant map

$$\mathrm{inv}_{\widetilde{K}|K} : H^2(\widetilde{K}|K) \xrightarrow{\simeq} \mathbb{Q}/\mathbb{Z}$$

for the maximal unramified extension $\widetilde{K}$ of K using the valuation of $\widetilde{K}$ with cohomological trivial kernel $U_{\widetilde{K}}$. The invariant maps for different Galois extensions L and N of K with $L \subseteq N$ commute with the injective inflation map $\inf_{L|K}^{N|K} : H^2(L|K) \to H^2(N|K)$ and the restriction map $\mathrm{res}_{N|K}^{N|L} : H^2(N|K) \to H^2(N|L)$. If the number fields in these maps are known from the context, we will also write inf or res.

The following lemma extends this canonical invariant map to the maximal separable extension $\bar{K}$ of K.

Lemma 1.4. *$H^2(\bar{K}|K) \simeq H^2(\widetilde{K}|K)$.*

Proof. [NSW00, Thm. (7.1.3)]. □

This result is obtained by identifying the cohomology groups $H^2(L|K)$ and $H^2(L'|K)$ for two extensions of the same degree. If K_n denotes the unramified extension of K of degree n, one has isomorphisms

$$H^2(\bar{K}|K) \simeq \varinjlim_{L} H^2(L|K) \simeq \varinjlim_{n\in\mathbb{N}} H^2(K_n|K) \simeq H^2(\widetilde{K}|K)$$

where L runs through all finite Galois extensions of K. In each of the *direct limits*, two elements are identified, if their inflation to the cohomology of their composite field is equal. Two different cohomology groups $H^2(L|K)$ and $H^2(L'|K)$ can both be considered as subgroups of $H^2((LL')|K)$. One therefore often writes $H^2(\bar{K}|K) \simeq \bigcup_L H^2(L|K)$ and $H^2(\widetilde{K}|K) \simeq \bigcup_{n\in\mathbb{N}} H^2(K_n|K)$. Especially, if L is an arbitrary Galois extension of K and $L'|K$ is the unramified extension of the same degree, then the inflation of $H^2(L|K)$ and $H^2(L'|K)$ are the same subgroups in $H^2((LL')|K)$.

Combining the previous results one then obtains a unique *local invariant map*

$$\mathrm{inv}_K : H^2(\bar{K}|K) \xrightarrow{\simeq} \mathbb{Q}/\mathbb{Z}.$$

Its restriction to the cohomology of finite Galois extensions $L|K$ provides an invariant map $\mathrm{inv}_{L|K} : H^2(L|K) \xrightarrow{\simeq} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ which is compatible with inflation and restriction.

Theorem 1.5. *The cohomology groups $H^2(L|K)$ satisfy the conditions of a* class formation[2] *with respect to the invariant maps* $\mathrm{inv}_{L|K}$*, i.e.*

(a) $H^1(L|K) = 1$ for every normal extension $L|K$.

[2] In general, class formations can be defined for profinite groups G acting on an discrete module A, cf. [NSW00, Def. (3.1.8)]. But here we will omit these details and state the properties explicitly for the cohomology of local and global fields. These explicit properties can also be found in [Neu69].

(b) The invariant maps $\mathrm{inv}_{L|K}$ *satisfy:*

(i) $\mathrm{inv}_{L|K} = \mathrm{inv}_{N|K} \circ \mathrm{inf}_{L|K}^{N|K}$ *for extensions* $N|L|K$ *with* $N|K$ *and* $L|K$ *normal,*

(ii) $\mathrm{inv}_{N|L} \circ \mathrm{res}_{N|K}^{N|L} = [L : K]\,\mathrm{inv}_{N|K}$ *for extensions* $N|L|K$ *with* $N|K$ *normal.*

Proof. [NSW00, (7.1.4) and (7.1.5)]. □

The compatibility of the invariant map with inflation and restriction, as in property (b), can also be summarized in the following commutative diagram:

$$\begin{array}{ccccc} H^2(L|K) & \xrightarrow{\mathrm{inf}} & H^2(N|K) & \xrightarrow{\mathrm{res}} & H^2(N|L) \\ \downarrow{\scriptstyle \mathrm{inv}_{L|K}} & & \downarrow{\scriptstyle \mathrm{inv}_{N|K}} & & \downarrow{\scriptstyle \mathrm{inv}_{N|L}} \\ \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} & \xrightarrow{\subseteq} & \frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z} & \xrightarrow{[L:K]} & \frac{1}{[N:L]}\mathbb{Z}/\mathbb{Z} \end{array} \tag{1.4}$$

By means of the invariant map one can then identify a canonical generator of $H^2(L|K)$.

Definition 1.6 (Fundamental class). *The unique generator* $u_{L|K} \in H^2(L|K)$*, which is the preimage of* $\frac{1}{[L:K]} + \mathbb{Z}$ *by the canonical local invariant map* $\mathrm{inv}_{L|K}$*, is called* local fundamental class.

We finish this section by specifying explicit representations of the local fundamental class for unramified and archimedean extensions.

Remark 1.7. (a) Let $L|K$ be an unramified extension of degree n and π an uniformizing element of K. The Galois group $\mathrm{Gal}(L|K)$ is generated by the Frobenius automorphism φ and the local fundamental class is defined by Theorem 1.3. Consider the cocycle

$$c(\varphi^i, \varphi^j) = \begin{cases} 1 & \text{if } i + j < n \\ \pi & \text{if } i + j \geq n \end{cases} \tag{1.5}$$

from [Rei03, Chp. 7, (30.1)] and apply the isomorphism (1.3). Its image in $\hat{H}^2(G, \mathbb{Z})$ is the cocycle $x \in C^2(G, \mathbb{Z})$ for which $x(\varphi^i, \varphi^j)$ is zero for $i+j < n$ and one for $i + j \geq n$.

Embedded in $C^2(G, \mathbb{Q})$ the cocycle x is a coboundary since it is the image of the 1-cocycle $y \in C^1(G, \mathbb{Q})$ defined by $y(\varphi^i) = \frac{i}{n}$: For $i + j < n$ one has $(\partial_1 y)(\varphi^i, \varphi^j) = \varphi^i(y(\varphi^j)) - y(\varphi^{i+j}) + y(\varphi^i) = \frac{j-(i+j)+i}{n} = 0$. And for $n \leq i+j < 2n$ one has $y(\varphi^{i+j}) = \frac{i+j-n}{n}$ and thus $(\partial_1 y)(\varphi^i, \varphi^j) = 1$. Hence $(\partial_1 y) = x$ and the image of c in $C^1(G, \mathbb{Q}/\mathbb{Z})$ is the projection $\bar{x}$ of x via $C^1(G, \mathbb{Q}) \twoheadrightarrow C^1(G, \mathbb{Q}/\mathbb{Z})$.

The last isomorphism in (1.3) sends the cocycle $\bar{x} \in C^1(G, \mathbb{Q}/\mathbb{Z})$ to the value at φ, which is $\frac{1}{n} + \mathbb{Z}$. Therefore $\mathrm{inv}_{L|K}(c) = \frac{1}{n} + \mathbb{Z}$ and the cocycle c represents the local fundamental class of $L|K$.

(b) For a Galois extension of local fields with *archimedian valuation*, there is actually just one non-trivial extension to consider: the *ramified extension* $L = \mathbb{C}$ over $K = \mathbb{R}$. In this case G and $\hat{H}^2(G, L^\times) = \hat{H}^2(G, \mathbb{C}^\times)$ are both cyclic groups of order two. So there is just one generator in the local cohomology group, and we define this generator to be the *local fundamental class for archimedian local fields*. The normalized cocycles $c(\sigma, \tau)$ in this group are uniquely defined by $c(\sigma, \sigma)$ for $\sigma \neq 1$ and the cocycle relation (1.1) directly implies $c(\sigma, \sigma) \in \mathbb{R}$.

A normalized 2-coboundary $c \in \hat{H}^2(G, L^\times)$ is the image of a normalized 1-cochain $a \in C^1(G, \mathbb{C}^\times)$, which implies $c(\sigma, \sigma) = \sigma(a(\sigma))a(\sigma) = |a(\sigma)|^2 > 0$. Therefore, the cocycle

$$c(\sigma, \tau) = \begin{cases} 1 & \text{for } \sigma = 1 \text{ or } \tau = 1 \\ -1 & \text{for } \sigma \neq 1 \text{ and } \tau \neq 1 \end{cases}$$

in $C^2(G, L^\times)$ cannot be a coboundary and, hence, it represents the local fundamental class in $\hat{H}^2(G, L^\times)$.

1.1.2 Cohomology of global fields

Whereas the multiplicative group has an important role in local class field theory, the counterpart for global class field theory is the idèle class group C_L.

For global fields L, we consider the completions L_v and their group of integral units $U_{L_v} := \mathcal{O}_{L_v}^\times$. For infinite places v, we define $U_{L_v} := L_v^\times$. For every place v we denote the decomposition group by G_v.

Definition 1.8 (Idèle class group). *Let L be a global field. The* idèle group *I_L of L is defined as the restricted product $I_L = \prod_v' L_v^\times$, where v runs through all places of L. The product is restricted w.r.t. the unit groups U_{L_v}, i.e. every element $x = (x_v) \in I_L$ has only finitely many components $x_v \notin U_{L_v}$.*

The units $L^\times$ of L are diagonally embedded into I_L. This diagonal embedding will be denoted by Δ and one defines the idèle class group *by $C_L = I_L/\Delta(L^\times)$.*

The diagonal embedding Δ is sometimes also applied implicitly and one writes $C_L = I_L/L^\times$. We summarize some properties of idèle groups and idèle class groups.

Lemma 1.9. *Let $L|K$ be a Galois extension of global fields with group G.*

(a) The groups I_L and C_L are G-modules with G action induced by the canonical G_v action on $L_v^\times$.

(b) $I_K = I_L^G$ and $C_K = C_L^G$.

(c) $\hat{H}^i(G, I_L) \simeq \bigoplus_v \hat{H}^i(G_v, L_v^\times)$.

Proof. [NSW00, Chp. VIII, § 1]. □

As in the local case, one can construct a canonical invariant map on the cohomology group $H^2(L|K) := \hat{H}^2(G, C_L)$, called *global invariant map*. For the cohomology group of the idèle group this is directly given by local invariant maps.

Definition 1.10 (Idèlic invariant map). *Using Lemma 1.9 we obtain a canonical homomorphism* $\mathrm{inv} : \hat{H}^2(G, I_L) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ *defined by the sum of the local invariant maps* $\mathrm{inv}_w : \hat{H}^i(G_w, L_w^\times) \to \frac{1}{[L_w:K_v]}\mathbb{Z}/\mathbb{Z}$. *We refer to this map as the* idèlic invariant map.

Although the idèlic invariant map is not an isomorphism and, hence, does not satisfy the conditions of a class formation, it is still compatible with inflation and restriction as in diagram (1.4), cf. [NSW00, Prop. (8.1.10)].

Since $\hat{H}^2(G, I_L) \to \hat{H}^2(G, C_L)$ is not surjective in general (e.g. see [NSW00, Chp. VIII, §1, p. 378]), the idèlic invariant map does not directly provide a well-defined global invariant map. Therefore, we first restrict to *cyclic extensions* which can be seen as analogue of the unramified extensions in the local case.

Lemma 1.11. *For cyclic extensions $L|K$ with group G the idèlic invariant map and the map $\hat{H}^2(G, I_L) \to \hat{H}^2(G, C_L)$ are both surjective.*

This can be proved using Chebotarev's density theorem:

Theorem 1.12 (Chebotarev's density theorem). *Let $L|K$ be a Galois extension of number fields with group G. For every $\sigma \in G$ denote its conjugacy class by $G \cdot \sigma = \{\tau\sigma\tau^{-1} \mid \tau \in G\}$. Then the set of places v of K, which are unramified in L and for which σ is the Frobenius automorphism φ_w for some place $w|v$, has density $\frac{\#(G\cdot\sigma)}{\#G}$.*

Proof. [Neu92, Chp. VII, Thm. (13.4)]. □

Corollary 1.13. *In every cyclic extension $L|K$ there are infinitely many unramified places, which are undecomposed.*

Proof. Let the Galois group G of $L|K$ be generated by τ. A place v of K which is unramified and undecomposed must have full inertia degree $f = \#G$. Hence, places v with $w|v$ and $\varphi_w = \tau$ are unramified and undecomposed. By Chebotarev's density theorem these places occur with density $1/\#G$.

This is also true for other generators τ of G and the total density of unramified undecomposed places is $k/\#G$, where k is the number of integers $1 \leq i \leq \#G$ for which $(i, \#G) = 1$. □

Using this consequence of Chebotarev's density theorem, we can given a simple proof of the surjectivity of the idèlic invariant map.

Proof of Lemma 1.11. By Corollary 1.13 there exists a place v of K which is undecomposed in L, i.e. there is exactly one place w in L above v and the decomposition group G_w is equal to G. Hence, one can find an element in $\hat{H}^2(G_w, L_w^\times) = H^2(L_w|K_v)$, which is the preimage of $\frac{1}{[L:K]} + \mathbb{Z}$, and by Lemma 1.9(c) this also yields a preimage in $\hat{H}^2(G, I_L)$. In conclusion, the idèlic invariant map is surjective.

The latter assertion follows from $\hat{H}^3(G, L^\times) = \hat{H}^1(G, L^\times) = 1$ for the cyclic group G. For more details see [NSW00, Prop. (8.1.15)]. □

Hence, for cyclic extensions we have the following diagram

$$\begin{tikzcd} \hat{H}^2(G, I_L) \arrow[r, two heads] \arrow[d, two heads] & \frac{1}{|G|}\mathbb{Z}/\mathbb{Z} \\ \hat{H}^2(G, C_L) \arrow[ur, dashed, two heads] & \end{tikzcd}$$

and by [NSW00, Prop. (8.1.15)] and its proof both of the above surjective maps have kernel $\hat{H}^2(G, L^\times)$. Therefore, the idèlic invariant map gives a well-defined invariant map $\mathrm{inv}_{L|K}$ on $\hat{H}^2(G, C_L)$.

This can be generalized to arbitrary extensions by considering the union of cyclic extensions.

Lemma 1.14. *For the cohomology groups of the idèle group and the idèle class group there are isomorphisms*

$$\hat{H}^2(\mathrm{Gal}(\bar{K}|K), I_{\bar{K}}) \simeq \bigcup_{\substack{L|K \\ cyclic}} \hat{H}^2(\mathrm{Gal}(L|K), I_L)$$

$$\textit{and} \qquad H^2(\bar{K}|K) \simeq \bigcup_{\substack{L|K \\ cyclic}} H^2(L|K).$$

Proof. [NSW00, Prop. (8.1.9) and proof of Prop. (8.1.20)]. □

As in the local case, this result is obtained by identifying cohomology groups from extensions of the same degree. In particular, if $L|K$ is an arbitrary Galois extension and $L'|K$ is a cyclic extension of the same degree, then the inflations of $H^2(L|K)$ and $H^2(L'|K)$ are the same subgroup in $H^2((LL')|K)$.

The previous results then define a canonical *global invariant map*

$$\mathrm{inv}_K : H^2(\bar{K}|K) \xrightarrow{\simeq} \mathbb{Q}/\mathbb{Z}$$

and its restriction to the cohomology of finite Galois extensions $L|K$ again provides an invariant map $\mathrm{inv}_{L|K} : H^2(L|K) \xrightarrow{\simeq} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$. The cohomology groups $H^2(L|K)$ then satisfy the conditions of a class formations with respect to $\mathrm{inv}_{L|K}$, cf. [NSW00, Thm. (8.1.22)].

Definition 1.15 (Global fundamental class). *The unique generator* $u_{L|K} \in H^2(L|K)$*, which is the preimage of* $\frac{1}{[L:K]} + \mathbb{Z}$ *by the canonical global invariant map* $\mathrm{inv}_{L|K}$*, is called* global fundamental class*.*

1.2 Brauer groups

In preparation for Chapter 2 an overview of Brauer groups and important properties is given in the following section. A detailed survey of the theory of algebras and Brauer groups can be found in [Rei03].

The Brauer group is used to study *central simple algebras* A over a field K, i.e. finite-dimensional K-algebras with *center* $\mathrm{Z}(A) = K$ which have only trivial two-sided ideals. They are used to classify division algebras over a field.

Proposition 1.16. *Let* A *be a central simple* K*-algebra. Then*

(i) $A \simeq M_n(D)$*, with* $n \in \mathbb{N}$ *unique and* D *is a skew field with center* K *which is unique up to isomorphism, and*

(ii) there exists a finite Galois extensions $L|K$ *such that* $A_L := A \otimes_K L \simeq M_n(L)$*.*

Proof. The first statement is a consequence of *Wedderburn's theorem* [Rei03, Chp. I, Thm. (7.4)] and the second is proved in [Rei03, Chp. VII, Cor. (28.11)].□

Definition 1.17. *A Galois extension* $L|K$ *as in the previous lemma is called* splitting field *for* A*. Two algebras* A *and* B *are called* similar*, denoted by* $A \sim B$*, if* $A \otimes_K M_r(K) \simeq B \otimes_K M_s(K)$ *for* $r, s \in \mathbb{N}$*.*

Definition 1.18 (Brauer group). *The Brauer group* $\mathrm{Br}(K)$ *of* K *is the group of similarity classes* $[A]$ *of central simple* K*-algebras* A *with multiplication*

$$[A][B] := [A \otimes_K B].$$

By [Rei03, Chp. I, Thm. (7.6)] the tensor product $A \otimes_K B$ is again central and simple and the multiplication in $\mathrm{Br}(K)$ is well-defined.

Definition 1.19 (Relative Brauer group). *For an extension* $L|K$*, the kernel* $\mathrm{Br}(L|K)$ *of the* restriction homomorphism

$$\begin{aligned} \mathrm{Br}(K) &\to \mathrm{Br}(L) \\ [A] &\mapsto [A \otimes_K L] \end{aligned}$$

is called relative Brauer group*.*

Every algebra $A \in \mathrm{Br}(K)$ has a splitting field L. One therefore obtains the identity $\mathrm{Br}(K) = \bigcup_L \mathrm{Br}(L|K)$ where L runs through all finite Galois extensions of K.

For every Galois extension $L|K$ with group G, the relative Brauer group $\mathrm{Br}(L|K)$ can be described cohomologically.

Proposition 1.20. *The map $\hat{H}^2(G, L^\times) \to \mathrm{Br}(L|K)$, sending a normalized two-cocycle $\gamma \in \hat{H}^2(G, L^\times)$ to the algebra $A = \bigoplus_{\sigma\in G} Le_\sigma$ with multiplication*

$$\Big(\sum_\sigma x_\sigma e_\sigma\Big)\Big(\sum_\tau y_\tau e_\tau\Big) = \sum_{\sigma,\tau} x_\sigma \sigma y_\tau \gamma(\sigma,\tau) e_{\sigma\tau},$$

is an isomorphism of groups.

Proof. [NSW00, Prop. (6.3.3) and (6.3.4)]. □

Combining the identifications for Brauer groups and cohomology groups one also has a cohomological description for the Brauer group:

$$\mathrm{Br}(K) = \bigcup_L \mathrm{Br}(L|K) \simeq \bigcup_L H^2(L|K) \simeq H^2(\bar{K}|K).$$

Now consider a local field K. For the Brauer group one then obtains a canonical isomorphism $\mathrm{Br}(K) \simeq \mathbb{Q}/\mathbb{Z}$ through the local invariant map, called the *Hasse invariant map*. The image of an algebra A under this isomorphism is called the *Hasse invariant* of A.[3]

1.3 Homological algebra

The following sections will give a short overview over some homological constructions used in this thesis. Most of these definitions and facts can be found in [HS71, Mac75] or [Wei94]. For more details and proofs we refer to those books.

1.3.1 Extensions

Let R be a ring (with one), let A and B be R-modules and fix an *injective resolution*

$$0 \longrightarrow B \xrightarrow{d_{-1}} I_0 \xrightarrow{d_0} I_1 \xrightarrow{d_1} \cdots$$

of B, where I_k, $0 \leq k$ is a family of injective modules. For a fixed integer n, denote $J_n := \mathrm{coker}(d_{n-2})$ and the corresponding projection by $p_n : I_{n-1} \to J_n$ such that

$$0 \longrightarrow B \xrightarrow{d_{-1}} I_0 \xrightarrow{d_0} \cdots \xrightarrow{d_{n-2}} I_{n-1} \xrightarrow{p_n} J_n \longrightarrow 0 \tag{1.6}$$

is an exact sequence of length $n+2$.

[3] Originally, the Hasse invariant was defined independently and then proved to coincide with the invariant obtained from local class field theory, c.f. [Ker07, Thm. (13.10) and Rem. (13.12)].

Definition 1.21 (Ext-group). *The map p_n induces a map $p_n^*:\operatorname{Hom}_G(A, I_{n-1}) \to \operatorname{Hom}_G(A, J_n)$ and we define the group of* n-extensions *by*

$$\operatorname{Ext}^n_R(A,B) = \operatorname{Hom}_R(A, J_n)/\operatorname{im}(p_n^*)$$

for $n \in \mathbb{N}$ and we set $\operatorname{Ext}^0_R(A,B) = \operatorname{Hom}_R(A,B)$.

One can prove that this definition does not depend on the choice of the injective resolution and one can equivalently define $\operatorname{Ext}^n_R(A,B)$ by $\operatorname{Hom}_R(Q_n, B)/\ker(i_n^*)$ using a *projective resolution* $\cdots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} A \longrightarrow 0$ with kernel $Q_n := \ker(d_{n-1})$ and $i_n : Q_n \hookrightarrow P_{n-1}$, cf. [HS71, Prop. 8.1].

The group $\operatorname{Ext}^n_R(A,B)$ can also be described using the following operation on n-extensions of A with B.

Definition 1.22 (Baer sum). *For two n-extensions e_1 and e_2 given by*

$$0 \to B \to E_1^i \to \cdots \to E_n^i \to A \to 0$$

for $i = 1, 2$ with $n \geq 2$, the sum $e_1 + e_2$ is defined to be the extension

$$0 \to B \to P \to E_2^1 \oplus E_2^2 \to \cdots \to E_{n-1}^1 \oplus E_{n-1}^2 \to Q \to A \to 0$$

where P is the pushout of $B \to E_1^1$ with $B \to E_1^2$ and Q is the pullback of $E_n^1 \to A$ with $E_n^2 \to A$. If $n = 1$, the sum is defined by

$$0 \to B \to Q/\langle (b, -b), b \in B\rangle \to A \to 0.$$

Example 1.23. Consider the case $n = 2$ and let E_1, E_2, F_1 and F_2 be R-modules with extensions

$$\begin{aligned} e:&\quad 0 \longrightarrow B \xrightarrow{\iota_1} E_1 \longrightarrow E_2 \xrightarrow{\pi_1} A \longrightarrow 0, \\ \text{and}\qquad f:&\quad 0 \longrightarrow B \xrightarrow{\iota_2} F_1 \longrightarrow F_2 \xrightarrow{\pi_2} A \longrightarrow 0. \end{aligned}$$

Denote the pushout of ι_1 and ι_2 by P and the pullback of π_1 and π_2 by Q. They can explicitly be written as

$$\begin{aligned} P &= \frac{E_1 \oplus F_1}{\langle (\iota_1(b), -\iota_2(b)), b \in B\rangle} \\ \text{and}\qquad Q &= \big\{ (x,y) \in E_2 \oplus F_2 \mid \pi_1(x) = \pi_2(y) \big\} \subseteq E_2 \oplus F_2 \end{aligned}$$

Then the sum $e + f$ is the extension

$$0 \longrightarrow B \longrightarrow P \longrightarrow Q \longrightarrow A \longrightarrow 0$$

where the map $P \to Q$ is canonically given by the map $E_1 \oplus F_1 \to E_2 \oplus F_2$. By the exactness of the extensions e and f, the map $P \to Q$ is well defined and the sum $e + f$ is again an exact sequence.

The operation on 1-extensions is due to Baer, and therefore called *Baer sum*. Its generalization was later introduced by Yoneda and defines the following group structure on n-extensions.

Definition 1.24 (Yoneda group). *The group* $\mathrm{Yext}_R^n(A,B)$ *of* Yoneda extensions *is the set of equivalence classes of n-extensions of A with B generated by the symmetric-transitive closure of the relation induced by commutative diagrams of the form*

$$\begin{tikzcd} 0 \arrow[r] & B \arrow[r] \arrow[d, equal] & E_1 \arrow[r] \arrow[d] & \cdots \arrow[r] & E_n \arrow[r] \arrow[d] & A \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & B \arrow[r] & E_1' \arrow[r] & \cdots \arrow[r] & E_n' \arrow[r] & A \arrow[r] & 0 \end{tikzcd} \tag{1.7}$$

The addition in this group is given by the Baer sum and the identity is the class of $0 \to B \xrightarrow{\mathrm{id}} B \xrightarrow{0} 0 \xrightarrow{0} \cdots \xrightarrow{0} 0 \xrightarrow{0} A \xrightarrow{\mathrm{id}} A \to 0$ *for* $n \geq 2$, *and the class of the split extension* $0 \to B \to B \oplus A \to A \to 0$ *for* $n = 1$. *Finally, the inverse of a class E is given by the pushout sequence of E with* $-\mathrm{id}_B$.

A verification of the group axioms and other details can be found in [Mac75, Chp. III, §§ 2 and 5].

Remark 1.25. Considering the pushout with $-\mathrm{id}_B$ more explicitly, the inverse of the extensions $\big[0 \to E_0 \xrightarrow{e_0} E_1 \xrightarrow{e_1} \cdots \xrightarrow{e_{n-1}} E_n \xrightarrow{e_n} E_{n+1} \to 0\big] \in \mathrm{Yext}_R^n(E_{n+1}, E_0)$ is given by $\big[0 \to E_0 \xrightarrow{-e_0} E_1 \xrightarrow{e_1} \cdots \xrightarrow{e_{n-1}} E_n \xrightarrow{e_n} E_{n+1} \to 0\big]$. Since every diagram

$$\begin{tikzcd} E_{i-1} \arrow[r, "-e_{i-1}"] \arrow[d, equal] & E_i \arrow[r, "e_i"] \arrow[d, "-\mathrm{id}_{E_i}"] & E_{i+1} \arrow[d, equal] \\ E_{i-1} \arrow[r, "e_{i-1}"] & E_i \arrow[r, "-e_i"] & E_{i+1} \end{tikzcd}$$

is commutative, every extension $\big[0 \to E_0 \to \cdots \xrightarrow{-e_i} \cdots \to E_{n+1} \to 0\big]$, where just one of the maps e_i is negated, represents the inverse in $\mathrm{Yext}_R^n(E_{n+1}, E_0)$.

We will often use the following identifications.

Proposition 1.26. *For R-modules A, A_i, B and B_i there are isomorphisms*

$$\mathrm{Ext}_R^n\big(\bigoplus_i A_i, B\big) \simeq \prod_i \mathrm{Ext}_R^n(A_i, B), \tag{1.8}$$

$$\mathrm{Ext}_R^n\big(A, \prod_i B_i\big) \simeq \prod_i \mathrm{Ext}_R^n(A, B_i), \tag{1.9}$$

$$\text{and} \quad \mathrm{Ext}_R^i(A,B) \simeq \mathrm{Yext}_R^i(A,B). \tag{1.10}$$

Proof. [HS71, Chp. III, Lem. 4.1 and Chp. IV, Thm. 9.1]. $\square$

If the group $\mathrm{Ext}^n_R\big(-,B\big)$ is represented using the fixed extension (1.6), then the isomorphism (1.8) is given by $\mathrm{Hom}(\bigoplus_i A_i, J_n) \simeq \prod_i \mathrm{Hom}\,(A_i, J_n)$, i.e. by restricting the homomorphism to A_i for all i. Similarly, the isomorphism (1.9) is given by canonical projections if $\mathrm{Ext}^n_R\big(A,-\big)$ is represented by a fixed projective resolution of A.

Given a homomorphism $\phi \in \mathrm{Hom}(A, J_n)$ representing an element in $\mathrm{Ext}^n_R(A,B)$ one gets the corresponding n-extension in $\mathrm{Yext}^n_R(A,B)$ by forming the pullback diagram of $p : I_{n-1} \twoheadrightarrow J_n$ with ϕ:

$$\begin{tikzcd} 0 \arrow[r] & B \arrow[r] \arrow[d, equal] & I_0 \arrow[r] \arrow[d, equal] & \cdots \arrow[r] & I_{n-2} \arrow[r] \arrow[d, equal] & Q \arrow[r] \arrow[d] & A \arrow[r] \arrow[d, "\phi"] & 0 \\ 0 \arrow[r] & B \arrow[r] & I_0 \arrow[r] & \cdots \arrow[r] & I_{n-2} \arrow[r] & I_{n-1} \arrow[r, "p"] & J_n \arrow[r] & 0 \end{tikzcd} \tag{1.11}$$

Combining (1.8) and (1.10) there is also an isomorphism

$$\mathrm{Yext}^n_R\,\Big(\bigoplus_i A_i, B\Big) \simeq \prod_i \mathrm{Yext}^n_R\,(A_i, B)$$

and similarly for the second variable using (1.9) and (1.10). We will make this isomorphism explicit using the following notation from [Mac75]:

For an extension $e \in \mathrm{Yext}^n_R(A,B)$ and a homomorphism $\phi \in \mathrm{Hom}(C,A)$, we write $e\phi \in \mathrm{Yext}^n_R(C,B)$ for the pullback sequence of e with ϕ. Note that, if $\psi \in \mathrm{Hom}(D,C)$ is another homomorphism, then $(e\phi)\psi = e(\phi\circ\psi)$ by the fundamental property of a pullback. Similarly we write $\phi e \in \mathrm{Yext}^n_R(A,C)$ for the pushout of e with $\phi \in \mathrm{Hom}(B,C)$ and $\psi(\phi e) = (\psi\circ\phi)e$ holds for $\psi \in \mathrm{Hom}(C,D)$.

Lemma 1.27. *(a) The maps*

$$\begin{array}{ccc} \mathrm{Yext}^n_R(A_1 \oplus A_2, B) & \simeq & \mathrm{Yext}^n_R(A_1,B) \oplus \mathrm{Yext}^n_R(A_2,B) \\ e & \mapsto & (e\iota_1, e\iota_2) \\ e_1\pi_1 + e_2\pi_2 & \leftarrow\!\shortmid & (e_1,e_2) \end{array} \tag{1.12}$$

with canonical embeddings $\iota_i : A_i \hookrightarrow A_1 \oplus A_2$ and projections $\pi_i : A_1 \oplus A_2 \twoheadrightarrow A_i$ are isomorphisms which are compatible with (1.10) and (1.8).

(b) Similarly the maps

$$\begin{array}{ccc} \mathrm{Yext}^n_R(A, B_1 \oplus B_2) & \simeq & \mathrm{Yext}^n_R(A,B_1) \oplus \mathrm{Yext}^n_R(A,B_2) \\ e & \mapsto & (\pi_1 e, \pi_2 e) \\ \iota_1 e_1 + \iota_2 e_2 & \leftarrow\!\shortmid & (e_1,e_2) \end{array}$$

with embeddings $\iota_i : B_i \hookrightarrow B_1 \oplus B_2$ and projections $\pi_i : B_1 \oplus B_2 \twoheadrightarrow B_i$ are isomorphisms which are compatible with (1.9) and (1.10).

Proof. (a) We first show that the map

$$\Phi : \mathrm{Yext}_R^n(A_1 \oplus A_2, B) \to \mathrm{Yext}_R^n(A_1, B) \oplus \mathrm{Yext}_R^n(A_2, B)$$

is compatible with (1.10) and (1.8) and then complete the proof by showing that the maps defined in (1.12) are inverse to each other, i.e. $\Phi \circ \Phi^{-1} = \mathrm{id}$.

Let C_n denote the complex (1.6) used to describe the groups $\mathrm{Ext}_R^n(-, B)$. Let $e \in \mathrm{Yext}_R^n(A_1 \oplus A_2, B)$ be any n-extension and let $\phi \in \mathrm{Hom}(A_1 \oplus A_2, J_n)$ be a representative of the image of e via (1.10), i.e. $e = C_n\phi$. Following (1.8) and (1.10), the components of the image $\Phi(e)$ are $C_n(\phi|_{A_i})$ for $i = 1, 2$, which each satisfy $C_n(\phi|_{A_i}) = C_n(\phi \circ \iota_i) = (C_n\phi)\iota_i = e\iota_i$ using the fundamental property of the pullback. This proves the first part.

Let (e_1, e_2) be a tuple of extensions $e_i \in \mathrm{Yext}_G^n(A_i, B)$. The first component of the image $(\Phi \circ \Phi^{-1})(e_1, e_2) = ((e_1\pi_1 + e_2\pi_2)\iota_i)_{i=1,2}$ is

$$(e_1\pi_1 + e_2\pi_2)\iota_1 = e_1\pi_1\iota_1 + e_2\pi_2\iota_1 = e_1 \,\mathrm{id}_{A_1} + e_2(\pi_2\iota_1)$$

where $\pi_2\iota_1$ is the zero map from A_1 to A_2. Hence, $e_2(\pi_2\iota_1) = e_2 0$ is the trivial extension class in $\mathrm{Yext}_G^n(A_1, B)$ and $(e_1\pi_1 + e_2\pi_2)\iota_1 = e_1 \,\mathrm{id}_{A_1} = e_1$. A similar computation for the second component shows that $(e_1\pi_1 + e_2\pi_2)\iota_2 = e_2$ and therefore $\Phi \circ \Phi^{-1} = \mathrm{id}$.

Part (b) is proved by the dual computations. □

1.3.2 Extensions and cohomology

For a ring R and a finite group G we now consider $R[G]$-modules.

Proposition 1.28. *Let A and B be $R[G]$-modules for some finite group G. If A is finitely generated and free as a $\mathbb{Z}$-module, there is also a cohomological description:*

$$\mathrm{Ext}_{R[G]}^i(A, B) \simeq \hat{H}^i(G, \mathrm{Hom}_{R[G]}(A, B)). \tag{1.13}$$

Proof. [Bro94, Chp. III, Prop. (2.2)]. □

For the rest of this section let A and C be $R[G]$-modules and let A be finitely generated and free as a $\mathbb{Z}$-module. Using Propositions 1.26 and 1.28 there are isomorphisms

$$\mathrm{Yext}_G^n(A, C) \simeq \mathrm{Ext}_G^n(A, C) \simeq \hat{H}^n(G, \mathrm{Hom}(A, C)). \tag{1.14}$$

If $\mathrm{Ext}_G^n(A, C)$ is described using an injective resolution of C, the corresponding Yoneda extension in $\mathrm{Yext}_G^n(A, C)$ can be constructed by the pullback sequence. Similarly, for a projective resolution of A one uses the pushout construction. But the other direction of this isomorphism and the construction of a corresponding cocycle in $\hat{H}^n(G, \mathrm{Hom}(A, C))$ is not as explicit in general.

However, the most interesting case for this thesis is $A = \mathbb{Z}$ and $n = 2$. In this special case, we represent $\mathrm{Ext}^2_G(\mathbb{Z}, -)$ by a fixed projective resolution of $\mathbb{Z}$. The following explicit constructions can be found in the literature:

$$\begin{tikzcd}[column sep=small] & \mathrm{Ext}^2_G(\mathbb{Z}, C) \arrow[dr, bend left, "\phi_1"] & \\ \hat{H}^2(G, C) \arrow[ur, bend left, "\phi_3"] \arrow[rr, bend left, "\phi_2^{-1}"] & & \mathrm{Yext}^2_G(\mathbb{Z}, C) \arrow[ll, bend left, "\phi_2"] \end{tikzcd} \tag{1.15}$$

Again ϕ_1 is the map given by pushout. The other constructions, which are based on the *splitting module* of a cocycle from [NSW00, Chp. III, § 1], are obtained as follows.

Let $\gamma \in \hat{H}^2(G, C)$ be represented by the cocycle $c \in Z^2(G, C)$. Then the module $C(\gamma)$ is defined as a $\mathbb{Z}$-module by

$$C(\gamma) = C \oplus \bigoplus_{\sigma \neq 1} \mathbb{Z} b_\sigma$$

where $\sigma \in G$. The G-action on the free generators b_σ is then defined by $\sigma b_\tau = b_{\sigma\tau} - b_\sigma + c(\sigma, \tau)$ and setting $b_1 = c(1, 1) \in C$. This satisfies the properties of a G-action and is called *splitting module* since $\hat{H}^2(G, C) \to \hat{H}^2(G, C(\gamma))$ maps γ to zero (see [NSW00, Chp. III, § 1, p. 115ff]).

Every exact sequence $0 \to C \to B^0 \to B^1 \to \mathbb{Z} \to 0$ gives rise to two short exact sequences $0 \to W \to B^1 \to \mathbb{Z} \to 0$ and $0 \to C \to B^0 \to W \to 0$ with $W = \ker(B^1 \to \mathbb{Z}) = \mathrm{im}(B^0 \to B^1)$. Below we will use corresponding connecting homomorphisms $\delta_1 : \hat{H}^0(G, \mathbb{Z}) \to \hat{H}^1(G, W)$ and $\delta_2 : \hat{H}^1(G, W) \to \hat{H}^2(G, C)$.

Proposition 1.29. *The isomorphism ϕ_2 is given by:*

$$\begin{aligned} \mathrm{Yext}^2_G(\mathbb{Z}, C) &\simeq \hat{H}^2(G, C) \\ [0 \to C \to B^0 \to B^1 \to \mathbb{Z} \to 0] &\mapsto \delta_2(\delta_1(1 + |G|\mathbb{Z})) \\ [0 \to C \xrightarrow{\subseteq} C(\gamma) \xrightarrow{h} \mathbb{Z}[G] \xrightarrow{\mathrm{aug}} \mathbb{Z} \to 0] &\leftarrow\!\shortmid \gamma \end{aligned}$$

with $h(c) = 0$ for $c \in C$ and $h(b_\sigma) = \sigma - 1$.

Proof. This is based on [NSW00, Chp. III, § 1]. A complete proof is given in [Jan10, Thm. 1.3.7]. □

If G is generated by $g_1, \ldots, g_r$, we consider the projective resolution

$$\mathbb{Z}[G]^r \xrightarrow{g} \mathbb{Z}[G] \xrightarrow{\mathrm{aug}} \mathbb{Z} \longrightarrow 0 \tag{1.16}$$

of $\mathbb{Z}$ where g maps $(a_i) \in \mathbb{Z}[G]^r$ to $\sum_{i=1}^r a_i(g_i - 1)$. For the computation of the isomorphism ϕ_3, we then define $Q = \ker(g)$, let $\iota : Q \hookrightarrow \mathbb{Z}[G]^r$, and use the representation $\mathrm{Ext}^2_G(\mathbb{Z}, C) = \mathrm{Hom}_G(Q, C)/\iota^* \mathrm{Hom}(\mathbb{Z}[G]^r, C)$.

Corollary 1.30. *The isomorphism ϕ_3 is given by restricting the homomorphism*

$$\begin{array}{rrcl} f_\gamma : & \mathbb{Z}[G]^r & \to & C(\gamma) \\ & (a_i)_{i=1\dots r} & \mapsto & \sum_{i=1}^r a_i b_{g_i} \end{array}$$

to Q.

Proof. It is easy to check that f_γ maps elements of Q to C and that the diagram

$$\begin{tikzcd} 0 \arrow[r] & Q \arrow[r, "\subseteq"] \arrow[d, "f_\gamma"] & \mathbb{Z}[G]^r \arrow[r, "g"] \arrow[d, "f_\gamma"] & \mathbb{Z}[G] \arrow[r, "\mathrm{aug}"] \arrow[d, equal] & \mathbb{Z} \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & C \arrow[r, "\subseteq"] & C(\gamma) \arrow[r, "h"] & \mathbb{Z}[G] \arrow[r, "\mathrm{aug}"] & \mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

is commutative. In other words, the homomorphism $f_\gamma \in \mathrm{Hom}_G(Q, C)$ represents the cocycle class γ in $\mathrm{Ext}^2_G(\mathbb{Z}, C)$ via isomorphism ϕ_3. For more details see [Jan10, Thm. 1.3.7]. □

This definition of ϕ_3 satisfies $\phi_1 \circ \phi_3 = \phi_2^{-1}$ by construction and makes diagram (1.15) commute.

1.3.3 Complexes

Let $A^\bullet$ denote a *complex*

$$\cdots \longrightarrow A^{i-1} \xrightarrow{\partial^{i-1}} A^i \xrightarrow{\partial^i} A^{i+1} \longrightarrow \cdots$$

of G-modules A^i with *differentials* $\partial^i : A^i \to A^{i+1}$ satisfying $\partial^{i+1} \circ \partial^i = 0$. It is called *bounded* if only finitely many A^i are non-zero. The *cohomology* of this complex is denoted by $H^i(A^\bullet) = \ker \partial^i / \operatorname{im} \partial^{i-1}$ and it is called *exact* if $H^i(A^\bullet) = 0$ for all i. If $A^\bullet$ is trivial outside degrees i and $i+1$, it always represents an exact sequence

$$0 \longrightarrow H^i(A^\bullet) \longrightarrow A^i \longrightarrow A^{i+1} \longrightarrow H^{i+1}(A^\bullet) \longrightarrow 0.$$

and therefore an element in $\mathrm{Yext}^2_G\big(H^{i+1}(A^\bullet), H^i(A^\bullet)\big)$.

Definition 1.31 (Chain map). *A* map of complexes *(or chain map) $\phi : A^\bullet \to B^\bullet$ between two complexes $A^\bullet$ and $B^\bullet$ with differentials α^i and β^i, respectively, is a family of homomorphisms $\phi_i : A^i \to B^i$ with $\phi_{i+1} \circ \alpha^i = \beta^i \circ \phi_i$ for all i.*

By a *projective resolution* $\cdots \to P_1^\bullet \to P_0^\bullet$ of a complex $A^\bullet$, we indicate compatible projective resolutions $\cdots \to P_1^j \to P_0^j$ of each of the modules A^j such that all diagrams

$$\begin{tikzcd} P_i^j \arrow[r] \arrow[d] & P_{i-1}^j \arrow[d] \\ P_i^{j+1} \arrow[r] & P_{i-1}^{j+1} \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} P_0^j \arrow[r] \arrow[d] & A^j \arrow[d] \\ P_0^{j+1} \arrow[r] & A^{j+1} \end{tikzcd}$$

are commutative.

For short exact sequences one can construct such a projective resolution using the following lemma, called *Horseshoe lemma.* It provides a projective resolution which is exact in every degree.

Lemma 1.32 (Horseshoe). *Let $0 \to A \to B \to C \to 0$ be a short exact sequence of G-modules and let $P_A^\bullet$ and $P_C^\bullet$ be projective resolutions of A and C respectively. Then the sequence $P_B^\bullet$ given by $P_B^i = P_A^i \oplus P_C^i$ is a projective resolution of B and there exist maps of complexes $P_A^\bullet \to P_B^\bullet \to P_C^\bullet$ which is an exact sequences in every degree.*

Proof. [Wei94, Lem. 2.2.8]. □

Explicitly, the maps $P_A^i \to P_B^i \to P_C^i$ in every degree are given by the lifting property of projective modules. For the maps $P_A^i \to P_B^i$ one considers the surjective maps $P_B^0 \twoheadrightarrow B$ and $P_B^i \twoheadrightarrow \operatorname{im}(P_B^i \to P_B^{i-1})$ and one can lift the composite homomorphisms $P_A^0 \to A \to B$ and $P_A^i \to P_A^{i-1} \to \operatorname{im}(P_B^i \to P_B^{i-1})$ as in the following diagrams:

$$\begin{tikzcd} & P_A^0 \arrow[d] \arrow[dl, dashed] \\ P_B^0 \arrow[r, two heads] & B \end{tikzcd} \qquad \begin{tikzcd} & P_A^i \arrow[d] \arrow[dl, dashed] \\ P_B^i \arrow[r, two heads] & \operatorname{im}(P_B^i \to P_B^{i-1}) \end{tikzcd}$$

In particular, these maps can be constructed if the projective modules are actually free modules.

Remark 1.33. A consequence of the Horseshoe lemma is the existence of projective resolutions of a complex $A^\bullet$.

If we denote the differentials of $A^\bullet$ by α^i, then we have short exact sequences $0 \to \ker(\alpha^i) \to A^i \to \operatorname{im}(\alpha^i) \to 0$. Let $P_i^\bullet$ and $Q_i^\bullet$ be projective resolutions of $\ker(\alpha^i)$ and $\operatorname{im}(\alpha^i)$. Then the Horseshoe lemma constructs projective resolutions $R_i^\bullet$ of A^i with maps of complexes $P_i^\bullet \to R_i^\bullet \to Q_i^\bullet$. By [Wei94, Thm. 2.2.6] the inclusion $\operatorname{im}(\alpha^i) \subseteq \ker(\alpha^{i+1})$ also induces chain maps $Q_i^\bullet \to P_{i+1}^\bullet$.

In conclusion, one obtains chain maps $R_i^j \to Q_i^j \to P_{i+1}^j \to R_{i+1}^j$ and since all the maps in this construction will commute, the double complex R is a projective resolution of $A^\bullet$.

A map of complexes $\phi : A^\bullet \to B^\bullet$ directly induces maps $H^i(A^\bullet) \to H^i(B^\bullet)$ on the cohomology groups: these are well-defined by the commutativity of the differentials and ϕ_i.

Definition 1.34 (Quasi-isomorphism). *A map of complexes $\phi : A^\bullet \to B^\bullet$ is called* quasi-isomorphism *if the induced homomorphisms on the cohomology $\phi_i : H^i(A^\bullet) \to H^i(B^\bullet)$ are isomorphisms.*

A complex $A^\bullet$ is called perfect *if it is quasi-isomorphic to a bounded complex $P^\bullet$ which consists of finitely-generated projective modules.*

Note that by [Mil80, Chp. VI, Lem. 8.17] every quasi-isomorphism $P^\bullet \to A^\bullet$, where $P^\bullet$ is a bounded complex of finitely-generated projective modules, also provides a quasi-isomorphism $A^\bullet \to P^\bullet$ and vice-versa.

As an important example, every bounded complex $A^\bullet$ of cohomologically trivial G-modules A^i with finitely generated cohomology groups $H^i(A^\bullet)$ is known to be perfect. This follows from the explicit constructions by Lang [Lan02, Chp. XXI, Prop. 1.1 and 1.2]. To recall Lang's proof we first introduce *mapping cones.*

Definition 1.35 (Mapping cone). *Let $\phi : A^\bullet \to B^\bullet$ be a chain map and denote the differentials of $A^\bullet$ and $B^\bullet$ by α^i and β^i, respectively. The* mapping cone *of ϕ is the complex $C^\bullet$ with $C^i = B^i \oplus A^{i+1}$ and differentials*

$$\begin{aligned}\gamma_i : B^i \oplus A^{i+1} &\to B^{i+1} \oplus A^{i+2}\\ (b, a) \quad &\mapsto (\beta_i(b) + \phi_{i+1}(a), -\alpha_{i+1}(a))\,.\end{aligned}$$

It is denoted by $\mathrm{cone}(\phi)$.

Keeping the notation of the definition, there always is a canonical map $B^\bullet \to C^\bullet$ given by the inclusion $B^i \subseteq C^i = B^i \oplus A^{i+1}$. Moreover, the projections $C^i \twoheadrightarrow A^{i+1}$ induce a chain map between $C^\bullet$ and the *shifted complex* which is given by modules A^{i+1} and differentials $-\partial^{i+1}$ in degree i, i.e. everything is shifted by one to the left. This results in a sequence of complexes

$$A^\bullet \to B^\bullet \to C^\bullet \to A^\bullet[1] \tag{1.17}$$

or equivalently

$$C^\bullet[-1] \to A^\bullet \to B^\bullet \to C^\bullet$$

called *distinguished triangle.* These sequences could be extended infinitely and give rise to a long exact sequence in cohomology.

Corollary 1.36. *For a chain map $\phi : A^\bullet \to B^\bullet$ with mapping cone $C^\bullet = \mathrm{cone}(\phi)$ there is a* long exact sequence

$$\cdots \to H^i(A^\bullet) \to H^i(B^\bullet) \to H^i(C^\bullet) \to H^{i+1}(A^\bullet) \to \cdots\,.$$

If a map of complexes is injective (or surjective), i.e. all its maps are injective (or surjective), then its mapping cone has an easy structure.

Lemma 1.37. *Let $\phi : A^\bullet \to B^\bullet$ be a mapping of complexes. If ϕ is surjective (injective), there exists a canonical quasi-isomorphism:* $\ker(\phi)[1] \xrightarrow{\simeq} \mathrm{cone}(\phi)$ *(or* $\mathrm{cone}(\phi) \xrightarrow{\simeq} \mathrm{coker}(\phi)$ *respectively).*

Proof. Denote the differentials of $A^\bullet$ and $B^\bullet$ by α^i and β^i, respectively. Furthermore, denote the cone by $C^\bullet = \mathrm{cone}(\phi)$ which consists of modules $C^i = B^i \oplus A^{i+1}$ and differentials

$$\begin{aligned}\gamma^i : B^i \oplus A^{i+1} &\to B^{i+1} \oplus A^{i+2}\\ (b, a) \quad &\mapsto \big(\beta^i(b) + \phi_{i+1}(a), -\alpha^{i+1}(a)\big)\,.\end{aligned}$$

(i) Let ϕ be surjective and let $K^\bullet$ be the kernel of ϕ with modules $K^i = \ker(\phi_i : A^i \twoheadrightarrow B^i)$ and differentials $\kappa^i = \alpha^i|_{K^i}$. Then there is a canonical injective map $\psi : K^\bullet[1] \hookrightarrow C^\bullet$ which is given by $\psi_i(x) = (0, x) \in B^i \oplus A^{i+1}$ for $x \in K^{i+1} \subseteq A^{i+1}$. The cokernel of ψ is the complex $D^\bullet$ with modules $D^i = B^i \oplus B^{i+1}$ and differentials $\delta^i(x, y) = (\beta^i(x) + y, -\beta^{i+1}(y))$ which arise from γ^i by projection onto the cokernel. Then we have constructed the following commutative diagram with exact columns:

$$
\begin{tikzcd}
K^\bullet[1] : \arrow[d, hook, "\psi"] & {} \arrow[r, "-\kappa^{i-1}"] & K^i \arrow[r, "-\kappa^i"] \arrow[d, hook, "\psi_{i-1}"] & K^{i+1} \arrow[r, "-\kappa^{i+1}"] \arrow[d, hook, "\psi_i"] & K^{i+2} \arrow[r, "-\kappa^{i+2}"] \arrow[d, hook, "\psi_{i+1}"] & {} \\
C^\bullet : \arrow[d, two heads] & {} \arrow[r, "\gamma^{i-2}"] & B^{i-1} \oplus A^i \arrow[r, "\gamma^{i-1}"] \arrow[d, two heads] & B^i \oplus A^{i+1} \arrow[r, "\gamma^i"] \arrow[d, two heads] & B^{i+1} \oplus A^{i+2} \arrow[r, "\gamma^{i+1}"] \arrow[d, two heads] & {} \\
D^\bullet : & {} \arrow[r, "\delta^{i-2}"] & B^{i-1} \oplus B^i \arrow[r, "\delta^{i-1}"] & B^i \oplus B^{i+1} \arrow[r, "\delta^i"] & B^{i+1} \oplus B^{i+2} \arrow[r, "\delta^{i+1}"] & {}
\end{tikzcd}
$$

The maps δ have kernels and images

$$
\begin{aligned}
\ker(\delta^i) &= \left\{(x, y) \in B^i \oplus B^{i+1} \mid \beta^{i+1}(y) = 0 \ \wedge \ \beta^i(x) + y = 0\right\} \\
\operatorname{im}(\delta^{i-1}) &= \left\{(\beta^{i-1}(x) + y, -\beta^i(y)) \mid x \in B^{i-1}, y \in B^i\right\}.
\end{aligned}
$$

Since $(x, y) = (x, -\beta^i(x)) = \delta^{i-1}(0, x)$ holds for elements $(x, y) \in \ker(\delta^i)$, the complex $D^\bullet$ has trivial cohomology groups $H^i(D^\bullet) = 0$. Hence, the cohomology groups of $K^\bullet[1]$ and $C^\bullet$ are isomorphic.

(ii) For the second statement we let $K^\bullet$ denote the cokernel of ϕ. Consider the canonical projection $\psi : C^\bullet \twoheadrightarrow K^\bullet$ defined by $\psi_i(b, a) = b + \phi_i(A^i) \in B^i/\phi_i(A^i)$. Now $D^\bullet$ denotes the kernel of ψ where the differentials δ^i are the restrictions of γ^i and we get the commutative diagram:

$$
\begin{tikzcd}
D^\bullet : \arrow[d, hook, "\psi"] & {} \arrow[r, "\delta^{i-2}"] & A^{i-1} \oplus A^i \arrow[r, "\delta^{i-1}"] \arrow[d, hook, "\psi_{i-1}"] & A^i \oplus A^{i+1} \arrow[r, "\delta^i"] \arrow[d, hook, "\psi_i"] & A^{i+1} \oplus A^{i+2} \arrow[r, "\delta^{i+1}"] \arrow[d, hook, "\psi_{i+1}"] & {} \\
C^\bullet : \arrow[d, two heads] & {} \arrow[r, "\gamma^{i-2}"] & B^{i-1} \oplus A^i \arrow[r, "\gamma^{i-1}"] \arrow[d, two heads] & B^i \oplus A^{i+1} \arrow[r, "\gamma^i"] \arrow[d, two heads] & B^{i+1} \oplus A^{i+2} \arrow[r, "\gamma^{i+1}"] \arrow[d, two heads] & {} \\
K^\bullet : & {} \arrow[r, "\beta^{i-2}"] & B^{i-1}/\phi(A^{i-1}) \arrow[r, "\beta^{i-1}"] & B^i/\phi(A^i) \arrow[r, "\beta^i"] & B^{i+1}/\phi(A^{i+1}) \arrow[r, "\beta^{i+1}"] & {}
\end{tikzcd}
$$

The maps δ have kernels and images

$$
\begin{aligned}
\ker(\delta^i) &= \left\{(x, y) \in A^i \oplus A^{i+1} \mid \alpha^{i+1}(y) = 0 \ \wedge \ \alpha^i(x) + y = 0\right\} \\
\operatorname{im}(\delta^{i-1}) &= \left\{(\alpha^{i-1}(x) + y, -\alpha^i(y)) \mid x \in A^{i-1}, y \in A^i\right\}.
\end{aligned}
$$

Here $(x, y) = (x, -\alpha^i(x)) = \delta^{i-1}(0, x)$ holds for elements $(x, y) \in \ker(\delta^i)$. This shows $H^i(D^\bullet) = 0$ and, hence, $H^i(C^\bullet) \simeq H^i(K^\bullet)$. $\square$

As an important result which will be essential in the conjectures of Chapters 5 and 6 we prove the following result for bounded complexes.

Proposition 1.38. *A bounded complex $A^\bullet$ of cohomologically trivial G-modules A^i with finitely generated cohomology groups $H^i(A^\bullet)$ is perfect.*

Proof. We recall the constructive proof from [Lan02, Chp. XXI, Prop. 1.1 and 1.2].

Let $A^\bullet$ be a complex with differentials α^i for which $A^i = 0$ for $i \notin \{1, \ldots, n\}$. Then we construct a complex $P^\bullet$ of finitely generated, projective modules and a chain map $\phi : P^\bullet \to A^\bullet$ by descending induction. Let $P^i = 0$, $\phi_i = 0$ for all $i > n$. Then the conditions

$$\begin{aligned} f_k : Z^k(P^\bullet) &\xrightarrow{\phi_k} H^k(A^\bullet) \text{ is surjective} \\ \text{and} \qquad H^j(P^\bullet) &\simeq H^j(A^\bullet) \text{ holds for all } j \geq k+1 \end{aligned} \tag{1.18}$$

is satisfied for $k \geq n+1$.

Induction step in degree i: Assume that (1.18) holds for $k = i+1$ and consider $B^{i+1} := \ker(f_{i+1}) \subseteq P^{i+1}$ for which $\phi_{i+1}(B^{i+1}) \subseteq \mathrm{im}(\alpha^i)$.

Let R^i and Q^i be finitely generated, projective modules with $\rho_i : R^i \twoheadrightarrow B^{i+1}$ and $\bar{q}_i : Q^i \twoheadrightarrow H^i(A^\bullet)$. Then one can again construct corresponding maps $r_i : R^i \to A^i$ and $q_i : Q_i \to Z^i(A)$ as in the following diagrams:

$$\begin{tikzcd} & R^i \arrow[dl, dashed, "\exists r_i"'] \arrow[d, "\phi_{i+1} \circ \rho_i"] \\ A^i \arrow[r, two heads] & \mathrm{im}(\alpha_i) \end{tikzcd} \qquad \begin{tikzcd} & Q^i \arrow[dl, dashed, "\exists q_i"'] \arrow[d, "\bar{q}_i"] \\ Z^i(A^\bullet) \arrow[r, two heads] & H^i(A^\bullet) \end{tikzcd}$$

Note that in degree $i = n$ one has $B^{n+1} = 0$ and one can choose $R^n = 0$. Set $P^i := Q^i \oplus R^i$, $\phi_i(q, r) := q_i(q) + r_i(r)$ and let $P^i \to P^{i+1}$ be the map $(q, r) \mapsto \rho_i(r)$. By construction the conditions (1.18) now hold for $k = i$.

Final step: By induction one has (1.18) for $k = 1$. We consider $B^1 := \ker(f_1) \subseteq P^1$, set $P^0 := B^1$ and $P^i := 0$ for all $i < 0$. Then ϕ is a quasi-isomorphism.

To finish the proof we have to show that B^1 is projective. The cone $C^\bullet := \mathrm{cone}(\phi)$ is a complex which is trivial outside degrees $-1, \ldots, n$ and for which $C^{-1} = P^0 = B^1$, $C^0 = P^1$, $C^n = A^n$ and $C^i = A^i \oplus P^{i+1}$. It is actually an exact sequence

$$0 \longrightarrow C^{-1} \xrightarrow{\gamma^{-1}} C^0 \xrightarrow{\gamma^0} C^1 \xrightarrow{\gamma^1} \cdots \xrightarrow{\gamma^{n-2}} C^{n-1} \xrightarrow{\gamma^{n-1}} C^n \xrightarrow{\gamma^n} 0$$

of length $n+2$ since ϕ is a quasi isomorphism and it induces short exact sequences of the form $0 \to \ker(\gamma^{i-1}) \to C^{i-1} \to \ker(\gamma^i) \to 0$ for $1 \leq i \leq n$. By construction of P^i all the modules C^i and $\ker(\gamma^n) = C^n$ are cohomologically trivial. Therefore, in each of these short exact sequences the cohomological triviality of the right and middle module will imply that the left-hand module is cohomologically trivial.

In conclusion, B^1 is cohomologically trivial and since it is $\mathbb{Z}$-free, it will also be projective. $\square$

1.4 K-theory

The conjectures we address in Chapters 5 and 6 are formulated as equations in relative K-groups for group rings. We will recall their definition from [Swa68] and the most important results. More details can be found in [CR87, Chp. 5] and [Bre04a, Chp. 2].

For a ring A we write $K_0(A)$ for the *Grothendieck group* of finitely generated projective A-modules. This is the free abelian group generated by isomorphism classes (P) for every finitely generated projective A-module P with relations $(P) - (P') - (P'')$ for every short exact sequence $0 \to P' \to P \to P'' \to 0$.

The *Whitehead group* $K_1(A)$ is defined to be the abelianization of the infinite general linear group $\mathrm{Gl}(A)$:

$$K_1(A) := \mathrm{Gl}(A)\big/[\mathrm{Gl}(A), \mathrm{Gl}(A)].$$

By *Whitehead's lemma* the commutator $[\mathrm{Gl}(A), \mathrm{Gl}(A)]$ is generated by elementary matrices $E(A) \subset \mathrm{Gl}(A)$, cf. [CR87, (40.24)]. One can also describe the elements of $K_1(A)$ by isomorphism classes of pairs (P, f) where f is an automorphism of a projective A-module P. These pairs also satisfy certain relations (see [CR87, § 40A] or [Bre04a, § 2.1.2]) and each of them is represented by a pair $(A^n, f) \in K_1(A)$ for some $n \in \mathbb{N}$ and an automorphism f.

Finally, we consider the relative K-group $K_0(A, \phi)$ for a ring homomorphism $\phi : A \to B$. Its objects are triples $[P, f, Q]$ with finitely generated projective A-modules P and Q and an isomorphism $f : B \otimes_A P \to B \otimes_A Q$ of B-modules. For the relations we again refer to [Swa68, p. 215], [CR87, (40.19)] or [Bre04a, § 2.1.3].

The K-groups defined above fit into an exact sequence (see [Swa68, Thm. 15.5] or [CR87, (40.20)]), which we recall in the setting of group rings. Let R be a ring, E an extension of $\mathrm{Quot}(R)$ and G a group. Then the relative K-group $K_0(R[G], \phi)$ corresponding to the homomorphism $\phi : R[G] \to E[G]$ induced by $R \subseteq E$ is also denoted by $K_0(R[G], E)$ and there is an exact sequence

$$K_1(R[G]) \to K_1(E[G]) \xrightarrow{\partial^1_{G,E}} K_0(R[G], E) \xrightarrow{\partial^0_{G,E}} K_0(R[G]) \to K_0(E[G]). \quad (1.19)$$

The maps $K_i(R[G]) \to K_i(E[G])$ for $i = 0, 1$ are induced by the operator $E[G] \otimes_{R[G]} -$ and the other maps are given by $\partial^1_{G,E}((E[G]^n, f)) = [R[G]^n, f, R[G]^n]$ and $\partial^0_{G,E}([P, f, Q]) = [P] - [Q]$.

Let H be a subgroup of G. Then every $R[H]$-module P gives rise to an $R[G]$-module $R[G] \otimes_{R[H]} P$. The induced *induction maps* on the associated K-groups will be denoted by ind_H^G.

Before we continue, we fix the following notations and recall some well-known facts from representation theory [CR81]. For a finite group G we write χ for a character with values in $\mathbb{C}$ associated to a representation $\rho : G \to \mathrm{Gl}_n(\mathbb{C})$. The set of irreducible $\mathbb{C}$-characters will be denoted by $\mathrm{Irr}_{\mathbb{C}}(G)$ and the complex conjugate to χ by $\bar{\chi}$.

By *Wedderburn's theorem* the center of the group ring $\mathbb{C}[G]$ will decompose into

$$\mathrm{Z}(\mathbb{C}[G]) \simeq \bigoplus_{\chi \in \mathrm{Irr}_{\mathbb{C}}(G)} \mathbb{C}.$$

For a subfield $F \subseteq \mathbb{C}$ the image of $\mathrm{Z}(F[G])$ in $\mathrm{Z}(\mathbb{C}[G])$ consists of tuples $(a_\chi)_\chi$ for which $a_{\sigma \circ \chi} = \sigma(a_\chi)$ for all $\sigma \in \mathrm{Aut}(\mathbb{C}|F)$, e.g. see [Ble10, Lem. 2.8]. We are therefore especially interested in characters $\chi \in \mathrm{Irr}_{\mathbb{C}}(G)$ modulo relations $\chi = \sigma \circ \psi$ for $\sigma \in \mathrm{Aut}(\mathbb{C}|F)$ and denote these characters by $\mathrm{Irr}_F(G)$.

1.4.1 Reduced norms and boundary homomorphisms

For every central simple K-algebra A there exists a *reduced norm map* $\mathrm{nr}_{A|K}$ on A into its center K as in [CR81, § 7D]. This also carries over to the group $K_1(A)$ where the reduced norm map, denoted by nr, is injective by [CR87, (45.3)] (see also [BF01, Prop. 2.2]).

For semi-simple K-algebras A one has to consider the *Wedderburn decomposition* $A \simeq \bigoplus_{i=1}^r A_i$ which induces decompositions $\mathrm{Z}(A) \simeq \bigoplus_{i=1}^r \mathrm{Z}(A_i)$ and $K_1(A) \simeq \bigoplus_{i=1}^r K_1(A_i)$, cf. [CR87, (38.29)]. This gives a well-defined reduced norm map

$$\mathrm{nr} : K_1(A) \to \mathrm{Z}(A)^\times \simeq \bigoplus_{i=1}^r K_i^\times$$

with $K_i := \mathrm{Z}(A_i)$.

We continue to consider the group ring case $E[G]$ for an extension $E|\mathbb{Q}$ which includes the m-th roots of unity with $m = \exp(G)$ denoting the exponent of G. Then $\mathrm{Irr}_E(G) = \mathrm{Irr}_{\mathbb{C}}(G)$ and since $E[G]$ is a semi-simple algebra, we have a reduced norm map

$$\mathrm{nr} : K_1(E[G]) \to \mathrm{Z}(E[G])^\times \simeq \bigoplus_{\chi \in \mathrm{Irr}_E(G)} E^\times$$

which is still injective.

Let $\rho : G \to \mathrm{Gl}_{\chi(1)}(E)$ denote a representation associated to χ and T_χ its linear continuation to $E[G]$. An element $\lambda \in K_1(E[G])$ is represented by a matrix $A = (a_{ij}) \in \mathrm{Gl}_n(E[G])$ for some $n \in \mathbb{N}$ and its reduced norm is given by

$$\mathrm{nr}(\lambda) = \big(\mathrm{det}_\chi(A)\big)_{\chi \in \mathrm{Irr}_E(G)} = \Big(\det\big((T_\chi(a_{ij}))_{ij}\big)\Big)_{\chi \in \mathrm{Irr}_E(G)}$$

where $(T_\chi(a_{ij}))_{ij}$ is a matrix of size $n\chi(1) \times n\chi(1)$. Note that these reduced norms can explicitly be computed as described in [BW09, § 3.3].

The injective reduced norm map provides a map $\widehat{\partial}^1_{R[G],E} = \partial^1_{R[G],E} \circ \mathrm{nr}^{-1}$ from $\mathrm{im}(\mathrm{nr})$ to $K_0(R[G],E)$ called *boundary homomorphism*.

The two cases we are interested in are the following. For $R = \mathbb{Z}_p$ and E an extension of $\mathbb{Q}_p$ the norm map is an isomorphism by [CR87, (45.3)] and we directly obtain a map $\widehat{\partial}^1_{G,E} := \widehat{\partial}^1_{\mathbb{Z}_p[G],E} = \partial^1_{\mathbb{Z}_p[G],E} \circ \mathrm{nr}^{-1}$ from $\mathrm{Z}(E[G])^\times$ to $K_0(\mathbb{Z}_p[G],E)$.

$$\begin{tikzcd}
\mathrm{Z}(E[G])^\times \arrow[dr, dashed, "\widehat{\partial}^1_{G,E}"] & \\
K_1(E[G]) \arrow[u, "\mathrm{nr}"', "\simeq"] \arrow[r, "\partial^1"] & K_0(\mathbb{Z}_p[G],E)
\end{tikzcd}$$

For $R = \mathbb{Z}$ and F and extension of $\mathbb{Q}$ the norm map is not surjective but the decomposition

$$K_0(\mathbb{Z}[G],\mathbb{Q}) \simeq \coprod_p K_0(\mathbb{Z}_p[G],\mathbb{Q}_p), \tag{1.20}$$

and the *weak approximation theorem* still allow us to define a map $\widehat{\partial}^1_{G,F}$ from $\mathrm{Z}(F[G])^\times$ to $K_0(\mathbb{Z}[G],F)$ by $\widehat{\partial}^1_{G,F}(x) := \widehat{\partial}^1_{\mathbb{Z}[G],F}(\lambda x) - \sum_p \widehat{\partial}^1_{\mathbb{Z}_p[G],\mathbb{Q}_p}(\lambda)$ where the summation ranges over all primes and $\lambda \in \mathrm{Z}(\mathbb{Q}[G])^\times \subseteq \mathrm{Z}(\mathbb{Q}_p[G])^\times$ must be chosen such that $\lambda x \in \mathrm{im}(\mathrm{nr})$. One can show that this definition does not depend on the choice of λ and provides a well-defined map from $\mathrm{Z}(F[G])$ to $K_0(\mathbb{Z}[G],F)$, cf. [BF01, § 4.2]:

$$\begin{tikzcd}
\mathrm{Z}(F[G])^\times \arrow[dr, dashed, "\widehat{\partial}^1_{G,F}"] & \\
K_1(F[G]) \arrow[u, hook, "\mathrm{nr}"'] \arrow[r, "\partial^1"] & K_0(\mathbb{Z}[G],F)
\end{tikzcd}$$

Altogether, we have well-defined maps

$$\begin{aligned}
&\partial^1_{G,E} : \mathrm{Z}(E[G])^\times \to K_0(\mathbb{Z}_p[G],E) \quad \text{for } E/\mathbb{Q}_p,\\
\text{and}\quad &\widehat{\partial}^1_{G,F} : \mathrm{Z}(F[G])^\times \to K_0(\mathbb{Z}[G],F) \quad \text{for } F/\mathbb{Q}
\end{aligned}$$

called *extended boundary homomorphisms*. In particular, the latter map will be used for $F = \mathbb{R}$.

