Arithmetic of Stark units in global fields

Dissertation
an der Fakultät für Mathematik, Informatik und Statistik
der Ludwig-Maximilians-Universität
München

vorgelegt von
Pascal Stucky
Datum: 16.08.2021

1. Gutachter: Prof. Dr. Werner Bley
2. Gutachter: Prof. Dr. Cornelius Greither
Tag der Disputation: 30.11.2021

Contents

Abstract

Since the introduction of Stark units by H. Stark in the 1970's, these elements and their higher-rank analogues are of major interest for algebraic number theory. They can be seen as the starting point of several recent developments such as the study of Euler systems or the equivariant Tamagawa Number Conjecture (eTNC).

In the known cases of Stark's conjecture for number fields, these units are a source of annihilators for ideal class groups as can be seen in the work of C. Greither and R. Kučera, respectively H. Chapdelaine and R. Kučera. One of the applications described in this thesis is the transfer of these results to the case of global function fields. A result obtained in the proof is an index formula for a group of elliptic units (which are essentially an instance of Stark units due to the work of D. Hayes), analogously to a result of H. Oukhaba for elliptic units.

Another application of Stark units (actually cyclotomic units in this case) is a construction of certain p-units by D. Solomon for abelian extensions over $\mathbb{Q}$. This construction was adapted to the case of imaginary quadratic base fields by W. Bley and M. Hofer and can be used as a major ingredient in proving the eTNC. In fact, the study of the valuations of these p-units is a vital part in solving the Iwasawa-theortic version of the Mazur-Rubin-Sano conjecture (IMRS) in these special cases. In the second part of this thesis, Solomon's construction is generalized to the case of totally real base fields and then a conjectural statement on the valuations is formulated. It is also shown that this statement is equivalent to the IMRS which provides theoretical evidence for the conjecture. Finally, an algorithm for numerical verification up to a certain p-adic precision together with some computational results is presented.

Zusammenfassung

Seit der Einführung von Stark-Einheiten durch H. Stark in den 1970er-Jahren sind sie und ihre Verwandten höheren Ranges von hohem Interesse für die algebraische Zahlentheorie. Sie können als Auslöser für verschiedene kürzliche Entwicklungen wie das Studium von Eulersystemen oder die äquivariante Tamagawazahlvermutung (eTNC) gesehen werden.

In den bekannten Fällen der Stark-Vermutung über Zahlkörpern sind diese Einheiten eine Quelle für Annihilatoren der Idealklassengruppe, wie man in den Arbeiten von C. Greither und R. Kučera bzw. H. Chapdelaine und R. Kučera sehen kann. Eine der in dieser Arbeit beschriebenen Anwendungen ist der Transfer dieser Resultate auf den Fall der globalen Funktionenkörper. Ein Resultat dieses Beweises ist eine Indexformel für eine Gruppe von elliptischen Einheiten (die, wie die Arbeit von D. Hayes zeigt, tatsächlich eine Instanz von Stark-Einheiten bilden), analog zu einem Ergebnis von H. Oukhaba für elliptische Einheiten.

Eine weitere Anwendung von Stark-Einheiten (in diesem Fall zyklotomische Einheiten) ist eine Konstruktion von p-Einheiten von D. Solomon für abelsche Erweiterungen über $\mathbb{Q}$. Diese Konstruktion wurde von W. Bley und M. Hofer auf den Fall von imaginär-quadratischen Grundkörpern übertragen und kann als eine der Hauptzutaten im Beweis der eTNC benutzt werden. Tatsächlich leistet das Studium der Bewertungen dieser p-Einheiten einen wichtigen Beitrag zur Lösung der Iwasawa-theoretischen Version der Mazur-Rubin-Sano-Vermutung (IMRS) in diesen Spezialfällen. Im zweiten Teil dieser Dissertation wird Solomon's Konstruktion auf den Fall von total reellen Grundkörpern verallgemeinert und anschließend eine Vermutung über die Bewertungen formuliert. Es wird auch gezeigt, dass diese Aussage äquivalent zur IMRS ist, was theoretische Evidenz für die Vermutung liefert. Abschließend wird ein Algorithmus zur numerischen Verifikation bis zu einer bestimmten p-adischen Präzision zusammen mit einigen rechnerischen Ergebnissen präsentiert.

Chapter 1

Introduction

The ideal class group of a number field is one of the main objects of interest in algebraic number theory. One approach of understanding these class groups is the study of annihilators. One of the first results in this direction is the famous result of L. Stickelberger in [Sti90]. Expressed in modern language, he explicitly constructed the Stickelberger element $\theta_{L/\mathbb{Q}} \in \mathbb{Q}[\mathrm{Gal}(L/\mathbb{Q})]$ for a finite abelian extension $L/\mathbb{Q}$ via the Galois action of $\mathrm{Gal}(L/\mathbb{Q})$ on certain roots of unity and used it to define the Stickelberger ideal $\theta_{L/\mathbb{Q}}\mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})] \cap \mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$. He then proved that this ideal annihilates the ideal class group of L, a statement which is nowadays known as *Stickelberger's Theorem.*

A natural question is now if it is possible to generalize this statement to other extensions. It turns out, that the Stickelberger element is in fact simply the equivariant combination of the values at $s = 0$ of the L-functions associated to those characters corresponding to the extension $L/\mathbb{Q}$. We can easily generalize this by defining $\theta_{L/K,S}$ to be the element in $\mathbb{C}[G]$ such that $\chi(\theta_{L/K,S}) = L_S(\chi, 0)$ for any character $\chi \in \mathrm{Hom}(G, \mathbb{C}^\times)$. The index S indicates that the Stickelberger element depends on a finite set of places S containing the archimedean places and the places which ramify in L/K. This element is then related to the S-truncated version of the L-functions. It was shown by H. Klingen and C. Siegel, that $\theta_{L/K,S}$ indeed has rational coefficients (see [Sie70]). In [DR80] P. Deligne and K. Ribet proved that $\mathrm{Ann}_{\mathbb{Z}[G]}(\mu(L))\theta_{L/K,S} \subseteq \mathbb{Z}[G]$, where $\mathrm{Ann}_{\mathbb{Z}[G]}(-)$ denotes the $\mathbb{Z}[G]$-annihilator and $\mu(L)$ is the group of roots of unity contained in L.

The generalization of Stickelberger's result is then

$$\mathrm{Ann}_{\mathbb{Z}[G]}(\mu(L))\theta_{L/K,S} \subseteq \mathrm{Ann}_{\mathbb{Z}[G]}(\mathrm{cl}_S(L)),$$

where $\mathrm{cl}_S(L)$ denotes the S-class group of L. This statement is known as *Brumer's conjecture.*

Around the same time, H. Stark published his series of papers ([Sta71], [Sta75], [Sta76] and [Sta80]) proposing the existence of certain units, now called *Stark units*, containing information about the first derivative of the S-truncated L-functions of characters of an arbitrary finite abelian extension of number fields. The set S is assumed to contain at least one completely split place, which implies that the L-functions vanish at $s = 0$. The Stickelberger element will therefore be trivial in this case, hence it seems natural to consider first derivatives here. Stark also proved the conjecture for abelian extensions of $\mathbb{Q}$, where the Stark units are simply given by cyclotomic units, and for abelian extensions of imaginary quadratic base fields, where the Stark units turn out to be elliptic units.

His approach was connected to the work of Brumer by J. Tate in [Tat81b] and [Tat81a] culminating in the *Brumer-Stark conjecture* (which was proven away from 2 very recently by S. Dasgupta and M. Kakde in [DK20]). He predicted not only that any ideal to the power $|\mu(L)| \cdot \theta_{L/K,S}$ is principal, but even determined a possible generator. The results of Stark and Tate are summarized in the lecture notes [Tat84]. In this formulation, Tate also included the case of global function fields under the common notion of *global fields*.

A few years before, D. Hayes and V. Drinfeld had developed the theory of elliptic modules (nowadays called *Drinfeld modules*), which enabled them to explicitly construct ray class fields of global function fields (see [Dri74], [Hay74] and [Hay79]). With this theoretical background, P. Deligne proved the Brumer-Stark conjecture for global function fields using the theory of 1-motives. Stark's conjecture is also known in this case, the Stark units here are function field analogues of the elliptic units as can be seen in [Hay85].

In the meantime, G. Gras proposed another approach towards annihilators of class groups. He considered the subgroup of cyclotomic units C_L in an abelian extension $L/\mathbb{Q}$ and conjecturally relates the Jordan-Hölder series of the p-part $(\mathcal{O}_L^\times/C_L)_p$ of the quotient of the unit group of L modulo this subgroup to the Jordan-Hölder series of the p-part of the ideal class group, where p is an odd prime not dividing $[L : K]$ (see [Gra77]). The conjecture was proven by B. Mazur and A. Wiles as a consequence of the Iwasawa main conjecture (see [MW84]).

A few years later, V. Kolyvagin reproved the Gras conjecture via the approach of Euler systems in [Kol90]. This theory is based on the work of F. Thaine in [Tha88], K. Rubin in [Rub87] and Kolyvagin himself in [Kol88]. Thaine used cyclotomic units to explicitly construct annihilators of the p-part of the class group of an abelian extension $L/\mathbb{Q}$. Rubin adapted this approach to extensions of an imaginary quadratic base field K using elliptic units instead of cyclotomic units. Kolyvagin's result was about Selmer groups of elliptic curves using Heegner points. In his work about Euler systems, he formalized these different approaches in a common language and collected the necessary common properties of these different objects to introduce the notion of an Euler system. The crucial breakthrough over the previous works of Thaine and Rubin was that this paper introduced an inductive procedure which enables Kolyvagin to bound the orders of these groups, rather than just to obtain an annihilator.

The Euler system machinery is summarized and further developed by K. Rubin in [Rub00] and is an established source of annihilators of ideal class groups and bounds of Selmer groups. It was also adapted to the case of global function fields (see e.g. [FX96] and [XZ01]). An analogue of the Gras conjecture for global function fields was stated and proven by C. Popescu in [Pop99].

However, there are limits to this approach. As indicated in [GK04], in the case of a cyclic extension of prime power degree the Euler system of cyclotomic units will produce an annihilation result which is even weaker than the annihilators obtained from genus theory. In order to improve this approach, C. Greither and R. Kučera enlarged the subgroup of the cyclotomic units by taking certain roots of the generators in the case of a cyclic extension of primer power degree (see [GK04], [GK06] and [GK15]). With these *semispecial numbers*, they were able to prove a stronger annihilation result for these extensions. This approach was adapted by H. Chapdelaine and R. Kučera to cyclic extensions of prime power degree over imaginary quadratic base fields in [CK19]. The cyclotomic units here are again replaced by elliptic units.

In both of these cases, the objects of interest are in fact instances of Stark units and the main ingredients for the proofs are the functorial behaviour of these units combined with the assumptions on the cyclic extension L/K. Since we know another instance of Stark units in the case of global function fields, it seems natural to ask the follwing

Question. Can we formulate and proof an analogous annihilation result for global function fields?

Question. Can we generalize these results to other global fields in terms of Stark units?

The answer to the first question is yes and is given in [Stu20]. We will repeat the arguments in Chapter 3 with some more details. In particular, we prove an index formula (see Theorem 3.3.9), show that we can take certain roots of the elliptic units (see Theorem 3.4.12) and prove the desired annihilation result (see Theorem 3.6.9).

The second question can not yet be answered completely. In its current form, the assumptions on the extension L/K imply that the Stark units are trivial in any other case, since the first derivatives of the L-functions vanish. However, there exist approaches to weaken these assumptions and extend the results (see e.g. [GK20a], [GK20b], [Fra20]).

Another approach might be to replace the Stark units by their analogues in the higher rank cases. The formulation of Stark's conjecture in [Tat84] already deals with the case that S contains at least $r \geq 0$ completely split places, hence the vanishing order of the S-truncated L-functions will be at least r. If $r = 0$, we recover the Stickelberger element, for $r = 1$ we obtain the Stark units as proposed by Stark himself. In the case of $r > 1$, Tate considers the r-th derivative of the S-truncated L-functions and imposes a rationality condition to the values at $s = 0$.

However, in Tate's formulation of Stark's conjecture for rank r, there is no analogue of the Stark units and hence no form of "integrality statement". This was resolved by K. Rubin in [Rub96]. He used an additional finite set T of places of K satisfying certain hypothesis and worked with a T-modified version of the L-functions. Considering the r-th derivatives, Rubin defined an element $\eta_{L,S,T} \in \bigwedge^r \mathbb{Q}\mathcal{O}_{L,S,T}^\times$, where $\mathcal{O}_{L,S,T}^\times$ is a certain $\mathbb{Z}[\mathrm{Gal}(L/K)]$-submodule of the S-units, the (S,T)-units of L. This element is called the *Rubin-Stark element* and although it is in general not contained in $\bigwedge^r \mathcal{O}_{L,S,T}^\times$, Rubin was able to predict a certain "integrality condition" on $\eta_{L,S,T}$.

Before we return to the questions about annihilators of ideal class groups, we will shortly indicate another important feature of Stark units and Rubin-Stark elements. These elements behave functorially when changing some of the input data, e.g. the set S, the set T or the top field L. This is discussed in detail in Section 2.4.2, but for now it suffices to note that if S contains more than r completely split places, then the corresponding Rubin-Stark element is trivial since the r-th derivatives of the S-truncated, T-modified L functions vanish. Hence if we change the top field L to a subfield L' such that there exist places in S that split completely in L' but not in L, we see that the Rubin-Stark element $\eta_{L',S,T}(r) \in \bigwedge^r \mathbb{Q}\mathcal{O}_{L',S,T}^\times$ is trivial (we modified the notation to reflect the considered rank here). But there may exist a non-trivial Rubin-Stark element $\eta_{L',S,T}(r') \in \bigwedge^{r'} \mathbb{Q}\mathcal{O}_{L',S,T}^\times$, where r' is the number of places in S which split completely in L'. This leads to the natural

Question. Can we relate the rank-r Rubin-Stark element $\eta_{L,S,T}(r)$ to the rank-r' Rubin-Stark element $\eta_{L',S,T}(r')$?

Although we do not have a definitive answer to this question, we have a conjectural statement which describes this relation, the Mazur-Rubin-Sano conjecture. This conjecture was independently formulated in [MR11] and [San14].

In [BKS17], the authors formulated an Iwasawa-theoretic version (IMRS) and used it as one of the main ingredients in a machinery for proving the equivariant Tamagawa Number Conjecture (eTNC). The IMRS is known when $K = \mathbb{Q}$ and its proof relies on a classical result of D. Solomon in [Sol92]. In the second part of his article, Solomon used the constructed p-unit to obtain an annihilation result on the ideal class group indicating that trying to prove the IMRS and to derive annihilation results is at least intrinsically linked.

Before one can try to obtain analogous annihilation results for other base fields, one has to generalize Solomon's construction. For imaginary quadratic base fields, this is done by W. Bley in [Ble04] for split primes p and by W. Bley and M. Hofer in [BH20] also for non-split primes. Studying the valuations of the constructed $\mathfrak{p}$-unit, they can also prove the IMRS and the eTNC for imaginary quadratic base fields with some additional assumptions (see [Ble06] and [Hof18]). These assumptions have been removed in recent work of D. Bullach and M. Hofer (see [BH21]).

In Chapter 4 of this thesis, we generalize Solomon's construction to the case of arbitrary totally real base fields and state a conjecture on the valuations of the resulting elements (see Conjecture 4.2.9). Then we show that the given generalization is indeed equivalent to the IMRS (see Theorem 4.3.2) which gives (additionally to the known cases described above) strong theoretical evidence for the formulated conjecture. In the last chapter, we also develop an algorithm to test Conjecture 4.2.9 up to a certain level (see Algorithm 5.3.1) and the computed cases described in Section 5.4 provide some numerical evidence.

1.1 Structure of the thesis

We will first introduce Stark's conjecture and the Rubin-Stark conjecture for any finite abelian extension of global fields in Chapter 2. We will also define the Stark units, Stark elements and Rubin-Stark elements and present some basic properties here.

Then in Chapter 3 we will consider the case of global function fields and will introduce elliptic units for such extensions, which can in fact be considered as Stark units. We will prove an index formula and derive a result on annihilators of the ideal class group for certain extensions.

Afterwards, we will move to the number field case and will introduce the Iwasawa-theoretic Mazur-Rubin-Sano conjecture in Chapter 4. Then we will generalize the κ-construction of Solomon resulting in a reformulation of IMRS in terms of the constructed element.

Finally, we will present an algorithmic approach on our refomulated conjecture in Chapter 5.

1.2 Acknowledgements

I want to to thank my advisor Werner Bley for the introduction to this field of mathematics, the interesting discussions, the helpful comments, the support and engagement throughout this project. Thanks also go to Hassan Oukhaba and Radan Kučera for their kind and helpful responses to my questions. I am very grateful for the friendship and support of my colleagues Martin Hofer, Dominik Bullach and Sören Kleine. They all contributed with inspiring comments and discussions to these results and also to the final form of this dissertation. Another big thanks (as in all of my theses) goes to Veronika Heerdt for improving my english grammar. I am also in the lucky position to have a great family which always supported me in my studies. I want to thank my parents, my brother Marcel Glas and also Monique Stucky and Christine Glas. Although she could not yet contribute to this thesis directly, I want to thank Clara Glas for making me the happiest uncle in the world. Last but not least, my thanks go to my girlfriend Elisabeth Pangerl for her patience, love and support over the last three years. I want to thank you for being on my side, helping me through tough times and always believing in me.

Chapter 2

Stark's conjecture and Rubin-Stark units in the abelian case

In this chapter we will state Stark's conjecture for a finite abelian extension of global fields and its integral refinement due to Rubin. Then we introduce (Rubin-)Stark elements, Stark units and state important properties of these.

2.1 Preliminaries

This section contains well-known definitions and results which will be used throughout this thesis.

2.1.1 Valuations

Let L/K be a finite abelian extension of global fields. Let v be a place of K (archimedean or non-archimedean) and w be a place of L above v. The Galois group $G := \mathrm{Gal}(L/K)$ acts transitively on the places above v by $\sigma w := w \circ \sigma$ (see e.g. [Neu92, Ch. II, Thm. (9.4)]) and we define the *decomposition group* of w as

$$D_w := \{\sigma \in G : \sigma w = w\}.$$

Since G is abelian, this subgroup is independent of the choice of w, hence we can write D_v instead of D_w. If D_v is trivial, i.e. there exist $[L : K]$ different places above v, we say that v is *completely split*.

Remark 2.1.1. Note that the decomposition group of an archimedean place can either be trivial (if v is complex or both v and w are real) or contain exactly one non-trivial element (if v is real and w is complex).

If v (and hence w) is non-archimedean, let $\mathcal{O}_w$ be the valuation ring associated to w and let $k(w) = \mathcal{O}_w/w$ be the residue class field of w. The *norm* of w is defined as $Nw := |k(w)|$. For an archimedean place w we set

$$Nw := \begin{cases} e, & w \text{ is real,} \\ e^2, & w \text{ is complex.} \end{cases}$$

We define the *inertia group*

$$I_w := \{\sigma \in D_v : \sigma x \equiv x \mod w \quad \forall x \in \mathcal{O}_w\} .$$

This is again independent of the choice of w since G is abelian and so we simply write I_v instead of I_w. If v and w are archimedean, then we set $I_v := D_v$.

The place v is *ramified* if I_v is non-trivial and the *ramification index* is defined as $t_v := |I_v|$. Hence an archimedean place can either be completely split if $D_v = \{\mathrm{id}\}$ or ramified with ramification index 2.

The quotient D_v/I_v is a cyclic group generated by the Frobenius automorphism and we define $\sigma_v \in D_v$ to be any lift of this Frobenius automorphism.

For a non-archimedean place v, we denote the corresponding normalized valuation by ord_v. For an archimedean place v associated to an embedding $\iota_v \colon K \longrightarrow \mathbb{C}$ (real or complex), we set

$$\mathrm{ord}_v(x) := -\log|\iota_v(x)| \quad \forall x \in K .$$

In any case, we define the *absolute value associated to* v by

$$|x|_v := Nv^{-\mathrm{ord}_v(x)} \quad \forall x \in K .$$

Note that if v is real, we get $|x|_v = |\iota_v(x)|$, and if v is complex, then $|x|_v = |\iota_v(x)|^2$.

2.1.2 Duals and exterior powers

Let R be a commutative, reduced, Noetherian ring. For an R-module M we define $M^* := \mathrm{Hom}_R(M, R)$ to be its dual module. Then for any $\varphi \in M^*$ and $r \geq 1$ there exists an R-homomorphism

$$\begin{aligned} \varphi^{(r)}\colon \qquad & \bigwedge_R^r M \longrightarrow \bigwedge_R^{r-1} M \\ & x_1 \wedge \cdots \wedge x_r \longmapsto \sum_{i=1}^{r} (-1)^{i-1} \varphi(x_i) \cdot x_1 \wedge \cdots \wedge \widehat{x_i} \wedge \cdots \wedge x_r , \end{aligned}$$

where the $\widehat{x_i}$-notation indicates that the x_i-term is omitted.

Iterating this construction, we obtain an R-homomorphism

$$\begin{aligned} \bigwedge_R^i M^* &\longrightarrow \mathrm{Hom}_R(\bigwedge_R^r M, \bigwedge_R^{r-i} M) \\ \varphi_1 \wedge \cdots \wedge \varphi_i &\longmapsto (m \mapsto \varphi_i^{(r-i+1)} \circ \cdots \circ \varphi_1^{(r)}(m)) \end{aligned} \tag{2.1.1}$$

for $0 \leq i \leq r$. Using this homomorphism, we will regard elements of $\bigwedge_R^i M^*$ as homomorphisms $\bigwedge_R^r M \longrightarrow \bigwedge_R^{r-i} M$.

Remark 2.1.2. In the case $r = i$ we find the explicit formula

$$(\varphi_1 \wedge \cdots \wedge \varphi_r)(x_1 \wedge \cdots \wedge x_r) = \det\left((\varphi_i(x_j))_{1 \leq i,j \leq r}\right) \tag{2.1.2}$$

(for example by induction and Laplace's formula).

We finish this section by a collection of useful facts on exterior powers and duals, the proofs of which will be omitted. They can for example be found in the author's master thesis. We also set $R'M := R' \otimes_R M$ for any commutative R-algebra R'.

Lemma 2.1.3. *Let R' be a commutative R-algebra. There is a canonical R'-module isomorphism $R' \otimes_R \bigwedge_R^r M \cong \bigwedge_{R'}^r R'M$.*

Now let $\mathrm{Frac}(R)$ be the total ring of fractions of R, i.e. the localization at the set of non-zero-divisors. Then we obtain

Lemma 2.1.4. *Let M be a finitely-generated R-module. Then the map*

$$\begin{aligned} M^* &\longrightarrow \mathrm{Hom}_{\mathrm{Frac}(R)}(\mathrm{Frac}(R)M, \mathrm{Frac}(R)) \\ \varphi &\longmapsto \left(\frac{x}{s} \mapsto \frac{\varphi(x)}{s}\right) \end{aligned}$$

is an injective R-module homomorphism and induces an isomorphism of $\mathrm{Frac}(R)$*-modules* $\mathrm{Frac}(R) \otimes_R M^* \cong \mathrm{Hom}_{\mathrm{Frac}(R)}(\mathrm{Frac}(R)M, \mathrm{Frac}(R))$.

Lemma 2.1.5. *Let G be a finite, abelian group and let M be a $\mathbb{Z}[G]$-module, then the canonical map*

$$\begin{aligned} \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z}) &\longrightarrow \mathrm{Hom}_{\mathbb{Z}[G]}(M, \mathbb{Z}[G]) \\ \varphi &\longmapsto (x \mapsto \sum_{\sigma \in G} \varphi(\sigma(x))\sigma^{-1}) \end{aligned}$$

is an isomorphism.

2.1.3 Idempotents

Let G be a finite, abelian group and $\widehat{G}$ be the group of irreducible characters of G. For any ring $R \subseteq \mathbb{C}$ we let a character $\chi \in \widehat{G}$ act on the group algebra $R[G]$ by extension of scalars, i.e. for $a = \sum_{\sigma \in G} a_\sigma \sigma$ with $a_\sigma \in R$, we let

$$\chi(a) = \sum_{\sigma \in G} a_\sigma \chi(\sigma) \in \mathbb{C}\,.$$

For $\chi \in \widehat{G}$ the *idempotent associated to* χ is defined as

$$e_\chi := \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1} \in \mathbb{C}[G]\,.$$

The values of a character χ are roots of unity, so when we adjoin all values of χ to $\mathbb{Q}$ we obtain a cyclotomic field denoted by $\mathbb{Q}(\chi)$. For a $\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$ we find that $\sigma \circ \chi \in \mathrm{Hom}(G, \mathbb{C}^\times) = \widehat{G}$, so this defines another irreducible character of G called χ^σ. Hence we obtain an equivalence relation

$$\chi \sim \psi \qquad \Longleftrightarrow \qquad \exists \sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q}) : \psi = \chi^\sigma\,.$$

We denote the equivalence class of χ by $[\chi]$, and the set of all these classes by $\widehat{G}/\sim$.

Let $\chi \in \widehat{G}$. Then the *rational idempotent associated to* χ is defined as

$$e_{[\chi]} := \sum_{\psi \in [\chi]} e_\psi \,.$$

Now we collect some properties of (rational) idempotents.

Lemma 2.1.6. *Let* $\chi \in \widehat{G}$*.*

(i) $e_{[\chi]} \in \mathbb{Q}[G]$.

(ii) The equality $\tau e_\chi = \chi(\tau) e_\chi$ *holds for all* $\tau \in G$ *(hence,* $a e_\chi = \chi(a) e_\chi$ *for all* $a \in \mathbb{C}[G]$*).*

(iii) Let $\psi \in \widehat{G}$*. Then* $e_\chi e_\psi = \delta_{\chi\psi} e_\chi$ *and* $e_{[\chi]} e_{[\psi]} = \delta_{[\chi][\psi]} e_{[\chi]}$*.*

(iv) We have $\sum_{\chi \in \widehat{G}} e_\chi = \sum_{[\chi] \in \widehat{G}/\sim} e_{[\chi]} = \mathrm{id}$*.*

(v) The set $\{e_\chi : \chi \in \widehat{G}\}$ *is an orthogonal basis for the* $\mathbb{C}$*-vector space* $\mathbb{C}[G]$*, i.e.*

$$\mathbb{C}[G] = \bigoplus_{\chi \in \widehat{G}} e_\chi \cdot \mathbb{C} \,.$$

Moreover, there is an isomorphism of $\mathbb{Q}$*-vector spaces*

$$\mathbb{Q}[G] \cong \bigoplus_{[\chi] \in \widehat{G}/\sim} e_{[\chi]} \cdot \mathbb{Q}(\chi) \,.$$

Note that by (v) we have an isomorphism of $\mathbb{Q}$-vector spaces $e_{[\chi]} \cdot \mathbb{Q}[G] \cong \mathbb{Q}(\chi)$.