Remark 1.39. In the local case the map $\partial^1 : K_1(E[G]) \twoheadrightarrow K_0(\mathbb{Z}_p[G],E)$ is surjective by [CR87][(39.10)] (see also [Bre04a, Lem. 2.5]). The extended boundary homomorphism $\widehat{\partial}^1_{G,E} : \mathrm{Z}(E[G])^\times \to K_0(\mathbb{Z}_p[G],E)$ is therefore also surjective. Consider an element in $K_0(\mathbb{Z}_p[G],E)$ given by a triple $[A,\theta,B]$ with projective $\mathbb{Z}_p[G]$-modules A, B and an isomorphism $\theta : A_E \xrightarrow{\simeq} B_E$ with $A_E = E[G] \otimes_{\mathbb{Z}_p[G]} A$ and $B_E = E[G] \otimes_{\mathbb{Z}_p[G]} B$. Then one can explicitly construct a preimage in $\mathrm{Z}(E[G])^\times$ as follows, cf. [BW09, § 4].

Projective modules over local rings are free. We therefore let $a_1, \dots, a_n$ and $b_1, \dots, b_n$ be $\mathbb{Z}_p[G]$-bases of A and B. Then the map θ is represented by a matrix $T \in \mathrm{Gl}_n(E[G])$ corresponding to bases $1 \otimes a_1, \dots, 1 \otimes a_n$ and $1 \otimes b_1, \dots, 1 \otimes b_n$ of A_E and B_E.

The matrix $T \in \mathrm{Gl}_n(E[G])$ represents an element in $K_1(E[G])$ for which $\partial^1(T) = [A, \theta, B]$. The norm $\mathrm{nr}(T)$ therefore represents the element $[A, \theta, B]$ in $\mathrm{Z}(E[G])^\times$.

1.4.2 Euler characteristics

Given a perfect complex Q of $R[G]$ modules, one can define corresponding elements in $K_0(R[G], E)$ which are called *Euler characteristics* of Q. These elements can also be defined in more general settings, but we will restrict to the case of group rings. For such a complex Q, let Q_E denote the complex of $E[G]$-modules which is obtained from Q by applying the operator $(-)_E := E[G] \otimes_{R[G]} -$. An isomorphism $t : H^+(Q_E) \xrightarrow{\simeq} H^-(Q_E)$ between the sum of cohomology groups in even and odd degree is called a *trivialization*.[4]

Let P be a bounded complex of finitely generated projective $R[G]$-modules. Applying the operator $(-)_E$ to the short exact sequences

$$\begin{aligned} & 0 \to B^i(P) \to Z^i(P) \to H^i(P) \to 0 \\ \text{and} \quad & 0 \to Z^i(P) \to P^i \to B^{i+1}(P) \to 0 \end{aligned}$$

maintains exactness and one obtains isomorphisms $Z^i(P_E) \simeq B^i(P_E) \oplus H^i(P_E)$ and $P_E^i \simeq Z^i(P_E) \oplus B^{i+1}(P_E)$ by choosing splittings. The trivialization t then induces an isomorphism $t_* : P_E^+ \xrightarrow{\simeq} P_E^-$ as follows:

$$\begin{aligned} t_* : P_E^+ &= \bigoplus_{i \text{ even}} P_E^i \simeq \bigoplus_{i \text{ even}} \big(Z^i(P_E) \oplus B^{i+1}(P_E)\big) \simeq \bigoplus_{i \text{ even}} H^i(P_E) \oplus \bigoplus_{i} B^i(P_E) \\ &\xrightarrow{t} \bigoplus_{i \text{ odd}} H^i(P_E) \oplus \bigoplus_{i} B^i(P_E) \simeq \bigoplus_{i \text{ odd}} \big(Z^i(P_E) \oplus B^{i+1}(P_E)\big) \simeq \bigoplus_{i \text{ odd}} P_E^i \\ &= P_E^-. \end{aligned}$$

Burns then introduced the following definition (see [Bur04, § 2][5]) which uses the inverse of t_*.

Definition 1.40 (Euler characteristic). *For a bounded complex P of finitely generated projective $R[G]$-modules and a trivialization $t : H^+(P_E) \to H^-(P_E)$ the* refined Euler characteristic *is defined by*

$$\bar{\chi}_{R[G],E}(P, t) = \big[P^-, (t_*)^{-1}, P^+\big] \in K_0(R[G], E).$$

[4] Sometimes trivializations are also defined to go from odd to even degree.

[5] In that paper the refined Euler characteristic is denoted by $\chi_{R[G]}(P, t)$ with t being a trivialization from odd to even degree.

Burns proved that this element in $K_0(R[G],E)$ is well-defined. Note that by the relations in $K_0(R[G],E)$ it is equal to $-\left[P^+,t_*,P^-\right]$.

The definition can also be extended to perfect complexes: if Q is a perfect complex of $R[G]$ modules with trivialization t and $\pi : P \to Q$ is a quasi-isomorphism with P being a bounded complex of finitely generated projective $R[G]$ modules, then $\pi : H^i(P) \simeq H^i(Q)$ induces a trivialization on P, denoted by $\pi^{-1}t\pi$, and one can set

$$\bar{\chi}_G(Q,t) := \bar{\chi}_G(P,\pi^{-1}t\pi) \in K_0(R[G],E).$$

By Burns [Bur04, Lem. 2.3] this element is again well-defined and the refined Euler characteristic is invariant under quasi-isomorphism.

Note, that Burns used trivializations from odd to even degree in his original definition. His refined Euler characteristic $\chi_{R[G]}$ from [Bur04] therefore satisfies $\chi_{R[G]}(Q,t^{-1}) = \bar{\chi}_{R[G],E}(Q,t)$. This should not lead to confusion because in any case it is clear how a trivialization t induces an isomorphism $Q_E^- \xrightarrow{\simeq} Q_E^+$. We will always use trivializations from even to odd degree as in the more recent definition of the refined Euler characteristic which we introduce in the following.

Burns and Breuning defined a canonical Euler characteristics $\chi_{R[G],E}$ in a more general setting and could first prove under which conditions triangles $A \to B \to C \to A[1]$ as in (1.17) with compatible trivializations t_A, t_B and t_C satisfy the additivity criterion

$$\chi_{R[G],E}(B,t_B) = \chi_{R[G],E}(A,t_A) + \chi_{R[G],E}(C,t_C),$$

cf. [BrB05, Cor. 6.6]. For K-groups of group rings their refined Euler characteristic satisfies the following relation.

Proposition 1.41. *The two definitions of Euler characteristics satisfy*

$$\chi_{R[G],E}(Q,t) = -\bar{\chi}_{R[G],E}(Q,t) + \partial_G^1((B^-(Q_E),-\mathrm{id})) \in K_0(R[G],E) \tag{1.21}$$

with $B^-(Q_E) := \bigoplus_{i \text{ odd}} B^i(Q_E)$.

Proof. [BrB05, Thm. 6.2]. □

Since we do not need the details of the construction of this canonical Euler characteristic, we will simply take this relation as the definition for $\chi_{R[G],E}(Q,t)$. This Euler characteristic has the advantage of interacting conveniently with shifted complexes. Also the latter term in the above equation can be proved to vanish in some cases.

Proposition 1.42. *(a)* $\chi_{R[G],E}(Q[1],t^{-1}) = -\chi_{R[G],E}(Q,t)$,

(b) $\partial_G^1((B^+(Q_E),-\mathrm{id})) = 0$ *if* Q *is acyclic outside degrees* 1 *and* 2.

Proof. [BrB05, Prop. 5.6, Lem. 6.3 and Rem. 6.4]. □

For the two Euler characteristics one can then deduce the following identities.

Corollary 1.43. *One has the following relations for a perfect complex Q and a trivialization $t : H^+(Q_E) \to H^-(Q_E)$:*

(a) $\chi_{R[G],E}(Q,t) = \chi_{R[G],E}(Q[2],t)$ *and* $\bar{\chi}_{R[G],E}(Q,t) = \bar{\chi}_{R[G],E}(Q[2],t)$

(b) If Q_E is acyclic outside two consecutive degrees i and $i+1$, then

  (i) $\chi_{R[G],E}(Q,t) = -\bar{\chi}_{R[G],E}(Q,t)$ *if* $2|(i+1)$,

  (ii) $\chi_{R[G],E}(Q,t) = \bar{\chi}_{R[G],E}(Q[-1],t^{-1})$ *if* $2|i$.

Proof. Part (a) follows from the definition of $\bar{\chi}$. For part (b) one can do the following computations: $\chi_{R[G],E}(Q,t) = \chi_{R[G],E}(Q[i-1],t) = -\bar{\chi}_{R[G],E}(Q[i-1],t) = -\bar{\chi}_{R[G],E}(Q,t)$ for odd integers i and $\chi_{R[G],E}(Q,t) = -\chi_{R[G],E}(Q[i-1],t^{-1}) = \bar{\chi}_{R[G],E}(Q[i-1],t^{-1}) = \bar{\chi}_{R[G],E}(Q[-1],t^{-1})$ for even integers i. $\square$

In the cases we consider in this thesis, the complex Q will be a bounded complex of finitely generated, cohomologically trivial modules. Then one can construct a perfect complex P quasi-isomorphic to Q using [Lan02, XXI, Prop. 1.1 and 1.2] as in Proposition 1.38.

In recent papers (e.g. [BrB07]) the more natural definition by $\chi_{R[G],E}$ is preferred. But the older definition of Burns is still of interest because it can be explicitly computed by definition.

In our applications, we will often consider a complex Q as in the following examples. As for the extended boundary homomorphism one may think of the two important cases: $R = \mathbb{Z}$, $\mathbb{Q} \subseteq E \subseteq \mathbb{R}$ or $R = \mathbb{Z}_p$, $\mathbb{Q}_p \subseteq E \subseteq \mathbb{C}_p$.

Example 1.44. Consider a complex $Q = \left[A \xrightarrow{f} B\right]$ of finitely generated, cohomologically trivial $R[G]$ modules which is trivial outside degrees $\{0,1\}$ and a trivialization $t : H^0(Q) \otimes E[G] \xrightarrow{\simeq} H^1(Q) \otimes E[G]$ for which we want to compute the Euler characteristic $\bar{\chi}_{R[G],E}(Q,t) \in K_0(R[G],E)$.

(a) First assume that both, A and B, are projective $R[G]$-modules. Then we have to consider the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & H^0(Q) \arrow[r] & A \arrow[rr, "f"] \arrow[dr] & & B \arrow[r] & H^1(Q) \arrow[r] & 0 \\ & & & W \arrow[ur] & & & \end{tikzcd}$$

in which $W := \ker(B \to \operatorname{coker}(f))$ and the Euler characteristic is

$$\bar{\chi}_{R[G],E}(Q,t) = \left[B,\theta,A\right] \in K_0(R[G],E).$$

where $\theta = (t_*)^{-1}$ is the isomorphism $B_E \simeq W_E \oplus H^1(Q)_E \xrightarrow{t^{-1}} W_E \oplus H^0(Q)_E \simeq A_E$.

(b) If B is projective and A is cohomologically trivial, we first need to construct a complex of projective modules which is quasi-isomorphic to Q. To this end, let $0 \to K \to F \to A \to 0$ be a two-term projective resolution of A with a free $R[G]$-module F. For example, if A is generated by r elements, one can choose $F = R[G]^r$. The kernel K will then be cohomologically trivial and $\mathbb{Z}$-torsion-free, and thus projective by [Bro94, Chp. VI, Thm. (8.10)].

Then the complex $P = \big[K \to F \to B\big]$ with K placed in degree -1 is a complex of finitely generated projective modules where the right-hand map is the composite $F \twoheadrightarrow A \to B$. This projective resolution gives a chain map $\pi : P \to Q$ as in the following diagram

$$\begin{tikzcd}
P\colon \arrow[d, "\pi"] & K \arrow[r] \arrow[d] & F \arrow[r] \arrow[d, two heads] & B \arrow[d, equal] \\
Q\colon & 0 \arrow[r] & A \arrow[r] & B
\end{tikzcd}$$

The map π is a quasi-isomorphism by

$$\begin{aligned}
H^{-1}(P) &= \ker(K \to F) = 0 = H^{-1}(Q), \\
H^{0}(P) &= \ker(F \to B)/K = \ker(A \to B) = H^{0}(Q), \\
\text{and}\quad H^{1}(P) &= \operatorname{coker}(F \to B) = \operatorname{coker}(A \to B) = H^{1}(Q).
\end{aligned}$$

From the definition of the Euler characteristic we then obtain

$$\bar{\chi}_{R[G],E}(Q, t) = \bar{\chi}_{R[G],E}(P, \pi^{-1} t \pi) = \big[K \oplus B, \theta, F\big] \in K_0(R[G], E).$$

The isomorphism θ can be computed very explicitly (see also [BlB03, Eq. (20)] or [BlBr08]) from the trivialization t using the following diagram

$$\begin{tikzcd}
& K \arrow[r, equal] \arrow[d, hook] & K \arrow[d, hook] & & & & \\
0 \arrow[r] & X \arrow[r] \arrow[d, two heads] & F \arrow[rr] \arrow[d, two heads] & & B \arrow[r] \arrow[d, equal] & H^1(P) \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & H^0(Q) \arrow[r] & A \arrow[rr, "f"] \arrow[dr, two heads] & & B \arrow[r] & H^1(Q) \arrow[r] & 0 \\
& & & W \arrow[ur, hook] & & &
\end{tikzcd}$$

in which again $W := \ker(B \to \operatorname{coker}(f))$. By choosing appropriate splittings of the maps $B_E \twoheadrightarrow H^1(Q)_E$, $A_E \twoheadrightarrow W_E$ and $F_E \twoheadrightarrow A_E$, one has isomorphisms $\rho_1 : B_E \xrightarrow{\simeq} W_E \oplus H^1(Q)_E$, $\rho_2 : A_E \xrightarrow{\simeq} W_E \oplus H^0(Q)_E$, and $\rho_3 : F_E \xrightarrow{\simeq} K_E \oplus A_E$ and θ is given by

$$\begin{aligned}
\theta : (K \oplus B)_E &\xrightarrow{\mathrm{id},\rho_1} K_E \oplus W_E \oplus H^1(Q)_E \xrightarrow{\mathrm{id},\mathrm{id},t^{-1}} K_E \oplus W_E \oplus H^0(Q)_E \\
&\xrightarrow{\mathrm{id},\rho_2^{-1}} K_E \oplus A_E \xrightarrow{\mathrm{id},\rho_3^{-1}} F_E.
\end{aligned} \tag{1.22}$$

(c) In a very special case of the latter example, the module A is *finite* and $B = 0$. Then $H^1(Q) = W$ and $H^0(Q)_E$ are trivial and the trivial map $t = 0$ is a trivialization (it is actually the only trivialization). Considering (1.22) one observes that the induced map t_* is actually the identity map $K_E \to F_E$ given by $K \subseteq F$. So the Euler characteristic is:

$$\bar{\chi}_{R[G],E}(Q,0) = \big[K, \mathrm{id}, F\big] \in K_0(R[G],E).$$

(d) As a last example, we consider the shifted complex $Q[-1] = \big[A \xrightarrow{-f} B\big]$ where A is placed in degree 1. For the computation of the Euler characteristic $\bar{\chi}_{R[G],E}(Q[-1],t^{-1})$ one can proceed as in (b) by switching even and odd degree.

However, one has to account for the signs in the maps that are introduced by the shifting process. In general, all the splittings obtained from $0 \to Z^i(Q) \to Q^i \to B^{i+1}(Q) \to 0$ in the computation of t_* will change by a sign (see [Bur04, Thm. 2.1(3) and p. 46]).

In this example this just affects the splitting of $A_E \twoheadrightarrow W_E$ and therefore the isomorphism $\rho_2 : A_E \xrightarrow{\simeq} W_E \oplus H^0(Q)_E$ changes by a sign. Let $\bar{\theta}$ denote the isomorphism (1.22) which incorporates this sign change in ρ_2. Then the refined Euler characteristic of $Q[-1]$ is

$$\bar{\chi}_{R[G],E}(Q[-1],t^{-1}) = \big[F, \bar{\theta}^{-1}, K \oplus B\big] = -\big[K \oplus B, \bar{\theta}, F\big] \in K_0(R[G],E).$$

Note that the complex $Q^{-1} = \big[A \xrightarrow{-f} B\big]$ with A in degree 0 is the inverse of Q considered as 2-extensions in $\mathrm{Yext}^2_G(H^1(Q), H^0(Q))$, see Remark 1.25. Since the complexes Q^{-1} and $Q[-1]$ differ from each other only in the fact that even and odd degrees are interchanged, their Euler characteristic differs by a sign:

$$\bar{\chi}_{R[G],E}(Q[-1],t^{-1}) = -\bar{\chi}_{R[G],E}(Q^{-1},t).$$

Since $Q[-1]$ is acyclic outside degrees 1 and 2, this implies

$$\chi_{R[G],E}(Q,t) = -\chi_{R[G],E}(Q[-1],t^{-1}) = \bar{\chi}_{R[G],E}(Q[-1],t^{-1}) = -\big[K \oplus \mathbb{Z}[G], \bar{\theta}, F\big].$$

by Corollary 1.43 and therefore we have the following simple relation:

$$\chi_{R[G],E}(Q,t) = -\bar{\chi}_{R[G],E}(Q^{-1},t).$$

1.5 L-functions

The conjectures we will address in Chapters 5 and 6 relate algebraic invariants to analytic values from L-functions. In the following section we recall the analytic results needed in this thesis. An overview of these facts can be found in [BrB07, § 2.3], for more details and background information we refer to [Bre04a, Frö83, Mar77] and [Neu92].

Let $L|K$ be a Galois extension of number fields with Group G and places v, w of K and L such that $w|v$. Then we consider the following local L-functions from [Frö83, Chp. I, § 5].

Definition 1.45 (Local Artin L-function). *Let w be a finite place of L and χ a character of G_w corresponding to the Galois-representation $\rho : G_w \to \mathrm{Gl}(V_\chi)$. Then the group G_w acts on $\mathrm{Gl}(V_\chi)$ via ρ and one defines the* local Artin L-function *by*

$$L_{L_w|K_v}(\chi, s) = \det\left(1 - \varphi_w \, \mathrm{N}_{K_v|\mathbb{Q}_p} \mathfrak{p}_{K_v}^{-s} \mid V_\chi^{I_\mathfrak{P}}\right)^{-1}.$$

Hereby, $\mathfrak{p}_{K_v}$ is the prime ideal of K_v, φ_w denotes a lift of the Frobenius automorphism in G_w/I_w, and the characteristic polynomial of $\rho(\varphi_w) \in \mathrm{Gl}(V_\chi^{I_\mathfrak{P}})$ is evaluated at $\mathrm{N}_{K_v|\mathbb{Q}} \mathfrak{p}_{K_v}^{-s}$.

For infinite places w we set $n = \dim_\mathbb{C}(V)$, $n^+ = \dim_\mathbb{C}(V^{G_w})$ and $n^- = n - n^+$ and define

$$L_{L_w|K_v}(\chi, s) = \begin{cases} \left(\pi^{-s/2}\Gamma(s/2)\right)^{n^+} \left(\pi^{-(s+1)/2}\Gamma((s+1)/2)\right)^{n^-} & \text{for } K_v = \mathbb{R}, \\ \left(2(2\pi)^{-s}\Gamma(s)\right)^n & \text{for } K_v = \mathbb{C}. \end{cases}$$

We let $\bar{\chi}$ denote the complex conjugate of χ, $W(\chi)$ the *Artin root number* and $\mathfrak{f}(\chi)$ the *conductor* of χ as defined by Fröhlich in [Frö83, Chp. I, § 5] and recall his definition of the *ε-function* from and the related Galois Gauss sum from (see also [Mar77, Chp. II, § 4]).

Definition 1.46 (ε-function, Galois Gauss sum). *For every character χ of G_w we define the* ε-function

$$\varepsilon_{L_w|K_v}(\chi, s) = \begin{cases} W_{\mathbb{Q}_p}(\mathrm{i}_{K_v}^{\mathbb{Q}_p}\bar{\chi})\left(\mathrm{N}_{K_v|\mathbb{Q}_p}(d_{K_v})^{\chi(1)} \, \mathrm{N}_{K_v|\mathbb{Q}_p}(\mathfrak{f}(\chi))\right)^{\frac{1}{2}-s} & \text{for } K_v|\mathbb{Q}_p, \\ W_\mathbb{R}(\mathrm{i}_{K_v}^{\mathbb{R}}\bar{\chi}) & \text{for } K_v|\mathbb{R} \end{cases}$$

and the local Galois Gauss sum *is given by*

$$\tau_{L_w|K_v}(\chi) = W_{K_v}(\bar{\chi})\sqrt{\mathrm{N}_{K_v|\mathbb{Q}_p} \mathfrak{f}(\chi)} \in \mathbb{C}$$

where d_{K_v} denotes the absolute discriminant of K_v.

Note that by the relations on root numbers and Artin conductors, the value of the ε-function $\varepsilon_{L_w|\mathbb{Q}_p}(\chi, 0)$ coincides with the Galois Gauss sum $\tau_{L_w|\mathbb{Q}_p}(\chi)$, cf. [Bre04a, § 3.4.4].

To define corresponding global functions we consider the localizations $L_w|K_v$ for all places w. We let S denote all places of K, S_f all the finite places of K, and for every $v \in S$ we fix a place w of L with $w|v$. Moreover, every character χ of G can be restricted to the decomposition group G_w of some place w to give a local character χ_w of G_w.

Definition 1.47. *For a Galois extension $L|K$ of global fields we define the* completed Artin L-function*, the* global ε-function*, and the* global Galois Gauss sum *by*

$$\Lambda_{L|K}(\chi,s) = \prod_{v\in S} L_{L_w|K_v}(\chi_w,s),$$
$$\varepsilon_{L|K}(\chi,s) = \prod_{v\in S} \varepsilon_{L_w|K_v}(\chi_w,s),$$
$$\textit{and} \quad \tau_{L|K}(\chi) = \prod_{v\in S_f} \tau_{L_w|K_v}(\chi).$$

Proposition 1.48. *The global Artin L-function is a meromorphic function defined on all $s\in\mathbb{C}$ and satisfies the* functional equation

$$\Lambda_{L|K}(\bar\chi,s) = \varepsilon_{L|K}(\chi,s)\ \Lambda_{L|K}(\chi,1-s).$$

For a finite set of places S of K we also consider the *S-truncated Artin L-function* of a character χ

$$L_{L|K,S}(\chi,s) = \prod_{v\notin S} L_{L_w|K_v}(\chi,s).$$

Its leading term in the Laurent-series expansion at $s=s_0$ will be denoted by $L^*_{L|K,S}(\chi,s_0)$.

Combining those series and functions for all $\chi\in\mathrm{Irr}_{\mathbb{C}}(G)$ defines *equivariant* functions[6]

$$\begin{aligned}\Lambda_{L|K}(s) &= (\Lambda_{L|K}(\chi,s))_{\chi\in\mathrm{Irr}_{\mathbb{C}}(G)},\\ \varepsilon_{L|K}(s) &= (\varepsilon_{L|K}(\chi,s))_{\chi\in\mathrm{Irr}_{\mathbb{C}}(G)},\\ \text{and}\quad \zeta_{L|K,S}(s) &= (L_{L|K,S}(\chi,s))_{\chi\in\mathrm{Irr}_{\mathbb{C}}(G)}.\end{aligned}\tag{1.23}$$

By definition these functions have values in $\mathrm{Z}(\mathbb{C}[G])^\times$ which by the *Wedderburn decomposition* is canonically isomorphic to $\prod_{\chi\in\mathrm{Irr}(G)}\mathbb{C}^\times$. Finally, the leading term in the Laurent-series expansion of $\zeta_{L|K,S}(s)$ at $s=s_0$ will be denoted by

$$\zeta^*_{L|K,S}(s_0) = (L^*_{L|K,S}(\chi,s_0))_{\chi\in\mathrm{Irr}_{\mathbb{C}}(G)}.$$

Note that the values $\varepsilon_{L|K}(0)$ and $\zeta^*_{L|K,S}(1)$ we will consider in Chapters 5 and 6 are actually values in $\mathrm{Z}(\mathbb{R}[G])^\times$, cf. [Bre04a, Lem. 3.12] and [BrB07, Lem. 2.7].

[6]Note that there exist different definitions in the literature, in particular for the equivariant functions. The definitions presented here coincides with those given in [BrB07] which is also our main reference for the equivariant Tamagawa number conjectures considered in Chapters 5 and 6.

Brauer Groups and Fundamental Classes

2 Brauer groups

The Brauer group $\mathrm{Br}(K)$ of a (local or global) number field K is an ascending union of relative Brauer groups:

$$\mathrm{Br}(K) \simeq \bigcup_L \mathrm{Br}(L|K) \simeq \bigcup_L \hat{H}^2(\mathrm{Gal}(L|K), L^\times),$$

where L runs through Galois extensions of K, see Section 1.2. We are therefore especially interested in the computation of cohomology groups $\hat{H}^2(\mathrm{Gal}(L|K), L^\times)$ for Galois extensions $L|K$ of number fields.

In the first part of this chapter, we will consider finite Galois extension $L|K$ of *local* fields over $\mathbb{Q}_p$, for which we also want to compute the *local fundamental class* in $\hat{H}^2(\mathrm{Gal}(L|K), L^\times)$. In this thesis, the computation of this special generator is especially motivated by the epsilon constant conjecture which is discussed in Chapter 5.

But local fundamental classes are also of independent interest. As a first application, their computation will also make computations in relative Brauer groups for number fields possible. Furthermore, according to the Shafarevic-Weil theorem [AT68, Chp. XV, Thm. 6] local fundamental classes can be used to compute Galois groups of local fields [Gre10].

2.1 Computing local Brauer groups

Let $L|K$ be a finite Galois extension of local fields over $\mathbb{Q}_p$ with group G. In the following section we will consider the computation of the finite cyclic group $\hat{H}^2(G, L^\times)$.

To compute the cohomology group $\hat{H}^q(G, M)$ for a finite group G, a finitely generated G-module M and small q, one can directly use the definition. For $q = 0, -1$ they are defined as in Section 1.1 and for $q \geq 1$ one considers the standard resolution of M

$$C^0(G, M) \xrightarrow{\partial_1} C^1(G, M) \xrightarrow{\partial_2} C^2(G, M) \xrightarrow{\partial_3} C^3(G, M) \longrightarrow \cdots$$

where $C^q(G, M)$ are the cochain groups, i.e. $C^0(G, M) = M$ and $C^q(G, M)$, $q \geq 1$, are the maps $G^q \to M$. With the present restrictions on G and M one can write $C^q(G, M)$ as (finitely-generated) $\mathbb{Z}$-module and explicitly represent the $\mathbb{Z}$-linear maps ∂_q by matrices. In this case the computation of $\hat{H}^q(G,M) = \ker \partial_{q+1} / \operatorname{im} \partial_q$ is pure linear algebra.[1]

However, for $q \geq 2$ the matrices for which kernels have to be computed can become very large (depending on the representation of G and M). For $q = 2$ one therefore describes $\hat{H}^q(G,M)$ by extension classes of M by G. A detailed overview of existing algorithms and details on the implementation in the computer algebra system Magma [BCP97] is given in [Hol06]. For algorithms on abelian groups and basic algorithms in number theory we refer to [Coh93].

In order to work with cohomology groups computationally, we therefore always need a finitely generated module M. In the case of local Brauer groups the module $L^\times$ is not finitely generated. Hence, we first need to find a finitely-generated module M for which $\hat{H}^2(G,M) \simeq \hat{H}^2(G,L^\times)$ holds. Such a module can be constructed as follows, cf. [Ble03, BlBr08].

Lemma 2.1. *There exists a finitely generated module M such that $\hat{H}^2(G,M) \simeq \hat{H}^2(G,L^\times)$. It is given by $M := L^\times / \exp(\mathscr{L})$ for a suitable full projective sublattice $\mathscr{L}$ of $\mathcal{O}_L$, where $\mathscr{L}$ can be constructed computationally.*

Proof. We briefly recall the construction of $\mathscr{L}$ from [Ble03, § 3.1]:

Suppose $\theta \in \mathcal{O}_L$ is a *normal basis element* for the extensions $L|K$, i.e. $\{\sigma\theta \mid \sigma \in G\}$ is a basis of $L|K$. Such an element can be computed using an algorithm by Girstmair [Gir99]. However, one discovers that "almost every" element in $\mathcal{O}_L$ is a normal basis element, and one can assume that $v_L(\theta) > e(L|\mathbb{Q}_p)/(p-1)$, $e(L|\mathbb{Q}_p)$ denoting the ramification index of $L|\mathbb{Q}_p$. Then $\mathscr{L} := \mathbb{Z}[G]\theta$ is a full projective sublattice of $\mathcal{O}_L$ on which the exponential function is injective.

Since $\mathscr{L}$ is a full lattice, the quotient $M := L^\times / \exp(\mathscr{L})$ is finitely generated and it inherits the G-structure from $L^\times$. The module $\exp(\mathscr{L})$ will again be projective and therefore cohomologically trivial. Hence, the long exact cohomology sequence associated to

$$0 \longrightarrow \exp(\mathscr{L}) \longrightarrow L^\times \longrightarrow L^\times / \exp(\mathscr{L}) \longrightarrow 0$$

implies $\hat{H}^2(G,L^\times) \simeq \hat{H}^2(G,M)$. □

Remark 2.2. Note that in general one can represent elements in the local field L only up to a finite precision. In order to do exact computations, for example concerning the Galois action on $L^f := L^\times / \exp(\mathscr{L})$, we will therefore consider completions of global Galois extensions of number fields.

[1] This is obviously also true in other cases, e.g. for $K[G]$-modules M which are finitely-generated over $\mathbb{Z}$ and where K is a field extension of $\mathbb{Q}$.

Let E/F be a global Galois extension of number fields with group Γ and $\mathfrak{P}$ a prime ideal in E dividing a prime ideal $\mathfrak{p}$ of F. Then $E_{\mathfrak{P}}/F_{\mathfrak{p}}$ is a local Galois extension, whose Galois group is the decomposition group $\Gamma_{\mathfrak{P}}$ of $\mathfrak{P}$:

$$\Gamma\left(\begin{array}{c} E \\ | \\ F \end{array}\right. \qquad \begin{array}{c} \mathfrak{P} \\ | \\ \mathfrak{p} \end{array} \qquad\qquad \left.\begin{array}{c} E_{\mathfrak{P}} = L \\ | \\ F_{\mathfrak{p}} = K \end{array}\right) G = \Gamma_{\mathfrak{P}}$$

In this case the normal basis element θ, the lattice $\mathscr{L}$, the k-units $U_L^{(k)}$ and the quotient $L/U_L^{(k)} \simeq E_{\mathfrak{P}}^\times/U_{E_{\mathfrak{P}}}^{(k)} \simeq \pi^{\mathbb{Z}} \times \big(\mathcal{O}_{E_{\mathfrak{P}}}^\times/U_{E_{\mathfrak{P}}}^{(k)}\big) \simeq \pi^{\mathbb{Z}} \times \big(\mathcal{O}_E/\mathfrak{P}^k\big)^\times$ can be computed globally, cf. [BlBr08, § 4.2.3]. If k is chosen such that $\mathfrak{P}^k \subseteq \mathscr{L}$, then the module $L^f = L^\times/\exp(\mathscr{L})$ is the cokernel of $\exp(\mathscr{L}) \to E_{\mathfrak{P}}^\times/U_{E_{\mathfrak{P}}}^{(k)}$ and it suffices to compute the values of the exponential function up to a certain precision, cf. [Ble03, Rem. 3.6].

From now on, L^f will always denote a finitely generated module for which there is an isomorphism in cohomology $\hat{H}^2(G, L^f) \simeq \hat{H}^2(G, L^\times)$. As explained above, the cohomology of $L^f := L^\times/\exp(\mathscr{L})$ can be computed by applying linear algebra methods to the standard resolution of L^f. In Magma, the command `CohomologyGroup` computes $\hat{H}^2(G, L^f)$ as an abstract group, together with maps from and to $Z^2(G, L^f)$. Hence, for cocycles $G \times G \to L^\times$ one can then algorithmically decide whether they are coboundaries (mapped to zero in $\hat{H}^2(G, L^f)$) or whether they differ by a coboundary (mapped to the same element of $\hat{H}^2(G, L^f)$).

Algorithm 2.3 (Local Brauer group).
Input: A finite Galois extension $L|K$ of local fields over $\mathbb{Q}_p$ with Galois group G.

Output: The group $\hat{H}^2(G, L^f) \simeq \hat{H}^2(G, L^\times)$ and maps to and from $Z^2(G, L^f)$.

1 Compute a normal basis element θ with $v_L(\theta) > e(L/\mathbb{Q}_p)/(p-1)$ and define $\mathscr{L} = \mathbb{Z}[G]\theta$.

2 Compute the module $L^f := L^\times/\exp(\mathscr{L})$.

3 Compute the cohomology group $\hat{H}^2(G, L^f)$ using Magma, as described in [Hol06].

Remark 2.4. If $\mathfrak{P}^k \subseteq \mathscr{L} \subseteq \mathfrak{P}^\ell$ for the prime ideal $\mathfrak{P}$ of L, then $\ell \leq k$ and there are surjective maps $L^\times/U_L^{(k)} \twoheadrightarrow L^\times/\exp(\mathscr{L}) \twoheadrightarrow L^\times/U_L^{(\ell)}$. On the cocycle groups this gives homomorphisms

$$Z^2\big(G, L^\times/U_L^{(k)}\big) \to Z^2\big(G, L^\times/\exp(\mathscr{L})\big) \to Z^2\big(G, L^\times/U_L^{(\ell)}\big).$$

Therefore, every cochain in $x \in C^2(G, L^\times)$ satisfying the cocycle condition[2]

$$x(\sigma\tau, \rho) + x(\sigma, \tau) = \sigma x(\tau, \rho) + x(\sigma, \tau\rho)$$

modulo $U^{(k)}$ defines a unique element in $\hat{H}^2(G, L^f)$. Similarly an element in $Z^2(G, L^f)$ determines a cochain in $C^2(G, L^\times)$ up to a precision $m \geq \ell$. Those cochains in $C^2\big(G, L^\times/U_L^{(m)}\big)$, $m \in \mathbb{N}$ will be called *cocycles of precision m*.

Furthermore, the isomorphism $\hat{H}^2(G, L^\times) \xrightarrow{\simeq} \hat{H}^2(G, L^f)$ is induced by the homomorphism $L^\times \twoheadrightarrow L^f = L^\times/\exp(\mathscr{L})$ which factors through $L^\times \twoheadrightarrow L^\times/U_L^{(k)}$ since $U_L^{(k)} \subseteq \exp(\mathscr{L})$. On the cohomology groups this induces the following homomorphisms:

$$\begin{tikzcd}
\hat{H}^2(G, L^\times) \arrow[rr, "\simeq"] & & \hat{H}^2(G, L^f) \\
Z^2(G, L^\times) \arrow[u, two heads] \arrow[dr] & & Z^2(G, L^f) \arrow[u, two heads] \\
& Z^2\big(G, L^\times/U_L^{(k)}\big) \arrow[ur] &
\end{tikzcd}$$

Therefore, every element in $\hat{H}^2(G, L^f)$ is represented by a cocycle of precision k in $Z^2\big(G, L^\times/U_L^{(k)}\big)$, i.e.

$$Z^2\big(G, L^\times/U_L^{(k)}\big) \twoheadrightarrow \hat{H}^2(G, L^f).$$

The algorithm above (or a similar variant) has already been implemented in Magma by Fieker, but is not yet available in the official version. Some algorithms in this thesis, for example those discussed in Section 2.3, are based on an own implementation[3] which computes the cohomology group for extensions of small degree (i.e. ≤ 20) within a few minutes.

2.2 Local fundamental classes

Now that we can compare cocycles and decide whether they are coboundaries etc. we are interested in computing their invariant, i.e. the image of a cocycle under the invariant map

$$\mathrm{inv} : \hat{H}^2(G, L^\times) \longrightarrow \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}.$$

In other words, if L^f denotes the finitely generated module $L^\times/\exp(\mathscr{L})$ from Lemma 2.1, we want to find the local fundamental class $u_{L|K} \in \hat{H}^2(G, L^f) \simeq \hat{H}^2(G, L^\times)$ whose image is $\mathrm{inv}(u_{L|K}) = \frac{1}{[L:K]} + \mathbb{Z}$. By the construction of L^f there

[2]See equation (1.1).
[3]Command `LocalBrauerGroup`, see documentation in Appendix B.1 on page 172.

exists an integer $k \in \mathbb{N}$ such that $\mathfrak{P}^k \subseteq \mathscr{L}$ and a cocycle of precision k determines an element in $\hat{H}^2(G, L^f)$ uniquely.

In the case where $L|K$ is an unramified extension, the invariant map is a canonical map which can be computed very explicitly. Then the Galois group of $L|K$ is cyclic and generated by the *Frobenius automorphism* φ. If q is the cardinality of the residue class field $\mathcal{O}_K/\mathfrak{P}_K$ of K, then the Frobenius automorphism satisfies $\varphi(x) \equiv x^q \mod \mathfrak{P}_L$ for elements $x \in \mathcal{O}_L$. Let π be any uniformizing element of K. Then by Remark 1.7 the cocycle

$$c(\varphi^i, \varphi^j) = \begin{cases} 1 & \text{if } i+j < [L:K] \\ \pi & \text{if } i+j \geq [L:K] \end{cases} \tag{2.1}$$

is a representative for the local fundamental class.

Below we discuss two methods for the computation of the local fundamental class in the general case:

(a) *Direct method:* Use the definition of local fundamental classes for general extensions $L|K$ directly (see Definition 1.6): Let N be an unramified extension of same degree and use the inflation maps to identify $\hat{H}^2(\mathrm{Gal}(N|K), N^\times)$ and $\hat{H}^2(\mathrm{Gal}(L|K), L^\times)$ in $\hat{H}^2(\mathrm{Gal}(LN|K), (LN)^\times)$.

(b) *Serre's approach:* A new algorithm based on theory in [Ser79, Chp. XI, § 2].

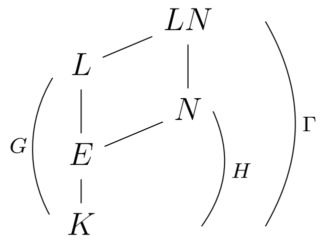
The first method will not be very efficient, but it is included because it can be considered to be the *standard method*. There are also a few other methods, which we will now discuss briefly.

For example one can construct the local fundamental class by computing with algebras. If $L|K$ is an arbitrary local Galois extension and $N|K$ the unramified extension of the same degree, then one has isomorphisms $\mathrm{Br}(L|K) \simeq H^2(L|K) \simeq H^2(N|K) \simeq \mathrm{Br}(N|K)$. Therefore, every K-algebra $A \in \mathrm{Br}(L|K)$ is equivalent to an algebra $B \in \mathrm{Br}(N|K)$ and vice versa. The identification of A and B can be made explicit and this provides a method for the construction of the local fundamental class. This was studied in detail in [Rot05] and has been implemented in Pari/Gp [Par08]. However, it turns out to be inefficient even for extensions of degree smaller than 10 over $\mathbb{Q}_p$.

Tamely ramified extensions $L|K$ have a Galois group G with cyclic inertia subgroup H and a maximal unramified subextension $L^H|K$ whose Galois group G/H is generated by the Frobenius automorphism φ. In this case G is always generated by two elements and one can construct the local fundamental class as described by Chinburg in [Chi85, § 6]. This approach has been implemented by Janssen [Jan10, § 3.1] and is actually the most efficient algorithm for this special case.

2.2.1 Direct method

As in Definition 1.6 we want to compute the local fundamental class of an extension $L|K$ using the fundamental class of an unramified extension $N|K$ of the same degree $[N:K]=[L:K]$. If we denote the maximal unramified extension in $L|K$ by E, i.e. $E = L \cap N$, we have the following situation:



Let us further denote the Galois groups involved by $G = \mathrm{Gal}(L|K)$, $H = \mathrm{Gal}(N|K)$ and $\Gamma = \mathrm{Gal}(LN|K)$.

Then the local fundamental class of L is defined to be the fundamental class of N by identifying their cohomology groups as subgroups of $\hat{H}^2(\Gamma, (LN)^\times)$ using inflation maps:

$$\begin{tikzcd}
 & \hat{H}^2(H, N^\times) \arrow[d, hook, "\mathrm{inf}"] \\
\hat{H}^2(G, L^\times) \arrow[r, hook, "\mathrm{inf}"] & \hat{H}^2(\Gamma, (LN)^\times)
\end{tikzcd}$$

For the construction of the local fundamental class, we consider the module L^f constructed in the previous section. Let $\mathscr{L}$ be the module from Lemma 2.1 such that $L^f := L^\times/\exp(\mathscr{L})$ is cohomologically isomorphic to $L^\times$ and let k be the smallest integer such that $\mathfrak{P}^k \subseteq \mathscr{L}$. Then by Remark 2.4 there is a surjective homomorphism $Z^2\big(G, L^\times/U_L^{(k)}\big) \twoheadrightarrow \hat{H}^2(G, L^f)$ and every element in $\hat{H}^2(G, L^f)$ is represented by a cocycle of precision k. It is therefore sufficient to compute the image of the local fundamental class in $\hat{H}^2\big(G, L^\times/U_L^{(k)}\big)$.

In [BlBr08, § 2.4] the authors show that the local fundamental class can be computed up to given precision n by considering the commutative diagram

$$\begin{tikzcd}
 & \hat{H}^2(H, N^\times) \arrow[d, hook, "\mathrm{inf}"] \\
\hat{H}^2(G, L^\times) \arrow[r, hook, "\mathrm{inf}"] \arrow[d] & \hat{H}^2(\Gamma, (LN)^\times) \arrow[d] \\
\hat{H}^2\big(G, L^\times/U_L^{(n)}\big) \arrow[r, hook, "\mathrm{inf}"] & \hat{H}^2\big(\Gamma, (LN)^\times/U_{LN}^{(n)}\big)
\end{tikzcd}$$

in which the bottom inflation map, induced by $L^\times \subseteq (LN)^\times$, is injective by [BlBr08, Lem. 2.5].

As the modules $L^\times/U_L^{(n)}$ and $(LN)^\times/U_{LN}^{(n)}$ are finitely generated, we can compute their cohomology groups. The local fundamental class $u_{N|K}$ of the unramified extension $N|K$ is represented by the cocycle of the form (2.1) and we can compute its inflation $\inf(u_{N|K}) \in Z^2(\Gamma,(LN)^\times)$ and its image in $\hat{H}^2\big(\Gamma,(LN)^\times/U_{LN}^{(n)}\big)$. For each generator of the group $\hat{H}^2\big(G,L^\times/U_L^{(n)}\big)$ we can also compute its inflation in $\hat{H}^2\big(\Gamma,(LN)^\times/U_{LN}^{(n)}\big)$. One of these generators must coincide with the image of $\inf(u_{N|K})$ and it represents the local fundamental class in $\hat{H}^2\big(G,L^\times/U_L^{(n)}\big)$.

Therefore, the definition of a local fundamental class for arbitrary extensions $L|K$ can directly be turned into an algorithm.

Algorithm 2.5 (Local fundamental class: direct method).
Input: A finite Galois extension $L|K$ over $\mathbb{Q}_p$ with group G and a precision $n \in \mathbb{N}$.

Output: The local fundamental class $u_{L|K} \in Z^2\big(G,L^\times/U_L^{(n)}\big)$ up to the finite precision n.

1 Let N be the unramified extension of K of degree $[L:K]$ and c a cocycle representing the local fundamental class $u_{N|K}$ as in (2.1).

2 Compute the cohomology group $\hat{H}^2\big(G,L^\times/U_L^{(n)}\big)$ and the group of boundaries $B^2\big(\Gamma,(LN)^\times/U_{LN}^{(n)}\big)$ using [Hol06].

3 Compute the inflation $\inf_{N|K}^{LN|K}(c) \in Z^2(\Gamma,(LN)^\times) \twoheadrightarrow \hat{H}^2\big(\Gamma,(LN)^\times/U_L^{(n)}\big)$.

4 Find a generator $g \in \hat{H}^2\big(G,L^\times/U_L^{(n)}\big)$ such that its inflation $\inf_{L|K}^{LN|K}(g) \in C^2\big(\Gamma,(LN)^\times/U_{LN}^{(n)}\big)$ satisfies $\inf_{N|K}^{LN|K}(c) - \inf_{L|K}^{LN|K}(g) \in B^2\big(\Gamma,(LN)^\times/U_{LN}^{(n)}\big)$.

Return: A representative of g in $Z^2\big(G,L^\times/U_L^{(n)}\big)$.

Notice that for the comparison in $\hat{H}^2\big(\Gamma,(LN)^\times/U_{LN}^{(n)}\big)$ in step 4 it is actually sufficient to compute the boundaries $B^2\big(\Gamma,(LN)^\times/U_{LN}^{(n)}\big)$. Considering the computation time this makes a huge difference to the computation of $\hat{H}^2\big(\Gamma,(LN)^\times/U_{LN}^{(n)}\big)$.

This direct method, however, turns out to be ineffective even for number fields of small degree. In the following example we compare the computation times of the implementation[4] of Algorithm 2.5 in Magma for some number fields.

[4]Command `LocalFundamentalClassDirect`, see documentation in Appendix B.1 on page 172.

Example 2.6. We compare the computation time[5] of the local fundamental class using the direct method in four extensions $L_i|\mathbb{Q}_p$. For each extension one has to consider the unramified extension N_i of degree $[L_i : \mathbb{Q}_p]$ over $\mathbb{Q}_p$ and the composite field L_iN_i.

We consider the following fields (with polynomials from the database [KM01]):

1. The totally ramified extension $L_1|\mathbb{Q}_3$ with group S_3 generated by $x^6 + 3 \in \mathbb{Z}[x]$,
2. the totally ramified extension $L_2|\mathbb{Q}_2$ with group D_4 generated by $x^8+38x^4+1 \in \mathbb{Z}[x]$,
3. the extension $L_3|\mathbb{Q}_5$ with group D_5 generated by $x^{10} - 10x^8 + 30x^7 + 90x^6 - 162x^5 + 125x^4 + 90x^3 - 80x^2 - 120x + 144 \in \mathbb{Z}[x]$ which has ramification index 5, and
4. the extension $L_4|\mathbb{Q}_3$ generated by $x^{12} - 6x^{11} - 30x^{10} + 190x^9 + 171x^8 - 1740x^7+124x^6+6420x^5-2409x^4-9630x^3+3330x^2+5214x-659 \in \mathbb{Z}[x]$ with ramification index 3 and whose Galois group is the generalized quaternion group Q_{12} of order 12.

In those examples, the Magma implementation of Algorithm 2.5 performed for the precisions $n = 10$ and $n = 20$ as shown in the following table:

				timings [min]	
extension	group	$\deg(L_i)$	$\deg(L_iN_i)$	$n = 10$	$n = 20$
$L_1\|\mathbb{Q}_3$	S_3	6	36	0.5	1.5
$L_2\|\mathbb{Q}_2$	D_4	8	64	12	30
$L_3\|\mathbb{Q}_5$	D_5	10	50	180	490
$L_4\|\mathbb{Q}_3$	Q_{12}	12	36	60	160

Table 2.1: Computation times for local fundamental classes using the direct method.

In all the examples most of the time is spent on the computation of the n-units $U_{L_iN_i}^{(n)}$ and their Galois-action, taking more than 90 percent of the time. To be able to compare these timings, the four fields L_i were constructed as an extension of $\mathbb{Q}_p$ which was known up to a precision of 50. However, one still has to be careful with the comparisons since the performance of computations in local fields also

[5] All computations were performed with Magma version 2.15-9 on a dual core AMD Opteron machine with 1.8 GHz and 16 GB memory.

depends on the field itself (i.e. its discriminant) and on the size of the prime p (which determines the size of the residue class field).

In any case, to double the precision of the local fundamental class, the duration was multiplied by a factor of about 2.5 in all the examples, which seems to be polynomial in n. But one also notices that the algorithm depends more on the degree of L_i and becomes inefficient for extensions of degree larger than 10.

2.2.2 Serre's approach

Serre describes in [Ser79, Chp. XI, § 2] and especially Exercise 2 from Chapter XIII § 5 how one can theoretically find the local fundamental class of an extension $L|K$. Chinburg used these results to describe a construction for tamely ramified extensions [Chi85, § 6] which has recently been implemented in MAGMA [Jan10].

Below we use the same theory to deduce a new algorithm for the general case. As in the direct method we will again work in the composite field LN. The main advantage will be the avoidance of the computation of any cohomology group in the construction of a cocycle representing the local fundamental class. But before we address the algorithm itself we have to introduce more theory.

Let E be the maximal unramified subextension of $L|K$ and $d := [E : K]$. Denote the maximal unramified extension of K by $\widetilde{K}$ and the Frobenius automorphism of $\widetilde{K}|K$ by φ, such that its Galois group is $\mathrm{Gal}(\widetilde{K}|K) = \overline{\langle\varphi\rangle}$ and $\mathrm{Gal}(\widetilde{K}/E) = \overline{\langle\varphi^d\rangle}$.

The maximal unramified extension of L is $\widetilde{L} = L\widetilde{K}$ and the Galois group of $\widetilde{L}|K$ is given by $\mathrm{Gal}(\widetilde{L}|K) = \{(\tau, \sigma) \in \mathrm{Gal}(\widetilde{K}|K) \times G \,\big|\, \sigma|_E = \tau|_E\}$. Furthermore, we consider the tensor product $L_{nr} := \widetilde{K} \otimes_K L$ for which we have the following representation:

Lemma 2.7. *(i) The map*

$$\begin{aligned} L_{nr} = \widetilde{K} \otimes_K L &\to \prod_{i=0}^{d-1} \widetilde{L} \\ a \otimes b &\mapsto \big(ab, \varphi(a)b, \ldots, \varphi^{d-1}(a)b\big) \end{aligned}$$

is an isomorphism.

(ii) The Galois action of $\mathcal{G} := \overline{\langle\varphi\rangle} \times G$ *on elements* $y = (y_0, y_1, \ldots, y_{d-1}) \in \prod_{i=0}^{d-1} \widetilde{L}$ *induced by this isomorphism is given (for* $\sigma \in G$*) by*

$$\begin{aligned} (\varphi \times 1)(y) &= \big(y_1, y_2, \ldots, y_{d-1}, \varphi^d(y_0)\big), \\ (\varphi^j \times \sigma)(y) &= \big(\hat\sigma(y_0), \hat\sigma(y_1), \ldots, \hat\sigma(y_{d-1})\big), \\ &\qquad \textit{if } \hat\sigma \in \mathrm{Gal}(\widetilde{L}|K) \textit{ satisfies } \hat\sigma|_L = \sigma \textit{ and } \hat\sigma|_{\widetilde{K}} = \varphi^j, \\ \textit{and} \qquad (1 \times \sigma)(y) &= \big(\varphi^{-j} \times 1\big)\big(\hat\sigma(y_0), \hat\sigma(y_1), \ldots, \hat\sigma(y_{d-1})\big). \end{aligned}$$

Proof. (i) Let $x \in L_{nr}$ be an element which maps to zero. Then x is an element of a finite extension, i.e. if $x = \sum_{i=0}^{m} a_i \otimes b_i$ then all the elements a_i generate a finite extension $K_0|E$ in $\widetilde{K}$, such that $x \in L_{nr}^0 := K_0 \otimes L$. Denote $L_0 = LK_0$, then we have to show that $L_{nr}^0 = \prod_{i=0}^{d-1} L_0$.

Denote the degrees of the extensions by $d = [E : K], m = [L : E]$ and $n = [K_0 : E] = [L_0 : L]$. Choose bases $\{\alpha_1, \dots, \alpha_d\}, \{\beta_1, \dots, \beta_m\}$ and $\{\gamma_1, \dots, \gamma_n\}$ of $E|K$, $L|E$ and $K_0|E$, respectively. Then $x \in L_{nr}^0$ is given by $x = \sum_{i,j,k,l} \lambda_{ijkl}\alpha_i\gamma_j \otimes \alpha_l\beta_k$, with $\lambda_{ijkl} \in K$ and $1 \le i, l \le d, 1 \le j \le n, 1 \le k \le m$. The assumption that x is mapped to zero is equivalent to

$$\begin{aligned}
& \sum_{i,j,k,l} \lambda_{ijkl}\sigma(\alpha_i\gamma_j)\alpha_l\beta_k = 0 \quad \forall \sigma \in \{\varphi^i \mid 0 \le i \le d-1\} \\
\Leftrightarrow \quad & \sum_i \left(\sum_l \lambda_{ijkl}\alpha_l \right) \sigma(\alpha_i) = 0 \quad \forall \sigma, j, k \\
\Leftrightarrow \quad & \sum_l \lambda_{ijkl}\alpha_l = 0 \quad \forall i, j, k
\end{aligned}$$

since $\sigma(\gamma_j)\beta_k$ form a basis of $L_0|E$ and $\det(\sigma(\alpha_i)) \neq 0$. The latter equation then implies that all $\lambda_{ijkl} = 0$ and this proves the injectivity.

As L_{nr}^0 and $\prod_{i=0}^{d-1} L_0$ have the same (finite) dimension over K, the K-linear map $L_{nr}^0 \to \prod_{i=0}^{d-1} L_0$ must also be surjective. This proves the statement since every element in L_{nr} lies in a finite subextension.

(ii) We prove the $\mathcal{G}$-action for primitive tensors. This immediately implies the general case (finite sum of primitives) since Galois automorphisms are homomorphisms.

Let $y = (y_i)_{i=0..d-1}$ be represented by a primitive tensor $a \otimes b$ which is mapped to $(\varphi^i(a)b)_{i=0..d-1}$ with $a \in \widetilde{K}$ and $b \in L$. Then

$$\begin{aligned}
(\varphi \times 1)y = \varphi(a) \otimes b \mapsto \left(\varphi^{i+1}(a)b\right)_{i=0..d-1} &= \left(\varphi(a)b, \dots, \varphi^{d-1}(a)b, \varphi^d(ab)\right) \\
&= \left(y_1, \dots, y_{d-1}, \varphi^d(y_0)\right)
\end{aligned}$$

since $\varphi^d(b) = b$ for all $b \in L$.

If $\hat{\sigma} \in \mathrm{Gal}(\widetilde{L}|K)$ satisfies $\hat{\sigma}|_L = \sigma$ and $\hat{\sigma}|_{\widetilde{K}} = \varphi^j$, then the action of $(\varphi^j \times \sigma)$ is given by:

$$\begin{aligned}
(\varphi^j \times \sigma)y = \varphi^j(a) \otimes \sigma(b) \mapsto \left(\varphi^{i+j}(a)\sigma(b)\right)_{i=0..d-1} &= \left(\hat{\sigma}(\varphi^i(a)b)\right)_{i=0..d-1} \\
&= \left(\hat{\sigma}(y_0), \hat{\sigma}(y_1), \dots, \hat{\sigma}(y_{d-1})\right).
\end{aligned}$$

The action of $(1 \times \sigma)$ is directly given by the other two cases by choosing some $\hat{\sigma}$ with $\hat{\sigma}|_L = \sigma$ and determining $j \in \mathrm{N}$ such that $\hat{\sigma}|_{\widetilde{K}} = \varphi^j$. $\square$

Remark 2.8. (1) According to this lemma, L_{nr} is obtained by inducing the module $\widetilde{L}$ from $\mathrm{Gal}(\widetilde{L}|K)$ to $\mathcal{G}$, and we also write $L_{nr} = \mathrm{ind}_{\mathrm{Gal}(\widetilde{L}|K)}^{\mathcal{G}} \widetilde{L}$.

(2) In the action of $(1 \times \sigma) \in \mathcal{G}$ one can choose $\hat{\sigma}$ to be any automorphism extending σ. There always exists a unique automorphism $\hat{\sigma} \in \mathrm{Gal}(\widetilde{L}|K)$ such that $\hat{\sigma}|_L = \sigma$ and $\left(\hat{\sigma}|_{\widetilde{K}}\right)^{-1} = \varphi^j$ with $j \in \{0, \dots, d-1\}$. If E is the maximal unramified of K in L and $\sigma|_E = \varphi^i$, $1 \le i \le d$, then j is given by $j = d - i$. If $\hat{\sigma}$ is always chosen to be this unique automorphism, the Galois action can be defined by:

$$\begin{aligned}(1 \times \sigma)(y) &= (\varphi^j \times 1)\big(\hat{\sigma}(y_0), \hat{\sigma}(y_1), \dots, \hat{\sigma}(y_{d-1})\big) \\ &= \big(\hat{\sigma}(y_j), \dots, \hat{\sigma}(y_{d-1}), \varphi^d(\hat{\sigma}(y_0)), \dots, \varphi^d(\hat{\sigma}(y_{j-1}))\big).\end{aligned} \tag{2.2}$$

This choice has the advantage that $(\varphi \times 1)$ is applied as few as possible to compute the Galois action. From now on, we will always assume that $\hat{\sigma}$ is chosen this way.

Let $\widehat{L}$ be the completion of the maximal unramified extension $\widetilde{L}$ of L. Then the residue class field of $\widehat{L}$ is algebraically closed.

Lemma 2.9. *For every $c \in U_{\widehat{L}}$ there exists $x \in \widehat{L}^\times$ such that $x^{\varphi^d - 1} = c$.*

Proof. This is [Neu92, Chp. V, Lem. 2.1] or [Ser79, Chp. XIII, Prop. 15] applied to the totally ramified extension L/E with φ^d generating $\mathrm{Gal}(\widetilde{K}/E)$. Since this will be an essential part of the algorithm, we sketch the constructive proof of [Neu92].

Denote the residue class field of $\widehat{L}$ by κ, the cardinality of the residue class field of E by q. Since κ is algebraically closed, one finds a solution to $x^{\varphi^d} \equiv x^q \equiv xc$ in κ and lifting this solution one can write $c = x_1^{\varphi^d - 1} a_1$ with $x_1 \in U_{\widehat{L}}$ and $a_1 \in U_{\widehat{L}}^{(1)}$. Similarly, one finds $x_2 \in U_{\widehat{L}}^{(1)}$ and $a_2 \in U_{\widehat{L}}^{(2)}$ such that $a_1 = x_2^{\varphi^d - 1} a_2$. Proceeding this way one has

$$c = (x_1 x_2 \cdots x_n)^{\varphi^d - 1} a_n, \quad x_1 \in U_{\widehat{L}},\ x_i \in U_{\widehat{L}}^{(i-1)},\ a_n \in U_{\widehat{L}}^{(n)} \tag{2.3}$$

and passing to the limit solves the equation in $\widehat{L}^\times$. □

A solution of type (2.3) will be called a *solution of precision n*.

Remark 2.10. (1) The constructive proof can directly be turned into an algorithm. First, consider the equations $x^{\varphi^d} = xc$ and $x^{\varphi^d} a_{i+1} = x a_i$ as polynomial equations over the residue class field of $\mathcal{O}_L$. If the factorization of the equation does not offer a linear factor (which means that the equation cannot be solved in L), generate an appropriate unramified extension L' of L and solve the equation there. From then on, consider the equations as polynomial equations over the residue class field of $\mathcal{O}_{L'}$ and continue with the construction of the solution.

Each step will increase the precision of the solution by at least one and might introduce a new finite extension. So we have an algorithm, which finds a solution of precision k in a finite extension $L'|L$ with $L' \subseteq \widehat{L}$ for any given $k \in \mathbb{N}$.

However, this can produce very large extensions L' and will even be inefficient for a small number of steps.

(2) In special cases, one can prove that solutions of arbitrary large (but still finite) precision can be constructed in a fixed extension F of L. For example consider the following case:

Let F be a finite unramified extension of L. Then the Galois group $H := \mathrm{Gal}(F|L)$ is generated by the Frobenius automorphism φ^d. Since $F|L$ is unramified, the group $\hat{H}^{-1}(H, U_F) = {}_{\mathrm{N}_H}U_F / I_H U_F$ is trivial. In other words, the equation $x^{\varphi^d - 1} = c$ has a solution $x \in U_F$ for every element $c \in U_F$ having norm $\mathrm{N}_{F|L}(c) = 1$, i.e. $c \in {}_{\mathrm{N}_H}U_F$.

Hence, given such an element c of norm one, we can find a solution $x \in U_F$ of arbitrary large precision using the construction described above. This fact will also be used for the computation of the local fundamental class, see Lemma 2.17.

Example 2.11. Let L be the extension of $\mathbb{Q}_3$ generated by the polynomial $f = x^6 + 6x^2 + 6 \in \mathbb{Z}[x]$. It is a Galois extension with group S_3 and it is totally ramified since f is an Eisenstein polynomial.

Let π be a root of f in L, $\sigma \in S_3$ some element of the Galois group and define $c = \frac{\sigma(\pi)}{\pi}$. Then c has valuation 0 and we can solve $u^{\varphi - 1} = c$ up to precision n using the constructive proof of Lemma 2.9 where φ denotes the Frobenius automorphism of $\widetilde{L}|L$.

This construction has been implemented[6] in MAGMA and the element u will be found in some unramified extension of L. These extensions quickly become very large, even in such a small extension. If $\sigma \in S_3$ is of order 3, a solution of precision 5 needs an unramified extension of degree 9 over L. And to find a solution of precision 20, one already has to consider an extension of degree 81 and its computation takes about 20 seconds. The main downside of this is that all computations which are based on this solution will now have to work with an extension which is much larger than the one we started with.

On the other hand, consider the unramified extension F of degree 3 over L, which can be defined by $g = x^3 + 2x + 1 \in \mathbb{Z}[x]$. If $-c$ is a root of this polynomial in $\mathcal{O}_F$, then the element c will have norm 1 over L. Using the same algorithm, we can then find solutions of the equation $u^{\varphi - 1} = c$ up to arbitrary large precision. Also the computation time is a lot shorter: a solution of precision 500 is found within a second.

If we use Lemma 2.9 to construct solutions of the form $u^{\varphi - 1} = c$, it is therefore very important to make a good choice for c whenever this is possible.

[6] Command `FrobeniusEquation`, see documentation in Appendix B.1 on page 173.

The kind of equations considered in Lemma 2.9 can also be generalized to L_{nr}. Let $\widehat{L}_{nr}$ be the completion of L_{nr} and $w : \widehat{L}_{nr} \to \mathbb{Z}$ the sum of the valuations.

Lemma 2.12. *For every $c \in \widehat{L}_{nr}^{\times}$ with $w(c) = 0$ there exists $x \in \widehat{L}_{nr}^{\times}$ such that $x^{\varphi-1} = c$.*

Proof. If $c = (c_0, \dots c_{d-1}) \in \prod_{i=0}^{d-1} \widehat{L}^{\times}$ and $w(c) = 0$, then $\prod_{i=0}^{d-1} c_i \in \widehat{L}^{\times}$ has valuation 0 and there exists $y \in \widehat{L}^{\times}$ for which $y^{\varphi^d-1} = \prod c_i$ by Lemma 2.9. Then the element $x = (y, yc_0, yc_0c_1, \dots, yc_0 \cdots c_{d-2})$ satisfies

$$x^{\varphi-1} = \frac{(yc_0, yc_0c_1, \dots, yc_0 \cdots c_{d-2}, \varphi^d(y))}{(y, yc_0, yc_0c_1, \dots, yc_0 \cdots c_{d-2})} = (c_0, c_1, \dots, c_{d-1}) = c$$

since $\varphi^d(y) = y \prod_{i=0}^{d-1} c_i$. Hence, x solves the equation $x^{\varphi-1} = c$. □

We can now prove the following lemma (cf. [Ser79, XIII § 5, Ex. 2(a)]).

Lemma 2.13. *(a)* $\ker(w) = \{y^{\varphi-1} \mid y \in \widehat{L}_{nr}^{\times}\}$*,*

(b) $\ker(\varphi - 1) = L^{\times}$*, $L^{\times}$ being diagonally embedded in $L_{nr}^{\times}$, and*

(c) $\widehat{L}_{nr}^{\times}$ is a cohomologically trivial G-module.

Proof. (a) This follows from $w(y^{\varphi}) = w(y)$ for any $y \in \widehat{L}_{nr}^{\times}$ and the previous lemma.

(b) By Lemma 2.7, every element $y \in \ker(\varphi - 1)$ is represented by a tuple $(y_0, \dots, y_{d-1}) \in \prod_d \widetilde{L}$ which satisfies

$$1 = y^{\varphi-1} = \left(\frac{y_1}{y_0}, \frac{y_2}{y_1}, \dots, \frac{y_{d-1}}{y_{d-2}}, \frac{\varphi^d(y_0)}{y_{d-1}}\right).$$

Therefore $y_0 = y_1 = \ldots = y_{d-1} = \varphi^d(y_0) \in \widetilde{L}^{\times}$ and this implies $y_0 \in L^{\times}$ because φ^d generates $\mathrm{Gal}(\widetilde{L}|L)$. Since L is diagonally embedded into $\prod_d \widetilde{L}$ we obtain $y \in L^{\times}$. Hence, $\ker(\varphi - 1)$ is exactly $L^{\times}$.

(c) As mentioned before, the module $\widehat{L}_{nr}^{\times} = \prod_{i=0}^{d-1} \widehat{L}^{\times}$ is an induced module by Lemma 2.7. Shapiro's lemma [NSW00, Prop. (1.6.3)] implies $\hat{H}^q(G, \widehat{L}_{nr}) = \hat{H}^q(\mathrm{Gal}(L|E), \widehat{L})$ and this is zero by [Ser79, Chp. XIII, § 5, Prop. 14]. For subgroups H of G, the module $L_{nr}^{\times}$ decomposes into a direct sum of H-modules and each of these modules has cohomology isomorphic to $\hat{H}^q(\mathrm{Gal}(L|E) \cap H, \widehat{L})$ which is again trivial. □

We denote $V := \ker(w)$ and from the above lemma we get the exact sequences

$$0 \longrightarrow V \longrightarrow \widehat{L}_{nr}^{\times} \xrightarrow{w} \mathbb{Z} \longrightarrow 0 \tag{2.4}$$

$$\text{and} \quad 0 \longrightarrow L^{\times} \longrightarrow \widehat{L}_{nr}^{\times} \xrightarrow{\varphi-1} V \longrightarrow 0. \tag{2.5}$$

By the cohomological triviality of $\widehat{L}_{nr}^{\times}$, the connecting homomorphisms from their long exact cohomology sequences provides isomorphisms $\delta_1 : \hat{H}^0(G,\mathbb{Z}) \xrightarrow{\simeq} \hat{H}^1(G,V)$, $\delta_2 : \hat{H}^1(G,V) \xrightarrow{\simeq} \hat{H}^2(G,L^{\times})$ and we consider the composition

$$\Phi_{L|K} : \hat{H}^0(G,\mathbb{Z}) \xrightarrow{\simeq} \hat{H}^2(G,L^{\times}). \tag{2.6}$$

Its inverse $\Phi_{L|K}^{-1}$ directly defines an isomorphism

$$\overline{\mathrm{inv}}_{L|K} : \hat{H}^2(G,L^{\times}) \simeq \hat{H}^0(G,\mathbb{Z}) \xrightarrow{\cdot\frac{1}{[L:K]}} \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

which satisfies the properties of an invariant map.

Proposition 2.14. *(a) The elements $\overline{u}_{L|K} := \Phi_{L|K}(1+[L:K]\mathbb{Z})$ are fundamental classes for the class formation with respect to the isomorphism $\overline{\mathrm{inv}}$, i.e. $\overline{\mathrm{inv}}_{L|K}(\overline{u}_{L|K}) = \frac{1}{[L:K]} + \mathbb{Z}$.*

(b) The element $\overline{u}_{L|K}$ is the inverse of the local fundamental class $u_{L|K}$.

Proof. This is [Ser79, Chp. XIII, § 5, Ex. 2(c) and (d)].

We will prove part (a) by verifying the axioms of a class formation w.r.t. $\overline{\mathrm{inv}}$. Then two elements $\overline{u}_{L|K}$ and $\overline{u}_{L'|K}$ with $[L':K]=[L:K]$ have the same invariant $\overline{\mathrm{inv}}_{L|K}(\bar{u}_{L|K}) = \overline{\mathrm{inv}}_{L'|K}(\bar{u}_{L'|K})$ and it is sufficient to prove (b) for unramified extensions.

For (a) we have to show

(i) $\overline{\mathrm{inv}}_{L|K} = \overline{\mathrm{inv}}_{N|K} \circ \inf_{L|K}^{N|K}$ for normal extensions $N|L|K$ with $K \subset L$ and $K \subset N$ normal.

(ii) $\overline{\mathrm{inv}}_{N|L} \circ \mathrm{res}_{N|K}^{N|L} = [L:K]\,\overline{\mathrm{inv}}_{N|K}$ for $K \subseteq L \subseteq N$ and $K \subseteq N$ normal.

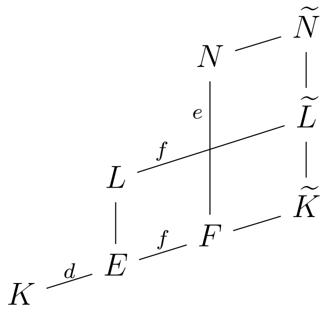
In (ii) we set $\Gamma := \mathrm{Gal}(N|K)$, $H := \mathrm{Gal}(N|L)$ and $\mathrm{res}_{N|K}^{N|L}$ denotes the restriction $\hat{H}^q(\Gamma,N^{\times}) \to \hat{H}^q(H,N^{\times})$. In (i) we also denote $G := \mathrm{Gal}(L|K) = \Gamma/H$ and $\inf_{L|K}^{N|K}$ is the injective inflation map

$$\hat{H}^q\left(G,L^{\times}\right) = \hat{H}^q\left(G,(N^{\times})^H\right) \xrightarrow{\inf_{L|K}^{N|K}} \hat{H}^q\left(\Gamma,N^{\times}\right)$$

which embeds $\hat{H}^2(G,L^{\times})$ into $\hat{H}^2(\Gamma,N^{\times})$.

We first prove (i). Let $K \subseteq L \subseteq N$ be extensions, $K \subseteq L$ and $K \subseteq N$ both normal. For $K \subseteq L$ we use the same notation as before, i.e. $[L:K]=n$, E is the maximal unramified subextension of $L|K$ which has degree $[E:K]=d$, $\widetilde{L} = L\widetilde{K}$ and $L_{nr} = \widetilde{K} \otimes_K L = \prod_d \widetilde{L}$.

Moreover, we define $m = [N:L]$ and let e and f be the ramification index and inertia degree of $N|L$ respectively, i.e. $m = ef$. Let F be the maximal unramified subextensions of $N|K$ of degree $d' = [F : K] = df$ and define $N_{nr} = \widetilde{K} \otimes_K N = \prod_{d'} \widetilde{N}$. The situation can be presented in the following diagram



(2.7)

where vertical and diagonal lines represent totally ramified and unramified extensions, respectively.

The module L_{nr} is canonically embedded in N_{nr} by the embedding of L in N. For the products of the fields $\widetilde{L}$ and $\widetilde{N}$ the embedding becomes:

$$\begin{aligned}
\iota : L_{nr} = \prod_{i=0}^{d-1} \widetilde{L} \quad &\hookrightarrow \quad N_{nr} = \prod_{i=0}^{d'-1} \widetilde{N} \\
(y_0, \ldots, y_{d-1}) &\mapsto \Big(y_0, \ldots, y_{d-1}, \varphi^d(y_0), \ldots, \varphi^d(y_{d-1}), \\
&\qquad \underline{\qquad}, \varphi^{d(f-1)}(y_0), \ldots, \varphi^{d(f-1)}(y_{d-1})\Big).
\end{aligned}$$

Let v_L and v_N be valuations such that $v_L(\pi_L) = v_N(\pi_N) = 1$ and $v_N(\pi_L) = e$. These valuations can uniquely be extended to $\widetilde{L}$ and $\widetilde{N}$ respectively. Let w_L and w_N be the sum of these valuations on $\widehat{L}_{nr}$ and $\widehat{N}_{nr}$. Then the following diagram commutes:

$$\begin{tikzcd}
L_{nr} \arrow[r, hook, "\iota"] \arrow[d, "w_L"] & N_{nr} \arrow[d, "w_N"] \\
\mathbb{Z} \arrow[r, "\cdot ef"] & \mathbb{Z}
\end{tikzcd} \tag{2.8}$$

The multiplication by ef in the lower map occurs since $d' = df$ and $v_L(x) = ev_N(x)$ for all $x \in \widetilde{L}$. Hence $V := \ker(w_L) \subseteq \ker(w_N) =: V'$ and more specifically $V = (V')^{1\times H}$.

Now we have to show the commutativity of the diagram

$$\begin{tikzcd}
\hat{H}^2(G, L^\times) \arrow[r, "\simeq"] \arrow[d, "\inf_{L|K}^{N|K}"] & \hat{H}^0(G, \mathbb{Z}) \arrow[r, "\cdot\frac{1}{[L:K]}"] \arrow[d, "\inf_{L|K}^{N|K}"] & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \arrow[d, "\subseteq"] \\
\hat{H}^2(\Gamma, N^\times) \arrow[r, "\simeq"] & \hat{H}^0(\Gamma, \mathbb{Z}) \arrow[r, "\cdot\frac{1}{[N:K]}"] & \frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z}
\end{tikzcd} \tag{2.9}$$

where the upper row represents $\overline{\mathrm{inv}}_{L|K}$ and the lower one represents $\overline{\mathrm{inv}}_{N|K}$. By [NSW00, (1.5.2)] the inflation map commutes with connecting homomorphisms.

This makes the left-hand square commutative. The commutativity of the right-hand square follows from the fact that the inflation map in degree zero is multiplication by $[N:L]$.

To prove (ii) consider the diagram

$$\begin{tikzcd} H^2(N|K) \arrow[r, "\simeq"] \arrow[d, "\mathrm{res}^{N|L}_{N|K}"] & H^0(\Gamma,\mathbb{Z}) \arrow[r, "\cdot\frac{1}{[N:K]}"] \arrow[d, "\mathrm{res}^{N|L}_{N|K}"] & \frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z} \arrow[d, "\cdot[L:K]"] \\ H^2(N|L) \arrow[r, "\simeq"] & H^0(H,\mathbb{Z}) \arrow[r, "\cdot\frac{1}{[N:L]}"] & \frac{1}{[N:L]}\mathbb{Z}/\mathbb{Z} \end{tikzcd} \tag{2.10}$$

where the rows represent the maps $\overline{\mathrm{inv}}_{N|K}$ and $\overline{\mathrm{inv}}_{N|L}$ again. The left-hand square is again commutative by [NSW00, Prop. (1.5.2)]. The middle vertical arrow is the restriction map in degree zero which is defined by

$$\begin{aligned} \mathrm{res}^{N|L}_{N|K} : \quad \hat{H}^0(\Gamma,\mathbb{Z}) &\longrightarrow \hat{H}^0(H,\mathbb{Z}) \\ x+[N:K]\mathbb{Z} &\longmapsto x+[N:L]\mathbb{Z}. \end{aligned}$$

This clearly makes the right square commute.

Altogether we verified that the cohomology groups satisfy the conditions of a class formation with respect to the invariant map $\overline{\mathrm{inv}}$.

(b) Before we consider unramified extensions $L|K$, we show how the image $\Phi_{L|K}(1+[L:K]\mathbb{Z})$ is obtained by the connecting homomorphisms δ_1 and δ_2 from (2.4) and (2.5) in the general case. For δ_1 we consider the commutative diagram

$$\begin{tikzcd} & & \widehat{L}^{\times}_{nr} \arrow[d, equal] & \mathbb{Z} \arrow[d, equal] & \\ 0 \arrow[r] & C^0(G,V) \arrow[r] \arrow[d] & C^0(G,\widehat{L}^{\times}_{nr}) \arrow[r, "w"] \arrow[d, "\partial_1"] & C^0(G,\mathbb{Z}) \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & C^1(G,V) \arrow[r] & C^1(G,\widehat{L}^{\times}_{nr}) \arrow[r, "w^*"] & C^1(G,\mathbb{Z}) \arrow[r] & 0 \end{tikzcd} \tag{2.11}$$

from the long exact cohomology sequence of (2.4), where w^* is the map on the group of cochains induced by w. If π is any uniformizing element of $\widehat{L}^{\times}$, the element $a=(1,\ldots,1,\pi)\in\widehat{L}^{\times}_{nr}=C^0(G,\widehat{L}^{\times}_{nr})$ is a preimage of 1 via w. Applying ∂_1 yields $\alpha\in C^1(G,\widehat{L}^{\times}_{nr})$, which is defined by[7]

$$\alpha(\sigma) := \frac{\sigma(a)}{a} = \begin{cases} \left(1,\ldots,1,\frac{\hat{\sigma}(\pi)}{\pi}\right), & \text{if } \hat{\sigma}|_{\widetilde{K}}=1 \\ \left(1,\ldots,1,\hat{\sigma}(\pi),\underbrace{1,\ldots,1,\frac{1}{\pi}}_{j \text{ components}}\right), & \text{if } \hat{\sigma}|_{\widetilde{K}}=\varphi^{-j}, 1\le j\le d-1 \end{cases}$$

[7]The equations in this proof use the unique extension $\hat{\sigma}$ of σ given in Remark 2.8. The Galois action of $(1\times\sigma)$ is then directly given by (2.2).

The commutativity of the diagram then implies $\alpha \in C^1(G, V)$.

For connecting homomorphism δ_2 we consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C^1(G, L^\times) & \longrightarrow & C^1(G, \widehat{L}_{nr}^\times) & \xrightarrow{\varphi - 1} & C^1(G, V) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \partial_2} & & \downarrow & & \\ 0 & \longrightarrow & C^2(G, L^\times) & \longrightarrow & C^2(G, \widehat{L}_{nr}^\times) & \longrightarrow & C^2(G, V) & \longrightarrow & 0 \end{array} \tag{2.12}$$

which arises from the cohomology sequence of (2.5). To find a preimage of α via $\varphi - 1$, we need elements in $\widehat{L}_{nr}^\times$ which are mapped to $\frac{\sigma(a)}{a}$ by $\varphi - 1$. By Lemma 2.12 these preimages are given by

$$\beta(\sigma) := \begin{cases} (u_\sigma, \ldots, u_\sigma) & \text{if } \hat{\sigma}|_{\widetilde{K}} = 1 \\ (u_\sigma, \ldots, u_\sigma, \underbrace{u_\sigma \hat{\sigma}(\pi), \ldots, u_\sigma \hat{\sigma}(\pi)}_{j \text{ components}}) & \text{if } \hat{\sigma}|_{\widetilde{K}} = \varphi^{-j}, 1 \le j \le d-1 \end{cases} \tag{2.13}$$

where u_σ solves $u_\sigma^{\varphi^d - 1} = \frac{\hat{\sigma}(\pi)}{\pi}$. The commutativity of the diagram again implies that the cocycle

$$\gamma(\sigma, \tau) := (\partial_2 \beta)(\sigma, \tau) = \frac{\sigma(\beta(\tau))\beta(\sigma)}{\beta(\sigma\tau)} \tag{2.14}$$

has values in $L^\times$ and we obtain $\bar{u}_{L|K} = \Phi_{L|K}(1 + [L:K]\mathbb{Z}) = \gamma \in \hat{H}^2(G, L^\times)$.

The element $\bar{u}_{L|K}$ is independent of the choices in the construction above because the connecting homomorphisms themselves are independent of these choices.

Now let $L|K$ be an unramified extension of degree n with Galois group G generated by the Frobenius automorphism φ. In this case the maximal unramified extensions of L and K are equal and the action of $(1 \times \varphi) \in \mathrm{Gal}(\widetilde{L}|K) \times G$ on L_{nr} defined in Lemma 2.7 is given by

$$\begin{aligned} (1 \times \varphi)(y_0, \ldots, y_n) &= (\varphi^{-1} \times 1)\big(\varphi(y_0), \ldots, \varphi(y_n)\big) \\ &= \big(y_n, \varphi(y_0), \ldots, \varphi(y_{n-1})\big). \end{aligned} \tag{2.15}$$

Recall that by the explicit description of the local fundamental class in Remark 1.7, the inverse of $u_{L|K}$ is given by the cocycle

$$c(\varphi^i, \varphi^j) = \begin{cases} 1 & \text{if } i + j < n \\ \frac{1}{\pi} & \text{if } i + j \ge n. \end{cases} \tag{2.16}$$

We will now make a direct computation of $\Phi_{L|K}(1 + [L:K]\mathbb{Z})$ using the constructions above.

Choose a uniformizing element π of K, which is also a uniformizing element of L. Then $\frac{\hat{\sigma}(\pi)}{\pi} = 1$ for all $\hat{\sigma} \in \mathrm{Gal}(\widetilde{L}|K)$ and every $u_\sigma \in L^\times$ solves $u_\sigma^{\varphi^n - 1} = \frac{\hat{\sigma}(\pi)}{\pi}$.

In the following we choose $u_\sigma = \frac{1}{\pi}$ for $\sigma \neq 1$ and $u_\sigma = 1$ otherwise. With these choices, the cochain β from (2.13) is given by $\beta(\varphi^i) = (\frac{1}{\pi}, \ldots, \frac{1}{\pi}, 1, \ldots, 1)$, $0 \leq i < n$, where the first i components are non-trivial.

Consider elements $\varphi^i, \varphi^j \in G$ with $i+j < n$. By (2.15) the action of $\varphi^i = (1 \times \varphi^i)$ on tuples in K is given by shifting i times to the right. Hence, we have the following images of β:

$$\beta(\varphi^{i+j}) = \Big(\underbrace{\frac{1}{\pi}, \ldots, \frac{1}{\pi}}_{i+j}, 1, \ldots, 1\Big), \quad \varphi^i(\beta(\varphi^j)) = \Big(\underbrace{1, \ldots, 1}_{i}, \underbrace{\frac{1}{\pi}, \ldots, \frac{1}{\pi}}_{j}, 1, \ldots, 1\Big).$$

We therefore have $\bar{u}_{L|K}(\varphi^i, \varphi^j) = \varphi^i(\beta(\varphi^j))\beta(\varphi^i)/\beta(\varphi^{i+j}) = (1, \ldots, 1) = 1 \in L^\times$. If $i + j \geq n$, we can write $i + j = n + k$ for some $0 \leq k < n$ and the two equations change to

$$\beta(\varphi^{i+j}) = \Big(\underbrace{\frac{1}{\pi}, \ldots, \frac{1}{\pi}}_{k}, 1, \ldots, 1\Big), \quad \varphi^i(\beta(\varphi^j)) = \Big(\underbrace{\frac{1}{\pi}, \ldots, \frac{1}{\pi}}_{k}, \underbrace{1, \ldots, 1}_{n-j}, \underbrace{\frac{1}{\pi}, \ldots, \frac{1}{\pi}}_{n-i}, \Big).$$

In this case we compute $\bar{u}_{L|K}(\varphi^i, \varphi^j) = (\frac{1}{\pi}, \ldots, \frac{1}{\pi}) = \frac{1}{\pi} \in L^\times$.

The cocycle $\bar{u}_{L|K} = \Phi_{L|K}(1 + [L : K]\mathbb{Z})$ therefore coincides with (2.16) and represents the inverse of the local fundamental class. $\square$

Corollary 2.15. *The exact sequence*

$$0 \longrightarrow L^\times \xrightarrow{\subseteq} \widehat{L}_{nr}^\times \xrightarrow{\varphi-1} \widehat{L}_{nr}^\times \xrightarrow{w} \mathbb{Z} \longrightarrow 0$$

represents the inverse of the local fundamental class in $\mathrm{Yext}^2_G(\mathbb{Z}, L^\times)$.

Proof. This follows from the above proposition if one considers the explicit description of the isomorphism $\mathrm{Yext}^2_G(\mathbb{Z}, L^\times) \simeq \hat{H}^2(G, L^\times)$. By Proposition 1.29 the image of an extension in $\hat{H}^2(G, L^\times)$ is given by applying the corresponding connecting homomorphisms to $1 + |G|\mathbb{Z}$, as we did in the above proof. $\square$

Remark 2.16. The construction in the proof can be directly turned into an algorithm. The main problem of this algorithm will be to find solutions u_σ of the equations $x^{\varphi^d - 1} = \frac{\hat{\sigma}(\pi)}{\pi}$ using Lemma 2.9.

As mentioned in Remark 2.10 the construction of such a solution can generate very large extensions of L which cannot be handled computationally. However, if we choose the uniformizing element π in a finite extension $F|L$ such that $\frac{\hat{\sigma}(\pi)}{\pi}$ has norm one, then a solution u_σ can be found in F up to an arbitrary large precision.

Lemma 2.17. *Let F be the unramified extension of L of degree $e = [L : E]$. Then there exists a uniformizing element $\pi \in F$ such that $x^{\varphi^d - 1} = \frac{\hat{\sigma}(\pi)}{\pi}$ has a solution in F for each $\hat{\sigma} \in \mathrm{Gal}(F|K)$.*

Proof. Denote $H = \mathrm{Gal}(F|L)$ and let π_K and π_L be uniformizing elements of K and L, respectively. Since $F|L$ is unramified, the group $\hat{H}^0(H, U_F) = U_L / \mathrm{N}_{F|L}(U_F)$ is trivial. Hence, the unit $u = \pi_K \pi_L^{-e} \in U_L$ is a norm of an element $v \in U_F$: $\mathrm{N}_{F|L}(v) = u$. Then $\pi = v\pi_L$ is another uniformizing element of F and its norm is $\mathrm{N}_{F|L}(\pi) = u\pi_L^e = \pi_K$. The group H is normal in $\mathrm{Gal}(F|K)$ and $\hat{\sigma}$ acts trivially on K. Therefore

$$\mathrm{N}_{F|L}\left(\frac{\hat{\sigma}(\pi)}{\pi}\right) = \frac{1}{\pi_K} \prod_{i=1}^{e} \varphi^{di}\Big(\hat{\sigma}(\pi)\Big) = \frac{1}{\pi_K}\, \hat{\sigma}\Big(\prod_{i=1}^{e} \varphi^{di}(\pi)\Big) = 1.$$

Hence, $\frac{\hat{\sigma}(\pi)}{\pi} \in {}_{\mathrm{N}_H}U_F$ and since $\hat{H}^{-1}(H, U_F) = {}_{\mathrm{N}_H}U_F / I_H U_F = 1$ for the unramified extension $F|L$, there exists $x \in U_F$ with $x^{\varphi^d - 1} = \frac{\hat{\sigma}(\pi)}{\pi}$. □

By choosing this special uniformizing element, we can solve the equations $x^{\varphi^d - 1} = \frac{\hat{\sigma}(\pi)}{\pi}$ up to an arbitrary large precision very effectively. As a result, the construction in the proof of Proposition 2.14 can be turned into an efficient algorithm. The most time consuming step in this algorithm will be to solve the norm equation $\mathrm{N}_{F|L}(v) = u$ in the proof above.

Algorithm 2.18 (Local fundamental class: Serre's approach).
Input: A finite Galois extension $L|K$ over $\mathbb{Q}_p$ with group G and a precision $k \in \mathbb{N}$.

Output: The local fundamental class $u_{L|K} \in Z^2\big(G, L^\times / U_L^{(k)}\big)$ up to the finite precision k.

1 Let π_K and π_L be uniformizing elements of K and L, E the maximal unramified subextension of $L|K$, $e = [L : E]$ the ramification degree and d the inertia degree. Let F be the unramified extension of L of degree e and $L_{nr} = \prod_d F$.

2 Solve the norm equation $\mathrm{N}_{F|L}(v) = u$ with $u = \pi_K \pi_L^{-e} \in U_L$ and $v \in U_F$ (e.g. using algorithms from [Pau06]) and define $\pi = v\pi_L$.

3 For each $\sigma \in G$ compute $u_\sigma \in F$ such that $u_\sigma^{\varphi^d - 1} = \frac{\hat{\sigma}(\pi)}{\pi} \mod U_F^{(k+2)}$.

4 Define $\beta \in C^1(G, L_{nr}^\times)$ and $\gamma \in C^2(G, L^\times)$ by (2.13) and (2.14).

Return: γ^{-1}.

Proof of the correctness. The direct computation in the proof of Proposition 2.14 shows that the cocycle γ from (2.14) represents the inverse of the local fundamental class.

If we compute the elements u_σ modulo $U_F^{(k+2)}$, we also know the images of β to the same precision. To compute γ^{-1} we divide by $\sigma(\beta(\tau))$ and $\beta(\sigma)$ and each of these divisions can reduce the precision by one. The other operations involved in ∂_2 (addition, multiplication and application of σ) do not reduce the precision (if F and all automorphisms σ are known to a precision higher than $k+2$). Hence, we know the images of γ modulo $U_F^{(k)}$. □

Example 2.19. The algorithm above has been implemented[8] in MAGMA. We consider the same extensions for which we computed the local fundamental classes with the direct method in Example 2.6. As mentioned before, the running time does not depend on the precision n up to which we compute the local fundamental class. The most time-consuming step is the solution of the norm equation in step 2. Afterwards the solutions u_σ can be computed up to an arbitrary large precision (which is just bounded by the precision up to which the local field itself was computed).

The performance of the MAGMA implementation of Algorithm 2.18 up to precision 20 is shown in the following table, which includes the timings from Example 2.6:

				timings [min]	
extension	group	$\deg(L_i)$	$\deg(L_iN_i)$	Alg. 2.5	Alg. 2.18
$L_1\|\mathbb{Q}_3$	S_3	6	36	1.5	0.02
$L_2\|\mathbb{Q}_2$	D_4	8	64	30	1.6
$L_3\|\mathbb{Q}_5$	D_5	10	50	490	15
$L_4\|\mathbb{Q}_3$	Q_{12}	12	36	160	19

Table 2.2: Computation times for local fundamental classes using Serre's approach.

As with Algorithm 2.5 one again notices that the computation time rises quickly with the degree of L. But the computation times of this new method are just a fraction of those using the direct method.

Remark 2.20. Combining the efficient computation of the local fundamental class with Algorithm 2.3, we can efficiently compute the invariant of a cocycle: If $\hat{H}^2(G, L^\times)$ is computed using the module $L^f = L^\times / \exp(\mathscr{L})$ for a suitable lattice $\mathscr{L}$, we will need an integer k such that $\mathfrak{P}^k \subseteq \mathscr{L}$ as in Remark 2.4. Then the local fundamental class up to precision k computed by Algorithm 2.18 defines a unique element in $u_{L|K} \in \hat{H}^2(G, L^f)$.

Given a cocycle γ of precision $m \geq k$, one can compute its invariant $\frac{j}{|G|}$ by solving $\gamma = u_{L|K}^j$ in $\hat{H}^2(G, L^f)$.

The efficient nature of Algorithm 2.18 (in comparison to other existing algorithms) makes a whole series of other algorithms possible. In the following sections and chapters this algorithm will be fundamental for computations in Brauer

[8] Command `LocalFundamentalClassSerre`, see documentation in Appendix B.1 on page 173.

groups of number fields, for global fundamental classes, for Tate's canonical class, and finally for the verification of epsilon constant conjectures.

Additionally, this algorithm can be used to compute Tate's canonical class following a construction of Chinburg from [Chi89]. Chinburg's construction is based on local fundamental classes and it has been implemented for tamely ramified extensions by Janssen [Jan10]. Algorithm 2.18 provides a generalization to arbitrary extensions.

Finally, Greve applied Algorithm 2.18 in [Gre10] to construct Galois groups of local number field extensions based on the Shafarevic-Weil theorem [AT68, Chp. XV, Thm. 6].

2.3 Global Brauer groups

As a first application of the algorithms for local Brauer groups and local fundamental classes, we present algorithms for the computation in the global Brauer group. Since $\mathrm{Br}(K) = \bigcup_L \mathrm{Br}(L|K)$, we restrict to computations in relative Brauer groups $\mathrm{Br}(L|K)$ for Galois extensions $L|K$.

Using the isomorphism $\mathrm{Br}(L|K) \simeq \hat{H}^2(G, L^\times)$ a first approach would be to find a finitely generated module M which is cohomologically isomorphic to $L^\times$. For such a module M, the cohomology group $\hat{H}^2(G, M)$ would also be finitely generated. Since G is finite and $|G|\hat{H}^2(G, M) = 0$, this would imply that the group $\hat{H}^2(G, M)$ is finite.

For global fields K and finite extensions $L|K$, however, the relative Brauer group $\mathrm{Br}(L|K)$ is known to be infinite [FS82]. We therefore cannot use this approach. Instead we will apply the algorithms for local Brauer groups and local fundamental classes from the previous sections.

Let K be a number field. The Brauer group $\mathrm{Br}(K)$ and the local Brauer groups $\mathrm{Br}(K_v)$ are related by the exact sequence

$$0 \longrightarrow \mathrm{Br}(K) \longrightarrow \bigoplus_v \mathrm{Br}(K_v) \xrightarrow{\mathrm{inv}_K} \mathbb{Q}/\mathbb{Z} \longrightarrow 0 \tag{2.17}$$

where v runs through all places of K and $\mathrm{inv}_K = \sum_v \mathrm{inv}_{K_v}$ is the sum of all local invariant maps (e.g. see [NSW00, Thm. (8.1.17)]). From this one easily deduces an exact sequence for relative Brauer groups.

Corollary 2.21. *Let $L|K$ be a Galois extensions of number fields. Then there is an exact sequence*

$$0 \longrightarrow \mathrm{Br}(L|K) \longrightarrow \bigoplus_v \mathrm{Br}(L_w|K_v) \xrightarrow{\mathrm{inv}_K} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

where v ranges over all places of K and w is a place of L dividing v.

Proof. The sequences (2.17) for L and K are connected by the restriction maps $\mathrm{res}_{L|K} : \mathrm{Br}(K) \to \mathrm{Br}(L)$ and $\mathrm{res}_{L_w|K_v} : \mathrm{Br}(K_v) \to \mathrm{Br}(L_w)$ whose kernels are the relative Brauer groups. This results in an exact commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathrm{Br}(L|K) \arrow[r] \arrow[d] & \bigoplus_v \mathrm{Br}(L_w|K_v) \arrow[r, "\mathrm{inv}_K"] \arrow[d] & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \arrow[d] & \\
0 \arrow[r] & \mathrm{Br}(K) \arrow[r] \arrow[d, "\mathrm{res}_{L|K}"] & \bigoplus_v \mathrm{Br}(K_v) \arrow[r, "\mathrm{inv}_K"] \arrow[d, "\oplus \mathrm{res}_{L_w|K_v}"] & \mathbb{Q}/\mathbb{Z} \arrow[r] \arrow[d, "\cdot[L:K]"] & 0 \\
0 \arrow[r] & \mathrm{Br}(L) \arrow[r] & \bigoplus_w \mathrm{Br}(L_w) \arrow[r, "\mathrm{inv}_L"] & \mathbb{Q}/\mathbb{Z} \arrow[r] \arrow[d] & 0 \\
 & & & 0 &
\end{tikzcd} \tag{2.18}$$

whose first row is the requested sequence. □

Using this representation of the relative Brauer group $\mathrm{Br}(L|K) \subset \bigoplus_v \mathrm{Br}(K_w|K_v)$, every element in this group is given by finitely many non-zero components which are elements of the local Brauer group $\mathrm{Br}(L_w|K_v) \simeq \hat{H}^2(G_w, L_w^\times)$ and whose invariants sum up to zero.

Hence, the algorithms from the previous sections can be used to compute in the global relative Brauer group. The two problems we want to solve are:

1. *Identify cocycles:* Given a global cocycle in $Z^2(G, L^\times)$, compute the invariants at each place v of K. This allows us to identify cocycles and to decide whether a cocycle is a coboundary.

2. *Construct cocycles:* Given invariants at finitely many places v which sum up to zero, compute a global cocycle respecting these local conditions.

We will address these problems in the following sections.

2.3.1 Identify cocycles

We will identify cocycles using Corollary 2.21 by computing invariants for every place w of L of the local cocycles obtained by the homomorphisms

$$\begin{aligned} \hat{H}^2(G, L^\times) &\to \hat{H}^2(G_w, L_w^\times) \\ \alpha &\mapsto \alpha_w. \end{aligned}$$

These are given by the embedding $L^\times \subset L_w^\times$ and by restricting to $G_w \subseteq G$. Since there are infinitely many places in L, we first need to restrict to a finite subset.

Lemma 2.22. *Let w be an unramified place of L and $\gamma \in Z^2(G, L^\times)$ a global cocycle for which the valuation $w(\gamma(\sigma, \tau))$ is trivial for each pair $\sigma, \tau \in G$. Then the local cocycle γ_w obtained as the image of $\hat{H}^2(G, L^\times) \to \hat{H}^2(G_w, L_w^\times)$ has invariant $\mathrm{inv}_w(\gamma_w) = 0 + \mathbb{Z}$.*

Proof. The local invariant map inv_w for the unramified place w is defined (see Theorem 1.3) as the following composition of isomorphisms:

$$\hat{H}^2(G_w, L_w^\times) \xrightarrow{w} \hat{H}^2(G_w, \mathbb{Z}) \xrightarrow{\simeq} \hat{H}^1(G_w, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\simeq} \frac{1}{[L_w : K_v]}\mathbb{Z}/\mathbb{Z}.$$

Here $w(\gamma_w)$ is trivial in $\hat{H}^2(G_w, \mathbb{Z})$ since $w(\gamma_w)(\sigma,\tau) = w(\gamma_w(\sigma,\tau)) = 0$ by assumption and hence $\mathrm{inv}_w(\gamma_w) = 0 + \mathbb{Z}$. □

So any global cocycle γ can only have non-trivial invariants at ramified places, at infinite places and at places which occur in the factorization of the principal ideals $(\gamma(\sigma,\tau))$ for every pair $\sigma,\tau \in G$. These are just finitely many places and the process of localization at these places gives an algorithm to identify global cocycles as a sequence of tuples (v, x_v) where v is a place of K and $x_v \in \frac{1}{|G_w|}\mathbb{Z}/\mathbb{Z}$ with $w|v$.

For a set of places S of L, we write $S(G)$ for a subset of representatives of the G-orbits in L.

Algorithm 2.23 (Identify global cocycle).
Input: A cocycle $\gamma \in Z^2(G, L^\times)$ for a Galois extensions $L|K$ of number fields with group G.

Output: A sequence of tuples (v, x_v) for a set of places v of K such that $x_v \in \mathbb{Q}/\mathbb{Z}$ is the local invariant of the localization γ_w with $w|v$.

1 Let S be the G-invariant set of places of L which includes the places that ramify in $L|K$, the infinite places of L and those places that occur in the factorization of $\lambda\mathcal{O}_L$ for any $\lambda = \gamma(\sigma,\tau), \sigma,\tau \in G$.

2 For each $w \in S(G)$ and a corresponding place v of K with $w|v$ compute $\gamma_w \in \hat{H}^2(G, L_w^\times)$ and $x_v := \mathrm{inv}_w(\gamma_w)$ using Algorithms 2.3 and 2.18.

Return: The sequence of tuples (v, x_v) for $w \in S(G)$ and $w|v$.

The performance of this algorithm will depend on the size of the field L (i.e. its degree over $\mathbb{Q}$ and its discriminant) because this affects the factorizations of $\lambda\mathcal{O}_L$ in step 1. But also the size of the localizations $L_w|K_v$ will be important since this determines the difficulty of the norm equations which have to be solve in Algorithm 2.18.

Remark 2.24. This algorithm has been implemented[9] in Magma for $K = \mathbb{Q}$. The main issue for $K \neq \mathbb{Q}$ is the fact that we need to write L_w as extension of K_v for places $w|v$ of L and K, respectively. In Magma each of those completions can be computed independently, but one does not get L_w as extension of K_v. Once this problem is solved, it is easy to generalize the implementation of Algorithm 2.23 to arbitrary extensions $L|K$.

Note that this also applies for Algorithm 2.27 below.

[9] Command `GlobalCocycleInvariants`, see documentation in Appendix B.1 on page 173.

2.3.2 Construct cocycles

For the construction of cocycles we again have the problem of L not being finitely generated over $\mathbb{Z}$. To work with the finitely generated S-units $U_S := \{a \in L \mid v(a) = 0 \; \forall v \notin S\}$ for a suitable finite set S of places of L and the homomorphism

$$\kappa : \hat{H}^2(G, U_S) \longrightarrow \hat{H}^2(G, L^\times)$$

instead, we also need to restrict to a finite set of places S in this case.

We denote the *S-ideal class group* by $Cl_S(L)$, which is defined to be the quotient of the *ideal class group* Cl_L modulo the subgroup generated by prime ideals corresponding to places in S.

Lemma 2.25. *Let $\alpha \in Z^2(G, L^\times)$ be a cocycle and consider a G-stable set S of places in L which*

(i) contains the ramified places and the infinite places of L,

(ii) satisfies $\mathrm{inv}_w(\alpha_w) = 0 + \mathbb{Z} \in \frac{1}{|G_w|}\mathbb{Z}/\mathbb{Z}$ for all $w \notin S$,

(iii) and is such that $Cl_S(L) = 0$.

Then there exists $\beta \in Z^2(G, U_S)$ such that $\kappa(\beta) = \alpha$.

Proof. Let T be the set of places w for which $w \in S$ or $w(\alpha(\sigma, \tau)) \neq 0$ for some $\sigma, \tau \in G$. Then α has values in U_T, and the proof is finished if $T = S$ holds.

Otherwise, let $v \in T \setminus S$, i.e. v is a place which is unramified in $L|K$ (by condition (i)) and $\mathrm{inv}_v(\alpha_v) = 0 + \mathbb{Z}$ (by condition (ii)). By condition (iii) the prime ideal $\mathfrak{P}_v$ corresponding to the place v can be written as $\mathfrak{P}_v = \mathfrak{a}_v(\pi_v)$ for some prime ideal $\mathfrak{a}_v$ which has support in S and a principal ideal (π_v). Then the generator π_v has valuations $v(\pi_v) = 1$ and $w(\pi_v) = 0$ for all $w \notin S \cup \{v\}$.

As v is unramified, there is an isomorphism

$$\hat{H}^2(G_v, L_v^\times) \simeq \hat{H}^2(G_v, \mathbb{Z})$$

induced by the valuation of v. We will therefore consider the valuations of the cocycle α. But before we deal with the general case, we consider the special case $G_v = G$.

Special case: $G_v = G$. By condition (ii) the cocycle α_v is trivial in $\hat{H}^2(G, L_v^\times) \simeq \hat{H}^2(G, \mathbb{Z})$, i.e. it is a coboundary: $\alpha_v = \partial_2(a)$ for some $a \in C^1(G, L_v^\times)$. Define $b \in C^1(G, L^\times)$ by $b(\sigma) = \pi_v^{v(\alpha(\sigma))}$ for all $\sigma \in G$. Then for all $\sigma \in G$ we have valuations

$$v(b(\sigma)) = v(a(\sigma)) \quad \text{and} \quad w(b(\sigma)) = 0 \text{ for } w \notin S \cup \{v\}.$$

We therefore consider the cocycle $\alpha' = \alpha\partial_2(b)^{-1}$ which is equal to α in $\hat{H}^2(G, L^\times)$. For all $\sigma, \tau \in G$ it satisfies

$$v(\alpha'(\sigma,\tau)) = 0 \quad \text{and} \quad w(\alpha'(\sigma,\tau)) = w(\alpha(\sigma,\tau)) \text{ for } w \notin S \cup \{v\}.$$

We conclude that α' only has non-trivial valuations for places $w \in T' := T \setminus \{v\}$. In other words, the cocycle α' has values in $U_{T'}$ with $T' \subsetneq T$ and continuing as above will construct a cocycle β with values in U_S which is equal to α in $\hat{H}^2(G, L^\times)$.

General case. In this case we have to consider all conjugate places of v. We therefore denote the fixed place in $T \setminus S$ by v_0 and each conjugate of v_0 by v. If we fix a system R of representatives of G/G_{v_0}, these conjugates are v_0^σ for $\sigma \in R$:

$$\begin{tikzcd}[column sep=small] L \arrow[d, dash, bend right=40, swap, "G"] \arrow[d, dash] & v_0 \arrow[dr, dash] & & v = v_0^\sigma \arrow[dl, dash] \\ K & & u & \end{tikzcd}$$

Since S is a G-stable set, each of these conjugates v satisfies $v \notin S$. As before, the prime ideals $\mathfrak{P}_v$ corresponding to each place v can be written as $\mathfrak{P}_v = \mathfrak{a}_v(\pi_v)$ with prime ideals $\mathfrak{a}_v$ having support in S and elements π_v satisfying $v(\pi_v) = 1$ and $w(\pi_v) = 0$ for all $w \notin S \cup \{v\}$.

If A is a G_{v_0}-module, then the *induced module* $\operatorname{ind}_{G_{v_0}}^G A$ can be identified with $\bigoplus_{\tau \in R} \tau A$ with G-action $(\sigma x)_{\tau'} = \sigma' x_\tau$ if $\sigma\tau = \tau'\sigma'$ for $\sigma' \in G_{v_0}$ and $x \in \bigoplus_{\tau \in R} \tau A$.

We now consider the homomorphism $\psi : \hat{H}^2(G, L^\times) \to \hat{H}^2\big(G, \operatorname{ind}_{G_{v_0}}^G \mathbb{Z}\big)$ from the following diagram

$$\begin{tikzcd} \hat{H}^2(G, L^\times) \arrow[r] & \hat{H}^2\big(G, \operatorname{ind}_{G_{v_0}}^G L_{v_0}^\times\big) \arrow[r, "\simeq", "(v)_{v|u}"'] \arrow[d, "\simeq"] & \hat{H}^2\big(G, \operatorname{ind}_{G_{v_0}}^G \mathbb{Z}\big) \arrow[d, "\simeq"] \\ & \hat{H}^2(G_{v_0}, L_{v_0}^\times) \arrow[r, "\simeq", "v_0"'] & \hat{H}^2(G_{v_0}, \mathbb{Z}) \end{tikzcd} \tag{2.19}$$

where the upper left horizontal map is given by the diagonal embedding $L^\times \hookrightarrow \operatorname{ind}_{G_{v_0}}^G L_{v_0}^\times \simeq \prod_{v|u} L_v^\times$ and the right-hand square is commutative with vertical isomorphisms given by Shapiro's lemma and horizontal isomorphisms induced by valuations. Hence, the image $\psi(\alpha)$ of α in $\hat{H}^2\big(G, \operatorname{ind}_{G_{v_0}}^G \mathbb{Z}\big)$ with $\operatorname{ind}_{G_{v_0}}^G \mathbb{Z} = \bigoplus_{\sigma \in R} \sigma\mathbb{Z}$ is given by taking valuations at each place v_0^σ, $\sigma \in R$.

By condition (ii), $v_0 \notin S$ implies that α_{v_0} is trivial in $\hat{H}^2(G_{v_0}, L_{v_0}^\times)$. Hence, the image of α will be trivial in any of the cohomology groups in the right-hand square of (2.19). Therefore, $\psi(\alpha)$ is a coboundary in $\hat{H}^2\big(G, \operatorname{ind}_{G_{v_0}}^G \mathbb{Z}\big)$, i.e. $\psi(\alpha) = \partial_2(a)$ for some $a \in C^1\big(G, \operatorname{ind}_{G_{v_0}}^G \mathbb{Z}\big)$.

We denote the component of $a(\sigma) \in \mathrm{ind}_{G_{v_0}}^G \mathbb{Z} = \bigoplus_{\tau \in R} \tau\mathbb{Z}$ at $\tau \in R$ by $a_\tau(\sigma) \in \mathbb{Z}$ and consider the cochain $b \in C^1(G, L^\times)$ given by

$$b(\sigma) = \prod_{\tau \in R} (\pi_{v_0^\tau})^{a_\tau(\sigma)}.$$

By the choice of π_v for each $v|u$, this cochain satisfies $\psi(\partial_2(b)) = \partial_2(a)$ because it has the same valuations as α for each $v|u$. Moreover, $w(\partial_2(b)) = 0$ for all $w \notin S \cup \{v_0^\tau \mid \tau \in R\}$.

Hence, the cocycle $\alpha' := \alpha\partial_2(b)^{-1}$ has the following valuations for each pair $\sigma, \tau \in G$:

$$\begin{aligned} v(\alpha'(\sigma,\tau)) &= 0 \text{ for all } v|u \\ \text{and} \quad w(\alpha'(\sigma,\tau)) &= w(\alpha(\sigma,\tau)) \text{ for all } w \notin S \cup \{v_0^\tau \mid \tau \in R\} \end{aligned}$$

and it is equal to α in $\hat{H}^2(G, L^\times)$.

In conclusion, the cocycle α' only has non-trivial valuations for places $w \in T' := T \setminus \{v_0^\tau \mid \tau \in R\}$. Proceeding as above with $T' \subsetneq T$ will generate the required cocycle β with values in U_S. □

Assume, that we have given local invariants $\{q_u \in \mathbb{Q}, u \in S'\}$ at a finite set of places S' of K such that $\sum_u q_u \in \mathbb{Z}$ and $[L_v : K_u]q_u \in \mathbb{Z}$ for $v|u$. Then there exists a cocycle in $Z^2(G, L^\times)$ with these invariants. We then consider a finite, Galois-invariant set of places S in L which

(i) includes places that ramify in $L|K$ and all the infinite places of L,

(ii) is such that $Cl_S(L) = 0$, and

(iii) contains the places $\{v \mid v|u \text{ and } u \in S'\}$ which lie above any place $u \in S'$.

Since such a set S satisfies the conditions of the above lemma, one can construct a cocycle in $Z^2(G, U_S)$ having these invariants and by $U_S \subset L^\times$ this defines the cocycle in $Z^2(G, L^\times)$. Since U_S is finitely generated, the conditions on the cocycle can be formulated by linear equations as follows.

For a set S of places, we denote the subset of finite places by $S_f \subseteq S$ and the subset of infinite places by S_∞.

Proposition 2.26. *Let $\{q_u, u \in S'\}$ be a set of local invariants $q_u \in \mathbb{Q}$ for a finite set of places S' of K such that $\sum_u q_u \in \mathbb{Z}$ and $[L_v : K_u]q_u \in \mathbb{Z}$ for a place v of L above u. Let S be a finite set of places in L satisfying the conditions (i)–(iii) above. Then one can find a cocycle $\gamma \in Z^2(G, U_S)$ having these local invariants by solving a system of linear equations.*

Proof. The S-units are finitely generated. Denote its $\mathbb{Z}$-generators by ε_i, such that $U_S = \prod_{i=1}^{s} \langle \varepsilon_i \rangle$, and let λ_i be the order of ε_i with $\lambda_i = 0$ if ε_i is a free generator.

Then a generic cochain $\gamma \in C^2(G, U_S)$ representing a cocycle is given by $|G|^2 s$ variables:

$$\gamma(\sigma, \tau) = \prod_{i=1}^{s} \varepsilon_i^{x_{\sigma,\tau,i}}, \quad x_{\sigma,\tau,i} \in \mathbb{Z}. \tag{2.20}$$

If the G-action on U_S is given by $\sigma(\varepsilon_i) = \prod_{j=1}^{s} \varepsilon_j^{\alpha_{\sigma,i,j}}$ with integers $\alpha_{\sigma,i,j}$, one can rewrite the cocycle condition on γ for all $\sigma, \tau, \rho \in G$ as follows:

$$\begin{aligned} & \gamma(\sigma\tau, \rho)\gamma(\sigma, \tau) = \sigma(\gamma(\tau, \rho))\gamma(\sigma, \tau\rho) & (2.21) \\ \Leftrightarrow \quad & \prod_{i=1}^{s} \varepsilon_i^{x_{\sigma\tau,\rho,i}} \prod_{i=1}^{s} \varepsilon_i^{x_{\sigma,\tau,i}} = \prod_{i=1}^{s} \varepsilon_i^{\sum_{j=1}^{s} \alpha_{\sigma,j,i} x_{\tau,\rho,j}} \prod_{i=1}^{s} \varepsilon_i^{x_{\sigma,\tau\rho,i}} & \\ \Leftrightarrow \quad & x_{\sigma\tau,\rho,i} + x_{\sigma,\tau,i} \equiv \sum_{j=1}^{s} \alpha_{\sigma,j,i} x_{\tau,\rho,j} + x_{\sigma,\tau\rho,i} \mod \lambda_i \mathbb{Z}, \qquad \forall i = 1 \dots s. & \\ & & (2.22) \end{aligned}$$

For each $w \in S_f(G)$ let $L_w^f = \prod_{i=1}^{r_w} \langle m_{w,i} \rangle$ be the module $L_w^f = L_w^\times / \exp(\mathscr{L}_w)$ from Lemma 2.1 for which $\hat{H}^2(G_w, L_w^\times) \simeq \hat{H}^2(G_w, L_w^f)$ and let ϕ_w be the map $L \to L_w^\times \twoheadrightarrow L_w^f$. Denote the order of $m_{w,i}$ by $\nu_{w,i} \in \mathbb{Z}$, with $\nu_{w,i} = 0$ if $m_{w,i}$ is a free generator. If $\gamma_w \in \hat{H}^2(G_w, L_w^f)$ is a local cocycle having the prescribed invariant q_u with $w|u$, then it is required that

$$\phi_w(\gamma(\sigma, \tau)) = \gamma_w(\sigma, \tau) b_w(\sigma, \tau) \tag{2.23}$$

holds in L_w^f for $\sigma, \tau \in G_w$ where b_w is a coboundary in $\hat{H}^2(G_w, L_w^f)$. The 2-coboundary b_w is defined using a 1-cochain $a_w \in C^1(G_w, L_w^f)$ by $b_w(\sigma, \tau) = \sigma(a_w(\tau)) a_w(\sigma) a_w(\sigma\tau)^{-1}$. This 1-cochain in turn is generically given by integers $y_{w,\sigma,i} \in \mathbb{Z}$: $a_w(\sigma) = \prod_{i=1}^{r_w} m_{w,i}^{y_{w,\sigma,i}}$.

Fix w and let the G-action on L_w^f be given by $\sigma(m_{w,i}) = \prod_{j=1}^{r_w} m_{w,j}^{\beta_{\sigma,i,j}}$ with integers $\beta_{\sigma,i,j}$, and let $\phi_w(\varepsilon_k) = \prod_{i=1}^{r_w} m_{w,i}^{e_{k,i}}$ with $e_{k,i} \in \mathbb{Z}$.

If for fixed $\sigma, \tau \in G_w$ we have $\gamma_w(\sigma, \tau) = \prod_{i=1}^{r} m_{w,i}^{c_i}$, then we can rewrite the condition (2.23) as follows:

$$\begin{aligned} & \phi_w(\gamma(\sigma, \tau)) = \gamma_w(\sigma, \tau) \sigma(a_w(\tau)) a_w(\sigma) a_w(\sigma\tau)^{-1} \\ \Leftrightarrow \quad & \prod_{i=1}^{r_w} m_{w,i}^{\sum_{k=1}^{s} e_{k,i} x_{\sigma,\tau,k}} = \prod_{i=1}^{r_w} m_{w,i}^{c_i + \sum_{j=1}^{r_w} \beta_{\sigma,j,i} y_{w,\tau,j} + y_{w,\sigma,i} - y_{w,\sigma\tau,i}} \\ \Leftrightarrow \quad & \sum_{k=1}^{s} e_{k,i} x_{\sigma,\tau,k} \equiv c_i + \sum_{j=1}^{r_w} \beta_{\sigma,j,i} y_{w,\tau,j} + y_{w,\sigma,i} - y_{w,\sigma\tau,i} \mod \nu_{w,i}\mathbb{Z} \\ & \hfill \forall i = 1 \dots r \quad (2.24) \end{aligned}$$

The condition at infinite places $w \in S_\infty$ with $G_w = \langle g_w \rangle \neq 1$ can be described as follows (compare Section 1.1.1 on page 11). If γ is a normalized cocycle, i.e. $\gamma(1,\sigma) = \gamma(\sigma,1) = 1$, then γ_w has values in $\mathbb{R}$ and it represents the local fundamental class if and only if $\gamma_w(g_w, g_w) < 0$. If ι_w is the embedding corresponding to w and if $J = \{j \in \{1,\dots,s\} \mid \iota_w(\varepsilon_j) \in \mathbb{R}, \iota_w(\varepsilon_j) < 0\}$ then we add the condition

$$\sum_{i\in J} x_{g_w,g_w,i} \equiv \begin{cases} 0 & \bmod 2\mathbb{Z} \\ 1 & \bmod 2\mathbb{Z} \end{cases} \tag{2.25}$$

to the linear system of equations, depending on whether we want trivial ($q_u \in \mathbb{Z}$) or non-trivial ($q_u \notin \mathbb{Z}$) invariant at w with $w|u$.

The generic cocycle γ and the 1-cochains a_w give a total minimum number of $|G|^2 s + \sum_{w\in S_f} |G_w|\, r_w$ variables. Any congruence for infinite places and any congruence of the form (2.22) or (2.24) with $\lambda_i \neq 0$ or $\nu_{w,i} \neq 0$, respectively, is turned into a linear equation by adding an additional variable to the system of equations. The number of (not necessarily independent) equations will be $|G|^3 s + \sum_{w\in S_f} |G_w|^2 r_w + |S_\mathbb{C}| + (2|G|-1)$ which arise from the cocycle conditions, the local conditions at $w \in S_f$, the conditions at complex places $w \in S_\mathbb{C} \subseteq S_\infty$ and the condition of a normalized cocycle, respectively.

By Lemma 2.25 there exists a solution of the constructed system of linear equations and using the solution of the variables $x_{\sigma,\tau,i}$ in (2.20) one gets a cocycle with values in U_S and prescribed local invariants. □

Algorithm 2.27 (Construct global cocycle).

Input: A finite Galois extensions $L|K$ of number fields with group G and local invariants $q_v \in \frac{1}{|G_w|}\mathbb{Z}$ for a finite set S' of places v of K (with w dividing v) which satisfy $\sum_v q_v \in \mathbb{Z}$.

Output: A global cocycle $\gamma \in Z^2(G, U_S)$ for a finite set of places S of L satisfying conditions (i)–(iii) whose localizations have invariant q_v at $v \in S'$ and 0 at $v \notin S'$.

1 Follow the proof of Proposition 2.26 to construct a system of linear equations, i.e. turn the equivalences (2.22), (2.24) and (2.25) into linear equations by introducing new variables and add equations for normalized cocycles.

2 Solve this system of equations, pick a solution and define the cochain γ by equation (2.20).

Return: The cocycle γ.

This algorithm has been implemented[10] in Magma for $K = \mathbb{Q}$. For arbitrary extension it would be necessary to compute completions $L_w|K_v$ of an extension $L|K$. This is, however, not yet possible in Magma, see Remark 2.24.

[10] Command `GlobalCocycle`, see documentation in Appendix B.1 on page 173.

Example 2.28. Let L be the splitting field of $x^3 + 9 \in \mathbb{Z}[x]$ over $\mathbb{Q}$. It is a Galois extension with group $G = S_3$. The prime 3 is undecomposed in L and 5 decomposes into three prime ideals. Therefore, there exists a cocycle in $\gamma \in Z^2(G, L^\times)$ which has invariants $\frac{1}{2}$ at the primes 3 and 5 and trivial invariant everywhere else.

Since 3 is the only prime which ramifies in L and L has class number 1, we can consider a set of primes S of L whose finite places $w \in S_f$ are those above 3 and 5. The linear system of equations from Proposition 2.26 considered in the algorithm above then becomes a system with 1748 equations in 608 variables. A solution of this system is found easily and in total Algorithm 2.27 takes about 3 seconds to construct the cocycle γ.

The invariants of γ can be verified using algorithm Algorithm 2.23. It will take just a second since all the local cohomology groups needed are already computed.

Since both primes, $p = 3$ and $p = 5$, are undecomposed in the subextension $\mathbb{Q}(\zeta_3)|\mathbb{Q}$ of $L|\mathbb{Q}$, the cocycle γ can also be represented as the inflation of a cocycle $\beta \in \hat{H}^2\big(\mathrm{Gal}(\mathbb{Q}(\zeta_3|\mathbb{Q}), \mathbb{Q}(\zeta_3)^\times\big)$. With Algorithm 2.23 one can easily verify that

$$\beta(\sigma,\tau) = \begin{cases} 15 & \sigma \neq 1, \tau \neq 1 \\ 1 & \text{else} \end{cases}$$

is a cocycle with the required invariants and that $\inf_{\mathbb{Q}(\zeta_3)|\mathbb{Q}}^{L|\mathbb{Q}} \beta = \gamma$.

In this example the construction of the cocycle was very simple (in terms of computation time). Actually, one discovers that more conditions on the cocycle will not affect the computation time by a lot for both algorithms. In other words, Magma's implementation of the factorization of prime ideals (step 1 of Algorithm 2.23) and the computation of kernels of integer matrices (step 2 of Algorithm 2.27) both perform well enough.

For extensions of higher degree (degree ≥ 10 over $\mathbb{Q}$) one will also observe that the computation of the local cohomology groups needed in both algorithms will be the main issue. Then the norm equations from Algorithm 2.18 become very difficult and these will dominate the computation time.

3 Global fundamental classes

Given a Galois extension of number fields $L|K$ with Galois group G, we denote the idèle class group by C_L as in Section 1.1.2. We will use the algorithms for local fundamental classes to describe an algorithm for the computation of the global fundamental class in $\hat{H}^2(G, C_L)$. It is the unique element whose invariant through the isomorphism

$$\mathrm{inv}_{L|K} : \hat{H}^2(G, C_L) \xrightarrow{\simeq} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

is $1/[L:K] + \mathbb{Z}$ (see Definition 1.15). The main ideas behind this method are the following:

1. Chinburg shows in [Chi85, § 2] how a finitely generated module M can be generated such that $\hat{H}^2(G, M) \simeq \hat{H}^2(G, C_L)$.
2. Given a finitely generated module M, one can compute with $\hat{H}^2(G, M)$ using linear algebra, as described in [Hol06].
3. Using the idèlic invariant map one can find the global fundamental class for cyclic extensions. In the general case one has to work with the composite with a cyclic extension of the same degree and work with the inflation on cohomology groups.

Compared to the computation of the local fundamental class this can be regarded as the *direct method* for the global fundamental class.

The computation of the cohomology group $\hat{H}^2(G, M)$ for finitely generated modules M has been discussed in Section 2.1. In this chapter we first address the finite approximation of the idèle class group introduced by Chinburg and turn it into an algorithm. This will then allow us to describe an algorithm to compute the global fundamental class.

3.1 Finite approximation of the idèle class group

We continue to use the notations from [NSW00, Chp. VIII, § 3] where I_L denotes the idèle group $\prod'_v L_v^\times$ as defined in Definition 1.8 and the product is restricted with respect to the unit groups U_{L_v} which are $U_{L_v} = \mathcal{O}_{L_v}^\times$ for finite places and $U_{L_v} = L_v^\times$ for infinite places. For a finite set S of places of L we define the S-*idèle class group* by $C_S(L) = I_L/L^\times U$ where $U = \prod_{v\in S}\{1\} \times \prod_{v\notin S} U_{L_v} \subseteq I_L$.

If S contains all the infinite places and all places that ramify in $L|K$, every place $v \notin S$ is unramified and has cohomologically trivial unit group $\mathcal{O}_{L_v}^\times$. Therefore, $U_{L,S}$ is cohomologically trivial and there is an isomorphism in cohomology

$$\hat{H}^i(G, C_L) \simeq \hat{H}^i(G, C_S(L)) \tag{3.1}$$

(see [NSW00, Prop. (8.3.1)]).

For the computation of the cohomology of C_L we have the problem that C_L itself or the S-idèle class group $C_S(L)$ are not finitely generated. Moreover, they are defined by I_L which is a product over infinitely many primes. As a first step, we will therefore replace I_L by the *S-idèle group*[1] $I_{L,S} := \prod_{v\in S} L_v^\times$ for a finite set S of places in L and factor by the units of the ring of *S-integers* $\mathcal{O}_{L,S} := \{a \in L \mid v(a) \geq 0 \ \forall v \notin S\}$. These *$S$-units* $\mathcal{O}_{L,S}^\times$ will also be denoted by $U_{L,S}$ or by U_S if L is known from the context.

In analogy to the idèle class group one then defines the group $C_{L,S} = I_{L,S}/U_{L,S}$ which is defined by a product over the finitely many primes in S. It is related to the S-idèle class group by the exact sequence (cf. [NSW00, Chp. VIII, (8.3.4)])

$$0 \longrightarrow C_{L,S} \longrightarrow C_S(L) \longrightarrow Cl_S(L) \longrightarrow 0 \tag{3.2}$$

where $Cl_S(L)$ denotes the *S-ideal class group*, which is the quotient of the ideal class group Cl_L of L by the classes of prime ideals corresponding to places in S.

In order to work with $C_{L,S}$ instead of $C_S(L)$, we therefore need S to be sufficiently large such that $Cl_S(L) = 0$. Such a finite set of places (corresponding to prime ideals) exists because the ideal class group is finite and every ideal class is represented by an ideal which factors into finitely many prime ideals. Actually, we also need the S-class group to be trivial for all subfields F in $L|K$ in order to represent elements in $C_F \subseteq C_L$ by the same set of places. This is a very strong condition on S and its verification can take quite a long time. The set of places u in a subfield $F \subseteq L$ for which there is a place $v \in S$ dividing u will again be denoted by S.

To have isomorphism (3.1), we will also require S to contain all ramified and infinite places. In total we have the following conditions on S:

(S1) it is Galois-invariant, i.e. if $v \in S$, also $v^\sigma \in S$ for $\sigma \in G$,

(S2) it contains the places that ramify in $L|K$,

(S3) it contains the infinite places of L, and

(S4) it is sufficiently large such that $Cl_S(F) = 0$ for all $K \subseteq F \subseteq L$.

By the arguments from above we have the following isomorphism in cohomology.

[1] Note that the S-idèle group is often also defined to be $\prod_{v\in S} L_v^\times \times \prod_{v\notin S} \mathcal{O}_{L_v}^\times$. In our applications, with S omitting only unramified places, the two definitions will be cohomologically isomorphic. Since we are only interested in the cohomology, we can choose either of them and we will keep the notation of [NSW00].

Lemma 3.1. *Let S be a set of places satisfying conditions (S1)–(S4). Then there is an isomorphism*

$$\hat{H}^i(G, C_L) \simeq \hat{H}^i(G, C_{L,S}).$$

Proof. [NSW00, Prop. (8.3.4) and (8.3.6)]. ☐

In the definition of $C_L = I_L/L^\times$ we factor by $L^\times$ which is known to satisfy $\hat{H}^1(H, L^\times) = 0$ for all subgroups $H \subseteq G$ by Hilbert's Theorem 90. To replace C_L by $C_{L,S} = I_{L,S}/U_{L,S}$ in the following we will similarly require the first cohomology groups of $U_{L,S}$ to be trivial. But this already follows from the conditions on S.

Lemma 3.2. *If S is a finite set of places satisfying conditions (S1)–(S4) and $H \subseteq G$ is a subgroup, then $\hat{H}^1(H, U_{L,S}) = 0$.*

Proof. We recall the proof from [Tat84, Chp. II, Thm. 6.8] which particularly motivates condition (S4).

The S-units $U_{L,S}$ fit into an exact sequence

$$0 \to U_{L,S} \to L^\times \to J_{L,S} \to 0$$

with $J_{L,S}$ denoting the ideals which are coprime to S and where the right-hand map is surjective since $Cl_S(L) = 0$. The cohomology sequence for a subgroup $H \subseteq G$ with $F = L^H$ provides

$$0 \to U_{F,S} \to F^\times \to J_{L,S}^H \to \hat{H}^1(H, U_{L,S}) \to 0.$$

Since S contains the ramified primes, one has $J_{L,S}^H = J_{F,S}$ and $F^\times \to J_{F,S}$ is surjective if and only if $Cl_S(F) = 0$. The condition (S4) on S therefore implies $\hat{H}^1(H, U_{L,S}) = 0$. ☐

For the finite places $v \in S_f$ the group $I_{L,S}$ contains $L_v^\times$ which we made finitely generated by taking the quotient with $\exp(\mathscr{L}_v)$ for a full projective lattice $\mathscr{L}_v \subseteq \mathcal{O}_{L_v}$ upon which the exponential map is defined, see Section 2.1. To get a similar result for the infinite places $v \in S_\infty$, we follow [Chi85, § 2] to construct finitely generated modules W_v which are cohomologically isomorphic to $L_v^\times$.

Proposition 3.3 (Chinburg). *Let $v \in S_\infty$ be a infinite place of L and ι_v the corresponding embedding $L \hookrightarrow L_v$. Then there exists a finitely generated G_v-submodule W of $L_v^\times$ such that*

(i) $\iota_v(U_{L,S}) \subseteq W$ *and* $W/\iota_v(U_{L,S})$ *is torsion-free,*

(ii) the inclusion $W \hookrightarrow L_v^\times$ *induces an isomorphism in* G_v*-cohomology, and*

(iii) if W' *is another module for which (i) and (ii) hold, there is a* G_v*-homomorphism* $f : W \to W'$ *for which* $f|_{\iota_v(U_{L,S})} = \mathrm{id}$ *and* f *induces an isomorphism in cohomology.*

We recall the proof of Chinburg from [Chi85, Lem. 2.1] but, in contrast to his proof, we also discuss the algorithmic details of the construction. In the following, we will sometimes omit the embedding ι_v and embed $U_{L,S}$ into L_v implicitly.

Proof. Let u denote the place of K below v. Consider the case $G_v = 1$. Then $K_u = L_v = \mathbb{R}$ or $K_u = L_v = \mathbb{C}$ and $\hat{H}^i(G_v, L_v^\times) = 0$ for all i. Hence, properties (ii) and (iii) are trivially satisfied for $W = \iota_v(U_{L,S})$.

In the other case $G_v = \{1, \sigma_v\}$, $K_u = \mathbb{R}$ and $L_v = \mathbb{C}$. The action by σ_v on $x \in \mathbb{C}$ is the complex conjugation, which we will also denote by $\overline{x}$. The cohomology groups of $L_v^\times = \mathbb{C}^\times$ are $\hat{H}^0(G_v, L_v^\times) = \mathbb{R}^\times/\mathbb{R}_{>0} \simeq \mathbb{Z}/2\mathbb{Z}$ and $\hat{H}^{-1}(G_v, L_v^\times) = 0$ by Hilbert's Theorem 90.

Let U_{tor} be the torsion subgroup of the S-units $U = U_{L,S}$ which is given the roots of unity μ_L in L. Then define $U_0 = U/U_{\mathrm{tor}}$ and construct W_v by the following steps:

1. There exists a non-trivial extension $(\mathbb{Z}; U_{\mathrm{tor}})$ of $\mathbb{Z}$ with U_{tor} (as $\mathbb{Z}[G_v]$-modules).

2. There is an isomorphism of $\mathbb{Z}[G_v]$-modules $U_0 \simeq \mathbb{Z}^a \oplus \mathbb{Z}[G_v]^b$ for suitable integers a and b.

3. One can construct an isomorphism $\psi : (\mathbb{Z}; U_{\mathrm{tor}}) \oplus \mathbb{Z}^{a-1} \oplus \mathbb{Z}[G_v]^b \simeq U$ and the generators $u_2, \ldots, u_a$ of the $\mathbb{Z}^{a-1}$-part in U satisfy $\iota_v(u_i) \in \mathbb{R}$ and can be chosen such that $\iota_v(\psi(u_i)) > 0$ in $\mathbb{R}$.

4. For $2 \le i \le a$, we choose $\lambda_i \in \mathbb{C}$ with $N_{G_v}\lambda_i = u_i$ algebraically independent such that $\prod_{i=2}^a \lambda_i^{a_i + b_i\sigma_v} = \prod_i \lambda_i^{a_i}\overline{\lambda}_i^{\,b_i} \in \iota_v(U)$ if and only if $a_i = b_i$ for all i.

5. Finally, the module $W := (\mathbb{Z}; U_{\mathrm{tor}}) \oplus \bigoplus_{i=2}^a \mathbb{Z}[G_v]\lambda_i \oplus \mathbb{Z}[G_v]^b$ has cohomology $\hat{H}^i(G, W) \simeq \hat{H}^i(G, (\mathbb{Z}; U_{\mathrm{tor}}))$ and satisfies the conditions of the proposition.

Step 1: The first cohomology group of U_{tor} is

$$\hat{H}^1(G_v, U_{\mathrm{tor}}) = \hat{H}^{-1}(G_v, U_{\mathrm{tor}}) = {}_{\mathrm{N}_{G_v}}U_{\mathrm{tor}} / \mathrm{I}_{G_v} U_{\mathrm{tor}} = U_{\mathrm{tor}}/U_{\mathrm{tor}}^2 \simeq \mathbb{Z}/2\mathbb{Z}.$$

Hence, up to isomorphism there is exactly one non-trivial extension $(\mathbb{Z}; U_{\mathrm{tor}})$ of $\mathbb{Z}$ with U_{tor}:

$$0 \longrightarrow U_{\mathrm{tor}} \longrightarrow (\mathbb{Z}; U_{\mathrm{tor}}) \longrightarrow \mathbb{Z} \longrightarrow 0. \tag{3.3}$$

Explicitly, it is given by choosing $\theta \in U_{\mathrm{tor}} \setminus U_{\mathrm{tor}}^2$ and defining $(\mathbb{Z}; U_{\mathrm{tor}}) = U_{\mathrm{tor}} \oplus \mathbb{Z}$ (as direct sum of groups) where σ_v acts naturally on the subgroup $U_{\mathrm{tor}} \subseteq (\mathbb{Z}; U_{\mathrm{tor}})$ and $\sigma_v(0,1) = (\theta, 1)$. On the other hand, if $\theta \in U_{\mathrm{tor}}^2 = \mathrm{I}_{G_v} U_{\mathrm{tor}}$ with $\theta = \sigma_v\eta/\eta$, $\eta \in U_{\mathrm{tor}}$, one can easily see that $(\sigma_v\eta, 1)$ is a G_v-invariant lift of $1 \in \mathbb{Z}$, i.e. $1 \mapsto (\sigma_v\eta, 1)$ is a G_v-section and $(\mathbb{Z}; U_{\mathrm{tor}})$ is isomorphic to $U_{\mathrm{tor}} \oplus \mathbb{Z}$ (direct sum as G_v-modules).