2.1.4 L-functions

Let v be a place of K and recall that $\sigma_v \in G$ is a lift of the Frobenius automorphism. Let $\chi \in \widehat{G}$ be a character of G and let

$$e_{I_v} := \frac{1}{|I_v|} \sum_{\sigma \in I_v} \sigma$$

be the idempotent associated to the subgroup I_v in G. Then the definition

$$\chi(v) := \chi(\sigma_v e_{I_v})$$

is independent of the choice of σ_v. Note that we have $\chi(v) \neq 0$ if and only if $I_v \subseteq \ker(\chi)$.

For a finite set of primes $S \supseteq S_\infty$ of K containing the archimedean places we define the *S-truncated L-function* $L_S(\chi, s)$ associated to χ as the Euler product

$$\prod_{v \notin S} (1 - \chi(v) N v^{-s})^{-1} \,, \qquad \mathrm{Re}(s) > 1 \,,$$

where the product runs over all places of K which are not contained in S.

If $S = S_\infty$, we simply write

$$L(\chi, s) = L_{S_\infty}(\chi, s)\,.$$

If $\chi = \mathbf{1}$ we obtain that

$$L_S(\mathbf{1}, s) = \zeta_{K,S}(s)$$

is the *S-truncated Dedekind ζ-function* of K.

Remark 2.1.7. If $v \in S_{ram}$, then the factor in the Euler product is 1 since $\chi(v) = 0$. We may therefore assume $S_{ram} \subseteq S$.

If K is a number field, it is well known that the above Euler product admits a meromorphic continuation to the whole complex plane. This continuation will also be denoted by $L_S(\chi, s)$. If $\chi = \mathbf{1}$, then $\zeta_{K,S}(s)$ has a simple pole at $s = 1$, otherwise the continuation is holomorphic everywhere.

If K is a global function field, we again obtain a meromorphic continuation to the complex plane which is holomorphic whenever $L_\chi = L^{\ker(\chi)}$ is not a constant field extension (see [Ros02, Thm. 9.25]).

We summarize some results on L-functions in the next

Proposition 2.1.8. *(i) If $L' \supseteq L$ is a finite abelian extension of K with Galois group G' and ψ is the inflation of χ to G', then we have*

$$L_S(\chi, s) = L_S(\psi, s)\,,$$

i.e. the L-function is invariant under inflation.

(ii) We have

$$\zeta_L(s) = \zeta_K(s) \cdot \prod_{\chi \neq 1} L(\chi, s)\,,$$

where the product runs over all non-trivial characters of G.

Proof. (i) This is [Neu92, Ch. VII, Thm. (10.4)(iii)].

(ii) This is [Neu92, Ch. VII, Cor. (10.5)(iii)]. □

Remark 2.1.9. Note that the proofs in [Neu92] do not use the fact that the L-functions considered there are defined over number fields. In fact, these statements even hold for non-abelian extensions and Artin-L-functions.

We combine the L-functions with the character idempotents to obtain the *equivariant S-truncated L-function*

$$\Theta_S(s) := \sum_{\chi \in \widehat{G}} L_S(\chi, s) e_{\chi^{-1}}$$

with values in $\mathbb{C}[G]$.

Now let T be a finite set of places of K which is disjoint from S (in particular, all places in T must be non-archimedean and unramified). Then we define

$$\delta_T(s) := \prod_{v \in T} (1 - \sigma_v^{-1} N v^{1-s})$$

and obtain the *S-truncated, T-modified L-function*

$$L_{S,T}(\chi, s) = L_S(\chi, s) \cdot \chi^{-1}(\delta_T(s)) = L_S(\chi, s) \cdot \prod_{v \in T} (1 - \chi(\sigma_v) N v^{1-s})$$

and its equivariant version

$$\Theta_{S,T} = \Theta_S(s) \cdot \delta_T(s) \,.$$

Since $\chi(\delta_T(0)) \neq 0$ for all $\chi \in \widehat{G}$, we see that the T-modification does not change the order of vanishing of the L-function at $s = 0$. We obtain

Lemma 2.1.10. *Suppose that $S \neq \emptyset$. The order of vanishing of $L_S(\chi, s)$ (and also $L_{S,T}(\chi, s)$) is given by*

$$r_{S,\chi} = \begin{cases} |\{v \in S : \chi(v) = 1\}| \,, & \chi \neq \mathbf{1}, \\ |S| - 1, & \chi = \mathbf{1}. \end{cases}$$

Proof. This can be found in the proof of [Tat84, Ch. I, Prop. 3.4]. □

2.1.5 S-units and Dirichlet's unit theorem

Let S be a non-empty finite set of places of K containing the archimedean places, i.e. $S \supseteq S_\infty$. Let $S_L := \{w \mid v : v \in S\}$ be the places of L above the places in S.

The *S-integers* of L/K are defined as

$$\mathcal{O}_{L,S} := \{u \in L^\times : \operatorname{ord}_w(u) \geq 0 \quad \forall w \notin S_L\} \,. \tag{2.1.3}$$

The *S-units* of L/K are the units of this ring, i.e.

$$\mathcal{O}_{L,S}^\times := \{u \in L^\times : \operatorname{ord}_w(u) = 0 \quad \forall w \notin S_L\} \,.$$

Let $Y_{L,S} = \bigoplus_{w \in S_L} \mathbb{Z} w$ be the group of S_L-divisors and let $X_{L,S}$ be the subgroup of divisors of degree 0. We consider the Dirichlet regulator

$$\begin{aligned} \lambda_S \colon \mathcal{O}_{L,S}^\times &\longrightarrow \mathbb{R} X_{L,S} \\ u &\longmapsto -\sum_{w \in S_L} \log |u|_w \, w \,. \end{aligned}$$

This map induces an exact sequence

$$1 \longrightarrow \mu(L) \longrightarrow \mathcal{O}_{L,S}^\times \xrightarrow{\lambda_S} \lambda_S(\mathcal{O}_{L,S}^\times) \longrightarrow 0 \,,$$

where $\mu(L)$ is the group of roots of unity of L. With extension of scalars and Dirichlet's unit theorem, we obtain an isomorphism

$$\lambda_S \colon \mathbb{R}\mathcal{O}_{L,S}^\times \xrightarrow{\cong} \mathbb{R} X_{L,S} \tag{2.1.4}$$

of $\mathbb{R}[G]$-modules. By representation theory, we obtain the following

Corollary 2.1.11. *The* $\mathbb{Q}[G]$*-modules* $\mathbb{Q}\mathcal{O}_{L,S}^{\times}$ *and* $\mathbb{Q}X_{L,S}$ *are isomorphic.*

Let $r \geq 0$. We define

$$\widehat{G}_{S,r} := \{\chi \in \widehat{G} \,:\, r_{S,\chi} = r\}$$

and the idempotent

$$e_{S,r} := \sum_{\chi \in \widehat{G}_{S,r}} e_{\chi}\,.$$

For characters $\chi \sim \psi$ we clearly have $\ker(\chi) = \ker(\psi)$, so $r_{S,\chi} = r_{S,\psi}$. This implies that for $\chi \in \widehat{G}_{S,r}$ we have $[\chi] \subseteq \widehat{G}_{S,r}$, so we can write

$$e_{S,r} = \sum_{[\chi] \subseteq \widehat{G}_{S,r}} \sum_{\psi \in [\chi]} e_{\psi} = \sum_{[\chi] \subseteq \widehat{G}_{S,r}} e_{[\chi]} \in \mathbb{Q}[G]\,.$$

Therefore, $e_{S,r} \cdot \mathbb{Q}X_{L,S}$ and $e_{S,r} \cdot \mathbb{Q}\mathcal{O}_{L,S}^{\times}$ are isomorphic $e_{S,r} \cdot \mathbb{Q}[G]$-modules.

Proposition 2.1.12. *The* $e_{S,r} \cdot \mathbb{Q}[G]$*-module* $e_{S,r} \cdot \mathbb{Q}X_{L,S}$ *is free of rank* r *for all* $r \geq 0$.

Remark 2.1.13.

- As a direct consequence of Proposition 2.1.12 we find that $e_{S,r} \cdot \mathbb{Q}\mathcal{O}_{L,S}^{\times}$ is a free $e_{S,r} \cdot \mathbb{Q}[G]$-module of rank r.
- A similar argument shows that $e_{S,r} \cdot \mathbb{R}X_{L,S} \cong e_{S,r} \cdot \mathbb{R}\mathcal{O}_{L,S}^{\times} \cong (e_{S,r} \cdot \mathbb{R}[G])^r$.

2.1.6 The analytic class number formula

As before, let S be a non-empty finite set with $S \supseteq S_\infty$. By choosing $\mathbb{Z}$-bases of the torsion-free part of $\mathcal{O}_{L,S}^{\times}$ and $X_{L,S}$, we can read $\lambda_S\colon \mathbb{R}\mathcal{O}_{L,S}^{\times} \longrightarrow \mathbb{R}X_{L,S}$ as an isomorphism of $\mathbb{R}$-vector spaces with respect to these bases. Then we define the *S-regulator of L* as

$$R_{L,S} = |\det(\lambda_S)| \in \mathbb{R}\,.$$

We also define the *S-class group* of L as the ideal class group $\mathrm{cl}_S(L)$ of $\mathcal{O}_{L,S}$. Then the *S-class number* $h_{L,S}$ of L is defined as $|\mathrm{cl}_S(L)|$. We set $w_L := |\mu(L)|$ and we obtain the analytic class number formula:

Theorem 2.1.14 (Analytic class number formula)**.** *Let* $r = |S_L| - 1$ *and let* $\zeta_{L,S}^{(r)}(0)$ *be the leading term of the Dedekind* ζ*-function, i.e.*

$$\zeta_{L,S}^{(r)}(0) := \lim_{s \to 0} s^{-r} \zeta_{L,S}(s)\,.$$

Then we obtain

$$\zeta_{L,S}^{(r)}(0) = -\frac{h_{L,S} R_{L,S}}{w_L}\,.$$

Proof. If K and L are number fields, this can be found e.g. in [Neu92, Ch. VII, Cor. (5.11)]. In the case of global function fields, this is [Ros02, Thm. 14.4]. □

2.2 Stark's conjecture

Let $r \geq 0$. We introduce the following hypothesis on S:

Hypothesis 2.2.1. The finite set of places S satisfies the following properties:

(i) $S \supseteq S_\infty \cup S_{ram}$.

(ii) S contains at least r places $V := \{v_0, ..., v_{r-1}\}$ which split completely in L.

(iii) $|S| \geq r + 1$.

With these hypotheses and Lemma 2.1.10, we find that $r_{S,\chi} \geq r$ for each character χ. Define

$$\Theta_S^{(r)}(0) := \lim_{s \to 0} s^{-r} \Theta_S(s)$$

and analogously $\Theta_{S,T}^{(r)} = \lim_{s\to 0} s^{-r}\Theta_{S,T}(s) = \delta_T(0)\Theta_S^{(r)}(0)$.

Let $v' \in S \setminus V$ be an arbitrary but fixed place. For each $i = 0, ..., r-1$, we fix a place $w_i \mid v_i$ of L (and also a place w' over v'). From (2.1.4), we get an induced isomorphism

$$(\bigwedge^r \lambda_S)\colon \mathbb{R} \bigwedge_{\mathbb{Z}[G]}^r \mathcal{O}_{L,S}^\times \longrightarrow \mathbb{R} \bigwedge_{\mathbb{Z}[G]}^r X_{L,S}$$

and we define the *Stark element* $\eta_{L,S} \in \mathbb{R} \bigwedge_{\mathbb{Z}[G]}^r \mathcal{O}_{L,S}^\times$ *of order* r by

$$(\bigwedge^r \lambda_S)(\eta_{L,S}) = \Theta_S^{(r)}(0) \cdot (w_0 - w') \wedge \cdots \wedge (w_{r-1} - w')\,.$$

Remark 2.2.2. We have $\eta_{L,S} \in e_{S,r} \cdot \mathbb{R} \bigwedge_{\mathbb{Z}[G]}^r \mathcal{O}_{L,S}^\times$, i.e. the Stark element lies in the $e_{S,r}$-component. Indeed, for a character $\chi \in \widehat{G}$ with $r_{S,\chi} > r$, we find $e_{[\chi]}\Theta_S^{(r)}(0) = 0$. Since $\bigwedge^r \lambda_S$ is an $\mathbb{R}[G]$-isomorphism, this implies $e_{[\chi]}\eta_{L,S} = 0$.

Since $e_{S,r} \cdot \mathbb{R} \bigwedge_{\mathbb{Z}[G]}^r \mathcal{O}_{L,S}^\times$ is a free $e_{S,r} \cdot \mathbb{R}[G]$-module of rank 1 by Remark 2.1.13, we can write

$$\eta_{L,S} = \lambda \cdot u_1 \wedge \cdots \wedge u_r\,, \tag{2.2.1}$$

with $\lambda \in e_{S,r} \cdot \mathbb{R}[G]$ and $u_1, ..., u_r \in \mathcal{O}_{L,S}^\times$.

Now we can state Stark's conjecture:

Conjecture 2.2.3 ($\mathrm{St}(L/K, S, r)$)**.** *The Stark element has rational coefficients, i.e.* $\eta_{L,S} \in \mathbb{Q} \bigwedge_{\mathbb{Z}[G]}^r \mathcal{O}_{L,S}^\times$.

Remark 2.2.4. As we will see in Corollary 2.4.2, this conjecture is implied by the Rubin-Stark conjecture (Conjecture 2.3.5 below). Hence Stark's conjecture holds whenever the Rubin-Stark conjecture is true and we give a list of known cases in Remark 2.3.6. Indeed, there are no cases known to the author where Stark's conjecture is proven but the Rubin-Stark conjecture is unknown.

2.2.1 The case $r = 1$

The statement of $\mathrm{St}(L/K, S, 1)$ is that the Stark element $\eta_{L,S}$ is contained in $\mathbb{Q}\mathcal{O}_{L,S}^\times$. We know that $\eta_{L,S} \in \mathbb{R}\mathcal{O}_{L,S}^\times$, hence there exists a unit $\varepsilon \in \mathcal{O}_{L,S}^\times$ and $\lambda \in \mathbb{R}$ such that $\eta_{L,S} = \lambda\varepsilon$. Then $\mathrm{St}(L/K, S, 1)$ is true if and only if $\lambda \in \mathbb{Q}$.

Remark 2.2.5. In fact, there exist infinitely many such pairs (λ, ε), since we get $(\alpha^{-1}\lambda)(\alpha\varepsilon) = \lambda\varepsilon = \eta_{L,S}$ for any $\alpha \in \mathbb{Z}$. However, if any of these coefficients λ is rational, then all such coefficients are rational.

For $w := w_0$, we consider the dual $w^* \in \mathrm{Hom}_{\mathbb{Z}[G]}(Y_{L,S}, \mathbb{Z}[G]) = Y_{L,S}^*$ obtained by Lemma 2.1.5, i.e.

$$w^*(\widetilde{w}) = \sum_{\substack{\sigma \in G \\ \sigma w = \widetilde{w}}} \sigma \qquad \forall \widetilde{w} \in S_L\,.$$

This induces a map $w^* \colon \mathbb{R}X_{L,S} \longrightarrow \mathbb{R}[G]$ and from the definition of $\eta_{L,S}$, we get that

$$\Theta_S'(0) = (w^* \circ \lambda_S)(\eta_{L,S}) = -\lambda \sum_{\sigma \in G} \log|\varepsilon^\sigma|_w\, \sigma^{-1}\,.$$

Considering the χ-components, we get

$$L_S'(\chi, 0) = -\lambda \sum_{\sigma \in G} \log|\varepsilon^\sigma|_w\, \chi(\sigma)$$

for all $\chi \in \widehat{G}$. In this special case, Stark considered a particular choice for the pair (λ, ε):

Conjecture 2.2.6 ($\mathrm{St}(L/K, S)$, cf. [Tat84, Ch. IV, Conj. 2.2]). *Let S be a finite set of places satisfying Hypothesis 2.2.1 for $r = 1$ and let w be a fixed place of L above the completely split place v. Then there exists a unit $\varepsilon_{L,S} \in \mathcal{O}_{L,S}^\times$ which satisfies:*

(i) $K(\varepsilon_{L,S}^{1/w_L})$ is abelian over K.

(ii) If $|S| \geq 3$ then $|\varepsilon_{L,S}|_{\widetilde{w}} = 1$ for all $\widetilde{w} \nmid v$. If $S = \{v, v'\}$ and w' is a place of L above v', then $|\varepsilon_{L,S}|_{\sigma w'} = |\varepsilon_{L,S}|_{w'}$ for all $\sigma \in G$.

(iii) For each character $\chi \in \widehat{G}$ we have

$$L_S'(\chi, 0) = -\frac{1}{w_L} \sum_{\sigma \in G} \log\left|\varepsilon_{L,S}^\sigma\right|_w \chi(\sigma)\,.$$

The element $\varepsilon_{L,S}$ is called the Stark unit.

Remark 2.2.7. (i) The Stark unit $\varepsilon_{L,S}$ is only defined up to a root of unity in L. Hence, all following equations should be read modulo $\mu(L)$.

(ii) If S contains a second place which splits completely in L we obtain $\varepsilon_{L,S} = 1$ (cf. Remark 2.3.6).

(iii) Stark units can be determined explicitly in several cases:

- $K = \mathbb{Q}$ and $v = \infty$. Then L is a totally real abelian extension of $\mathbb{Q}$ and hence contained in $\mathbb{Q}(\zeta_m)$ for some $m \in \mathbb{N}$. Let $S = S_{ram}(L/K) \cup \{\infty\}$. Then we have

$$\varepsilon_{L,S} = N_{\mathbb{Q}(\zeta_m)/L}(1 - \zeta_m)\,,$$

  (cf. [Pop11, Remark 4.4.2]).

- K is an imaginary quadratic number field and $v = \infty$. Then $\varepsilon_{L,S}$ is essentially an elliptic unit. Let $S = S_{ram}(L/K) \cup \{\infty\}$ and let $\mathfrak{f}$ be the conductor of L. Using the elliptic unit $\varphi_{L,\mathfrak{f},Ou}$ defined by Oukhaba in [Ouk03, §3], we obtain with the Kronecker limit formula (2.4) in loc. cit.

$$\varepsilon_{L,S} = \varphi_{L,\mathfrak{f},Ou}^{\frac{w_L}{12h_K w_K f_\mathfrak{f}}}\,,$$

  where $f_\mathfrak{f}$ is the least positive integer contained in $\mathfrak{f}$.

- K is a global function field and v is a fixed prime ∞. Let $\mathfrak{f}$ be the conductor of L (this is an integral ideal of $\mathcal{O}_{K,S}$). Then there is an analogue $\alpha_{\mathfrak{f},Ha}$ of the elliptic units constructed by Hayes in [Hay85, Thm. 4.17]. With the Kronecker limit formula in this case (cf. last equation in loc. cit.), we then obtain

$$\varepsilon_{L,S} = N_{H_\mathfrak{f}/L}(\alpha_{\mathfrak{f},Ha})^{\frac{w_L}{w_{H_\mathfrak{f}}}}\,,$$

  where $H_\mathfrak{f}$ is the real ray class field of conductor $\mathfrak{f}$ (for a precise definition see Section 3.1).

In these cases, Stark's conjecture is known to be valid.

2.3 The Rubin-Stark conjecture

We will now introduce an integral refinement of $\mathrm{St}(L/K, S, r)$, the Rubin-Stark conjecture.

2.3.1 The additional set T

The group of S-units still has $\mathbb{Z}$-torsion. Although this is irrelevant when we talk about rationality (since the torsion is killed by tensoring with $\mathbb{Q}$), it clearly matters when we consider integrality statements (as we have already seen in Section 2.2.1). We can avoid this problem by working with the T-modified version of the L-functions and a torsion-free T-modified unit group.

Hypothesis 2.3.1. The finite set of places T satisfies the following properties:

(i) $S \cap T = \emptyset$.

(ii) Let T_L be the set of places of L over the places in T. Then

$$\{\zeta \in \mu(L) : \zeta \equiv 1 \mod w \quad \forall w \in T_L\} = \{1\}.$$

The hypothesis is satisfied if e.g. T contains two primes of different residue characteristic or if T contains one prime of residue characteristic not dividing w_L.

Definition 2.3.2. Let S satisfy the Hypothesis 2.2.1 and let T be a finite set of places such that $S \cap T = \emptyset$. The (S,T)-*units of* L are defined as

$$\mathcal{O}_{L,S,T}^{\times} := \{u \in \mathcal{O}_{L,S}^{\times} : u \equiv 1 \mod w \quad \forall w \in T_L\}.$$

Lemma 2.3.3. *If T satisfies Hypothesis 2.3.1, then*

(i) $\mathcal{O}_{L,S,T}^{\times}$ is a free $\mathbb{Z}$-module.

(ii) $\mathbb{Q}\mathcal{O}_{L,S}^{\times} \cong \mathbb{Q}\mathcal{O}_{L,S,T}^{\times}$.

(iii) If $u \in \mathcal{O}_{L,S}^{\times}$, then $u^{\delta_T(0)} \in \mathcal{O}_{L,S,T}^{\times}$.

Then we obtain a T-version of the Stark element, the *Rubin-Stark element* $\eta_{L,S,T} \in \mathbb{R}\bigwedge_{\mathbb{Z}[G]}^{r}\mathcal{O}_{L,S,T}^{\times}$ which is defined by

$$(\bigwedge^{r}\lambda_S)(\eta_{L,S,T}) = \Theta_{S,T}^{(r)}(0)\cdot(w_0 - w')\wedge\cdots\wedge(w_{r-1}-w').$$

Analogously to Remark 2.2.2, the Rubin-Stark element is contained in the $e_{S,r}$-component and we obtain a representation

$$\eta_{L,S,T} = \lambda_T u_{1,T}\wedge\cdots\wedge u_{r,T} \tag{2.3.1}$$

with $\lambda_T \in e_{S,r}\cdot\mathbb{R}[G]$ and $u_{1,T},...,u_{r,T} \in \mathcal{O}_{L,S,T}^{\times}$.

Then the T-version of Stark's conjecture is

Conjecture 2.3.4 (St$(L/K,S,T,r)$)**.** *The Rubin-Stark element has rational coefficients, i.e. $\eta_{L,S,T} \in \mathbb{Q}\bigwedge_{\mathbb{Z}[G]}^{r}\mathcal{O}_{L,S,T}^{\times}$.*

2.3.2 Rubin's lattice

We define *Rubin's lattice* by

$$\bigcap_{\mathbb{Z}[G]}^{r}\mathcal{O}_{L,S,T}^{\times} := \left\{u \in \mathbb{Q}\bigwedge_{\mathbb{Z}[G]}^{r}\mathcal{O}_{L,S,T}^{\times} \,|\, (\varphi_1\wedge\cdots\wedge\varphi_r)(u) \in \mathbb{Z}[G] \quad \forall\varphi_1,...,\varphi_r \in (\mathcal{O}_{L,S,T}^{\times})^*\right\}.$$

Then the Rubin-Stark conjecture is

Conjecture 2.3.5 (RS$(L/K,S,T,r)$)**.** *The Rubin-Stark element is contained in Rubin's lattice, i.e. $\eta_{L,S,T} \in \bigcap_{\mathbb{Z}[G]}^{r}\mathcal{O}_{L,S,T}^{\times}$.*

Remark 2.3.6. The Rubin-Stark conjecture is known in the following cases:

- S contains more than r places which split completely in L: Then clearly $e_{S,r} = 0$ and hence $\eta_{L,S,T} = 0$.
- $L = K$: As a corollary of the previous case.
- $r = 0$: This is shown e.g. in [Tat84, Ch. III, Thm. 1.2]. In the number field case, this is essentially the result of Deligne and Ribet, see [DR80].
- $[L : K] = 2$: See [Rub96, Thm. 3.5].
- Certain multi-quadratic extensions if $r = 1$, for the proof and more details see [DST97].
- The cases listed in Remark 2.2.7 (in these cases we always have $r = 1$).
- Whenever the eTNC holds (see [Bur07, Cor. 9.2]), e.g. if $K = \mathbb{Q}$ (see [BG03] and [Fla11]), K is imaginary quadratic (see [Ble06] and [BH21]) or K is a global function field (see [Bur11]).
- K is a totally real number field and L is a CM-extension of K as a consequence of the Brumer-Stark conjecture which is proven in [DK20].

For our results in Chapter 4, we want to consider a p-component of the Rubin-Stark conjecture as stated in [BKS17, Conj. 2.1]. So we fix an odd prime p and set

$$U_{L,S,T} := \mathbb{Z}_p \mathcal{O}^{\times}_{L,S,T}.$$

By fixing an isomorphism $\mathbb{C} \cong \mathbb{C}_p$, we can consider $\eta_{L,S,T} \in \mathbb{C}_p \bigwedge^r_{\mathbb{Z}_p[G]} U_{L,S,T}$, and we define

$$\bigcap^r_{\mathbb{Z}_p[G]} U_{L,S,T} := \left\{ u \in \mathbb{Q}_p \bigwedge^r_{\mathbb{Z}[G]} U_{L,S,T} \,|\, (\varphi_1 \wedge \cdots \wedge \varphi_r)(u) \in \mathbb{Z}_p[G] \quad \forall \varphi_1, ..., \varphi_r \in U^*_{L,S,T} \right\}.$$

Note that $U_{L,S,T}$ is a $\mathbb{Z}_p[G]$-module and $U^*_{L,S,T} = \mathrm{Hom}_{\mathbb{Z}_p[G]}(U_{L,S,T}, \mathbb{Z}_p[G])$. There is a natural isomorphism $\mathbb{Z}_p \bigcap^r_{\mathbb{Z}[G]} \mathcal{O}^{\times}_{L,S,T} \cong \bigcap^r_{\mathbb{Z}_p[G]} U_{L,S,T}$. Then the p-component of the Rubin-Stark conjecture reads

Conjecture 2.3.7 (RS$(L/K, S, T, r)_p$)**.** $\eta_{L,S,T} \in \bigcap^r_{\mathbb{Z}_p[G]} U_{L,S,T}$.

We will simply write $\bigwedge^r$ or $\bigcap^r$ from now on, whenever the considered ring is clear from the context.

2.4 Rubin-Stark elements and their properties

2.4.1 Relation of the different elements

First, we consider the relation of the different elements introduced in the last sections:

Lemma 2.4.1. *(i) For a fixed data $(L/K, S, T, r)$, the Stark element and the Rubin-Stark element satisfy the relation*

$$\eta_{L,S,T} = \delta_T(0)\eta_{L,S} = \prod_{v\in T}(1-\sigma_v^{-1}Nv)\cdot\eta_{L,S} \in \mathbb{R}\bigwedge^r \mathcal{O}_{L,S,T}^\times .$$

(ii) If $r = 1$ and $\mathrm{St}(L/K, S)$ holds, then the Stark unit and the Stark element satisfy the relation

$$\varepsilon_{L,S} = w_L \cdot \eta_{L,S} \in \mathbb{Q}\mathcal{O}_{L,S}^\times .$$

Then it follows directly that

$$\eta_{L,S,T} = \frac{\delta_T(0)}{w_L}\varepsilon_{L,S} .$$

Proof. (i) Since $\Theta_{S,T}^{(r)}(0) = \delta_T(0)\Theta_S^{(r)}(0)$ and $\bigwedge^r \lambda_S$ is an $\mathbb{R}[G]$-isomorphism, the desired relation follows directly from the definitions of $\eta_{L,S}$ and $\eta_{L,S,T}$.