Furthermore, if $M = U_{\mathrm{tor}} \oplus \mathbb{Z}$ is another extension with G_v-action $\sigma_v(0,1) = (\theta', 1)$, $\theta' \in U_{\mathrm{tor}} \setminus U_{\mathrm{tor}}^2$, then there exists $\eta \in U_{\mathrm{tor}}^2$ satisfying $\sigma_v \eta/\eta = \theta'/\theta$ since $\theta'/\theta \in U_{\mathrm{tor}}^2 = \mathrm{I}_{G_v} U_{\mathrm{tor}}$ and $U_{\mathrm{tor}}/U_{\mathrm{tor}}^2 \simeq \mathbb{Z}/2\mathbb{Z}$. Hence, there is a G_v-module isomorphism $M \to (\mathbb{Z}; U_{\mathrm{tor}})$ given by the identity on U_{tor} and $(0,1) \mapsto (\eta, 1)$.

For the rest of the proof, we fix an element $\theta \in U_{\mathrm{tor}} \setminus U_{\mathrm{tor}}^2$ representing the action on $g_1 := (0,1)$ in $(\mathbb{Z}; U_{\mathrm{tor}})$.

Step 2: Recall that by Lemma 3.2 the conditions on S imply $\hat{H}^{-1}(G_v, U) = 0$. The quotient $U_0 = U/U_{\mathrm{tor}}$ gives an exact sequence

$$0 = \hat{H}^{-1}(G_v, U) \to \hat{H}^{-1}(G_v, U_0) \to \hat{H}^{0}(G_v, U_{\mathrm{tor}}) \to \hat{H}^{0}(G_v, U)$$

of cohomology groups where $\hat{H}^0(G_v, U_{\mathrm{tor}}) = U_{\mathrm{tor}}^{G_v}/(1+\sigma_v)U_{\mathrm{tor}} \simeq \mathbb{Z}/2\mathbb{Z}$ and $\hat{H}^{-1}(G_v, U_0) = 1$ since $-1 \in U_{\mathrm{tor}}^{G_v} \subseteq U^{G_v}$ is not in $(1+\sigma_v)U$. From $\hat{H}^{-1}(G_v, U_0) = 1 \neq \hat{H}^{-1}(G_v, \mathbb{Z}^-)$ we know that there is no $\mathbb{Z}^-$ part in U_0. So by Corollary 3.5 proved below there is a $\mathbb{Z}[G_v]$-decomposition $U_0 = \mathbb{Z}^a \oplus \mathbb{Z}[G_v]^b$ with appropriate $a, b \in \mathbb{Z}$. The integers a, b and a corresponding basis $\bar{x}_1, \ldots, \bar{x}_a, \bar{y}_1, \ldots, \bar{y}_b$ can be computed by the constructive proof of [CR62, Thm. (74.3)], see Remark 3.6.

Step 3: Applying Lemma 1.27 to the isomorphism $U_0 \simeq \mathbb{Z}^a \oplus \mathbb{Z}[G_v]^b$ we get an isomorphism

$$\mathrm{Yext}^1_{G_v}(U_0, U_{\mathrm{tor}}) \simeq \bigoplus_{i=1}^{a} \mathrm{Yext}^1_{G_v}(\mathbb{Z}, U_{\mathrm{tor}}) \oplus \bigoplus_{i=1}^{b} \mathrm{Yext}^1_{G_v}(\mathbb{Z}[G_v], U_{\mathrm{tor}}).$$

Through this isomorphism the module $(\mathbb{Z}, U_{\mathrm{tor}}) \oplus \mathbb{Z}^{a-1} \oplus \mathbb{Z}[G_v]^b$ is an extension of U_0 with U_{tor} corresponding to the tuple consisting of the non-trivial extension (3.3) in $\mathrm{Yext}^1_{G_v}(\mathbb{Z}, U_{\mathrm{tor}})$, $a-1$ trivial extensions in $\mathrm{Yext}^1_{G_v}(\mathbb{Z}, U_{\mathrm{tor}})$ and b trivial extensions in $\mathrm{Yext}^1_{G_v}(\mathbb{Z}[G_v], U_{\mathrm{tor}})$. It is therefore a non-trivial extension of U_0 with U_{tor}. The module U is also a non-trivial extension because otherwise $\hat{H}^{-1}(G_v, U) = \hat{H}^{-1}(G_v, U_{\mathrm{tor}}) \oplus \hat{H}^{-1}(G_v, U_0)$ which is a contradiction to $\hat{H}^{-1}(G_v, U) = 0 \neq \hat{H}^{-1}(G_v, U_{\mathrm{tor}})$. Then the isomorphism $\psi : (\mathbb{Z}; U_{\mathrm{tor}}) \oplus \mathbb{Z}^{a-1} \oplus \mathbb{Z}[G_v]^b \simeq U$ can be constructed as follows.

Since U is a non-trivial extension of U_0 with U_{tor}, at least one of the generators $\bar{x}_i$ of the $\mathbb{Z}^a$ part in U_0 does not have a G_v-invariant lift. Otherwise, by the arguments used in step 1 the module U would be a trivial extension of U_0 with U_{tor}. Denote the lifts of $\bar{x}_i, \bar{y}_i$ to U by x_i, y_i. By reordering the basis of U_0, we can assume that for some appropriate integer $c \geq 1$ the first c generators $\bar{x}_1, \ldots, \bar{x}_c$ do not have a G_v-invariant lift and that $x_{c+1}, \ldots x_a$ are elements of U^{G_v}.

Each generator x_i, $1 \leq i \leq c$, corresponds to a non-trivial extension of $\mathbb{Z}$ with U_{tor} (via Lemma 1.27), where the G_v-action $\sigma_v x_i = \theta_i x_i$ is given by an element $\theta_i \in U_{\mathrm{tor}} \setminus U_{\mathrm{tor}}^2$ (see step 1). Since $U_{\mathrm{tor}}/U_{\mathrm{tor}}^2 \simeq \mathbb{Z}/2\mathbb{Z}$, the quotients θ/θ_i are elements in $U_{\mathrm{tor}}^2 = \mathrm{I}_{G_v} U_{\mathrm{tor}}$ and one can find $\eta_i \in U_{\mathrm{tor}}$ satisfying $\eta_i^{\sigma_v - 1} = \theta/\theta_i$. Here, $\theta \in U_{\mathrm{tor}}$ is the fixed element from the construction of $(\mathbb{Z}; U_{\mathrm{tor}})$ in step 1.

In $(\mathbb{Z};U_{\mathrm{tor}})\oplus\mathbb{Z}^{a-1}\oplus\mathbb{Z}[G_v]^b$ denote the $\mathbb{Z}[G_v]$-generators of the $\mathbb{Z}^{a-1}$ part by $g_2,\dots g_a$, those of the $\mathbb{Z}[G_v]^b$ part by $h_1,\dots,h_b$ and let $(\mathbb{Z};U_{\mathrm{tor}})=U_{\mathrm{tor}}\oplus\mathbb{Z}$ be the module constructed in step 1 with $g_1=(0,1)$. Then define the homomorphism $\psi:(\mathbb{Z};U_{\mathrm{tor}})\oplus\mathbb{Z}^{a-1}\oplus\mathbb{Z}[G_v]^b\to U$ by

$$\begin{aligned}\psi(u)&=u\quad\text{for } u\in U_{\mathrm{tor}},\\ \psi(h_i)&=y_i,\\ \text{and}\quad \psi(g_i)&=\begin{cases}x_1\eta_1 & \text{for } i=1,\\ \frac{x_i}{x_1}\cdot\frac{\eta_i}{\eta_1} & \text{for } 2\le i\le c,\\ x_i & \text{for } c+1\le i\le a.\end{cases}\end{aligned}\tag{3.4}$$

This is a G_v-module homomorphism since

$$\begin{aligned}\sigma_v\psi(g_1)&=\sigma_v(x_1\eta_1)=\theta_1x_1\frac{\theta\eta_1}{\theta_1}=\theta x_1\eta_1=\psi(\theta g_1)=\psi(\sigma_v g_1),\\ \text{and}\quad\sigma_v\psi(g_i)&=\frac{\sigma_v(x_i\eta_i)}{\sigma_v(x_1\eta_1)}=\frac{\theta x_i\eta_i}{\theta x_1\eta_1}=\psi(g_i)=\psi(\sigma_v g_i)\quad\text{ for } 2\le i\le a.\end{aligned}$$

The homomorphism ψ induces a G_v-homomorphism ϕ on U_0 given by $\phi(\bar{x}_1)=\bar{x}_1$, $\phi(\bar{x}_i)=\bar{x}_i-\bar{x}_1$, and $\phi(\bar{y}_1)=\bar{y}_1$. The map ϕ obviously is an isomorphism and by the snake lemma ψ must then also be an isomorphism. This can be combined in the following commutative diagram:

$$\begin{tikzcd} 0 \arrow[r] & U_{\mathrm{tor}} \arrow[r] \arrow[d, equal] & (\mathbb{Z};U_{\mathrm{tor}})\oplus\mathbb{Z}^{a-1}\oplus\mathbb{Z}[G_v]^b \arrow[r] \arrow[d, "\psi", "\simeq"'] & U_0 \arrow[r] \arrow[d, "\phi", "\simeq"'] & 0 \\ 0 \arrow[r] & U_{\mathrm{tor}} \arrow[r] & U \arrow[r] & U_0 \arrow[r] & 0 \end{tikzcd}\tag{3.5}$$

For $2\le i\le a$ the images $\psi(g_i)$ are G_v invariant and therefore $\iota_v(\psi(g_i))\in\mathbb{R}$. If one changes the image $\psi(g_i)$ for some $2\le i\le a$ such that $\psi(g_i)=-(x_i/x_1\cdot\eta_i/\eta_1)$ (or $\psi(g_i)=-x_i$ if $i>c$), then ψ is still an isomorphism and does not affect the commutativity since $-1\in U_{\mathrm{tor}}$. Hence, we can define ψ in such a way that the elements $u_i:=\psi(g_i)$, $2\le i\le a$ have a positive embedding $\iota_v(u_i)>0$ in $\mathbb{R}$.

Step 4: Since $\hat{H}^0(G_v,L_v^\times)=\hat{H}^0(G_v,\mathbb{C})=\mathbb{R}^\times/\mathbb{R}_{>0}$ there exist elements $\lambda_i\in\mathbb{C}$ satisfying $\mathrm{N}_{G_v}(\lambda_i)=\iota_v(u_i)$. Multiplying these elements λ_i by suitable (transcendental) elements on the unit circle, they become algebraically independent[2] and $\prod_{i=2}^a\lambda_i^{a_i+b_i\sigma_v}\in\iota_v(U)$ implies $a_i=b_i$ for $i=2,\dots,a$. Note that for our purposes it is enough to know the existence of these elements λ_i. In our applications, we can work with abstract generators λ_i for which we define the G_v-action by $\sigma_v\lambda_i=u_i\lambda_i^{-1}$.

[2] By Baker's methods on linear forms in logarithms, elements $\alpha_2,\dots,\alpha_a\in\mathbb{C}$ are already algebraically independent if $\log(\alpha_i)$ and 1 are linearly independent over $\mathbb{Q}$.

Step 5: We finally define $W = (\mathbb{Z}; U_{\mathrm{tor}}) \oplus \bigoplus_{i=2}^{a} \mathbb{Z}[G_v]\lambda_i \oplus \mathbb{Z}[G_v]^b$ which can be seen as subset of $\mathbb{C}$ by $\lambda_i \in \mathbb{C}^\times$ and by the composite $\iota_v \circ \psi$.

Verification of (i) and (ii): As an abelian group $W = \iota_v(U) \oplus \bigoplus_{i=2}^{a} \mathbb{Z}\lambda_i \subset \mathbb{C}^\times$ which can be identified as a submodule of $\mathbb{C}$ in the obvious way. It contains $\iota_v(U)$ and $W/\iota_v(U) \simeq \bigoplus_{i=1}^{a-1} \mathbb{Z}\lambda_i$ is torsion-free. By construction of W the cohomology groups of W are $\hat{H}^i(G_v, W) = \hat{H}^i(G_v, (\mathbb{Z}; U_{\mathrm{tor}}))$, so we need to prove that the cohomology of $(\mathbb{Z}; U_{\mathrm{tor}})$ and $L_v^\times = \mathbb{C}^\times$ are isomorphic.

We therefore consider the cyclic cohomology diagram corresponding to (3.3)

$$\begin{tikzcd}
& \underset{=\mathbb{Z}/2\mathbb{Z}}{\hat{H}^0(G_v, U_{\mathrm{tor}})} \arrow[r, "f_1"] & \hat{H}^0(G_v, (\mathbb{Z}; U_{\mathrm{tor}})) \arrow[dr, "f_2"] & \\
\underset{=0}{\hat{H}^{-1}(G_v, \mathbb{Z})} \arrow[ur] & & & \underset{=\mathbb{Z}/2\mathbb{Z}}{\hat{H}^0(G_v, \mathbb{Z})} \arrow[dl, "f_3"] \\
& \hat{H}^{-1}(G_v, (\mathbb{Z}; U_{\mathrm{tor}})) \arrow[ul] & \underset{=\mathbb{Z}/2\mathbb{Z}}{\hat{H}^{-1}(G_v, U_{\mathrm{tor}})} \arrow[l, "f_4"'] &
\end{tikzcd}$$

in which the cohomology of U_{tor} is known by previous computations. By definition of the connecting homomorphism, f_3 maps 1 to $g_1^{\sigma_v - 1} = \theta \in U_{\mathrm{tor}} = {}_{\mathrm{N}_{G_v}}U_{\mathrm{tor}}$ which is not in $\mathrm{I}_{G_v} U_{\mathrm{tor}}$ by definition of $(\mathbb{Z}; U_{\mathrm{tor}})$ in step 3. Hence, the image $f_3(1)$ is nonzero in $\hat{H}^{-1}(G_v, U_{\mathrm{tor}}) \simeq {}_{\mathrm{N}_{G_v}}U_{\mathrm{tor}} / \mathrm{I}_{G_v} U_{\mathrm{tor}} \simeq \mathbb{Z}/2\mathbb{Z}$ and f_3 is an isomorphism. As a consequence, $f_2 = f_4 = 0$ and f_1 is also an isomorphism. This implies $\hat{H}^{-1}(G_v, (\mathbb{Z}; U_{\mathrm{tor}})) = 0$ and $\hat{H}^0(G_v, (\mathbb{Z}; U_{\mathrm{tor}})) = \mathbb{Z}/2\mathbb{Z}$.

Altogether, this gives isomorphisms

$$\begin{aligned}
&\hat{H}^{-1}(G_v, W) \simeq \hat{H}^{-1}(G_v, (\mathbb{Z}; U_{\mathrm{tor}})) \simeq 0 \simeq \hat{H}^{-1}(G_v, L_v^\times) \\
\text{and} \quad &\hat{H}^0(G_v, W) \simeq \hat{H}^0(G_v, (\mathbb{Z}; U_{\mathrm{tor}})) \simeq \hat{H}^0(G_v, U_{\mathrm{tor}}) \simeq \hat{H}^0(G_v, L_v^\times),
\end{aligned} \tag{3.6}$$

the latter being induced by $U_{\mathrm{tor}} \subseteq (\mathbb{Z}; U_{\mathrm{tor}}) \subseteq W$ and $U_{\mathrm{tor}} \subseteq L_v^\times$. Hence, W_v has the same cohomology as $L_v^\times$. $\square$

We quote the following theorem of Diederichsen and Reiner and derive a corollary which will complete the proof.

Theorem 3.4. *For a cyclic group $G = \langle\sigma\rangle$ of prime order p every finitely generated, torsion-free $\mathbb{Z}[G]$-module M splits into a direct sum $M \simeq M_0 \oplus \cdots \oplus M_n$ of indecomposable modules. These modules M_i are either*

(i) $\mathbb{Z}$ with trivial G-action,

(ii) an $\mathcal{O}_K$-ideal $\mathfrak{a}$ of $K = \mathbb{Q}(\theta)$ with θ being a primitive p-th root of unity and G-action $\sigma a = \theta a$ for $a \in \mathfrak{a}$,

(iii) or a module $(\mathfrak{a}, a_0) := \mathfrak{a} \oplus \mathbb{Z}\lambda$ (direct sum as $\mathbb{Z}$-modules), with $\mathfrak{a}$ as in (ii) and $\sigma\lambda = a_0 + \lambda$ for a fixed element $a_0 \in \mathfrak{a} \setminus (\theta - 1)\mathfrak{a}$, i.e. $(\mathfrak{a}, a_0)$ is a non-split extension of $\mathbb{Z}$ with $\mathfrak{a}$.

Moreover, the isomorphism class of M is determined by the numbers of modules of the three types that occur and the ideal classes of the ideals $\mathfrak{a}$.

Proof. [CR62, Thm. (74.3)] or [CR81, Thm. (34.31)]. □

The constructive proof of [CR62, Thm. (74.3)] also shows how $\mathbb{Z}[G]$-generators of the decomposition can be computed. For the cyclic group of order two one therefore has the following decomposition.

Corollary 3.5. *Let $G = \langle\sigma\rangle$ be a group of order 2. Any finitely generated, torsion free $\mathbb{Z}[G]$-module M decomposes into*

$$M \simeq \mathbb{Z}^a \oplus (\mathbb{Z}^-)^b \oplus \mathbb{Z}[G]^c. \tag{3.7}$$

Here, the G action on $\mathbb{Z}$ is trivial and $\mathbb{Z}^-$ denotes the module $\mathbb{Z}$ with σ acting as multiplication by -1.

Proof. In the special case $p = 2$ of Theorem 3.4, the parameters of the decomposition become: $\theta = -1$, $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$. The class number of $\mathbb{Q}$ is 1, so we can assume that every ideal $\mathfrak{a}$ is equal to $\mathbb{Z}$. All modules of type (ii) are then isomorphic to $\mathbb{Z}^-$. In (iii), $a_0 \notin 2\mathbb{Z}$ and since $(\mathfrak{a}, a_0) \simeq (\mathfrak{a}, ca_0)$ for $2 \nmid c$ (see [CR62, Lem. (74.2)]), we can assume $a_0 = 1$ and $(\mathfrak{a}, a_0) = (\mathbb{Z}, 1) = \mathbb{Z}^- + \mathbb{Z}\lambda$ with G-action $\sigma\lambda = 1 + \lambda$. Since

$$\begin{aligned} \mathbb{Z}^- + \mathbb{Z}\lambda &\to \mathbb{Z}[G] \\ x + y\lambda &\mapsto x(1-\sigma) + y\sigma \end{aligned}$$

is an isomorphism of G-modules, the modules of type (iii) are isomorphic to $\mathbb{Z}[G]$. Altogether, we get the isomorphism (3.7). □

Remark 3.6. In general the computation of a $\mathbb{Z}[G]$-basis of a free $\mathbb{Z}[G]$-module M is a sophisticated task. The constructive proof of [CR62, Thm. (74.3)] is restricted to cyclic groups G of prime order p, which is a strong condition on the group G. In order to see that those generators can indeed be constructed, we recall the proof for a cyclic group $G = \{1, \sigma\}$ of order 2.

The kernel $K = \ker(1+\sigma)$ is a free submodule of M and there exists a $\mathbb{Z}$-module X such that $M = K \oplus X$ as $\mathbb{Z}$-modules. The module $(\sigma - 1)M \subseteq K$ is a $\mathbb{Z}$-module of the same rank $n \in \mathbb{N} \cup \{0\}$ and by the elementary divisor theorem there exists a basis $b_1, \dots, b_n$ of $K = \ker(1+\sigma)$ and integers $e_1, \dots, e_n$ such that

$$\begin{aligned} K &= \mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_n, \\ (\sigma - 1)M &= \mathbb{Z}e_1b_1 \oplus \cdots \oplus \mathbb{Z}e_nb_n. \end{aligned}$$

Such a basis can be computed using the *Smith normal form* as for example in [Coh93, Alg. 2.4.14]. By $(\sigma-1)K \subseteq (\sigma-1)M \subseteq K$ one obtains $\mathbb{Z}2b_i \subseteq \mathbb{Z}e_ib_i \subseteq \mathbb{Z}b_i$ and discovers that $e_i \in \{1, 2\}$.

Let r be an integer such that $e_1 = \cdots = e_r = 1$ and $e_{r+1} = \cdots = e_n = 2$. Then the quotient $Q = (\sigma - 1)M/(\sigma - 1)K$ is $Q \simeq (\mathbb{Z}/2\mathbb{Z})^r$ and the images $b_1^*, \ldots, b_r^*$ of $b_1, \ldots, b_r$ generate Q.

Consider the surjective homomorphism $\phi : X \to Q$, $x \mapsto (\sigma - 1)x + (\sigma - 1)M$ and let $x_1', \ldots, x_k'$ be a $\mathbb{Z}$-basis of X. Then $k \geq r$ and ϕ is given by a matrix $A = (a_{ij}) \in \mathrm{Mat}_{k \times r}(\mathbb{Z}/2\mathbb{Z})$ such that $\phi(x_i') = \sum_{j=1}^{r} a_{ij} b_j^*$. By diagonalizing A over $\mathbb{Z}/2\mathbb{Z}$ one finds a matrix $\bar{U} \in \mathrm{Gl}_k(\mathbb{Z}/2\mathbb{Z})$ and a corresponding lift $U \in \mathrm{Gl}_k(\mathbb{Z})$ such that the basis $x_i = \sum_{j=1}^{k} u_{ij} x_j'$ satisfies $\phi(x_i) = c_i b_i^*$ for $1 \leq i \leq r$ and $\phi(x_j) = 0$ for $r < j \leq n$ for suitable $c_i \in \mathbb{Z} \setminus 2\mathbb{Z}$.

Let $\lambda_i \in K$ such that $(\sigma - 1)x_i = c_i b_i + (\sigma - 1)\lambda_i$ for $1 \leq i \leq r$ and $(\sigma - 1)x_j = (\sigma - 1)\lambda_j$ for $r < j \leq n$. Then the elements $y_i := x_i - \lambda_i$ satisfy $\sigma y_i = c_i b_i + y_i$ for $1 \leq i \leq r$ and $\sigma y_j = y_j$ for $r < j \leq n$.

One therefore obtains

$$\begin{aligned} M = {} & (\mathbb{Z}b_1 \oplus \mathbb{Z}y_1) \oplus \cdots \oplus (\mathbb{Z}b_r \oplus \mathbb{Z}y_r) \\ & \oplus \mathbb{Z}b_{r+1} \oplus \cdots \oplus \mathbb{Z}b_n \oplus \mathbb{Z}y_{r+1} \oplus \cdots \oplus \mathbb{Z}y_k \end{aligned}$$

with $\mathbb{Z}[G]$-module isomorphisms $\mathbb{Z}b_j \simeq \mathbb{Z}^-$, $\mathbb{Z}y_j \simeq \mathbb{Z}^+$ for $j > r$ and

$$\begin{aligned} \mathbb{Z}[G] & \simeq \mathbb{Z}b_i \oplus \mathbb{Z}y_i \\ 1 & \mapsto -y_i - (c_i' + 1)b_i \end{aligned}$$

where $c_i = 2c_i' + 1$. This completes the construction of a $\mathbb{Z}[G]$-basis of M which provides an isomorphism of the form (3.7).

The constructive aspects of Proposition 3.3 can now be turned into the following algorithm. For ramified infinite places $v \in S_\infty$ whose decomposition group $G_v = \{1, \sigma_v\}$ is cyclic of order two, we write the action of σ_v on $x \in L_v = \mathbb{C}$ as conjugation $\overline{x}$ and ι_v for the embedding $L \hookrightarrow L_v = \mathbb{C}$.

For algorithms on abelian groups and basic algorithms in number theory we refer to [Coh93].

Algorithm 3.7 (Construction of modules W).

Input: A finite Galois extension $L|K$ of number fields with group G and an infinite place v of L.

Output: A finitely generated $Z[G]$-module W_v satisfying the conditions (i)–(iii) of Proposition 3.3.

1 Compute the S-units $U = U_{L,S}$ using [Coh00, Alg. 7.4.6], its torsion subgroup U_{tor} and define $U_0 = U/U_{\mathrm{tor}}$.

2 If $G_v = 1$, define $W_v = \iota_v(U_{L,S})$ and terminate.

3 Choose $\theta \in U_{\mathrm{tor}} \setminus U_{\mathrm{tor}}^2$ and define $(\mathbb{Z}; U_{\mathrm{tor}}) = U_{\mathrm{tor}} \oplus \mathbb{Z}$ with G_v-action $\overline{(0,1)} = (\theta, 1)$.

4 Compute $a, b \in \mathbb{Z}$ such that $U_0 \simeq \mathbb{Z}^a \oplus \mathbb{Z}[G]^b$ and a corresponding basis $\bar{x}_1, \dots, \bar{x}_a, \bar{y}_1, \dots, \bar{y}_b$ using the proof of [CR62, Thm. (74.3)] as described in Remark 3.6. Denote lifts of the basis of U_0 by x_i and y_i, respectively, and choose the basis of U_0 such that $x_{c+1}, \dots, x_a \in U^{G_v}$ and $\bar{x}_1, \dots \bar{x}_c$ do not have G_v-invariant lifts (for some $c \in \mathbb{N}$).

5 For $1 \leq i \leq c$, let the G_v-action on $x_i \in U$ be given by $\sigma_v(x_i) = \theta_i x_i$ with appropriate $\theta_i \in U_{\mathrm{tor}}$. Compute elements $\eta_i \in U_{\mathrm{tor}}$ such that $\eta_i^{\sigma_v - 1} = \theta/\theta_i$ with θ as chosen in step 3.

6 Define the isomorphism $\psi : (\mathbb{Z}; U_{\mathrm{tor}}) \oplus \mathbb{Z}^{a-1} \oplus \mathbb{Z}[G]^b \to U$ as in (3.4). For $i = 2, \dots, a$ the signs should be chosen such that the images $u_i := \psi(g_i)$ have a positive embedding $\iota_v(u_i) > 0$ in $\mathbb{R}$.

7 Compute algebraically independent elements $\lambda_i \in \mathbb{C}$ which satisfy $\lambda_i \bar{\lambda}_i = u_i$ such that $\prod_{i=2}^{a} \lambda_i^{a_i + b_i \sigma} \in U$ implies $a_i = b_i$ for $i = 2, \dots, a$.

Return: The module $W_v := (\mathbb{Z}; U_{\mathrm{tor}}) \oplus \bigoplus_{i=2}^{a} \mathbb{Z}[G]\lambda_i \oplus \mathbb{Z}[G]^b$ which is embedded in $\mathbb{C}$ via ψ and $\lambda_i \in \mathbb{C}$.

If an explicit embedding into $\mathbb{C}$ is not needed, one can also consider abstract generators λ_i upon which the σ_v-action is defined by $\sigma_v(\lambda_i)\lambda_i = u_i$. This will actually be the case in all our applications.

For any place v we can now construct a finitely generated module L_v^f which is cohomologically isomorphic to $L_v^\times$. For finite places v it is given by the module $L_v^f := L_v^\times / \exp(\mathscr{L}_v)$ constructed in Lemma 2.1 using a full projective sublattice $\mathscr{L}_v$ of $\mathcal{O}_{L_v}$. For infinite places v it is given by the module $L_v^f := W_v \subset \mathbb{C}^\times$ constructed by Algorithm 3.7.

We continue to construct a finitely generated approximation to the idèle class group by fixing a set of G-representatives $S(G)$ in S and corresponding modules L_v^f. Then we define

$$I_{L,S}^f := \bigoplus_{v \in S(G)} \mathrm{ind}_{G_v}^G L_v^f \quad \text{and} \quad C_{L,S}^f := I_{L,S}^f / U_{L,S} \tag{3.8}$$

which are finitely generated modules.

Proposition 3.8. *There are isomorphisms*

$$\hat{H}^2\big(G, I_{L,S}^f\big) \simeq \hat{H}^2(G, I_{L,S}) \quad \textit{and} \quad \hat{H}^2\big(G, C_{L,S}^f\big) \simeq \hat{H}^2(G, C_L).$$

Proof. [Chi85, Prop. 2.1]. □

Explicitly, the isomorphisms are induced by the projections $L_v^\times \twoheadrightarrow L_v^\times / \exp(\mathscr{L}_v) = L_v^f$ for finite places v and injections $L_v^f = W_v \hookrightarrow L_v^\times$ for infinite places v. Each of those maps induce isomorphisms $\hat{H}^2(G_v, L_v^\times) \simeq \hat{H}^2(G_v, L_v^f)$ and therefore $I_{L,S}^f$ and $I_{L,S}$ are cohomologically isomorphic.

The analog isomorphism for $C^f_{L,S}$ and C_L is then obtained by applying the five lemma to the long cohomology sequences arising from the diagram

$$\begin{tikzcd}
0 \arrow[r] & U_{L,S} \arrow[r] \arrow[d, equal] & I^f_{L,S} \arrow[r] \arrow[d, hook] & C^f_{L,S} \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & U_{L,S} \arrow[r] & I^q_{L,S} \arrow[r] & C^q_{L,S} \arrow[r] & 0 \\
0 \arrow[r] & U_{L,S} \arrow[r] \arrow[u, equal] & I_{L,S} \arrow[r] \arrow[u, two heads] & C_{L,S} \arrow[r] \arrow[u, two heads] & 0
\end{tikzcd} \tag{3.9}$$

where $I^q_{L,S} := \bigoplus_{v \in S_f(G)} \operatorname{ind}^G_{G_v} L^f_v \oplus \bigoplus_{v \in S_\infty(G)} \operatorname{ind}^G_{G_v} L^\times_v$ and $C^q_{L,S} := I^q_{L,S}/U_{L,S}$.

These isomorphisms allow the computation of the cohomology of the idèle class group using the finite approximations (3.8).

Algorithm 3.9 (Idèle class group).
Input: A finite Galois extension $L|K$ of number fields with Galois group G.

Output: A finitely generated $\mathbb{Z}[G]$-module $C^f_{L,S}$ which is cohomologically isomorphic to C_L.

1 Let S be a set of places of L satisfying conditions (S1)–(S4).

2 For every finite place $v \in S_f(G)$ compute a finitely generated module L^f_v as in Lemma 2.1.

3 For every infinite place $v \in S_\infty(G)$ compute the module $L^f_v = W_v$ using Algorithm 3.7.

4 Compute induced modules $\operatorname{ind}^G_{G_v} L^f_v$ and the groups $I^f_{L,S}$ and $C^f_{L,S}$ as in (3.8).

Note that the verification of the conditions on S in step 1 can be very difficult. For the condition (S4), which requires the S-idèle class group $Cl_S(L)$ to be trivial, one has to compute the class group Cl_L of L and this is known to be a sophisticated task. In the computation one uses the *Minkowski bound* which gives a bound on the norm of the ideals which will generate Cl_L. If one assumes the generalized Riemann hypothesis, one can replace this bound by the *Bach bound* which is much smaller.[3] This results in a significant speedup which will also be used in our implementation.

Since $C^f_{L,S}$ is a finitely generated module, one can compute its cohomology group $\hat{H}^2(G, C^f_{L,S}) \simeq \hat{H}^2(G, C_L)$ using [Hol06]. The construction of $C^f_{L,S}$ and its cohomology has been implemented as part of Algorithm 3.13 which constructs the global fundamental class in $\hat{H}^2(G, C^f_{L,S})$.

[3] See also the documentation of the command `ClassGroup` in the documentation [BCFS10] of Magma.

3.2 Computing global fundamental classes

After the computation of $\hat{H}^2(G, C_L)$ using the finite approximation $C^f_{L,S}$ in the last section, we want to find the global fundamental class in this group.

In analogy to the direct method for local fundamental classes[4], we construct the global fundamental class for a general Galois extension $L|K$ of number fields by considering a cyclic extension $L'|K$ of the same degree.

3.2.1 Cyclic case

Let $L'|K$ be a cyclic Galois extension of number fields with Galois group G'. Then the idèlic invariant map on the idèle group

$$\mathrm{inv} : \hat{H}^2(G', I_{L'}) \twoheadrightarrow \frac{1}{[L':K]}\mathbb{Z}/\mathbb{Z}$$

from Definition 1.10 is surjective by Lemma 1.11 (see also [Neu69, Chp. III, (5.6)]). So there exists a cocycle in $Z^2(G', I_{L'})$ representing the global fundamental class of $L'|K$. This element can be constructed from a single place u_0 of K which is *undecomposed* in L', i.e. there is just one place v_0' in L' dividing u_0.

Let us first assume, that we have such a place u_0. Then the decomposition group $G'_{v_0'}$ is equal to G. We may therefore apply Algorithm 2.18 to compute the local fundamental class u' of the extension $L'_{v_0'}|K_{u_0}$ as a cocycle in $Z^2\big(G', L'_{v_0'}\big)$. Then the element $(\ldots, 1, u', 1, \ldots) \in \hat{H}^2(G', I_{L'}) \subseteq \prod'_u \hat{H}^2\big(\mathrm{Gal}(L'_{v'}/K_u), L'^{\times}_{v'}\big)$ has invariant $1/[L':K]$ and thus represents the global fundamental class of $L'|K$.

If S' is a finite set of places satisfying (S1)–(S4), we set $S = S' \cup \{v_0'\}$ and use the finite product $I_{L',S}$ in which the images of the cocycle u' can explicitly be represented up to a finite precision.

Obviously, this computation of the global fundamental class does not depend on G' being cyclic, but on the existence of an undecomposed place u_0. It can therefore also be applied to general extensions $L|K$ for which an undecomposed prime is known. However, for cyclic extensions the existence of undecomposed primes is an immediate consequence of *Chebotarev's density theorem,* see Corollary 1.13.

If the extension is non-cyclic, there can still be an undecomposed prime. But this prime then must be among the (finitely many) ramified primes, which is a very strong condition on the number field.

[4]Compare Section 2.2.1.

3.2.2 General case

Let $L|K$ be a finite Galois extension of number fields with group G and $L'|K$ an extension of the same degree with cyclic Galois group G'. Denote their composite field by $N = LL'$ and the Galois groups by $\Gamma = \mathrm{Gal}(N|K)$, $H = \mathrm{Gal}(N|L)$ and $H' = \mathrm{Gal}(N|L')$:

$$\begin{tikzcd}
 & N \arrow[dl, dash] \arrow[dd, dash] \arrow[dd, bend left, dash, "H'"] \arrow[dddl, bend left=60, dash, "\Gamma"] \\
L \arrow[dd, dash] \arrow[ur, bend left, dash, "H"] & \\
 & L' \arrow[dl, dash] \arrow[dl, bend left, dash, "G'"] \\
K \arrow[uu, bend left, dash, "G"] &
\end{tikzcd}$$

Denote the places of K, L, L' and N by u, v, v' and w, respectively. Again, let S be a set of places of N satisfying (S1)–(S4). As in the cyclic case, let u_0 be a place of K which does not decompose in L' and assume that S contains all places of N dividing u_0.

As in the direct method for the local fundamental class one can then compute all the cohomology groups involved and find the global fundamental class of $L|K$ by inflating the global fundamental class for the cyclic extension $L'|K$. However, in order to avoid computations in the complex numbers, we have to make sure that the inflation maps can operate on $C^f_{L,S}$ and $C^f_{L',S}$ directly, i.e. on the modules W_v as abstract groups without using embeddings $W_v \hookrightarrow \mathbb{C}$.

Below we therefore construct $C^f_{L,S}$ and $C^f_{L',S}$ as subgroups of $C^f_{N,S}$ which are fixed by H and H'.

As in the previous section, for each Γ-representative w of the places in S, let N^f_w be a finitely generated module which is cohomologically isomorphic to $N^\times_w$. That is $N^f_w = N_w/\exp(\mathscr{L}_w)$ for finite places w and $N^f_w = W_w \subset \mathbb{C}^\times$ for infinite places w. Then define

$$I^f_{N,S} := \bigoplus_{w \in S(\Gamma)} \mathrm{ind}^{\Gamma}_{\Gamma_w} N^f_w. \tag{3.10}$$

As before we write $C^f_{N,S} = I^f_{N,S}/U_{N,S}$ and we have $\hat{H}^2\big(\Gamma, C^f_{N,S}\big) \simeq \hat{H}^2(\Gamma, C_N)$. To get a corresponding representation for $C^f_{L,S}$ and $C^f_{L',S}$ such that we can easily compute inflations $\hat{H}^2\big(G, C^f_{L,S}\big) \hookrightarrow \hat{H}^2\big(\Gamma, C^f_{N,S}\big)$ and $\hat{H}^2\big(G', C^f_{L',S}\big) \hookrightarrow \hat{H}^2\big(\Gamma, C^f_{N,S}\big)$ we have to compute $C^f_{L,S}$ and $C^f_{L',S}$ using submodules of $\mathscr{L}_w$ and W_w as described in the following proposition.

Proposition 3.10. *(i) The fixed group $\big(I^f_{N,S}\big)^H$ is given by*

$$I^f_{L,S} = \bigoplus_{u \in S_f} \mathrm{ind}^G_{G_v} L^\times_v / \exp(\mathscr{L}_v) \oplus \bigoplus_{u \in S_\infty} \mathrm{ind}^G_{G_v} W^{H_w}_w$$

where for each place u we fix v such that $w|v|u$ *and* $\mathscr{L}_v := \mathscr{L}_w \cap \mathcal{O}_{L_v}$.

(ii) The module $\mathscr{L}_v$ *satisfies the properties of Lemma 2.1: it is a projective module and* $L_v^\times / \exp(\mathscr{L}_v)$ *is finitely generated and cohomologically isomorphic to* $L_v^\times$.

(iii) The module $W_v := W_w^{H_w}$ *satisfies the properties from Proposition 3.3.*

Note that these statements also hold for L' by using the subgroup H' of Γ. The proof of the first part is based on the following lemma for $\mathbb{Z}[G]$ modules.

Lemma 3.11. *Let* Γ *be a group,* $\Gamma_w \subseteq \Gamma$ *a subgroup,* $H \subseteq \Gamma$ *a normal subgroup, and let* M *be a* Γ_w*-module. Denote* $G = \Gamma/H$, $H_w = H \cap \Gamma_w$, $G_v = \Gamma_w/H_w$. *Then*

$$\left(\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Gamma_w]} M\right)^H \simeq \mathbb{Z}[G] \otimes_{\mathbb{Z}[G_v]} M^{H_w}$$

or equivalently $\left(\mathrm{Ind}_{\Gamma_w}^{\Gamma} M\right)^H \simeq \mathrm{Ind}_{G_v}^{G} M^{H_w}$ *are isomorphisms as* $\mathbb{Z}[G]$*-modules.*

Proof. As in [NSW00, Chp. I, § 6], we can write the elements of induced modules as homomorphisms. By rewriting the condition to be fixed by H we can prove directly:

$$\begin{aligned}
&\left(\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[\Gamma_w]} M\right)^H = \left(\mathrm{Ind}_{\Gamma_w}^{\Gamma} M\right)^H \\
&= \{f : \Gamma \to M \mid \sigma f(x) = f(\sigma x)\ \forall \sigma \in \Gamma_w, x \in \Gamma\}^H \\
&\qquad\qquad \text{with } \Gamma\text{-action } (\sigma f)(x) = f(x\sigma) \text{ for } \sigma \in \Gamma \\
&= \{f : \Gamma/H \to M \mid \sigma f(xH) = f(\sigma x H)\ \forall \sigma \in \Gamma_w, x \in \Gamma\} \\
&\qquad\qquad \text{since elements fixed by } H \text{ have only one value per coset} \\
&= \{f : \Gamma/H \to M^{H_w} \mid \sigma f(xH) = f(\sigma x H)\ \forall \sigma \in \Gamma_w, x \in \Gamma\} \\
&\qquad\qquad \text{as } \tau f(xH) = f(\tau x H) = f(xH)\ \forall \tau \in \Gamma_w \cap H = H_w \\
&= \{f : \Gamma/H \to M^{H_w} \mid \sigma H_w f(xH) = f(\sigma H_w x H)\ \forall \sigma \in \Gamma_w/H_w, x \in \Gamma\} \\
&\qquad\qquad \text{because the values of } f \text{ are fixed under } H_w \\
&= \{f : G \to M^{H_w} \mid \tau f(y) = f(\tau y)\ \forall \tau \in G_v, y \in G\} \\
&= \mathrm{Ind}_{G_v}^{G} M^{H_w} = \mathbb{Z}[G] \oplus_{\mathbb{Z}[G_v]} M^{H_w}.
\end{aligned}$$

□

Proof of Proposition 3.10. (i) This is Lemma 3.11 since $G = \Gamma/H$, $L_v^\times = (N_w^\times)^{H_w}$, and $\mathscr{L}_v = \mathscr{L}_w^{H_w}$.

(ii) Let $\mathscr{L}_w = \mathbb{Z}[\Gamma_w]\theta$ be a full projective module as in Lemma 2.1 used in the computation of N_w^f. Since $\mathscr{L}_w$ is projective (and hence cohomologically trivial), one has $\mathscr{L}_w^{H_w} = \mathrm{N}_{H_w}(\mathscr{L}_w) = \mathrm{N}_{H_w}(\mathbb{Z}[\Gamma_w]\theta)$. This latter group is equal to $\mathbb{Z}[G_v]\,\mathrm{N}_{H_w}(\theta)$ because for every $\sigma \in \Gamma_w$ the right coset $H_w\sigma$ is equal to the left coset σH_w and the left cosets are represented by elements in G_v.

Therefore, the module $\mathscr{L}_v := \mathscr{L}_w \cap \mathcal{O}_{L_v} = \mathscr{L}_w^{H_w} = \mathbb{Z}[G_v]\,\mathrm{N}_{H_w}(\theta)$ is a projective $\mathbb{Z}[G_v]$-module. Since θ satisfies $v_N(\theta) > \frac{e(N_w|\mathbb{Q}_p)}{p-1}$ by construction (see the proof of Lemma 2.1), the element $\mathrm{N}_{H_w}(\theta)$ also satisfies the condition

$$v_L(\mathrm{N}_{H_w}(\theta)) = \frac{1}{e(N_w|L_v)} v_N(\mathrm{N}_{H_w}(\theta)) \geq v_N(\theta) > \frac{e(N_w|\mathbb{Q}_p)}{p-1} \geq \frac{e(L_v|\mathbb{Q}_p)}{p-1}.$$

of Lemma 2.1. Hence, the v-adic exponential function will be injective on $\mathscr{L}_v$ and $\hat{H}^2(G_v, L_v^\times) \simeq \hat{H}^2(G_v, L_v^\times / \exp(\mathscr{L}_v))$.

(iii) By definition $W_w \subseteq N_w^\times$ satisfies the properties for N. So $U_{N,S} \subseteq W_w$, $W_w/U_{N,S}$ is torsion-free, and the inclusion $W_w \hookrightarrow N_w^\times$ induces an isomorphism in Γ_w-cohomology. For L we know $U_{L,S} \subseteq W_w^{H_w}$ and its quotient is still torsion-free. The construction of W_w shows that $\hat{H}^1(H_w, W_w) = 0$, see (3.6). Therefore $L_v^\times/W_v \simeq (N_w^\times/W_w)^{H_w}$ and the fact that $N_w^\times/W_w$ is cohomologically trivial (as Γ_w-module) implies that $L_v^\times/W_v$ is cohomologically trivial as G_w-module with $G_w \simeq \Gamma_w/H_w$, c.f. [NSW00, Prop. (1.7.2)]. Hence, the injection $W_v \hookrightarrow L_v^\times$ induces an isomorphism in cohomology. □

Remark 3.12. The computation of the modules $\mathscr{L}_v$ and W_v as in the above proposition provides well-defined embeddings

$$L_v^\times / \exp(\mathscr{L}_v) = \left(N_w^\times / \exp(\mathscr{L}_w)\right)^{H_w} \hookrightarrow N_w^\times / \exp(\mathscr{L}_w)$$

given by $L_v^\times \subseteq N_w^\times$ and $W_v \hookrightarrow W_w$. This also induces a well-defined embedding of the finitely-generated modules $I_{L,S}^f \hookrightarrow I_{N,S}^f$.

For $C_{L,S}^f = (I_{N,S}^f)^H/U_{L,S}$ one can therefore explicitly compute the inflation map

$$\hat{H}^2\big(G, C_{L,S}^f\big) \hookrightarrow \hat{H}^2\big(\Gamma, C_{N,S}^f\big).$$

It is given by sending a cocycle $\gamma \in Z^2(G, I_{L,S}^f)$ to the element in $\hat{H}^2\big(\Gamma, C_{N,S}^f\big)$ represented by $\sigma, \tau \mapsto \gamma(\sigma H, \tau H) \in I_{L,S}^f \subseteq I_{N,S}^f$.

Similarly, this also works for the subfield L' of N. To sum up, we can explicitly compute inflations on the cohomology groups if we use the lattices above.

The computation of the global fundamental class is then described in the following diagram:

$$\begin{tikzcd} \hat{H}^2(G', I_{L',S}) \arrow[r, "\simeq"] & \hat{H}^2\big(G', I_{L',S}^f\big) \arrow[r, two heads] & \hat{H}^2\big(G', C_{L',S}^f\big) \arrow[r, hook] & \hat{H}^2\big(\Gamma, C_{N,S}^f\big) \\ & & & \hat{H}^2\big(G, C_{L,S}^f\big) \arrow[u, hook] \end{tikzcd} \tag{3.11}$$

As described in the cyclic case above, the local fundamental class for $L'_{v'_0}|K_{u_0}$ computed by Algorithm 2.18 gives a representation of the global fundamental class $u_{L'|K}$ in $C^2(G', I_{L',S})$ up to a finite precision. We can find its projection in $\hat{H}^2(G', C^f_{L',S})$ and inflate it to $\hat{H}^2(\Gamma, C^f_{N,S})$. Then we compute $\hat{H}^2(G, C^f_{L,S})$, choose a generator and inflate it to $\hat{H}^2(\Gamma, C^f_{N,S})$ as well. A comparison with the image of $u_{L'|K}$ then gives $u_{L|K}$ in $\hat{H}^2(G, C^f_{L,S})$.

Algorithm 3.13 (Global fundamental class).
Input: A finite Galois extension $L|K$ of number fields with group G.
Output: The global fundamental class $u_{L|K}$ as an element of an abstract group $\hat{H}^2(G, C^f_{L,S})$.

1 Consider a cyclic extension $L'|K$ of degree $[L' : K] = [L : K]$ and a prime u_0 of K such that there is only one prime v'_0 in L' dividing u_0.
2 Let N denote the composite LL' with Galois group $\Gamma = \mathrm{Gal}(N|K)$ and S a set of places satisfying the conditions (S1)–(S4).
3 For every $w \in S_f(\Gamma)$ compute a module $\mathscr{L}_w \subseteq \mathcal{O}_{N_w}$ as in Lemma 2.1.
4 For every $w \in S_\infty(\Gamma)$ compute a module W_w using Algorithm 3.7.
5 Compute $I^f_{N,S}$, $C^f_{N,S}$ by (3.8) and fixed modules $I^f_{L,S} = (I^f_{N,S})^H$, $C^f_{L,S} = (C^f_{N,S})^H$.
6 Compute the cohomology group $\hat{H}^2(G, C^f_{L,S})$ and the boundaries $B^2(\Gamma, C^f_{N,S})$ using [Hol06].
7 Let $k \in \mathbb{N}$ such that $\mathfrak{P}^k_{v'_0} \subseteq \mathscr{L}_{v'_0} = \mathscr{L}_w \cap \mathcal{O}_{L'_{v_0}}$. Compute the local fundamental class of $L'_{v'_0}|K_{u_0}$ of precision k using Algorithm 2.18. It represents the global fundamental class $u_{L'|K}$ in $Z^2(G', I_{L',S})$. Compute its inflation $\inf^{N|K}_{L|K}(u_{L'|K}) \in C^2(\Gamma, C^f_{N,S})$.
8 Find a generator g of the group $\hat{H}^2(G, C^f_{L,S})$ such that its inflation $\inf^{N|K}_{L|K}(g) \in C^2(\Gamma, C^f_{N,S})$ satisfies $\inf^{N|K}_{L'|K}(u_{L'|K}) - \inf^{N|K}_{L|K}(g) \in B^2(\Gamma, C^f_{N,S})$.

Return: The group $\hat{H}^2(G, C^f_{L,S})$ and its canonical generator g.

As in the direct method for local fundamental classes (see Algorithm 2.5), it is sufficient to compute the boundaries $B^2(\Gamma, C^f_{N,S})$ for the comparison in step 8. The group $Z^2(\Gamma, C^f_{N,S})$ and their quotient $\hat{H}^2(\Gamma, C^f_{N,S})$ are not needed. Again this makes a huge difference (in computation time) to the complete computation of $\hat{H}^2(\Gamma, C^f_{N,S})$.

This algorithm has been implemented for totally real fields L. In this case, the modules W_v can be chosen to be $U_{L,S}$ for every infinite place $v \in S_\infty(G)$. The modules $I^f_{N,S}$ and $C^f_{N,S}$ in the algorithm quickly get very large and will dominate the computation time of the algorithm.

Example 3.14. Let L be the splitting field of $f = x^3 - 4x + 1$ over $\mathbb{Q}$, which is a Galois extension with group S_3. Then f has discriminant 229 and $\mathbb{Q}(\sqrt{229})$ is a subfield of L. A suitable cyclic number field L' can be found as a subfield of $\mathbb{Q}(\zeta_{229})$. Let L' be the field generated by $g = x^6 - x^5 - 95x^4 + 530x^3 - 925x^2 + 367x + 187$. It is a cyclic number field in which the prime 229 is undecomposed, and $N = LL'$ has degree 18 over $\mathbb{Q}$.

A set S of places in L lying above the places $\{3, 7, 11, 229, \infty\}$ of $\mathbb{Q}$ satisfies conditions (S1)–(S4). As the field N is totally real, the module W_v we have to consider for one infinite place v of N can be chosen to be $W_v = U_{N,S}$. The S-units already have 36 generators and, therefore, the induced module $\mathrm{ind}_1^\Gamma W_v$ is generated by $36 \cdot 18 = 648$ elements (containing a free part of rank 630). The part of $I_{N,S}^f$ given by the finite places only has 21 generators.

In total, the module $I_{N,S}^f$ has 669 generators with a free part of rank 648 and its torsion subgroup (containing three copies of $\mathbb{Z}/228\mathbb{Z}$) has about 3 trillion elements.

The Magma implementation[5] of the above algorithm takes about 22 minutes to compute the global fundamental class of L. Most of the time (10 minutes) is spent on the computation of $I_{N,S}^f$. The verification of the conditions on S and the computation of the cohomology of $C_{N,S}^f$ each take another 5 minutes. Hence, these three parts already make more than 90% of the computation time.

The performance of Algorithm 3.13 is not very satisfactory and it would be interesting to find an approach similar to Serre's in the computation of local fundamental classes. As in the direct method for local fundamental classes, the main issue in the example above is the computation of the module $I_{N,S}^f$ whose biggest part is that at the infinite places. In the general case, the modules W_v for complex places v will even be more complicated. As a consequence, it is a main task to find a better approach to the construction of $C_{L,S}^f$ (or even another module which is cohomologically isomorphic to C_L) in order to get an efficient algorithm for the computation of global fundamental classes.

Therefore, Algorithm 3.7 has not been implemented yet and Algorithm 3.13 is restricted to totally real fields N.

[5]Command `GFCCompositum`, see documentation in Appendix B.2 on page 175.

4 Tate's canonical class

Tate's canonical class is an element which expresses the compatibility of local and global class field theory. For a fixed Galois extension $L|K$ of number fields, we will define an element which will incorporate information from the global fundamental class $u_{L|K}$ and all local fundamental classes $u_{L_v|K_p}$, where v runs through a finite, Galois invariant set S of places in L and p is the place of K below v. This combination of local fundamental classes will be called the *semi-local fundamental class*.

In this chapter we will first introduce this semi-local class and show how it can be computed. Afterwards, we define Tate's canonical class and also show its algorithmic construction. The main references for the definition of these classes is [Tat66] and the algorithmic construction is based on results presented in [Chi85] and [Chi89].

Let $L|K$ be a fixed Galois extension of number fields with group G and let S be a finite set of places in L satisfying conditions (S1)–(S4) from before (see page 70): i.e. S is a Galois invariant set of places including all ramified and infinite places and it contains enough places such that the S-ideal class group $Cl_S(F)$ is trivial for all $K \subseteq F \subseteq L$. Remember that these conditions were necessary to describe the cohomology of C_L using $C_{L,S}$.

We continue using the notation from the last chapters and let p denote places of K and v and w places of L:

$$
\begin{array}{cccc}
 & L & v & v, w \in S \\
G\Big(& \Big| & \Big| & \\
 & K & p &
\end{array}
$$

For a subgroup H of G we denote a (fixed) subset of representatives of the H-orbits in S by $S(H)$.[1] If v is a place in S with decomposition group G_v we will fix the set $S(G_v)$ in such a way that $v \in S(G_v)$. Note that any choice of $S(G_v)$ corresponds to a system R_v of representatives of G/G_v, i.e. $\sigma \in G$ is in R if and only if $v^\sigma \in S(G_v)$. Then $v \in S(G_v)$ implies $1 \in R$ and in the following we will always assume that the representatives are chosen this way.

[1]The set $S(v)$ of [Chi89] is then denoted by $S(G_v)$.

4.1 The semi-local fundamental class

The local fundamental classes $u_{L_v|K_p} \in \hat{H}^2(G_v, L_v^\times) \simeq \mathrm{Ext}^2_{G_v}(\mathbb{Z}, L_v^\times)$ will be combined as 2-extension where the left-most and right-most modules are finite products over $v \in S$ of the modules $\mathbb{Z}$ and $L_v^\times$, respectively.

More precisely, we define the group $Y = \bigoplus_{v \in S(G)} Y_v$ using $Y_v := \mathrm{ind}_{G_v}^G \mathbb{Z}$ and construct an extension in $\mathrm{Ext}^2_G(Y, I_{L,S})$ where $I_{L,S} = \prod_{v \in S} L_v^\times$ denotes the S-idèle group as before.

We can always think of elements in Y_v to be represented by a tuple of elements in $\mathbb{Z}$, i.e. $Y_v = \mathrm{ind}_{G_v}^G \mathbb{Z} = \bigoplus_{\sigma \in R_v} \sigma\mathbb{Z}$. By our fixed choice of representatives $S(G_v)$ and R_v, we can therefore identify $\mathbb{Z}$ with the subgroup $1 \cdot \mathbb{Z} \subseteq Y_v$.

Since the module Y is finitely generated and $\mathbb{Z}$-free, there is an isomorphism

$$\mathrm{Ext}^r_G(Y, I_{L,S}) \simeq \hat{H}^r(G, \mathrm{Hom}(Y, I_{L,S}))$$

between the extension group and the cohomology group (see Proposition 1.28 or [Bro94, Chp. III, Prop. (2.2)]). We therefore consider the following cohomological identifications from [Tat66] and [Chi89, Chp. III, § 2].

Proposition 4.1.

(a) $\hat{H}^r(G, \mathrm{Hom}(Y, M)) \simeq \prod_{v \in S(G)} \hat{H}^r(G_v, M)$ *for any* G*-module* M *and* $r \in \mathbb{Z}$.

(b) $\hat{H}^r(H, I_{L,S}) \simeq \prod_{v \in S(H)} \hat{H}^r(H \cap G_v, L_v^\times)$ *for any subgroup* $H \subseteq G$.

Proof. (a) The decomposition $\mathrm{Hom}(Y, M) = \prod_{v \in S(G)} \mathrm{Hom}(Y_v, M)$ in Proposition 1.26 and Shapiro's lemma for $\mathrm{Hom}(Y_v, M) = \mathrm{ind}_{G_v}^G \mathrm{Hom}(\mathbb{Z}, M)$ imply the isomorphisms

$$\hat{H}^r(G, \mathrm{Hom}(Y, M)) \simeq \prod_{v \in S(G)} \hat{H}^r(G, \mathrm{Hom}(Y_v, M)) \simeq \prod_{v \in S(G)} \hat{H}^r(G_v, \mathrm{Hom}(\mathbb{Z}, M)).$$

They are canonically given by restricting the images of a cocycle (which are homomorphisms in $\mathrm{Hom}(Y, M)$) to $Y_v \subseteq Y$ and then to $1 \cdot \mathbb{Z} \subseteq Y_v$. Composing the above isomorphism with $\hat{H}^r(G_v, \mathrm{Hom}(\mathbb{Z}, M)) \simeq \hat{H}^r(G_v, M)$ finishes the proof of (a).

(b) For $I_{L,S} = \bigoplus_{v \in S(G)} I_{L,v}$ with $I_{L,v} := \mathrm{ind}_{G_v}^G L_v^\times$, the same arguments yield

$$\hat{H}^r(G, I_{L,S}) \simeq \prod_{v \in S(G)} \hat{H}^r(G, I_{L,v}) \simeq \prod_{v \in S(G)} \hat{H}^r(G_v, L_v^\times).$$

This isomorphism just depends on L and the set S, which was a set of places in L, and it is independent of $K = L^G$. By considering a subgroup $H \subseteq G$, we implicitly consider L as an extensions of L^H and the isomorphism becomes $\hat{H}^r(H, I_{L,S}) \simeq \prod_{v \in S(H)} \hat{H}^r(H_v, L_v^\times)$. Since the decomposition group is $H_v = G_v \cap H$, this finishes the proof of (b). $\square$

By the first isomorphism we can then define the *semi-local fundamental class* as in [Tat66, Eq. (8)].

Definition 4.2 (Semi-local fundamental class). *The unique element $\alpha_2 \in \hat{H}^2(G, \mathrm{Hom}(Y, I_{L,S})) \simeq \prod_{v\in S(G)} \hat{H}^2(G_v, I_{L,S})$ which is given by the local fundamental classes $u_{L_v|K_p} \in \hat{H}^2(G_v, L_v^\times) \to \hat{H}^2(G_v, I_{L,S})$ using $L_v^\times \subseteq I_{L,S}$ is called* semi-local fundamental class.

This notion is well-defined with respect to the choice of the G-representatives $S(G)$ of G, cf. [Tat66, Eq. (8')]. If v^σ, $\sigma \in G$, is a place conjugated to v, then the completions at these places are also conjugated within the induced module $I_{L,v}$ by $L_{v^\sigma} = (L_v)^\sigma$. So restricting the induction of the local fundamental class $u_{L_v|K_p}$ to G_{v^σ} and projecting the images to $L_{v^\sigma}^\times$ will yield the local fundamental class of $L_{v^\sigma}|K_p$. For unramified extensions $L_v|K_p$, in which the invariant map is given through valuations, this follows from $v(x) = v^\sigma(x^\sigma)$ for $x \in L_v$. The general case then results from the fact that the fundamental classes satisfy the axioms of a *class formation*.

Corollary 4.3. *Using $M = I_{L,S}$ in isomorphism (a) and $H = G_w$ in isomorphism (b), Proposition 4.1 implies*

$$\begin{aligned} \hat{H}^r(G, \mathrm{Hom}(Y, I_{L,S})) &\xrightarrow{\simeq} \prod_{v\in S(G)} \prod_{w\in S(G_v)} \hat{H}^r(G_v \cap G_w, L_w^\times) \\ \beta &\longmapsto \Big((\pi_w \circ \iota_v^*)\beta\Big)_{v\in S(G), w\in S(G_v)} \end{aligned}$$

where ι_v denotes the embedding $1\cdot\mathbb{Z} \subseteq Y_v \subseteq Y = \bigoplus_{v\in S(G)} Y_v$ and $\pi_w : I_{L,S} \twoheadrightarrow L_w^\times$ is the canonical projection.

To be precise, one has cochains $(\pi_w \circ \iota_v^*)\beta \in C^r\big(G, \mathrm{Hom}(\mathbb{Z}, L_w^\times)\big)$. The restriction to $G_v \cap G_w$ and the evaluation at $1 \in \mathbb{Z}$ provides the corresponding image in $\hat{H}^r(G_v \cap G_w, L_w^\times)$ by the proof of Proposition 4.1.

Remark 4.4. We use the isomorphism of Corollary 4.3 in degree $r = 2$ to characterize the semi-local fundamental class α_2 by invariants. Let $\mathrm{inv}(G_v \cap G_w, w)$ denote the invariant map $\hat{H}^2(G_v \cap G_w, L_w^\times) \xrightarrow{\simeq} \frac{1}{|G_v\cap G_w|}\mathbb{Z}/\mathbb{Z}$ then Definition 4.2 implies

$$\mathrm{inv}(G_v \cap G_w, w)\big((\pi_w \circ \iota_v^*)\alpha_2\big) = \begin{cases} \frac{1}{|G_v|} & \text{if } w = v, \\ 0 & \text{otherwise} \end{cases}$$

because each local fundamental class $u_{L_v|K_p} \in \hat{H}^2(G_v, L_v^\times) \to \hat{H}^2(G_v, I_{L,S})$ has values in $I_{L,S} \simeq \prod_{v\in S} L_v^\times$ which are trivial at all places $w \neq v$.

4.2 Computing semi-local fundamental classes

The semi-local fundamental class can be viewed as an element in one of the isomorphic groups

$$\hat{H}^2(G, \mathrm{Hom}(Y, I_{L,S})) \simeq \mathrm{Yext}^2_G(Y, I_{L,S}) \simeq \mathrm{Ext}^2_G(Y, I_{L,S}).$$

As introduced in the last chapter, we replace $I_{L,S}$ by the finitely generated and cohomologically isomorphic module $I^f_{L,S}$ for computational purposes. It was defined by

$$I^f_{L,S} = \prod_{v \in S_f(G)} \mathrm{ind}^G_{G_v} L_v^\times / \exp_v(\mathscr{L}_v) \times \prod_{v \in S_\infty(G)} \mathrm{ind}^G_{G_v} W_v$$

with appropriate lattices $\mathscr{L}_v$ from Lemma 2.1 and modules W_v from Proposition 3.3. In our applications we are interested in the semi-local fundamental class as an element of $\mathrm{Ext}^2_G\big(Y, I^f_{L,S}\big)$ and in the following we will show how it can be constructed.

From Definition 4.2 the semi-local fundamental class as a cocycle can be computed from the local fundamental classes by making the isomorphism

$$\prod_{v \in S(G)} \hat{H}^2\big(G_v, I^f_{L,S}\big) \xrightarrow{\simeq} \hat{H}^2\big(G, \mathrm{Hom}(Y, I^f_{L,S})\big)$$

explicit. If we consider the proof of Proposition 4.1 again, this isomorphism is given by inducing each class from $\hat{H}^2\big(G_v, I^f_{L,S}\big) \simeq \hat{H}^2\big(G_v, \mathrm{Hom}(\mathbb{Z}, I^f_{L,S})\big)$ to $\hat{H}^2\big(G, \mathrm{Hom}(Y_v, I^f_{L,S})\big)$ and combining those to a cocycle in $\hat{H}^2\big(G, \mathrm{Hom}(Y, I^f_{L,S})\big)$.

Since the construction of the semi-local fundamental class in $\mathrm{Ext}^2_G\big(Y, I^f_{L,S}\big)$ is partly based on the construction as a cocycle, we summarize it in the following algorithm.

Algorithm 4.5 (Semi-local fundamental class as cocycle).
Input: A finite Galois extension $L|K$ of number fields with group G and a finite set of places S satisfying conditions (S1)–(S4) on page 70.

Output: A cocycle in $Z^2\big(G, \mathrm{Hom}(Y, I^f_{L,S})\big)$ representing the semi-local fundamental class.

1 Compute the finitely generated modules L^f_v and $I^f_{L,S}$ as in Algorithm 3.9.

2 For every finite place $v \in S(G)$ compute a cocycle representing the local fundamental class in $Z^2\big(G_v, L^f_v\big)$ using Algorithm 2.18.

3 For infinite places $v \in S(G)$ which are ramified (i.e. $G_v = \{1, \sigma_v\}$), the cocycle given by $c(1,1) = c(\sigma_v, 1) = c(1, \sigma_v) = 1$ and $c(\sigma_v, \sigma_v) = -1$ represents the local fundamental class in $Z^2\big(G_v, L^f_v\big)$, see Remark 1.7. The non-ramified infinite places have trivial decomposition group G_v and in this case every cocycle represents the fundamental class.

4. Compute their images in $Z^2\big(G_v, I^f_{L,S}\big) \simeq Z^2\big(G_v, \mathrm{Hom}(\mathbb{Z}, I^f_{L,S})\big)$ and the induced cocycle in $Z^2\big(G, \mathrm{Hom}(Y_v, I^f_{L,S})\big)$.
5. Combine these cocycles to get an element in $\alpha_2 \in Z^2\big(G, \mathrm{Hom}(Y, I^f_{L,S})\big)$.

Return: The cocycle α_2.

To construct the semi-local fundamental class as extension from the cocycle we would have to apply the isomorphisms

$$\hat{H}^2\big(G, \mathrm{Hom}(Y, I^f_{L,S})\big) \xrightarrow{\simeq} \mathrm{Yext}^2_G\left(Y, I^f_{L,S}\right) \xrightarrow{\simeq} \mathrm{Ext}^2_G\big(Y, I^f_{L,S}\big).$$

But the explicit description of the first isomorphism using the *splitting module* from [NSW00, Chp. III, § 1] (compare Proposition 1.29) is only applicable to extensions with $\mathbb{Z}$ in the first variable. Moreover, the second isomorphism is obtained by choosing a projective resolution of Y and solving a system of linear equations which, in this case, quickly becomes very large. Only the isomorphism $\mathrm{Ext}^2_G\big(Y, I^f_{L,S}\big) \xrightarrow{\simeq} \mathrm{Yext}^2_G\left(Y, I^f_{L,S}\right)$ is known to be given by constructing the push-out sequence (see Proposition 1.26).

Instead, we can use the isomorphisms

$$\hat{H}^2\big(G_v, I^f_{L,S}\big) \simeq \mathrm{Yext}^2_{G_v}\left(\mathbb{Z}, I^f_{L,S}\right) \simeq \mathrm{Ext}^2_{G_v}\left(\mathbb{Z}, I^f_{L,S}\right) \tag{4.1}$$

between the local cohomology groups and their corresponding extension groups. They can be performed explicitly as described in Section 1.3.2. Moreover, the isomorphism

$$\prod_{v \in S(G)} \mathrm{Ext}^2_{G_v}\big(\mathbb{Z}, I^f_{L,S}\big) \xrightarrow{\simeq} \mathrm{Ext}^2_G\big(Y, I^f_{L,S}\big) \tag{4.2}$$

is again given by induction and summation over all $v \in S(G)$ (see Proposition 1.26). To perform this isomorphism explicitly we fix the following projective resolutions.