(ii) The first relation follows directly from the arguments in Section 2.2.1. The second relation is obtained by combining the first relation with part (i). □

As a consequence, we obtain several implications between the conjectures:

Corollary 2.4.2. *(i) $\mathrm{St}(L/K, S, r)$ is equivalent to $\mathrm{St}(L/K, S, T, r)$ for all sets T satisfying Hypothesis 2.3.1.*

(ii) $\mathrm{St}(L/K, S, r)$ is equivalent to $\mathrm{St}(L/K, S, T, r)$ for any set T satisfying Hypothesis 2.3.1.

(iii) $\mathrm{RS}(L/K, S, T, r)$ implies $\mathrm{St}(L/K, S, T, r)$ and hence also $\mathrm{St}(L/K, S, r)$.

(iv) If $r = 1$, $\mathrm{St}(L/K, S)$ is equivalent to $\mathrm{RS}(L/K, S, T, 1)$ for all T satisfying Hypothesis 2.3.1.

Proof. For (i) and (ii) we show

$$\begin{aligned} &St(L/K, S, T, r) \text{ for some set } T \\ &\quad\Longrightarrow\quad St(L/K, S, r) \\ &\qquad\quad\Longrightarrow\quad St(L/K, S, T, r) \text{ for all sets } T. \end{aligned}$$

For the first implication, we only have to show that $1-\sigma_v^{-1}Nv$ is invertible in $\mathbb{Q}[G]$ for all v. Then we can invert $\delta_T(0)$ in $\mathbb{Q}[G]$ and the implication follows from Lemma 2.4.1 (i). For the inverse element we can use the geometric sum up to $n := |D_v| - 1$:

$$\sum_{k=0}^{n}(\sigma_v^{-1}Nv)^k = \frac{1-(\sigma_v^{-1}Nv)^{n+1}}{1-\sigma_v^{-1}Nv} = \frac{1-Nv^{n+1}}{1-\sigma_v^{-1}Nv}\,.$$

Hence, we get

$$(1-\sigma_v^{-1}Nv)^{-1} = \frac{1}{1-Nv^{n+1}}\sum_{k=0}^{n}(\sigma_v^{-1}Nv)^k \in \mathbb{Q}[G]\,.$$

The second implication follows directly from Lemma 2.4.1 (i).

Part (iii) is clear since $\bigcap^r \mathcal{O}_{L,S,T}^{\times} \subseteq \mathbb{Q}\bigwedge^r \mathcal{O}_{L,S,T}^{\times}$.

Part (iv) is shown for instance in [Rub96, Prop. 2.5]. □

2.4.2 Functorial Behaviour

In this section, we want to cite some results on the functorial behaviour of Rubin-Stark elements under several changes of the basic data. We fix K, L, S, T and r satisfying the Hypotheses 2.2.1 and 2.3.1. By Lemma 2.4.1, the same results can be applied to the Stark units and the Stark elements.

Changing the set S

Let $S' \supseteq S$ be a finite set of primes disjoint to T. Then the data K, L, S', T and r satisfies the hypotheses of the Rubin-Stark conjecture and we get the

Proposition 2.4.3. $\mathrm{RS}(L/K, S, T, r)$ *implies* $\mathrm{RS}(L/K, S', T, r)$ *and we get*

$$\eta_{L,S',T} = \prod_{v\in S'\setminus S}(1-\sigma_v^{-1})\cdot \eta_{L,S,T}\,.$$

Proof. See [Rub96, Prop. 3.6] and [Rub96, Prop. 6.1]. □

Note that r is fixed here, i.e. Proposition 2.4.3 is only non-trivial, if $S' \setminus S$ does not contain a prime which splits completely. For adding completely split primes to S, we have to introduce some more notation and fix an ordering of the set S'.

Concretely, let $S' = \{v_0, ..., v_n\}$ such that $V' = \{v_0, ..., v_{r'-1}\}$ are completely split. Moreover, we assume $V = \{v_0, ..., v_{r-1}\} \subseteq S$ and $S' \setminus S = V' \setminus V = \{v_r, ..., v_{r'-1}\}$. We choose a prime $w_i \mid v_i$ of L for each $i = r, ..., r'-1$. Define $W := \{w_r, ..., w_{r'-1}\}$. For each of these w_i, we obtain the G-equivariant valuation by applying Lemma 2.1.5:

$$\begin{aligned}\mathrm{Ord}_{w_i}\colon L^{\times} &\longrightarrow \mathbb{Z}[G]\\ x &\longmapsto \sum_{\sigma\in G}\mathrm{ord}_{w_i}(\sigma(x))\sigma^{-1}\,.\end{aligned}$$

Combining these maps restricted to $\mathcal{O}_{L,S',T}^{\times}$, we get

$$\mathrm{Ord}_W := (\mathrm{Ord}_{w_r}\wedge\cdots\wedge\mathrm{Ord}_{w_{r'-1}}) \in \mathrm{Hom}_{\mathbb{Z}[G]}\Big(\bigwedge^{r'}\mathcal{O}_{L,S',T}^{\times}, \bigwedge^{r}\mathcal{O}_{L,S',T}^{\times}\Big)\,.$$

Remark 2.4.4. If $W = \{w\}$ consists only of one place, we will simplify the notation and write Ord_w instead of $\mathrm{Ord}_{\{w\}}$. It will be clear from the context whether Ord_w is the map applied to a number field element or the map applied to an element in an exterior power. In fact, the definitions are consistent and meet in the case $r' = 1$ and $r = 0$.

Now we can state the next

Proposition 2.4.5. *For S and S' as above,* $\mathrm{RS}(L/K, S', T, r')$ *implies* $\mathrm{RS}(L/K, S, T, r)$ *and*

$$\eta_{L,S,T} = (-1)^{re} \, \mathrm{Ord}_W(\eta_{L,S',T}) \, ,$$

where $e = r' - r$.

Proof. See [Rub96, Prop. 5.2 and Thm. 5.3]. □

Remark 2.4.6. The ordering described here is in fact the ordering as in [BKS16, §5.3] shifted by one index. The shift is not necessary, but it turns out to be more convenient for the statement of the conjectures in Chapter 4.

We also want to consider a variant of the previous proposition. Suppose that $S = S' \setminus \{v_i\}$ for any $i \in \{0, ..., r' - 1\}$, i.e. we assume that we only remove one completely split prime but this prime can be at an arbitrary position in V'. Then we obtain

Proposition 2.4.7. *For S and S' as above,* $\mathrm{RS}(L/K, S', T, r')$ *implies* $\mathrm{RS}(L/K, S, T, r)$ *and*

$$\eta_{L,S,T} = (-1)^i \, \mathrm{Ord}_{w_i}(\eta_{L,S',T}) \, .$$

Proof. See [Rub96, Prop. 5.2 and Thm. 5.3]. □

Changing the set T

Proposition 2.4.8. *Let $T' \supseteq T$ be a finite set of primes disjoint to S. Then* $\mathrm{RS}(L/K, S, T, r)$ *implies* $\mathrm{RS}(L/K, S, T', r)$ *and*

$$\eta_{L,S,T'} = \prod_{v \in T' \setminus T} (1 - \sigma_v^{-1} N v) \cdot \eta_{L,S,T} \, .$$

Proof. See [Pop02, Prop. 5.3.1]. □

Change of the top field

As a last case, we want to take a look at the top field L.

Proposition 2.4.9. *Suppose we have an intermediate field $K \subseteq L' \subseteq L$, then* $\mathrm{RS}(L/K, S, T, r)$ *implies* $\mathrm{RS}(L'/K, S, T, r)$ *and*

$$\eta_{L',S,T} = (\bigwedge^r N_{L/L'})(\eta_{L,S,T}) \, .$$

Proof. See [Rub96, Prop. 6.1]. □

Chapter 3

An annihilation result for global function fields

In this chapter we define a group of elliptic units for global function fields and derive an index formula for this group. Then we use these elliptic units to prove an annihilation result for the ideal class group for cyclic extensions of prime power degree. The content of this chapter is also presented in [Stu20] and is accepted for publication in Acta Arithmetica.

3.1 Class field theory in global function fields

We start with some new notation and a short review of some basic class field theoretical facts for global function fields. This review is based on [Hay85, §3, §4].

Let K be a global function field and ∞ be a fixed place of K. We fix the following notation:

- $\mathbb{F}_q$ is the constant field of K,
- $\mathcal{O}_K$ is the ring of functions which have no poles away from ∞, i.e. we have $\mathcal{O}_K = \mathcal{O}_{K,\{\infty\}}$ in the sense of (2.1.3),
- d_∞ is the degree of ∞,
- $h(K)$ (resp. $h := h_K$) is the class number of K (resp. $\mathcal{O}_K$), i.e. $h = h_{K,\{\infty\}}$,
- $w_\infty := q^{d_\infty} - 1$,
- for any integral ideal $\mathfrak{m}$ of K let $S_\mathfrak{m} := \{\mathfrak{p} \subseteq \mathcal{O}_K \mid \mathfrak{p} \text{ prime}, \mathfrak{p} \mid \mathfrak{m}\}$ be the support of $\mathfrak{m}$.

As in the previous chapter, we let ord_∞ be the valuation at ∞ and let K_∞ be the completion of K at ∞ with constant field $\mathbb{F}_\infty$. For any prime $\mathfrak{p}$ of K we let $k(\mathfrak{p})$ be the residue class field at $\mathfrak{p}$ and $N\mathfrak{p} = |k(\mathfrak{p})|$. Note that we have $N\mathfrak{p} = q^{\deg(\mathfrak{p})}$. Further we get

$$h = h(K)d_\infty .$$

Now let ρ be a sign-normalized rank-1 Drinfeld module with respect to a fixed sign-function sgn. Then we set $K_{(1)}$ to be the extension of K generated by all coefficients of ρ_x, $x \in \mathcal{O}_K$. Note that this extension is finite. Now for any integral ideal $\mathfrak{m} \subseteq \mathcal{O}_K$, we introduce:

- $\rho_{\mathfrak{m}}$ is the generator of the principal ideal generated by the elements ρ_x for all $x \in \mathfrak{m}$,
- $\Lambda_{\mathfrak{m}}$ is the set of $\mathfrak{m}$-torsion points of ρ,
- $K_{\mathfrak{m}} := K_{(1)}(\Lambda_{\mathfrak{m}})$,
- $H_{\mathfrak{m}}$ is the maximal real subfield of $K_{\mathfrak{m}}$ and is called the *real ray class field* of K modulo $\mathfrak{m}$ (in particular $H = H_{(1)}$ is the *real Hilbert class field* of K),
- $H_{\mathfrak{m}^\infty} := \bigcup_{n \geq 1} H_{\mathfrak{m}^n}$.

For any extension L/K we define:

- $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L,
- h_L is the class number of $\mathcal{O}_L$,
- if $\mathfrak{p} \subseteq \mathcal{O}_K$ is a prime ideal, then $\mathfrak{p}_L$ is the product of all ideals of $\mathcal{O}_L$ above $\mathfrak{p}$,
- if L/K is abelian and $\mathfrak{m}$ is an integral ideal of K, then we set $L_{\mathfrak{m}} = L \cap H_{\mathfrak{m}}$,
- $S_\infty(L)$ is the set of places of L above ∞.

As before, we let $\mu(L)$ be the group of roots of unity in L and set $w_L := \mu(L)$. Note that $w_K = q - 1$. We also define

$$R_L := \frac{R_{L,S_\infty(L)}}{(d_\infty \log(q))^{[L:K]-1}}$$

(cf. [Ros02, Ch. 14]).

Remark 3.1.1. It is shown in [Hay85, §3, §4] that

(i) $w_{H_{\mathfrak{m}}} = w_\infty$ for all $\mathfrak{m}$ (see [Hay85, §3]), so $\mathbb{F}_\infty$ is the constant field of $H_{\mathfrak{m}}$,

(ii) $[H_{\mathfrak{m}} : K] = \frac{h}{w_K} |(\mathcal{O}_K/\mathfrak{m})^\times|$ (see [Hay85, Eq. (3.2)]) for $\mathfrak{m} \neq (1)$ and $[H : K] = h$,

(iii) $[K_{\mathfrak{m}} : H_{\mathfrak{m}}] = w_\infty$ for $\mathfrak{m} \neq 1$ (see [Hay85, §4]) and $[K_{(1)} : H] = \frac{w_\infty}{w_K}$ for $\mathfrak{m} = (1)$ (see [Hay85, Cor. 4.8(2)]).

Now suppose that the extension L/K is Galois and $\mathfrak{p}$ is a prime of K. Then we recall that

- $D_{\mathfrak{P}} \subseteq \mathrm{Gal}(L/K)$ is the decomposition group of a prime $\mathfrak{P}$ of L above $\mathfrak{p}$. If L/K is abelian, this subgroup does not depend on the choice of the prime $\mathfrak{P}$, hence we write $D_{\mathfrak{p}}$ in this case.
- $I_{\mathfrak{P}} \subseteq D_{\mathfrak{P}}$ is the inertia subgroup. If L/K is abelian we write again $I_{\mathfrak{p}}$.

- $(\mathfrak{P}, L/K)$ (or $\sigma_{\mathfrak{P}}$ if the extension is clear) is a lift to $\mathrm{Gal}(L/K)$ of the corresponding Frobenius element in $D_{\mathfrak{P}}/I_{\mathfrak{P}}$. These elements form a conjugacy class in $\mathrm{Gal}(L/K)$ which will be denoted by $(\mathfrak{p}, L/K)$ (or $\sigma_{\mathfrak{p}}$). If L/K is abelian and $\mathfrak{p}$ is unramified, this conjugacy class contains only one element which coincides with the Artin symbol.

For any abelian group G, the group of irreducible characters of G will again be denoted by $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^\times)$. For any subset $U \subseteq G$, we define

$$NU := \sum_{\sigma \in U} \sigma \in \mathbb{Z}[G]\,.$$

Additionally to the character idempotents, we define the idempotent associated to a subgroup U

$$e_U := \frac{1}{|U|} NU \in \mathbb{Q}[G]\,.$$

3.2 Elliptic units

Let Ω be the completion of the algebraic closure of K_∞ and let Γ be a lattice in Ω, i.e. a finitely generated projective $\mathcal{O}_K$-module. The *exponential function* associated to Γ is defined by

$$\begin{aligned} e_\Gamma \colon \Omega &\longrightarrow \Omega \\ z &\longmapsto z \prod_{\substack{\gamma \in \Gamma \\ \gamma \neq 0}} \left(1 - \frac{z}{\gamma}\right)\,. \end{aligned}$$

We say that Γ is *special*, if the rank-1 Drinfeld module associated to Γ (see [Hay85, §5]) is sign-normalized with respect to the fixed sign-function sgn. For each Γ, there exists an invariant $\xi(\Gamma) \in \Omega^\times$ such that $\xi(\Gamma)\Gamma$ is special. This invariant is unique up to multiplication by an element of $\mathbb{F}_\infty$.

3.2.1 Unramified elliptic units

Following [Ouk97, §2], we can fix a fractional ideal $\mathfrak{c}$ of K and a choice of the invariant $\xi(\mathfrak{c})$ such that the sign-normalized rank-1 Drinfeld module associated to $\Gamma := \xi(\mathfrak{c})\mathfrak{c}$ is exactly ρ. Let D be the differential of the twisted polynomial ring (see e.g. [Hay85, §4]). Then for any integral ideal $\mathfrak{a}$ of K, the rank-1 Drinfeld module associated to $D(\rho_{\mathfrak{a}})\mathfrak{a}^{-1}\Gamma$ is sign-normalized with respect to sgn, hence we can choose $\xi(\mathfrak{a}^{-1}\mathfrak{c}) = D(\rho_{\mathfrak{a}})\xi(\mathfrak{c})$. Any fractional ideal of K is of the form $\mathfrak{d} = \mathfrak{a}\mathfrak{b}^{-1}\mathfrak{c}$ and setting $\tau := (\mathfrak{d}^{-1}\mathfrak{c}, K_{(1)}/K)$, we can define

$$\xi(\mathfrak{d}) = \frac{D(\rho_{\mathfrak{b}})}{D(\rho_{\mathfrak{a}})^\tau} \xi(\mathfrak{c})\,.$$

Lemma 3.2.1. *The element $\xi(\mathfrak{d})$ is well defined, i.e. it is independent of the choice of $\mathfrak{a}$ and $\mathfrak{b}$. It may depend on the choice of $\mathfrak{c}$ and $\xi(\mathfrak{c})$.*

Proof. Suppose that $\mathfrak{d} = \mathfrak{a}\mathfrak{b}^{-1}\mathfrak{c} = \mathfrak{a}'\mathfrak{b}'^{-1}\mathfrak{c}$. This implies $\mathfrak{a}\mathfrak{b}' = \mathfrak{a}'\mathfrak{b}$ and hence

$$\rho_{\mathfrak{a}\mathfrak{b}'} = \rho_{\mathfrak{a}'\mathfrak{b}} \,.$$

The ideal class group acts on the set of isomorphism classes of rank-1 Drinfeld modules and via this action we obtain (cf. [Ros02, Prop. 13.15])

$$\begin{aligned} \rho_{\mathfrak{a}\mathfrak{b}'}\rho_{\mathfrak{a}'}^{\sigma_{\mathfrak{a}\mathfrak{b}'}} &= \rho_{\mathfrak{a}\mathfrak{a}'\mathfrak{b}'} = \rho_{\mathfrak{b}'}^{\sigma_{\mathfrak{a}\mathfrak{a}'}}\rho_{\mathfrak{a}\mathfrak{a}'} \,, \\ \rho_{\mathfrak{a}'\mathfrak{b}}\rho_{\mathfrak{a}}^{\sigma_{\mathfrak{a}'\mathfrak{b}}} &= \rho_{\mathfrak{a}\mathfrak{a}'\mathfrak{b}} = \rho_{\mathfrak{b}}^{\sigma_{\mathfrak{a}\mathfrak{a}'}}\rho_{\mathfrak{a}\mathfrak{a}'} \,. \end{aligned}$$

Since $\mathfrak{a}\mathfrak{a}' \neq 0$ (we only consider nonzero ideals), we have $D(\rho_{\mathfrak{a}\mathfrak{a}'}) \neq 0$. Further we have $\sigma_{\mathfrak{a}\mathfrak{b}'} = \sigma_{\mathfrak{a}'\mathfrak{b}} = \tau\sigma_{\mathfrak{a}\mathfrak{a}'}$, so we get

$$\begin{aligned} \left(\frac{D(\rho_{\mathfrak{b}})}{D(\rho_{\mathfrak{a}})^{\tau}}\right)^{\sigma_{\mathfrak{a}\mathfrak{a}'}} &= \frac{D(\rho_{\mathfrak{b}}^{\sigma_{\mathfrak{a}\mathfrak{a}'}})}{D(\rho_{\mathfrak{a}}^{\sigma_{\mathfrak{a}'\mathfrak{b}}})} = \frac{D(\rho_{\mathfrak{a}'\mathfrak{b}})}{D(\rho_{\mathfrak{a}\mathfrak{a}'})} \\ &= \frac{D(\rho_{\mathfrak{a}\mathfrak{b}'})}{D(\rho_{\mathfrak{a}\mathfrak{a}'})} = \frac{D(\rho_{\mathfrak{b}'}^{\sigma_{\mathfrak{a}\mathfrak{a}'}})}{D(\rho_{\mathfrak{a}'}^{\sigma_{\mathfrak{a}\mathfrak{b}'}})} = \left(\frac{D(\rho_{\mathfrak{b}'})}{D(\rho_{\mathfrak{a}'})^{\tau}}\right)^{\sigma_{\mathfrak{a}\mathfrak{a}'}} \,. \end{aligned}$$ □

With these definitions, we obtain analogously to [Ouk97, Lemma 3] the following explicit form of the principal ideal theorem

Lemma 3.2.2. *Let $\mathfrak{d}_1, \mathfrak{d}_2$ and $\mathfrak{d}$ be fractional ideals of K. Then the ideal $\mathfrak{d}_2\mathfrak{d}_1^{-1}\mathcal{O}_{K_{(1)}}$ is principal generated by $\xi(\mathfrak{d}_1)/\xi(\mathfrak{d}_2)$. Moreover, we have*

$$\left(\frac{\xi(\mathfrak{d}_1)}{\xi(\mathfrak{d}_2)}\right)^{(\mathfrak{d},K_{(1)}/K)} = \frac{\xi(\mathfrak{d}_1\mathfrak{d}^{-1})}{\xi(\mathfrak{d}_2\mathfrak{d}^{-1})} \,.$$

Now let $\sigma \in \mathrm{Gal}(H/K)$ be arbitrary and let $\mathfrak{a} \subseteq \mathcal{O}_K$ be such that $(\mathfrak{a}^{-1}, H/K) = \sigma$. Let $x \in \mathcal{O}_K$ be a generator of the principal ideal $\mathfrak{a}^h$, then we can define

$$\partial(\sigma) := \left(x\xi(\mathfrak{a})^h\right)^{w_\infty/w_K} \,.$$

Remark 3.2.3. (i) The element $\partial(\sigma)^{w_K}$ is well-defined, i.e. it is independent of the choice of $\mathfrak{a}$ and x. Indeed, it is even independent of the choice of $\mathfrak{c}$ and $\xi(\mathfrak{c})$: If $\mathfrak{c}'$ and $\xi'(\mathfrak{c}')$ were used to define invariants $\xi'(\mathfrak{d})$ for any fractional ideal $\mathfrak{d}$, then $\xi'(\mathfrak{d})\mathfrak{d}$ would again correspond to a sign-normalized rank-1 Drinfeld module. Since these lattices only differ by an element of $\mu(H)$ (see e.g. [Ouk97, §2]), we obtain $\xi(\mathfrak{d}) = \zeta\xi'(\mathfrak{d})$ for some $\zeta \in \mu(H)$. Taking the w_∞-th power kills the root of unity, so the element $\partial(\sigma)^{w_K}$ will be the same.

(ii) The above definition differs from the one given in [Ouk97] by the factor $1/w_K$ in the exponent. This definition of $\partial(\sigma)$ still depends on the choice of the generator x and of the ideal $\mathfrak{c}$ and $\xi(\mathfrak{c})$. However, two different choices only differ by an element of $\mu(K)$. Since we are only interested in subgroups of the units containing $\mu(K)$, it suffices to define $\partial(\sigma)$ "up to roots of unity".

Lemma 3.2.4. *Let $\sigma, \sigma_1, \sigma_2 \in \mathrm{Gal}(H/K)$. Then $\frac{\partial(\sigma_1)}{\partial(\sigma_2)} \in \mathcal{O}_H^\times$ and*

$$\left(\frac{\partial(\sigma_1)}{\partial(\sigma_2)}\right)^{\sigma} = \frac{\partial(\sigma_1\sigma)}{\partial(\sigma_2\sigma)} \,.$$

Proof. Let $\mathfrak{d}_i \subseteq \mathcal{O}_K$ be such that $(\mathfrak{d}_i^{-1}, H/K) = \sigma_i$ and let $x_i \in \mathcal{O}_K$ be a generator of $\mathfrak{d}_i^h$ for $i = 1, 2$. From Lemma 3.2.2, we obtain that

$$\frac{\xi(\mathfrak{d}_1)^h}{\xi(\mathfrak{d}_2)^h}\mathcal{O}_{K_{(1)}} = \mathfrak{d}_2^h(\mathfrak{d}_1^h)^{-1}\mathcal{O}_{K_{(1)}} = \frac{x_2}{x_1}\mathcal{O}_{K_{(1)}} .$$

Therefore,

$$\frac{x_1\xi(\mathfrak{d}_1)^h}{x_2\xi(\mathfrak{d}_2)^h} \in \mathcal{O}_{K_{(1)}}^\times .$$

It is shown in [Yin97, Lemma 1.5 (1)] that

$$[\mathcal{O}_{K_{(1)}}^\times : \mathcal{O}_H^\times] = \frac{w_\infty}{w_K} ,$$

hence we get

$$\frac{\partial(\sigma_1)}{\partial(\sigma_2)} = \left(\frac{x_1\xi(\mathfrak{d}_1)^h}{x_2\xi(\mathfrak{d}_2)^h}\right)^{w_\infty/w_K} \in \mathcal{O}_H^\times .$$

Now let $\mathfrak{d} \subseteq \mathcal{O}_K$ be such that $(\mathfrak{d}^{-1}, H/K) = \sigma$ and let $x \in \mathcal{O}_K$ be a generator of $\mathfrak{d}^h$. Then $x_i x$ is a generator of $(\mathfrak{d}_i\mathfrak{d})^h$ and we obtain

$$\frac{x_1 x\xi(\mathfrak{d}_1\mathfrak{d})^h}{x_2 x\xi(\mathfrak{d}_2\mathfrak{d})^h} = \frac{x_1}{x_2}\left(\frac{\xi(\mathfrak{d}_1\mathfrak{d})}{\xi(\mathfrak{d}_2\mathfrak{d})}\right)^h .$$

Now we can apply Lemma 3.2.2 to the second quotient and obtain

$$\frac{x_1 x\xi(\mathfrak{d}_1\mathfrak{d})^h}{x_2 x\xi(\mathfrak{d}_2\mathfrak{d})^h} = \frac{x_1}{x_2}\left(\left(\frac{\xi(\mathfrak{d}_1)}{\xi(\mathfrak{d}_2)}\right)^{(\mathfrak{d}^{-1}, K_{(1)}/K)}\right)^h .$$

Since $x_1, x_2 \in K$, we get $(x_1/x_2)^{(\mathfrak{d}^{-1}, K_{(1)}/K)} = x_1/x_2$ and hence

$$\frac{x_1 x\xi(\mathfrak{d}_1\mathfrak{d})^h}{x_2 x\xi(\mathfrak{d}_2\mathfrak{d})^h} = \left(\frac{x_1}{x_2}\left(\frac{\xi(\mathfrak{d}_1)}{\xi(\mathfrak{d}_2)}\right)^h\right)^{(\mathfrak{d}^{-1}, K_{(1)}/K)} = \left(\frac{x_1\xi(\mathfrak{d}_1)^h}{x_2\xi(\mathfrak{d}_2)^h}\right)^{(\mathfrak{d}^{-1}, K_{(1)}/K)} .$$

Raising to the w_∞/w_K-th power gives

$$\frac{\partial(\sigma_1\sigma)}{\partial(\sigma_2\sigma)} = \left(\frac{\partial(\sigma_1)}{\partial(\sigma_2)}\right)^{(\mathfrak{d}^{-1}, K_{(1)}/K)} .$$

Since $\partial(\sigma_1)/\partial(\sigma_2) \in H$ and

$$(\mathfrak{d}^{-1}, K_{(1)}/K)|_H = (\mathfrak{d}^{-1}, H/K) = \sigma ,$$

we obtain the desired result. □

3.2.2 Ramified elliptic units

Using the exponential function, we can define the elements

$$\lambda_{\mathfrak{m}} := \xi(\mathfrak{m}) e_{\mathfrak{m}}(1)$$

for each integral ideal $\mathfrak{m} \neq (1)$. It is shown in [Hay85, §5] that this element is a generator of the $\mathfrak{m}$-torsion points $\Lambda'_{\mathfrak{m}}$ of the sign-normalized rank-1 Drinfeld module ρ' associated to $\xi(\mathfrak{m})\mathfrak{m}$. The construction of $K_{\mathfrak{m}}$ does not depend on the chosen Drinfeld module but only on the sign-function, hence $\lambda_{\mathfrak{m}} \in K_{(1)}(\Lambda'_{\mathfrak{m}}) = K_{\mathfrak{m}}$ (cf. [Hay85, §4]). Indeed, if $\mathfrak{b}$ is an integral ideal of $\mathcal{O}_K$ such that $\mathfrak{b}$ is prime to $\mathfrak{m}$ and $(\mathfrak{b}, K_{(1)}/K) = (\mathfrak{m}^{-1}, K_{(1)}/K)$, then one can show that $(\mathfrak{bc}, K_{\mathfrak{m}}/K)$ defines a bijection $\Lambda_{\mathfrak{m}} \longrightarrow \Lambda'_{\mathfrak{m}}$ (note that $\xi(\mathfrak{m})\mathfrak{m}$ is associated to the Drinfeld module $\mathfrak{bc} * \rho$, then use [Hay85, Thm. 4.12]). It is also shown in [Hay85, Thm. 4.17] that

$$\alpha_{\mathfrak{m}} := -N_{K_{\mathfrak{m}}/H_{\mathfrak{m}}}(\lambda_{\mathfrak{m}}) = \lambda_{\mathfrak{m}}^{w_\infty} \in H_{\mathfrak{m}}$$

is a unit if $\mathfrak{m}$ is not a prime power and that $\alpha_{\mathfrak{p}^k}$ generates the ideal $\mathfrak{p}_{H_{\mathfrak{m}}}^{w_\infty/w_k}$.