For every $v \in S(G)$ we consider the resolution

$$\mathbb{Z}[G_v]^{r_v} \longrightarrow \mathbb{Z}[G_v] \xrightarrow{\mathrm{aug}} \mathbb{Z} \longrightarrow 0$$

where $r_v \in \mathbb{Z}$ is the number of generators $g_1, \ldots, g_{r_v}$ of G_v and $\mathbb{Z}[G_v]^{r_v} \to \mathbb{Z}[G_v]$ is given by mapping the i-th component $a_i \in \mathbb{Z}[G_v]$ to $a_i(g_i - 1)$. By inducing these modules to G and summing over all $v \in S(G)$ we get a projective resolution of Y_S. If Σ_v denotes the kernel of $\mathbb{Z}[G_v]^{r_v} \to \mathbb{Z}[G_v]$, we therefore have extensions

$$0 \longrightarrow \Sigma_v \xrightarrow{\iota_v} \mathbb{Z}[G_v]^{r_v} \longrightarrow \mathbb{Z}[G_v] \longrightarrow \mathbb{Z} \longrightarrow 0$$

and

$$\begin{array}{ccccccccc} 0 \longrightarrow & \bigoplus_v \mathrm{ind}^G_{G_v} \Sigma_v & \xrightarrow{\iota} & \bigoplus_v \mathrm{ind}^G_{G_v} \mathbb{Z}[G]^{r_v} & \longrightarrow & \bigoplus_v \mathrm{ind}^G_{G_v} \mathbb{Z}[G] & \longrightarrow & \bigoplus_v \mathrm{ind}^G_{G_v} \mathbb{Z} & \longrightarrow 0 \\ & \| & & \| & & \| & & \| & \\ & \Sigma_2 & & G^0 & & G^1 & & Y_S & \end{array}$$

which can be used to describe the following extension groups:

$$\begin{aligned} \operatorname{Ext}^2_{G_v}\big(\mathbb{Z}, I^f_{L,S}\big) &= \operatorname{Hom}_{G_v}\big(\Sigma_v, I^f_{L,S}\big)/\iota_v^* \operatorname{Hom}_{G_v}\big(\mathbb{Z}[G_v]^{r_v}, I^f_{L,S}\big) \\ \text{and} \quad \operatorname{Ext}^2_G\big(Y, I^f_{L,S}\big) &= \operatorname{Hom}_G\big(\Sigma_2, I^f_{L,S}\big)/\iota^* \operatorname{Hom}_G\big(G^0, I^f_{L,S}\big). \end{aligned}$$

Then the isomorphism (4.2) is explicitly induced by

$$\prod_{v \in S(G)} \operatorname{Hom}_{G_v}\big(\Sigma_v, I^f_{L,S}\big) \longrightarrow \operatorname{Hom}_G\big(\Sigma_2, I^f_{L,S}\big)$$

using induction and summation.

Combining isomorphisms (4.1) and (4.2) we can therefore construct the semi-local fundamental class as extension in $\operatorname{Ext}^2_G\big(Y, I^f_{L,S}\big)$. This is summarized in the following algorithm.

Algorithm 4.6 (Semi-local fundamental class as extension).
Input: A finite Galois extension $L|K$ of number fields with group G and a finite set of places S satisfying conditions (S1)–(S4) on page 70.

Output: The semi-local fundamental class in $\operatorname{Ext}^2_G\big(Y, I^f_{L,S}\big)$, represented by an element in $\operatorname{Hom}_G\big(\Sigma_2, I^f_{L,S}\big)$.

1. For every $v \in S$ let L_v^f be a finitely generated module which is cohomologically isomorphic to $L_v^\times$. Then compute local fundamental classes $u_{L_v|K_p} \in \hat{H}^2\big(G_v, L_v^f\big)$ as in steps 1–3 of Algorithm 4.5 and their image in $\hat{H}^2\big(G_v, I^f_{L,S}\big)$.
2. Apply Corollary 1.30 to construct maps $f_v \in \operatorname{Hom}_{G_v}\big(\Sigma_v, I^f_{L,S}\big)$ which correspond to the local fundamental classes by the isomorphism $\hat{H}^2\big(G_v, I^f_{L,S}\big) \simeq \operatorname{Ext}^2_{G_v}\big(\mathbb{Z}, I^f_{L,S}\big)$.
3. Induce the homomorphisms f_v from $\operatorname{Hom}_{G_v}\big(\Sigma_v, I^f_{L,S}\big)$ to $\operatorname{Hom}_G\big(\operatorname{ind}^G_{G_v}\Sigma_v, I^f_{L,S}\big)$ and take a sum over all $v \in S(G)$ to get an element $\bigoplus_v \operatorname{ind}^G_{G_v} f_v$ in the group $\operatorname{Hom}_G\big(\Sigma_2, I^f_{L,S}\big)$ which represents the semi-local fundamental class in $\operatorname{Ext}^2_G\big(Y, I^f_{L,S}\big)$.

Return: $\bigoplus_v \operatorname{ind}^G_{G_v} f_v \in \operatorname{Hom}_G\big(\Sigma_2, I^f_{L,S}\big)$.

Remark 4.7. If $\operatorname{Ext}^2_G\big(Y, I^f_{L,S}\big)$ is represented by another resolution, we can still compute a representative of the semi-local fundamental class with the above algorithm. Let

$$0 \longrightarrow \bar{\Sigma}_2 \longrightarrow \bar{G}^0 \longrightarrow \bar{G}^1 \longrightarrow Y \longrightarrow 0$$

be an exact sequence with $\bar{G}^0$ and $\bar{G}^1$ projective such that $\operatorname{Ext}^2_G\big(Y, I^f_{L,S}\big) \simeq \operatorname{Hom}_G\big(\bar{\Sigma}_2, I^f_{L,S}\big)/\iota^* \operatorname{Hom}_G\big(\bar{G}^0, I^f_{L,S}\big)$. Then by [Wei94, Thm. 2.2.6] there exists a commutative diagram

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \bar{\Sigma}_2 & \longrightarrow & \bar{G}^0 & \longrightarrow & \bar{G}^1 & \longrightarrow & Y & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & \Sigma_2 & \longrightarrow & G^0 & \longrightarrow & G^1 & \longrightarrow & Y & \longrightarrow & 0 \end{array}$$

whose vertical maps are constructed by lifting the maps $\bar{G}^1 \to Y$ and $\bar{G}^0 \to \bar{G}^1 \to \operatorname{im}(G^0 \to G^1)$ as in the following diagrams:

$$\begin{tikzcd} & \bar{G}^1 \arrow[d] \arrow[dl, dashed] \\ G^1 \arrow[r, two heads] & Y \end{tikzcd} \qquad \begin{tikzcd} & \bar{G}^0 \arrow[d] \arrow[dl, dashed] \\ G^0 \arrow[r, two heads] & \operatorname{im}(G^0 \to G^1) \end{tikzcd}$$

In particular, these lifts can easily be computed if $\bar{G}^0$ and $\bar{G}^1$ are free G-modules, which will be the case in our applications. Then every homomorphism $\operatorname{Hom}_G\big(\Sigma_2, I^f_{L,S}\big)$ can be lifted to $\operatorname{Hom}_G\big(\bar{\Sigma}_2, I^f_{L,S}\big)$ and we can compute a representative of the semi-local fundamental class in $\operatorname{Hom}_G\big(\bar{\Sigma}_2, I^f_{L,S}\big)$.

Recall that one can construct the semi-local fundamental class as Yoneda extension in $\operatorname{Yext}^2_G\big(Y, I^f_{L,S}\big)$ from the above algorithm by computing the pushout sequence. In conclusion, there are explicit algorithms to compute the semi-local fundamental class as cocycle, as extension or as Yoneda extension. In the construction of Tate's canonical class below, we will use the semi-local fundamental class as an element of $\operatorname{Ext}^2_G\big(Y, I^f_{L,S}\big)$.

4.3 Definition of Tate's canonical class

We continue to consider $Y = \bigoplus_{v \in S(G)} \operatorname{ind}^G_{G_v} \mathbb{Z}$ and define X to be the kernel of the augmentation map $\operatorname{aug} : Y \to \mathbb{Z}$. We study the two sequences of G-modules

$$(X) \qquad 0 \longrightarrow X \longrightarrow Y \xrightarrow{\operatorname{aug}} \mathbb{Z} \longrightarrow 0$$

and

$$(U) \qquad 0 \longrightarrow U_{L,S} \longrightarrow I_{L,S} \longrightarrow C_{L,S} \longrightarrow 0.$$

Remember that by the conditions (S1)–(S4) on S, the S-idèle class group $C_{L,S}$ is cohomologically isomorphic to the idèle class group C_L by Lemma 3.1.

We define $\operatorname{Hom}((X),(U))$ as the group of maps of complexes between (X) and (U), i.e. compatible homomorphisms f_1, f_2, f_3 which form a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ & & \big\downarrow f_3 & & \big\downarrow f_2 & & \big\downarrow f_1 & & \\ 0 & \longrightarrow & U_{L,S} & \longrightarrow & I_{L,S} & \longrightarrow & C_{L,S} & \longrightarrow & 0 \end{array} \tag{4.3}$$

Note that in such a commutative diagram f_1 and f_2 determine the homomorphism f_3 uniquely; and similarly f_2 and f_3 determine f_1. For $(f_3, f_2, f_1) = f \in \mathrm{Hom}((X), (U))$ we also denote the projections f_i by $\pi_i(f)$. The group $\mathrm{Hom}((X), (U))$ is a G-module by the action $\sigma(f_3, f_2, f_1) = (\sigma f_3, \sigma f_2, \sigma f_1)$ where σf_i is defined by $(\sigma f_i)(x) = \sigma f_i(\sigma^{-1} x)$. The triple $(\sigma f_3, \sigma f_2, \sigma f_1)$ will again form a commutative diagram since each of the horizontal homomorphisms in (4.3) commute with the G-action.

Theorem 4.8 (Tate). *There is a unique class $\alpha \in \hat{H}^2\big(G, \mathrm{Hom}((X), (U))\big)$ whose projections $\alpha_1 \in \hat{H}^2\big(G, \mathrm{Hom}(\mathbb{Z}, C_{L,S})\big)$ and $\alpha_2 \in \hat{H}^2\big(G, \mathrm{Hom}(Y, I_{L,S})\big)$ are the global and semi-local fundamental class.*

Proof. [Tat66, p. 716]. □

Definition 4.9 (Tate's canonical class). *The projection $\alpha_3 = \pi_3(\alpha)$ of the unique class $\alpha \in \hat{H}^2\big(G, \mathrm{Hom}((X), (U))\big)$ onto the group $\hat{H}^2\big(G, \mathrm{Hom}(X, U_{L,S})\big)$ is called* Tate's canonical class.

Remark 4.10. One important property of Tate's canonical class as extension in $\mathrm{Ext}^2_G(X, U_{L,S}) \simeq \hat{H}^2(G, \mathrm{Hom}(X, U_{L,S}))$ is that its pushout along $U_{L,S} \to I_{L,S}$ in $\mathrm{Ext}^2_G(X_S, I_{L,S})$ is the same class as the pullback of the semi-local fundamental class along $X_S \to Y_S$ in $\mathrm{Ext}^2_G(X_S, I_{L,S})$. This follows directly from the definition of $\mathrm{Hom}((X), (U))$.

4.4 Computing Tate's canonical class

For the computation of Tate's canonical class we consider the complex

$$(U^f) \qquad 0 \longrightarrow U_{L,S} \longrightarrow I^f_{L,S} \longrightarrow C^f_{L,S} \longrightarrow 0$$

with finitely generated modules $I^f_{L,S}$ and $C^f_{L,S}$ from Section 3.1 and S-units $U_{L,S}$. These modules are finitely generated and cohomologically isomorphic to the S-idèle group $I_{L,S} = \prod_{v \in S} L_v^\times$ and the idèle class group C_L, respectively, and therefore the complex (U^f) is finitely generated cohomologically isomorphic (in every degree) to (U).

In the following we will construct Tate's canonical class as an extension in $\mathrm{Ext}^2_G(X, U_{L,S})$. Again, we will describe this extension group by a projective resolution of X. Since we will construct Tate's class from the semi-local and global fundamental class represented as extensions, we also need projective resolutions of Y and $\mathbb{Z}$. For computational purposes, we require those three projective resolutions to be compatible, i.e. we need a projective resolution (of degree two) of the complex (X).

Such a resolution of (X) can be constructed using the *Horseshoe lemma*, see Lemma 1.32. Explicitly, if $P_X^\bullet$ and $P_\mathbb{Z}^\bullet$ are projective resolutions of X and $\mathbb{Z}$, then the sequence $P_Y^\bullet$ given by $P_Y^i = P_X^i \oplus P_\mathbb{Z}^i$ is a projective resolution of Y and there exist chain maps $P_X^\bullet \to P_Y^\bullet \to P_\mathbb{Z}^\bullet$ which induce short exact sequences in every degree. In our case we can actually choose $P_X^\bullet$ and $P_\mathbb{Z}^\bullet$ to be free resolutions and these chain maps can be constructed easily.

We can therefore construct a commutative exact diagram

$$\begin{tikzcd}
0 \arrow[r] & \Sigma_3 \arrow[r, "\iota_3"] \arrow[d, hook] & F^0 \arrow[r] \arrow[d, hook] & F^1 \arrow[r] \arrow[d, hook] & X \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & \Sigma_2 \arrow[r, "\iota_2"] \arrow[d, two heads] & G^0 \arrow[r] \arrow[d, two heads] & G^1 \arrow[r] \arrow[d, two heads] & Y \arrow[r] \arrow[d, two heads] & 0 \\
0 \arrow[r] & \Sigma_1 \arrow[r, "\iota_1"] & H^0 \arrow[r] & H^1 \arrow[r] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd} \tag{4.4}$$

with G-modules Σ_i, F^i, G^i and H^i. If we denote the vertical complexes by (Σ), (P^0), (P^1) and (X), respectively, we have an exact sequence

$$0 \longrightarrow (\Sigma) \longrightarrow (P^0) \longrightarrow (P^1) \longrightarrow (X) \longrightarrow 0$$

of complexes.

We continue the construction of Tate's canonical class by using the following representations

$$\begin{aligned}
\operatorname{Ext}^2_G(X, U_{L,S}) &= \operatorname{Hom}_G(\Sigma_3, U_{L,S}) / \iota_3^* \operatorname{Hom}_G(F^0, U_{L,S}) \\
\operatorname{Ext}^2_G\big(Y, I^f_{L,S}\big) &= \operatorname{Hom}_G\left(\Sigma_2, I^f_{L,S}\right) / \iota_2^* \operatorname{Hom}_G\left(G^0, I^f_{L,S}\right) \\
\text{and}\quad \operatorname{Ext}^2_G\big(\mathbb{Z}, C^f_{L,S}\big) &= \operatorname{Hom}_G\left(\Sigma_1, C^f_{L,S}\right) / \iota_1^* \operatorname{Hom}_G\left(H^0, C^f_{L,S}\right).
\end{aligned} \tag{4.5}$$

Moreover, we get the identification

$$\operatorname{Ext}^2_G\big((X), (U^f)\big) = \operatorname{Hom}_G\big((\Sigma), (U^f)\big) / \iota^* \operatorname{Hom}_G\big((P^0), (U^f)\big). \tag{4.6}$$

Hence, the canonical class $(\alpha) \in \hat{H}^2\big(G, \operatorname{Hom}((X), (U^f))\big) \simeq \operatorname{Ext}^2\big((X), (U^f)\big)$ is represented by an tuple $(\varphi_3, \varphi_2, \varphi_1) \in \operatorname{Hom}\big((\Sigma), (U^f)\big)$ of homomorphisms forming an exact diagram

$$\begin{tikzcd}
0 \arrow[r] & \Sigma_3 \arrow[r] \arrow[d, "\varphi_3"] & \Sigma_2 \arrow[r, "g"] \arrow[d, "\varphi_2"] & \Sigma_1 \arrow[r] \arrow[d, "\varphi_1"] & 0 \\
0 \arrow[r] & U_{L,S} \arrow[r] & I^f_{L,S} \arrow[r, "h"] & C^f_{L,S} \arrow[r] & 0
\end{tikzcd} \tag{4.7}$$

and where φ_1 and φ_2 represent the global and semi-local fundamental class respectively.

Now let H^i be such that the bottom row of (4.4) is our standard projective resolution of $\mathbb{Z}$ as in (1.16):

$$\mathbb{Z}[G]^r \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$$

with G being generated by r elements. Then we can use Algorithm 3.13 and Corollary 1.30 to compute a representative $\varphi_1 \in \mathrm{Hom}_G\left(\Sigma_1, C^f_{L,S}\right)$ of the global fundamental class. A representative $\varphi_2 \in \mathrm{Hom}_G\left(\Sigma_2, I^f_{L,S}\right)$ of the semi-local fundamental class can be found by combining Algorithm 4.6 (which uses another projective resolution of Y) with [Wei94, Thm. 2.2.6] as discussed in Remark 4.7.

The maps φ_1 and φ_2, however, do not necessarily make the right-hand square of (4.7) commute. But by the uniqueness of the canonical class α in Theorem 4.8 there must exist homomorphisms $\lambda \in \mathrm{Hom}_G\left(G^0, I^f_{L,S}\right)$ and $\mu \in \mathrm{Hom}_G\left(H^0, C^f_{L,S}\right)$ such that $h \circ (\varphi_2 + \lambda \circ \iota_2) = (\varphi_1 + \mu \circ \iota_1) \circ g$ holds. The following lemma shows that such a map λ still exists if require $\mu = 0$.

Lemma 4.11. *If $h \circ (\varphi_2 + \lambda \circ \iota_2) = (\varphi_1 + \mu \circ \iota_1) \circ g$ for $\lambda \in \mathrm{Hom}_G\left(G^0, I^f_{L,S}\right)$ and $\mu \in \mathrm{Hom}_G\left(H^0, C^f_{L,S}\right)$, then there exists $\lambda' \in \mathrm{Hom}_G\left(G^0, I^f_{L,S}\right)$ such that $h \circ (\varphi_2 + \lambda' \circ \iota_2) = \varphi_1 \circ g$.*

Proof. Consider the following diagram

$$\begin{tikzcd}
& \Sigma_2 \arrow[r, "\iota_2"] \arrow[dl, "\varphi_2"'] \arrow[dd, dashed, "g"] & G^0 \arrow[dd, "g_0"] \arrow[dll, dashed, "\lambda"] \\
I^f_{L,S} \arrow[dd, "h"] & & \\
& \Sigma_2 \arrow[r, "\iota_1"] \arrow[dl, "\varphi_1"'] & H^0 \arrow[dll, dashed, "\mu"] \\
C^f_{L,S} & &
\end{tikzcd}$$

in which both squares commute (but not necessarily the triangles). Then $\iota_1 \circ g = g_0 \circ \iota_2$ holds and since G^0 is projective there exists $\lambda'' \in \mathrm{Hom}_G\left(G^0, I^f_{L,S}\right)$ such that $h \circ \lambda'' = \mu \circ g_0 \in \mathrm{Hom}_G\left(G^0, C^f_{L,S}\right)$. Let $\lambda' = \lambda - \lambda'' \in \mathrm{Hom}_G\left(G^0, C^f_{L,S}\right)$, then

$$\begin{aligned} h \circ (\varphi_2 + \lambda' \circ \iota_2) &= h \circ (\varphi_2 + \lambda \circ \iota_2) - h \circ \lambda'' \circ \iota_2 = (\varphi_1 + \mu \circ \iota_1) \circ g - \mu \circ g_0 \circ \iota_2 \\ &= (\varphi_1 + \mu \circ \iota_1) \circ g - \mu \circ \iota_1 \circ g = \varphi_1 \circ g \end{aligned}$$

which completes the proof. □

From the algorithms constructing the global and semi-local fundamental class we can therefore find homomorphisms φ_1 and φ_2 which make diagram (4.7) commute. The restriction of φ_2 to Σ_3 will then always be a homomorphism in $\mathrm{Hom}_G(\Sigma_3, U_{L,S})$ which represents Tate's canonical class.

The construction of Tate's canonical class which we developed above is summarized in the following algorithm.

Algorithm 4.12 (Tate's canonical class as extension).

Input: A finite Galois extension $L|K$ of number fields with group G and a finite set of places S satisfying conditions (S1)–(S4) on page 70.

Output: Tate's canonical class in $\mathrm{Ext}^2_G(X, U_{L,S})$, represented by an element in $\mathrm{Hom}_G(\Sigma_3, U_{L,S})$.

1. Construct diagram (4.4) and represent extension groups as in (4.5).
2. Compute a representative $\varphi_1 \in \mathrm{Hom}_G\big(\Sigma_1, C^f_{L,S}\big)$ of the global fundamental class using Algorithm 3.13 combined with Corollary 1.30.
3. Compute a representative $\varphi_2 \in \mathrm{Hom}_G\big(\Sigma_2, I^f_{L,S}\big)$ of the semi-local fundamental class using Algorithm 4.6 combined with Remark 4.7.
4. Use linear algebra to construct $\lambda \in \mathrm{Hom}_G\big(G^0, I^f_{L,S}\big)$ such that $\varphi_2' = \varphi_2 + \lambda \circ \iota_2$ satisfies $h \circ \varphi_2' = \varphi_1 \circ g$.
5. Then the restriction φ_1 of φ_2' to Σ_3 is an element in $\mathrm{Hom}_G(\Sigma_3, U_{L,S})$.

Return: $\varphi_1 \in \mathrm{Hom}_G(\Sigma_3, U_{L,S})$.

Remark 4.13. Let $(\varphi_3, \varphi_2, \varphi_1) \in \mathrm{Hom}\big((\Sigma), (U^f)\big)$ be a tuple of homomorphisms representing the canonical class in $\hat{H}^2\big(G, \mathrm{Hom}((X), (U^f))\big)$. By definition of $\mathrm{Hom}\big((\Sigma), (U^f)\big)$ these homomorphisms make diagram (4.7) commute. By simultaneously constructing pushout sequences using the rows of diagram (4.4) and the homomorphisms φ_i one can then construct a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & U_{L,S} \arrow[r] \arrow[d, hook] & \bar{F}^0 \arrow[r] \arrow[d, hook] & F^1 \arrow[r] \arrow[d, hook] & X \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & I^f_{L,S} \arrow[r] \arrow[d, two heads] & \bar{G}^0 \arrow[r] \arrow[d, two heads] & G^1 \arrow[r] \arrow[d, two heads] & Y \arrow[r] \arrow[d, two heads] & 0 \\
0 \arrow[r] & C^f_{L,S} \arrow[r] & \bar{H}^0 \arrow[r] & H^1 \arrow[r] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd} \tag{4.8}$$

in which the rows represent Tate's canonical class, the semi-local fundamental class and the global fundamental class as Yoneda extensions.

This is exactly the diagram from Chinburg [Chi85, Chp. III, (3.1)]. Using the algorithms presented in the preceding chapters, this diagram can now be constructed explicitly.

4.5 Special case: undecomposed prime

In Section 3.2.1 we have seen that the computation of the global fundamental class is much simpler if there exists an undecomposed prime. Due to the relations among the canonical classes, it is not amazing that this also applies for the construction of Tate's canonical class. Chinburg studied this case in detail in [Chi89] and characterized the image of Tate's canonical class in $\mathrm{Ext}^2_G(X, I_{L,S})$ using local invariants as follows.

Let $L|K$ be a finite Galois extension of number fields with group G and S a set of places satisfying (S1)–(S4). Furthermore, assume that $v_0 \in S$ is undecomposed in $L|K$ and p_0 is the place of K below v_0:

$$G\left(\begin{array}{c} L \\ | \\ K \end{array}\right. \qquad \begin{array}{c} v_0 \\ | \\ p_0 \end{array} \qquad\qquad \left.\begin{array}{c} L_{v_0} \\ | \\ K_{p_0} \end{array}\right)G_{v_0} = G$$

The G-orbit of v_0 in S just contains v_0. Therefore, the set $S' = S \setminus \{v_0\}$ is also G-stable and from every set $S(G)$ of G-representatives in S one gets a set $S(G) \setminus \{v_0\}$ of G-representatives in S'. Furthermore, there is an isomorphism

$$\phi : \bigoplus_{v \in S'(G)} Y_v \xrightarrow{\simeq} X \subseteq Y = \bigoplus_{v \in S(G)} Y_v \tag{4.9}$$

of G-modules which sends $(y_v)_{v \in S'(G)}$ to $(y_v)_{v \in S(G)}$ with $y_{v_0} = -\sum_{v \in S'(G)} \mathrm{aug}(y_v)$. To avoid confusion, we further write $Y_S = Y = \bigoplus_{v \in S(G)} Y_v$ and $Y_{S'} = \bigoplus_{v \in S'(G)} Y_v$. By Proposition 4.1 the above isomorphism implies

$$\mathrm{Ext}^r_G(X, M) \simeq \prod_{v \in S'(G)} \mathrm{Ext}^r_G(Y_v, M) \simeq \prod_{v \in S'(G)} \hat{H}^r(G_v, M) \tag{4.10}$$

for any G-module M. In particular, for $r = 2$ and $M = I_{L,S}$ we obtain

$$\mathrm{Ext}^2_G(X, I_{L,S}) \simeq \prod_{v \in S'(G)} \hat{H}^2(G_v, I_{L,S}) \simeq \prod_{v \in S'(G)} \prod_{w \in S(G_v)} \hat{H}^2(G_w \cap G_v, L_w^\times). \tag{4.11}$$

Note that v just runs through $S'(G)$ due to the isomorphism ϕ, but w still runs through $S(G)$ since we consider $I_{L,S}$ (and not $I_{L,S'}$). Also remember that this isomorphism is explicitly described by

$$\begin{array}{ccc} \hat{H}^2\big(G, \mathrm{Hom}(X, I_{L,S})\big) & \simeq & \displaystyle\prod_{v \in S'(G)} \prod_{w \in S(G_v)} \hat{H}^2(G_w \cap G_v, L_w^\times) \\ \beta & \mapsto & \Big((\pi_w \circ \iota_v^*)\beta\Big)_{v \in S'(G), w \in S(G_v)} \end{array}$$

with embeddings $\iota_v : Y_v \hookrightarrow X$ via ϕ and projections $\pi_w : I_{L,S} \twoheadrightarrow L_w^\times$ as in Corollary 4.3.

Then the image $\beta \in \hat{H}^2\big(G, \mathrm{Hom}(X, I_{L,S})\big)$ of the semi-local fundamental class $\alpha_2 \in \hat{H}^2\big(G, \mathrm{Hom}(Y_S, I_{L,S})\big)$ through the homomorphism

$$\hat{H}^2\big(G, \mathrm{Hom}(Y_S, I_{L,S})\big) \to \hat{H}^2\big(G, \mathrm{Hom}(X, I_{L,S})\big)$$

can be characterized using local invariants as follows. Recall that this homomorphism is simply given by the pullback along $X \to Y_S$ and denote the invariant map on $\hat{H}^2(G_w \cap G_v, L_w^\times)$ by $\mathrm{inv}(G_v \cap G_w, w)$.

Proposition 4.14. *Let $\phi : Y_{S'} \xrightarrow{\simeq} X$ be the isomorphism (4.9) above. Then the image $\beta \in \hat{H}^2\big(G, \mathrm{Hom}(X, I_{L,S})\big)$ of the semi-local fundamental class α_2 is characterized by*

$$\mathrm{inv}(G_v \cap G_w, w)\big((\pi_w \circ \iota_v^*)\beta\big) = \begin{cases} \frac{1}{|G_v|} & \text{if } w = v, \\ -\frac{1}{|G_v|} & \text{if } w = v_0, \text{ and} \\ 0 & \text{otherwise.} \end{cases} \tag{4.12}$$

These invariants are exactly those stated by Chinburg in [Chi89, Chp. III, § 2, p. 24], for which we can now give a complete proof.

Proof. Consider the following homomorphisms

$$\begin{array}{ccc} \hat{H}^2\big(G, \mathrm{Hom}(Y_S, I_{L,S})\big) & \simeq & \prod\limits_{v \in S(G)} \prod\limits_{w \in S(G_v)} \hat{H}^2(G_w \cap G_v, L_w^\times) \\ \downarrow & & \\ \hat{H}^2\big(G, \mathrm{Hom}(X, I_{L,S})\big) & & \\ \simeq \downarrow \phi & & \\ \hat{H}^2\big(G, \mathrm{Hom}(Y_{S'}, I_{L,S})\big) & \simeq & \prod\limits_{v \in S'(G)} \prod\limits_{w \in S(G_v)} \hat{H}^2(G_w \cap G_v, L_w^\times) \end{array}$$

in which the upper vertical map is given by the pullback along $X \to Y_S$ and the lower vertical map is induced by the isomorphism ϕ. The horizontal isomorphisms are those from Proposition 4.1 which were given in its proof as follows: if γ is a cocycle in $\hat{H}^2\big(G, \mathrm{Hom}(Y_S, I_{L,S})\big)$, then its image at $v \in S(G)$, $w \in S(G_v)$ is the cocycle

$$\sigma, \tau \longmapsto \pi_w\big(\gamma(\sigma, \tau)(1_v)\big)$$

where $\sigma, \tau \in G_v \cap G_w$, π_w denotes the projection $I_{L,S} \twoheadrightarrow L_w^\times$ and 1_v denotes the element $1 \in 1 \cdot \mathbb{Z} \subseteq Y_v \subseteq Y_S$. The bottom isomorphism is analog, with v being a place of $S'(G)$.

Let α_2 denote the semi-local fundamental class. It has invariant $\frac{1}{|G_v|}$ for $v = w$ and 0 otherwise as described in Remark 4.4. Its image $\beta \in \hat{H}^2\big(G, \mathrm{Hom}(Y_{S'}, I_{L,S})\big)$ is the cocycle obtained by composition with $\phi : Y_{S'} \to X$ and $j : X \hookrightarrow Y_S$:

$$\beta(\sigma, \tau) = \alpha_2(\sigma, \tau) \circ j \circ \phi \in \mathrm{Hom}(Y_{S'}, I_{L,S}) \quad \text{for all } \sigma, \tau \in G.$$

To compute its invariant at $v \in S'(G)$, $w \in S(G_v)$ we have to consider the cocycle

$$\sigma, \tau \longmapsto \pi_w\big(\beta(\sigma,\tau)(1_v)\big) \quad \sigma, \tau \in G_v \cap G_w$$

and by $\phi(1_v) = 1_v - 1_{v_0}$ this is

$$\sigma, \tau \longmapsto \pi_w\big(\alpha_2(\sigma,\tau)(1_v)\big) - \pi_w\big(\alpha_2(\sigma,\tau)(1_{v_0})\big).$$

By the definition of the semi-local fundamental class α_2 the left-hand term vanishes if $w \neq v$ and the right-hand term similarly if $w \neq v_0$. For $w = v$ the cocycle β therefore has the same invariant as α_2 and for $w = v_0$ we get the inverse of the local fundamental class in $\hat{H}^2(G_{v_0}, L_{v_0}^\times)$ restricted to $G_v \cap G_{v_0} = G_v$. This restriction is actually the inflation map which maps the local fundamental class of $L_{v_0}|K_{p_0}$ to the one of $L_{v_0}|L_{v_0}^{G_v}$. Hence, the invariant at $w = v_0$ is $-\frac{1}{|G_v|}$. This proves that β has the invariants (4.12). □

By the above proposition, the pullback of the semi-local fundamental class in $\mathrm{Ext}^2_G(X, I_{L,S})$ can be characterized using local invariants. From Remark 4.10 we know that this element coincides with the pushout of Tate's canonical class through the homomorphism

$$\mathrm{Ext}^2_G(X, U_{L,S}) \longrightarrow \mathrm{Ext}^2_G(X, I_{L,S}). \tag{4.13}$$

Applying (4.10) for $r = 1$ and $M = C_{L,S}$, there is an isomorphism

$$\mathrm{Ext}^1_G(X, C_{L,S}) \simeq \prod_{v \in S'(G)} \hat{H}^1(G_v, C_{L,S})$$

and this group is trivial since the first cohomology group of the idèle class group is always trivial. Therefore, the homomorphism (4.13) is injective and the invariants from Proposition 4.14 also characterize Tate's canonical class. In this case it is therefore possible to construct the corresponding *Tate sequence* in $\mathrm{Ext}^2_G(X, U_{L,S})$ without computing the global fundamental class.

This construction of Tate's canonical class using Chinburg's conditions has been turned into an algorithm by Janssen in [Jan10]. There the conditions (4.12) are explicitly reformulated as linear equations. Although this approach is very explicit, these equations contain interactions between different places in S and they become very complicated.

In comparison to the general construction, the injectivity of (4.13) implies the following for diagram (4.7):

$$\begin{tikzcd}
0 \arrow[r] & \Sigma_3 \arrow[r] \arrow[d, "\varphi_3"] & \Sigma_2 \arrow[r] \arrow[d, "\varphi_2"] & \Sigma_1 \arrow[r] \arrow[d, "\varphi_1"] & 0 \\
0 \arrow[r] & U_{L,S} \arrow[r] & I^f_{L,S} \arrow[r] & C^f_{L,S} \arrow[r] & 0
\end{tikzcd}$$

Whenever the right-hand square commutes with φ_2 representing the semi-local fundamental class (without conditions on φ_1), its restriction to Σ_3 will represent Tate's canonical class. Hence, the general construction will also be independent of the global fundamental class.

Note that the characterization by invariants depends critically on the description of X using isomorphism (4.9). In the general case such a representation will therefore not be possible and the construction of Tate's class will depend on the global fundamental class as in Algorithm 4.12.

Tamagawa Number Conjectures

Overview

In the following chapters, we will consider the equivariant Tamagawa number conjectures for Galois extensions of number fields as formulated in [BlB03, Bre04b, BrB07, BF01]. The three fundamental classes, which were studied in detail in the previous chapters, will play an important role in those conjectures.

The equivariant Tamagawa number conjectures for number fields are known to generalize the conjectures of Chinburg formulated in [Chi85]. In the following an overview of Chinburg's conjectures and their refinements is given.

Let $L|K$ be a fixed Galois extension of number fields with group G. In the previous chapters we obtained an exact commutative diagram of finitely generated $\mathbb{Z}[G]$-modules representing relations between the three fundamental classes (see Remark 4.13):

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & U_{L,S} & \longrightarrow & A_3 & \longrightarrow & B_3 & \longrightarrow & X & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I_{L,S}^f & \longrightarrow & A_2 & \longrightarrow & B_2 & \longrightarrow & Y & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & C_{L,S}^f & \longrightarrow & A_1 & \longrightarrow & B_1 & \longrightarrow & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

For projective modules A one has a rank map $\mathrm{rank}(A) = \mathrm{rank}_{\mathbb{Q}[G]}(A \otimes_{\mathbb{Z}[G]} \mathbb{Q}[G])$ and it can be extended to cohomologically trivial modules using Schanuel's lemma. This provides integers $r_i = \mathrm{rank}(A_i) - \mathrm{rank}(B_i)$ and in [Chi85] Chinburg defined the elements $\Omega_i(L|K) = (A_i) - (B_i) - r_i(\mathbb{Z}[G]) \in K_0(\mathbb{Z}[G])$, one for each of the rows in the diagram.[2] From the exactness of the middle two columns one directly obtains the relation

$$\Omega_2(L|K) = \Omega_1(L|K) + \Omega_3(L|K)$$

in $K_0(\mathbb{Z}[G])$, cf. [Chi85, Eq. (3.2)]. Chinburg then formulated the following conjectures [Chi85, Question 3.2, Question 3.1, and Conj. 3.1]:

Ω_1-*conjecture:* $\Omega_1(L|K) = 0$,

Ω_2-*conjecture:* $\Omega_2(L|K) = W(L|K)$,

Ω_3-*conjecture:* $\Omega_3(L|K) = W(L|K)$.

[2] If $0 \to K \to P \to A \to 0$ is a projective resolution of a cohomologically trivial $\mathbb{Z}[G]$-module A, then A is represented by $(P) - (K)$ in $K_0(\mathbb{Z}[G])$.

Here, $W(L|K)$ denotes the *root number class* associated to *Artin root numbers* $W(\chi)$ as it is defined by Fröhlich in [Frö78], see also [Chi84, § 7] or [Chi89, Chp. I].

Chinburg's conjectures are known to generalize other conjectures. The second conjecture can be regarded as a generalization of *Fröhlich's conjecture* from [Frö83], which was proved by Taylor in [Tay81], to wildly ramified number field extensions. The other two conjectures refine the *class number formula.*

Chinburg also proved that the elements are in fact in the class group $Cl(\mathbb{Z}[G])$ which can be identified with the kernel $\ker\big(K_0(\mathbb{Z}[G]) \to K_0(\mathbb{R}[G])\big) = \operatorname{im}(\partial^0_{G,\mathbb{R}})$. It is therefore convenient to *lift these conjectures*, i.e. to formulate refined conjectures in the relative K-group $K_0(\mathbb{Z}[G], \mathbb{R})$ which imply Chinburg's conjectures through the map $\partial^0_{G,\mathbb{R}}$. This is done by the *equivariant Tamagawa number conjectures.*

The Tamagawa number conjectures relate leading coefficients $\zeta^*_{L|K,S}(s)$ of the equivariant Artin L-function $\Lambda_{L|K}(s)$ as defined in Section 1.5 to algebraic terms corresponding to the extension $L|K$. An overview of these conjectures for number fields is given in [BrB07, §§ 3–5] and a more general survey is provided in [Fla04]. The following summary should give a rough impression of what these conjecture look like.

Leading term at $s = 0$: This conjecture relates the value $\zeta^*_{L|K,S}(0)$ to an Euler characteristic constructed from Tate's canonical class (the upper row in the above diagram) and a canonical isomorphism between $X_\mathbb{R}$ and $\mathbb{R}[G]\otimes_{\mathbb{Z}[G]}U_{L,S}$ obtained from the regulator map $\operatorname{Reg}_S : \mathbb{R}[G] \otimes_{\mathbb{Z}[G]} U_{L,S} \xrightarrow{\simeq} \mathbb{R}[G] \otimes_{\mathbb{Z}[G]} X$, $u \mapsto (\log |u|_w)_{w\in S}$.

This construction results in an element in the relative K-group $K_0(\mathbb{Z}[G], \mathbb{R})$ which is often denoted by $T\Omega(L|K, 0)$. The map $\partial^0_{G,\mathbb{R}}$ maps $T\Omega(L|K, 0)$ to $\Omega_3(L|K) - W(L|K)$ and it is conjectured that $T\Omega(L|K, 0)$ is zero in $K_0(\mathbb{Z}[G], \mathbb{R})$, cf. [BrB07, Prop. 4.4 and Conj. 4.1].

An algorithm to verify this conjecture was discussed in detail by Janssen in [Jan10], and in special cases her algorithm also gives a proof.

Leading term at $s = 1$: Similarly, the value $\zeta^*_{L|K,S}(1)$ is conjecturally related to an Euler characteristic from the global fundamental class (the bottom row in the above diagram) and a canonical isomorphism obtained from the embedding maps $L \to L_w$ for all infinite places w of L.

The construction results in an element $T\Omega(L|K, 1) \in K_0(\mathbb{Z}[G], \mathbb{R})$ which is mapped to $\Omega_1(L|K)$ by $\partial^0_{G,\mathbb{R}}$ and it is also conjectured that this element is zero, cf. [BrB07, Prop. 3.6 and Conj. 3.3]. This conjecture will be studied in Chapter 6.

Compatibility conjecture: The leading terms $\zeta^*_{L|K,S}(0)$ and $\zeta^*_{L|K,S}(1)$ of Artin L-function used in the conjectures above are related by the functional equation, see Proposition 1.48 in Section 1.5. Moreover, the global fundamental class and Tate's canonical class are related by local fundamental classes (see Chapter 4).

Together this gives rise to a compatibility of the two conjectures, also called *epsilon constant conjecture*. It relates the values of the epsilon functions $\varepsilon_{L|K}(s)$ at $s = 0$ to an equivariant discriminant and a sum of Euler characteristics which are obtained from local fundamental classes with a *trivialization* induced by valuations on L.

This construction leads to an element $T\Omega^{\mathrm{loc}}(L|K, 1) \in K_0(\mathbb{Z}[G], \mathbb{R})$ which is mapped to $\Omega_2(L|K) - W(L|K)$ by $\partial^0_{G,\mathbb{R}}$, cf. [BrB07, Rem. 5.5]. It is also conjectured that the element $T\Omega^{\mathrm{loc}}(L|K, 1)$ vanishes in $K_0(\mathbb{Z}[G], \mathbb{R})$ and it can be proved that $T\Omega^{\mathrm{loc}}(L|K, 1) = 0$ implies the equivalence of the other two conjectures, cf. [BrB07, Conj. 5.3 and Thm. 5.8],

The relation to local fundamental classes reveals the local structure of this conjecture and it is in fact a consequence of a corresponding conjecture for local fields which was introduced by Breuning [Bre04b]. The epsilon constant conjectures will be studied algorithmically in the following chapter.

5 Epsilon constant conjectures

In the following we consider the statements of the global and local epsilon constant conjectures for number fields from [BlB03] and [Bre04b]. These conjectures are formulated as equations in relative K-groups for group rings.

Let $L|K$ be a fixed Galois extension of number fields with group G. As usual, we denote a finite, Galois-invariant set of places in L by S. The places of L will be denoted by w, and those of K by v:

$$\begin{array}{cccc} & L & w & \in S \\ G & \Big| & \Big| & \\ & K & v & \end{array}$$

Given such a set of places S, we also consider a fixed subset $S(G)$ of representatives of the G-orbits in S, i.e. for all places $w_1, \ldots, w_n$ in S dividing the same place v of K we choose a fixed place w above v.

5.1 Statement of the conjectures

5.1.1 The global epsilon constant conjecture

The global epsilon constant conjecture is formulated in the relative K-group $K_0(\mathbb{Z}[G], \mathbb{R})$. For a Galois extension $L|K$ of number fields it describes a relation between epsilon factors arising in the functional equation of the Artin L-function and algebraic invariants related to $L|K$. We recall its formulation as it was given in [BlB03]. Also remember that we introduced the following K-theoretic diagram in Section 1.4:

$$\begin{tikzcd} \mathrm{Z}(\mathbb{R}[G])^\times \arrow[dr, dashed, "\widehat{\partial}^1_{G,\mathbb{R}}"] & & \\ K_1(\mathbb{R}[G]) \arrow[u, hook, "\mathrm{nr}"] \arrow[r, "\partial^1"] & K_0(\mathbb{Z}[G], \mathbb{R}) \arrow[r, "\partial^0"] & K_0(\mathbb{Z}[G]) \end{tikzcd} \tag{5.1}$$

The analytic term of this conjecture is based on the equivariant epsilon function $\varepsilon_{L|K}(s)$ as defined in Section 1.5. Its value at $s = 0$ is an element in $\mathrm{Z}(\mathbb{R}[G])^\times$ by [Bre04a, Lem. 3.12] and it is called the *equivariant global epsilon constant.* The *extended boundary homomorphism* $\widehat{\partial}^1_{G,\mathbb{R}}$ gives a corresponding element $\mathscr{E}_{L|K} := \widehat{\partial}^1_{G,\mathbb{R}}(\varepsilon_{L|K}(0))$ in the relative K-group $K_0(\mathbb{Z}[G], \mathbb{R})$ which is also called *equivariant global epsilon constant.*

Let S be a finite, Galois-invariant set of places of L, including all infinite places and all places which ramify in $L|K$. For each $w \in S(G)$ with $w|p$, we choose a full projective $\mathbb{Z}_p[G_w]$-sublattice $\mathscr{L}_w$ of $\mathcal{O}_{L_w}$ upon which the p-adic exponential map is well-defined and injective. For each place $w \notin S$ we set $\mathscr{L}_w = \mathcal{O}_{L_w}$ and we define $\mathscr{L} \subseteq \mathcal{O}_L$ by its p-adic completions

$$\mathscr{L}_p = \prod_{v|p} \mathscr{L}_w \otimes_{\mathbb{Z}_p[G_w]} \mathbb{Z}_p[G] \subseteq L_p := L \otimes_{\mathbb{Q}} \mathbb{Q}_p,$$

where w is the fixed place above v. Let $\Sigma(L)$ denote all embeddings of L into $\mathbb{C}$. Then we define the *G-equivariant discriminant* by

$$\delta_{L|K}(\mathscr{L}) = [\mathscr{L}, \pi_L, H_L] \in K_0(\mathbb{Z}[G], \mathbb{R})$$

where $H_L = \prod_{\sigma \in \Sigma(L)} \mathbb{Z}$ and π_L is induced by

$$\begin{aligned} \rho_L : L \otimes_{\mathbb{Q}} \mathbb{C} &\to H_L \otimes_{\mathbb{Z}} \mathbb{C} \\ l \otimes z &\mapsto (\sigma(l)z)_{\sigma \in \Sigma(L)} \end{aligned}$$

as in [BlB03, § 3.2].

We continue to use the notation from Chapter 2, in particular, the finitely generated module $L_w^f := L_w^\times / \exp_w(\mathscr{L}_w)$ which is cohomologically isomorphic to $L_w^\times$. Using the *splitting module* construction from [NSW00, Chp. III, § 1, p. 115] as in Proposition 1.29 the local fundamental class $\gamma \in \hat{H}^2(G_w, L_w^f)$ is represented by an extension

$$0 \to L_w^f \to L_w^f(\gamma) \to \mathbb{Z}[G] \to \mathbb{Z} \to 0 \tag{5.2}$$

in $\mathrm{Yext}^2_{G_w}(\mathbb{Z}, L_w^f) \simeq \hat{H}^2(G_w, L_w^f)$. Then the perfect complex $P_w := \left[L_w^f(\gamma) \to \mathbb{Z}[G]\right]$ with $L_w^f(\gamma)$ in degree 0 also represents the local fundamental class and has cohomology L_w^f in degree 0 and $\mathbb{Z}$ in degree 1.

In Section 1.4 we defined an Euler characteristic $\bar{\chi}_{G_w}(Q, t) \in K_0(\mathbb{Z}[G_w], \mathbb{R})$ for any perfect complex Q and a *trivialization* $t : H^+(Q) \to H^-(Q)$ from cohomology in even to odd degree. Here, the valuation $w : L_w \to \mathbb{Q}$ induces a trivialization $w : L_w^\times / \exp(\mathscr{L}_w) \otimes \mathbb{Q} \simeq \mathbb{Q}$ of P_w and we denote the Euler characteristic $\bar{\chi}_{G_w}(P_w, w)$ by $E_w(\mathscr{L}_w)$. For the construction of a triple representing $E_w(\mathscr{L}_w)$ in $K_0(\mathbb{Z}[G_w], \mathbb{Q})$ see Section 1.4.2.

Furthermore, let $m_w \in \mathrm{Z}(\mathbb{Q}[G_w])^\times$ be the element defined in [BlB03, § 4.1] which is also called the *correction term.* It is defined as follows. For a subgroup $H \subseteq G$ and $x \in \mathrm{Z}(\mathbb{Q}[H])$ we let ${}^*x \in \mathrm{Z}(\mathbb{Q}[H])^\times$ denote the invertible element which on the *Wedderburn decomposition* $\mathrm{Z}(\mathbb{Q}[H]) = \prod_{i=1}^r F_i$ for suitable extensions $F_i|\mathbb{Q}$ is given by $x = (x_i)_{i=1\ldots r} \mapsto ({}^*x_i)$ with ${}^*x_i = 1$ if $x_i = 0$ and ${}^*x_i = x_i$ otherwise. Let φ_w denote a lift of the Frobenius automorphism in G_w/I_w, then the correction term is defined by

$$m_w = \frac{{}^*(|G_w/I_w| e_{G_w}) \cdot {}^*((1 - \varphi_w \mathrm{N}v^{-1}) e_{I_w})}{{}^*((1 - \varphi_w^{-1}) e_{I_w})} \in \mathrm{Z}(\mathbb{Q}[G_w])^\times. \tag{5.3}$$

Finally, we define elements

$$R\Omega^{\mathrm{loc}}(L|K,1) := \delta_{L|K}(\mathscr{L}) + \sum_{w\in S(G)} \mathrm{ind}_{G_w}^{G}\big(\widehat{\partial}^1_{G_w,\mathbb{Q}_p}(m_w) - E_w(\mathscr{L}_w)\big)$$

$$\text{and}\quad T\Omega^{\mathrm{loc}}(L|K,1) := \widehat{\partial}^1_{G,\mathbb{R}}\big(\varepsilon_{L|K}(0)\big) - R\Omega^{\mathrm{loc}}(L|K,1)$$

in $K_0(\mathbb{Z}[G],\mathbb{R})$. One can show that $T\Omega^{\mathrm{loc}}(L|K,1)$ is independent of the choices of S or $\mathscr{L}$ (cf. [BlB03, Rem. 4.2]) and we state the conjecture as follows.

Conjecture 5.1 (Global epsilon constant conjecture). *For every finite Galois extension $L|K$ of number fields the element $T\Omega^{\mathrm{loc}}(L|K,1) \in K_0(\mathbb{Z}[G],\mathbb{R})$ is zero. We denote this conjecture by* $\mathrm{EPS}(L|K)$.

Remark 5.2. In [BrB07, § 5], the formulation of this conjecture uses the Euler characteristic χ_G and a complex which corresponds to the local fundamental class by representing Ext^2_G using *injective resolutions.* In contrast, the formulation of [BlB03] (used here) applies Burns' original Euler characteristic $\bar{\chi}_G$ to the sequence (5.2) which corresponds to the local fundamental class if Ext^2_G is represented by a *projective resolution* of $\mathbb{Z}$. However, the difference between these representations of the extension group and the relation between the two different Euler characteristics which was discussed in Example 1.44(d) imply that the two definitions of $T\Omega^{\mathrm{loc}}(L|K,1)$ coincide. For a detailed discussion see [BrB07, Rem. 5.4].

5.1.2 The local epsilon constant conjecture

We will now describe a related conjecture for Galois extensions $L_w|K_v$ of local number fields over $\mathbb{Q}_p$ with group G_w, which was introduced by Breuning in [Bre04b]. Consider the following situation:

$$G\left(\begin{array}{c} L \\ | \\ K \end{array}\right. \qquad \begin{array}{c} w \\ | \\ v \end{array} \qquad\qquad \left.\begin{array}{c} L_w \\ | \\ K_v \end{array}\right)G_w$$

The equivariant global epsilon function of $L|K$ can be written as a product of equivariant local epsilon functions related to its completions $L_w|K_v$ as in Definition 1.47 and (1.23). Their value at zero is called the *equivariant local epsilon constant* and the local conjecture describes it in terms of algebraic invariants associated to the extension $L_w|K_v$. Here we refer to [Bre04a, Bre04b] for details.

Let $\mathbb{C}_p$ denote the completion of an algebraic closure of $\mathbb{Q}_p$. In analogy to (5.1) we introduced the following diagram in Section 1.4:

$$\begin{tikzcd} \mathrm{Z}(\mathbb{C}_p[G_w])^\times \arrow[dr, dashed, "\widehat{\partial}^1_{G_w,\mathbb{C}_p}"] & & \\ K_1(\mathbb{C}_p[G_w]) \arrow[u, "\mathrm{nr}", "\simeq"'] \arrow[r, two heads, "\partial^1"] & K_0(\mathbb{Z}_p[G_w],\mathbb{C}_p) \arrow[r, "\partial^0"] & 0, \end{tikzcd} \tag{5.4}$$

where the surjectivity of the map ∂^1 follows from [CR87, (39.10)] (see also [Bre04a, Lem. 2.5]). The extended boundary homomorphism $\widehat{\partial}^1_{G_w,\mathbb{C}_p}$ will therefore also be surjective.

For every character χ of $G_w = \mathrm{Gal}(L_w|K_v)$ one has an induced character $\mathrm{i}_{K_v}^{\mathbb{Q}_p}\chi$ of $\mathrm{Aut}(\mathbb{C}_p|\mathbb{Q}_p)$. The local Galois Gauss sum from [Mar77, Chp. II, § 4] of this induced character was denoted by $\tau_{L_w|K_v}(\chi) \in \mathbb{C}$ in Section 1.5 and we set

$$\tau_{L_w|K_v} := \big(\tau_{L_w|K_v}(\chi)\big)_{\chi\in\mathrm{Irr}_{\mathbb{C}}(G_w)} \in \mathrm{Z}(\mathbb{C}[G_w])^\times.$$

The choice of an embedding $\iota\colon \mathbb{C} \to \mathbb{C}_p$ induces a map $\mathrm{Z}(\mathbb{C}[G_w])^\times \to \mathrm{Z}(\mathbb{C}_p[G_w])^\times$ and we obtain the *equivariant local epsilon constant*

$$T_{L_w|K_v} := \widehat{\partial}^1_{G_w,\mathbb{C}_p}(\iota(\tau_{L_w|K_v})) \in K_0(\mathbb{Z}_p[G_w],\mathbb{C}_p).$$

As in the global case one chooses a full projective $\mathbb{Z}_p[G_w]$-sublattice $\mathscr{L}_w$ of $\mathcal{O}_{L_w}$ upon which the exponential function is well-defined. Similarly one defines the *equivariant local discriminant* in $K_0(\mathbb{Z}_p[G_w],\mathbb{C}_p)$ by

$$\delta_{L_w|K_v}(\mathscr{L}_w) = [\mathscr{L}_w, \rho_{L_w}, H_{L_w}], \tag{5.5}$$

where $H_{L_w} = \bigoplus_{\sigma\in\Sigma(L_w)} \mathbb{Z}_p$ and ρ_{L_w} is the isomorphism

$$\begin{aligned} \rho_{L_w} : \mathscr{L}_w \otimes_{\mathbb{Z}_p} \mathbb{C}_p &\to H_{L_w} \otimes_{\mathbb{Z}_p} \mathbb{C}_p \\ l \otimes z \quad &\mapsto (\sigma(l)z)_{\sigma\in\Sigma(L_w)}. \end{aligned}$$

Hereby $\Sigma(L_w)$ denotes the set of embeddings $L_w \hookrightarrow \mathbb{C}_p$. By the surjectivity of the homomorphism ∂^1 the equivariant local discriminant is represented by an element $d_{L_w|K_v} \in \mathbb{C}_p[G_w]^\times \subseteq K_1(\mathbb{C}_p[G_w])$. This element will be used later and an explicit formula is given in (5.8).

We write $E_w(\mathscr{L}_w)_p$ for the projection of the Euler characteristic $E_w(\mathscr{L}_w)$ onto $K_0(\mathbb{Z}_p[G_w],\mathbb{Q}_p)$ by the decomposition

$$K_0(\mathbb{Z}[G],\mathbb{Q}) \simeq \coprod_p K_0(\mathbb{Z}_p[G],\mathbb{Q}_p). \tag{5.6}$$

The difference $E_w(\mathscr{L}_w)_p - \delta_{L_w|K_v}(\mathscr{L}_w)$, which is denoted by $C_{L_w|K_v}$ in [Bre04b], is independent of $\mathscr{L}_w$ by [Bre04b, Prop. 2.6] and is called the *cohomological term* of $L_w|K_v$.

To state the local conjecture we also need the *unramified term* $U_{L_w|K_v} \in K_0(\mathbb{Z}_p[G_w],\mathbb{C}_p)$. It is a unique element which is mapped to zero by the scalar extension map $K_0(\mathbb{Z}_p[G_w],\mathbb{Q}_p) \to K_0(\mathcal{O}_p^t[G_w],\mathbb{C}_p)$ where $\mathcal{O}_p^t$ is the ring of integers of the maximal tamely ramified extension of $\mathbb{Q}_p$ in $\mathbb{C}_p$. The proof of the existence in [Bre04b, Prop. 2.12] includes an explicit formula for a representative $u_{L_w|K_v} \in \mathbb{C}_p[G_w]^\times \subseteq K_1(\mathbb{C}_p[G_w])$ with $\partial^1(u_{L_w|K_v}) = U_{L_w|K_v}$, which we will recall in (5.9).

We can now state the followgin conjecture for local extensions.

Conjecture 5.3 (Local epsilon constant conjecture). *For every Galois extension $L_w|K_v$ of local fields over $\mathbb{Q}_p$ the element*

$$R_{L_w|K_v} := T_{L_w|K_v} + C_{L_w|K_v} + U_{L_w|K_v} - \widehat{\partial}^1_{G_w,\mathbb{C}_p}(m_w)$$

is zero in $K_0(\mathbb{Z}_p[G_w], \mathbb{C}_p)$. We denote this conjecture by $\mathrm{EPS}^{\mathrm{loc}}(L_w|K_v)$.

5.2 Basic properties and state of research

The global epsilon constant conjecture $\mathrm{EPS}(L|K)$ is known to be valid modulo the torsion subgroup $K_0(\mathbb{Z}[G], \mathbb{Q})_{\mathrm{tor}}$, and the local conjecture modulo the subgroup $K_0(\mathbb{Z}_p[G_w], \mathbb{Q}_p)$.

Proposition 5.4. *(a) The element $T\Omega^{\mathrm{loc}}(L|K, 1)$ is an element of the torsion subgroup $K_0(\mathbb{Z}[G], \mathbb{Q})_{\mathrm{tor}}$ of $K_0(\mathbb{Z}[G], \mathbb{Q}) \subseteq K_0(\mathbb{Z}[G], \mathbb{R})$.*

(b) $R_{L_w|K_v}$ is an element of the subgroup $K_0(\mathbb{Z}_p[G_w], \mathbb{Q}_p) \subseteq K_0(\mathbb{Z}_p[G_w], \mathbb{C}_p)$.

Proof. [BlB03, Prop. 3.4] shows that $T\Omega^{\mathrm{loc}}(L|K, 1) \in K_0(\mathbb{Z}[G], \mathbb{Q})$ and [BlB03, Cor. 6.3] implies $T\Omega^{\mathrm{loc}}(L|K, 1) \in K_0(\mathbb{Z}[G], \mathbb{Q})_{\mathrm{tor}}$. For part (b) see [Bre04b, Prop. 3.4]. □

We can therefore write $T\Omega^{\mathrm{loc}}(L|K, 1)_p$ for the projection onto $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ via the decomposition (5.6) of $K_0(\mathbb{Z}[G], \mathbb{Q})$ and the corresponding conjectural equality $T\Omega^{\mathrm{loc}}(L|K, 1)_p = 0$ in $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ will be denoted by $\mathrm{EPS}_p(L|K)$. For this p-part of the global conjecture we get the following relation.

Corollary 5.5. *The global conjecture $\mathrm{EPS}(L|K)$ is valid if and only if its p-part $\mathrm{EPS}_p(L|K)$ is valid for all primes p.*

The local conjecture can then be regarded as a refinement of the p-part of the global conjecture.

Theorem 5.6 (Local-global principle). *One has the equality*

$$T\Omega^{\mathrm{loc}}(L|K, 1)_p = \sum_{v|p} \mathrm{i}^G_{G_w}(R_{L_w|K_v})$$

in $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ and one can deduce:

(a) $\mathrm{EPS}^{\mathrm{loc}}(M|N)$ for all $M|N|\mathbb{Q}_p \Rightarrow \mathrm{EPS}_p(L|K)$ for all $L|K|\mathbb{Q}$,

(b) if $p \neq 2$: $\mathrm{EPS}_p(L|K)$ for all $L|K|\mathbb{Q} \Rightarrow \mathrm{EPS}^{\mathrm{loc}}(M|N)$ for all $M|N|\mathbb{Q}_p$, and

(c) for fixed $L|K|\mathbb{Q}$ and p: $\mathrm{EPS}^{\mathrm{loc}}(L_w|K_v)$ for all $w|v|p \Rightarrow \mathrm{EPS}_p(L|K)$.

Proof. [Bre04b, Thm. 4.1 and Thm. 4.3]. □

So for odd primes, there is an equivalence between the local conjecture and the p-part of the global conjecture. Another important property that both (local and global) conjectures satisfy, is the so called *functorial property.*

Proposition 5.7 (Functorial property). *For a Galois extension $L|K$ of number fields with intermediate field $F|K$ and a local Galois extension $M|N$ over $\mathbb{Q}_p$ with intermediate field $E|K$ one has:*

(a) $\mathrm{EPS}(L|K) \Rightarrow \mathrm{EPS}(L|F)$ *and* $\mathrm{EPS}(L|K) \Rightarrow \mathrm{EPS}(F|K)$ *if $F|K$ is Galois.*

(b) $\mathrm{EPS}^{\mathrm{loc}}(M|N) \Rightarrow \mathrm{EPS}^{\mathrm{loc}}(M|E)$ *and* $\mathrm{EPS}^{\mathrm{loc}}(M|N) \Rightarrow \mathrm{EPS}^{\mathrm{loc}}(E|K)$ *if $E|K$ is Galois.*

Proof. [BlB03, Thm. 6.1] and [Bre04b, Prop. 4.25]. □

Proposition 5.8. *The global epsilon constant conjecture implies Chinburg's $\Omega(2)$-conjecture from [Chi85, Question 3.1].*

Proof. [BlB03, Rem. 4.2(iv)]. □

Furthermore, there are the following results. The global epsilon constant conjecture is known to be valid

(A) for tamely ramified extensions [BlB03],

(B) for abelian extensions of $\mathbb{Q}$ [BlB03, BF06], and

(C) for some (infinite families of) dihedral, quaternion and S_3–extensions by [BlB03, Bre04b, Sna03].

Using the local-global principle those results also carry over to the local conjecture and actually some were proved using local results. By [Bre04b] the local conjecture is known to be valid

(D) for tamely ramified extensions,

(E) for abelian extensions $M|\mathbb{Q}_p$ with $p \neq 2$, and

(F) for S_3–extensions of $\mathbb{Q}_3$.

It is well-known that for fixed p and n there are just finitely many Galois extensions $M|\mathbb{Q}_p$ with degree $[M : \mathbb{Q}_p] = n$. From the theoretical results above we can deduce the following implications from the local conjecture for Galois extensions $M|\mathbb{Q}_p$ with $p \leq n$ (all extensions below are assumed to be Galois):

$$\begin{array}{lll}
\mathrm{EPS}^{\mathrm{loc}}(M|\mathbb{Q}_p) & \forall [M:\mathbb{Q}_p] \leq n, p \leq n & \\
\Rightarrow \mathrm{EPS}^{\mathrm{loc}}(M|\mathbb{Q}_p) & \forall [M:\mathbb{Q}_p] \leq n, \forall p & \text{(result (D) for tame extensions)} \\
\Rightarrow \mathrm{EPS}_p(L|\mathbb{Q}) & \forall [L:\mathbb{Q}] \leq n, \forall p & \text{(by Theorem 5.6)} \\
\Rightarrow \mathrm{EPS}(L|\mathbb{Q}) & \forall [L:\mathbb{Q}] \leq n & \text{(by Corollary 5.5)} \\
\Rightarrow \mathrm{EPS}(F|K) & \forall F \subseteq L, [L:\mathbb{Q}] \leq n & \text{(by Proposition 5.7)}
\end{array}$$

In other words, the local epsilon constant conjecture for a finite set of local extensions of degree $\leq n$ implies the global epsilon constant conjecture for all Galois extensions $F|K$ where $F \subseteq L$ and $L|\mathbb{Q}$ is a Galois extension of degree at most n (see also [Bre04a, Thm. 5.7]). From an algorithm proving the local conjecture for a fixed Galois extension $M|\mathbb{Q}_p$ it will therefore automatically be possible to give a computational proof of the global conjecture up to a finite degree n.

Such an algorithm for $\mathrm{EPS}^{\mathrm{loc}}(M|\mathbb{Q}_p)$, with $M|\mathbb{Q}_p$ Galois, is described by Bley and Breuning in [BlBr08]. But it has not been implemented because there were a few steps for which (at the time the paper was written) no practical solution was known. One of these problem was the computation of local fundamental classes for which we gave an efficient algorithm in Section 2.2.2. The issues of computations in algebraic K-groups are studied in detail in [BW09] and its main result will be discussed below in Proposition 5.13. Finally, a remaining problem is the fact that this approach needs the extension $M|\mathbb{Q}_p$ to be represented by a global Galois extension of number fields in order to do exact computations.

To sum up, an algorithm to prove the *global* epsilon constant conjecture using the implications above is given by the following steps.

1. For a finite integer n, compute all local Galois extensions of $\mathbb{Q}_p$ up to degree n, with $p \leq n$.

2. Find global Galois extensions of number fields representing all these local extensions.

3. Apply the algorithm by Bley and Breuning [BlBr08] to prove the local epsilon constant conjecture of these extensions.

Step 1: Up to degree 11, the database by Jones and Roberts [JR] contains polynomials for all local extensions of $\mathbb{Q}_p$ and more generally, one can use an algorithm by Pauli and Roblot [PR01] to compute all extensions of $\mathbb{Q}_p$ of a given degree.

The latter algorithm performs well enough up to degree 15. However, we were not able to compute all local extensions of degree 16 of $\mathbb{Q}_2$. The implementation in Pari/Gp terminated after a few days with an out of memory error[1], and Magma did not compute a result within 50 days. We therefore have to restrict to extensions of degree $n \leq 15$ and will only consider primes $p \leq 15$ since extensions of $\mathbb{Q}_p$, $p > 15$, will be tamely ramified. A complete list of the Galois groups which occur up to this degree is given in Table A.1 on page 160.

Step 2: In the following section we will define what we mean by those global representations and will discuss how to find them.

Step 3: In Section 5.4 we will recall the algorithm of Bley and Breuning and give algorithmic results that were found using the global representations from step 2.

[1]using more than 10 GB of memory

5.3 Global representations of local Galois extensions

We say that a number field K with prime ideal $\mathfrak{p}$, denoted as a pair $(K, \mathfrak{p})$, is a global representation for a local field M over $\mathbb{Q}_p$ if $M \simeq K_{\mathfrak{p}}$. An extension $(L, \mathfrak{P})|(K, \mathfrak{p})$ is an extension $L|K$ of number fields with a prime ideal $\mathfrak{P}$ dividing $\mathfrak{p}$ and $[L : K] = [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$, i.e. $\mathfrak{p}$ is *undecomposed* in L. A global representation for a local extension $M|N$ is an extension $(L, \mathfrak{P})|(K, \mathfrak{p})$ with $(L, \mathfrak{P})$ and $(K, \mathfrak{p})$ representing M and N, respectively:

$$\begin{array}{ccccc} L & \mathfrak{P} & \qquad & M \simeq L_{\mathfrak{P}} \\ \Big| & \Big| & & \Big| \\ K & \mathfrak{p} & & N \simeq K_{\mathfrak{p}} \end{array}$$

Lemma 5.9. *Every Galois extension $M|N$ of p-adic fields has a global representation $(L, \mathfrak{P})|(K, \mathfrak{p})$ with $L|K$ Galois.*

Proof. [BlBr08, Lem. 2.1 and 2.2]. □

From now on, a global representation will always refer to such a representation where $L|K$ is Galois. In order to do exact computations we will need such a global representation. The proof of the existence in this theorem involves the Galois closure of a number field, but for computational reasons we need a representation which has small degree over $\mathbb{Q}$, or even better with $K = \mathbb{Q}$.

In the following, we will restrict ourselves to the case $M|\mathbb{Q}_p$ using the functorial properties of the conjectures. For this case, Henniart shows in [Hen01] the following result.

Theorem 5.10. *For $M|\mathbb{Q}_p$ there exist a global representation $(L, \mathfrak{P})|(K, \mathfrak{p})$ which is Galois and where $K = \mathbb{Q}$ if $p \neq 2$ and K is quadratic over $\mathbb{Q}$ if $p = 2$.*

Unfortunately, it is not clear how to find these small representations algorithmically, cf. [BlBr08, Rem. 2.4]. For the construction of a global Galois extension $L|K$, with $K = \mathbb{Q}$ or $K = \mathbb{Q}(\sqrt{d})$, representing fixed local Galois extension $M|\mathbb{Q}_p$ we will therefore use the following heuristics and discuss their performance for extensions up to degree 15.

5.3.1 Heuristics

Search database of Klüners and Malle

The database of Klüners and Malle [KM01] contains polynomials generating Galois extensions of $\mathbb{Q}$ for all subgroups G of permutation groups S_n up to degree

$n = 15$. In particular, the database contains polynomials for all Galois groups of order $n \leq 15$. Among those one will often find a polynomial generating a global representation $(K, \mathfrak{p})$ for M, if $[M : \mathbb{Q}_p] \leq 15$.

Generic polynomials

In this context we consider polynomials $f \in K(t_1, \dots, t_n)[x]$ with arbitrary indeterminates t_i over a field K. It is said to be *generic* for a group G, if the splitting field L of f is a Galois extension of $K(t_1, \dots, t_n)$ with group G and, moreover, all extensions of $K(t_1, \dots, t_n)$ with group G are given by a polynomial f of this form. For specializations of values $t_1, \dots t_n \in \mathbb{Q}$ (possibly with certain restrictions) and $K = \mathbb{Q}$ one will get a Galois extension of $\mathbb{Q}$ with this group G and randomly testing different values will also return a global representation for M.

The book [JLY02] by Jensen et. al. contains generic polynomials (or methods to construct them) for a lot of groups. In particular, it contains polynomials for all non-abelian groups of order ≤ 15, except for the generalized quaternion group Q_{12} of order 12. However, there do not exist generic polynomials for all groups. The smallest group for which the non-existence is proved is the cyclic group of order eight [JLY02, § 2.6].

Class field theory

As a last heuristic, we will use class field theory to construct abelian extensions with prescribed ramification.[2] For a field extensions K of $\mathbb{Q}$, there is a one-to-one correspondence between abelian extensions $L|K$ and subgroups of the idèle class group C_K and each of those extensions $L|K$ has Galois group $\mathrm{Gal}(L|K) \simeq C_K / \mathrm{N}_{L|K} C_L$, cf. [Neu92, Chp. VI, § 6].

For a *modulus* $\mathfrak{m} = \prod \mathfrak{p}^{n_\mathfrak{p}}$ — where $\mathfrak{p}$ runs through all (finite and infinite) places and $n_\mathfrak{p} \in \mathbb{N} \cup \{0\}$ and $n_\mathfrak{p} \in \{0, 1\}$ for $\mathfrak{p}|\infty$ — one studies in particular the ray class field $K^\mathfrak{m}|K$. It is the extension corresponding to the subgroup $\big(\prod_\mathfrak{p} U_\mathfrak{p}^{(n_\mathfrak{p})}\big) K^\times / K^\times \subseteq C_K$ where $U_\mathfrak{p}^{(0)} = \mathcal{O}_{K_\mathfrak{p}}^\times$ and $U_\mathfrak{p}^{(n_\mathfrak{p})} = 1 + \mathfrak{p}^n$ for finite $\mathfrak{p}$, $U_\mathfrak{p}^{(0)} = \mathbb{R}^\times$ and $U_\mathfrak{p}^{(1)} = \mathbb{R}_{>0}$ for real $\mathfrak{p}$, and $U_\mathfrak{p}^{(n_\mathfrak{p})} = \mathbb{C}^\times$ for complex $\mathfrak{p}$. This abelian extension of K can be constructed using algorithms described by Cohen in [Coh00, Chp. 4]. A discussion of algorithms implemented in Magma is given by Fieker in [Fie06].

Given an extension $L|K$ one defines the *conductor* $\mathfrak{f}$ to be the greatest common divisor of all moduli $\mathfrak{m}$ for which $L \subseteq K^\mathfrak{m}$. For this conductor one can prove that $\mathfrak{p}|\mathfrak{f}$ if and only if $\mathfrak{p}$ is ramified in $L|K$ and, moreover, $\mathfrak{p}^2|\mathfrak{f}$ if and only if $\mathfrak{p}$ is wildly ramified in $L|K$, cf. [Fie06, § 2.4, p. 44].

One can therefore possibly find abelian extensions of K with prescribed ramification at certain places by choosing an appropriate modulus, constructing the corresponding ray class field, and computing suitable subfields of the requested degree.

[2]Thanks to Jürgen Klüners for suggesting the application of this method.

5.3.2 Results up to degree 15

In the algorithm of Bley and Breuning we will have to consider the local situation

$$\begin{tikzcd} M \arrow[d, dash] \arrow[d, dash, bend right=60, "G"'] & \\ \mathbb{Q}_p \arrow[r, dash] & N_f \end{tikzcd}$$

where $M|\mathbb{Q}_p$ is a Galois extension with group G and N_f is the unramified extension of $\mathbb{Q}_p$ of degree $f = \exp(G^{\mathrm{ab}})$, where f denotes the exponent of the abelianization G^{ab} of G. Since the local conjecture is known to be valid for tamely ramified extensions and abelian extensions of $\mathbb{Q}_p$, $p \neq 2$, we will discuss the performance of the heuristic methods in the following cases:

(a) wildly ramified extensions M of $\mathbb{Q}_p$ with non-abelian Galois group G,

(b) wildly ramified extensions M of $\mathbb{Q}_2$, with abelian Galois group G, and

(c) unramified extensions of $\mathbb{Q}_p$ of degree $f = \exp(G^{\mathrm{ab}})$ in each of the two situations above.

In all of these cases we restrict to extensions of degree ≤ 15 since for degree 16 we cannot compute all extensions of $\mathbb{Q}_2$. The hypothesis of wild ramification implies that we only have to consider primes $p = 2, 3, 5$ and 7. The primes 11 and 13 are not considered because they can only occur (up to degree ≤ 15) in abelian extensions of degree 11 and 13, which are not considered in the cases above.

The theory does not guarantee the existence of global representations with base field $\mathbb{Q}$ in the case $p = 2$. But after all, the heuristics also worked in most of those cases.

Case a

First consider extensions with *non-abelian* Galois group. For almost all those non-abelian wildly-ramified local extensions we found polynomials of the appropriate degree in the database [KM01] generating a global representation. Table 5.1 on page 120 gives an overview of all the global representations that were found using this database. For each group (using the standard notation as introduced in Appendix A.1) it contains the number of extensions over $\mathbb{Q}_p$ (as listed in the database [JR] or computed by [PR01]) and whether they were represented globally by a polynomial in the database of Klüners and Malle.

In fact, there were just three D_4–extensions of $\mathbb{Q}_2$ and three D_7–extensions of $\mathbb{Q}_7$ not being represented by any polynomial (of degree 8 or 14 respectively) in this database.

By [JLY02, Cor. 2.2.8] every D_4–extension of $\mathbb{Q}$ is the splitting field of a polynomial $f(x) = x^4 - 2stx^2 + s^2t(t-1) \in \mathbb{Q}[x]$ with suitable $s, t \in \mathbb{Q}$. Experimenting with small integers s and t and computing the splitting field of f quickly provides global representations for all D_4–extensions of $\mathbb{Q}_2$.

Finally, we used class field theory to construct global Galois representations for the three non-isomorphic D_7–extensions of $\mathbb{Q}_7$: by taking quadratic extensions K of $\mathbb{Q}$ which are undecomposed at $p = 7$ and computing all C_7–extensions of K which are subfields of $K^{\mathfrak{m}}$, $\mathfrak{m} = 49\mathcal{O}_K$, one finds D_7–extensions where $p = 7$ is ramified with ramification index 7 or 14 and where p does not decompose. Experimenting with different fields K as above one finds global Galois representations for all three D_7–extensions of $\mathbb{Q}_7$.

This completes the construction of global representations for all non-abelian wildly ramified local extensions of $\mathbb{Q}_p$, $p = 2, 3, 5, 7$, up to degree 15.[3]

Case b

Using the database [KM01] we can again find polynomials for almost all extensions in question. However, there were also quite a few extensions (of degree 8 and 12) for which the above heuristics did not work (see Table 5.2 on page 120). However, by Henniart's result (see Theorem 5.10 or [Hen01]) we only know that such a representation exists over some field K where K is quadratic over $\mathbb{Q}$.

One can therefore search the database [KM01] for polynomials whose splitting field is of degree 16 (or 24) and where the prime $p = 2$ decomposes into two prime ideals. Then the completion at any prime above 2 will be an extension of degree 8 (or 12 respectively) of $\mathbb{Q}_2$.

Using this method, we could find polynomials representing the last $C_2 \times C_4$ extension and 3 more C_8–extensions. But there are still 13 C_8 and 4 C_{12}–extensions for which we did not find a global representation.

However, to obtain a *global* result up to degree 15 (see Corollary 5.18), one can use the theoretic results for abelian extensions. Then it is sufficient to consider abelian extensions over $\mathbb{Q}_p$ of degree ≤ 7. Indeed, if $L|\mathbb{Q}$ is non-abelian of degree ≤ 15 and its completion $L_{\mathfrak{P}}|\mathbb{Q}_p$ has abelian Galois group, then $[L_{\mathfrak{P}} : \mathbb{Q}_p] \leq 7$ since the local Galois group is a proper subgroup of the global Galois group.

Case c

For each of the pairs $(L|\mathbb{Q}, p)$ with Galois group G constructed in cases (a) and (b), Algorithm 5.12 also needs a extension N of $\mathbb{Q}$ which is unramified and undecomposed at p and is of degree $f = \exp(G^{\mathrm{ab}})$.

Most of these unramified extensions can be constructed as a subfield of a cyclotomic field $\mathbb{Q}(\zeta_n)$ generated by an n-th root of unity ζ_n. The decomposition of primes in a cyclotomic field is well-known and can easily be computed, see [Neu92, Chp. I, Thm. (10.3)].

For non-abelian extensions of degree ≤ 15 the maximum degree of N can easily be determined to be $f = 4$. Polynomials generating these unramified extensions are given in Table 5.3 on page 121. For the abelian extensions of $\mathbb{Q}_2$ we also have

[3] Appendix A.1 gives a complete list which also contains all abelian Galois groups.

n	p	group	#ext.	in [KM01]	n	p	group	#ext.	in [KM01]
6	2	S_3	1	✓	12	2	D_6	3	✓
	3	S_3	6	✓			Q_{12}	4	✓
8	2	D_4	18	15	12	3	A_4	0	
		Q_8	6	✓			D_6	6	✓
10	2	D_5	0				Q_{12}	2	✓
	5	D_5	3	✓	14	2	D_7	0	
12	2	A_4	1	✓		7	D_7	3	0

Table 5.1: Non-abelian local Galois extensions of $\mathbb{Q}_p$ of degree $n \leq 15$ with possible wild ramification.

n	group	#ext.	in [KM01]	n	group	#ext.	in [KM01]
2	C_2	7	✓	8	C_2^3	1	✓
4	C_4	12	✓	10	C_{10}	7	✓
	V_4	7	✓	12	C_{12}	12	8
6	C_6	7	✓		$C_3 \times V_4$	11	✓
8	C_8	24	8	14	C_{14}	7	✓
	$C_2 \times C_4$	18	17				

Table 5.2: Abelian local Galois extensions of $\mathbb{Q}_2$ of degree $n \leq 15$ with possible wild ramification.

degree	polynomial	unramified primes
2	x^2+1	$2,3,7$
	x^2+x+1	5
3	$x^3-7x^2+14x-7$	$2,3,5$
	x^3-6x^2+9x-3	7
4	$x^4+x^3+x^2+x+1$	$2,3,7$
	x^4+13x^2+13	5

Table 5.3: Unramified extensions of $\mathbb{Q}_p$, $p=2,3,5,7$, up to degree 4.

degree	polynomial
5	$x^5-x^4-4x^3+3x^2+3x-1$
6	$x^6-x^5-7x^4+2x^3+7x^2-2x-1$
7	$x^7-x^6-12x^5+7x^4+28x^3-14x^2-9x-1$
8	splitting field of $x^8-3x^5-x^4+3x^3+1$
9	$x^9-x^8-8x^7+7x^6+21x^5-15x^4-20x^3+10x^2+5x-1$
10	$x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$
11	$x^{11}+x^{10}-10x^9-9x^8+36x^7+28x^6-56x^5-35x^4+35x^3+15x^2-6x-1$
12	$x^{12}-x^{11}-12x^{10}+11x^9+54x^8-43x^7-113x^6+71x^5+110x^4-46x^3-40x^2+8x+1$
12	$x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$
13	$x^{13}-x^{12}-24x^{11}+19x^{10}+190x^9-116x^8-601x^7+246x^6+738x^5-215x^4-291x^3+68x^2+10x-1$
14	$x^{14}-x^{13}-13x^{12}+12x^{11}+66x^{10}-55x^9-165x^8+120x^7+210x^6-126x^5-126x^4+56x^3+28x^2-7x-1$
15	$x^{15}-x^{14}-22x^{13}+17x^{12}+166x^{11}-102x^{10}-533x^9+270x^8+729x^7-352x^6-393x^5+173x^4+80x^3-27x^2-6x+1$

Table 5.4: Unramified extensions of $\mathbb{Q}_2$ up to degree 14.

to consider unramified extensions of higher degree. For $f \neq 8$ these can again be constructed as subfields of cyclotomic extensions and extensions of relatively small discriminant can be found be searching [KM01] (see Table 5.4).

Only $f = 8$ turns out to be a special case: By Wang's counterexample to Grunwald's original statement of his theorem there is no global representation $L|\mathbb{Q}$ for the unramified C_8–extension of $\mathbb{Q}_2$. But such a representation exists over some field K where K is quadratic over $\mathbb{Q}$.

We can therefore search the database [KM01] for polynomials whose splitting field is of degree 16 and where the prime $p = 2$ decomposes into two prime ideals which each have cyclic decomposition group. Then the completion at any prime above 2 will be an unramified extension of degree 8 of $\mathbb{Q}_2$. For example the splitting field of the polynomial $x^8 - 3x^5 - x^4 + 3x^3 + 1$ satisfies these conditions. In comparison to the other global representation we found heuristically, it is the only case (up to degree 15) in which the base field K of the global representation is not equal to $\mathbb{Q}$.

This completes the construction of unramified extensions needed in all situations. But in some cases one can also be more specific and construct extensions N such that the composite field LN has small degree over $\mathbb{Q}$.

Let L be a Galois extension of $\mathbb{Q}$ with group G and $\mathfrak{P}$ a prime ideal of L dividing p and let $G_{\mathfrak{P}}$ be the decomposition group of $\mathfrak{P}$. Then consider the *inertia subfield* of L at $\mathfrak{P}$, i.e. the fixed field of the inertia subgroup

$$I_{\mathfrak{P}} = \{\sigma \in G_{\mathfrak{P}} \mid \sigma x \equiv x \bmod \mathfrak{P},\ \forall x \in \mathcal{O}_L\}.$$

The inertia subfield $L^{I_{\mathfrak{P}}}$ is the maximal subfield of $L|\mathbb{Q}$ such that p is unramified.

In some cases one can directly consider $N = L^{I_{\mathfrak{P}}}$, and in other cases one can construct unramified extensions N of $L^{I_{\mathfrak{P}}}$ with appropriate degree over $\mathbb{Q}$. For example if $L^{I_{\mathfrak{P}}}$ has degree 2 over $\mathbb{Q}$ and we search for an unramified extensions N of degree $f = 4$, then we can use the following embedding result.

Proposition 5.11. *A quadratic extension $K(\sqrt{a})|K$ can be embedded into a C_4–extension if and only if a is the sum of two squares in K. The C_4–extensions of K containing $K(\sqrt{a})$ are*

(a) $K(\sqrt{r(a + x\sqrt{a}})$ if $a = x^2 + y^2$ for $x, y \in K$ and

(b) $K(\sqrt{r(\alpha + \beta\sqrt{a}})$ if $a = \alpha^2 - a\beta^2$ for $\alpha, \beta \in K$

with parameter $r \in K^\times$.

Proof. [JLY02, Thm. 2.2.5]. □

To sum up, using the heuristic methods described above we were able to compute global representations for all non-abelian wildly ramified local extensions of $\mathbb{Q}_p$, $p = 2, 3, 5, 7$, of degree ≤ 15 and for all abelian extensions of $\mathbb{Q}_2$ of degree ≤ 6. These polynomials were used to prove the local epsilon constant conjecture and can be found in Appendix A.2.

5.4 Description of the algorithm

The following algorithm to prove the local epsilon constant conjecture for a fixed number field extension was described by Bley and Breuning in [BlBr08]. We will recall the algorithm and discuss some details on the implementation. Afterwards we will present some results which were obtained by computational proofs. But first we give a brief overview of the algorithm.

For the rest of this section, fix the Galois extensions $L|K$ and $N|K$ and a prime $\mathfrak{p}$ of K as in the input of the algorithm. For simplicity, the unique prime ideal above $\mathfrak{p}$ in the fields L, N, or any subextension of $L|K$ will also be denoted by $\mathfrak{p}$. If it is necessary to avoid confusion, we will write $\mathfrak{p}_K$, $\mathfrak{p}_L$ and $\mathfrak{p}_N$. Furthermore, we will identify the ideals $\mathfrak{p}_L|\mathfrak{p}_K$ with places $w|v$ of L and K, respectively, such that $L_w = L_\mathfrak{p}$ and $K_v = K_\mathfrak{p}$.

Algorithm 5.12 (Proof of the local epsilon constant conjecture).
Input: An extension $(L,\mathfrak{P})|(K,\mathfrak{p})$ with $K_\mathfrak{p} = \mathbb{Q}_p$ in which $L|K$ is Galois with group G and a Galois extension $N|K$ of degree $\exp(G^{\mathrm{ab}})$ in which $\mathfrak{p}$ is undecomposed and unramified.

Output: True if $\mathrm{EPS}^{\mathrm{loc}}(L_\mathfrak{P}|\mathbb{Q}_p)$ was successfully checked.

(Construction of the coefficient field)

1 Compute all characters χ of G and use Brauer induction to find an integer t such that the Galois Gauss sums can be computed in $\mathbb{Q}(\zeta_m, \zeta_{p^t})$, $m = \exp(G^{\mathrm{ab}})$.

2 Construct the composite field E of L, N and $\mathbb{Q}(\zeta_m, \zeta_{p^t})$ and fix a complex embedding $\iota : E \hookrightarrow \mathbb{C}$ and a prime ideal $\mathfrak{Q}$ of E above p.

(Computation of cohomological term)

3 Compute a suitable lattice $\mathscr{L} \subseteq \mathcal{O}_{L_\mathfrak{P}}$ as in Lemma 2.1 and k such that $(\mathfrak{P}\mathcal{O}_{L_\mathfrak{P}})^k \subseteq \mathscr{L}$, denote $L_\mathfrak{P}^f := L_\mathfrak{P}^\times / \exp(\mathscr{L})$.

4 Compute an element in $\mathrm{Yext}^2_G(\mathbb{Z}, L_\mathfrak{P}^f)$ representing the local fundamental class using Algorithm 2.18 and Proposition 1.29.

5 Compute the Euler characteristic $E_w(\mathscr{L}) \in K_0(\mathbb{Z}[G], \mathbb{Q})$ as in Example 1.44.

(Computation of the terms in $\prod_\chi E^\times$)

6 Compute the correction term $m_{L_\mathfrak{P}|\mathbb{Q}_p} = m_w \in \mathrm{Z}(\mathbb{Q}[G])^\times \subseteq \mathrm{Z}(E[G])^\times \simeq \prod_\chi E^\times$ defined in (5.3).

7 Compute the element $d_{L_\mathfrak{P}|\mathbb{Q}_p} \in L[G]^\times \subseteq E[G]^\times$ from (5.8), which represents the equivariant discriminant $\delta_{L_\mathfrak{P}|\mathbb{Q}_p}(\mathscr{L}) \in K_0(\mathbb{Z}[G], E_\mathfrak{Q})$ defined in (5.5).

8 Compute the element $u_{L_\mathfrak{P}|\mathbb{Q}_p} \in N[G]^\times \subseteq E[G]^\times$ using (5.9), which represents the unramified term $U_{L_\mathfrak{P}|\mathbb{Q}_p} \in K_0(\mathbb{Z}[G], E_\mathfrak{Q})$.

9 Use the canonical homomorphism $E[G]^\times \to K_1(E[G])$, the reduced norm map $\mathrm{nr} : K_1(E[G]) \to \mathrm{Z}(E[G])$ and Wedderburn decomposition of $\mathrm{Z}(E[G])$ to represent these three terms in $\prod_\chi E^\times$.

10 Compute the equivariant epsilon constant $\tau_{L_\mathfrak{P}|\mathbb{Q}_p} \in \prod_\chi \mathbb{Q}(\zeta_{p^t}, \zeta_m)^\times \subseteq \prod_\chi E^\times$ via Galois Gauss sums.

(Computations in relative K-groups)

11 Read $E_w(\mathscr{L})$ and the tuples from above as elements in $K_0(\mathbb{Z}_p[G], E_\mathfrak{Q})$.

12 Compute the sum $R_{L_\mathfrak{P}|\mathbb{Q}_p} \in K_0(\mathbb{Z}_p[G], E_\mathfrak{Q})$ of the resulting elements.

Return: True if $R_{L_\mathfrak{P}|\mathbb{Q}_p}$ is zero, and false otherwise.

We will discuss each part for the algorithm separately.

Constructing the coefficient field

As explained in [BlBr08, § 4.2.2] we need to construct a global field E, in which all the computations take place.

For the computation of the unramified term, we will need a cyclic extensions $N|K$ which is unramified and undecomposed at $\mathfrak{p}$.

Another extension involved is $\mathbb{Q}(\zeta_m, \zeta_{p^t})$, where m is the exponent of G^{ab} and t is computed as in [BlBr08, Rem. 2.7]: By representation theory the field $\mathbb{Q}(\zeta_m)$ contains the values of all characters of G. The root of unity ζ_{p^t} is used to represent Galois Gauss sums and the integer t is determined as follows.

For each character χ of G one computes subgroups H, linear characters ϕ of H, and coefficients $c_{(H,\phi)} \in \mathbb{Z}$ such that $\chi - \chi(1)1_G = \sum_{(H,\phi)} c_{(H,\phi)} \mathrm{ind}_H^G(\phi - 1_H)$. Such a relation exists by Brauer's induction theorem, cf. [BlBr08, § 2.5]. If $\mathfrak{f}(\phi)$ denotes the *Artin conductor* of ϕ and e the ramification index of $(L^H)_\mathfrak{p}|\mathbb{Q}_p$, then t must satisfy $t \geq v_\mathfrak{p}(\mathfrak{f}(\phi))/e$ for all pairs (H, ϕ) and all χ. Below, this choice of t allows us to compute the epsilon constants as elements of $\mathbb{Q}(\zeta_m, \zeta_{p^t})$, see also [BlBr08, Rem. 2.7].

The composite field of the three fields L, N and $\mathbb{Q}(\zeta_m, \zeta_{p^t})$ is denoted by E, giving the following situation:

$$\begin{tikzcd} & E \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\zeta_m, \zeta_{p^t}) \arrow[dr, dash] & L \arrow[d, dash] & N \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd} \tag{5.7}$$

We then fix a complex embedding $\iota : E \hookrightarrow \mathbb{C}$. Since E contains the roots of unity ζ_m, the center $\mathrm{Z}(E[G])$ decomposes into $\mathrm{Z}(E[G]) = \prod_{\chi \in \mathrm{Irr}_\mathbb{C}(G)} E$.

The fixed embedding ι is essential because some of the elements in the conjecture depend on the particular choice of the embedding: for example, the definition of the standard additive character below, see also [BlBr08, § 2.5]. So once we compute an algebraic element representing this value, we have to maintain its embedding into $\mathbb{C}$. Since we still try to avoid computations in such a big field E, this implies the following: whenever we do calculations in a subfield $F \subseteq E$, we have to choose embeddings $\iota_1 : F \hookrightarrow \mathbb{C}$ and $\iota_2 : F \hookrightarrow E$ such that the diagram

$$\begin{tikzcd} E \arrow[r, hook, "\iota"] & \mathbb{C} \\ F \arrow[u, hook, "\iota_2"] \arrow[ur, hook, "\iota_1"'] & \end{tikzcd}$$

is commutative, i.e. $\iota_1 = \iota|_F$.

We also fix a prime ideal $\mathfrak{Q}$ of E above p and an embedding $E \hookrightarrow E_{\mathfrak{Q}}$ such that $E \hookrightarrow E_{\mathfrak{Q}} \hookrightarrow \mathbb{C}_p$ and $E \overset{\iota}{\hookrightarrow} \mathbb{C} \hookrightarrow \mathbb{C}_p$ commute. Then all the invariants appearing in the conjecture lie in the subgroup $K_0(\mathbb{Z}_p[G], E_{\mathfrak{Q}})$ of $K_0(\mathbb{Z}_p[G], \mathbb{C}_p)$ and by Remark 1.39 they can therefore be represented by tuples in $\mathrm{Z}(E_{\mathfrak{Q}}[G]) \simeq \prod_{\chi\in\mathrm{Irr}(G)} E_{\mathfrak{Q}}^\times$. In fact, we will see that all these elements are also represented by elements in $\prod_{\chi\in\mathrm{Irr}(G)} E^\times$ and can be computed globally.

Computation of cohomological term

By Lemma 2.1, the lattice $\mathscr{L} = \mathbb{Z}[G]\theta \subseteq \mathcal{O}_L$ is computed using a normal basis element θ (see also [BlBr08, § 4.2.3]). The integer k for which $\mathfrak{p}^k \subseteq \mathscr{L}$ can then be found experimentally by global computations.

We compute a cocycle $\gamma \in Z^2(G, L_w^\times/U_{L_w}^{(k)})$ representing the local fundamental class up to precision k using Algorithm 2.18 and its projection in $\hat{H}^2(G, L_w^f) \simeq \hat{H}^2(G, L_w^\times)$. By Proposition 1.29 we can construct the corresponding complex $P_w = \left[L_w^f(\gamma) \to \mathbb{Z}[G]\right]$ using the splitting module $L_w^f(\gamma)$ from [NSW00, Chp. III, § 1, p. 115]. Then the Euler characteristic $E_w(\mathscr{L}_w) = \bar{\chi}_G(P_w, v_{L_w}^{-1}) \in K_0(\mathbb{Z}[G], \mathbb{Q})$ can be computed using the explicit construction from [BlBr08, § 4.2.4] as described in Example 1.44(b).

Computation of the terms in $\prod_\chi E^\times$

The correction term m_w is directly defined as tuple in $\prod_\chi E^\times$ by (5.3). For the equivariant discriminant and the unramified term we have the following formulas from [BlBr08, §§ 4.2.5 and 4.2.7]:

$$d_{L_w|\mathbb{Q}_p} = \sum_{\sigma\in G} \sigma(\theta)\sigma^{-1} \in L[G]^\times \subseteq E[G]^\times, \tag{5.8}$$

$$u_{L_w|\mathbb{Q}_p} = \sum_{i=0}^{s-1} \varphi_{\mathfrak{p}}^i(\xi)\sigma^{-i} \in N[G]^\times \subseteq E[G]^\times. \tag{5.9}$$

Hereby, $\varphi_\mathfrak{p}$ denotes the Frobenius automorphism of $N|K$ with respect to $\mathfrak{p}$, $\xi \in \mathcal{O}_N$ is an integral normal basis element for $N_\mathfrak{p}|K_\mathfrak{p}$, and σ is a lift of the local norm residue symbol $(p, F_\mathfrak{p}|K_\mathfrak{p}) \in \mathrm{Gal}(F_\mathfrak{p}|K_\mathfrak{p}) \simeq \mathrm{Gal}(F|K)$ where F is the maximal abelian subextension in $L|K$. An algorithm to compute local norm residue symbols is described in [AK00, Alg. 3.1].

These group ring elements provide elements in $K_1(\mathbb{C}_p[G])$ through the homomorphism $E[G]^\times \to K_1(\mathbb{C}_p[G])$ by $E[G] \subseteq E_\mathfrak{Q}[G] \subseteq \mathbb{C}_p[G]$. The element $u_{L_w|\mathbb{Q}_p} \in N[G]$ represents the unramified term by definition ([Bre04b, Prop. 2.12]) and $d_{L_w|\mathbb{Q}_p} \in L[G]$ represents the equivariant discriminant through the surjective homomorphism $\partial^1 : K_1(\mathbb{C}_p[G]) \to K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$ by [BlBr08, § 4.2.5].

Using the reduced norm map $\mathrm{nr} : K_1(E[G]) \hookrightarrow \mathrm{Z}(E[G])^\times$ one obtains elements in $\mathrm{Z}(E[G])^\times$ and by the *Wedderburn decomposition* $\mathrm{Z}(E[G])^\times \simeq \prod_\chi E^\times$ the equivariant discriminant and the unramified term are finally represented by tuples in $\prod_{\chi\in\mathrm{Irr}(G)} E^\times \subset \prod_{\chi\in\mathrm{Irr}(G)} E_\mathfrak{Q}^\times$.

The equivariant epsilon constant $\tau_{L_\mathfrak{p}|\mathbb{Q}_p}$ is computed in $\prod_\chi E^\times$ by *local Galois Gauss sums* as follows, cf. [BlBr08, § 2.5].

For each χ, we already computed subgroups H of G, linear characters ϕ of H, and coefficients $c_{(H,\phi)} \in \mathbb{Z}$ such that $\chi - \chi(1)1_G = \sum_{(H,\phi)} c_{(H,\phi)}\mathrm{ind}_H^G(\phi - 1_H)$ by Brauer induction. Then the Galois Gauss sum of χ can be computed by Galois Gauss sums of abelian extensions $L^{\ker(\phi)}|L^H$:

$$\tau(L_\mathfrak{p}|\mathbb{Q}_p, \chi) = \prod_{(H,\phi)} \tau\big((L^{\ker(\phi)})_\mathfrak{p}|(L^H)_\mathfrak{p}, \phi\big)^{c(H,\phi)} \in \mathbb{Q}(\zeta_m, \zeta_{p^t}) \subseteq E^\times.$$

For localizations of the abelian extension $M = L^{\ker(\phi)}$ over $N = L^H$, Galois Gauss sums are given by the formula

$$\tau(M_\mathfrak{p}|N_\mathfrak{p}, \phi) = \sum_x \phi\Big(\Big(\frac{x}{c}, M_\mathfrak{p}|N_\mathfrak{p}\Big)\Big)\, \psi_{N_\mathfrak{p}}\Big(\frac{x}{c}\Big) \in \mathbb{Q}(\zeta_m, \zeta_{p^t}) \subseteq E^\times$$

where x runs through a system of representatives of $\mathcal{O}_{N_\mathfrak{p}}^\times / U_{N_\mathfrak{p}}^{(s)} \simeq (\mathcal{O}_N/\mathfrak{p}^s)^\times$, s is the valuation $v_\mathfrak{p}(\mathfrak{f}(\phi))$ of the *Artin conductor* $\mathfrak{f}(\phi)$ of ϕ, $c \in N$ generates the ideal $\mathfrak{f}(\phi)\mathcal{D}_{N_\mathfrak{p}}$, $\mathcal{D}_{N_\mathfrak{p}}$ denotes the *different* of the extension $N_\mathfrak{p}|\mathbb{Q}_p$, and $\psi_{N_\mathfrak{p}}$ is the *standard additive character* of $N_\mathfrak{p}$.

The above formulas allow the construction of the equivariant epsilon constant as tuple $\tau_{L_\mathfrak{p}|\mathbb{Q}_p} = \big(\tau(L_\mathfrak{p}|\mathbb{Q}_p, \chi)\big)_\chi \in \prod_\chi E^\times$. For details see [BlBr08, § 2.5].

Computations in relative K-groups

In the following we have to combine the computations from the previous steps to find $R_{L_\mathfrak{p}|\mathbb{Q}_p}$ and show that its sum represents zero in $K_0(\mathbb{Z}_p[G], E_\mathfrak{Q})$. In [BW09] Bley and Wilson describe the relative K-group as an abstract group. Using their methods it will be clear how to read elements of the form $\widehat{\partial}^1_{G_w,\mathbb{Q}_p}(x)$ for $x \in \prod_\chi E^\times$ and triples $[A, \theta, B]$ in the group $K_0(\mathbb{Z}_p[G], E_\mathfrak{Q})$.

We recall the description from [BW09] for group rings and — since their algorithms are not yet implemented in full generality — we will discuss a simple modification for extensions F of $\mathbb{Q}$ which are totally split at a given prime p.

First we introduce some more notation: Let K be a number field and G a finite group. The *Wedderburn decomposition* of $K[G]$ gives a decomposition of its center $C := \mathrm{Z}(K[G])$ into character fields K_i such that $C = \bigoplus_{i=1}^r K_i$. Each character field K_i corresponds to an irreducible character $\chi_i \in \mathrm{Irr}_K(G)$ and K_i is the field $K(\chi_i)$ which is obtained from K by adjoining the values of χ_i.

Choose a maximal $\mathcal{O}_K$-order $\mathcal{M}$ of $K[G]$ containing $\mathcal{O}_K[G]$ and a two-sided ideal $\mathfrak{f}$ of $\mathcal{M}$ which is included in $\mathcal{O}_K[G]$ (e.g. $\mathfrak{f} = |G|\,\mathcal{M}$) and define $\mathfrak{g} := \mathcal{O}_C \cap \mathfrak{f}$. Then the decomposition of C similarly splits $\mathcal{M}$ into $\bigoplus_{i=1}^r \mathcal{M}_i$ and the ideals $\mathfrak{f}$ and $\mathfrak{g}$ into ideals $\mathfrak{f}_i$ of $\mathcal{M}_i$ and $\mathfrak{g}_i$ of $\mathcal{O}_{K_i}$. For a prime $\mathfrak{p}$ in $\mathcal{O}_K$, we further write $C_\mathfrak{p}$ for the localization $C_\mathfrak{p} = K_\mathfrak{p} \otimes_\mathbb{Q} C = \bigoplus_{i=1}^r K_\mathfrak{p} \otimes_\mathbb{Q} K_i = \bigoplus_{i=1}^r \bigoplus_{\mathfrak{P}|\mathfrak{p}} (K_i)_\mathfrak{P}$, and $\mathfrak{a}_{i,\mathfrak{p}}$ for the part of an ideal $\mathfrak{a}_i$ of $\mathcal{O}_{K_i}$ above $\mathfrak{p}$.

The reduced norm map induces a homomorphism $\mu_\mathfrak{p} : K_1(\mathcal{O}_{K_\mathfrak{p}}[G]/\mathfrak{f}_\mathfrak{p}) \to \bigoplus_{i=1}^r (\mathcal{O}_{K_i}/\mathfrak{g}_{i,\mathfrak{p}})^\times$ whose cokernel is used in the description of the relative K-group $K_0(\mathcal{O}_{K_\mathfrak{p}}[G], K_\mathfrak{p})$.

Then the main result of Bley and Wilson is the following.

Proposition 5.13. *There are isomorphisms*

$$K_0(\mathcal{O}_{K_\mathfrak{p}}[G], K_\mathfrak{p}) \xrightarrow{\bar{n}} C_\mathfrak{p}^\times / \mathrm{nr}(\mathcal{O}_{K_\mathfrak{p}}[G]^\times) \xrightarrow{\bar{\varphi}} I(C_\mathfrak{p}) \times \mathrm{coker}(\mu_\mathfrak{p}),$$

$\bar{n}$ being a natural isomorphism and $\bar{\varphi}$ being induced by

$$\begin{aligned} \varphi:\quad C_\mathfrak{p}^\times = \bigoplus_{i=1}^r (K_i)_\mathfrak{p} \quad &\longrightarrow \quad I(C_\mathfrak{p}) \times \bigoplus_{i=1}^r (\mathcal{O}_{K_i}/\mathfrak{g}_{i,\mathfrak{p}})^\times \\ (\nu_1, \dots, \nu_r) \quad &\longmapsto \quad \Big(\big(\textstyle\prod_\mathfrak{P} \mathfrak{P}^{v_\mathfrak{P}(\nu_i)} \big)_i, (\bar{\mu}_1, \dots, \bar{\mu}_r) \Big), \end{aligned} \tag{5.10}$$

where $\mu_i := \nu_i \prod_\mathfrak{P} \pi_{i,\mathfrak{P}}^{-v_\mathfrak{P}(\nu_i)}$ and $\pi_{i,\mathfrak{P}} \in \mathcal{O}_{K_i}$ are uniformizing elements having valuation 1 at $\mathfrak{P}$ and which are congruent to 1 modulo $\mathfrak{g}_{\mathfrak{P}'}$ for all other primes $\mathfrak{P}'$ above $\mathfrak{p}$ in $K_i|K$.

Proof. [BW09, Prop. 2.7]. □

Bley and Wilson describe an algorithm to compute the group $I(C_\mathfrak{p}) \times \mathrm{coker}(\mu_\mathfrak{p})$ From the definition of φ, it is clear how a tuple $\nu = (\nu_i)_i$ of elements with values $\nu_i \in K_i$ represents an element in this group. Furthermore, for every triple $[A, \theta, B] \in K_0(\mathcal{O}_K[G], K)$ with projective $\mathcal{O}_K[G]$-modules A and B and $\theta : A_K \xrightarrow{\simeq} B_K$, one can compute a representative of $[A_\mathfrak{p}, \theta_\mathfrak{p}, B_\mathfrak{p}]$ in this group as follows. As discussed in Remark 1.39 every element $[A_\mathfrak{p}, \theta_\mathfrak{p}, B_\mathfrak{p}]$ is represented by an element in $K_1(K_\mathfrak{p}[G])$ by choosing $\mathcal{O}_{K_\mathfrak{p}}[G]$-bases of $A_\mathfrak{p}$ and $B_\mathfrak{p}$ and computing a matrix in $\mathrm{Gl}_n(K_\mathfrak{p}[G])$ which represents the isomorphism $\theta_\mathfrak{p}$ with respect to this basis. From the reduced norm map $\mathrm{nr} : K_1(K_\mathfrak{p}[G]) \xrightarrow{\simeq} \mathrm{Z}(K_\mathfrak{p}[G])$ one then obtains a representative in $C_\mathfrak{p}^\times$ and applying $\bar{\varphi}$ finally provides the element in $I(C_\mathfrak{p}) \times \mathrm{coker}(\mu_\mathfrak{p})$ which corresponds to $[A_\mathfrak{p}, \theta_\mathfrak{p}, B_\mathfrak{p}]$. For details we refer to [BW09, § 4].

In theory, this solves the remaining problems for Algorithm 5.12. But in practice, this has only been implemented in Magma for $K = \mathbb{Q}$ and $\mathfrak{p} = p\mathbb{Z}$. In our case, however, we have to work with the decomposition field $F \subseteq E$ of $\mathfrak{Q}$. This field F is a global extension of $\mathbb{Q}$ which is totally split at p. Then for any prime $\mathfrak{q}|p$ we obviously have $F_\mathfrak{q} = \mathbb{Q}_p$ and $K_0(\mathbb{Z}_p[G], F_\mathfrak{q}) \simeq K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$. If F satisfies certain conditions, this isomorphism of relative K-groups is canonically given by isomorphisms on the ideal part $I(C_\mathfrak{p})$ and the cokernel part $\mathrm{coker}(\mu_\mathfrak{p})$.

Proposition 5.14. *Let $F|\mathbb{Q}$ be a number field which is totally split at p and for which $F \cap K_i = K = \mathbb{Q}$ for all i. Let $\mathfrak{q}$ be a fixed prime ideal of F above p. Then the following holds:*

(i) The center $C' = \mathrm{Z}(F[G])$ splits into character fields $F_i = FK_i$.

(ii) For every ideal $\mathfrak{P}$ of K_i there is exactly one prime ideal $\mathfrak{Q}$ in F_i lying above $\mathfrak{P}$ and $\mathfrak{q}$.

(iii) There are canonical isomorphisms

$$I(C_\mathfrak{p}) \simeq I(C'_\mathfrak{q}) \quad \text{and} \quad \bigoplus_{i=1}^{r} (\mathcal{O}_{K_i}/\mathfrak{g}_{i,\mathfrak{p}})^\times \simeq \bigoplus_{i=1}^{r} (\mathcal{O}_{F_i}/\mathfrak{h}_{i,\mathfrak{q}})^\times$$

where $\mathfrak{h} := \mathcal{O}_{C'} \cap \mathfrak{f}$.

Proof. (i) The character fields K_i arise from $K = \mathbb{Q}$ by adjoining the values of a specific character in $\mathrm{Irr}_\mathbb{Q}(G)$. Since F and K_i are disjoint over $\mathbb{Q}$, one has the same irreducible characters over F: $\mathrm{Irr}_\mathbb{Q}(G) = \mathrm{Irr}_F(G)$. The character fields F_i then arise by adjoining the same character values and $F_i = FK_i$.

(ii) If $\mathfrak{Q}'$ is any prime ideal in F_i above $\mathfrak{p}$ and $\mathfrak{P}' = \mathfrak{Q}' \cap K_i$, $\mathfrak{q}' = \mathfrak{Q}' \cap F$, then the automorphisms τ and σ for which $\tau(\mathfrak{P}') = \mathfrak{P}$ and $\sigma(\mathfrak{q}') = \mathfrak{q}$ define an element $\rho = \sigma \times \tau$ in the Galois group of $F_i|\mathbb{Q}$ and $\mathfrak{Q} = \rho(\mathfrak{Q}')$ is a prime ideal which lies above both $\mathfrak{P}$ and $\mathfrak{q}$. The uniqueness of $\mathfrak{Q}$ follows from degree arguments.

(iii) Let $\mathfrak{P}$ be a prime ideal of K_i and $\mathfrak{Q}$ the prime ideal of F_i which lies above $\mathfrak{q}$ and $\mathfrak{P}$. Then the valuation $v_\mathfrak{Q}$ of F_i extends the valuation $v_\mathfrak{P}$ of K_i and if we identify each pair $(\mathfrak{P}, \mathfrak{Q})$, we get an isomorphism

$$I(C_\mathfrak{p}) = \prod_{i=1}^{r} \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^\mathbb{Z} \simeq \prod_{i=1}^{r} \prod_{\mathfrak{Q}|\mathfrak{q}} \mathfrak{Q}^\mathbb{Z} = I(C'_\mathfrak{q}).$$

Since $\mathfrak{P} \subset K_i$ is totally split in F_i we have isomorphisms $\mathcal{O}_{K_i}/\mathfrak{P} \simeq \mathcal{O}_{F_i}/\mathfrak{Q}$. Moreover, the $\mathfrak{q}$-part of $\mathfrak{h}$ is given by the part of $\mathfrak{g}\mathcal{O}_{C'}$ lying above $\mathfrak{q}$. The inclusions $\mathcal{O}_{K_i} \subseteq \mathcal{O}_{F_i}$ therefore induce isomorphisms $(\mathcal{O}_{K_i}/\mathfrak{g}_{i,\mathfrak{p}})^\times \simeq (\mathcal{O}_{F_i}/\mathfrak{h}_{i,\mathfrak{q}})^\times$. □

Remarks 5.15. 1. As mentioned before, the algorithms from [BW09] to compute $K_0(\mathbb{Z}_p[G], F_\mathfrak{q})$ are just implemented for $F = \mathbb{Q}$. The extension to $F|\mathbb{Q}$ described above will work if F is totally split at p and $F \cap \mathbb{Q}(\chi) = \mathbb{Q}$ for all characters χ. The first condition is always true since we want to work with the decomposition field $F \subseteq E$ of $\mathfrak{Q}$, and the latter condition is valid in all cases we consider in the computational results below.

2. The computation of the prime ideal $\mathfrak{Q}$ in E is a though job when the degree of E gets large. In the last part of Algorithm 5.12 we will therefore proceed as follows.

Let $\mathcal{I} := \tau_{L_w|\mathbb{Q}_p} u_{L_w|\mathbb{Q}_p}/(m_w d_{L_w|\mathbb{Q}_p}) \in \prod_\chi E^\times$ be the element combining all the invariants except the cohomological term. Then $R_{L_w|K_v} = \widehat{\partial}^1_{G_w,E_\mathfrak{Q}}(\mathcal{I}) + E_w(\mathscr{L}_w)_p$. Since $R_{L_w|K_v}$ and $E_w(\mathscr{L}_w)_p$ are both elements of $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$, the element $\widehat{\partial}^1_{G_w,E_\mathfrak{Q}}(\mathcal{I})$ is also in $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$. Hence, $\mathcal{I} \in \mathrm{Z}(\mathbb{Q}_p[G])^\times$ and each component $\mathcal{I}_\chi \in \mathbb{Q}_p(\zeta_m)$, $m = \exp(G)$. Since each component $\mathcal{I}_\chi$ is determined by a global element in E, we have $\mathcal{I}_\chi \in F' := \mathbb{Q}_p(\zeta_m) \cap E$. Here, the intersection is taken in the fixed completion of the algebraic closure $\mathbb{C}_p$ of $E_\mathfrak{Q}$. We therefore obtain $\mathcal{I} \in \mathrm{Z}(F'[G])^\times \simeq \prod_\chi (F')^\times$ and if $F = E^{G_\mathfrak{Q}}$ denotes the decomposition field of $\mathfrak{Q}$, then $F' = F(\zeta_m)$.

As mentioned above, we want to omit the computation of $\mathfrak{Q}$. So instead of working with E, we would like to work with a small subfield of E. The field $F' = F(\zeta_m)$ would be a good choice but this still involves the computation of the decomposition field of $\mathfrak{Q}$ and hence also the computation of $\mathfrak{Q}$ itself.

Instead we continue as follows: for every χ we compute the minimal polynomial m_χ of $\mathcal{I}_\chi$. Then we compute the composite field F' of the splitting fields of the polynomials m_χ with $\mathbb{Q}(\zeta_m)$. Although the computation of the splitting fields is also a difficult task, we note that these fields will always be subfields of E and where this approach could take hours, the computation of $\mathfrak{Q}$ did not succeed in several days.

In the end, F' is the composite field such that $\mathcal{I}_\chi, \zeta_m \in F'$. Compute the ideal $\mathfrak{q}'$ of F' above p, denote the decomposition field of $\mathfrak{q}'$ by F, and compute $\mathfrak{q} = \mathcal{O}_F \cap \mathfrak{q}'$. Then it follows from above that $\mathcal{I}_\chi \in F(\zeta_m)$ and $\mathcal{I} = \tau_{L_w|\mathbb{Q}_p} u_{L_w|\mathbb{Q}_p}/(m_w d_{L_w|\mathbb{Q}_p}) \in \prod_\chi F(\zeta_m)^\times$.

Note that all computations were independent of the choice of the prime ideal $\mathfrak{Q}$ above p because all invariants were actually computed globally. The proof of the conjecture will therefore also be independent of the choice of $\mathfrak{q}'$.

5.5 Computational results

Algorithm 5.12 has been implemented in Magma [BCP97], see Appendix B.4, and has been tested for various extensions up to degree 20. The computation time especially depends on the degree of the composite field E.

The most complicated number field for which we proved the local epsilon constant conjecture was an extension of degree 10 of $\mathbb{Q}_5$ with Galois group D_5. The composite field E then had degree 200 over $\mathbb{Q}$. The computation of the epsilon constants, which needs an embeddings $E \hookrightarrow \mathbb{C}$, already took about 7 hours, but the most time-consuming part (about 6.5 days) of Algorithm 5.12 was the computation of minimal polynomials and their splitting field mentioned in Remark 5.15. The field F' then just had degree 4 over $\mathbb{Q}$ making the remaining computations very fast. The total time needed to prove the local conjecture in this case was about 7 days.

Using the global representations obtained in Section 5.3 we can prove the following algorithmic result.

Theorem 5.16. *The local epsilon constant conjecture is valid for all wildly ramified, non-abelian Galois extensions $M|\mathbb{Q}_p$ with degree $[M : \mathbb{Q}_p] \leq 15$ and for all abelian extensions $M|\mathbb{Q}_2$ with $[M : \mathbb{Q}_p] \leq 6$.*

Proof. Since the local conjecture is valid for abelian extensions of $\mathbb{Q}_p$, $p \neq 2$, the only primes to consider are $p = 2, 3, 5, 7$. All local extensions for these primes of degree ≤ 15 that are either non-abelian, or abelian with $p = 2$ have been considered in Section 5.3.2 and global representations have been found by using the heuristics described in Section 5.3.1. Also global representations for the corresponding unramified extensions — which are of degree at most 6 — could be found using the database [KM01].

For each of those extensions we then continued with Algorithm 5.12 to prove the local epsilon constant conjecture computationally.[4] This completes the proof. □

Corollary 5.17. *The local epsilon constant conjecture is valid for all Galois extensions*

(a) $M|\mathbb{Q}_p$, $p \neq 2$ of degree $[M : \mathbb{Q}_p] \leq 15$,

(b) $M|\mathbb{Q}_2$ non-abelian and of degree $[M : \mathbb{Q}_p] \leq 15$,

(c) $M|\mathbb{Q}_2$ of degree $[M : \mathbb{Q}_p] \leq 7$.

[4] A list of polynomials generating the global representations and a few details on each computational proof is given in Appendix A.2.

Proof. The cases not considered in the theorem above are extensions of $\mathbb{Q}_p$, $p \neq 2$ which are either tamely ramified or have abelian Galois group, and extensions of $\mathbb{Q}_2$ which are tamely ramified. These cases have already been proved before (see page 114). Note that for degree 7 there is just one extension of $\mathbb{Q}_2$ which is also tamely ramified. □

Combining Algorithm 5.12 with the local-global principle (Theorem 5.6) the functorial properties (Proposition 5.7) and known results for tame extensions and abelian extensions, we obtain an algorithm to prove the global epsilon constant conjecture for number field extensions $L|\mathbb{Q}$ up to a finite degree as described on page 114. Then the above results for the local epsilon constant conjecture imply the following result for global fields.

Corollary 5.18. *The global epsilon constant conjecture is valid for all Galois extensions L of $\mathbb{Q}$ with degree $[L : \mathbb{Q}] \leq 15$.*

Proof. If $L|\mathbb{Q}$ is abelian, the global conjecture is already known to be valid. For the non-abelian case, we recall that by Theorem 5.6 conjecture $\mathrm{EPS}(L|\mathbb{Q})$ is valid if $\mathrm{EPS}^{\mathrm{loc}}(L_w|\mathbb{Q}_p)$ is valid for all primes p and places $w|p$. If $L|\mathbb{Q}$ is non-abelian of degree ≤ 15, the local extension $L_w|\mathbb{Q}_p$ is either non-abelian of degree at most 15 or abelian of degree at most 7. Therefore the result follows from Corollary 5.17. □

The projection onto the class group also proves Chinburg's conjecture.

Corollary 5.19. *Chinburg's $\Omega(2)$-conjecture from [Chi85, Question 3.1] is valid for all Galois extensions L of $\mathbb{Q}$ with degree $[L : \mathbb{Q}] \leq 15$.*

Moreover, the functorial properties for global epsilon constant conjectures state that the conjecture for $L|K$ implies the conjecture for $E|F$ in a tower $L|E|F|K$ of number field extensions in which $L|K$ and $E|F$ are Galois. This proves the following result.

Corollary 5.20. *The global epsilon constant conjecture and Chinburg's $\Omega(2)$-conjecture are valid for Galois extensions $E|F$ of number fields for which E is contained in a Galois extension $L|\mathbb{Q}$ with $[L : \mathbb{Q}] \leq 15$.*

6 The equivariant Tamagawa number conjecture at $s = 1$

The equivariant Tamagawa number conjecture for a Galois extension $L|K$ of number fields with group G relates the leading term of the equivariant Artin L-function to algebraic invariants of the extension $L|K$. There are two instances of this conjecture, denoted by $\mathrm{ETNC}(L|K, 0)$ and $\mathrm{ETNC}(L|K, 1)$, which consider the leading coefficient at $s = 0$ and $s = 1$, respectively.

The conjecture at $s = 0$ relates the leading term $\zeta^*_{L|K,S}(0)$ for a finite set of places S to an invariant which is constructed from a Tate sequence for $L|K$. An algorithm which verifies this conjecture up to the precision of the computation and which also gives a proof in special cases was discussed by Janssen in [Jan10].

The conjecture at $s = 1$ relates the value $\zeta^*_{L|K,S}(1)$ for a finite set of places S to invariants based on the global fundamental class $u_{L|K} \in \hat{H}^2(G, C_L)$. Although the validity of $\mathrm{ETNC}(L|K, 0)$ and the compatibility conjecture $\mathrm{ETNC}^{\mathrm{loc}}(L|K, 1)$ discussed in the previous chapter imply the conjecture $\mathrm{ETNC}(L|K, 1)$, the latter conjecture is still of interest because the algorithm in [Jan10] was just implemented using the construction of Tate's canonical class in the special case described in Section 4.5, which assumes the existence of a place of K which is undecomposed in L. For the general case one can construct the Tate sequence using Algorithm 4.12. But that algorithm depends on the construction of the global fundamental class, and it makes therefore sense to consider $\mathrm{ETNC}(L|K, 1)$ directly.

In this chapter, we recall the statement of the equivariant Tamagawa number conjecture at $s = 1$ for number fields as it is given in [BrB07, § 3] and develop an algorithm which verifies $\mathrm{ETNC}(L|K, 1)$ numerically.

Let $L|K$ be a fixed Galois extension of number fields with group G. As usual, we denote a finite, Galois-invariant set of places in L by S. The places of K below the places of S will again be denoted by S, but we avoid confusion by denoting places in L by w and those in K by v:

$$\begin{tikzcd} L \arrow[d, dash] \arrow[d, bend right=60, dash, "G"'] & w \arrow[d, dash] \\ K & v \end{tikzcd}$$

Again, for every place v we will choose a fixed place $w \in S$ dividing v. In other words, we fix a set $S(G)$ of representatives of the G-orbits in S.

6.1 Statement of the conjecture

The *analytic part* of the conjecture will be given by the leading term $\zeta^*_{L|K,S}(1)$ of the equivariant S-truncated Artin L-function $\zeta_{L|K,S}(s)$ in the Laurent series expansion at $s = 1$. See Section 1.5 for a definition of $\zeta_{L|K,S}(s)$. To define the *algebraic part,* we again have to make some choices and have to introduce more notation.

Let S be a finite set of places of L containing the infinite places, all places which ramify in $L|K$ and let S be such that the S-ideal class group $Cl_S(L)$ is trivial. For each $w \in S(G)$ and $w|v$ we choose a full projective sublattice $\mathscr{L}_w \subseteq \mathcal{O}_{L_w}$ upon which the exponential map is defined and, as for epsilon constant conjectures, we define the lattice $\mathscr{L} \subseteq \mathcal{O}_L$ by its p-adic completions

$$\mathscr{L}_p = \prod_{v|p} \mathscr{L}_w \otimes_{\mathbb{Z}_p[G_w]} \mathbb{Z}_p[G] \subseteq L_p := L \otimes_{\mathbb{Q}} \mathbb{Q}_p,$$

where w is the fixed place above v.

Furthermore, we consider the G-modules $L_S = \prod_{v\in S} L_v = \prod_{w\in S(G)} \mathrm{ind}_{G_w}^G L_w$ and $\mathscr{L}_S = \prod_{w\in S(G)} \mathrm{ind}_{G_w}^G \mathscr{L}_w = \prod_{w\in S(G)} \mathscr{L}_w \otimes_{\mathbb{Z}_p[G_w]} \mathbb{Z}_p[G]$ where $\mathscr{L}_w = L_w$ for all infinite places w. The diagonal embedding of L into L_S will be denoted by Δ_S, and $\exp_S : \mathscr{L}_S \to L_S^\times$ is the (p-adic, real or complex) exponential map on each component.[1]

We will also consider restrictions to finite or infinite places: we set $L_f = \prod_{v\in S_f} L_v$, $\mathscr{L}_f = \prod_{v\in S_f} \mathscr{L}_v$, $L_\infty = \prod_{v\in S_\infty} L_v$, and use the maps $\Delta_\infty : L \to L_\infty$ and $\exp_\infty : L_\infty \to L_\infty^\times$.

As in Chapter 3 the *S-idèle class group* will be denoted by $C_S(L)$. It was defined as the quotient of the idèle group I_L by $U_{L,S} = \prod_{v\in S}\{1\} \times \prod_{v\notin S} \mathcal{O}_{L_v}^\times \subseteq I_L$. Let $E_S = \big[A \to B\big]$ be a complex representing the global fundamental class in $\mathrm{Yext}_G^2(\mathbb{Z}, C_S(L)) \simeq \hat{H}^2(G, C_S(L))$ with A and B cohomologically trivial $\mathbb{Z}[G]$-modules. It is a complex which is trivial outside degrees 0 and 1 and has cohomology groups $H^0(E_S) = C_S(L)$ and $H^1(E_S) = \mathbb{Z}$.

Moreover, consider the complex $\big[\mathscr{L}_S \xrightarrow{0} \mathscr{L}\big]$ with $\mathscr{L}_S$ in degree 0 and a chain map $\alpha : \big[\mathscr{L}_S \xrightarrow{0} \mathscr{L}\big] \to E_S$ given by $\mathscr{L}_S \xrightarrow{\exp_S} L_S^\times \to C_S(L) \subseteq A$ in degree 0 and a lift tr' of $\mathrm{tr}_{L|\mathbb{Q}} : \mathscr{L} \to \mathbb{Z}$ in degree 1 via the surjection $B \twoheadrightarrow \mathbb{Z}$. These maps can be summarized in the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & \mathscr{L}_S \arrow[r, "\mathrm{id}"] \arrow[d, "\exp_S"] & \mathscr{L}_S \arrow[r, "0"] \arrow[d] & \mathscr{L} \arrow[r, "\mathrm{id}"] \arrow[d, "\mathrm{tr}'"] & \mathscr{L} \arrow[r] \arrow[d, "\mathrm{tr}_{L|\mathbb{Q}}"] & 0 \\
0 \arrow[r] & C_S(L) \arrow[r, "\subseteq"] & A \arrow[r] & B \arrow[r] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd} \tag{6.1}$$

Then the algebraic part of the conjecture will depend on the cone $E_S(\mathscr{L})$ of α.

[1]Note that the units $L_S^\times$ where denoted by $I_{L,S}$ in Chapters 3 and 4.

It is the complex $E_S(\mathscr{L}) = \big[\mathscr{L}_S \xrightarrow{\exp} A \oplus \mathscr{L} \longrightarrow B\big]$ with $\mathscr{L}_S$ in degree -1 and where the differential in degree zero is the sum of the maps $A \to B$ and tr'.

To describe the cohomology of $E_S(\mathscr{L}) = \mathrm{cone}(\alpha)$, we introduce the following notations: consider the map

$$\begin{aligned} \mathrm{tr}_\infty : \qquad L_\infty \quad &\to \quad \mathbb{R} \\ (l_w)_{w\in S_\infty} &\mapsto \textstyle\sum_{w\in S_\infty} \mathrm{tr}_{L_w|\mathbb{R}}(l_w) \end{aligned}$$

and denote the kernels of the trace maps by $L^0_\infty := \ker(\mathrm{tr}_\infty)$ and $L^0 := \ker(\mathrm{tr}_{L|\mathbb{Q}})$. Then one has an exact commutative diagram of $\mathbb{R}[G]$-modules

$$\begin{tikzcd} 0 \arrow[r] & L^0 \otimes_{\mathbb{Q}} \mathbb{R} \arrow[r, "\subseteq"] \arrow[d, "\mu_L"] & L \otimes_{\mathbb{Q}} \mathbb{R} \arrow[r, "\mathrm{tr}_{L|\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{R}"] \arrow[d, "\mu'_L"] & \mathbb{R} \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & L^0_\infty \arrow[r, "\subseteq"] & L_\infty \arrow[r, "\mathrm{tr}_\infty"] & \mathbb{R} \arrow[r] & 0 \end{tikzcd}$$

where μ_L is the restriction of the canonical isomorphism

$$\begin{aligned} \mu'_L : L \otimes_{\mathbb{Q}} \mathbb{R} &\to L_\infty \\ l \otimes x &\mapsto (\sigma_w(l)x)_{w\in S_\infty} \end{aligned}$$

given by embeddings $\sigma_w : L \to L_w$ for all infinite places w.

Remark 6.1. Let r_1 and r_2 denote the number of real and pairs of complex embeddings. Then we can also identify L_∞ with

$$\big\{(x_i) \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} \mid \overline{x_{r_1+j}} = x_{r_1+r_2+j}, 1 \le j \le r_2\big\} \subseteq \mathbb{C}^{r_1+2r_2}.$$

We also denote the corresponding real embeddings by $\sigma_1, \dots, \sigma_{r_1}$ and the complex pairs by $\sigma_{r_1+j}, \overline{\sigma_{r_1+j}} = \sigma_{r_1+r_2+j}$ for $1 \le j \le r_2$.

Finally, for any subset $X \subseteq L_\infty^\times$ we let $\log_\infty(X) = \{x \in L_\infty \,|\, \exp_\infty(x) \in X\}$ denote the full preimage of X in L_∞ through $\exp_\infty$. And for $U \subseteq \mathcal{O}_L^\times$ it is defined by

$$\log_\infty(U) = \{x \in L_\infty \mid \exp_\infty(x) \in \Delta_\infty(U)\} \subseteq L_\infty$$

which is equal to $\log_\infty(\Delta_\infty(U))$.

Remark 6.2. The subgroup of totally positive units in $\mathcal{O}_L^\times$, denoted by $\mathcal{O}_L^+$, has finite $\mathbb{Z}$-index in $\mathcal{O}_L^\times$. Let U be a full lattice in $\mathcal{O}_L^+$. Then the homomorphism $\exp_\infty : \log_\infty(U) \to \Delta_\infty(U)$ is surjective (on every component) and we obtain an exact sequence

$$0 \longrightarrow \Gamma_1 \longrightarrow \log_\infty(U) \xrightarrow{\exp_\infty} \Delta_\infty(U) \longrightarrow 0$$

which is also given in [Tat84, Chp. I, § 8]. The kernel Γ_1 corresponds to the kernel of the exponential function for complex places in L_∞:

$$\Gamma_1 = \prod_{w\in S(\mathbb{R})} 0 \times \prod_{w\in S(\mathbb{C})} 2\pi i\mathbb{Z} \subset L_\infty.$$

Using the identification of the remark above, the elements of $(x_\sigma) \in \Gamma_1$ are zero at real places, and for complex embeddings σ one has $\overline{x_\sigma} = x_{\bar\sigma} \in 2\pi\mathrm{i}\mathbb{Z}$.

By Dirichlet's unit theorem, the group U has rank $r+s-1$ and therefore $\log_\infty(U)$ has rank $r+2s-1$. If $U = \langle \varepsilon_1, \ldots, \varepsilon_t \rangle_{\mathbb{Z}}$, then the group $\log_\infty(U)$ is a lattice in L_∞ which is generated by the elements

$$\begin{array}{ll} \big(\log \sigma_k(\varepsilon_j)\big)_{k=1\ldots n} & 1 \le j \le t, \\ \big(2\pi\mathrm{i}(\delta_{jk} - \delta_{(j+r_2)k})\big)_{k=1\ldots n} & r_1+1 \le j \le r_1+r_2 \end{array}$$

with $\delta_{jk} = 1$ for $j = k$ and $\delta_{ij} = 0$ otherwise.

Lemma 6.3. *The set* $\log_\infty(\mathcal{O}_L^\times) \subseteq L_\infty$ *is a full lattice in* L_∞^0.

Proof. Let r_1 denote the number of real embeddings of L, r_2 the number of pairs of complex embeddings, and let τ run through $r_1 + r_2$ embeddings $L \hookrightarrow \mathbb{C}$ by choosing one of each complex pair. By the proof of Dirichlet's unit theorem [Neu92, Chp. I, § 5] there is a commutative diagram

$$\begin{array}{ccc} L^\times & \xrightarrow{l \circ \Delta_\infty} & \prod_\tau \mathbb{R} \\ \downarrow{\scriptstyle \mathrm{N}_{L|\mathbb{Q}}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q}^\times & \xrightarrow{x \mapsto \log|x|} & \mathbb{R} \end{array}$$

in which Tr is the map which adds all components, and l denotes the map $(x_\tau)_\tau \mapsto (\lambda_\tau \log|x_\tau|)_\tau$ with $\lambda_\tau = 1$ for real and $\lambda_\tau = 2$ for complex embeddings τ. The commutativity shows that $\log_\infty(\mathcal{O}_L^\times) \subseteq L_\infty^0$.

Then the remark above and the fact that $\mathcal{O}_L^+$ has finite index in $\mathcal{O}_L^\times$ imply that $\log_\infty(\mathcal{O}_L^\times)$ is a lattice of rank $r_1 + 2r_2 - 1$ and therefore a full lattice in L_∞^0. □

Recall that for a perfect complex P and a *trivialization* $t : H^+(P)_\mathbb{R} \to H^-(P)_\mathbb{R}$, the Euler characteristic in $K_0(\mathbb{Z}[G], \mathbb{R})$ introduced in Section 1.4.2 was denoted by $\chi_G(P, t)$.

Proposition 6.4. *The complex* $E_S(\mathscr{L})$ *has the following properties:*

(a) It is a perfect complex of $\mathbb{Z}[G]$*-modules.*

(b) The complex $E_S(\mathscr{L}) \otimes \mathbb{Q}$ *is acyclic outside degrees* -1 *and* 0 *and has cohomology* $H^{-1}(E_S(\mathscr{L})) \otimes \mathbb{Q} \simeq \log_\infty(\mathcal{O}_L^\times) \otimes \mathbb{Q}$ *and* $H^0(E_S(\mathscr{L})) \otimes \mathbb{Q} \simeq L^0$.

(c) The canonical isomorphism $\log_\infty(\mathcal{O}_L^\times) \otimes \mathbb{R} \simeq L_\infty^0$ *induces a trivialization* μ_L *of* $E_S(\mathscr{L})$ *and the Euler characteristic* $\chi_G(E_S(\mathscr{L}), \mu_L)$ *depends only on* $L|K$ *and* S.

Proof. [BrB07, Lem. 3.1]. □

The explicit construction of the cohomology groups and the canonical trivialization obtained from the proof will be considered in detail in Section 6.2 below. For now we use the Euler characteristic to define the element

$$T\Omega(L|K,1) := \widehat{\partial}_G^1\big(\zeta^*_{L|K,S}(1)\big) + \chi_G(E_S(\mathscr{L}),\mu_L) \in K_0(\mathbb{Z}[G],\mathbb{R}).$$

which can be proved to depend only upon the extension $L|K$, cf. [BrB07, Prop. 3.4].

Conjecture 6.5. *For any Galois extension $L|K$ of number fields the element $T\Omega(L|K,1)$ is zero in $K_0(\mathbb{Z}[G],\mathbb{R})$.*

We will denote this conjecture by $\mathrm{ETNC}(L|K,1)$. It implies conjectures of Stark and Chinburg as follows.

Proposition 6.6. *(a) $T\Omega(L|K,1) \in K_0(\mathbb{Z}[G],\mathbb{Q})$ if and only if the Stark conjecture at $s=1$ from [Tat84, Chp. I, Conj. 8.2] is valid for $L|K$.*

(b) $T\Omega(L|K,1) \in \ker\big(\partial_G^0 : K_0(\mathbb{Z}[G],\mathbb{R}) \to K_0(\mathbb{Z}[G])\big)$ if and only if Chinburg's Ω_1-conjecture stated in [Chi85, Question 3.2] is valid for $L|K$ (see also [CCFT91, §4.2, Conj. 3]).

Proof. [BrB07, Prop. 3.6]. □

The fact that $T\Omega(L|K,1)$ lies in the subgroup $K_0(\mathbb{Z}[G],\mathbb{Q})$ of $K_0(\mathbb{Z}[G],\mathbb{R})$ can be regarded as an independent conjecture, called the *rationality conjecture.* By the above proposition the rationality conjecture is equivalent to Stark's conjecture. As in Proposition 5.7 we have the following functorial properties:

Proposition 6.7. *For a Galois extension $L|K$ of number fields with intermediate field $F|K$:*

(i) $\mathrm{ETNC}(L|K,1) \Rightarrow \mathrm{ETNC}(L|F,1)$*, and*

(ii) $\mathrm{ETNC}(L|K,1) \Rightarrow \mathrm{ETNC}(F|K,1)$ *if $F|K$ is Galois.*

Proof. [BrB07, Prop. 3.5]. □

We now want to consider this conjecture computationally. However, we cannot construct the complex $E_S(\mathscr{L})$ itself since it does not consist of finitely generated modules. Being a perfect complex, we know that $E_S(\mathscr{L})$ is quasi-isomorphic to a bounded complex P of finitely generated, projective modules. There are constructive methods (e.g. see Proposition 1.38) to find such a complex, but it is not clear how to apply them explicitly since the modules in $E_S(\mathscr{L})$ are not finitely generated.