Remark 3.2.5. (i) The element $\lambda_{\mathfrak{m}}$ depends on the choice of $\mathfrak{c}$ which was used to define the invariants $\xi(\mathfrak{m})$. As already noted in Remark 3.2.3, changing $\mathfrak{c}$ would change $\xi(\mathfrak{m})$ by a root of unity in H, therefore $\alpha_{\mathfrak{m}} = \lambda_{\mathfrak{m}}^{w_\infty}$ is independent of this choice.

(ii) Note that our definition of $\alpha_{\mathfrak{m}}$ differs from the one in [Hay85] by a sign, i.e. $\alpha_{\mathfrak{m}} = -\alpha_{\mathfrak{m},Ha}$. This is neccessary for obtaining the correct norm relation, see Proposition 3.2.9 below.

3.2.3 The group of elliptic units in an arbitrary real abelian extension

Now let L be a real abelian extension of K of conductor $\mathfrak{m}$. Remember that for any integral ideal $\mathfrak{n} \subseteq \mathcal{O}_K$ we defined $L_{\mathfrak{n}} = L \cap H_{\mathfrak{n}}$. Set

$$\varphi_{L,\mathfrak{n}} := N_{H_{\mathfrak{n}}/L_{\mathfrak{n}}}(\alpha_{\mathfrak{n}})^h .$$

Remark 3.2.6. Raising to the h-th power is neccessary to ensure compatibility with the unramified elliptic units for the desired index formula. If there are no unramified elliptic units (e.g. when L/K is a totally ramified extension), we can also work with the elements $\eta_{\mathfrak{n}} = \varphi_{L,\mathfrak{n}}^{1/h}$, see Section 3.4.

Corollary 3.2.7. *(i) If $\mathfrak{n}$ is not a prime power, then $\varphi_{L,\mathfrak{n}} \in \mathcal{O}_{L_{\mathfrak{n}}}^\times$.*

(ii) If $\mathfrak{n} = \mathfrak{p}^k$, then $\varphi_{L,\mathfrak{n}}$ generates the ideal $\mathfrak{p}_{L_{\mathfrak{n}}}^{[H:L_{(1)}]hw_\infty/w_K}$.

Proof. This follows directly from [Hay85, Thm. 4.17]. □

Definition 3.2.8. (i) For $\sigma_1, \sigma_2 \in \mathrm{Gal}(L_{(1)}/K)$ define

$$\frac{\partial_L(\sigma_1)}{\partial_L(\sigma_2)} := N_{H/L_{(1)}}\left(\frac{\partial(\widehat{\sigma}_1)}{\partial(\widehat{\sigma}_2)}\right),$$

where $\widehat{\sigma}_i$ is any lift of σ_i to $\mathrm{Gal}(H/K)$.

(ii) The subgroup Δ_L of $\mathcal{O}_{L_{(1)}}^{\times}$, generated by $\mu(L)$ and the elements

$$\frac{\partial_L(\sigma_1)}{\partial_L(\sigma_2)}$$

for $\sigma_1, \sigma_2 \in \mathrm{Gal}(L_{(1)}/K)$, is the *group of unramified elliptic units* of L.

(iii) The elements $\varphi_{L,\mathfrak{n}}$ for $\mathfrak{n} \mid \mathfrak{m}$, $\mathfrak{n} \neq (1)$ are called the *ramified elliptic numbers* of L.

(iv) The $\mathrm{Gal}(L/K)$-submodule P_L of $L^{\times}$ generated by Δ_L and the ramified elliptic numbers is called the *group of elliptic numbers* of L.

(v) The *group of elliptic units* C_L of L is defined by $C_L := P_L \cap \mathcal{O}_L^{\times}$.

Proposition 3.2.9. *We have*

$$N_{L_{\mathfrak{np}}/L_{\mathfrak{n}}}(\varphi_{L,\mathfrak{np}}) = \begin{cases} \varphi_{L,\mathfrak{n}}, & \mathfrak{p} \mid \mathfrak{n}, \\ \varphi_{L,\mathfrak{n}}^{1-\sigma_{\mathfrak{p}}^{-1}}, & \mathfrak{p} \nmid \mathfrak{n}, \mathfrak{n} \neq (1), \\ x_{\mathfrak{p}}^{w_\infty/w_K[H:L_{(1)}]}\left(\frac{\partial_L(1)}{\partial_L(\sigma_{\mathfrak{p}}^{-1})}\right), & \mathfrak{n} = (1), \end{cases}$$

where $\sigma_{\mathfrak{p}} = (\mathfrak{p}, L_{\mathfrak{n}}/K)$ and $x_{\mathfrak{p}}$ is a generator of $\mathfrak{p}^h$. The last equation should be read modulo roots of unity (cf. Remark 3.2.3).

Proof. We start with the definition of $\varphi_{L,\mathfrak{np}}$ and obtain

$$\begin{aligned} N_{L_{\mathfrak{np}}/L_{\mathfrak{n}}}(\varphi_{L,\mathfrak{np}}) &= N_{H_{\mathfrak{np}}/L_{\mathfrak{n}}}(\alpha_{\mathfrak{np}})^h = N_{H_{\mathfrak{n}}/L_{\mathfrak{n}}}(N_{H_{\mathfrak{np}}/H_{\mathfrak{n}}}(\alpha_{\mathfrak{np}}))^h \\ &= N_{H_{\mathfrak{n}}/L_{\mathfrak{n}}}(N_{H_{\mathfrak{np}}/H_{\mathfrak{n}}}(\lambda_{\mathfrak{np}}^{w_\infty}))^h. \end{aligned}$$

Now we obtain from [Tat84, Ch. IV, Lemme 1.1] that w_∞ is the greatest common divisor of elements in the set $\{N\mathfrak{a} - 1 \mid \sigma_{\mathfrak{a}} = (\mathfrak{a}, H_{\mathfrak{m}}/K) = 1\}$. Then there exist ideals $\mathfrak{a}_1, ..., \mathfrak{a}_n$ with $\sigma_{\mathfrak{a}_i} = 1$ for each i such that

$$w_\infty = \sum_{i=1}^{n} N\mathfrak{a}_i - 1\,,$$

and we obtain

$$N_{L_{\mathfrak{np}}/L_{\mathfrak{n}}}(\varphi_{L,\mathfrak{np}}) = \prod_{i=1}^{n} N_{H_{\mathfrak{n}}/L_{\mathfrak{n}}}(N_{H_{\mathfrak{np}}/H_{\mathfrak{n}}}(\lambda_{\mathfrak{np}}^{N\mathfrak{a}_i - 1}))^h\,.$$

In [Ouk95] Oukhaba defined elliptic units $\psi(1; \mathfrak{n}, \mathfrak{a}^{-1}\mathfrak{n})$ for $(\mathfrak{a}, \mathfrak{n}) = 1$ which satisfy

$$\psi(1; \mathfrak{n}, \mathfrak{a}^{-1}\mathfrak{n}) = \lambda_{\mathfrak{n}}^{N\mathfrak{a} - \sigma_{\mathfrak{a}}}\,.$$

He also proved

$$N_{H_{\mathfrak{n}\mathfrak{p}}/H_{\mathfrak{n}}}(\psi(1;\mathfrak{n}\mathfrak{p},\mathfrak{a}^{-1}\mathfrak{n}\mathfrak{p})) = \begin{cases} \psi(1;\mathfrak{n},\mathfrak{a}^{-1}\mathfrak{n}), & \mathfrak{p} \mid \mathfrak{n}, \\ \psi(1;\mathfrak{n},\mathfrak{a}^{-1}\mathfrak{n})^{1-\sigma_{\mathfrak{p}}^{-1}}, & \mathfrak{p} \nmid \mathfrak{n}, \mathfrak{n} \neq (1). \end{cases}$$

Inserting this yields for $\mathfrak{p} \mid \mathfrak{n}$

$$N_{L_{\mathfrak{n}\mathfrak{p}}/L_{\mathfrak{n}}}(\varphi_{L,\mathfrak{n}\mathfrak{p}}) = \prod_{i=1}^{n} N_{H_{\mathfrak{n}}/L_{\mathfrak{n}}}(\lambda_{\mathfrak{n}}^{N\mathfrak{a}_i - 1})^h = N_{H_{\mathfrak{n}}/L_{\mathfrak{n}}}(\lambda_{\mathfrak{n}}^{w_\infty})^h = \varphi_{L,\mathfrak{n}} \,.$$

The case $\mathfrak{p} \nmid \mathfrak{n}$, $\mathfrak{n} \neq (1)$ follows analogously.

In the case $\mathfrak{n} = 1$, we use [Ouk97, Remark 1], where he showed that

$$N_{K_{\mathfrak{p}}/K_{(1)}}(\mu_{\mathfrak{p}}) = \frac{\xi(\mathfrak{p}^{-1}\mathfrak{c})}{\xi(\mathfrak{c})}$$

for a generator $\mu_{\mathfrak{p}}$ of $\Lambda_{\mathfrak{p}}$. As noted above, we can choose $\mu_{\mathfrak{p}} = \lambda_{\mathfrak{p}}^{(\mathfrak{b}\mathfrak{c},K_{\mathfrak{p}}/K)^{-1}}$, where $\mathfrak{b}$ is an integral ideal prime to $\mathfrak{p}$ such that $(\mathfrak{b}, K_{(1)}/K) = (\mathfrak{p}^{-1}, K_{(1)}/K)$. Then we obtain with Lemma 3.2.2

$$N_{K_{\mathfrak{p}}/K_{(1)}}(\lambda_{\mathfrak{p}}) = N_{K_{\mathfrak{p}}/K_{(1)}}(\mu_{\mathfrak{p}})^{(\mathfrak{b}\mathfrak{c},K_{(1)}/K)} = \left(\frac{\xi(\mathfrak{p}^{-1}\mathfrak{c})}{\xi(\mathfrak{c})}\right)^{(\mathfrak{p}^{-1}\mathfrak{c},K_{(1)}/K)} = \frac{\xi(\mathcal{O}_K)}{\xi(\mathfrak{p})} \,.$$

Set $x := x_{\mathfrak{p}}$, then the above observation yields

$$\begin{aligned} N_{L_{\mathfrak{p}}/L_{(1)}}(\varphi_{L,\mathfrak{p}}) &= N_{L_{\mathfrak{p}}/L_{(1)}}\left(N_{K_{\mathfrak{p}}/L_{\mathfrak{p}}}(\lambda_{\mathfrak{p}})^h\right) = N_{K_{\mathfrak{p}}/L_{(1)}}(\lambda_{\mathfrak{p}})^h \\ &= N_{K_{(1)}/L_{(1)}}\left(N_{K_{\mathfrak{p}}/K_{(1)}}(\lambda_{\mathfrak{p}})\right)^h \\ &= N_{H/L_{(1)}}\left(N_{K_{(1)}/H}\left(\frac{\xi(\mathcal{O}_K)}{\xi(\mathfrak{p})}\right)^h\right) \\ &= N_{H/L_{(1)}}\left(N_{K_{(1)}/H}\left(x^{w_\infty/w_K}\frac{\xi(\mathcal{O}_K)^{hw_\infty/w_K}}{(x\xi(\mathfrak{p})^h)^{w_\infty/w_K}}\right)^{w_K/w_\infty}\right) \\ &= x^{[K_{(1)}:L_{(1)}]}N_{H/L_{(1)}}\left(N_{K_{(1)}/H}\left(\frac{\partial(1)}{\partial(\sigma_{\mathfrak{p}}^{-1})}\right)^{w_K/w_\infty}\right) \\ &= x^{w_\infty/w_K[H:L_{(1)}]}N_{H/L_{(1)}}\left(\frac{\partial(1)}{\partial(\sigma_{\mathfrak{p}}^{-1})}\right) \\ &= x^{w_\infty/w_K[H:L_{(1)}]}\left(\frac{\partial_L(1)}{\partial_L(\sigma_{\mathfrak{p}}^{-1})}\right) \,. \end{aligned}$$

□

3.2.4 Kronecker's Limit Formulae

We fix a prime $w_0 \in S_\infty(H_{\mathfrak{m}})$. Then for each subfield M of $H_{\mathfrak{m}}$, there is a unique prime in $S_\infty(M)$ below w_0. Since ∞ splits completely in $H_{\mathfrak{m}}$, the valuations of these primes are compatible. By abuse of notation, we denote each of these valuations by ord_∞, i.e. for an element $x \in H_{\mathfrak{m}}$ we implicitly set

$$\mathrm{ord}_\infty(x) := \mathrm{ord}_{w_0}(x)$$

and analogously for each subfield M of $H_{\mathfrak{m}}$. The same convention will be used for absolute values.

Now we can state Kronecker's second limit formula:

Proposition 3.2.10. *(i) Let* $(1) \neq \mathfrak{n} \mid \mathfrak{m}$ *and let* $\chi \in \widehat{\mathrm{Gal}(H_\mathfrak{n}/K)}$. *Then we have*

$$L_{S_\mathfrak{n}}(\chi, 0) = \frac{1}{w_\infty} \sum_{\sigma \in \mathrm{Gal}(H_\mathfrak{n}/K)} \mathrm{ord}_\infty(\alpha_\mathfrak{n}^\sigma)\chi(\sigma)\,.$$

(ii) For any non-trivial character $\chi \in \widehat{\mathrm{Gal}(H/K)}$, *we have*

$$L(\chi, 0) = \frac{1}{w_\infty h} \sum_{\sigma \in \mathrm{Gal}(H/K)} \mathrm{ord}_\infty(\partial(\sigma))\chi(\sigma)\,.$$

Proof. Part (i) is exactly the last equation in [Hay85], whereas part (ii) follows directly from [Ouk97, Proof of Prop. 3] and Remark 3.2.3. □

Remark 3.2.11. The proposition shows that we can regard the ramified elliptic units as Stark units which was already indicated in Remark 2.2.7. Indeed, for $\mathfrak{n} \neq 1$ the set $S := S_\mathfrak{n} \cup \{\infty\}$ contains all places which ramify in $H_\mathfrak{n}/K$ and $|S| \geq 2$. Moreover, S contains the completely split prime ∞. By definition of the L-function, we obtain

$$L_S(\chi, s) = (1 - \chi(\infty)N\infty^{-s})L_{S_\mathfrak{n}}(\chi, s) = (1 - N\infty^{-s})L_{S_\mathfrak{n}}(\chi, s)$$

and hence

$$\begin{aligned} L'_S(\chi, 0) = \log(N\infty)L_{S_\mathfrak{n}}(\chi, 0) &= -\frac{1}{w_\infty} \sum_{\sigma \in \mathrm{Gal}(H_\mathfrak{n}/K)} \log\left(N\infty^{-\mathrm{ord}_\infty(\alpha_\mathfrak{n}^\sigma)}\right)\chi(\sigma) \\ &= -\frac{1}{w_\infty} \sum_{\sigma \in \mathrm{Gal}(H_\mathfrak{n}/K)} \log|\alpha_\mathfrak{n}^\sigma|_\infty\, \chi(\sigma)\,. \end{aligned}$$

Comparing this with Conjecture 2.2.6 yields $\varepsilon_{H_\mathfrak{n},S} = \alpha_\mathfrak{n}$ up to roots of unity.

3.3 An index formula

3.3.1 Sinnott's module

Remember that for a prime $\mathfrak{p}$ of K the element $\sigma_\mathfrak{p} \in G = \mathrm{Gal}(L/K)$ is the lift of an associated Frobenius element in $D_\mathfrak{p}/I_\mathfrak{p}$. Define $\tau_\mathfrak{p} := \sigma_\mathfrak{p}^{-1} e_{I_\mathfrak{p}} \in \mathbb{Q}[G]$.

Definition 3.3.1. (i) For any integral ideal $\mathfrak{n}$ of $\mathcal{O}_K$, we define

$$\rho'_\mathfrak{n} := N\,\mathrm{Gal}(L/L_\mathfrak{n}) \prod_{\mathfrak{p}|\mathfrak{n}} (1 - \tau_\mathfrak{p})\,.$$

(ii) The $\mathbb{Z}[G]$-submodule U' of $\mathbb{Q}[G]$ generated by $\rho'_\mathfrak{n}$, where $\mathfrak{n}$ runs through all integral ideals of $\mathcal{O}_K$ is called *Sinnott's module.*

(iii) Define U'_0 to be the kernel of multiplication by NG in U'.

Remark 3.3.2. (i) The notation U' and $\rho'_{\mathfrak{n}}$ is adopted from [CK19]. In the second part of this chapter, we use a modification of Sinnott's module which will be denoted by U.

(ii) Note that for all integral ideals $\mathfrak{n}$, we have $L_{\mathfrak{n}} = L_{\gcd(\mathfrak{n},\mathfrak{m})}$, hence $\rho'_{\mathfrak{n}} = \rho'_{\gcd(\mathfrak{n},\mathfrak{m})}$. Therefore, it suffices to consider the elements $\rho'_{\mathfrak{n}}$ with $\mathfrak{n} \mid \mathfrak{m}$.

(iii) If $\mathfrak{n} \neq (1)$, we have $\rho'_{\mathfrak{n}} \in U'_0$. As in the imaginary quadratic case (cf. [Ouk03]) the component of U' generated by $\rho'_{(1)}$ intersected with U'_0 is generated by

$$\rho'_{(1)}(1-\sigma)\,, \quad \sigma \in G\,.$$

If $\sigma, \sigma' \in G$ are lifts of the same element $\tau \in \mathrm{Gal}(L_{(1)}/K)$, then

$$\rho'_{(1)}(1-\sigma) = \rho'_{(1)}(1-\sigma')\,,$$

hence it suffices to consider the elements

$$\rho'_{(1)}(1-\widetilde{\tau})\,, \quad \tau \in \mathrm{Gal}(L_{(1)}/K)\,,$$

where $\widetilde{\tau} \in G$ is an arbitrary lift of τ.

Now recall the convention introduced in Section 3.2.4 and consider the logarithmic map

$$\begin{aligned} l_L\colon L^\times &\longrightarrow \mathbb{Q}[G] \\ x &\longmapsto \sum_{\sigma\in G} \mathrm{ord}_\infty(x^\sigma)\sigma^{-1} \end{aligned}$$

and the element

$$\omega := h w_\infty \sum_{\substack{\chi\in\widehat{G} \\ \chi\neq 1}} L(\chi,0) e_{\chi^{-1}}\,.$$

Also define

$$l_L^* := (1-e_G) l_L\,.$$

The analogue of [Ouk03, Prop. 6] is then the next

Proposition 3.3.3. *Let $\mathfrak{n} \neq 1$ be such that $\mathfrak{n} \mid \mathfrak{m}$ and let $\tau \in \mathrm{Gal}(L_{(1)}/K)$, then*

$$\begin{aligned} l_L^*(\varphi_{L,\mathfrak{n}}) &= \omega\rho'_{\mathfrak{n}}\,, \\ l_L^*\left(\frac{\partial_L(1)}{\partial_L(\tau)}\right) &= \omega\rho'_{(1)}(1-\widetilde{\tau})\,, \end{aligned}$$

where $\widetilde{\tau} \in G$ is any lift of τ.

Proof. We can verify the equalities on the χ-components where χ runs through all non-trivial characters of G. Let $\mathfrak{m}_\chi$ be the conductor of χ. Since $\varphi_{L,\mathfrak{n}} \in L_\mathfrak{n}$, we compute

$$\begin{aligned}\chi(l_L^*(\varphi_{L,\mathfrak{n}})) &= \sum_{\sigma\in G} \mathrm{ord}_\infty\left(\varphi_{L,\mathfrak{n}}^\sigma\right)\chi^{-1}(\sigma)\\ &= \sum_{\sigma\in \mathrm{Gal}(L_\mathfrak{n}/K)}\ \sum_{\tau\in\mathrm{Gal}(L/L_\mathfrak{n})} \mathrm{ord}_\infty\left(\varphi_{L,\mathfrak{n}}^{\sigma\tau}\right)\chi^{-1}(\sigma)\chi^{-1}(\tau)\\ &= \chi(N\,\mathrm{Gal}(L/L_\mathfrak{n}))\sum_{\sigma\in \mathrm{Gal}(L_\mathfrak{n}/K)} \mathrm{ord}_\infty\left(\varphi_{L,\mathfrak{n}}^\sigma\right)\chi^{-1}(\sigma)\,.\end{aligned}$$

We first observe that if $\mathfrak{m}_\chi \nmid \mathfrak{n}$ then $\chi(N\,\mathrm{Gal}(L/L_\mathfrak{n}))=0$, so

$$\chi(l_L^*(\varphi_{L,\mathfrak{n}})) = 0 = \chi(\omega\rho'_\mathfrak{n})\,.$$

Therefore, it suffices to consider the characters such that $\mathfrak{m}_\chi \mid \mathfrak{n}$. In this case, we have $\mathrm{Gal}(L/L_\mathfrak{n}) \subseteq \ker(\chi)$ and hence χ is the inflation of a character of $\mathrm{Gal}(L_\mathfrak{n}/K)$ which we will also denote by χ (this is justified by Proposition 2.1.8 (i)). This character can be inflated to a character χ of $\mathrm{Gal}(H_\mathfrak{n}/K)$ with $\mathrm{Gal}(H_\mathfrak{n}/L_\mathfrak{n}) \subseteq \ker(\chi)$. Then we obtain with Proposition 3.2.10 (i)

$$\begin{aligned}\chi(l_L^*(\varphi_{L,\mathfrak{n}})) &= \chi(N\,\mathrm{Gal}(L/L_\mathfrak{n}))h\sum_{\sigma\in \mathrm{Gal}(L_\mathfrak{n}/K)} \mathrm{ord}_\infty\left(N_{H_\mathfrak{n}/L_\mathfrak{n}}(\alpha_\mathfrak{n})^\sigma\right)\chi^{-1}(\sigma)\\ &= \chi(N\,\mathrm{Gal}(L/L_\mathfrak{n}))h\sum_{\sigma\in \mathrm{Gal}(L_\mathfrak{n}/K)}\ \sum_{\tau\in\mathrm{Gal}(H_\mathfrak{n}/K)} \mathrm{ord}_\infty\left(\alpha_\mathfrak{n}^{\sigma\tau}\right)\chi^{-1}(\sigma\tau)\\ &= \chi(N\,\mathrm{Gal}(L/L_\mathfrak{n}))h\sum_{\sigma\in \mathrm{Gal}(H_\mathfrak{n}/K)} \mathrm{ord}_\infty\left(\alpha_\mathfrak{n}^{\sigma}\right)\chi^{-1}(\sigma)\\ &= \chi(N\,\mathrm{Gal}(L/L_\mathfrak{n}))hw_\infty L_{S_\mathfrak{n}}(\chi^{-1},0)\\ &= \chi(N\,\mathrm{Gal}(L/L_\mathfrak{n}))\prod_{\mathfrak{p}\mid\mathfrak{n}}(1-\chi^{-1}(\mathfrak{p}))\chi(\omega)\\ &= \chi(\rho'_\mathfrak{n}\omega)\,.\end{aligned}$$

The other equation follows analogously with Proposition 3.2.10 (ii). □

Corollary 3.3.4. *We have* $l_L^*(P_L) = \omega\cdot U'_0$.

Proof. This follows directly from Remark 3.3.2. □

3.3.2 Index computations

We briefly recall the definition of Sinnott's Index (see [Ouk03, §4]). Let V be a finite-dimensional vector space over $L=\mathbb{Q}$ or $\mathbb{R}$. A subgroup X of V is called *lattice* if $\mathrm{rk}_\mathbb{Z}(X) = \dim_L(V)$ and $LX = V$. If A and B are lattices of V and γ is an automorphism of V such that $\gamma(A) = B$, then we define

$$[A : B] := |\det(\gamma)|\ .$$

If $B \subseteq A$, then $[A : B]$ is the usual group index. Now we can prove

Proposition 3.3.5. *We have*

$$[U_0' : l_L^*(P_L)] = (hw_\infty)^{[L:K]-1} \cdot \frac{w_K h_L R_L}{w_L h} .$$

Proof. We can adjust the proof of [Ouk03, Prop. 7] to our situation. Using Proposition 2.1.8 (ii) and

$$L'_{\{\infty\}}(\chi, 0) = \log(N\infty) \cdot L(\chi, 0) = d_\infty \log(q) \cdot L(\chi, 0) ,$$

we obtain with the analytic class number formula 2.1.14

$$\begin{aligned} \zeta^{(r)}_{L,S_\infty(L)}(0) &= \zeta_{K,\{\infty\}}(0) \cdot \prod_{\chi \neq 1} L'_{\{\infty\}}(\chi, 0) \\ &= -\frac{hR_{K,\{\infty\}}}{w_K} (d_\infty \log(q))^{[L:K]-1} \prod_{\chi \neq 1} L(\chi, 0) , \end{aligned}$$

where $r = |S_\infty(L)| - 1$. Note that $R_{K,\{\infty\}} = 1$ since $\mathcal{O}^\times_{K,\{\infty\}} = \mu(K)$. Remember that $R_L = \frac{R_{L,S_\infty(L)}}{(d_\infty \log(q))^{[L:K]-1}}$. Applying Theorem 2.1.14 once again, this yields

$$\prod_{\chi \neq 1} L(\chi, 0) = \frac{w_K h_L R_L}{w_L h} .$$

By Corollary 3.3.4 we have $l_L^*(P_L) = \omega U_0'$ and hence we obtain

$$\begin{aligned} [U_0' : l_L^*(P_L)] &= [U_0' : \omega U_0'] = |\det(\omega)| \\ &\overset{(*)}{=} \prod_{\chi \neq 1} \chi(\omega) \\ &= (hw_\infty)^{[L:K]-1} \prod_{\chi \neq 1} L(\chi^{-1}, 0) \\ &= (hw_\infty)^{[L:K]-1} \cdot \frac{w_K h_L R_L}{w_L h} . \end{aligned}$$

The equality $(*)$ follows from [Sin80, Lemma 1.2 (b)]. □

Let $\mathfrak{p} \mid \mathfrak{m}$ be a prime ideal of K. The norm relation of Proposition 3.2.9 implies that $x_\mathfrak{p}^{w_\infty / w_K [H:L_{(1)}]} \in P_L$, where $x_\mathfrak{p}$ is a generator of $\mathfrak{p}^h$.

Definition 3.3.6. Let Q_L be the subgroup of P_L generated by $\mu(L), \Delta_L$ and the elements $x_\mathfrak{p}^{w_\infty / w_K [H:L_{(1)}]}$ for all $\mathfrak{p} \mid \mathfrak{m}$.

Now we can state the analogue of [Ouk03, Prop. 8]

Proposition 3.3.7. *We have*

$$[l_L^*(P_L) : l_L(C_L)] = \frac{\prod_\mathfrak{p} [L \cap H_{\mathfrak{p}^\infty} : L_{(1)}]}{[P_L^{w_L} \cap K : Q_L^{w_L} \cap K]} ,$$

where $\mathfrak{p}$ runs though all maximal ideals of $\mathcal{O}_K$.

For the proof we need the following

Lemma 3.3.8. *(i)* $\ker(l_L) \cap \mathcal{O}_L^\times = \mu(L)$.

(ii) $l_L(C_L) = l_L^*(C_L)$.

Proof. (i) The inclusion $\mu(L) \subseteq \ker(l_L) \cap \mathcal{O}_L^\times$ is clear. So let $x \in \ker(l_L) \cap \mathcal{O}_L^\times$, then by definition of $\mathcal{O}_L^\times$, the valuation of x at every place which is not dividing ∞ is 0. But since $x \in \ker(l_L)$, we find

$$0 = l_L(x) = \sum_{\sigma \in G} \operatorname{ord}_\infty(x^\sigma)\sigma^{-1}$$

and hence $\operatorname{ord}_\infty(x^\sigma) = 0$ for all $\sigma \in G$. Therefore, the valuation of x at any place is 0, so x must be in the field of constants. Since $x \neq 0$, we obtain $x \in \mu(L)$.

(ii) Let $u \in C_L$, then

$$e_G \cdot l_L(u) = \frac{1}{|G|} l_L(N_{L/K}(u)) .$$

Since $N_{L/K}(u) \in \mathcal{O}_K^\times = \mu(K)$, we get by part (i)

$$e_G \cdot l_L(u) = 0 ,$$

hence

$$l_L(u) = l_L^*(u) .$$

□

Proof of Proposition 3.3.7. We easily see that if $L \subseteq H$, then $P_L = Q_L = C_L$ and $L = L_{(1)} = L \cap H_{\mathfrak{p}^\infty}$, so there is nothing to show. Hence we can assume $\mathfrak{m} \neq (1)$. Defining $P' := P_L^{w_L}$ and $C' := P' \cap \mathcal{O}_L^\times = C_L^{w_L}$, we compute

$$\begin{aligned}
[l_L^*(P_L) : l_L^*(C_L)] &= \frac{[l_L^*(P_L) : l_L^*(C')]}{[l_L^*(C_L) : l_L^*(C')]} \\
&= \frac{[l_L^*(P_L) : l_L^*(P')]}{[l_L^*(C_L) : l_L^*(C')]} [l_L^*(P') : l_L^*(C')] \\
&= [l_L^*(P') : l_L^*(C')]
\end{aligned}$$

since

$$[l_L^*(P_L) : l_L^*(P')] = w_L^{[L:K]-1} = [l_L^*(C_L) : l_L^*(C')] .$$

We also define $Q' := Q_L^{w_L}$ and $\Delta' := Q' \cap \mathcal{O}_L^\times$. Then we claim that $Q' \cap \ker(l_L^*) = Q' \cap K$ and $P' \cap \ker(l_L^*) = P' \cap K$. One of the inclusions is clear in both cases, since obviously $K^\times \subseteq \ker(l_L^*)$. For the other inclusion let $x \in \ker(l_L^*)$. Then for any $\sigma \in G$ we find

$$0 = \sigma l_L^*(x) = l_L(x^{\sigma - 1}) ,$$

so $x^{\sigma-1} \in \ker(l_L)$. From [Hay85, Cor. 4.13] we get that $x^{\sigma-1} \in \mathcal{O}_L^\times$ for every $x \in P'$, hence also for every $x \in Q'$. By Lemma 3.3.8 we conclude that $x^{\sigma-1} \in \mu(L)$, and since x is a w_L-th power, we find $x^{\sigma-1} = 1$ for every $\sigma \in G$. Hence $x \in K$.

From this we obtain the following commutative diagramm with exact rows and columns:

$$\begin{array}{ccccccccc} & & 1 & & 1 & & 1 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & Q' \cap K & \longrightarrow & Q'/\Delta' & \xrightarrow{l_L^*} & l_L^*(Q')/l_L^*(\Delta') & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & P' \cap K & \longrightarrow & P'/C' & \xrightarrow{l_L^*} & l_L^*(P')/l_L^*(C') & \longrightarrow & 1 \end{array}$$

Applying the snake lemma gives

$$\frac{[l_L^*(P') : l_L^*(C')]}{[l_L^*(Q') : l_L^*(\Delta')]} = \frac{[P'/C' : Q'/\Delta']}{[P' \cap K : Q' \cap K]} .$$

Since $K^\times \subseteq \ker(l_L^*)$ we get $l_L^*(Q') = l_L^*(\Delta')$. Now suppose that $\mathfrak{m} = \prod_{i=1}^s \mathfrak{p}_i^{e_i}$ is the prime decomposition of the conductor of L. For the computation of the index $[P'/C' : Q'/\Delta']$ we choose prime ideals $\mathfrak{P}_i \subseteq \mathcal{O}_L$ such that $\mathfrak{P}_i \mid \mathfrak{p}_i$ and define t_i to be the ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}_i$. Let ord_i be the valuation associated to $\mathfrak{P}_i$, then we can consider the map

$$\begin{aligned} \mathrm{ord}_L \colon L^\times &\longrightarrow \mathbb{Z}^s \\ x &\longmapsto (\mathrm{ord}_1(x), ..., \mathrm{ord}_s(x)) . \end{aligned}$$

It is clear that $C' = P' \cap \ker(\mathrm{ord}_L)$ and hence we obtain

$$[P'/C' : Q'/\Delta'] = [\mathrm{ord}_L(P') : \mathrm{ord}_L(Q')] .$$

For this index we compute for $1 \leq i \leq s$ and $1 \leq e \leq e_i$

$$\begin{aligned} \mathrm{ord}_i(\varphi_{L,\mathfrak{p}_i^e}) &= \mathrm{ord}_i(N_{H_{\mathfrak{p}_i^e}/L_{\mathfrak{p}_i^e}}(\alpha_{\mathfrak{p}_i^e})^h) \\ &= h \cdot t(L/L_{\mathfrak{p}_i^e}) \cdot \widetilde{\mathrm{ord}}_i(N_{H_{\mathfrak{p}_i^e}/L_{\mathfrak{p}_i^e}}(\alpha_{\mathfrak{p}_i^e})) , \end{aligned}$$

where $t(L/L_{\mathfrak{p}_i^e})$ denotes the ramification index of $\mathfrak{p}_i' := \mathfrak{P}_i \cap L_{\mathfrak{p}_i^e}$ in $L/L_{\mathfrak{p}_i^e}$ and $\widetilde{\mathrm{ord}}_i$ is the valuation associated to $\mathfrak{p}_i'$. Recall that

$$\alpha_{\mathfrak{p}_i^e} \mathcal{O}_{H_{\mathfrak{p}_i^e}} = (\mathfrak{p}_i)_{H_\mathfrak{m}}^{w_\infty/w_K} = \prod_{\mathfrak{q} \mid \mathfrak{p}_i} \mathfrak{q}^{w_\infty/w_K} ,$$

so we obtain

$$\widetilde{\mathrm{ord}}_i(N_{H_{\mathfrak{p}_i^e}/L_{\mathfrak{p}_i^e}}(\alpha_{\mathfrak{p}_i^e})) = \frac{w_\infty}{w_K} \left| \left\{ \mathfrak{q} \subseteq \mathcal{O}_{H_{\mathfrak{p}_i^e}} \mid \mathfrak{q} \text{ prime}, \mathfrak{q} \mid \mathfrak{p}_i' \right\} \right| \cdot f(H_{\mathfrak{p}_i^e}/F_{\mathfrak{p}_i^e}) = \frac{w_\infty}{w_K} \cdot [H : L_{(1)}] ,$$

where $f(H_{\mathfrak{p}_i^e}/L_{\mathfrak{p}_i^e})$ is the inertia degree of $\mathfrak{p}_i'$ in $H_{\mathfrak{p}_i^e}$, and hence

$$\mathrm{ord}_i(\varphi_{L,\mathfrak{p}_i^e}) = \frac{w_\infty}{w_K} h t(L/L_{\mathfrak{p}_i^e})[H : L_{(1)}] .$$

This gets clearly minimal for $e = e_i$ hence we obtain

$$\operatorname{ord}_L(P') = \bigoplus_{i=1}^{s} \left(\frac{w_L w_\infty}{w_K} h \cdot t(L/L_{\mathfrak{p}_i^{e_i}})[H : L_{(1)}]\mathbb{Z} \right) .$$

On the other hand we find

$$\operatorname{ord}_i \left(x_{\mathfrak{p}_i}^{[H:L_{(1)}]w_\infty/w_K} \right) = \frac{w_\infty}{w_K}[H : L_{(1)}] \operatorname{ord}_i(x_{\mathfrak{p}_i}) .$$

Since $x_{\mathfrak{p}_i}$ is a generator of $\mathfrak{p}_i^h$, we obtain

$$\operatorname{ord}_i(x_{\mathfrak{p}_i}) = h \cdot |I_{\mathfrak{p}_i}|$$

and hence

$$\operatorname{ord}_L(Q') = \bigoplus_{i=1}^{s} (\frac{w_L w_\infty}{w_K} h \, |I_{\mathfrak{p}_i}| \, [H : L_{(1)}]\mathbb{Z}) .$$

Putting these results together, we find

$$[\operatorname{ord}_L(P') : \operatorname{ord}_L(Q')] = \prod_{i=1}^{s} \frac{|I_{\mathfrak{p}_i}|}{t(L/L_{\mathfrak{p}_i^{e_i}})} .$$

With $[L_{\mathfrak{p}_i^{e_i}} : L_{(1)}] = \frac{|I_{\mathfrak{p}_i}|}{t(L/L_{\mathfrak{p}_i^{e_i}})}$, we obtain the desired result. □

Now we can state the index formula analogously to [Ouk03, Thm. 1]:

Theorem 3.3.9. *Set $d(L) := [P_L^{w_L} \cap K : Q_L^{w_L} \cap K]$. Then we get*

$$[\mathcal{O}_L^\times : C_L] = \frac{(hw_\infty)^{[L:K]-1} w_K h_L}{w_L h} \frac{\prod_{\mathfrak{p}} [L \cap H_{\mathfrak{p}^\infty} : L_{(1)}]}{[L : L_{(1)}]} \frac{[\mathbb{Z}[G] : U']}{d(L)} .$$

Proof. Let $R = \mathbb{Z}[G]$ and let R_0 be the kernel of multiplication by NG in R. Since $\ker(l_L) \cap \mathcal{O}_L^\times = \mu(L)$ by Lemma 3.3.8 (i), we get

$$\begin{aligned} [\mathcal{O}_L^\times : C_L] &= [l_L(\mathcal{O}_L^\times) : l_L(C_L)] = [l_L(\mathcal{O}_L^\times) : R_0][R_0 : l_L(C_L)] \\ &= \frac{[R_0 : U_0']}{[R_0 : l_L(\mathcal{O}_L^\times)]}[U_0' : l_L(C_L)] \\ &= \frac{[R_0 : U_0']}{[R_0 : l_L(\mathcal{O}_L^\times)]}[U_0' : l_L^*(P_L)][l_L^*(P_L) : l_L(C_L)] . \end{aligned}$$

Note that all the indices above are defined since each of the $\mathbb{Z}$-modules has the same rank. By definition of Sinnott's index, one can easily show that

$$[R_0 : l_L(\mathcal{O}_L^\times)] = |\det(A)| ,$$

where A is the matrix with entries

$$(\operatorname{ord}_w(u_i))_{\substack{w \in S_\infty(L)\setminus\{w_0\} \\ i \in \{1,\dots,[L:K]-1\}}} ,$$

where w_0 is an arbitrary place in $S_\infty(L)$ and the units $u_1, ..., u_{[L:K]-1} \in \mathcal{O}_L^\times$ project to a basis of $\mathcal{O}_L^\times/\mu(L)$. By the definition of the regulator, we hence get

$$R_L = |\det(-A)| = |\det(A)| \ ,$$

so $[R_0 : l_L(\mathcal{O}_L^\times)] = R_L$. Moreover, the identity

$$[R : U'] = [NG \cdot R : NG \cdot U'][R_0 : U_0']$$

holds. It is clear that $NG \cdot R = NG \cdot \mathbb{Z}$ and for computing $NG \cdot U'$ we just have to consider

$$NG \cdot \rho'_{(1)} = NG \cdot N\,\mathrm{Gal}(L/L_{(1)}) = \left|\mathrm{Gal}(L/L_{(1)})\right| \cdot NG\,.$$

Therefore, $NG \cdot U' = \left|\mathrm{Gal}(L/L_{(1)})\right| \cdot NG \cdot \mathbb{Z}$ and together we get

$$[NG \cdot R : NG \cdot U'] = \left|\mathrm{Gal}(L/L_{(1)})\right| = [L : L_{(1)}]$$

and hence

$$[R_0 : U_0'] = \frac{[R : U']}{[L : L_{(1)}]}\,.$$

Using these computations and the results of the Propositions 3.3.5 and 3.3.7 we obtain

$$[\mathcal{O}_L^\times : C_L] = \frac{(hw_\infty)^{[L:K]-1} w_K h_L}{w_L h} \frac{\prod_{\mathfrak{p}} [L \cap H_{\mathfrak{p}^\infty} : L_{(1)}]}{[L : L_{(1)}]} \frac{[R : U']}{d(L)}\,. \qquad \square$$

We state some results on $[R : U']$ similar to [Ouk03, §6, §7]:

Proposition 3.3.10. *(i) The index $[R : U']$ is an integer divisible only by primes dividing $[L : L_{(1)}]$. Moreover, if $\mathrm{Gal}(L/L_{(1)})$ is the direct product of its inertia groups or if at most two primes ramify in L/K, then $[R : U'] = 1$.*

(ii) If G is cyclic, then $[R : U'] = 1$.

(iii) If $L = H_{\mathfrak{m}}$ for some integral ideal $\mathfrak{m} = \prod_{i=1}^s \mathfrak{p}_i^{e_i}$ for some $s \geq 3$ and $(h, w_K) = 1$, we get

$$[R : U'] = w_K^{e(2^{s-2}-1)}\,,$$

where e is the index of the subgroup generated by the classes of $\mathfrak{p}_i$ in $\mathrm{cl}(K)$.

Proof. (i) This is [Ouk03, Prop. 16].

(ii) This is [Sin80, Thm. 5.3].

(iii) This is [Ouk03, Prop. 18].

Note that the arguments are based only on the group structure of G and hence can also be applied in the case of function fields. $\square$

Remark 3.3.11. (i) In [Ouk92] H. Oukhaba defined a group $\mathcal{E}_L$ of elliptic units in an unramified extension L/K. He also showed that the elements of $\mathcal{E}_L^{w_K w_\infty h}$ are of the form

$$\prod_{\tau \in G} \left(\frac{\partial_L(1)\partial_L(\tau\sigma^{-1})}{\partial_L(\sigma^{-1})\partial_L(\tau)} \right)^{w_K m_\tau}$$

for $\sigma \in G$ and certain rational numbers $m_\tau \in \mathbb{Q}$ (cf. Prop. 3.6 in loc. cit.). He also derived an index formula in this case:

$$[\mathcal{O}_L^\times : \mathcal{E}_L] = \frac{h_L}{[H:L]}\,.$$

In this case, our index formula yields

$$[\mathcal{O}_L^\times : C_L] = (hw_\infty)^{[L:K]-1} \frac{w_K h_L}{w_L h}\,.$$

From the above description we find that $\mathcal{E}_L^{w_\infty h} \subseteq C_L$ and we get

$$[C_L : \mathcal{E}_L^{w_\infty h}] = h \frac{w_L}{w_K}\,.$$

(ii) In [Yin97] L. Yin defined a group $\overline{C}$ of extended cyclotomic units in the ray class fields $K_\mathfrak{m}$. The ramified elliptic units in this article are in fact norms of Yin's cyclotomic units. However our construction of the unramified units is quite different to the one in [Yin97]. Nevertheless, Yin also computed an index formula

$$[\mathcal{O}_{H_\mathfrak{m}}^\times : (\overline{C} \cap \mathcal{O}_{H_\mathfrak{m}}^\times)] = w_K^a h_{H_\mathfrak{m}}\,,$$

where $a = 0$ if $s \leq 2$ and $a = e(2^{s-2}-1) - (s-2)$ if $s \geq 3$. Note that there is the additional assumption $(h, w_K) = 1$ in the case $s \geq 3$. With these assumptions, we get from our index formula

$$[\mathcal{O}_{H_\mathfrak{m}}^\times : C_{H_\mathfrak{m}}] = (hw_\infty)^{[H_\mathfrak{m}:K]-1} \frac{w_K h_{H_\mathfrak{m}}}{w_\infty h} w_K^{-(s-1)} [R : U']\,.$$

With Proposition 3.3.10, this yields

$$[\mathcal{O}_{H_\mathfrak{m}}^\times : C_{H_\mathfrak{m}}] = (hw_\infty)^{[H_\mathfrak{m}:K]-2} w_K^a h_{H_\mathfrak{m}}\,.$$

3.3.3 The index $d(L)$

To conclude this section, we want to analyze the index $d(L)$ in some detail. We obtain $d(L) = 1$ in essentially the same cases as listed in [Ouk03, Remark 2] for imaginary quadratic base fields. First we see that if $L \subseteq H$, then there are no ramified elliptic units and hence $P_L = Q_L = C_L$, so $d(L) = 1$. Hence we can assume $\mathfrak{m} \neq (1)$ for the rest of this section.

Lemma 3.3.12. *The quotient* $(P_L^{w_L} \cap K)/(Q_L^{w_L} \cap K)$ *is annihilated by*

(i) $[H : L_{(1)}]$.

(ii) the least common multiple of $[L_{\mathfrak{p}_i^{e_i}} : L_{(1)}]$ *for* $i = 1, ..., s$.

The proof of part (i) is similar to the one of [Ouk03, Lemma 2] and needs the following analogue of [Ouk03, Lemma 1]:

Lemma 3.3.13. *Let* $x \in P_L$. *Then there exists* $\alpha \in K$, *an abelian extension* M/K *and* $y \in M$ *such that*

(i) $x^{w_L} = \alpha^{w_L w_\infty / w_K} y^f$, *where* $f = h w_L w_\infty$,

(ii) The valuation of α *at every prime ideal of* $\mathcal{O}_K$ *is divisible by* h.

Proof. It suffices to check the claim for the generators of P_L. If $x \in \mu(L)$, $x^{w_L} = 1$ and hence we can choose $\alpha = y = 1$.

Let $x = \varphi_{L,\mathfrak{n}}$ for some $\mathfrak{n} \mid \mathfrak{m}$, $\mathfrak{n} \neq (1)$. Then by definition, we get

$$x^{w_L} = N_{H_\mathfrak{n}/L_\mathfrak{n}}(\lambda_\mathfrak{n}^{w_\infty})^{h w_L} = \left(\prod_{\tau \in \mathrm{Gal}(H_\mathfrak{n}/L_\mathfrak{n})} \widehat{\tau}(\lambda_\mathfrak{n}) \right)^f ,$$

where $\widehat{\tau}$ is any lift of τ to $\mathrm{Gal}(K_\mathfrak{n}/L_\mathfrak{n})$. Setting $\alpha := 1$ and

$$y := \prod_{\tau \in \mathrm{Gal}(H_\mathfrak{n}/L_\mathfrak{n})} \widehat{\tau}(\lambda_\mathfrak{n}) \in K_\mathfrak{n} ,$$

we obtain the desired properties.

Now let $x = \frac{\partial_L(1)}{\partial_L(\sigma)}$ for some $\sigma \in \mathrm{Gal}(L_{(1)}/K)$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ such that $(\mathfrak{p}, L_{(1)}/K) = \sigma^{-1}$. Let β be a generator of $\mathfrak{p}^h$. Then by the norm relation 3.2.9 we get

$$\begin{aligned} x^{w_L} &= \beta^{-[H:L_{(1)}] w_L w_\infty / w_K} N_{L_\mathfrak{p}/L_{(1)}}(\varphi_{L,\mathfrak{p}})^{w_L} \\ &= \beta^{-[H:L_{(1)}] w_L w_\infty / w_K} N_{H_\mathfrak{p}/L_{(1)}}(\lambda_\mathfrak{p}^{w_\infty})^{h w_L} \\ &= \beta^{-[H:L_{(1)}] w_L w_\infty / w_K} \left(\prod_{\tau \in \mathrm{Gal}(H_\mathfrak{p}/L_{(1)})} \widehat{\tau}(\lambda_\mathfrak{p}) \right)^f , \end{aligned}$$

where $\widehat{\tau}$ is any lift of τ to $\mathrm{Gal}(K_\mathfrak{p}/L_{(1)})$. Hence we obtain the desired result by setting $\alpha := \beta^{-[H:L_{(1)}]}$ and

$$y := \prod_{\tau \in \mathrm{Gal}(H_\mathfrak{p}/L_{(1)})} \widehat{\tau}(\lambda_\mathfrak{p}) \in K_\mathfrak{p} .$$ □

Proof of Lemma 3.3.12. (i) Let $\mathcal{R}$ be the subgroup of $K^\times$ generated by $x_{\mathfrak{p}_i}^{w_L w_\infty / w_K}$ for $i = 1, ..., s$. Since Q_L is generated by $\mu(L), \Delta_L$ and the $x_{\mathfrak{p}_i}^{[H:L_{(1)}] w_\infty / w_K}$, we obtain that $Q_L^{w_L}$ is generated by $\Delta_L^{w_L}$ and the $x_{\mathfrak{p}_i}^{[H:L_{(1)}] w_L w_\infty / w_K}$. Since

$$\Delta_L^{w_L} \cap K = \Delta_L^{w_L} \cap \mathcal{O}_K = \Delta_L^{w_L} \cap \mu(K) = 1 ,$$

we finally obtain that

$$Q_L^{w_L} \cap K = \mathcal{R}^{[H:L_{(1)}]} \,.$$

Now we are left to show $P_L^{w_L} \cap K \subseteq \mathcal{R}$. For this purpose let $x \in P_L$ be such that $x^{w_L} \in P_L^{w_L} \cap K$. By Lemma 3.3.13, we obtain elements $\alpha \in K$ and $y \in M$ such that $x^{w_L} = \alpha^{w_L w_\infty / w_K} y^f$. Since $x^{w_L} \in K$, we find that $y^f \in K$. Since $K(y) \subseteq M$ is abelian over K, we can apply [Sta80, Lemma 6] to obtain an element $z \in K$ such that $y^{f w_K} = z^f$ (note that $w_K \mid f$). Therefore, we get that $y^f = \zeta \cdot z^{f/w_K}$ for some $\zeta \in \mu(K)$, so

$$x^{w_L} = \zeta \cdot (\alpha z^h)^{w_L w_\infty / w_K} \,.$$

Therefore, $\zeta \in L^{w_L} \cap \mu(K) = 1$. Since x is a unit outside $\mathfrak{p}_1, ..., \mathfrak{p}_s$, so is αz^h. Since each valuation of α is a multiple of h by part (ii) of Lemma 3.3.13, we get

$$\alpha z^h \mathcal{O}_K = \mathfrak{p}_1^{h r_1} \cdots \mathfrak{p}_s^{h r_s} = \left(\prod_{i=1}^{s} x_{\mathfrak{p}_i}^{r_i} \right) \mathcal{O}_K$$

for some $r_i \in \mathbb{N}$. Hence,

$$x^{w_L} = \zeta \cdot \left(\prod_{i=1}^{s} x_{\mathfrak{p}_i}^{r_i} \right)^{w_L w_\infty / w_K} ,$$

where ζ is again an element of $L^{w_L} \cap \mu(K) = 1$. Therefore, $x^{w_L} \in \mathcal{R}$.