In the following sections we use the finite approximation of the idèle class group from Section 3.1 to compute such a complex P and this will also provide an explicit construction of the Euler characteristic $\chi_G(E_S(\mathscr{L}),\mu_L)$.

6.2 Cohomology of $E_S(\mathscr{L})$

We investigate the proof of Proposition 6.4 from [BrB07, Lem. 3.1] to compute the cohomology of $E_S(\mathscr{L})$ explicitly. The cohomology groups of the distinguished triangle $\left[\mathscr{L}_S \xrightarrow{0} \mathscr{L}\right] \to E_S \to E_S(\mathscr{L})$ give rise to a long exact sequence of cohomology groups

$$\begin{aligned} 0 \longrightarrow H^{-1}(E_S(\mathscr{L})) \longrightarrow \mathscr{L}_S \xrightarrow{\exp_S} C_S(L) \longrightarrow \\ H^0(E_S(\mathscr{L})) \longrightarrow \mathscr{L} \xrightarrow{\operatorname{tr}_{L|\mathbb{Q}}} \mathbb{Z} \longrightarrow H^1(E_S(\mathscr{L})) \longrightarrow 0. \end{aligned} \tag{6.2}$$

from which one can compute the cohomology.

Therefore $H^1(E_S(\mathscr{L})) = \mathbb{Z}/\operatorname{tr}_{L|\mathbb{Q}}(\mathscr{L})$, $H^{-1}(E_S(\mathscr{L})) = \ker(\mathscr{L}_S \to C_S(L))$, and in degree zero there is a short exact sequence

$$0 \longrightarrow \operatorname{coker}\big(\mathscr{L}_S \to C_S(L)\big) \longrightarrow H^0(E_S(\mathscr{L})) \longrightarrow \ker(\operatorname{tr}_{L|\mathbb{Q}}) \longrightarrow 0.$$

Since the kernel and cokernel of the trace map can be computed explicitly, it remains to investigate the kernel and cokernel of the map $\mathscr{L}_S \to C_S(L)$ which is the composite of $\exp_S : \mathscr{L}_S \to L_S^\times$ and $L_S^\times \twoheadrightarrow C_S(L)$.

Lemma 6.8. *If we set* $U := \left\{\varepsilon \in \mathcal{O}_L^\times \mid \sigma_w(\varepsilon) \in \exp_w(\mathscr{L}_w)\ \forall w \in S\right\}$*, then the kernel of* $\mathscr{L}_S \to C_S(L)$ *is isomorphic to*

$$\log_\infty(U) = \{x = (x_w) \in L_\infty \mid \exp_\infty(x) \in \Delta_\infty(U)\}$$

and its cokernel is the finite module $L_S^\times/\exp_S(\mathscr{L}_S) \cdot \Delta_S(U_{L,S})$.

Proof. (i) The kernel of $\exp_S(\mathscr{L}_S) \to C_S(L)$ consists of elements in $\exp_S(\mathscr{L}_S)$ which are also in the kernel $\Delta_S(U_{L,S})$ of $L_S^\times \twoheadrightarrow C_S(L)$. Therefore:

$$\begin{aligned} \ker\big(\exp_S(\mathscr{L}_S) \to C_S(L)\big) &= \Delta_S(U_{L,S}) \cap \exp_S(\mathscr{L}_S) \\ &= \{\Delta_S(\varepsilon) \mid \varepsilon \in U_{L,S} \text{ s.th. } \sigma_w(\varepsilon) \in \exp_w(\mathscr{L}_w)\ \forall w \in S\} \end{aligned}$$

In the latter set, $w(\varepsilon) = 0$ for all $w \in S_f$ since $\sigma_w(\varepsilon) \in \exp_w(\mathscr{L}_w)$. This implies $\varepsilon \in \mathcal{O}_L^\times$ and hence $\ker\big(\exp_S(\mathscr{L}_S) \to C_S(L)\big) \subseteq \Delta_S(U)$. Since every element in $\Delta_S(\mathcal{O}_L^\times)$ is zero in $C_S(L)$, one has $\ker\big(\exp_S(\mathscr{L}_S) \to C_S(L)\big) = \Delta_S(U)$. Then the kernel of the composite map is $\{x \in \mathscr{L}_S \mid \exp_S(x) \in \Delta_S(U)\}$. The projection to $\log_\infty(U)$ provides a map

$$\begin{aligned} \psi : \{x \in \mathscr{L}_S \mid \exp_S(x) \in \Delta_S(U)\} &\to \{x \in L_\infty \mid \exp_\infty(x) \in \Delta_\infty(U)\} = \log_\infty(U) \\ \big((x_w)_{w|\infty}, (y_w)_{w\nmid\infty}\big) &\mapsto \big((x_w)_{w|\infty}\big). \end{aligned}$$

Since the exponential function $\exp_w$ for finite $w \in S_f$ is injective on $\mathscr{L}_w$, the map ψ is an isomorphism: If $x_w = 0$ for all $w|\infty$, then there exists $\varepsilon \in U$ with

$1 = \exp_w(x_w) = \sigma_w(\varepsilon)$ for $w|\infty$. Hence, $\varepsilon = 1$ and $\exp(y_w) = \sigma_w(\varepsilon) = 1$ which implies $y_w = 0$ for all $w \nmid \infty$. This proves injectivity of ψ. If $(x_w) \in \log_\infty(U)$ is given with $\exp_w(x_w) = \sigma_w(\varepsilon)$ for $\varepsilon \in U$, then by definition of U there exist $y_w \in \mathscr{L}_w$ with $\sigma_w(\varepsilon) = \exp_w(y_w)$ for all $w \nmid \infty$. Therefore, (x_w) has a preimage and ψ is surjective. In summary, the projection ψ is an isomorphism and the kernel of $\mathscr{L} \to C_S(L)$ is isomorphic to $\log_\infty(U)$.

(ii) By the conditions on S, Lemma 3.1 implies that there is an isomorphism $C_S(L) \simeq C_{L,S} = L_S^\times/\Delta(U_{L,S})$. Hence, the cokernel of $\mathscr{L} \to C_S(L)$ is isomorphic to $L_S^\times/\exp_S(\mathscr{L}_S) \cdot \Delta_S(U_{L,S})$. The quotient $L_S^\times/\exp_S(\mathscr{L}_S)$ is

$$L_S^\times/\exp_S(\mathscr{L}_S) = \prod_{w \in S_f} L_w^\times/\exp_w(\mathscr{L}_w) \times \prod_{w \in S(\mathbb{R})} \mathbb{R}^\times/\mathbb{R}_{>0} \times \prod_{w \in S(\mathbb{C})} \mathbb{C}^\times/\mathbb{C}^\times.$$

and therefore the projection onto $L_S^\times/\exp_S(\mathscr{L}_S) \cdot \Delta_S(U_{L,S})$ will be finite. $\square$

6.3 Finite approximation of $E_S(\mathscr{L})$

The explicit construction of the Euler characteristic from Section 1.4.2 cannot be applied to the complex $E_S(\mathscr{L})$ directly since it does not consist of finitely generated modules. Therefore, we construct a complex $E_S^f(\mathscr{L})$ of finitely generated modules which will be quasi-isomorphic to $E_S(\mathscr{L})$. The construction of $E_S^f(\mathscr{L})$ is based on the construction of the global fundamental class from Chapter 3.

Recall that we used an approximation of Chinburg [Chi85] to the S-idèle class group $C_S(L)$ in the computation of the global fundamental class. It was obtained as follows.

In a first step we considered the module $C_{L,S}$ which was isomorphic to $C_S(L)$ if S satisfied the conditions (S1)–(S4) from page 70. Then we defined the following modules in Section 3.1 using the finitely generated modules $W_w \subseteq L_w^\times$ for infinite places $w \in S_\infty(G)$, and lattices $\exp_w(\mathscr{L}_w) \subseteq \mathcal{O}_{L_w}^\times$ for finite places $w \in S_f(G)$:

$$I_{L,S}^q = \prod_{w \in S_f(G)} \operatorname{ind}_{G_w}^G L_w^\times/\exp_w(\mathscr{L}_w) \times \prod_{w \in S_\infty(G)} \operatorname{ind}_{G_w}^G L_w^\times, \qquad C_{L,S}^q = I_{L,S}^q/U_{L,S},$$

$$I_{L,S}^f = \prod_{w \in S_f(G)} \operatorname{ind}_{G_w}^G L_w^\times/\exp_w(\mathscr{L}_w) \times \prod_{w \in S_\infty(G)} \operatorname{ind}_{G_w}^G W_w, \qquad C_{L,S}^f = I_{L,S}^f/U_{L,S}.$$

The modules $I_{L,S}^f$ and $C_{L,S}^f$ were both constructed to be finitely generated and we obtained the diagram

$$\begin{tikzcd} I_{L,S} \arrow[r, two heads] \arrow[d, two heads] & I_{L,S}^q \arrow[d, two heads] & I_{L,S}^f \arrow[l, hook'] \arrow[d, two heads] \\ C_{L,S} \arrow[r, two heads] & C_{L,S}^q & C_{L,S}^f \arrow[l, hook'] \end{tikzcd} \tag{6.3}$$

in which the horizontal arrows induce isomorphisms in cohomology, see (3.9).

From the isomorphism $\hat{H}^2(G, M) \simeq \mathrm{Ext}^2_G(\mathbb{Z}, M)$ for any G-module M, we then have isomorphisms $\mathrm{Ext}^2_G(\mathbb{Z}, C_{L,S}) \simeq \mathrm{Ext}^2_G(\mathbb{Z}, C^q_{L,S}) \simeq \mathrm{Ext}^2_G(\mathbb{Z}, C^f_{L,S})$ and similarly for the Yoneda groups. Assume that the complexes $E_S = \big[A \to \mathbb{Z}[G]\big]$ and $E^f_S = \big[A^f \to \mathbb{Z}[G]\big]$ with cohomologically trivial $\mathbb{Z}[G]$-modules A^f and A represent the global fundamental class in $\mathrm{Yext}^2_G(\mathbb{Z}, C_{L,S})$ and $\mathrm{Yext}^2_G(\mathbb{Z}, C^f_{L,S})$. The isomorphisms with $\mathrm{Yext}^2_G(\mathbb{Z}, C^q_{L,S})$ are applied by constructing the pushout sequences with $C_{L,S} \twoheadrightarrow C^q_{L,S}$ and $C^f_{L,S} \hookrightarrow C^q_{L,S}$. One then obtains commutative diagrams

$$\begin{tikzcd} 0 \arrow[r] & C_{L,S} \arrow[r] \arrow[d, two heads] & A \arrow[r] \arrow[d, two heads] & \mathbb{Z}[G] \arrow[r] \arrow[d, equal] & \mathbb{Z} \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & C^q_{L,S} \arrow[r] & A^q \arrow[r] & \mathbb{Z}[G] \arrow[r] & \mathbb{Z} \arrow[r] & 0 \end{tikzcd} \tag{6.4}$$

and

$$\begin{tikzcd} 0 \arrow[r] & C^f_{L,S} \arrow[r] \arrow[d, hook] & A^f \arrow[r] \arrow[d, hook] & \mathbb{Z}[G] \arrow[r] \arrow[d, equal] & \mathbb{Z} \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & C^q_{L,S} \arrow[r] & \widetilde{A}^q \arrow[r] & \mathbb{Z}[G] \arrow[r] & \mathbb{Z} \arrow[r] & 0 \end{tikzcd} \tag{6.5}$$

in which the complexes $E^q_S = \big[A^q \to \mathbb{Z}[G]\big]$ and $\widetilde{E}^q_S = \big[\widetilde{A}^q \to \mathbb{Z}[G]\big]$ both represent the global fundamental class in $\mathrm{Yext}^2_G(\mathbb{Z}, C^q_{L,S}) \simeq \mathrm{Ext}^2_G(\mathbb{Z}, C^q_{L,S})$. In other words, the complexes E^q_S and $\widetilde{E}^q_S$ are quasi-isomorphic and the quasi-isomorphism induces identity maps $H^0(E^q_S) = C^q_{L,S} = H^0(\widetilde{E}^q_S)$ and $H^1(E^q_S) = \mathbb{Z} = H^1(\widetilde{E}^q_S)$ on the cohomology groups.

Remember that only the complex E^f_S, which represents the global fundamental class in $\mathrm{Ext}^2_G(\mathbb{Z}, C^f_{L,S})$, can be computed since the others do not consist of finitely generated modules. The complex E^f_S can be constructed using the cocycle from Algorithm 3.13 and applying Proposition 1.29. To approximate the complex $E_S(\mathscr{L})$ using the complex E^f_S we will consider the modules

$$W_\infty = \prod_{w \in S_\infty(G)} \mathrm{ind}^G_{G_w} W_w \subseteq L^\times_\infty \subseteq I^f_{L,S}$$
$$\text{and} \quad \log_\infty(W_\infty) = \{x \in L_\infty \mid \exp_\infty(x) \in W_\infty\} \subseteq L_\infty.$$

By definition of W_∞, the module $\log_\infty(W_\infty)$ is also an induced module: we have $\log_\infty(W_\infty) = \bigoplus_{w \in S(G)} \mathrm{ind}^G_{G_w} \log_w(W_w)$ where $\log_w(W_w)$ denotes the module $\{x \in L_w \mid \exp_w(x) \in W_w \subseteq L^\times_w\}$. We can then prove the following.

Lemma 6.9. *Each module* $\log_w(W_w) \subseteq L_w$ *is cohomologically trivial as* G_w*-module and therefore* $\log_\infty(W_\infty)$ *is cohomologically trivial as* G*-module.*

Proof. If $w \in S_\infty$ is a place with trivial decomposition group $G_w = 1$, then every G_w-module is cohomologically trivial. Consider a complex place w with decomposition group $G_w \neq 1$. Since each module W_w contains the S-units

$U_{L,S}$ by construction[2] — and in particular the element $1 \in U_{L,S}$ — the module $\log_w(W_w)$ will contain the kernel of the exponential map, resulting in a commutative diagram:

$$\begin{tikzcd}
2\pi\mathrm{i}\,\mathbb{Z} \arrow[r, hook] \arrow[d, equal] & \log_w(W_w) \arrow[r, two heads] \arrow[d, hook] & W_w \arrow[d, hook] \\
2\pi\mathrm{i}\,\mathbb{Z} \arrow[r, hook] & \mathbb{C} \arrow[r, two heads, "\exp"] \arrow[d, two heads] & \mathbb{C}^\times \arrow[d, two heads] \\
& \mathbb{C}/\log_w(W_w) \arrow[r, "\simeq"] & \mathbb{C}^\times/W_w
\end{tikzcd}$$

By construction of W_w, the quotient $\mathbb{C}^\times/W_w$ is a cohomologically trivial G_w-module and as the bottom row is an isomorphism, this also holds for $\mathbb{C}/\log_w(W_w)$. Since $\mathbb{C}$ is cohomologically trivial as well (considered as additive module), this implies the cohomological triviality of $\log_w(W_w)$. Using the induced description of the module $\log_\infty(W_\infty)$, Shapiro's lemma finally implies that $\log_\infty(W_\infty)$ is cohomologically trivial. $\square$

We now construct complexes in a similar way as we obtained $E_S(\mathscr{L})$. In particular, we will again use the lift of the trace map $\mathrm{tr}' : \mathscr{L} \to \mathbb{Z}[G]$. We then consider the chain map $\alpha_q : \left[L_\infty \xrightarrow{0} \mathscr{L}\right] \to E_S^q$ with $L_\infty \xrightarrow{\exp_\infty} L_\infty^\times \to C_{L,S}^q \subseteq A^q$ in degree 0 and tr' in degree 1. The cone of α_q is the complex

$$E_S^q(\mathscr{L}) = \left[L_\infty \xrightarrow{\exp_\infty} A^q \oplus \mathscr{L} \longrightarrow \mathbb{Z}[G]\right]$$

with L_∞ in degree -1. The differential in degree 0 is the sum of the maps $A^q \to \mathbb{Z}[G]$ and tr'. For the complex $\widetilde{E}_S^q$ one obtains a quasi-isomorphic complex

$$\widetilde{E}_S^q(\mathscr{L}) = \left[L_\infty \xrightarrow{\exp_\infty} \widetilde{A}^q \oplus \mathscr{L} \longrightarrow \mathbb{Z}[G]\right]$$

using the same construction and the quasi-isomorphism will again induce the identity map on the cohomology.

Similarly, there is a map of complexes $\alpha_f : \left[\log_\infty(W_\infty) \xrightarrow{0} \mathscr{L}\right] \to E_S^f$ given by $\log_\infty(W_\infty) \xrightarrow{\exp_\infty} W_\infty \to C_{L,S}^f \subseteq A^f$ in degree 0 and tr' in degree 1. The cone $E_S^f(\mathscr{L})$ of α_f is the complex

$$E_S^f(\mathscr{L}) = \left[\log_\infty(W_\infty) \xrightarrow{\exp_\infty} A^f \oplus \mathscr{L} \longrightarrow \mathbb{Z}[G]\right]$$

where $\log_\infty(W_\infty)$ is placed in degree -1 and the differential in degree 0 is the sum of $A^f \to \mathbb{Z}[G]$ and tr'.

Note that the complexes $E_S^q(\mathscr{L})$, $\widetilde{E}_S^q(\mathscr{L})$ and $E_S^f(\mathscr{L})$ consist of cohomologically trivial modules. By Proposition 1.38 they are actually perfect complexes if their cohomology groups are finitely generated, which is part of the following proof.

[2]See Proposition 3.3 for the construction of W_w.

Theorem 6.10. *The complex $E_S^f(\mathscr{L})$ is a perfect complex which is quasi-isomorphic to $E_S(\mathscr{L})$. Therefore μ_L induces a trivialization μ_L^f of $E_S^f(\mathscr{L})$ and*

$$\chi_G(E_S(\mathscr{L}), \mu_L) = \chi_G(E_S^f(\mathscr{L}), \mu_L^f).$$

Proof. As in the proof of [BrB07, Prop. 3.6] we first consider the commutative diagram

$$\begin{tikzcd}
 & \mathscr{L}_f \arrow[r, "\exp"] \arrow[d, hook] & \exp(\mathscr{L}_f) \arrow[d, hook] & \\
E_S(\mathscr{L}): \arrow[d] & \mathscr{L}_S \arrow[r] \arrow[d] & A \oplus \mathscr{L} \arrow[r] \arrow[d] & \mathbb{Z}[G] \arrow[d, equal] \\
E_S^q(\mathscr{L}): & L_\infty \arrow[r] & A^q \oplus \mathscr{L} \arrow[r] & \mathbb{Z}[G]
\end{tikzcd} \tag{6.6}$$

in which $\exp(\mathscr{L}_f)$ is the kernel of $A \to A^q$ by diagram (6.4). The upper complex is acyclic since the exponential function is injective for every finite place. Thus, the map $E_S(\mathscr{L}) \to E_S^q(\mathscr{L})$ is a quasi-isomorphism which induces a trivialization μ_L^q of $E_S^q(\mathscr{L})$. Then the following holds for the Euler characteristics:

$$\chi_G(E_S(\mathscr{L}), \mu_L) = \chi_G(E_S^q(\mathscr{L}), \mu_L^q).$$

The quasi-isomorphism of $E_S^q(\mathscr{L})$ and $\widetilde{E}_S^q(\mathscr{L})$ similarly induces a trivialization $\widetilde{\mu}_L^q$ of $\widetilde{E}_S^q(\mathscr{L})$ for which $\chi_G(E_S^q(\mathscr{L}), \mu_L^q) = \chi_G(\widetilde{E}_S^q(\mathscr{L}), \widetilde{\mu}_L^q)$.

To describe the Euler characteristic in terms of $E_S^f(\mathscr{L})$, consider the commutative diagram

$$\begin{tikzcd}
E_S^f(\mathscr{L}): \arrow[d, hook] & \log_\infty(W_\infty) \arrow[r, "\exp_\infty"] \arrow[d, hook] & A^f \oplus \mathscr{L} \arrow[r] \arrow[d, hook] & \mathbb{Z}[G] \arrow[d, equal] \\
\widetilde{E}_S^q(\mathscr{L}): & L_\infty \arrow[r, "\exp_\infty"] \arrow[d] & \widetilde{A}^q \oplus \mathscr{L} \arrow[r] \arrow[d] & \mathbb{Z}[G] \\
 & L_\infty/\log_\infty(W_\infty) \arrow[r, "\exp_\infty"] & L_\infty^\times/W_\infty &
\end{tikzcd} \tag{6.7}$$

in which $L_\infty^\times/W_\infty$ is the cokernel of $A^f \to \widetilde{A}^q$ by diagram (6.5) and the complex in the bottom row is quasi-isomorphic to the cone of the injective map of complexes $E_S^f(\mathscr{L}) \to E_S^q(\mathscr{L})$ by Lemma 1.37.

The map $\exp_\infty : L_\infty/\log_\infty(W_\infty) \to L_\infty^\times/W_\infty$ is injective because we factored modulo the preimage $\log_\infty(W_\infty)$ of W_∞. Its cokernel is trivial since

$$L_\infty^\times/\exp_\infty(L_\infty) = \Big(\prod_{w \in S(\mathbb{R})} \mathbb{R}^\times/\mathbb{R}_{>0} \times \prod_{w \in S(\mathbb{C})} 1 \Big)$$

and W_∞ contains $-1 \in U_{L,S} \subseteq W_w \subset W_\infty$ at every real place w. Hence, the complex is acyclic and $E_S^f(\mathscr{L}) \to E_S^q(\mathscr{L})$ is again a quasi-isomorphism. It induces a trivialization μ_L^f of $E_S^f(\mathscr{L})$ and one obtains

$$\chi_G(\widetilde{E}_S^q(\mathscr{L}), \mu_L) = \chi_G(E_S^f(\mathscr{L}), \mu_L^f)$$

which completes the proof. $\square$

Note that all quasi-isomorphisms in the above proof induce identity maps on the cohomology groups by the projections in (6.6), the inclusions in (6.7), and the identification of E_S^q and $\widetilde{E}_S^q$ in $\mathrm{Ext}_G^2(\mathbb{Z}, C_{L,S}^q)$. Therefore the trivialization μ_L^f can be identified with μ_L and we will further consider μ_L as trivialization of $E_S^f(\mathscr{L})$.

We finish this section by an explicit description of the computation of the Euler characteristic $\chi_G(E_S^f(\mathscr{L}), \mu_L) \in K_0(\mathbb{Z}[G], \mathbb{R})$. The complex $E_S^f(\mathscr{L})_\mathbb{R}$ is acyclic outside degrees -1 and 0 and by Corollary 1.43 this implies $\chi_G(E_S^f(\mathscr{L}), \mu_L) = -\bar{\chi}_G(E_S^f(\mathscr{L}), \mu_L)$. If P is a complex of finitely generated projective modules, which is quasi-isomorphic to $E_S^f(\mathscr{L})$ through a chain map $\pi : P \to E_S^f(\mathscr{L})$, then this is $\chi_G(E_S^f(\mathscr{L}), \mu_L) = \chi_G(P, \pi^{-1}\mu_L\pi) = \left[P^+, \theta, P^-\right]$ where θ denotes the isomorphism of $P_\mathbb{R}^+$ and $P_\mathbb{R}^-$ induced by μ_L as in Section 1.4.2.

From the construction by Proposition 1.38 one obtains such a complex P and a quasi-isomorphism $\pi : P \to E_S(\mathscr{L})$ as in the following diagram:

$$\begin{array}{ccccccccc} P: & & P^{-2} & \xrightarrow{p_{-2}} & P^{-1} & \xrightarrow{p_{-1}} & P^0 & \xrightarrow{p_0} & P^1 \\ \downarrow{\scriptstyle\pi} & & & & \downarrow & & \downarrow & & \| \\ E_S^f(\mathscr{L}): & & & & \log_\infty(W_\infty) & \xrightarrow{f_{-1}} & A^f \oplus \mathscr{L} & \xrightarrow{f_0} & \mathbb{Z}[G] \end{array}$$

If we consider the proof of Proposition 1.38 in more detail, we also see that p_{-2} is injective and that we can choose $P^1 = \mathbb{Z}[G]$. Moreover, the quasi-isomorphism π induces $\mathbb{Z}[G]$-isomorphisms $\pi_i : H^i(P) \xrightarrow{\simeq} H^i(E_S(\mathscr{L}))$.

Therefore, the Euler characteristic $\chi_G(E_S^f(\mathscr{L}), \mu_L) = \chi_G(P, \pi^{-1}\mu_L\pi)$ is a triple $\left[P^{-2} \oplus P^0, \theta, P^{-1} \oplus \mathbb{Z}[G]\right]$ and the isomorphism θ is induced by μ_L as follows. From the complex P we have short exact sequences

$$\begin{array}{rl} & 0 \to \ker(p_i) \to \quad P^i \quad \to \ \mathrm{im}(p_i) \ \to 0, \\ \text{and} & 0 \to \ \mathrm{im}(p_i) \ \to \ker(p_{i+1}) \to H^{i+1}(P) \to 0 \end{array}$$

in every degree. All these short exact sequences remain exact after tensoring with $\mathbb{R}[G]$ over $\mathbb{Z}[G]$ and choosing $\mathbb{R}[G]$-splittings gives isomorphisms

$$\begin{aligned} \rho_i : P_\mathbb{R}^i &\xrightarrow{\simeq} \ker(p_i)_\mathbb{R} \oplus \mathrm{im}(p_i)_\mathbb{R}, \\ \rho'_{i+1} : \ker(p_{i+1})_\mathbb{R} &\xrightarrow{\simeq} \mathrm{im}(p_i)_\mathbb{R} \oplus H^{i+1}(P)_\mathbb{R}. \end{aligned}$$

By $H^1(P)_\mathbb{R} = 0$ one has $\mathrm{im}(p_0)_\mathbb{R} \simeq P_\mathbb{R}^1$ and the isomorphism θ is given by

$$\begin{aligned} (P^{-2} \oplus P^0)_\mathbb{R} &\xrightarrow{\rho_{-2}, \rho_0} \mathrm{im}(p_{-2})_\mathbb{R} \oplus \ker(p_0)_\mathbb{R} \oplus \mathrm{im}(p_0)_\mathbb{R} \\ &\xrightarrow{\rho'_0} \mathrm{im}(p_{-2})_\mathbb{R} \oplus \mathrm{im}(p_{-1})_\mathbb{R} \oplus H^0(P)_\mathbb{R} \oplus \mathrm{im}(p_0)_\mathbb{R} \\ &\xrightarrow{\pi_1^{-1}\mu_L\pi_0} \mathrm{im}(p_{-1})_\mathbb{R} \oplus \mathrm{im}(p_{-2})_\mathbb{R} \oplus H^{-1}(P)_\mathbb{R} \oplus \mathrm{im}(p_0)_\mathbb{R} \qquad (6.8) \\ &\xrightarrow{(\rho'_{-1})^{-1}} \mathrm{im}(p_{-1})_\mathbb{R} \oplus \ker(p_{-1})_\mathbb{R} \oplus \mathrm{im}(p_0)_\mathbb{R} \\ &\xrightarrow{(\rho_{-1})^{-1}} P_\mathbb{R}^{-1} \oplus P_\mathbb{R}^1. \end{aligned}$$

Note that all the maps ρ_i and ρ_i' are also isomorphisms if one only tensors with $\mathbb{Q}$ instead of $\mathbb{R}$. Since the modules $(P^{-2} \oplus P^0)_{\mathbb{Q}}$ and $(P^{-1} \oplus P^1)_{\mathbb{R}}$ are $\mathbb{Q}[G]$-free, all isomorphisms in (6.8), except the one induced by μ_L, can therefore be represented by $\mathbb{Q}[G]$-matrices.

6.4 Description of the algorithm

Using the theoretical preparations from above we can present an algorithm which gives numerical evidence for $\mathrm{ETNC}(L|\mathbb{Q}, 1)$. The algebraic term of the conjecture is the Euler characteristic $\chi_G(E_S(\mathscr{L}), \mu_L)$ which can be computed using Theorem 6.10 and the construction above.

The analytic term of $T\Omega(L|K, 1)$ depends on the leading term $\zeta^*_{L|\mathbb{Q},S}(1) \in \mathrm{Z}(\mathbb{R}[G])^\times$. The Artin L-function and the leading coefficient of the S-truncated Artin L-function can be computed in Magma using algorithms by Dokchitser [Dok04]. Using his algorithm and the fact that the order of the Artin L-function is known (e.g. see [Tat84, Chp. I, § 8]), one can compute $\zeta^*_{L|\mathbb{Q},S}(1) \in \mathrm{Z}(\mathbb{R}[G])^\times$ as a tuple of (real or complex) values.

In the algorithm below, we will compute a representative of the Euler characteristic $\chi_G(E^f_S(\mathscr{L}), \mu_L)$ in $\mathrm{Z}(\mathbb{R}[G])^\times$ and its product with $\zeta^*_{L|\mathbb{Q},S}(1)$ up to computation precision. Then we check the rationality conjecture numerically by verifying that the product in $\mathrm{Z}(\mathbb{R}[G])^\times \subseteq \prod_{\chi \in \mathrm{Irr}_{\mathbb{C}}(G)} \mathbb{C}$ approximates an element in $\mathrm{Z}(\mathbb{Q}[G])^\times \simeq \prod_{\chi \in \mathrm{Irr}_{\mathbb{Q}}(G)} \mathbb{Q}(\chi) \subseteq \prod_{\chi \in \mathrm{Irr}_{\mathbb{C}}(G)} \mathbb{C}$. Using this approximation we will then continue to verify $\mathrm{ETNC}(L|\mathbb{Q}, 1)$ numerically.

Before we discuss each step in more detail, we give an overview of the algorithm.

Algorithm 6.11 (Numerical evidence for ETNC($L|\mathbb{Q}, 1$)).
Input: A Galois extension $L|\mathbb{Q}$ of number fields with group G and a complex precision r.

Output: True if $\mathrm{ETNC}(L|\mathbb{Q}, 1)$ could be verified up to precision r, and False otherwise.

(Initialization)

1 Compute a set of places S satisfying conditions (S1)–(S4) from page 70.

(Analytic Part)

2 Compute the S-truncated Artin L-function for $L|\mathbb{Q}$ and the leading term $\zeta^*_{L|\mathbb{Q},S}(1)$ using algorithms of Dokchitser [Dok04].

(Algebraic Part)

3 Compute the inverse of the global fundamental class $\gamma^{-1} \in \hat{H}^2(G, C^f_{L,S})$ with Algorithm 3.13. This involves the construction of finitely generated modules $W_\infty \subseteq L_\infty$ and $C^f_{L,S}$ using Algorithms 3.7 and 3.9. The local lattices $\mathscr{L}_v \subseteq \mathcal{O}_{L_v}$ for finite places v give rise to a global lattice $\mathscr{L}$ using [Ble03, § 3.1].

4 Compute a complex representing the cocycle γ^{-1} using the construction from Section 1.3.2 with splitting module $A^f = C^f_{L,S}(\gamma^{-1})$.

5 Construct all modules and maps of $E^f_S(\mathscr{L})$ explicitly and use Proposition 1.38 as above to construct a complex P of finitely-generated, projective $\mathbb{Z}[G]$-modules and a quasi-isomorphism $\pi : P \to E^f_S(\mathscr{L})$. Let $\theta : (P^{-2} \oplus P^0)_{\mathbb{R}} \to (P^{-1} \oplus P^1)_{\mathbb{R}}$ denote the isomorphism (6.8).

(Comparison)

6 Compute a $\mathbb{Q}[G]$-basis B of $(P^{-2} \oplus P^0)_{\mathbb{Q}} \simeq \mathbb{Q}[G]^d$ and $(P^{-1} \oplus P^1)_{\mathbb{Q}} \simeq \mathbb{Q}[G]^d$ and let H be the finite set of primes p, including $p \mid |G|$ and those for which B is not a $\mathbb{Z}_p[G]$-basis of $(P^{-2} \oplus P^0)_{\mathbb{Z}_p}$ or $(P^{-1} \oplus P^1)_{\mathbb{Z}_p}$.

For primes $p \notin H$:

7 Compute the matrix $A \in \mathrm{Gl}_d(\mathbb{R}[G])$ representing θ with respect to this basis.

8 Compute an approximation $\xi \in \mathrm{Z}(\mathbb{Q}[G])^\times$ of the product $\zeta^*_{L|\mathbb{Q},S}(1)\,\mathrm{nr}(A)$ as tuple $(\xi_1, \ldots, \xi_r) \in \prod_{i=1}^r \mathbb{Q}(\chi_i)$.

9 Check whether the ideals of the prime ideal decomposition of $\xi_i \mathcal{O}_{\mathbb{Q}(\chi_i)}$ have support in H.

For every other prime $p \in H$:

10 Compute a $\mathbb{Z}_p[G]$-basis of $(P^{-2} \oplus P^0)_{\mathbb{Z}_p}$ and $(P^{-1} \oplus P^1)_{\mathbb{Z}_p}$ using [BW09, § 4.2].

11 Compute the matrix $A \in \mathrm{Gl}_d(\mathbb{R}[G])$ representing θ with respect to this basis.

12 Compute an approximation $\xi_p \in \mathrm{Z}(\mathbb{Q}[G])^\times \subseteq \mathrm{Z}(\mathbb{Q}_p[G])^\times$ of $\zeta^*_{L|\mathbb{Q},S}(1)\,\mathrm{nr}(A)$.

13 Compute $K_0(\mathbb{Z}[G], \mathbb{Q}_p)$ using the algorithms from [BW09] and check whether $\widehat{\partial}^1_{G,\mathbb{Q}_p}(\xi_p)$ is zero.

Return: True, if all comparisons were correct and False otherwise.

Remarks 6.12. *Algebraic part:* The lattice used in the construction of $C^f_{L,S}$ should be the same lattice which also occurs in the construction of $E^f_S(\mathscr{L})$. In the description of the above algorithm we use [Ble03, § 3.1] to construct the global lattice $\mathscr{L} \subseteq \mathcal{O}_L$ from local lattices $\mathscr{L}_v \subseteq \mathcal{O}_{L_v}$ established in the computation of the global fundamental class. In this case, however, it might be easier to construct an appropriate global lattice and compute its localizations afterwards. In any case, we have to make sure to use the same lattice in both parts of our algorithm.

The extension class constructed using the splitting module $A^f = C^f_{L,S}(\gamma)$ represents the global fundamental class in $\mathrm{Yext}^2_G(\mathbb{Z}, C^f_{L,S})$ by means of a projective resolution of $\mathbb{Z}$. The conjecture, however, is formulated by representing extension groups using injective resolutions of the second variable. Following Remark 5.4

in [BrB07] we therefore have to consider the inverse of the global fundamental class in our construction.

Finally, the computation of the Euler characteristic $\chi_G(E_S(\mathscr{L}), \mu_L)$ is explained in detail in Section 6.3.

Comparison: If M is a finitely generated $\mathbb{Z}[G]$-module and $B = \{b_1, \ldots, b_n\}$ is a $\mathbb{Q}[G]$-basis of $M \otimes_{\mathbb{Z}[G]} \mathbb{Q}[G]$ with $b_i \in M$, then $\langle b_1, \ldots, b_n \rangle_{\mathbb{Z}[G]}$ has finite index k in M, and k becomes a unit in $\mathbb{Z}_p[G]$ if $p \nmid k$. Hence, B is also a basis for $M \otimes_{\mathbb{Z}[G]} \mathbb{Z}_p[G]$ if $p \nmid k$. Applying this fact to the modules $P^{-2} \oplus P^0$ and $P^{-1} \oplus P^1$, we can therefore compute the finite set H in step 6.

For the primes $p \in H$ we compute a $\mathbb{Z}_p[G]$-basis of the modules $(P^{-2} \oplus P^0)_{\mathbb{Z}_p}$ and $(P^{-1} \oplus P^1)_{\mathbb{Z}_p}$ separately. The algorithm of [BW09, § 4.2] actually computes these bases by considering the localizations $\mathbb{Z}_{(p)}$ instead of $\mathbb{Z}_p$. By $\mathbb{Z}_{(p)} \subset \mathbb{Q} \subset \mathbb{R}$ these bases will then also provide corresponding bases of $(P^{-2} \oplus P^0)_{\mathbb{R}}$ and $(P^{-1} \oplus P^1)_{\mathbb{R}}$.

In both cases we can therefore compute a matrix $A \in \mathrm{Gl}_d(\mathbb{R}[G])$ which represents θ with respect to these bases and were $d \in \mathbb{N}$ is appropriate.

If we apply the proof of [Jan10, Thm. 3.3.2] to the case $\mathrm{ETNC}(L|K, 1)$, we know that the rationality $T\Omega(L|K, 1) \in K_0(\mathbb{Z}[G], \mathbb{Q})$ holds if and only if $\eta = \zeta^*_{L|\mathbb{Q},S}(1)\,\mathrm{nr}(A) \in \mathrm{Z}(\mathbb{Q}[G])^\times$ holds. By assuming the *rationality conjecture,* one can therefore compute an approximation $\xi \in \mathrm{Z}(\mathbb{Q}[G])^\times$ to $\eta \in \mathrm{Z}(\mathbb{C}[G])^\times$.

This is done by representing η by a tuple $(\eta_\chi) \in \prod_{\chi \in \mathrm{Irr}_{\mathbb{C}}(G)} \mathbb{C}$ through the Wedderburn decomposition. Since values at conjugate characters must be conjugated, the polynomials $\prod_{\psi = \sigma \circ \chi}(X - \eta_\psi) \in \mathbb{C}[X]$ must actually have coefficients in $\mathbb{Q}$ for all $\chi \in \mathrm{Irr}_{\mathbb{Q}}(G)$. We can therefore approximate each of the coefficients with rational numbers, and we can then compute the roots in $\mathbb{Q}(\chi)$ exactly. Together these roots provide a tuple $\xi = (\xi_\chi) \in \prod_{\chi \in \mathrm{Irr}_{\mathbb{C}}(G)} \mathbb{Q}(\chi)$ which approximates η.

By the decomposition of $K_0(\mathbb{Z}[G], \mathbb{Q})$ into p-parts $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$, we know that ξ represents zero if and only if it is zero in every group $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$. For primes not dividing $|G|$ the torsion subgroup of $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ is trivial. To represent zero in the relative K-group, ξ must therefore be a p-adic unit. This can be checked by computing the support of the factorization of $\xi\mathcal{O}_L$, compare Proposition 5.13.

For the other (finitely many) primes, ξ represents zero in $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p)$ if it is an element in $\mathrm{nr}(\mathbb{Z}_p[G]^\times)$. This can be checked using algorithms from [BW09].

In special cases the algorithm above can also be used to give a proof of the equivariant Tamagawa number conjecture at $s = 1$. By the rationality conjecture one expects that

$$\zeta^*_{L|K,S}(1)\,\mathrm{nr}(A) \in \mathrm{Z}(\mathbb{Q}[G])^\times \simeq \prod_{\chi \in \mathrm{Irr}_{\mathbb{Q}}(G)} \mathbb{Q}(\chi)^\times.$$

Therefore, the transcendental parts of $\zeta^*_{L|K,S}(1)$ and $\mathrm{nr}(A)$ have to cancel and the main issue is to compute the algebraic part exactly.

Remark 6.13. Let M_1 and M_2 be free $\mathbb{Q}[G]$-modules and $\phi : M_1 \to M_2$ and isomorphism of $\mathbb{Q}[G]$-modules. If $a_1, \dots, a_n$ and $b_1, \dots, b_n$ are $\mathbb{Q}[G]$-bases and if $A \in \mathrm{Gl}_n(\mathbb{Q}[G])$ represents ϕ with respect to these bases, then the reduced norm $\mathrm{nr}(A) = (\det_\chi(A))_{\chi \in \mathrm{Irr}_\mathbb{C}(G)}$ is an element in $\mathrm{Z}(\mathbb{Q}[G])^\times$, i.e. each component satisfies $\det_\chi(A) \in \mathbb{Q}(\chi)^\times$ and $\mathrm{nr}(A)$ is Galois invariant by $\mathrm{nr}(A)_{\sigma\circ\chi} = \sigma(\mathrm{nr}(A)_\chi)$ for $\sigma \in \mathrm{Aut}(\mathbb{Q}(\chi)|\mathbb{Q})$.

Now consider the modules $M_{1,\mathbb{R}} = \mathbb{R}[G] \otimes_{\mathbb{Q}[G]} M_1$ and $M_{2,\mathbb{R}} = \mathbb{R}[G] \otimes_{\mathbb{Q}[G]} M_2$ and the isomorphism induced by ϕ. The bases a_i and b_i of M_1 and M_2 induce bases $a_i \otimes 1$ and $b_i \otimes 1$ of $M_{1,\mathbb{R}}$ and $M_{2,\mathbb{R}}$, respectively. Then the matrix representing the isomorphism $\phi : M_{1,\mathbb{R}} \to M_{2,\mathbb{R}}$ with respect to these bases will again be the same matrix $A \in \mathrm{Gl}_n(\mathbb{Q}[G]) \subset \mathrm{Gl}_n(\mathbb{R}[G])$.

We apply this fact to the isomorphism $\theta : (P^{-2} \oplus P^0)_\mathbb{R} \to (P^{-1} \oplus P^1)_\mathbb{R}$ from (6.8) which can be divided into three parts:

$$
\begin{aligned}
&\theta_1 : (P^{-2} \oplus P^0)_\mathbb{Q} \to M_{1,\mathbb{Q}} \\
&\theta_2 : M_{1,\mathbb{R}} \to M_{2,\mathbb{R}} \\
&\theta_3 : M_{2,\mathbb{Q}} \to (P^{-1} \oplus P^1)_\mathbb{Q}, \\
\text{with}\quad &M_1 = \mathrm{im}(p_{-2}) \oplus \mathrm{im}(p_{-1}) \oplus H^0(P) \oplus \mathrm{im}(p_0), \\
&M_2 = \mathrm{im}(p_{-1}) \oplus \mathrm{im}(p_{-2}) \oplus H^{-1}(P) \oplus \mathrm{im}(p_0).
\end{aligned}
$$

As discussed in Section 6.3 the isomorphisms θ_1 and θ_3 were induced by splittings and were therefore already defined over $\mathbb{Q}$. Hence, the reduced norm of $\mathbb{Q}[G]$-matrices representing θ_1 and θ_3 will be in $\mathrm{Z}(\mathbb{Q}[G])^\times$ for any $\mathbb{Q}[G]$-basis. Indeed, all these modules are $\mathbb{Q}[G]$-free by a lemma of Swan (see [CR81, Thm. (32.11)]) since they are $\mathbb{Z}[G]$-projective.

As a result, the most significant part in $\theta = \theta_{3,\mathbb{R}} \circ \theta_2 \circ \theta_{1,\mathbb{R}}$ is given by θ_2. More precisely, let B_1, B_2, B_3 and B_4 denote $\mathbb{Q}[G]$-bases of the four modules $(P^{-2} \oplus P^0)_\mathbb{Q}, M_{1,\mathbb{Q}}, M_{2,\mathbb{Q}}$ and $(P^{-1} \oplus P^1)_\mathbb{Q}$, let A be the matrix representing θ with respect to the induced bases $B_{1,\mathbb{R}}$ and $B_{4,\mathbb{R}}$ and A_1 the matrix representing θ_2 with respect to $B_{2,\mathbb{R}}$ and $B_{3,\mathbb{R}}$. Then $\mathrm{nr}(A) = \lambda\, \mathrm{nr}(A_1)$ for some factor $\lambda \in \mathrm{Z}(\mathbb{Q}[G])^\times$ which arises from the $\mathbb{Q}[G]$-isomorphisms θ_1 and θ_3.

To get a proof of the equivariant Tamagawa number conjecture with Algorithm 6.11 it is therefore crucial to control the transcendental elements in the reduced norm of the isomorphism $\theta_2 : M_{1,\mathbb{R}} \xrightarrow{\simeq} M_{2,\mathbb{R}}$ with respect to $\mathbb{Q}[G]$-bases of $M_{1,\mathbb{Q}}$ and $M_{2,\mathbb{Q}}$. This isomorphism was induced by

$$\mu_L : H^0\big(E_S^f(\mathscr{L})\big)_\mathbb{R} \xrightarrow{\simeq} H^{-1}\big(E_S^f(\mathscr{L})\big)_\mathbb{R}.$$

The investigation in the proof of Theorem 6.15 will use this fact in order to restrict the analysis of θ to μ_L, whose determinant will change by a factor in $\mathrm{Z}(\mathbb{Q}[G])^\times$. But first we prove the following identities.

Lemma 6.14. *For a subgroup H of G, let $e_H = \frac{1}{|H|}\sum_{h\in H} h$ and $F = L^H$. Then there are identifications*

(a) $e_H L^0 = F^0$, *and*

(b) $e_H\big(\log_\infty(\mathcal{O}_L^\times)\otimes_{\mathbb{Z}}\mathbb{Q}\big) \simeq \log_\infty(\mathcal{O}_F^\times)\otimes_{\mathbb{Z}}\mathbb{Q}$.

Proof. (a) Consider an element $x \in e_H L^0$. It is fixed by any group element $h \in H$ and therefore $x \in (L^0)^H \subseteq F$. For its trace we compute $0 = \mathrm{tr}_{L|\mathbb{Q}}(x) = \sum_{\sigma\in G}\sigma(x) = [L:F]\sum_{\tau\in G/H}\tau(x) = [L:F]\,\mathrm{tr}_{F|\mathbb{Q}}(x)$ where τ runs through a set of representatives of G/H. This implies $x \in F^0$ and, hence, $e_H L^0 \subseteq F^0$. On the other hand, every $x \in F^0$ satisfies $x = e_H x \in e_H L^0$.

(b) For primitive elements $x \in e_H(\log_\infty(\mathcal{O}_L^\times)\otimes_{\mathbb{Z}}\mathbb{Q})$ one has $x = e_H(x'\otimes q)$ for $x' \in \log_\infty(\mathcal{O}_L^\times)$ and $q \in \mathbb{Q}$. Therefore, $x = \big(\sum_{\tau\in H}\tau(x')\big)\otimes\frac{q}{|H|} \in \log_\infty(\mathcal{O}_L^\times)^H\otimes\mathbb{Q}$ and for the latter module we use the identification

$$\begin{aligned}\log_\infty(\mathcal{O}_L^\times)^H &= \{x \in L_\infty \mid \exp_\infty(x) \in \Delta_\infty(\mathcal{O}_L^\times) \text{ and } h(x) = x\ \forall h \in H\}\\ &\simeq \{x \in F_\infty \subseteq L_\infty \mid \exp_\infty(x) \in \Delta_\infty(\mathcal{O}_L^\times)\}\end{aligned}$$

where $F_\infty = F\otimes_{\mathbb{Q}}\mathbb{R}$. Since $x \in F_\infty$ implies $\exp_\infty(x) \in F_\infty$ and $\Delta_\infty(\mathcal{O}_L^\times)\cap F_\infty = \Delta_\infty(\mathcal{O}_L^\times\cap F) = \Delta_\infty(\mathcal{O}_F^\times)$, one obtains $\big(\log_\infty(\mathcal{O}_L^\times)\big)^H = \log_\infty(\mathcal{O}_F^\times)$ which proves $e_H(\log_\infty(\mathcal{O}_L^\times)\otimes_{\mathbb{Z}}\mathbb{Q}) \subseteq \log_\infty(\mathcal{O}_F^\times)\otimes_{\mathbb{Z}}\mathbb{Q}$.

On the other hand, one has $\log_\infty(\mathcal{O}_F^\times) \subseteq \log_\infty(\mathcal{O}_L^\times)$ and every primitive element $x \in \log_\infty(\mathcal{O}_F^\times)\otimes_{\mathbb{Z}}\mathbb{Q}$ with $x = x'\otimes q$ for $x' \log_\infty(\mathcal{O}_F^\times)$ and $q \in \mathbb{Q}$ satisfies $x = x'\otimes q = \big(\sum_{\tau\in H}\tau(x')\big)\otimes\frac{q}{|H|} \in e_H(\log_\infty(\mathcal{O}_L^\times)\otimes_{\mathbb{Z}}\mathbb{Q})$. □

Since we consider the modules after tensoring with $\mathbb{Q}$, part (b) also holds for every submodule of $\mathcal{O}_L^\times$ of finite index. We will apply this result for the module $\mathcal{O}_L^+$ of totally positive units in $\mathcal{O}_L^\times$, which was already used in Remark 6.2.

Theorem 6.15. *If all characters $\chi \in \mathrm{Irr}_{\mathbb{C}}(G)$ are rational or abelian, then one can compute the product*

$$\zeta^*_{L|\mathbb{Q},S}(1)\,\mathrm{nr}(A) \in \mathrm{Z}(\mathbb{Q}[G])^\times$$

in Algorithm 6.11 exactly.

Proof. (i) Let χ be a character with rational values $\chi(\sigma) \in \mathbb{Q}$ for all $\sigma \in G$. By *Artin's inductions theorem* the character χ satisfies the equation

$$m\chi = \sum_{H\subseteq G} n_H \mathrm{ind}_H^G 1_H \tag{6.9}$$

for integers m and n_H, where H runs through subgroups of G. In the following, we assume that $m = 1$. For $m > 1$ see Remarks 6.16 below.

As in Algorithm 6.11 the matrix A represents the isomorphism

$$\theta : (P^{-2} \oplus P^0)_{\mathbb{R}} \xrightarrow{\simeq} (P^{-1} \oplus P^1)_{\mathbb{R}}$$

and by Section 1.4.1 the reduced norm $\mathrm{nr}(\theta)$ is given by determinants $\det_\chi(A)$. By the conditions on χ one then has

$$\begin{aligned} \det_\chi(A) &= \prod_{H \subseteq G} \det_{\mathrm{ind}_H^G 1_H}(A)^{n_H} \\ \text{and} \quad L^*_{L|\mathbb{Q},S}(\chi, 1) &= \prod_{H \subseteq G} \zeta^*_{F,S}(1)^{n_H} \end{aligned} \tag{6.10}$$

where $F = L^H$, $\zeta_{F,S}(s)$ denotes the S-truncated Dedekind ζ-function of $F|\mathbb{Q}$ and $\zeta^*_{F,S}(1)$ its leading term at $s = 1$.

To compute the product of the leading coefficient of $\zeta_{L|K,S}(s)$ and the reduced norm of A we therefore have to consider products

$$\det_{\mathrm{ind}_H^G 1_H}(A)\zeta^*_{F,S}(1).$$

If $(P^{-2} \oplus P^0)_{\mathbb{R}}$ and $(P^{-1} \oplus P^1)_{\mathbb{R}}$ are $\mathbb{R}[G]$-modules of rank d, the matrix A induces an isomorphism $\mathbb{C}[G]^d \simeq \mathbb{C}[G] \otimes_{\mathbb{R}[G]} \mathbb{R}[G]^d \xrightarrow{A} \mathbb{C}[G] \otimes_{\mathbb{R}[G]} \mathbb{R}[G]^d \simeq \mathbb{C}[G]^d$ which in turn induces

$$\phi : (e_H\mathbb{C}[G])^d \xrightarrow{\simeq} (e_H\mathbb{C}[G])^d.$$

As in the proof of [Jan10, Thm. 3.3.5] one has $\det_{\mathrm{ind}_H^G 1_H}(A) = \det_{\mathbb{C}}(\phi)$. Following Remark 6.13 we therefore only need to consider the $\mathbb{C}$-determinant of

$$\mu_L : e_H(L^0 \otimes_{\mathbb{Q}} \mathbb{C}) \xrightarrow{\simeq} e_H(\log_\infty(\mathcal{O}_L^\times) \otimes_{\mathbb{Z}} \mathbb{C})$$

by choosing $\mathbb{Q}$-bases of the modules $e_H(L^0)$ and $e_H(\log_\infty(\mathcal{O}_L^\times) \otimes_{\mathbb{Z}} \mathbb{Q})$. The reduced norm of ϕ with respect to any pair of $\mathbb{Q}$-bases will only differ by a factor $\lambda_\chi \in \mathbb{Q}(\chi)^\times$ which is actually rational by the conditions on χ.

By Lemma 6.14 we can use identifications $F^0 = e_H(L^0)$ and $\log_\infty(\mathcal{O}_F^\times) \otimes_{\mathbb{Z}} \mathbb{Q} = e_H(\log_\infty(\mathcal{O}_L^\times) \otimes_{\mathbb{Z}} \mathbb{Q})$ and consider the commutative diagram

$$\begin{tikzcd} e_H(L^0 \otimes_{\mathbb{Q}} \mathbb{Q}) \arrow[r, "\simeq", "\mu_L"'] \arrow[d, "\simeq"] & e_H(\log_\infty(\mathcal{O}_L^\times) \otimes_{\mathbb{Z}} \mathbb{Q}) \arrow[d, "\simeq"] \\ F^0 \arrow[r, "\simeq", "\mu_F"'] & \log_\infty(\mathcal{O}_F^\times) \otimes_{\mathbb{Z}} \mathbb{Q} \end{tikzcd}$$

in which each isomorphism is defined over $\mathbb{Q}$. The $\mathbb{C}$-determinant of the isomorphism $\mu_L : e_H(L^0 \otimes_{\mathbb{Q}} \mathbb{C}) \xrightarrow{\simeq} e_H(\log_\infty(\mathcal{O}_L^\times) \otimes_{\mathbb{Z}} \mathbb{C})$ will therefore be a rational multiple of the determinant from $\mu_F : F^0 \otimes \mathbb{C} \xrightarrow{\simeq} \log_\infty(\mathcal{O}_F^\times) \otimes_{\mathbb{Z}} \mathbb{C}$.

As in Remark 6.2 we now consider the subgroup of totally positive units $\mathcal{O}_F^+$ in $\mathcal{O}_F^\times$ which is a subgroup of finite index, so that $\log_\infty(\mathcal{O}_F^+) \otimes_\mathbb{Z} \mathbb{Q} \simeq \log_\infty(\mathcal{O}_F^\times) \otimes_\mathbb{Z} \mathbb{Q}$. Note that this restriction might introduce another factor in $\mathbb{Q}(\chi) = \mathbb{Q}$.

As a result, we only have to compute the determinant of μ_F exactly, which we now consider in two steps

$$\begin{array}{ccccc} F^0 \otimes_\mathbb{Q} \mathbb{C} & \xrightarrow{\mu_F} & F^0_\infty \otimes_\mathbb{R} \mathbb{C} & \xrightarrow{\text{id}} & F^0_\infty \otimes_\mathbb{R} \mathbb{C} \\ B_1 & & B_2 & & B_3 \end{array} \tag{6.11}$$

with respect to bases B_1, B_2 and B_3.

We denote $n = [F : K] = r_1 + 2r_2$ where r_1 and r_2 are the number of real and pairs of complex embeddings of F. Let $y_2, \dots, y_n$ be any $\mathbb{Q}$-basis of F^0 and set $B_1 = \{y_2 \otimes 1, \dots, y_n \otimes 1\}$.

Similar to the representation of F_∞ in Remark 6.1, we identify $F_\infty \otimes_\mathbb{R} \mathbb{C}$ with $\prod_{r_1} \mathbb{C} \times \prod_{r_2} \mathbb{C} \times \prod_{r_2} \mathbb{C}$ where the components at $r_1 + j$ and $r_1 + r_2 + j$ correspond to a pair of complex embeddings. In other words, the embeddings $\sigma_i : F \hookrightarrow \mathbb{C}$ are ordered such that $\sigma_1, \dots, \sigma_{r_1}$ are real embeddings, and $\sigma_{r_1+j}, \overline{\sigma_{r_1+j}} = \sigma_{r_1+r_2+j}$ are pairs of complex embeddings for $j = 1, \dots, r_2$. Then the isomorphism is explicitly given by

$$\begin{aligned} F_\infty \otimes_\mathbb{R} \mathbb{C} &\simeq \prod_{r_1} \mathbb{C} \times \prod_{r_2} \mathbb{C} \times \prod_{r_2} \mathbb{C} \\ x \otimes z &\mapsto \big(\sigma_1(x)z, \dots, \sigma_{r_1+r_2}(x)z, \overline{\sigma_{r_1+1}(x)}z, \dots, \overline{\sigma_{r_1+r_2}(x)}z\big). \end{aligned}$$

Note that if ι is a fixed embedding, every other embedding is of the form $\iota \circ \sigma$ for $\sigma \in \mathrm{Gal}(F|\mathbb{Q})$. The element in $\mathrm{Gal}(F|\mathbb{Q})$ corresponding to the embedding σ_i will also be denoted by σ_i.

Let $b_1, \dots, b_n$ denote the standard basis of $\prod_{r_1} \mathbb{C} \times \prod_{2r_2} \mathbb{C}$. Then the set $B_2 = \{b_2 - b_1, \dots, b_n - b_1\}$ is a basis of $L^0_\infty \otimes_\mathbb{R} \mathbb{C}$.

Finally, we consider fundamental units $\varepsilon_1, \dots, \varepsilon_t$ of $\mathcal{O}_F^+$ with $t = r_1 + r_2 - 1$. Then the elements

$$\begin{aligned} f_k &:= \sum_{i=1}^n \log(\sigma_i \varepsilon_k) b_i & k &= 1, \dots, t \\ f_{t+j} &:= 2\pi \mathrm{i} b_{r_1+j} - 2\pi \mathrm{i} b_{r_1+r_2+j} & j &= 1, \dots, r_2 \end{aligned}$$

provide a $\mathbb{Z}$-basis of the lattice $\log(\mathcal{O}_F^+)$ by Remark 6.2. Since this is a full lattice, these elements form a $\mathbb{Q}$-basis of $\log(\mathcal{O}_F^\times) \otimes_\mathbb{Z} \mathbb{Q}$ and $B_3 = \{f_i \otimes 1, 1 \le i < n\}$ is a basis of $L^0_\infty \otimes \mathbb{C}$.

Note again that by Remark 6.13 these choices of bases B_1 and B_3 allow the computation of the determinant of $\det_\chi(A)$ up to a rational factor.

Next we compute the matrices representing μ_F with respect to these bases. The equations

$$\mu_L(y_k) = \sum_{i=1}^n \sigma_i(y_k) b_i = \sum_{i=2}^n \sigma_i(y_k)(b_i - b_1)$$

using $\mathrm{tr}_{F|\mathbb{Q}}(y_k) = \sum_{i=1}^n \sigma_i(y_k) = 0$ show that the first isomorphism of (6.11) is represented by the matrix $A_1 = \big(\sigma_i(y_k)\big)_{2\le i,k\le n}$. Its determinant is closely related to the discriminant d_F of F: The elements $y_1 = 1, y_2, \ldots, y_n$ provide a basis of F and if $T \in \mathrm{Gl}_n(\mathbb{Q})$ denotes a base change between this basis and an integral basis of $\mathcal{O}_F$, then the discriminant $d(1, y_2, \ldots, y_n)$ is

$$d(1, y_2, \ldots, y_n) = \det\Big(\big(\sigma_i(y_k)\big)_{1\le i,k\le n}\Big)^2 = \det(T)^2 d_F.$$

By adding every column to the first column and using the relations $\mathrm{tr}_{F|\mathbb{Q}}(y_k) = \sum_{i=1}^n \sigma_i(y_k) = 0$ for $y_2, \ldots, y_n$ we obtain

$$\det\Big(\big(\sigma_i(y_k)\big)_{1\le i,k\le n}\Big) = \det\begin{pmatrix} 1 & \cdots & 1 \\ \sigma_1(y_2) & \cdots & \sigma_n(y_2) \\ \vdots & \ddots & \vdots \\ \sigma_1(y_n) & \cdots & \sigma_n(y_n) \end{pmatrix} = \det\begin{pmatrix} n & 1 & \cdots & 1 \\ 0 & \sigma_2(y_2) & \cdots & \sigma_n(y_2) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \sigma_2(y_n) & \cdots & \sigma_n(y_n) \end{pmatrix}$$
$$= n\det\Big(\big(\sigma_i(y_k)\big)_{2\le i,k\le n}\Big) = n\det(A_1).$$

Since the discriminant d_F is negative if and only if r_2 is odd, we have $\det(A_1) = \pm \mathrm{i}^{r_2} \frac{1}{n}\det(T)\sqrt{|d_F|}$.

The second isomorphism of (6.11) is a base change from B_2 to B_3. Using the equality $\sum_{i=1}^n \log(\sigma_i\varepsilon_k) = 0$ from [Neu92, Chp. I, § 7] we have

$$\begin{aligned} f_k &:= \sum_{i=2}^n \log(\sigma_i\varepsilon_k)(b_i - b_1), && k = 1, \ldots, t, \\ \text{and}\quad f_{t+j} &:= 2\pi\mathrm{i}(b_{r_1+j} - b_1) - 2\pi\mathrm{i}(b_{r_1+r_2+j} - b_1), && j = 1, \ldots, r_2. \end{aligned}$$

The base change from B_3 to B_2 is therefore represented by the matrix

$$\begin{pmatrix} \log(\sigma_2\varepsilon_1) & \cdots & \log(\sigma_{r_1+1}\varepsilon_1) & \cdots & \cdots & \log(\sigma_{r_1+r_2+1}\varepsilon_1) & \cdots & \log(\sigma_n\varepsilon_1) \\ \vdots & & \vdots & & & \vdots & & \vdots \\ \log(\sigma_2\varepsilon_t) & \cdots & \log(\sigma_{r_1+1}\varepsilon_t) & \cdots & \cdots & \log(\sigma_{r_1+r_2+1}\varepsilon_t) & \cdots & \log(\sigma_n\varepsilon_t) \\ & & 2\pi\mathrm{i} & & & -2\pi\mathrm{i} & & \\ 0 & & & \ddots & & & \ddots & \\ & & & & 2\pi\mathrm{i} & & & -2\pi\mathrm{i} \end{pmatrix}.$$

Since the embeddings $\sigma_{r_1+r_2+j}$ and σ_{r_1+j} are conjugated for $1 \le j \le r_2$, the entries $\log(\sigma_{r_1+r_2+j}\varepsilon_k)$ and $\log(\sigma_{r_1+j}\varepsilon_k)$ are equal. Adding the $(r_1 + r_2 + j)$-th column to the $(r_1 + j)$-th column for all $j = 1, \dots, r_2$ and eliminating the upper right entries provides a matrix

$$\begin{pmatrix} \big(\delta_i \log(\sigma_i \varepsilon_k)\big)_{i,k} & & & \\ & -2\pi\mathrm{i} & & \\ & & \ddots & \\ & & & -2\pi\mathrm{i} \end{pmatrix}$$

with $\delta_i = 1$ for real and $\delta_i = 2$ for complex places σ_i. By [Neu92, Chp. I, Thm. (7.5)] this latter matrix has determinant $\pm R_F (2\pi\mathrm{i})^{r_2}$ where R_F denotes the regulator of F if $\varepsilon_1, \dots, \varepsilon_t$ was a system of fundamental units for $\mathcal{O}_F^\times$. Since we considered $\mathcal{O}_F^+$, we obtain the multiple $\pm R_F (2\pi\mathrm{i})^{r_2} [\mathcal{O}_F^+ : \mathcal{O}_F^\times]$.

In isomorphism (6.11) we need the inverse of this base change, and combining the two steps we get the determinant

$$\det_{\mathbb{C}}(\phi) = \lambda_\chi \sqrt{|d_F|} R_F^{-1} (2\pi)^{-r_2}$$

for some rational factor $\lambda_\chi \in \mathbb{Q}(\chi) = \mathbb{Q}$.

On the other hand, the residue $\zeta_F^*(1) = \operatorname{res}_{s=1} \zeta_F(s)$ is

$$\zeta_F^*(1) = \frac{2^{r_1} (2\pi)^{r_2}}{|\mu_F| |d_F|^{1/2}} h_F R_F$$

by [Neu92, Chp. VII, § 5, p. 488], where h_F is the class number of F and μ_F denotes the set of roots of unity in F. Since $\zeta_{F,S}^*(1)$ is a rational multiple of $\zeta_F^*(1)$, the products $\det_{\mathrm{ind}_H^G 1_H}(A) \zeta_{F,S}^*(1)$ used in the computation of the determinant $\det_\chi(A)$ will be a rational numbers.

(ii) Now let χ be an abelian character. Then χ is a homomorphism and we assume that χ is not the trivial character, which is already handled by the first case. Set $H = \ker(\chi)$, so that χ is actually a character of $F = L^H$. If f denotes the conductor of χ, then F can be embedded in $\mathbb{Q}(\zeta_f)$:

$$\begin{tikzcd}[arrows=dash] L \arrow[d, "H"'] & \\ F \arrow[d, "\bar{G}"'] \arrow[r, "\Gamma_1"] & \mathbb{Q}(\zeta_f) \arrow[dl, bend left, "\Gamma"] \\ \mathbb{Q} & \end{tikzcd}$$

We set $\Gamma = \mathrm{Gal}(\mathbb{Q}(\zeta_f)|\mathbb{Q})$, $\Gamma_1 = \mathrm{Gal}(\mathbb{Q}(\zeta_f)|F)$ and $\bar{G} = \mathrm{Gal}(F|\mathbb{Q}) \simeq G/H$.

We can now also consider χ as a character of $\Gamma \simeq (\mathbb{Z}/f\mathbb{Z})^\times$ by inflation, and moreover as a Dirichlet character of $\mathbb{Z}/f\mathbb{Z}$:

$$\chi(a) = \begin{cases} \chi(a + \Gamma_1) & \text{if } a \in (\mathbb{Z}/f\mathbb{Z})^\times \simeq \Gamma, \\ 0 & \text{otherwise.} \end{cases}$$

For an abelian character χ, the Artin L-series of χ coincides with the *Dirichlet L-series* of χ and its leading term at $s = 1$ is given by the following equations

$$L^*_{F|\mathbb{Q}}(\chi, 1) = \begin{cases} \pi \mathrm{i} \dfrac{\tau(\chi)}{f} \displaystyle\sum_{a=1}^{f} \bar{\chi}(a) a & \text{for } \chi(-1) = -1, \\ -\dfrac{\tau(\chi)}{f} \displaystyle\sum_{a=1}^{f} \bar{\chi}(a) \log|1 - \zeta_f^a| & \text{for } \chi(-1) = 1 \end{cases} \tag{6.12}$$

with Galois Gauss sum $\tau(\chi) = \sum_{a=1}^{f} \bar{\chi}(a)\zeta_f^a$, cf. [Was97, Thm. 4.9]. Again, the values of $L^*_{F|\mathbb{Q},S}(\chi, 1)$ just differ from $L^*_{F|\mathbb{Q}}(\chi, 1)$ by some factor in $\mathbb{Q}(\chi)$.

For the algebraic part of the conjecture, we again consider the isomorphism

$$\mu_L : e_\chi(L^0 \otimes_\mathbb{Q} \mathbb{C}) \xrightarrow{\simeq} e_\chi(\log_\infty(\mathcal{O}_L^\times) \otimes_\mathbb{Z} \mathbb{C}).$$

The idempotent e_χ of the G-character χ can be written as $e_{\bar{\chi}} e_H$ where $e_{\bar{\chi}}$ is the corresponding idempotent of χ as G/H-character.