(ii) Let $x \in P_L$ be such that $x^{w_L} \in P_L^{w_L} \cap K$. By the definition of P_L, x can be written as

$$x = u \cdot \prod_{i=1}^{s} \varphi_{L, \mathfrak{p}_i^{e_i}}^{\lambda_i} ,$$

where $u \in \mathcal{O}_L^\times$ and $\lambda_i \in \mathbb{Z}[G]$ (note that the elliptic numbers $\varphi_{L,\mathfrak{p}_i^e}$ for $1 < e < e_i$ can be written as a norm of $\varphi_{L,\mathfrak{p}_i^{e_i}}$). Now we define $\mathrm{ord}_{i,K}$ to be the valuation associated to $\mathfrak{p}_i$. Remember that ord_i is the valuation of a fixed prime ideal $\mathfrak{P}_i$ of L over $\mathfrak{p}_i$. Then we obtain

$$\mathrm{ord}_{i,K}(x^{w_L}) = \frac{1}{|I_{\mathfrak{p}_i}|} \mathrm{ord}_i(x^{w_L}) = \frac{w_L}{|I_{\mathfrak{p}_i}|} \mathrm{ord}_i(\varphi_{L,\mathfrak{p}_i^{e_i}}^{\lambda_i}) \,.$$

Using the valuation computed in the proof of Proposition 3.3.7 and defining $\mu_i \in \mathbb{Z}$ to be the sum over the coefficients of λ_i (i.e. μ_i is λ_i evaluated by the trivial character), we get

$$\mathrm{ord}_{i,K}(x^{w_L}) = \frac{\mu_i t(L/L_{\mathfrak{p}_i^{e_i}})}{|I_{\mathfrak{p}_i}|} \cdot \frac{w_\infty}{w_K} w_L h [H : L_{(1)}] \in \mathbb{Z} \,.$$

Let g be the least common multiple of the $[L_{\mathfrak{p}_i^{e_i}} : L_{(1)}]$ for $i = 1, ..., s$. Since $[L_{\mathfrak{p}_i^{e_i}} : L_{(1)}] = \frac{|I_{\mathfrak{p}_i}|}{t(L/L_{\mathfrak{p}_i^{e_i}})}$, we get that

$$\mathrm{ord}_{i,K}(x^{w_L g}) \in \frac{w_\infty}{w_K} w_L h [H : L_{(1)}] \mathbb{Z} \,.$$

But we know that the ideal $\mathfrak{p}_i^{w_\infty/w_K\cdot w_L h[H:L_{(1)}]}$ is generated by $x_{\mathfrak{p}_i}^{w_\infty/w_K\cdot w_L[H:L_{(1)}]}$ which is an element of $Q_L^{w_L}\cap K$. Since x is a unit outside of $\mathfrak{p}_1,...,\mathfrak{p}_s$, we find

$$x^{w_L g}\mathcal{O}_K = \prod_{i=1}^{s}\mathfrak{p}_i^{r_i\cdot w_\infty/w_K\cdot w_L h[H:L_{(1)}]} = \left(\prod_{i=1}^{s} x_{\mathfrak{p}_i}^{r_i\cdot w_\infty/w_K\cdot w_L[H:L_{(1)}]}\right)\mathcal{O}_K$$

for some $r_i\in\mathbb{Z}$ and hence $x^{w_L g}\in Q_L^{w_L}\cap K$. □

With the results above, we deduce

Proposition 3.3.14. *If one of the following conditions holds, then $d(L)=1$:*

(i) $L\subseteq H$,

(ii) $H\subseteq L$,

(iii) $[H:L_{(1)}]$ *and* $[L:L_{(1)}]$ *are coprime.*

Proof. (i) This was already noted in the beginning of this section.

(ii) This is Lemma 3.3.12 (i), since $[H:L_{(1)}]=1$ in this case.

(iii) Since $[L_{\mathfrak{p}_i^{e_i}}:L_{(1)}]\mid[L:L_{(1)}]$, the combination of Lemma 3.3.12 (i) and 3.3.12 (ii) proves this case. □

In order to obtain more results on the index $d(L)$, we establish a connection to distribution theory. This approach was already used in [Ouk03] for imaginary quadratic base fields.

For this purpose, we set $D:=P_L^{w_L}/(Q_L^{w_L}\cap K)$. The $\mathbb{Z}$-rank of $P_L^{w_L}$ is $[L:K]-1+s$. Moreover, we have seen in the proof of Lemma 3.3.12 that $Q_L^{w_L}\cap K$ is generated by $x_{\mathfrak{p}_i}^{[H:L_{(1)}]w_L w_\infty/w_K}$, hence the $\mathbb{Z}$-rank of $Q_L^{w_L}\cap K$ is s and D has $\mathbb{Z}$-rank $[L:K]-1$. By the construction of Q_L, it is also clear that $NG\cdot D=0$, so $(P_L^{w_L}\cap K)/(Q_L^{w_L}\cap K)=D^G$. Let

$$\Sigma=\bigoplus_{\mathfrak{n}\mid\mathfrak{m}}\mathbb{Z}[\mathrm{Gal}(L_\mathfrak{n}/K)]$$

and let $S\subseteq\Sigma$ be the submodule generated by the following relations: For $\mathfrak{n}\mid\mathfrak{m}$ and a prime $\mathfrak{q}$ such that $\mathfrak{n}':=\mathfrak{n}\mathfrak{q}\mid\mathfrak{m}$ take

$$\begin{aligned}
&N\,\mathrm{Gal}(L_{\mathfrak{n}'}/L_\mathfrak{n})-1_{\mathrm{Gal}(L_\mathfrak{n}/K)} && \text{if } \mathfrak{q}\mid\mathfrak{n}\,,\\
&N\,\mathrm{Gal}(L_{\mathfrak{n}'}/L_\mathfrak{n})-(1_{\mathrm{Gal}(L_\mathfrak{n}/K)}-(\mathfrak{q},L_\mathfrak{n}/K)^{-1}) && \text{if } \mathfrak{q}\nmid\mathfrak{n}\,,
\end{aligned}$$

where $1_{\mathrm{Gal}(L_\mathfrak{n}/K)}$ denotes the element 1 in the component $\mathbb{Z}[\mathrm{Gal}(L_\mathfrak{n}/K)]$.

Now let $\mathcal{T}$ be the set of all ideals $\mathfrak{n}\mid\mathfrak{m}$ such that $\mathfrak{n}=\prod_{i=1}^{s}\mathfrak{p}_i^{e_i r_i}$ with $r_i\in\{0,1\}$. For any $\mathfrak{n}\in\mathcal{T}$ define $S(\mathfrak{n})$ to be the ideal of $\mathbb{Z}[\mathrm{Gal}(L_\mathfrak{n}/K)]$ generated by the elements $NI_{\mathfrak{p}_i}(\mathfrak{n})$ for $\mathfrak{p}_i\mid\mathfrak{n}$, where $I_{\mathfrak{p}_i}(\mathfrak{n})$ is the inertia subgroup of $\mathfrak{p}_i$ in $\mathrm{Gal}(L_\mathfrak{n}/K)$. Let $z_\mathfrak{n}$ be the exponent of the torsion subgroup of $\mathbb{Z}[\mathrm{Gal}(L_\mathfrak{n}/K)]/S(\mathfrak{n})$. Then we obtain the next

Theorem 3.3.15. *We have*

$$\mathrm{rk}_{\mathbb{Z}}(\Sigma/S) = [L : K]\,.$$

Moreover, the torsion subgroup $\mathrm{Tor}(\Sigma/S)$ *of* Σ/S *is finite and annihilated by* $\prod_{\mathfrak{n}\in\mathcal{T}} z_{\mathfrak{n}}$.

Proof. One can use the proof of [BO01, Thm. 3.1]. Note that we do not work with ray class fields here, but using $L_{\mathfrak{n}}$ instead of $K_{\mathfrak{n}}$ and then defining the same objects will give the same result for our case. □

Proposition 3.3.16. *If* Σ/S *is* $\mathbb{Z}$*-torsion free, then* $d(L) = 1$.

Proof. First, we claim that we obtain a surjective map $f\colon \Sigma/S \longrightarrow D$. Indeed, we can define $f'\colon \Sigma \longrightarrow D$ by sending $\sigma \in \mathrm{Gal}(L_{\mathfrak{n}}/K)$ to the class of $\varphi_{L,\mathfrak{n}}^{w_L\sigma}$ if $\mathfrak{n} \neq (1)$ and to the class of $\left(\frac{\partial_L(\sigma^{-1})}{\partial_L(1)}\right)^{w_L}$ if $\mathfrak{n} = (1)$. This map is clearly surjective and by the norm relations in Proposition 3.2.9, we obtain that $S \subseteq \ker(f')$. Hence, we obtain a surjective map $f\colon \Sigma/S \longrightarrow D$.

On the other hand, we can define a map $g'\colon \Sigma \longrightarrow U'$ by sending $\sigma \in \mathrm{Gal}(L_{\mathfrak{n}}/K)$ to $\widetilde{\sigma}\rho'_{\mathfrak{n}}$, where $\widetilde{\sigma}$ is any lift of σ to $\mathrm{Gal}(L/K)$. This map is again surjective and $S \subseteq \ker(g')$, hence we obtain a surjective map $g\colon \Sigma/S \longrightarrow U'$.

Since g is surjective and we have $\mathrm{rk}_{\mathbb{Z}}(U') = [L : K] = \mathrm{rk}_{\mathbb{Z}}(\Sigma/S)$, we obtain that $\ker(g) \subseteq \mathrm{Tor}(\Sigma/S)$. Whenever Σ/S is $\mathbb{Z}$-torsion free, we hence obtain that g is an isomorphism. If this is true, we can define $\varphi\colon U' \longrightarrow D$ by $\varphi = f \circ g^{-1}$. This is clearly a surjective map and since $\varphi(NG \cdot u) = NG \cdot \varphi(u) = 0$, we get that $NG \cdot U' \subseteq \ker(\varphi)$. Since U'_0, U' and $NG \cdot U'$ are torsion-free, we get $U'_0 \cong U'/NG \cdot U'$ as $\mathbb{Z}$-modules and therefore we obtain a surjective map $U'_0 \twoheadrightarrow D$. Since U'_0 has $\mathbb{Z}$-rank $[L : K] - 1$ and is $\mathbb{Z}$-torsion-free, we obtain $U'_0 \cong D$. Finally, since $(U'_0)^G = \{0\}$, we get that $D^G = \{1\}$ and hence $d(L) = 1$. □

Proposition 3.3.17. *If one of the following conditions holds,* Σ/S *is* $\mathbb{Z}$*-torsion free and hence* $d(L) = 1$*:*

(i) $\mathrm{Gal}(L/L_{(1)})$ *is the direct product of its inertia subgroups.*

(ii) $s \in \{0, 1, 2\}$.

(iii) $\mathrm{Gal}(L/L_{(1)})$ *is cyclic.*

Proof. (i) Here we can use the proof of [BO01, Prop. 3.5], modified to our case by replacing $K_{\mathfrak{n}}$ by $L_{\mathfrak{n}}$. Then the claim is simply [BO01, Cor. 3.8].

(ii) The case $s = 0$ is already covered by Proposition 3.3.14.

For $s = 1$, we have $\mathfrak{m} = \mathfrak{p}^e$ and hence $\mathrm{Gal}(L/L_{(1)}) = I_{\mathfrak{p}}$. Therefore, this case follows from part (i).

For $s = 2$, we have $\mathfrak{m} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}$. We clearly get that $L_{\mathfrak{p}_i^{e_i}}/L_{(1)}$ is totally ramified at each prime above $\mathfrak{p}_i$ and unramified everywhere else, so $L_{\mathfrak{p}_1^{e_1}} \cap L_{\mathfrak{p}_2^{e_2}} = L_{(1)}$. Comparing the ramification indices and the degrees of the extensions shows that $L = L_{\mathfrak{p}_1^{e_1}} L_{\mathfrak{p}_2^{e_2}}$ and we get $I_{\mathfrak{p}_1} \cap I_{\mathfrak{p}_2} = \{1\}$ and $I_{\mathfrak{p}_1} \times I_{\mathfrak{p}_2} \cong \mathrm{Gal}(L/L_{(1)})$, so the claim follows again from part (i).

(iii) Let $\ell \in \mathbb{Z}$ be a prime number, then we will show that $\ell \nmid z_{\mathfrak{n}}$ for each $\mathfrak{n} \in \mathcal{T}$ with the same method as in the proof of [BO01, Prop. 3.5]. For this purpose let $I_{\mathfrak{p}}(\mathfrak{n})$ be the inertia group of $\mathfrak{p}$ in $\mathrm{Gal}(L_{\mathfrak{n}}/L_{(1)})$ and let $\tilde{S}(\mathfrak{n})$ be the ideal of $\mathbb{Z}[\mathrm{Gal}(L_{\mathfrak{n}}/L_{(1)})]$ generated by $NI_{\mathfrak{p}}(\mathfrak{n})$ for $\mathfrak{p} \mid \mathfrak{n}$. We decompose

$$\mathbb{Z}[\mathrm{Gal}(L_{\mathfrak{n}}/K)]/S(\mathfrak{n}) \cong \bigoplus_{\tau \in \mathrm{Gal}(L_{(1)}/K)} \mathbb{Z}[\mathrm{Gal}(L_{\mathfrak{n}}/L_{(1)})]/\tilde{S}(\mathfrak{n})\widetilde{\tau}\,,$$

where $\widetilde{\tau}$ is a lift of τ to $\mathrm{Gal}(L_{\mathfrak{n}}/K)$. So we have to show that $\mathbb{Z}[\mathrm{Gal}(L_{\mathfrak{n}}/L_{(1)})]/\tilde{S}(\mathfrak{n})$ has no ℓ-torsion, or equivalently that

$$\mathbb{Z}_\ell \otimes \mathbb{Z}[\mathrm{Gal}(L_{\mathfrak{n}}/L_{(1)})]/\tilde{S}(\mathfrak{n}) = \mathbb{Z}_\ell[\mathrm{Gal}(L_{\mathfrak{n}}/L_{(1)})]/\tilde{S}(\mathfrak{n})$$

is $\mathbb{Z}_\ell$-torsion-free (by abuse of notation we denote the ideal $\tilde{S}(\mathfrak{n})\mathbb{Z}_\ell[\mathrm{Gal}(L_{\mathfrak{n}}/L_{(1)})]$ also by $\tilde{S}(\mathfrak{n})$).

Now let $\mathrm{Gal}(L_{\mathfrak{n}}/L_{(1)}) = G' \times G_\ell(\mathfrak{n})$, where $G_\ell(\mathfrak{n})$ is the ℓ-Sylow subgroup of $\mathrm{Gal}(L_{\mathfrak{n}}/L_{(1)})$ and $\ell \nmid |G'|$. Similarly to the arguments in [BO01], we obtain a decomposition by the irreducible characters of G' and hence we have to show that

$$A_\chi[G_\ell(\mathfrak{n})]/\tilde{S}(\mathfrak{n})A_\chi[G_\ell(\mathfrak{n})]$$

has no $\mathbb{Z}_\ell$-torsion, where $A_\chi = e_\chi \mathbb{Z}_\ell[G']$. If we decompose $I_{\mathfrak{p}}(\mathfrak{n}) = I'_{\mathfrak{p}}(\mathfrak{n}) \times I_{\mathfrak{p},\ell}(\mathfrak{n})$ into its ℓ-Sylow subgroup $I_{\mathfrak{p},\ell}(\mathfrak{n})$ and its prime-to-ℓ-part $I'_{\mathfrak{p}}(\mathfrak{n})$, we find that

$$e_\chi \cdot NI_{\mathfrak{p}}(\mathfrak{n}) = \begin{cases} e_\chi \cdot NI_{\mathfrak{p},\ell}(\mathfrak{n}), & \chi(I'_{\mathfrak{p}}(\mathfrak{n})) = 1, \\ 0, & \chi(I'_{\mathfrak{p}}(\mathfrak{n})) \neq 1. \end{cases}$$

Hence, the ideal $\tilde{S}(\mathfrak{n})A_\chi[G_\ell(\mathfrak{n})]$ is generated by $e_\chi \cdot NI_{\mathfrak{p},\ell}(\mathfrak{n})$ for all $\mathfrak{p} \mid \mathfrak{n}$ such that $\chi(I'_{\mathfrak{p}}(\mathfrak{n})) = 1$. Since $\mathrm{Gal}(L/L_{(1)})$ is cyclic, so are $G_\ell(\mathfrak{n})$ and each $I_{\mathfrak{p},\ell}(\mathfrak{n})$. Hence, the $I_{\mathfrak{p},\ell}(\mathfrak{n})$ are totally ordered by inclusion and we can find a prime $\mathfrak{q}$ such that $I_{\mathfrak{q},\ell}(\mathfrak{n}) \subseteq I_{\mathfrak{p},\ell}(\mathfrak{n})$ for all other primes $\mathfrak{p} \mid \mathfrak{n}$ with $\chi(I'_{\mathfrak{p}}(\mathfrak{n})) = 1$. Therefore,

$$\tilde{S}(\mathfrak{n})A_\chi[G_\ell(\mathfrak{n})] = (e_\chi \cdot NI_{\mathfrak{q},\ell}(\mathfrak{n}))\,.$$

The $\mathbb{Z}_\ell$-module

$$A_\chi[G_\ell(\mathfrak{n})]/(e_\chi \cdot NI_{\mathfrak{q},\ell}(\mathfrak{n}))$$

is free, so it is $\mathbb{Z}_\ell$-torsion free and therefore $\ell \nmid z_{\mathfrak{n}}$. Since this is true for each prime ℓ and each $\mathfrak{n} \in \mathcal{T}$, we find that Σ/S is $\mathbb{Z}$-torsion-free and hence $d(L) = 1$. $\square$

3.4 A non-trivial root of an elliptic unit

With this definition of elliptic units we can prove an analogue of the main result of [CK19] in the case of global function fields. In the first step towards this annihilation result, we will take certain roots of our elliptic units.

3.4.1 Preliminaries

We use the notation from the previous sections with the following additional assumptions:

- Suppose p is an odd prime such that $p \nmid q \cdot (q-1) \cdot h$.
- L is a real cyclic extension of K of degree p^k for some positive integer k.
- We change the notation to $\Gamma := \mathrm{Gal}(L/K)$. Let σ be a generator of Γ.

Remark 3.4.1. Note that the assumption on L and $p \nmid h$ are exactly the same as in [CK19]. The assumption $p \nmid (q-1) = w_K$ is also implied by the hypotheses stated there. The only new assumption is $p \nmid q$, i.e. we suppose that p is prime to the characteristic of K, which is a natural hypothesis when dealing with function fields.

Note that since $p \nmid h$, we have

$$L \cap H = K$$

and we assume that there are exactly $s \geq 2$ primes $\mathfrak{p}_1, ..., \mathfrak{p}_s$ of K which ramify in L. We introduce the additional notation:

- $I := \{1, ..., s\}$,
- $x_j := x_{\mathfrak{p}_j}$ is a generator of $\mathfrak{p}_j^h$,
- $\mathfrak{P}_j$ is a fixed prime ideal of L over $\mathfrak{p}_j$,
- For any abelian extension M/K let $D_j(M) := D_{\mathfrak{p}_j} \subseteq \mathrm{Gal}(M/K)$ be the decomposition group of $\mathfrak{p}_j$ and $I_j(M) := I_{\mathfrak{p}_j} \subseteq D_j(M)$ be the inertia group of $\mathfrak{p}_j$,
- $t_j := |I_j(L)|$ is the ramification index of $\mathfrak{P}_j$ over $\mathfrak{p}_j$,
- $n_j := [G : D_j(L)]$.

Then it follows that $t_j n_j \mid p^k$ and

$$\mathfrak{p}_j \mathcal{O}_L = \prod_{i=0}^{n_j-1} \mathfrak{P}_j^{t_j \sigma^i}.$$

Since $p \nmid q$, this implies that the extension L/K is tamely ramified and hence its conductor is square-free. Therefore the conductor is given by $\mathfrak{m}_I := \mathfrak{m} = \prod_{j \in I} \mathfrak{p}_j$.

3.4.2 The distinguished subfields F_j

For any subset $\emptyset \neq J \subseteq I$ we set $\mathfrak{m}_J := \prod_{j\in J} \mathfrak{p}_j$. With our previous observation we find that $L \subseteq H_{\mathfrak{m}_I}$.

Lemma 3.4.2. $L \subseteq \prod_{j\in I} H_{\mathfrak{p}_j}$.

Proof. By class field theory, we have a canonical isomorphism (see e.g. [Hay85, Eq. (3.1)])

$$\mathrm{Gal}(H_{\mathfrak{m}}/H) \cong (\mathcal{O}_K/\mathfrak{m})^\times / \operatorname{im}(\mu(K)).$$

With the Chinese Remainder Theorem, we get

$$\begin{aligned}[H_{\mathfrak{m}} : \prod_{j\in I} H_{\mathfrak{p}_j}] &= \frac{[H_{\mathfrak{m}} : H]}{[\prod_{j\in I} H_{\mathfrak{p}_j} : H]} = \frac{|(\mathcal{O}_K/\mathfrak{m})^\times| / w_K}{\prod_{j\in I}[H_{\mathfrak{p}_j} : H]} = \frac{\prod_{j\in I} |(\mathcal{O}_K/\mathfrak{p}_j)^\times|}{w_K \prod_{j\in I} |(\mathcal{O}_K/\mathfrak{p}_j)^\times| / w_K} \\ &= w_K^{s-1}.\end{aligned}$$

The second equality follows since for any $2 \leq j \leq s$ we obtain $H_{\mathfrak{p}_j} \cap \prod_{i=1}^{j-1} H_{\mathfrak{p}_i} = H$ by considering the ramification of $\mathfrak{p}_j$. Since $p \nmid w_K$, we get $L \subseteq \prod_{j\in I} H_{\mathfrak{p}_j}$. $\square$

Using the canonical isomorphism of the above proof, we obtain

$$\mathrm{Gal}(H_{\mathfrak{p}_j}/H) \cong (\mathcal{O}_K/\mathfrak{p}_j)^\times / \operatorname{im}(\mu(K)),$$

which is a cyclic group. Since $t_j \mid [L_{\mathfrak{p}_j} : K] \mid [H_{\mathfrak{p}_j} : K]$ and $p \nmid h$, it follows that $t_j \mid [H_{\mathfrak{p}_j} : H]$. Using $p \nmid h$ and [CK19, Lemma 2.1] we can define F_j to be the unique subfield of $H_{\mathfrak{p}_j}$ such that $[F_j : K] = t_j$. Then $F_j \cap H = K$ and F_j/K is totally ramified at $\mathfrak{p}_j$ and unramified everywhere else.

From now on, we will write $H_J := H_{\mathfrak{m}_J}$ for each $\emptyset \neq J \subseteq I$ and

$$F_J := \prod_{j\in J} F_j \subseteq H_J.$$

Note that the conductor of F_J is $\mathfrak{m}_J$. The definition of F_I implies that the Galois group $\mathrm{Gal}(F_I/F_{I\setminus\{j\}}) = I_j(F_I)$ is the inertia subgroup of a prime of F_I above $\mathfrak{p}_j$, in particular for each $j \in I$ we have $\left|\mathrm{Gal}(F_I/F_{I\setminus\{j\}})\right| = t_j$.

Lemma 3.4.3. *For any two subsets $\emptyset \neq J_1 \subseteq J_2 \subseteq I$, we have $F_{J_1} = F_{J_2} \cap H_{J_1}$. Moreover, $F_I \cap H = K$.*

Proof. The inclusion $F_{J_1} \subseteq F_{J_2} \cap H_{J_1}$ is clear. For the other inclusion, we use induction on $n = |J_2 \setminus J_1|$. The case $n = 0$, i.e. $J_1 = J_2$, is clear. If $n \geq 1$, we fix an index $j \in J_2 \setminus J_1$ and we see that

$$F_{J_2} \cap H_{J_1} \subseteq F_{J_2} \cap H_{J_2\setminus\{j\}} \subseteq F_{J_2\setminus\{j\}}$$

by the induction hypothesis. But we clearly also have $F_{J_2} \cap H_{J_1} \subseteq H_{J_1}$, hence

$$F_{J_2} \cap H_{J_1} \subseteq F_{J_2\setminus\{j\}} \cap H_{J_1} \subseteq F_{J_1}$$

by the induction hypothesis.

The second assertion follows, since $[F_I : K]$ is a p-power and $p \nmid h$. $\square$

Proposition 3.4.4. *For each $j \in I$ we have $F_j H_{I\setminus\{j\}} = LH_{I\setminus\{j\}}$. The Galois group*

$$G = \mathrm{Gal}(F_I/K) = \prod_{j\in I} \mathrm{Gal}(F_I/F_{I\setminus\{j\}})$$

is the direct product of its inertia subgroups. Moreover $L \subseteq F_I$.

Proof. We can take the proof of [CK19, Prop. 2.2] here, since no changes are necessary. □

Corollary 3.4.5. *(i) For each $j \in I$ we have*

$$I_j(L) = \mathrm{Gal}(L/L \cap F_{I\setminus\{j\}}) = \langle \sigma^{p^k/t_j} \rangle \, .$$

Moreover, $F_{I\setminus\{j\}}L = F_I$ and $[L \cap F_{I\setminus\{j\}} : K] = \frac{p^k}{t_j}$.

(ii) F_I/L is an unramified abelian extension.

(iii) There exists at least one index $j_0 \in I$ such that $t_{j_0} = p^k$ so that $G = \mathrm{Gal}(F_I/K)$ has exponent p^k.

Proof. See [CK19, Cor. 2.3]. □

3.4.3 The elliptic units

Since $F_I \cap H = K$ by Lemma 3.4.3, there are no unramified elliptic units and we define

$$\eta_J := N_{H_J/F_J}(\alpha_{\mathfrak{m}_J}) = \varphi_{F_I,\mathfrak{m}_J}^{1/h} \in \mathcal{O}_{F_J} \, ,$$

cf. Remark 3.2.6. Let $\sigma_j \in G = \mathrm{Gal}(F_I/K)$ be the lift of the Frobenius of $\mathfrak{p}_j$ which is uniquely defined by $\sigma_j|_{F_{I\setminus\{j\}}} = (\mathfrak{p}_j, F_{I\setminus\{j\}}/K)$ and $\sigma_j|_{F_j} = 1$. Then we can state the next

Lemma 3.4.6. *For any $j \in I$ we have*

$$D_j(L) = \langle \sigma^{n_j} \rangle = \langle \sigma_j|_L, \sigma^{p^k/t_j} \rangle \, .$$

Proof. See [CK19, Lemma 3.1]. □

Analogously to [CK19, Lemma 3.2], we obtain

Lemma 3.4.7. *We have $\mu(F_I) = \mu(K)$.*

Proof. For $\zeta \in \mu(F_I)$, the extension $K(\zeta)/K$ is a constant field extension. Since all constant field extensions are unramified, we get $K(\zeta) \subseteq F_I \cap H = K$, so $\zeta \in \mu(K)$. □

Proposition 3.2.9 implies that for each $J \subseteq I$ and each $j \in J$

$$N_{F_J/F_{J\setminus\{j\}}}(\eta_J) = \begin{cases} \eta_{J\setminus\{j\}}^{1-\sigma_j^{-1}}, & J \setminus \{j\} \neq \emptyset, \\ \zeta x_j^{w_\infty/w_K} & J \setminus \{j\} = \emptyset, \end{cases} \tag{3.4.1}$$

for some $\zeta \in \mu(K)$.

In analogy to [CK19], we use the following definition of elliptic units:

Definition 3.4.8.
- The *group of elliptic numbers* $\mathcal{P}_{F_I}$ *of* F_I is defined to be the $\mathbb{Z}[G]$-submodule of $F_I^\times$ generated by $\mu(K)$ and by η_J for all $\emptyset \neq J \subseteq I$.
- The *group of elliptic units* $\mathcal{C}_{F_I}$ *of* F_I is then defined as $\mathcal{C}_{F_I} := \mathcal{P}_{F_I} \cap \mathcal{O}_{F_I}^\times$.
- The *group of elliptic numbers* $\mathcal{P}_L$ *of* L is defined as the $\mathbb{Z}[\Gamma]$-submodule of $L^\times$ generated by $\mu(K)$ and $N_{F_J/F_J\cap L}(\eta_J)$ for all $\emptyset \neq J \subseteq I$.
- The *group of elliptic units* $\mathcal{C}_L$ *of* L is defined as $\mathcal{C}_L := \mathcal{P}_L \cap \mathcal{O}_L^\times$.

Since $F_I \cap H = K = L \cap H$, one can check that these elliptic units are related to the units of Definition 3.2.8 by

$$C_{F_I} = \mathcal{C}_{F_I}^h \cdot \mu(K)\,,$$
$$C_L = \mathcal{C}_L^h \cdot \mu(K)\,.$$

This fact and Theorem 3.3.9 imply the next Lemma. We first need the following

Notation. Let $\widetilde{L}$ be the maximal subfield of L containing K such that $\widetilde{L}/K$ is ramified in at most one prime ideal of K.

Note that since Γ is cyclic and of prime power order, the field $\widetilde{L}$ is unique.

Lemma 3.4.9. *(i) We have*

$$[\mathcal{O}_{F_I}^\times : \mathcal{C}_{F_I}] = w_\infty^{[F_I:K]-1}\frac{h_{F_I}}{h}\,,$$
$$[\mathcal{O}_L^\times : \mathcal{C}_L] = w_\infty^{[L:K]-1}\frac{h_L}{h[L:\widetilde{L}]}\,.$$

(ii) For $\beta \in \mathcal{P}_{F_I}$ *we have* $\beta \in \mathcal{C}_{F_I}$ *if and only if* $N_{F_I/K}(\beta) \in \mu(K)$.

Sketch of a proof. For more details and part (ii) see [CK19, Lemma 3.4]. First, we see that by the observation above $[\mathcal{C}_{F_I} : C_{F_I}] = h^{[F_I:K]-1}$ and $[\mathcal{C}_L : C_L] = h^{[L:K]-1}$. Moreover, it follows from Proposition 3.4.4, Proposition 3.3.10 (ii) (resp. 3.3.10 (i)) and Proposition 3.3.17 (iii) (resp. 3.3.17 (i)) that the last quotient in Theorem 3.3.9 is equal to 1 for L (resp. F_I). We also obtain $w_{F_I} = w_L = w_K$ by Lemma 3.4.7, $L_{(1)} = K$, $F_I \cap H_{\mathfrak{p}^\infty} = F_j$ for $\mathfrak{p} = \mathfrak{p}_j$ and $\prod_{j=1}^s [F_j : K] = [F_I : K]$, which yields the first equation. For the second equation, we consider the definition of $\widetilde{L}$. By part (iii) of Corollary 3.4.5 we know that there is at least one prime $\mathfrak{p}_i$ which is totally ramified in L. Therefore, $\widetilde{L}$ is the maximal subfield of L which is unramified at every prime except $\mathfrak{p}_i$, hence $\widetilde{L} = L \cap H_{\mathfrak{p}_i^\infty}$. Since for $\mathfrak{p} \neq \mathfrak{p}_i$ the extension $L \cap H_{\mathfrak{p}^\infty}$ is unramified at $\mathfrak{p}_i$ and $\mathfrak{p}_i$ is totally ramified in L, we find that $L \cap H_{\mathfrak{p}^\infty} = K$ for $\mathfrak{p} \neq \mathfrak{p}_i$ hence we obtain $\prod_{\mathfrak{p}} [L \cap H_{\mathfrak{p}^\infty} : K] = [\widetilde{L} : K]$. □

Now we use a modification of Sinnott's module defined in [GK14b]. This module U is a $\mathbb{Z}[G]$-submodule of $\mathbb{Q}[G] \oplus \mathbb{Z}^s$ generated over $\mathbb{Z}[G]$ by certain elements ρ_J, $J \subseteq I$. Each $\mathbb{Z}$-summand is endowed with the trivial G-action and has a standard basis element denoted by e_j.

Define

$$\begin{aligned} \Psi\colon \mathcal{P}_{F_I} &\longrightarrow U \\ \eta_J &\longmapsto \rho_{I\setminus J} \end{aligned}$$

for $\emptyset \neq J \subseteq I$ and $\Psi(\mu(K)) = 0$.

Lemma 3.4.10. *The map Ψ is a well-defined $\mathbb{Z}[G]$-module homomorphism satisfying $\ker(\Psi) = \mu(K)$ and $U = \Psi(\mathcal{P}_{F_I}) \oplus (NG \cdot \mathbb{Z})$.*

Proof. The proof closely follows the proof of [CK19, Lemma 3.5].

From [GK14b] we get that

$$U = \langle \{\rho_J \mid J \subsetneq I\} \rangle_{\mathbb{Z}[G]} \oplus NG \cdot \mathbb{Z} \,. \tag{3.4.2}$$

Hence, we obtain an embedding of $\mathbb{Z}[G]$-modules $\iota\colon U/NG \cdot \mathbb{Z} \longrightarrow U$ such that $\mathrm{im}(\iota) = \langle \{\rho_J | J \subsetneq I\} \rangle_{\mathbb{Z}[G]}$. Define a map $\Phi\colon U \longrightarrow \mathcal{P}_{F_I}$ by

$$\begin{aligned} \Phi(\rho_J) &= \eta_{I\setminus J}\,, \qquad J \subsetneq I\,, \\ \Phi(\rho_I) &= 0\,. \end{aligned}$$

Comparing the relations [GK14b, (1.10)] with the norm relations in Proposition 3.2.9 shows that Φ is a well-defined $\mathbb{Z}[G]$-module homomorphism. By the definition $\rho_I = NG$ from [GK14b], we get $\Phi(NG \cdot \mathbb{Z}) = \Phi(\rho_I \mathbb{Z}) = 0$ and since

$$\mathcal{P}_{F_I} = \langle \{\eta_J \mid \emptyset \neq J \subseteq I\} \cup \mu(K) \rangle_{\mathbb{Z}[G]} = \langle \Phi(U) \cup \mu(K) \rangle_{\mathbb{Z}[G]}\,,$$

we obtain a surjective $\mathbb{Z}[G]$-homomorphism $\widetilde{\Phi}\colon U/NG \cdot \mathbb{Z} \longrightarrow \mathcal{P}_{F_I}/\mu(K)$. Note that U (and hence $U/NG \cdot \mathbb{Z}$ via ι) and $\mathcal{P}_{F_I}/\mu(K)$ are $\mathbb{Z}$-torsion-free, therefore $\widetilde{\Phi}$ is an isomorphism if and only if both modules have the same $\mathbb{Z}$-rank (see (3.4.3) below).

We note that since the elliptic numbers are S-units where S consists of the s ramifying places, the Dirichlet unit theorem implies that $\mathrm{rk}_{\mathbb{Z}}(\mathcal{P}_{F_I}) \leq s + \mathrm{rk}_{\mathbb{Z}}(\mathcal{O}_{F_I}^{\times})$. Moreover, we know from the norm relations (3.4.1) that $\mathcal{P}_{F_I}$ contains powers of $x_1, ..., x_s$. These are linearly independent over $\mathbb{Z}$ and are clearly not contained in $\mathcal{C}_{F_I}$ hence we find that

$$s + \mathrm{rk}_{\mathbb{Z}}(\mathcal{O}_{F_I}^{\times}) \geq \mathrm{rk}_{\mathbb{Z}}(\mathcal{P}_{F_I}) \geq s + \mathrm{rk}_{\mathbb{Z}}(\mathcal{C}_{F_I})$$

and since the elliptic units have finite index in $\mathcal{O}_{F_I}^{\times}$, we obtain equality. Therefore,

$$\mathrm{rk}_{\mathbb{Z}}(\mathcal{P}_{F_I}) = s + \mathrm{rk}_{\mathbb{Z}}(\mathcal{O}_{F_I}^{\times}) = s + [F_I : K] - 1 = \mathrm{rk}_{\mathbb{Z}}(U) - 1\,, \tag{3.4.3}$$

where the last equation follows from [GK14b, Remark 1.4]. Hence $\widetilde{\Phi}$ is an isomorphism and we can define $\Psi'\colon \mathcal{P}_{F_I} \longrightarrow U$ as the composition of maps

$$\mathcal{P}_{F_I} \twoheadrightarrow \mathcal{P}_{F_I}/\mu(K) \xrightarrow[\cong]{\widetilde{\Phi}^{-1}} U/NG \cdot \mathbb{Z} \overset{\iota}{\hookrightarrow} U\,.$$

By definition, we then obtain

$$\Psi'(\eta_J) = \rho_{I\setminus J}\,,$$
$$\Psi'(\mu(K)) = 0\,,$$

so $\Psi = \Psi'$. The decomposition $U = \Psi(\mathcal{P}_{F_I}) \oplus (NG\cdot\mathbb{Z})$ follows from (3.4.2). □

We call

$$\eta := N_{F_I/L}(\eta_I)$$

the *top generator* of both $\mathcal{P}_L$ and $\mathcal{C}_L$. Set $B := \mathrm{Gal}(F_I/L) \subseteq \mathrm{Gal}(F_I/K) = G$, then we have $\Gamma = \langle\sigma\rangle \cong G/B$.

Lemma 3.4.11. *An elliptic number $\beta \in \mathcal{P}_{F_I}$ belongs to L if and only if $\Psi(\beta)$ is fixed by B, i.e. $\Psi(\mathcal{P}_{F_I})^B = \Psi(\mathcal{P}_{F_I} \cap L)$.*

Proof. See [CK19, Lemma 4.1]. □

Recall that n_i is the index of the decomposition group of the ideal $\mathfrak{P}_i \subseteq L$ in Γ. Without loss of generality we can assume

$$n_1 \le n_2 \le \cdots \le n_s$$

and we set $n = n_s = \max\{n_i \mid i \in I\}$. Since $p \mid t_s$ we have $n \mid p^{k-1}$ and by Corollary 3.4.5 (iii) we get $t_1 = p^k$ and hence $n_1 = 1$. Let L' be the unique subfield of L containing K such that $[L' : K] = n$. Note that $\langle\sigma^n\rangle = \mathrm{Gal}(L/L')$ and that $\mathfrak{p}_s$ splits completely in L'/K. Now we can state

Theorem 3.4.12. *There is a unique $\alpha \in L$ such that $N_{L/L'}(\alpha) = 1$ and such that $\eta = \alpha^y$ holds, where $y = \prod_{i=2}^{s-1}(1-\sigma^{n_i})$. This α is an elliptic unit of F_I, so that $\alpha \in \mathcal{C}_{F_I} \cap L$. Moreover, there is $\gamma \in L^\times$ such that $\alpha = \gamma^{1-\sigma^n}$.*

Proof. See [CK19, Thm. 4.2]. We repeat the proof here in order to make some of the arguments more explicit. The main idea is to use the next

Proposition 3.4.13. *Let $f \in \mathbb{Z}[X] \setminus \{0, \pm 1\}$ and let $A = \mathbb{Z}[X]/f\mathbb{Z}[X]$. Let $\mathcal{M}$ be a finitely generated A-module without $\mathbb{Z}$-torsion. Then*

(i) $\mathrm{Ext}^1_A(\mathcal{M}, A) = 0$.

(ii) Let y be a nonzerodivisor in A, and let $x \in \mathcal{M}$. Then $x \in y\mathcal{M}$ if and only if for all $\varphi \in \mathrm{Hom}_A(\mathcal{M}, A)$ we have $\varphi(x) \in yA$.

Proof. See [GK14a, Prop. 6.2]. □

If $s = 2$ then $y = 1$ and we can set $\alpha = \eta$. Clearly $\alpha = \eta^y$ and since $\mathfrak{p}_s$ splits completely in L' we obtain that $N_{L/L'}(\alpha) = 1$ from the norm relation (see (3.4.4) below). If $s > 2$, y is always a zero divisor in $\mathbb{Z}[\Gamma]$ (note that since $n_i \mid p^k$, we get that $X^{n_i} - 1 \mid X^{p^k} - 1$ and hence $\sigma^{n_i} - 1 \mid \sigma^{p^k} - 1 = 0$ for each i). So in order to apply Proposition 3.4.13, we need to work in an appropriate quotient of $\mathbb{Z}[\Gamma]$, where y is a nonzerodivisor. Let $N_n = \sum_{i=1}^{p^k/n} \sigma^{in}$, then N_n can be understood as the norm operator from L to L'. Let $R = \mathbb{Z}[\Gamma]/N_n\mathbb{Z}[\Gamma]$ and let $\gamma\colon R \longrightarrow (1-\sigma^n)\mathbb{Z}[\Gamma]$ be the multiplication by $1-\sigma^n$. Since the annihilator of $1-\sigma^n$ is exactly given by $\mathbb{Z}\cdot N_n = N_n\mathbb{Z}[\Gamma]$ (see e.g. [Neu11, Thm. (1.3)]), γ is an isomorphism of $\mathbb{Z}[\Gamma]$-modules. Define

$$\mathcal{M} := \{x \in \Psi(\mathcal{P}_{F_I})^B \mid N_n x = 0\}$$

where Ψ is the map from Lemma 3.4.10. It is clearly an R-module and since $\mathcal{M} \subseteq U$ it has no $\mathbb{Z}$-torsion. Using the definition of η and the norm relation 3.2.9, we obtain

$$\Psi(\eta) = \Psi(N_{F_I/L}(\eta_I)) = NB \cdot \Psi(\eta_I) = NB \cdot \rho_\emptyset\,,$$

where $NB = \sum_{\tau\in B}\tau \in \mathbb{Z}[G]$, and

$$N_{L/L'}(\eta) = N_{F_I/L'}(\eta_I) = N_{F_{\{1,\ldots,s-1\}}/L'}(\eta_{\{1,\ldots,s-1\}})^{1-\sigma_s^{-1}} = 1\,. \qquad (3.4.4)$$

Here we used that $\sigma_s|_{L'} = \mathrm{id}$ since $\mathfrak{p}_s$ splits completely in L'. In particular we get that $\Psi(\eta) = NB \cdot \rho_\emptyset \in \mathcal{M}$.

Note that the $\mathbb{Z}[\Gamma]$-module structure on $\mathcal{M}$ is compatible with its R-module structure via the natural projection $\mathbb{Z}[\Gamma] \longrightarrow R$. Since we get $U^B = \Psi(\mathcal{P}_{F_I})^B \oplus NG\cdot\mathbb{Z}$ from Lemma 3.4.10, we may view $\mathcal{M}$ as a $\mathbb{Z}[\Gamma]$-submodule of U^B. Then $U^B/\mathcal{M}$ has no $\mathbb{Z}$-torsion: suppose that there exists $x \in U^B$ with $cx \in \mathcal{M}$ for a positive integer c. Then $c(N_n x) = N_n(cx) = 0$. Since $N_n x \in U$ and U has no $\mathbb{Z}$-torsion, this implies $N_n x = 0$ and hence $x \in \mathcal{M}$.

To each R-linear map $\psi \in \mathrm{Hom}_R(\mathcal{M}, R)$ we may associate the $\mathbb{Z}[\Gamma]$-linear map $\gamma\circ\psi \in \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(\mathcal{M}, \mathbb{Z}[\Gamma])$. Fixing such a ψ we want to prove that $\psi(NB\cdot\rho_\emptyset) \in yR$.

Setting $f = X^{p^k} - 1$ in Proposition 3.4.13, we get $A = \mathbb{Z}[X]/f\mathbb{Z}[X] \cong \mathbb{Z}[\Gamma]$. Since $U^B/\mathcal{M}$ has no $\mathbb{Z}$-torsion, part (i) implies that $\mathrm{Ext}^1_{\mathbb{Z}[\Gamma]}(U^B/\mathcal{M}, \mathbb{Z}[\Gamma]) = 0$. With the definition of Ext^1 we get the existence of $\varphi \in \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U^B, \mathbb{Z}[\Gamma])$ such that $\varphi|_{\mathcal{M}} = \gamma\circ\psi$. Define $v \in \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U^B, \mathbb{Z}[\Gamma])$ by $v(x) = (1-\sigma)\varphi(x)$. For the next step we observe:

(i) For all $i \in I$, $t_i e_i \in U^B$, where $t_i = |I_i|$ with $I_i = \mathrm{Gal}(F_I/F_{I\setminus\{i\}})$ and e_i is defined in [GK14b]. Moreover, $v(t_i e_i) = 0$ since σ acts trivially on e_i.

(ii) We get from Lemma 3.4.6 that $1-\sigma_i|_L \in (1-\sigma^{n_i})\mathbb{Z}[\Gamma]$ since $\sigma_i|_L$ is a power of σ^{n_i}. Similarly, for $\tau \in I_i$ we get from Corollary 3.4.5 (i) that $\tau|_L$ is a power of σ^{p^k/t_i} which is indeed a power of σ^{n_i}, hence $1-\tau|_L \in (1-\sigma^{n_i})\mathbb{Z}[\Gamma]$.

These observations combine with the formula in [GK14b, Cor. 1.7(ii)] to give

$$v(NB\cdot\rho_\emptyset) \in \prod_{i=1}^{s}(1-\sigma^{n_i})\mathbb{Z}[\Gamma]\,.$$

We want to reduce this formula by $1-\sigma$, so we have to show that multiplication by $1-\sigma$ is injective on $(1-\sigma)^n\mathbb{Z}[\Gamma]$. Suppose that $x \in (1-\sigma)^n\mathbb{Z}[\Gamma]$ and $(1-\sigma)x = 0$. Then x is in the annihilator of $1-\sigma$ in $\mathbb{Z}[\Gamma]$. But as x is a multiple of $(1-\sigma)^n$, we find that $x^2 = 0$. Since $f = X^{p^k} - 1$ is square-free, the ring $\mathbb{Z}[X]/f\mathbb{Z}[X] \cong \mathbb{Z}[\Gamma]$ has no nilpotent elements, therefore $x = 0$ and multiplication by $1-\sigma$ is injective on $(1-\sigma^n)\mathbb{Z}[\Gamma]$. This implies

$$\gamma\circ\psi(NB\cdot\rho_\emptyset) = \varphi(NB\cdot\rho_\emptyset) \in \prod_{i=2}^{s}(1-\sigma^{n_i})\mathbb{Z}[\Gamma]\,.$$

Since γ is an R-module isomorphism, we obtain

$$\psi(NB \cdot \rho_\emptyset) \in \prod_{i=2}^{s-1}(1-\sigma^{n_i})R = yR\,.$$

Now set $g = \sum_{i=1}^{p^k/n} X^{(i-1)n}$. From $n \mid p^{k-1}$, we get that $g \notin \{0, \pm 1\}$ and applying Proposition 3.4.13 (ii) to $A = \mathbb{Z}[X]/g\mathbb{Z}[X] \cong R$, we get an element $\delta \in \mathcal{M}$ such that $y\delta = NB \cdot \rho_\emptyset = \Psi(\eta)$. Note that y is a nonzerodivisor in R: Since $(X^n-1)g = X^{p^k}-1$ is separable, the zeros of $X^n - 1$ and g are distinct. Identifying y with the image of the polynomial $\prod_{i=2}^{s-1}(1-X^{n_i})$ in A, we see that each factor appearing in the product is a divisor of $X^n - 1$ and is hence prime to g. Therefore, this product is no zero divisor in A and so y is no zero divisor in R.

Since $\delta \in \mathcal{M}$, we have $\delta \in \Psi(\mathcal{P}_{F_I})^B$ and $N_n\delta = 0$. By Lemma 3.4.11, there exists $\alpha' \in \mathcal{P}_{F_I} \cap L$ unique up to a root of unity such that $\delta = \Psi(\alpha')$. We get

$$\Psi(N_{L/L'}(\alpha')) = N_n\Psi(\alpha') = N_n\delta = 0\,,$$

hence $N_{L/L'}(\alpha') = \zeta \in \mu(K)$. As $p \nmid w_K$, there is $\zeta' \in \mu(K)$ such that $N_{L/L'}(\zeta') = \zeta^{-1}$. Setting $\alpha := \alpha'\zeta' \in \mathcal{P}_{F_I} \cap L$, we get that $N_{L/L'}(\alpha) = 1$ and $\delta = \Psi(\alpha)$. Therefore, we find $\Psi(\alpha^y) = y\delta = \Psi(\eta)$, so $\zeta'' = \alpha^{-y}\eta \in \ker(\Psi) = \mu(K)$. Furthermore, we clearly get $1 = N_{L/L'}(\alpha^{-y}\eta) = (\zeta'')^{p^k/n}$ and since $p \nmid w_K$ this implies $\zeta'' = 1$. From $N_{L/K}(\alpha) = 1$ we get that α is indeed an elliptic unit of F_I.

The uniqueness of α can be found in [CK19]. The existence of γ as in the theorem is just an application of Hilbert's Theorem 90 to the extension L/L'. □

Remark 3.4.14. There is an alternative description of a power of α in terms of the conjugates of η (cf. [CK19, Remark 4.3]). For each $j = 1, ..., s$ define the elements

$$N_{n_j} = \sum_{i=1}^{p^k/n_j} \sigma^{in_j}, \qquad \Delta_{n_j} = \sum_{i=1}^{p^k/n_j - 1} i\sigma^{in_j}\,.$$

Then we obtain

$$(1-\sigma^{n_j})N_{n_j} = 0\,, \qquad (1-\sigma^{n_j})\Delta_{n_j} = N_{n_j} - \frac{p^k}{n_j}\,.$$

Also note that the norm operator $N_{L/L'}$ corresponds to the element N_n. We obtain from Theorem 3.4.12 that $\eta = \alpha^y$. Since $N_{L/L'}(\alpha) = \alpha^{N_n} = 1$, we also get that $\alpha^{N_{n_j}} = 1$ for all $j = 1, ..., s$. Hence, we obtain

$$\eta^{\prod_{i=2}^{s-1}\Delta_{n_i}} = \alpha^{\prod_{i=2}^{s-1}(N_{n_i} - p^k/n_i)} = \alpha^{(-1)^s\prod_{i=2}^{s-1}p^k/n_i} = \alpha^{(-1)^s r}\,,$$

where $r := \prod_{i=2}^{s-1}\frac{p^k}{n_i}$ is a power of p. Therefore, $\alpha^r = \eta^{(-1)^s\prod_{i=2}^{s-1}\Delta_{n_i}}$.

3.4.4 Enlarging the group $\mathcal{C}_L$ of elliptic units of L

We label the subfields of L containing K by

$$K = L_0 \subsetneq L_1 \subsetneq L_2 \subsetneq \cdots \subsetneq L_k = L$$

hence we obtain $[L_i : K] = p^i$. Moreover, we define

$$M_i := \{j \in I \mid t_j > p^{k-i}\} .$$

Since we have already seen that $n_s = 1$, we obtain from the definition of M_i that

$$1 \in M_1 \subseteq M_2 \subseteq \cdots \subseteq M_k = I .$$

For $j \in M_i$ we get $p^i > \frac{p^k}{t_j}$ and with Corollary 3.4.5 (i) we obtain that $\mathfrak{p}_j$ ramifies in L_i. On the other hand, if $\mathfrak{p}_j$ ramifies in L_i, this implies that $t_j > [L : L_i] = p^{k-i}$. This shows that the conductor of L_i is equal to $\mathfrak{m}_{M_i}$ and so $L_i \subseteq F_{M_i}$ by Proposition 3.4.4, applied to L_i. Define

$$\eta_i := N_{F_{M_i}/L_i}(\eta_{M_i})$$

for $i = 1, ..., k$, then $\eta_k = \eta \in L$ is the top generator of $\mathcal{C}_L$.

Now we fix $j \in \{1, ..., s\}$ and let $L_i = L^{T_j}$ hence the index i is determined by $t_j = p^{k-i}$. By Lemma 3.4.6 we get that

$$\langle \sigma^{n_j} \rangle / \langle \sigma^{p^k/t_j} \rangle = \langle \sigma_j|_L, \sigma^{p^k/t_j} \rangle / \langle \sigma^{p^k/t_j} \rangle .$$

This quotient group can be interpreted as the restriction to L_i since $\sigma^{p^k/t_j} = \sigma^{p^i}$ generates $\mathrm{Gal}(L/L_i)$, so we can find a smallest positive integer c_j such that $\sigma^{-c_j n_j}|_{L_i} = \sigma_j|_{L_i}$. Moreover, we see that $\mathfrak{p}_j$ splits completely in L_i/K if and only if $n_j = \frac{p^k}{t_j}$, in this case we get in particular that $c_j = 1$ since σ^{n_j} is already an element of the inertia group of $\mathfrak{p}_j$ of L/K. If $\mathfrak{p}_j$ does not split completely in L_i/K, we find that $n_j < \frac{p^k}{t_j}$ and hence $\langle \sigma^{n_j}|_{L_i} \rangle = \langle \sigma_j|_{L_i} \rangle$. In each case, we find that $p \nmid c_j$, so $1 - \sigma^{c_j n_j}$ and $1 - \sigma^{n_j}$ are associated in $\mathbb{Z}[\Gamma]$.

Now let $i \in \{1, ..., k\}$ be such that $|M_i| > 1$. We want to apply Theorem 3.4.12 to the extension L_i/K and obtain an elliptic unit $\alpha_i \in \mathcal{C}_{F_{M_i}} \cap L_i$ and a number $\gamma_i \in L_i^\times$ such that

(i) $\eta_i = \alpha_i^{y_i}$, where $y_i = \prod_{\substack{j \in M_i \\ 1 < j < \max M_i}} (1 - \sigma^{c_j n_j})$,

(ii) $\alpha_i = \gamma_i^{z_i}$, where $z_i = 1 - \sigma^{c_{\max M_i} n_{\max M_i}}$.

Note that the new c_j factors can be obtained since $1 - \sigma^{n_j}$ and $1 - \sigma^{c_j n_j}$ are associated. In particular we find for $|M_i| = 2$ that $y_i = 1$ and $\alpha_i = \eta_i$ as the product is empty. For $i \in \{1, ..., k\}$ with $|M_i| = 1$ we set $\gamma_i = \eta_i$ and $\alpha_i = \eta_i^{1-\sigma}$.

Definition 3.4.15. The $\mathbb{Z}[\Gamma]$-submodule $\overline{\mathcal{C}_L}$ of $\mathcal{O}_L^\times$ generated by $\mu(K)$ and $\alpha_1, ..., \alpha_k$ is called the *extended group of elliptic units.*

Then we obtain a similar result as given in [CK19, Thm. 5.2]

Theorem 3.4.16. *The group of elliptic units $\mathcal{C}_L$ of L is a subgroup of $\overline{\mathcal{C}_L}$ of index $[\overline{\mathcal{C}_L} : \mathcal{C}_L] = p^\nu$, where*

$$\nu = \sum_{j=1}^{k} \sum_{\substack{i \in M_j \\ 1 < i < \max M_j}} n_i \, .$$

Moreover, setting $\varphi_L := (\prod_{i=1}^{s} t_i^{n_i}) \cdot \prod_{j=1}^{k} p^{-n_{\max M_j}}$, we get

$$p^\nu = \varphi_L \cdot [L : \widetilde{L}]^{-1}$$

and

$$[\mathcal{O}_L^\times : \overline{\mathcal{C}_L}] = w_\infty^{p^k - 1} \cdot \frac{h_L}{h} \cdot \varphi_L^{-1} \, .$$

Proof. We use the same proof as in [GK15, Thm. 3.1]. Note that we need the factors c_j appearing in the definition of the α_i here. □

Remark 3.4.17. If $p \nmid w_\infty$, we obtain $\varphi_L \mid h_L$. As in [CK19, Remark 5.3], this divisibility statement is really stronger than $[F_I : L] \mid h_L$ (which we obtain since F_I/L is unramified). Indeed, by [GK15, Prop. 3.4], $[F_I : L] \mid \varphi_L$ and we obtain equality if and only if $n_1 = \cdots n_{s-1} = 1$.