We therefore let e_χ denote the idempotent of χ as character of $\bar{G}$ from now on, and we consider the $\mathbb{C}$-determinant of the isomorphism

$$\mu_F : e_\chi(F^0 \otimes_\mathbb{Q} \mathbb{C}) \xrightarrow{\simeq} e_\chi(\log_\infty(\mathcal{O}_F^\times) \otimes_\mathbb{Z} \mathbb{C}) \tag{6.13}$$

with respect to bases induced by $\mathbb{Q}(\chi)$-bases of the modules $e_\chi(F^0 \otimes_\mathbb{Q} \mathbb{Q}(\chi))$ and $e_\chi(\log_\infty(\mathcal{O}_F^\times) \otimes_\mathbb{Z} \mathbb{Q}(\chi))$. Here, we are again just interested in the determinant up to a factor in $\mathbb{Q}(\chi)$. Note that by $e_\chi \mathbb{C}[G] \simeq \mathbb{C} \simeq \mathbb{Q}(\chi) \otimes_{\mathbb{Q}(\chi)} \mathbb{C}$ and $F_\infty \otimes_\mathbb{R} \mathbb{C} \simeq \mathbb{C}[G]$ these modules have $\mathbb{Q}(\chi)$-rank one.

We use the standard basis $b_1, \dots, b_n$ of $F_\infty \otimes_\mathbb{R} \mathbb{C}$ introduced before and use the fact that every basis element $b_i = b_\sigma$ corresponds to an embedding $\iota \circ \sigma$ for $\sigma \in \bar{G}$. In the group ring $\mathbb{C}[G]$ one has $e_\chi \sigma = \chi(\sigma) e_\chi$ and using $F_\infty \otimes_\mathbb{R} \mathbb{C} \simeq \mathbb{C}[G]$ one similarly obtains $e_\chi b_\sigma = \chi(\sigma) e_\chi b_1$.

A $\mathbb{Q}(\chi)$-basis of $e_\chi F^0_\infty \otimes_\mathbb{R} \mathbb{C}$ is $e_\chi b_1$. Set $\theta = \mathrm{tr}_{\mathbb{Q}(\zeta_f)|F}(\zeta_f) \in F$, then $e_\chi \theta$ is a $\mathbb{Q}(\chi)$-basis of $e_\chi F^0 \otimes_\mathbb{Q} \mathbb{Q}(\chi)$ and

$$\mu_F(e_\chi \theta) = e_\chi \sum_{\sigma \in \bar{G}} \iota(\sigma\theta) b_\sigma = \sum_{\sigma \in \bar{G}} \iota(\sigma\theta)\chi(\sigma) e_\chi b_1 = \tau(\bar{\chi}) e_\chi b_1.$$

Therefore, the $\mathbb{C}$-determinant of (6.13) with respect to these bases is a $\mathbb{Q}_\chi$-multiple of the Gauss sum $\tau(\bar{\chi})$.

As in the case of rational characters we still have to make a base change to a basis of $e_\chi(F^0_\infty \otimes_\mathbb{Q} \mathbb{C})$ which is induced by a $\mathbb{Q}(\chi)$-basis of $e_\chi(\log_\infty(\mathcal{O}_F^\times) \otimes_\mathbb{Z} \mathbb{Q}(\chi))$. And if we consider a sublattice U in $\mathcal{O}_F^\times$ of finite index and a $\mathbb{Q}(\chi)$-basis of $\log_\infty(U) \otimes_\mathbb{Z} \mathbb{Q}(\chi)$, the determinant is just changed by a factor in $\mathbb{Q}(\chi)$.

First case: $\chi(-1) = -1$. Consider the basis $f_1, \dots, f_{n-1}$ of $\log_\infty(\mathcal{O}_F^+)$ introduced in case (i) and let $\tau \in \bar{G}$ denote the complex conjugate with $F^+ = F^\tau$. Since $\chi(\tau) = \chi(-1) = -1$ and $\tau\varepsilon = \varepsilon$ for the fundamental units $\varepsilon \in \mathcal{O}_F^+$ one computes

$$\begin{aligned} e_\chi f_k &= \frac{1}{|\bar{G}|}\sum_{\sigma\in\bar{G}} \chi(\sigma)\sigma^{-1} f_k = \frac{1}{|\bar{G}|}\sum_{\sigma\in\bar{G}/\langle\tau\rangle} \big(\chi(\sigma)\sigma^{-1} f_k + \chi(\sigma\tau)\tau^{-1}\sigma^{-1} f_k\big) \\ &= 0 \qquad\qquad\qquad\qquad \text{for } k = 1,\dots,t \\ \text{and}\quad e_\chi f_{t+j} &= e_\chi(2\pi \mathrm{i} b_{r_1+j} - 2\pi\mathrm{i} b_{r_1+r_2+j}) \\ &= 4\pi\mathrm{i}\chi(\sigma_{r_1+j}) e_\chi b_1 \qquad \text{for } j = 1,\dots,r_2. \end{aligned}$$

One notices again that the $\mathbb{Q}(\chi)$-rank is one, and a basis for $\log_\infty(\mathcal{O}_F^+)\otimes_\mathbb{Z}\mathbb{Q}(\chi)$ is $e_\chi f_{t+1}$. The above computations also show that the base change from $e_\chi b_1$ to $e_\chi f_{t+1}$ has determinant $(4\pi\mathrm{i}\chi(\sigma_{r_1+1}))^{-1}$ with σ_{r_1+1} denoting a fixed complex embedding.

Second case: $\chi(-1) = 1$. In analogy to the above case, one verifies $e_\chi f_{t+j} = 0$ for $j = 1,\dots,r_2$. This also includes the case where F is totally real and $r_2 = 0$.

By [CNT87, Chp. 1, § 3] the element $\varepsilon = \mathrm{N}_{\mathbb{Q}(\zeta_f)|F}(1-\zeta_f)$ is a fundamental unit of $\mathcal{O}_F^+$ and we choose the basis

$$e_\chi \sum_{\sigma\in\bar{G}} \log(\sigma\varepsilon) b_\sigma = \sum_{\sigma\in\bar{G}} \log(\sigma\varepsilon)\chi(\sigma) e_\chi b_1$$

of $\log_\infty(\mathcal{O}_F^+)\otimes_\mathbb{Z}\mathbb{Q}(\chi)$. The determinant of the base change will therefore be the inverse of

$$\begin{aligned} \sum_{\sigma\in\bar{G}} \chi(\sigma)\log\big(\mathrm{N}_{\mathbb{Q}(\zeta_f)|F}(1-\zeta_f)^\sigma\big) &= \sum_{\sigma\in\bar{G}}\chi(\sigma)\sum_{\tau\in\Gamma_1}\log|1-\zeta_f^{\sigma\tau}| \\ &= \sum_{\sigma\in\Gamma}\chi(\sigma)\log|1-\zeta_f^\sigma| = \sum_{a=1}^{f}\chi(a)\log|1-\zeta_f^a| \end{aligned}$$

in this case.

In conclusion one has

$$\det\nolimits_\chi(A) = \begin{cases} \lambda_\chi\tau(\bar{\chi})\big(4\pi\mathrm{i}\chi(\sigma_{r_1+1})\big)^{-1} & \text{for } \chi(-1) = -1 \\ \lambda_\chi\tau(\bar{\chi})\Big(\displaystyle\sum_{a=1}^{f}\chi(a)\log|1-\zeta_f^a|\Big)^{-1} & \text{for } \chi(-1) = 1 \end{cases}$$

for some factor $\lambda_\chi \in \mathbb{Q}(\chi)$. The relations of Gauss sums from [Was97, Lem. 4.7 and 4.8] show that $\tau(\chi)\tau(\bar{\chi}) = \tau(\chi)\overline{\tau(\chi)}\chi(-1) = \chi(-1)|\tau(\chi)|^2 = \chi(-1)f$. Then a comparison with (6.12) show that every product $L^*_{F|\mathbb{Q},S}(\chi,1)\det_\chi(A)$ has values in $\mathbb{Q}(\chi)$ and can therefore be computed exactly.

As a result, the product $\zeta^*_{L|K,S}(1)\,\mathrm{nr}(A)$ can be computed exactly in $\mathrm{Z}(\mathbb{Q}[G])^\times = \prod_{\chi\in\mathrm{Irr}_\mathbb{Q}(G)}\mathbb{Q}(\chi)^\times$. □

Remarks 6.16. 1. For an implementation, the result above is actually not accurate enough because one will need the factor $\lambda_\chi \in \mathbb{Q}(\chi)$ explicitly. To compute this factor one will have to analyze every index that is introduced by the choice of the bases in the proof.

2. If $m > 1$ in the equation (6.9) obtained from Artin's induction theorem, then we would get

$$\left(\det_\chi(A) L^*_{L|\mathbb{Q},S}(\chi,1)\right)^m = \prod_{H \subseteq G} \det_{\mathrm{ind}_H^G 1_H}(A)^{n_H} \zeta^*_{F,S}(1)^{n_H}$$

instead of (6.10) in the proof above. Then we can just compute the m-th power ξ^m of the value $\xi = \det_\chi(A) L^*_{L|\mathbb{Q},S}(\chi,1)$ exactly. By considering an appropriate number field extension, we could compute all the m-th roots of ξ^m exactly and use numerical approximations as in Algorithm 6.11 to find the right one among them.

Appendix

Appendix A

Computational results for the epsilon constant conjecture

A.1 Local Galois groups up to degree 15

In Section 5.3.2 we applied several heuristics to find global representations of local Galois extensions $L|\mathbb{Q}_p$ up to degree 15 with primes $p \leq 15$. Table A.1 gives an overview of all Galois groups which occur up to this degree and how many of them are represented by polynomials in the database of Klüners and Malle [KM01].

This result was obtained by computing all local extensions of degree $n \leq 15$ of $\mathbb{Q}_p$ with $p|n$ using Pauli's implementation in Magma of the algorithm described in [PR01] and searching the database [KM01] for appropriate polynomials. The computation of all those extensions can be very time-consuming, especially for extensions $L|\mathbb{Q}_2$ of degree 8 and extensions $L|\mathbb{Q}_3$ of degree 9. We therefore also use the database [JR] which list all local extensions of $\mathbb{Q}_p$ up to degree $n \leq 11$ for $p|n$.

In the table we use the following common notations:

- A_n is the alternating group of order $n!/2$,
- C_n is the cyclic group of order n,
- D_n is the dihedral group of order $2n$,
- Q_n is the generalized quaternion group of order n,
- S_n is the symmetric group of order $n!$, and
- V_4 is the Klein four-group $C_2 \times C_2$.

n	p	group	#ext.	in [KM01]	n	p	group	#ext.	in [KM01]
2	2	C_2	7	✓	10	5	D_5	3	✓
3	3	C_3	4	✓	11	11	C_{11}	12	1
4	2	C_4	12	✓	12	2	C_{12}	12	8
		V_4	7	✓			$C_3 \times V_4$	11	✓
5	5	C_5	6	✓			A_4	1	✓
6	2	C_6	7	✓			D_6	3	✓
		S_3	1	✓			Q_{12}	4	✓
	3	C_6	12	✓		3	C_{12}	8	4
		S_3	6	✓			$C_3 \times V_4$	4	2
7	7	C_7	8	2			A_4	0	
8	2	C_8	24	8			D_6	6	✓
		$C_2 \times C_4$	18	17			Q_{12}	2	✓
		C_2^3	1	✓	13	13	C_{13}	14	1
		D_4	18	15	14	2	C_{14}	7	✓
		Q_8	6	✓			D_7	0	
9	3	C_9	12	9		7	C_{14}	24	3
		C_3^2	1	✓			D_7	3	0
10	2	C_{10}	7	✓	15	3	C_{15}	4	✓
		D_5	0			5	C_{15}	6	2
10	5	C_{10}	18	6					

Table A.1: Local Galois extensions over $\mathbb{Q}_p$ of degree $n \leq 15$ with primes p dividing n.

A.2 Computations in the proof of Theorem 5.16

The following pages present an overview of the computations for the proof of the local epsilon constant conjecture for

- abelian wildly ramified extensions over $\mathbb{Q}_2$ of degree ≤ 6, and
- non-abelian wildly ramified extensions of degree ≤ 15

as in Theorem 5.16.

The tables below give a complete list of all non-isomorphic extensions which occur in those cases. These extensions can be computed as presented by Pauli and Roblot in [PR01]. Their algorithm was implemented in Magma[1] and Pari/Gp[2]. Up to degree 11 one can also find polynomial generating these extensions in the database of local fields by Jones and Roberts [JR]. This gives a total list of 52 non-abelian extensions and 37 abelian extensions of $\mathbb{Q}_2$.

For each such extensions M of $\mathbb{Q}_p$ we list the following information:

(a) The non-abelian Galois group G of $M/\mathbb{Q}_p$ and the prime p dividing $|G|$.

(b) A polynomial from the database of local fields [JR] generating the extension M locally (only possible up to degree 11).

(c) A polynomial generating a global representation of $M/\mathbb{Q}_p$. These polynomials were mostly found using the database of Klüners and Malle [KM01], as discussed in Section 5.3.2.

(d) The ramification index of p in M.

(e) A polynomial generating the cyclic extension N in which the unramified term is computed (also discussed in Section 5.3.2).

(f) The degree of the composite field E, in which all computations take place.

(g) The time needed to verify the local conjecture for $M/\mathbb{Q}_p$.

More details on every single computation can be found in the log-files on the enclosed CD. All computations were performed with Magma version 2.15-9 on a dual core AMD Opteron machine with 1.8 GHz and 16 GB memory. The hardest case is one of the D_5-extensions which took about 7 days.

[1]command: `AllExtensions`
[2]command: `padicfields`

group	p	local polynomial	global polynomial	e	N	$\deg(E)$	time
C_2	2	x^2+2x+2	x^2-7	2	x^2+x+1	8	1s
C_2	2	x^2+2x-2	x^2-3	2	x^2+x+1	4	1s
C_2	2	x^2+2	x^2-14	2	x^2+x+1	16	2s
C_2	2	x^2+10	x^2-6	2	x^2+x+1	8	2s
C_2	2	x^2+6	x^2-10	2	x^2+x+1	16	3s
C_2	2	x^2+14	x^2-2	2	x^2+x+1	8	3s
C_2	2	x^2-x+1	x^2-x-1	1	x^2-x-1	2	1s
C_4	2	x^4+4x^2+10	x^4-60x^2+810	4	$x^4+x^3+x^2+x+1$	64	1m
C_4	2	x^4+8x+6	x^4-60x^2+90	4	$x^4+x^3+x^2+x+1$	64	1m
C_4	2	x^4+12x^2+10	x^4-20x^2+10	4	$x^4+x^3+x^2+x+1$	32	15s
C_4	2	$x^4+8x^2+8x+22$	x^4-20x^2+90	4	$x^4+x^3+x^2+x+1$	32	20s
C_4	2	x^4+4x^2+18	x^4-12x^2+18	4	$x^4+x^3+x^2+x+1$	64	45s
C_4	2	$x^4+8x+14$	$x^4-32x^2-56x+46$	4	$x^4+x^3+x^2+x+1$	64	2m
C_4	2	x^4+12x^2+18	$x^4-24x^2-40x+14$	4	$x^4+x^3+x^2+x+1$	32	40s
C_4	2	x^4+12x^2+2	x^4-4x^2+2	4	$x^4+x^3+x^2+x+1$	32	45s

Table A.2: Galois extensions of $\mathbb{Q}_2$ with abelian group and possible wild ramification up to degree 6.

group	p	local polynomial	global polynomial	e	N	$\deg(E)$	time
C_4	2	$x^4 - x^2 + 5$	$x^4 - 5x^2 + 5$	2	$x^4 + 20x^2 + 80$	8	15s
C_4	2	$x^4 - 2x^2 + 20$	$x^4 - 10x^2 + 20$	2	$x^4 + 20x^2 + 80$	16	15s
C_4	2	$x^4 + 2x^2 + 20$	$x^4 + 2x^3 - 31x^2 - 62x + 121$	2	$x^4 + 20x^2 + 80$	32	25s
C_4	2	$x^4 - x + 1$	$x^4 - x^3 - 4x^2 + 4x + 1$	1	$x^4 - x^3 - 4x^2 + 4x + 1$	8	4s
V_4	2	$x^4 + 6x^2 + 1$	$x^4 - 8x^2 + 9$	4	$x^4 + x^3 + x^2 + x + 1$	32	5s
V_4	2	$x^4 + 2x^2 + 4x + 10$	$x^4 - 8x^2 + 1$	4	$x^4 + x^3 + x^2 + x + 1$	32	10s
V_4	2	$x^4 + 6x^2 + 4x + 14$	$x^4 - 4x^2 + 1$	4	$x^4 + x^3 + x^2 + x + 1$	32	10s
V_4	2	$x^4 + 6x^2 + 4x + 6$	$x^4 - 20x^2 + 25$	4	$x^4 + x^3 + x^2 + x + 1$	32	20s
V_4	2	$x^4 + 6x^2 + 1$	$x^4 - 8x^2 + 9$	4	$x^4 + x^3 + x^2 + x + 1$	32	20s
V_4	2	$x^4 + 6x^2 + 4x + 6$	$x^4 - 20x^2 + 25$	4	$x^4 + x^3 + x^2 + x + 1$	32	20s
V_4	2	$x^4 + 2x^2 + 4x + 10$	$x^4 - 8x^2 + 1$	4	$x^4 + x^3 + x^2 + x + 1$	32	30s
V_4	2	$x^4 + 6x^2 + 4x + 14$	$x^4 - 4x^2 + 1$	4	$x^4 + x^3 + x^2 + x + 1$	32	30s
V_4	2	$x^4 + 8x^2 + 4$	$x^4 + 2x^3 - 10x^2 + 4x + 4$	2	$x^4 - 60x^2 + 720$	16	10s
V_4	2	$x^4 - 2x^2 + 4$	$x^4 - 18x^2 + 36$	2	$x^4 + 100x^2 + 2000$	32	45s
V_4	2	$x^4 - 6x^2 + 4$	$x^4 - 6x^2 + 4$	2	$x^4 + 20x^2 + 80$	16	1m

Table A.2: (continued)

group	p	local polynomial	global polynomial	e	N	deg(E)	time
C_6	2	$x^6+2x^4+x^2-7$	$x^6-7x^4+14x^2-7$	2	$x^6-x^5-7x^4+2x^3+7x^2-2x-1$	48	15s
C_6	2	$x^6-2x^4+x^2-3$	$x^6-6x^4+9x^2-3$	2	$x^6-9x^4-4x^3+9x^2+3x-1$	24	10s
C_6	2	$x^6-4x^4+4x^2+8$	$x^6-14x^4+56x^2-56$	2	$x^6-x^5-7x^4+2x^3+7x^2-2x-1$	96	7m
C_6	2	$x^6+4x^4+4x^2-24$	$x^6-12x^4+36x^2-24$	2	$x^6-9x^4-4x^3+9x^2+3x-1$	48	35s
C_6	2	$x^6-4x^4+4x^2+24$	$x^6-44x^4-14x^3+349x^2-322x-41$	2	$x^6-x^5-7x^4+2x^3+7x^2-2x-1$	48	1m
C_6	2	$x^6+4x^4+4x^2-8$	$x^6-10x^4+24x^2-8$	2	$x^6-x^5-7x^4+2x^3+7x^2-2x-1$	48	45s
C_6	2	x^6-x+1	$x^6-x^5-7x^4+2x^3+7x^2-2x-1$	1	$x^6-x^5-7x^4+2x^3+7x^2-2x-1$	12	5s

Table A.2: (continued)

group	p	local polynomial	global polynomial	e	N	$\deg(E)$	time
S_3	3	x^6+3x^2+3	$x^6-3x^5-6x^4+17x^3+9x^2-18x+4$	6	x^2+1	24	10s
S_3	3	x^6+3	x^6+3	6	x^2+1	36	25s
S_3	3	x^6+12	$x^6-18x^4-24x^3+27x^2+36x-6$	6	x^2+1	72	3m
S_3	3	x^6+21	$x^6-36x^4+12x^3+27x^2-18x+3$	6	x^2+1	72	4m
S_3	3	x^6+6x^2+6	$x^6-3x^5-6x^4+17x^3-6x^2-3x+1$	6	x^2+1	24	1m
S_3	3	x^6+9x^2+9	$x^6+3x^5-18x^4+9x^3+24x^2-15x-5$	3	x^2+3x-9	36	6m
D_4	2	x^8+12x^4+16	$x^8-2x^7-20x^6+16x^5+63x^4-16x^3-20x^2+2x+1$	4	$x^4+x^3+x^2+x+1$	64	1m
D_4	2	x^8+12x^4+144	$x^8+4x^7-12x^6-74x^5-85x^4+50x^3+142x^2+78x+13$	4	x^4+26x^2+117	32	3m
D_4	2	$x^8+6x^6+6x^4+8x^3+4x^2+8x+20$	$x^8-40x^6+84x^5+285x^4-1176x^3+1418x^2-672x+109$	4	$x^4+x^3+x^2+x+1$	64	2m
D_4	2	$x^8+4x^6+40x^2+4$	$x^8-16x^6+75x^4-88x^2+1$	4	x^4+26x^2+117	64	1m
D_4	2	$x^8+8x^5+6x^4+16x^3+8x^2+12$	$x^8+4x^7-22x^6-80x^5+139x^4+416x^3-262x^2-484x+139$	4	x^4+20x^2+80	64	3m
D_4	2	$x^8+12x^6+10x^4+8x^2+36$	$x^8-4x^7-22x^6+80x^5+91x^4-320x^3-118x^2+292x-29$	4	x^4-80x^2+1280	64	5m

Table A.3: Local Galois extensions with non-abelian Galois group and wild ramification up to degree 11.

group	p	local polynomial	global polynomial	e	N	deg(E)	time
D_4	2	$x^8+4x^7+2x^4+4x^2+14$	$x^8+4x^7-28x^6-68x^5+292x^4+212x^3-940x^2+92x+529$	8	$x^4+x^3+x^2+x+1$	64	7m
D_4	2	$x^8+4x^7+10x^4+4x^2+14$	$x^8-4x^7-4x^6+20x^5+4x^4-20x^3-4x^2+4x+1$	8	$x^4+x^3+x^2+x+1$	64	8m
D_4	2	$x^8+4x^7+10x^4+4x^2+6$	$x^8-20x^6+160x^4-600x^2+4356$	8	$x^4+x^3+x^2+x+1$	64	11m
D_4	2	$x^8+4x^7+14x^4+12x^2+10$	x^8+38x^4+1	8	$x^4+x^3+x^2+x+1$	32	12m
D_4	2	$x^8+4x^7+6x^4+12x^2+2$	$x^8-4x^7-20x^6+32x^5+162x^4+136x^3-20x^2-56x-14$	8	$x^4+x^3+x^2+x+1$	64	18m
D_4	2	x^8+152x^4+16	$x^8+16x^6+52x^4+64x^2+36$	8	$x^4+x^3+x^2+x+1$	32	16m
D_4	2	$x^8+4x^7+2x^4+4x^2+6$	$x^8+20x^6+160x^4+600x^2+4356$	8	$x^4+x^3+x^2+x+1$	64	22m
D_4	2	$x^8+4x^7+14x^4+12x^2+2$	$x^8-4x^7-8x^6+24x^5+30x^4-16x^3-20x^2+2$	8	$x^4+x^3+x^2+x+1$	64	20m
D_4	2	$x^8+2x^4+8x^3+12x^2+8x+18$	$x^8-12x^6+24x^4-12x^2+1$	8	$x^4+x^3+x^2+x+1$	64	26m
D_4	2	x^8+44x^4+100	$x^8-20x^6+48x^4-20x^2+1$	8	$x^4+x^3+x^2+x+1$	64	33m
D_4	2	$x^8+12x^6+6x^4+4x^2+8x+2$	$x^8-64x^6+168x^5+886x^4-5040x^3+9120x^2-6552x+1233$	8	$x^4+x^3+x^2+x+1$	64	35m
D_4	2	x^8+52x^4+36	$x^8-80x^6+1972x^4-14880x^2+36$	8	$x^4+x^3+x^2+x+1$	64	45m

Table A.3: (continued)

group	p	local polynomial	global polynomial	e	N	deg(E)	time
Q_8	2	$x^8+8x^6+6x^4+16x^2+16x+4$	$x^8-60x^6+810x^4-1800x^2+900$	4	$x^4+x^3+x^2+x$	128	20m
Q_8	2	$x^8+8x^7+8x^5+6x^4+24x^2+12$	$x^8-60x^6+1170x^4-9000x^2+22500$	4	$x^4+x^3+x^2+x$	128	17m
Q_8	2	$x^8+14x^4+8x^3+12x^2+8x+14$	$x^8-12x^6+36x^4-36x^2+9$	8	$x^4+x^3+x^2+x$	64	3m
Q_8	2	$x^8+8x^7+14x^4+8x^3+12x^2+8x+22$	$x^8-96x^6+168x^5+1566x^4-504x^3-10188x^2-14616x-6282$	8	$x^4+x^3+x^2+x$	128	45m
Q_8	2	$x^8+14x^4+8x^3+12x^2+8x+30$	$x^8-80x^6+264x^5+396x^4-2040x^3+184x^2+2832x+409$	8	$x^4+x^3+x^2+x$	64	2m
Q_8	2	$x^8+4x^6+2x^4+4x^2+8x+6$	$x^8-84x^6+2268x^4-19404x^2+441$	8	$x^4+x^3+x^2+x$	128	25m
D_5	5	$x^{10}+15x^4+5$	$x^{10}+10x^9-55x^8-350x^7+640x^6+2350x^5-2315x^4-4250x^3+825x^2+1800x+320$	10	x^2+x+1	40	1m
D_5	5	$x^{10}+5x^4+10$	$x^{10}-5x^9-20x^8+110x^7+50x^6-556x^5+245x^4+575x^3-260x^2-140x+49$	10	x^2+x+1	80	3m
D_5	5	$x^{10}+10x^9+35x^8+5x^7+115x^6+105x^4+20x^3+30x^2+10x+32$	$x^{10}-10x^8+30x^7+90x^6-162x^5+125x^4+90x^3-80x^2-120x+144$	5	$x^2-20x+400$	200	7days

Table A.3: (continued)

group	p	global polynomial	e	N	deg(E)	time
A_4	2	$x^{12}-6x^{11}-30x^{10}+182x^9+173x^8-1432x^7+628x^6+1472x^5-173x^4-650x^3-238x^2-30x-1$	4	$x^3-6x^2-40x-8$	48	90s
D_6	2	$x^{12}-6x^{11}-3x^{10}+64x^9-30x^8-234x^7+121x^6+354x^5-132x^4-192x^3+51x^2+18x-3$	6	$x^4+x^3+x^2+x+1$	96	10m
D_6	2	$x^{12}-22x^{10}+120x^8-252x^6+220x^4-72x^2+4$	6	$x^4+592x^2+85248$	96	6m
D_6	2	$x^{12}-24x^{10}+192x^8-628x^6+864x^4-408x^2+4$	6	$x^4+x^3+x^2+x+1$	192	4h
D_6	3	$x^{12}-27x^{10}-20x^9+210x^8+240x^7-525x^6-750x^5+255x^4+670x^3+318x^2+60x+4$	6	x^4-50x^2+500	48	3m
D_6	3	$x^{12}+6x^{11}-15x^{10}-130x^9-6x^8+822x^7+665x^6-1494x^5-1305x^4+1132x^3+612x^2-384x+4$	6	x^4-8x^2+8	48	7m
D_6	3	$x^{12}-72x^{10}+40x^9+1581x^8-1800x^7-11068x^6+20280x^5+12636x^4-47920x^3+33168x^2-8640x+736$	6	x^4-20x^2+50	144	4h
D_6	3	$x^{12}-6x^{11}+21x^{10}-50x^9+90x^8-126x^7+135x^6-108x^5+135x^4-170x^3+66x^2+12x+4$	6	$x^4+x^3+x^2+x+1$	144	42m
D_6	3	$x^{12}-36x^{10}+24x^9+324x^8-180x^7-1134x^6+324x^5+1593x^4+108x^3-810x^2-324x-18$	6	x^4-16x^2+32	144	6h
D_6	3	$x^{12}+6x^{11}-27x^{10}-196x^9-57x^8+780x^7+230x^6-1032x^5+87x^4+430x^3-171x^2+12x+1$	6	x^4+10x^2+20	144	10h

Table A.4: Local Galois extensions with non-abelian Galois group and wild ramification up to degree 15.

group	p	global polynomial	e	N	deg(E)	time
Q_{12}	2	$x^{12}-6x^{11}-30x^{10}+190x^9+171x^8-1740x^7+124x^6+6420x^5-2409x^4-9630x^3+3330x^2+5214x-659$	6	x^4-140x^2+3920	48	30m
Q_{12}	2	$x^{12}-6x^{11}-5x^{10}+90x^9+386x^8-2830x^7+79x^6+24130x^5+33026x^4-234990x^3+63675x^2+1330954x+3527681$	6	$x^4+1690x^2+710645$	192	18h
Q_{12}	2	$x^{12}-10x^{11}-53x^{10}+550x^9+1826x^8-10850x^7-41997x^6+56794x^5+408280x^4+416390x^3-440067x^2-970982x-422951$	6	$x^4-444x^2+47952$	96	30m
Q_{12}	2	$x^{12}-24x^{10}-10x^9+216x^8+180x^7-844x^6-1080x^5+1056x^4+2200x^3+720x^2-240x-80$	3	$x^4-42x^3+504x^2-918x-7209$	48	90s
Q_{12}	3	$x^{12}-24x^{10}-10x^9+216x^8+180x^7-844x^6-1080x^5+1056x^4+2200x^3+720x^2-240x-80$	6	x^4+20x^2+80	144	3h
Q_{12}	3	$x^{12}-6x^{11}-30x^{10}+190x^9+171x^8-1740x^7+124x^6+6420x^5-2409x^4-9630x^3+3330x^2+5214x-659$	3	$x^4-96x^3+3186x^2-43416x+202581$	144	5h
D_7	7	$x^{14}-7x^{13}+21x^{12}-35x^{11}+35x^{10}-35x^8+65x^7-35x^6+35x^4-35x^3+21x^2-7x+1$	14	x^2+1	84	5m
D_7	7	$x^{14}+14x^{12}+63x^{10}+728x^8+7231x^6+9702x^4+3969x^2+61236$	14	x^2+1	168	3h
D_7	7	$x^{14}-112x^{12}+2982x^{10}-20608x^8+55321x^6-62496x^4+27216x^2-3456$	7	$x^2-462x-211239$	84^*	3h

Table A.4: (continued)

*The degree of the compositum E in this example would have been 588! It could only be reduced to 84 after computing the epsilon constants which were all rational.

Appendix B

Magma Packages

The following sections give an overview of algorithms that were implemented in Magma. The four packages we describe below are:

Brauer groups: A package for computations in local and global Brauer groups as well as algorithms for local fundamental classes.

Global fundamental class: This package contains the algorithms for global fundamental classes described in Chapter 3.

Global representations: This combines the heuristic methods for the construction of global representations described in Section 5.3.1.

Local epsilon constant conjecture: This package is the most comprehensive of these four. It includes all the algorithms and methods described in Chapter 5 for the computational proof of the local epsilon constant conjecture.

B.1 Brauer groups

Filename: brauer.m

This package contains methods to compute in local and global Brauer groups as well as algorithms for the local fundamental class.

Basic usage and examples

Let $L|\mathbb{Q}$ be a finite extensions and $\mathfrak{P}$ a prime ideal of p above L. Then we can compute the local Brauer group $\hat{H}^2(G, L_{\mathfrak{P}}^\times)$ by:

```
> rec := LocalBrauerGroup(L,3);
```

It returns a record, which contains all the important structures which are computed by Algorithm 2.3.

To compute the local fundamental class in this group one can either use the command `LocalFundamentalClassDirect` (which will also compute the cohomology group itself) or the command `LocalFundamentalClassSerre`. Both functions take the completion $L_{\mathfrak{P}}$ and a precision of computation as input:

```
> LP, iota := Completion(L, P : Precision := 300);
> c := LocalFundamentalClassSerre(LP, pAdicField(LP), 30);
```

For the computation in the global Brauer group $\hat{H}^2(G, L^\times)$ we can use the command `GlobalCocycle` to construct element by through local conditions

```
> L := SplittingField(x^3+9);
> c := GlobalCocycle(L, [ <2, 1/2>, <3, 1/2> ]);
```

The global cocycle is computed as a representative $C^2(G, U_{L,S})$ with appropriate set of places S. In other words `c` is a map $G \times G \to U_{L,S}$. Given such a global cocycle, one can identify the invariants using `GlobalCocycleInvariants`:

```
> GlobalCocycleInvariants(L,c);
```

Documentation

For local Brauer groups the following structure is defined:

```
locBrGrp := recformat<
    L : FldNum,         P : RngOrdIdl,  p : RngIntElt,
    M : GrpAb,          actM : Map,     qM : Map,
    theta : RngOrdElt,
    C : ModCoho,        f1 : Map,
    lfc : ModTupRngElt
>;
```

It includes the following information as in Algorithm 2.3: the number field L with prime ideal $\mathfrak{P}$ dividing the prime p, the module M from Lemma 2.1 defined by an element $\theta \in L$ with corresponding Galois action and homomorphism $L \to M$, a cohomology module C as computed by `CohomologyModule` with corresponding map f_1 to and from M, and the local fundamental class as element of C.

```
LocalBrauerGroup(L::FldNum, p::RngIntElt) -> Rec
LocalBrauerGroup(L::FldNum, P::RngOrdIdl) -> Rec
```

Optional parameters: `autMap:=0, lfc:=false`
Computes the local cohomology group $\hat{H}^2(G_{\mathfrak{P}}, L_{\mathfrak{P}}^\times)$ for an ideal $\mathfrak{P}$ dividing p as record of type `locBrGrp` using Algorithm 2.3. Optionally one can pass the Galois action on L as map $G \to \mathrm{Aut}(L|K)$ and if `lfc` is true, a representative of the local fundamental class is computed using Algorithm 2.18.

```
LocalFundamentalClassDirect(L::FldPad, n::RngIntElt) -> Map
```

Compute a cocycle representing the local fundamental class of $L|\mathbb{Q}_p$ up to the given precision using the direct method, see Algorithm 2.5.

```
LocalFundamentalClassSerre(L::FldPad, K::FldPad, steps::RngIntElt)
  -> Map
LocalFundamentalClassSerre(L::RngPad, K::RngPad, steps::RngIntElt)
  -> Map
```

Optional parameters: `psi:=0`
Compute the cocycle representing the local fundamental class of $L|K$ up to the given precision using Serre's approach, see Algorithm 2.18. Optionally, one can pass the map $\psi : G \to \mathrm{Aut}(L|K)$ representing the Galois action on L.

```
GlobalCocycleInvariants(L::FldNum, gamma::Map) -> SeqEnum
```

Compute the invariants of the cocycle $\gamma \in \hat{H}^2(G, L^\times)$ for a global Galois extension $L|K$ of number fields with group G, see Algorithm 2.23.

```
GlobalCocycle(L::FldNum, locCond::SeqEnum) -> Map
```

Computes a global cocycle in $\hat{H}^2(G, L^\times)$ respecting the given local conditions. These must be given as sequence of tuples $\langle p, i_p \rangle$ with i_p in $1/|G_{\mathfrak{P}}|\mathbb{Z}$ where $\mathfrak{P}$ is an ideal of L dividing p and $\sum i_p = 0 + \mathbb{Z}$.

```
FrobeniusEquation(c::RngPadElt, precision::RngIntElt)
  -> RngPadElt, Map
FrobeniusEquation(c::RngPadElt, precision::RngIntElt, OK::RngPad)
  -> RngPadElt, Map
FrobeniusEquation(C::SeqEnum, precision::RngIntElt)
  -> SeqEnum, Map
FrobeniusEquation(C::SeqEnum, precision::RngIntElt, OK::RngPad)
  -> SeqEnum, Map
```

Solves the equation $x^{\varphi-1} = c, c$ in $\mathcal{O}_E^\times$, up to the given precision, where φ is the Frobenius automorphism of $\mathcal{O}_K$, see Remark 2.10. The solution x and the automorphism φ are returned. If a sequence C of elements is given, a sequence of solutions is returned. If $\mathcal{O}_K$ is not given, $\mathcal{O}_K = \mathcal{O}_E$ is used. Otherwise, $\mathcal{O}_E$ must be an extension of $\mathcal{O}_K$. Note, that whenever the norm of c over $\mathcal{O}_K$ is not 1, this can generate huge extensions of $\mathcal{O}_E$.

B.2 Global fundamental class

Filename: gfc.m

This package contains methods to compute the global fundamental class.

Basic usage and examples

There exist two commands for the computation of global fundamental classes which correspond to the cyclic case in Section 3.2.1 and the general case in Section 3.2.2.

The cyclic case is not restricted to cyclic extensions but can also be applied to other extensions $L|\mathbb{Q}$ in which there exists a prime p which is undecomposed in L. The following example computes the global fundamental class for a Galois extension $L|\mathbb{Q}$ with group C_6.

```
> L := NumberField(x^6 - 12*x^4 + 36*x^2 - 24);
> time C, f1, gfc := gfcUndecomposed(L, 3);
```

The command computes a cohomology structure `C`, a map `f1` which reads cocycles in this structure and vice versa, and the canonical generator in $\hat{H}^2(G, C_L)$.

For arbitrary extensions $L|\mathbb{Q}$, in which such an undecomposed place does not exist, we need to specify a cyclic extension $N|\mathbb{Q}$ of the same degree. For computational reasons it is essential that the composite field LN has small degree over $\mathbb{Q}$. In the following example we consider an extension $L|\mathbb{Q}$ with group S_3. It has a subfield $\mathbb{Q}(\sqrt{229})$ which can be embedded into a cyclic extension $N|\mathbb{Q}$ of degree 6 with $N \subset \mathbb{Q}(\zeta_{229})$. The composite field will then have degree 18 over $\mathbb{Q}$.

```
> L := SplittingField(x^3 - 4*x + 1);
> L1 := NumberField(x^6 - 4580*x^5 + 517540*x^4 - 17136986*x^3
>    + 164417420*x^2 - 53936828*x + 229);
> time gfcCompositum(L, L1);
```

Documentation

```
gfcUndecomposed(L::FldNum, p0::RngIntElt) -> ModCoho, Map,
  ModTupRngElt
```

Optional parameters: `psiL:=0`
Computes the global fundamental class for a (totally real) number field L in which the prime p_0 is undecomposed, see Section 3.2.1. Optionally one can pass the Galois action on L as map $G \to \mathrm{Aut}(L|\mathbb{Q})$.

```
gfcCompositum(L::FldNum, L1::FldNum) -> ModCoho, Map, ModTupRngElt
```

Given an arbitrary (totally real) Galois extension $L|\mathbb{Q}$ and a cyclic extension $L_1|\mathbb{Q}$ of the same degree, this method computes then global fundamental class of $L|\mathbb{Q}$ as in Algorithm 3.13.

```
trivialSClassNumberPrimes(L::FldNum) -> SeqEnum
```

Optional parameters: `primes:=[]`
Compute a sequence of primes such that the S-class number of all subfields of L is trivial. Optionally specify a set of primes which will be included in S.

```
inducedModule(M::GrpAb, phi::Map, G::Grp) -> GrpAb, Map, SeqEnum,
  SeqEnum, SeqEnum
```

Given a (left) H-module M as abelian group with H-action by $\varphi : H \to \mathrm{Aut}(M)$ and H a subgroup of G. Compute the induced module N as a direct sum and return N, the G-action on N, a left representation system R of G/H, and sequences of embeddings $M \to N$ and projections $N \to M$ according to R.

B.3 Global representations

Filename: globalrep.m

This package contains heuristic methods to compute global representations of local Galois extensions.

Basic usage and examples

The most important command in this package is `GlobalRepresentations`. It can be used to find global representations for local Galois extensions. For example the command

```
> GlobalRepresentations( SymmetricGroup(3), 3 );
```

finds global representations for S_3 extensions of $\mathbb{Q}_3$. This is done by computing all extensions of degree 6 of $\mathbb{Q}_3$ using the command `AllExtensions`, sending an internet request to the database of Klüners and Malle to get a list of polynomials generating S_3 extensions, and selecting appropriate polynomials for the local extensions. The internet request is implemented using the Unix `wget` command and will therefore not work if this command is not available on your system. In this case, a list of candidate polynomials can be passed using the optional parameter `candlist`.

Using the same command, one can also find global representations for multiple Galois groups and primes. And as a last option, one can find global representations for a list of local extensions for which the Galois group is known.

The result presented in Appendix A.1, is found using the following commands

```
> list := [ < SmallGroup(n,i), p > :
>             i in [1..NumberOfSmallGroups(n)],
>             p in [x[1] : x in Factorization(n)],
>             n in [2..15] ];
> GlobalRepresentations( list );
```

However, the computation of all local extensions over $\mathbb{Q}_2$ and $\mathbb{Q}_3$ of degree 8 and 9, respectively, will take a long time.

One can therefore also use the database by Jones and Roberts [JR]. On their website the authors provide files, which contain all those local extensions and corresponding Galois information. After defining a few polynomial rings, one can load these files and compute global representations. As an example, this is done for the degree 8 extensions of $\mathbb{Q}_2$ by the following commands with a computation time of about a minute:

```
> Zy<y> := PolynomialRing(Integers());
> Zt<t> := PolynomialRing(Integers());
> Zx<x> := PolynomialRing(Integers());
> load "JR/Q2deg8a.m";
> GlobalRepresentationsJR( pols, 2 );
```

The two databases can also be accessed directly using `kluenersMallePols` or `jonesRobertsPols`.

Finally, a few formulas of [JLY02] were implemented. With the commands `genericC4Pol` and `genericD4pol` one can construct polynomials generating C_4- and D_4-extensions. And `embeddingC2C4` embeds a given C_2 extension into a C_4-extension, if possible.

Documentation

```
GlobalRepresentations(G::Grp, p::RngIntElt) -> .
GlobalRepresentations(list::SeqEnum) -> .
```

Optional parameters: `JR:=false, candlist:=[]`
Given a Galois group G and a prime p or a list of tuples $\langle G, p\rangle$. For each tuple compute all local extensions of degree $\#G$ of $\mathbb{Q}_p$, and search for global representations using the database by Klüners/Malle. Also shows corresponding polynomials from the database by Jones/Roberts if `JR` is set to true.

```
GlobalRepresentations(ext::SeqEnum, G::Grp) -> SeqEnum
```

Optional parameters: `JR:=false, candlist:=[]`
Given a list of local extensions which have Galois group G. Search for global representations using the database by Klüners/Malle. Also shows corresponding polynomials from the database by Jones/Roberts if `JR` is set to true.

```
GlobalRepresentationsJR(pols::List, p::RngIntElt) -> .
GlobalRepresentationsJR(pols::List, n::RngIntElt, p::RngIntElt) ->.
```

Given a list of polynomials in format of the database by Jones/Roberts, representing extensions of degree n of $\mathbb{Q}_p$. For each Galois group of this degree, select corresponding polynomials from the list and search for global representations using the database by Klüners/Malle.

```
allExtensionsForGroup(G::., p::RngIntElt) -> SeqEnum
```

Optional parameters: `precision:=100, ext:=[]`
Compute all extensions of $\mathbb{Q}_p$ using `AllExtensions` and select those which have the given Galois group. If a list `ext` of extensions is given, this list is being searched for suitable extensions.

```
kluenersMallePols(d::RngIntElt, t::RngIntElt) -> SeqEnum
```

Get all polynomials of degree d with Galois group identifier $\langle d, t\rangle$ from the database by Klüners/Malle. Note that the identifier of Magma does not always agree with the identifier of Klüners/Malle. Depends on an internet connection and the Unix `wget` command.

```
kluenersMallePolsG(G::Grp) -> SeqEnum
```

Get all polynomials with Galois group G from the database by Klüners/Malle. Depends on an internet connection and the Unix `wget` command.

```
jonesRobertsPols(n::RngIntElt, p::RngIntElt) -> SeqEnum
```

Get polynomials generating all extensions of degree n of $\mathbb{Q}_p$ from the database by Jones/Roberts. Depends on an internet connection and the Unix `wget` command.

```
genericC4Pol(s::FldRatElt, t::FldRatElt) -> RngUPolElt
genericC4Pol(s::FldNumElt, t::FldNumElt) -> RngUPolElt
```

Returns the generic C_4-Polynomial for s and t from [JLY02, Cor. 2.2.6]. The given polynomial generates a C_4-extension if $s \neq 0$ and $1 + t^2$ is not a square.

```
genericD4Polynomial(a::., b::. ) -> RngUPolElt
```

If b and $b(a^2-4b)$ are both not square, the polynomial $f = bX^4 + aX^2 + 1$ which generates a D_4 extension is returned. Otherwise an error occurs. See [JLY02, Cor. 2.2.4].

```
randomD4Polynomial(K::., bound::RngIntElt) -> RngUPolElt
```

Optional parameters: `maxTries:=5`
Computes a random polynomial generating a D_4 extension over K.

```
embeddingC2C4(K::FldNum) -> BoolElt, RngUPolElt
```

Optional parameters: `p:=0`
Computes a generating polynomial for a C_4-Extension $L|\mathbb{Q}$ which includes $K|\mathbb{Q}, [K : \mathbb{Q}] = 2$. If p is specified, L will be unramified and undecomposed at p. L can either be created as absolute field over $\mathbb{Q}$ or relative over K. See [JLY02, Thm. 2.2.5].

B.4 Local epsilon constant conjecture

Filenames: epsconj.m, characters.m, artin.m

This package contains algorithms to prove the local epsilon constant conjecture computationally as in Algorithm 5.12, see Chapter 5. Some algorithms are organized in separate files since they might be of independent interest.

Basic usage and examples

The functions for the Local Epsilon Constant Conjecture all start with the prefix `LEC`. The main function is `LECverify` which applies Algorithm 5.12. It requires a global field which is undecomposed at a given prime.

```
> L := NumberField(x^6+3);
> LECverify(L,3);
```

The verification of the conjecture works on a special record-format (`LECrec`) which holds all necessary information. To experiment with specific values of the conjecture (e.g. the equivariant discriminant $d_{L|K}$), one can proceed as follows:

```
> lec := LECcreateRec(L, 3);
> LECverify(~lec);
> lec`dLK;
```

`LECverify` will call the following functions:

- `LECpreparations`: computes the composite field E,
- `LECcomputeValues`: computes all values for the conjecture,
- `LECimagesK0Rel`: read these values in the same relative K-group,
- `LECcheck`: check the conjecture.

Some parts of the algorithm are further split: one can compute each part of the conjecture separately (commands `LECdiscriminant`, `LECcorrectionTerm`, `LECunramifiedTerm`, `LECcohomologicalTerm`, and `LECepsilonConstant`) by either passing an `LEC`-record or all necessary parameters.

The values in the `LEC`-format that already exist will be used by `LECverify`, as far as it makes sense. The algorithm will then omit the computation of those values. This allows to reuse values which are already computed.

In the following example, we discover that the epsilon constants are actually rational numbers. We can then replace the field $\mathbb{Q}(\zeta_m, \zeta_{p^t})$ used to compute the epsilon constants by the field $\mathbb{Q}(\zeta_m)$ and the rest of the conjecture is proved by using a smaller composite field E.

```
> L := NumberField(x^6 + 3*x^5 - 18*x^4 + 9*x^3 + 24*x^2 - 15*x - 5);
> lec := LECcreateRec(L,3);
> LECepsilonConstant(~lec);
> assert &and( [x in Rationals() : x in lec`tLK] );
> lec`tLK := [* Rationals()!t  : t in lec`tLK*];
> lec`Qmpt := CyclotomicField( Exponent(lec`G) );
> LECverify(~lec);
```

This approach was also used in the last example listed in Table A.4, see also the footnote on page 169.

Documentation

```
LECverify(L::FldNum, p::RngIntElt, N::FldNum) -> BoolElt
LECverify(L::FldNum, p::RngIntElt) -> BoolElt
```

Verify the local epsilon constant conjecture for $L|\mathbb{Q}$ at p. N must be an extension of degree $[L^{ab} : \mathbb{Q}]$ such that p is unramified in N. The prime p must not decompose in L or N. If not given, N is found heuristically as a subfield of a cyclotomic field (for $p \neq 2$).

```
LECverify(setting::Rec) -> BoolElt
LECverify(~setting::Rec)
```

Verify the local epsilon constant conjecture for the given setting, as created for example by LECcreateRec. No further checks are made on the given parameters.

```
LECcreateRec(L::FldNum, p::RngIntElt) -> Rec
```

Creates an LEC-record for the number field L and prime p and computes the automorphism group of $L|\mathbb{Q}$.

```
LECpreparations(~setting::Rec)
```

Preparation for the verification of the local epsilon constant conjecture. Computes: a lattice $\mathscr{L}$, the completion of L at $\mathfrak{P}$, the composite field E, and the relative group K-group.

```
LECcomputeValues(~setting::Rec)
```

Optional parameters: `forceAllComputations:=false`
Compute the five terms going into the local epsilon constant conjecture: the equivariant discriminant, the correction term, the unramified term, the cohomological term, and the equivariant epsilon constant.

```
LECimagesK0Rel(~setting)
```

Read all the values of the Epsilon Constant Conjecture, as computed by `LECcomputeValues`, in the same relative K-group.

```
LECcheck(setting) -> BoolElt
LECcheck(~setting)
```

Verify the local epsilon constant conjecture for the given setting, where the reduced norms are already computed.

Methods to compute the values of the conjecture independently

```
LECdiscriminant(psi::Map, theta::RngOrdElt) -> AlgGrpElt
LECdiscriminant(setting::Rec) -> AlgGrpElt
LECdiscriminant(~setting::Rec)
```

Compute the equivariant discriminant of a lattice as described in (5.8), see also [BlBr08, § 4.2.5].

```
LECcorrectionTerm(setting::Rec) -> .
LECcorrectionTerm(~setting::Rec)
LECcorrectionTerm(QG::AlgGrp, psi::Map, P::RngOrdIdl) -> AlgGrpElt
```

Compute the correction term as defined by (5.3).

```
LECunramifiedTerm(psi::Map, p::RngIntElt, N::FldNum) -> AlgGrpElt
LECunramifiedTerm(setting::Rec) -> AlgGrpElt
LECunramifiedTerm(~setting::Rec)
```

Compute the unramified term in $N[G]$ for an extension $L|\mathbb{Q}$, a prime p, $\psi : \mathrm{Gal}(L|\mathbb{Q}) \to \mathrm{Aut}(L)$, and N an unramified extension with $[N : \mathbb{Q}] = [L^{ab} : \mathbb{Q}]$, see (5.9) and also [BlBr08, § 4.2.7].

```
LECcohomologicalTerm(setting::Rec) -> Rec
LECcohomologicalTerm(~setting::Rec)
```

Compute the cohomological term for the local epsilon constant conjecture as described in Section 5.4 on page 125, see also [BlBr08, § 4.2.4].

It depends on several attributes in the `LEC`-record, as computed by `LECcreateRec` and `LECpreparations`. The algorithm first computes a cocycle for the local fundamental class and then continues by computing the splitting module $C(\gamma)$, its projective resolution, and finally the $\mathbb{Q}[G]$-isomorphism between $K + \mathbb{Q}[G]$ and $\mathbb{Q}[G]^r$.

```
LEClattice(P::RngOrdIdl, pi::RngOrdElt, psi::Map) -> FldNumElt,
  RngIntElt
LEClattice(~setting)
```

Given a prime ideal $\mathfrak{P}$ of L with uniformizing element π and automorphism map $\psi : G \to \mathrm{Aut}(L)$. Compute a generator θ of a suitable lattice and an integer m such that the lattice includes $\mathfrak{P}^m$.

For the `LEC`-record, a few suitable lattices are computed and the (computationally) best one is chosen for further computations.

```
LECcomputeLPmulModX(setting::Rec) -> ModTupRng, SeqEnum, Map
```

Compute the module $L^f = L_{\mathfrak{P}}^\times / X, X = \exp(\mathscr{L})$ from Lemma 2.1 for the given setting as well as a sequence of matrices representing the G-action and a map $L_{\mathfrak{P}}^\times \twoheadrightarrow L^f$.

```
LECepsilonConstant(L::FldNum, p::RngIntElt) -> List
LECepsilonConstant(setting::Rec) -> List
LECepsilonConstant(~setting::Rec)
```

Compute epsilon constants as described in in Section 5.4 on page 126, see also [BlBr08, § 2.5]. It depends on several attributes in the `LEC`-record, as computed by `LECpreparations` or `LECprepareEps`.

```
LECprepareEps(~setting::Rec)
```

Compute Brauer inductions of all irreducible characters and the required precision t for the Galois Gauss sums, see [BlBr08, Rem. 2.7].

Functions for norm residue symbols

```
localNormResidueSymbol(x::FldNumElt, N::FldNum, M::FldNum, PM::.)
 -> GrpElt, FldAb
localNormResidueSymbol(x::FldNumElt, Na::FldAb, PM::.) -> GrpElt
```

Let $N|M$ be a global abelian extension, $x \in M^\times$ and $\mathfrak{P}_M$ an ideal of M such that there is just one prime ideal $\mathfrak{P}_N$ in N above $\mathfrak{P}_M$. Compute the local norm residue symbol $(x, N_{\mathfrak{P}_N}/M_{\mathfrak{P}_M})$ in $\mathrm{Gal}(N|M)$. The extension $N|M$ can also be given as abelian field.

```
localNormResidueSymbolAsGlobalIdeal(alpha::FldNumElt, F::SeqEnum,
  PK::RngOrdIdl) -> RngOrdIdl
localNormResidueSymbolAsGlobalIdeal(alpha::FldRatElt, F::SeqEnum,
  PK::RngInt) -> RngOrdIdl
```

Given the factorization F of the Artin conductor of an abelian extension $N|M$, an element α in M and an ideal $\mathfrak{P}_M$ of M such that there is just one prime ideal $\mathfrak{P}_N$ of N above $\mathfrak{P}_M$. Compute an ideal $\mathfrak{a}$ of M such that the global Artin symbol $(\mathfrak{a}, N|M)$ is equal to the local norm residue symbol $(\alpha, N_{\mathfrak{P}_N}/M_{\mathfrak{P}_M})$.

```
globalArtinSymbol(a::RngOrdFracIdl, psi::Map) -> GrpElt
globalArtinSymbol(a::RngInt, psi::Map) -> GrpElt
```

For an abelian extension $N|M$, an ideal $\mathfrak{a}$ in M and $\psi : \mathrm{Gal}(N|M) \to \mathrm{Aut}(L)$. Compute the Artin symbol $(\mathfrak{a}, N|M) \in \mathrm{Gal}(N|M)$.

Functions for characters

```
brauerInductionDeg0(chi::AlgChtrElt) -> SeqEnum
```

Given a character χ of G, compute the Brauer Induction of $\chi - \chi(1)1_G$, i.e. compute triples (H, φ, c), where H is a subgroup of G, φ is a linear character of H, and $c_{H,\varphi}$ is an integer, such that

$$\chi - \chi(1)1_G = \sum_{H,\varphi} c_{H,\varphi} \mathrm{ind}_H^G(\varphi - 1_H).$$

```
conductor(chi::AlgChtrElt, P::RngOrdIdl) -> RngIntElt
conductor(chi::AlgChtrElt, RamGroups::SeqEnum) -> RngIntElt
```

For a character χ of G compute the conductor

$$n(\chi) = \sum_{i=0}^{\infty} \frac{\#G_i}{\#G_0} \operatorname{codim}(V_\chi^{G_i}),$$

where G_i denotes the i-th ramification group of $\mathfrak{P}$. Either the prime $\mathfrak{P}$ or a list of the non-trivial ramification groups is needed.

```
det(chi::AlgChtrElt, lambda::AlgGrpElt) -> AlgMatElt
```

Given $\lambda \in \mathbb{Q}[G]$, compute $\det_\chi(\lambda)$ using Brauer induction and determinants of linear characters.

```
det(chi::AlgChtrElt) -> AlgChtrElt
```

Compute the character ψ given by the linear representation $\psi(g) = \det_\chi(g)$.

```
det(chi::AlgChtrElt, psi::Map, p::RngIntElt, x::FldRatElt) ->
  FldCycElt
```

Given an extension $L|\mathbb{Q}$, a character $\chi \in \operatorname{Irr}(G)$ and $x \in \mathbb{Q}$, compute $\det_\chi(x)$ using Brauer induction. If $N|M$ is the abelian extension for χ, then $\det_\chi(x) = \det_\chi((x, N|M))$. For the definition see [Bre04a, Prop. 3.6(4)].

```
galoisActionOnCharacters(G::Grp, psiG::Map, Irr::SeqEnum) -> Map
```

Given a group G, $\psi : G \to \operatorname{Aut}(L)$ and the irreducible characters of G. Compute the Galois action $G \times \operatorname{Irr}(G) \to \operatorname{Irr}(G)$.

Bibliography

[AK00] Vincenzo Acciaro and Jürgen Klüners. *Computing local Artin maps, and solvability of norm equations.* J. Symbolic Comput. **30** (2000), no. 3, 239–252.

[AT68] Emil Artin and John Tate. *Class field theory.* W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[BCFS10] Wieb Bosma, John Cannon, Claus Fieker and A. Steel, eds. *Handbook of Magma functions.* Edition 2.16, 2010.

[BCP97] Wieb Bosma, John Cannon and Catherine Playoust. *The Magma algebra system I: The user language.* J. Symbolic Comput. **24** (1997), 235–265.

[BF01] David Burns and Matthias Flach. *Tamagawa numbers for motives with (non-commutative) coefficients.* Doc. Math. **6** (2001), 501–570 (electronic).

[BF06] David Burns and Matthias Flach. *On the equivariant Tamagawa number conjecture for Tate motives. II.* Doc. Math. (2006), Extra Vol., 133–163 (electronic).

[BG03] David Burns and Cornelius Greither. *On the equivariant Tamagawa number conjecture for Tate motives.* Invent. Math. **153** (2003), no. 2, 303–359.

[BlB03] Werner Bley and David Burns. *Equivariant epsilon constants, discriminants and étale cohomology.* Proc. Lond. Math. Soc. (3) **87** (2003), no. 3, 545–590.

[BlBr08] Werner Bley and Manuel Breuning. *Exact algorithms for p-adic fields and epsilon constant conjectures.* Illinois J. Math. **52** (2008), no. 3, 773–797.

[Ble10] Werner Bley. *Numerical evidence for the equivariant Birch and Swinnerton-Dyer conjecture.* To appear in Experiment. Math. Preprint 2010.

[Ble03] Werner Bley. *Numerical evidence for a conjectural generalization of Hilbert's Theorem 132. With an appendix by D. Kusnezow.* LMS J. Comput. Math. **6** (2003), 68–88.

[BrB05] Manuel Breuning and David Burns. *Additivity of Euler characteristics in relative algebraic K-groups.* Homology, Homotopy Appl. **7** (2005), no. 3, 11–36.

[BrB07] Manuel Breuning and David Burns. *Leading terms of Artin L-functions at $s = 0$ and $s = 1$.* Compos. Math. **143** (2007), no. 6, 1427–1464.

[Bre04a] Manuel Breuning. *Equivariant epsilon constants for Galois extensions of number fields and p-adic fields.* Ph.D. thesis, King's College, London, May 2004.

[Bre04b] Manuel Breuning. *Equivariant local epsilon constants and étale cohomology.* J. Lond. Math. Soc. (2) **70** (2004), no. 2, 289–306.

[Bro94] Kenneth S. Brown. *Cohomology of groups*, vol. 87 of *Graduate Texts in Mathematics.* Springer, New York, 1994. Corrected reprint of the 1982 original.

[Bur01] David Burns. *Equivariant Tamagawa numbers and Galois module theory. I.* Compos. Math. **129** (2001), no. 2, 203–237.

[Bur04] David Burns. *Equivariant Whitehead torsion and refined Euler characteristics.* In *Number theory*, vol. 36 of *CRM Proc. Lecture Notes*, pages 35–59. Amer. Math. Soc., Providence, RI, 2004.

[BW09] Werner Bley and Stephen M. J. Wilson. *Computations in relative algebraic K-groups.* LMS J. Comput. Math. **12** (2009), 166–194.

[CCFT91] Philippe Cassou-Noguès, Ted Chinburg, Albrecht Fröhlich and Martin J. Taylor. *L-functions and Galois modules.* In *L-functions and arithmetic (Durham, 1989)*, vol. 153 of *London Math. Soc. Lecture Note Ser.*, pages 75–139. Cambridge Univ. Press, Cambridge, 1991. Based on notes by D. Burns and N. P. Byott.

[Chi84] Ted Chinburg. *Multiplicative Galois module structure.* J. Lond. Math. Soc. (2) **29** (1984), no. 1, 23–33.

[Chi85] Ted Chinburg. *Exact sequences and Galois module structure.* Ann. of Math. (2) **121** (1985), no. 2, 351–376.

[Chi89] Ted Chinburg. *The analytic theory of multiplicative Galois structure.* Mem. Amer. Math. Soc. **77** (1989), no. 395, iv+158.

[CNT87] Philippe Cassou-Noguès and Martin J. Taylor. *Elliptic functions and rings of integers.* Birkhäuser Boston Inc., Boston, MA, 1987.

[Coh93] Henri Cohen. *A course in computational algebraic number theory.* Springer, Berlin, 1993.

[Coh00] Henri Cohen. *Advanced topics in computational number theory*, vol. 193 of *Graduate Texts in Mathematics.* Springer, New York, 2000.

[CR62] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras.* Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962.

[CR81] Charles W. Curtis and Irving Reiner. *Methods of representation theory. Vol. I.* John Wiley & Sons Inc., New York, 1981.

[CR87] Charles W. Curtis and Irving Reiner. *Methods of representation theory. Vol. II.* John Wiley & Sons Inc., New York, 1987.

[Dok04] Tim Dokchitser. *Computing special values of motivic L-functions.* Experiment. Math. **13** (2004), no. 2, 137–149.

[Fie06] Claus Fieker. *Applications of the class field theory of global fields.* In *Discovering mathematics with Magma*, pages 31–62. Springer, Berlin, 2006.

[Fla04] Matthias Flach. *The equivariant Tamagawa number conjecture: a survey.* In *Stark's conjectures: recent work and new directions*, vol. 358 of *Contemp. Math.*, pages 79–125. Amer. Math. Soc., Providence, RI, 2004. With an appendix by C. Greither.

[Frö78] Albrecht Fröhlich. *Some problems of Galois module structure for wild extensions.* Proc. Lond. Math. Soc. (3) **37** (1978), no. 2, 193–212.

[Frö83] Albrecht Fröhlich. *Galois module structure of algebraic integers.* Springer, Berlin, 1983.

[FS82] Burton Fein and Murray Schacher. *Relative Brauer groups. III.* J. Reine Angew. Math. **335** (1982), 37–39.

[Gir99] Kurt Girstmair. *An algorithm for the construction of a normal basis.* J. Number Theory **78** (1999), no. 1, 36–45.

[Gre10] Christian Greve. *Galoisgruppen von Eisensteinpolynomen über p-adischen Körpern.* Ph.D. thesis, Universität Paderborn, Oct. 2010.

[GRW99] Karl W. Gruenberg, Jürgen Ritter and Alfred Weiss. *A local approach to Chinburg's root number conjecture.* Proc. Lond. Math. Soc. (3) **79** (1999), no. 1, 47–80.

[Hen01] Guy Henniart. *Relèvement global d'extensions locales: quelques problèmes de plongement.* Math. Ann. **319** (2001), no. 1, 75–87.

[Hol06] Derek F. Holt. *Cohomology and group extensions in Magma.* In *Discovering mathematics with Magma*, pages 221–241. Springer, Berlin, 2006.

[HS71] Peter J. Hilton and Urs Stammbach. *A course in homological algebra.* Springer, New York, 1971. Graduate Texts in Mathematics, Vol. 4.

[Jan10] Dörthe Janssen. *Ein Algorithmus zur numerischen Verifikation der äquivarianten Tamagawazahlvermutung für eine Familie von Zahlkörpererweiterungen.* Ph.D. thesis, Universität Kassel, Apr. 2010.

[JLY02] Christian U. Jensen, Arne Ledet and Noriko Yui. *Generic Polynomials.* Cambridge University Press, 2002.

[JR] John W. Jones and David P. Roberts. *Database of local fields.* URL `http://math.la.asu.edu/~jj/localfields/`.

[Ker07] Ina Kersten. *Brauergruppen.* Universitätsverlag Göttingen, 2007.

[KM01] Jürgen Klüners and Gunter Malle. *A database for field extensions of the rationals.* LMS J. Comput. Math. **4** (2001), 182–196. URL `http://www.math.uni-duesseldorf.de/~klueners/minimum/`.

[Lan02] Serge Lang. *Algebra*, vol. 211 of *Graduate Texts in Mathematics.* Springer, New York, third edn., 2002.

[Mac75] Saunders MacLane. *Homology*, vol. 114 of *Die Grundlehren der mathematischen Wissenschaften.* Springer, Berlin, third edn., 1975.

[Mar77] Jacques Martinet. *Character theory and Artin L-functions.* In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 1–87. Academic Press, London, 1977.

[Mil80] James S. Milne. *Étale cohomology*, vol. 33 of *Princeton Mathematical Series.* Princeton University Press, Princeton, N.J., 1980.

[Neu69] Jürgen Neukirch. *Klassenkörpertheorie.* Bibliographisches Institut Mannheim, 1969. B. I-Hochschulskripten, 713/713a*.

[Neu92] Jürgen Neukirch. *Algebraische Zahlentheorie.* Springer, 1992.

[NSW00] Jürgen Neukirch, Alexander Schmidt and Kay Wingberg. *Cohomology of number fields.* Springer, Berlin, 2000.

[Par08] The PARI Group, Bordeaux. *PARI/GP, version 2.3.4*, 2008. URL `http://pari.math.u-bordeaux.fr`.

[Pau06] Sebastian Pauli. *Constructing class fields over local fields.* J. Théor. Nombres Bordeaux **18** (2006), no. 3, 627–652.

[PR01] Sebastian Pauli and Xavier-François Roblot. *On the computation of all extensions of a p-adic field of a given degree.* Math. Comp. **70** (2001), 1641–1659.

[Rei03] Irving Reiner. *Maximal orders*, vol. 28 of *London Mathematical Society Monographs. New Series.* The Clarendon Press Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original, with a foreword by M. J. Taylor.

[Rot05] Stefan Rothbauer. *Algorithmische Berechnung von lokalen Fundamentalklassen.* Diplomarbeit, Universität Augsburg, Aug. 2005.

[Ser79] Jean-Pierre Serre. *Local fields.* Springer, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[Sna03] Victor Snaith. *Burns' equivariant Tamagawa invariant* $T\Omega^{\mathrm{loc}}(n/\mathbf{Q},1)$ *for some quaternion fields.* J. Lond. Math. Soc. (2) **68** (2003), no. 3, 599–614.

[Swa68] Richard G. Swan. *Algebraic K-theory.* Lecture Notes in Mathematics (76). Springer, Berlin, 1968.

[Tat66] John Tate. *The cohomology groups of tori in finite Galois extensions of number fields.* Nagoya Math. J. **27** (1966), 709–719.

[Tat84] John Tate. *Les conjectures de Stark sur les fonctions L d'Artin en* $s = 0$, vol. 47 of *Progress in Mathematics.* Birkhäuser Boston Inc., Boston, MA, 1984. Lecture notes edited by Dominique Bernardi and Norbert Schappacher.

[Tay81] Martin J. Taylor. *On Fröhlich's conjecture for rings of integers of tame extensions.* Invent. Math. **63** (1981), no. 1, 41–79.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, vol. 83 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edn., 1997.

[Wei94] Charles A. Weibel. *An Introduction to Homological Algebra.* Cambridge University Press, 1994.

Index

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.

Kassel, im Februar 2011