3.5 Semispecial numbers

We use the same notation as before and fix m, which is a power of p such that $p^{ks} \mid m$. We know that for a prime ideal $\mathfrak{q}$ of K we have

$$\mathrm{Gal}(H_\mathfrak{q}/H) \cong (\mathcal{O}_K/\mathfrak{q})^\times / \operatorname{im}(\mu(K))$$

via Artin's reciprocity map. In particular, $\mathrm{Gal}(H_\mathfrak{q}/H)$ is cyclic. This enables us to formulate the next

Definition 3.5.1. For a prime ideal $\mathfrak{q}$ of K such that $|\mathcal{O}_K/\mathfrak{q}| \equiv 1 \mod m$, we define $K[\mathfrak{q}]$ to be the (unique) subfield of $H_\mathfrak{q}$ containing K such that $[K[\mathfrak{q}] : K] = m$. For a finite field extension M/K, we define $M[\mathfrak{q}] := MK[\mathfrak{q}]$.

Note that since $|\mathcal{O}_K/\mathfrak{q}| \equiv 1 \mod m$ and $p \nmid |\mu(K)|$, we get that the order of $\mathrm{Gal}(H_\mathfrak{q}/H)$ is divisible by m. Hence we obtain the existence and uniqueness of $K[\mathfrak{q}]$ from the fact that $p \nmid h$ and [CK19, Lemma 2.1]. Since $K[\mathfrak{q}]$ is contained in $H_\mathfrak{q}$ it is unramified outside $\mathfrak{q}$. Moreover, since $p \nmid h$ we get that $H \cap K[\mathfrak{q}] = K$ and hence it is totally ramified at $\mathfrak{q}$. Finally, since $p \nmid |\mathcal{O}_K/\mathfrak{q}|$ we find that this ramification is tame.

Definition 3.5.2. Let $\mathcal{Q}_m$ be the set of all prime ideals $\mathfrak{q}$ of K such that

(i) $|\mathcal{O}_K/\mathfrak{q}| \equiv 1 + m \mod m^2$,

(ii) $\mathfrak{q}$ splits completely in L,

(iii) for each $j = 1, ..., s$, the class of x_j is an m-th power in $(\mathcal{O}_K/\mathfrak{q})^\times$.

Now we want to study condition (iii) in some more detail. Let $\mathfrak{q}$ be such that $|\mathcal{O}_K/\mathfrak{q}| \equiv 1 \mod m$. Since $H \cap K[\mathfrak{q}] = K$, we get $\mathrm{Gal}(H[\mathfrak{q}]/H) \cong \mathrm{Gal}(K[\mathfrak{q}]/K)$ by restriction. The first group is the unique quotient of the cyclic group $\mathrm{Gal}(H_\mathfrak{q}/H)$ of order m, hence it is obtained by factoring out m-th powers. Therefore, we get with the Artin reciprocity map and $p \nmid w_K$

$$(\mathcal{O}_K/\mathfrak{q})^\times/m \cong \mathrm{Gal}(H[\mathfrak{q}]/H) \cong \mathrm{Gal}(K[\mathfrak{q}]/K)\,,$$

where the composition map takes the class of $\alpha \in \mathcal{O}_K \setminus \mathfrak{q}$ to $(\alpha\mathcal{O}_K, K[\mathfrak{q}]/K)$. Now the facts that $x_j\mathcal{O}_K = \mathfrak{p}_j^h$ and $p \nmid h$ imply that condition (iii) is equivalent to

$$(\mathfrak{p}_j, K[\mathfrak{q}]/K) = 1 \qquad \forall j = 1, ..., s\,.$$

Definition 3.5.3. A number $\varepsilon \in L^\times$ is called *m-semispecial* if for all but finitely many $\mathfrak{q} \in \mathcal{Q}_m$, there exists a unit $\varepsilon_\mathfrak{q} \in \mathcal{O}_{L[\mathfrak{q}]}^\times$ satisfying

(i) $N_{L[\mathfrak{q}]/L}(\varepsilon_\mathfrak{q}) = 1$,

(ii) if $\mathfrak{q}_{L[\mathfrak{q}]}$ is the product of all primes of $L[\mathfrak{q}]$ above $\mathfrak{q}$, then ε and $\varepsilon_\mathfrak{q}$ have the same image in $(\mathcal{O}_{L[\mathfrak{q}]}/\mathfrak{q}_{L[\mathfrak{q}]})^\times/(m/p^{k(s-1)})$.

Since each $\mathfrak{q} \in \mathcal{Q}_m$ is totally ramified in $K[\mathfrak{q}]/K$ and splits completely in L/K, we find that $L[\mathfrak{q}]/L$ is totally ramified at each prime above $\mathfrak{q}$ and $L \cap K[\mathfrak{q}] = K$. This implies that the two maps $\mathrm{Gal}(L[\mathfrak{q}]/L) \longrightarrow \mathrm{Gal}(K[\mathfrak{q}]/K)$ and $\mathrm{Gal}(L[\mathfrak{q}]/K[\mathfrak{q}]) \longrightarrow \mathrm{Gal}(L/K)$ given by restriction are isomorphisms.

Analogously to [CK19, Thm. 6.4], we get the next

Theorem 3.5.4. *The elliptic unit $\alpha \in \mathcal{C}_{F_I} \cap L$ from Theorem 3.4.12 is m-semispecial.*

Proof. Recall that α is a y-th root of the top generator η of $\mathcal{C}_L$. We need to show that for almost all $\mathfrak{q} \in \mathcal{Q}_m$, there exists an $\varepsilon_\mathfrak{q}$ satisfying the conditions (i) and (ii) of Definition 3.5.3. In fact, we construct such an $\varepsilon_\mathfrak{q}$ for *each* $\mathfrak{q} \in \mathcal{Q}_m$. The idea will be similar to the one used in the proof of Theorem 3.4.12.

We fix a prime $\mathfrak{q} \in \mathcal{Q}_m$ and set $Q := |\mathcal{O}_K/\mathfrak{q}|$. To simplify the notation, we set $\mathfrak{p}_{s+1} := \mathfrak{q}$, $F_{s+1} := K[\mathfrak{q}]$ and $I' := \{1, ..., s+1\}$. For any non-empty subset $J \subseteq I'$, we define $F_J := \prod_{j\in J} F_j$, $\mathfrak{m}_J := \prod_{j\in J} \mathfrak{p}_j$ (the conductor of F_J) and

$$\eta_J := N_{H_J/F_J}(\alpha_{\mathfrak{m}_J})\,.$$

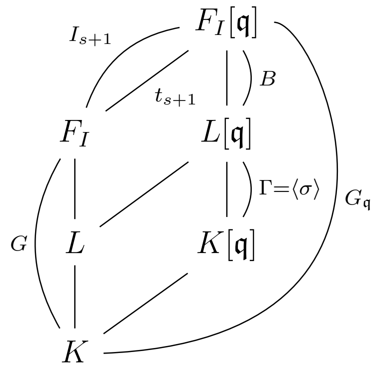
If $J \subseteq I$ we just recover the old definitions of F_J and η_J. By construction we find that $F_I[\mathfrak{q}] = F_{I'}$ and $\mathfrak{m}_{I'} = \mathfrak{q}\mathfrak{m}_I$. Since $F_I[\mathfrak{q}]$ is totally ramified at each prime of F_I over $\mathfrak{q}$, we still have $\mu(F_I[\mathfrak{q}]) = \mu(K)$. Let $G_\mathfrak{q} := \mathrm{Gal}(F_I[\mathfrak{q}]/K)$ and let $\mathcal{P}_{F_I[\mathfrak{q}]}$ be the group of elliptic numbers of $F_I[\mathfrak{q}]$, i.e. $\mathcal{P}_{F_I[\mathfrak{q}]}$ is the $\mathbb{Z}[G_\mathfrak{q}]$-submodule of $F_I[\mathfrak{q}]^\times$ generated by $\mu(K)$ and by η_J for all $\emptyset \neq J \subseteq I'$.

Let $U_\mathfrak{q} \subseteq \mathbb{Q}[G_\mathfrak{q}] \oplus \mathbb{Z}^{s+1}$ be the modification of Sinnott's module defined in [GK14b] for the parameters $v = s+1$, $I_j = \mathrm{Gal}(F_{I'}/F_{I'\setminus\{j\}})$ for $j = 1, ..., v$ (this is the inertia group of $\mathfrak{p}_j$ in $G_\mathfrak{q}$) and $\sigma_j \in G_\mathfrak{q}$ is such that $\sigma_j|_{F_j} = 1$ and $\sigma_j|_{F_{I'\setminus\{j\}}} = (\mathfrak{p}_j, F_{I'\setminus\{j\}}/K)$.

Using the sequence

$$\mathrm{Gal}(F_I[\mathfrak{q}]/K[\mathfrak{q}]) \subseteq G_\mathfrak{q} \longrightarrow G = \mathrm{Gal}(F_I/K)\ ,$$

we can identify $\mathrm{Gal}(F_I[\mathfrak{q}]/K[\mathfrak{q}])$ with G via the restriction map. In particular, for $i \neq s+1$ the group I_i is just the same as before. Analogously, we recover the subgroup B via this identification by setting $B := \mathrm{Gal}(F_I[\mathfrak{q}]/L[\mathfrak{q}])$. Since $\mathfrak{q} \in \mathcal{Q}_m$, we find by condition (iii) (i.e. $(\mathfrak{p}_j, K[\mathfrak{q}]/K) = 1$) that the σ_i map to the old σ_i for $i \in I$ and that $\sigma_{s+1} \in B$ since $\mathfrak{q}$ splits completely in L. The situation is illustrated in the following diagram:



Recall that $U = \langle \rho_J \mid J \subseteq I \rangle_{\mathbb{Z}[G]}$ and the standard basis of $\mathbb{Z}^s$ is denoted by $e_1, ..., e_s$. Define $\pi\colon \mathbb{Q}[G] \oplus \mathbb{Z}^s \longrightarrow \mathbb{Q}[G]$ to be the projection onto the first summand. Then the module $U' := \pi(U)$ is generated by $\rho'_J := \pi(\rho_J)$ for $J \subseteq I$. For the new module $U_\mathfrak{q}$ we denote the $\mathbb{Z}[G_\mathfrak{q}]$-generators by $\widetilde{\rho}_J$ and the standard basis of $\mathbb{Z}^{s+1}$ by $\widetilde{e}_1, ..., \widetilde{e}_{s+1}$. Then we can cite the next

Lemma 3.5.5 ([GK15, Lemma 2.1])**.** *There are injective $\mathbb{Z}[G]$-homomorphisms $\chi\colon U \longrightarrow U_\mathfrak{q}$ and $\chi'\colon U' \longrightarrow U_\mathfrak{q}$ defined by*

$$\chi(\rho_J) = \widetilde{\rho}_{J\cup\{s+1\}}\ , \qquad \chi'(\rho'_J) = \widetilde{\rho}_J\ ,$$

for each $J \subseteq I$. Moreover, $U_\mathfrak{q} \cong U \oplus \mathbb{Z} \oplus (U')^{m-1}$ as $\mathbb{Z}[G]$-modules.

Applying Lemma 3.4.10 to the new situation, we obtain a homomorphism

$$\Psi_\mathfrak{q}\colon \mathcal{P}_{F_I[\mathfrak{q}]} \longrightarrow U_\mathfrak{q}$$

of $\mathbb{Z}[G_\mathfrak{q}]$-modules defined by $\Psi_\mathfrak{q}(\eta_J) = \widetilde{\rho}_{I'\setminus J}$ for $\emptyset \neq J \subseteq I'$ and $\Psi_\mathfrak{q}(\mu(K)) = 0$. Moreover, $\ker(\Psi_\mathfrak{q}) = \mu(K)$ and $U_\mathfrak{q} = \Psi_\mathfrak{q}(\mathcal{P}_{F_I[\mathfrak{q}]}) \oplus NG_\mathfrak{q} \cdot \mathbb{Z}$. Setting $\hat{\eta} := N_{F_I[\mathfrak{q}]/L[\mathfrak{q}]}(\eta_{I'})$ to be the top generator of $\mathcal{C}_{L[\mathfrak{q}]}$, we have

$$\Psi_\mathfrak{q}(\hat{\eta}) = NB \cdot \Psi_\mathfrak{q}(\eta_{I'}) = NB \cdot \widetilde{\rho}_\emptyset$$

and $\Psi_{\mathfrak{q}}(\mathcal{P}_{F_I[\mathfrak{q}]} \cap L[\mathfrak{q}]) = \Psi_{\mathfrak{q}}(\mathcal{P}_{F_I[\mathfrak{q}]})^B$ (cf. Lemma 3.4.11). Let again $n := \max\{n_i \mid i \in I\}$, $N_n := \sum_{i=1}^{p^k/n} \sigma^{in}$ and $R := \mathbb{Z}[\Gamma]/N_n\mathbb{Z}[\Gamma]$, where now $\Gamma = \mathrm{Gal}(L[\mathfrak{q}]/K[\mathfrak{q}]) = \langle\sigma\rangle$. Note that the new σ can be chosen such that it restricts to the old σ.

Let $\gamma\colon R \longrightarrow (1-\sigma^n)\mathbb{Z}[\Gamma]$ be the isomorphism of $\mathbb{Z}[\Gamma]$-modules induced by the multiplication by $1-\sigma^n$. Note that we can understand N_n as the norm operator of $L[\mathfrak{q}]/L'[\mathfrak{q}]$, where L' is again the unique subfield of L such that $[L' : K] = n$.

Analogously to what we did in the proof of Theorem 3.4.12, we find that the set

$$\mathcal{M}_{\mathfrak{q}} := \{x \in \Psi_{\mathfrak{q}}(\mathcal{P}_{F_I[\mathfrak{q}]})^B \mid N_n x = 0\}$$

is an R-module without $\mathbb{Z}$-torsion such that $U_{\mathfrak{q}}^B/\mathcal{M}_{\mathfrak{q}}$ has no $\mathbb{Z}$-torsion. Then we can apply Proposition 3.4.13 with the polynomial $f = X^{p^k} - 1$ to obtain

$$\mathrm{Ext}^1_{\mathbb{Z}[\Gamma]}(U_{\mathfrak{q}}^B/\mathcal{M}_{\mathfrak{q}}, \mathbb{Z}[\Gamma]) = 0\,.$$

Since $\mathfrak{p}_s$ splits completely in L' and also in $K[\mathfrak{q}]$, it splits completely in $L'[\mathfrak{q}]$. Hence, we can use the norm relation 3.2.9 to obtain

$$\hat{\eta}^{N_n} = N_{L[\mathfrak{q}]/L'[\mathfrak{q}]}(\hat{\eta}) = N_{F_I[\mathfrak{q}]/L'[\mathfrak{q}]}(\eta_{I'}) = 1\,.$$

This implies that $NB\cdot\widetilde{\rho}_\emptyset \in \mathcal{M}_{\mathfrak{q}}$. To each $\psi \in \mathrm{Hom}_R(\mathcal{M}_{\mathfrak{q}}, R)$ we associate the map $\gamma\circ\psi$ which can be naturally viewed as an element of $\mathrm{Hom}_{\mathbb{Z}[\Gamma]}(\mathcal{M}_{\mathfrak{q}}, \mathbb{Z}[\Gamma])$. Then the vanishing of Ext^1 implies the existence of a $\varphi \in \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U_{\mathfrak{q}}^B, \mathbb{Z}[\Gamma])$ such that $\varphi|_{\mathcal{M}_{\mathfrak{q}}} = \gamma\circ\psi$. Restricting the projection $\pi\colon \mathbb{Q}[G]\oplus\mathbb{Z}^s \longrightarrow \mathbb{Q}[G]$ to U, we obtain a surjective map $\pi|_U\colon U \longrightarrow U'$ which can be composed with the map χ' from Lemma 3.5.5 to the $\mathbb{Z}[G]$-linear map $\chi'\circ\pi|_U\colon U \longrightarrow U_{\mathfrak{q}}$. By restricting further to U^B we hence obtain $\chi'\circ\pi|_{U^B} \in \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U^B, U_{\mathfrak{q}}^B)$ and $\varphi\circ\chi'\circ\pi|_{U^B} \in \mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U^B, \mathbb{Z}[\Gamma])$.

Using the same notation as in the proof of Theorem 3.4.12, we see that clearly $\pi(t_je_j) = 0$ for all $j \in I$. Hence we get the same observations for the map $v = \varphi\circ\chi'\circ\pi|_{U^B}$ and can apply [GK14b, Cor. 1.7(ii)] to obtain

$$\varphi(NB\cdot\widetilde{\rho}_\emptyset) = \varphi\circ\chi'\circ\pi(NB\cdot\rho_\emptyset) \in \prod_{i=1}^{s}(1-\sigma^{n_i})\mathbb{Z}[\Gamma] = (1-\sigma)y(1-\sigma^n)\mathbb{Z}[\Gamma]\,, \quad (3.5.1)$$

where $y = \prod_{i=2}^{s-1}(1-\sigma^{n_i})$ as before. The first equality follows from the fact that $\chi'\circ\pi(\rho_\emptyset) = \widetilde{\rho}_\emptyset$ by Lemma 3.5.5 and by the linearity of $\chi'\circ\pi|_{U^B}$.

Since $NB\cdot\widetilde{\rho}_\emptyset \in \mathcal{M}_{\mathfrak{q}}$, we can apply any $\psi \in \mathrm{Hom}_R(\mathcal{M}_{\mathfrak{q}}, R)$ to it. From the injectivity of γ and (3.5.1), we get that

$$\psi(NB\cdot\widetilde{\rho}_\emptyset) \in (1-\sigma)yR\,.$$

With Proposition 3.4.13 we get the existence of an element $\delta \in \mathcal{M}_{\mathfrak{q}}$ such that

$$(1-\sigma)y\cdot\delta = NB\cdot\widetilde{\rho}_\emptyset = \Psi_{\mathfrak{q}}(\hat{\eta})\,.$$

Since $\delta \in \mathcal{M}_{\mathfrak{q}}$, we find $\beta' \in \mathcal{P}_{F_I[\mathfrak{q}]} \cap L[\mathfrak{q}]$ such that $\delta = \Psi_{\mathfrak{q}}(\beta')$ and $\Psi_{\mathfrak{q}}(N_{L[\mathfrak{q}]/L'[\mathfrak{q}]}(\beta')) = 0$. Therefore, $\xi := N_{L[\mathfrak{q}]/L'[\mathfrak{q}]}(\beta') \in \ker(\Psi_{\mathfrak{q}}) = \mu(K)$. Then $N_{L[\mathfrak{q}]/L'[\mathfrak{q}]}(\xi) = \xi^{p^k/n}$ and since $p \nmid |\mu(K)|$, there is $\xi' \in \mu(K)$ such that $N_{L[\mathfrak{q}]/L'[\mathfrak{q}]}(\xi') = \xi^{-1}$. Setting $\beta := \beta'\xi'$, we still have $\delta = \Psi_\mathfrak{q}(\beta)$ and obtain $N_{L[\mathfrak{q}]/L'[\mathfrak{q}]}(\beta) = 1$. With the same argument as in the proof of Theorem 3.4.12, we find that $\beta^{(1-\sigma)y} = \hat{\eta}$.

As $N_{L[\mathfrak{q}]/L'[\mathfrak{q}]}(\beta) = 1$, we obtain that $N_{F_I[\mathfrak{q}]/K}(\beta) = 1$ and hence we get with Lemma 3.4.9 (ii) that $\beta \in \mathcal{C}_{F_I[\mathfrak{q}]} \cap L[\mathfrak{q}]$.

We want to show that $\alpha = \varepsilon$ is m-semispecial, so we need to construct a unit $\varepsilon_\mathfrak{q} \in L[\mathfrak{q}]$ which satisfies the norm relation (i) and the congruence relation (ii) of Definition 3.5.3. Setting $\varepsilon_\mathfrak{q} := \beta^{1-\sigma}$, we obtain such a unit:

For the norm relation, we can repeat the computation of Remark 3.4.14 to obtain

$$\beta^{r(1-\sigma)} = \hat{\eta}^{(-1)^s \prod_{i=2}^{s-1} \Delta_{n_i}} .$$

Applying Δ_1 to each side and using $N_{L[\mathfrak{q}]/L'[\mathfrak{q}]}(\beta) = \beta^{N_n} = 1$, we get

$$\beta^{rp^k} = \hat{\eta}^{(-1)^{s+1} \prod_{i=1}^{s-1} \Delta_{n_i}} . \tag{3.5.2}$$

Since $\mathfrak{q}$ splits completely in L/K, we can use the norm relation 3.2.9 (adapted to the new situation) to obtain

$$N_{L[\mathfrak{q}]/L}(\hat{\eta}) = N_{F_I[\mathfrak{q}]/L}(\eta_{I'}) = N_{F_I/L}(\eta_I)^{1-\sigma_{s+1}^{-1}} = 1 . \tag{3.5.3}$$

Inserting (3.5.2) into (3.5.3) together with $p \nmid w_K$ implies $N_{L[\mathfrak{q}]/L}(\beta) = 1$, so the first condition of Definition 3.5.3 is satisfied.

For the congruence relation, we need the next

Proposition 3.5.6. *Let $\mathfrak{q} \in \mathcal{Q}_m$, $Q := |\mathcal{O}_K/\mathfrak{q}|$ and let $\mathfrak{q}_{L[\mathfrak{q}]}$ be the product of all primes of $L[\mathfrak{q}]$ above $\mathfrak{q}$. Then*

$$\hat{\eta}^{Q(1-\sigma)} \equiv \eta^{(1-\sigma)\frac{Q-1}{m}} \mod \mathfrak{q}_{L[\mathfrak{q}]} ,$$

where η is the top generator of $\mathcal{C}_L$ and $\hat{\eta}$ is the top generator of $\mathcal{C}_{L[\mathfrak{q}]}$.

Before proving this, we will finish the proof of Theorem 3.5.4. Using the notation from Remark 3.4.14, one can easily show that Proposition 3.5.6 implies

$$\beta^{r(1-\sigma)^2 Q} \equiv \alpha^{r\frac{Q-1}{m}(1-\sigma)} \mod \mathfrak{q}_{L[\mathfrak{q}]} ,$$

where $r = \prod_{i=2}^{s-1} \frac{p^k}{n_i}$. Applying $\Delta_1 = \sum_{i=1}^{p^k-1} i\sigma^i$ and using the facts that $\alpha^{N_1} = 1$, $(1-\sigma)\Delta_1 = N_1 - p^k$ and $(\sigma - 1)N_1 = 0$, we get

$$\beta^{p^k r(1-\sigma)Q} \equiv \alpha^{p^k r\frac{Q-1}{m}} \mod \mathfrak{q}_{L[\mathfrak{q}]} .$$

By dividing out m-th powers, we get that $\beta^{p^k r(1-\sigma)}$ and $\alpha^{p^k r}$ have the same image in $(\mathcal{O}_{L[\mathfrak{q}]}/\mathfrak{q}_{L[\mathfrak{q}]})^\times/m$, since $\frac{Q-1}{m} \equiv 1 \mod m$ by condition (i) on primes in $\mathcal{Q}_m$. Since $r \mid p^{k(s-2)}$, we deduce that $\beta^{1-\sigma}$ and α have the same image in $(\mathcal{O}_{L[\mathfrak{q}]}/\mathfrak{q}_{L[\mathfrak{q}]})^\times/(m/p^{k(s-1)})$. Hence $\varepsilon = \alpha$ and $\varepsilon_\mathfrak{q} = \beta^{1-\sigma}$ satisfy the congruence relation. $\square$

Proof of Proposition 3.5.6. Let $x \in \mathcal{O}_K$ such that $x\mathcal{O}_K = \mathfrak{q}^h$. Let $K_m := K(\zeta_m)$, where ζ_m is a primitive m-th root of unity. Then K_m/K is a constant field extension and hence it is unramified everywhere. Moreover, it is an abelian extension. Now we can define $M := K_m(x^{1/p})$, and since $\mathcal{O}_K^\times = \mu(K)$, $p \nmid |\mu(K)|$ and K_m contains a primitive p-th root of unity, this definition is independent of the choice of the generator x and of its p-th root. Then M/K is a Galois extension.

We claim that x is not a p-th power in K_m. If $x = \alpha^p$, then the valuation of x at $\mathfrak{q}$ would be p-times the valuation of α at $\mathfrak{q}$ since K_m/K is unramified. But $x\mathcal{O}_K = \mathfrak{q}^h$ and as $p \nmid h$, this is a contradiction. Hence the extension M/K_m is cyclic of degree p. For finishing the proof, we need the next

Lemma 3.5.7. *Let $\mathfrak{q} \in \mathcal{Q}_m$ and recall that σ is the unique generator of* $\mathrm{Gal}(L[\mathfrak{q}]/K[\mathfrak{q}])$ *which restricts to the original generator of* $\mathrm{Gal}(L/K)$. *Then there exists a prime $\mathfrak{l}$ of K such that*

(i) $|\mathcal{O}_K/\mathfrak{l}| \equiv 1 \mod m$,

(ii) $\mathfrak{l}$ is unramified in $L[\mathfrak{q}]$ and $(\mathfrak{l}, L[\mathfrak{q}]/K) = \sigma^{-1}$,

(iii) $\mathfrak{q}$ is inert in $K[\mathfrak{l}]/K$.

Proof. By an explicit analysis of the Galois automorphisms, one can check that K_m/K is an abelian extension whereas M/K_m is not. Since $[M : K_m] = p$, there are no intermediate fields and hence K_m/K is the maximal abelian subextension of M. This implies that $M \cap L[\mathfrak{q}] = K_m \cap L[\mathfrak{q}]$, as $L[\mathfrak{q}]/K$ is an abelian extension. Since $K_m \cap L[\mathfrak{q}]$ is unramified and $p \nmid h$, we find $K_m \cap L[\mathfrak{q}] = K$. Then there exists a $\tau \in \mathrm{Gal}(L[\mathfrak{q}] \cdot M/K)$ which restricts to $\sigma^{-1} \in \mathrm{Gal}(L[\mathfrak{q}]/K)$ and to a generator of $\mathrm{Gal}(M/K_m) \subseteq \mathrm{Gal}(M/K)$.

Using a variant of Čebotarev's Density Theorem (cf. [Ros02, Thm. 9.13B]), we see that there exists a prime $\mathfrak{l}$ such that the Frobenius of $\mathfrak{l}$ is the conjugacy class of τ and $|\mathcal{O}_K/\mathfrak{l}| \equiv 1 \mod m$. Then the first two conditions are satisfied and it remains to prove that $\mathfrak{q}$ is inert in $K[\mathfrak{l}]$.

Since τ acts as the identity on K_m, we find that $\mathfrak{l}$ splits completely in K_m/K. Let $\mathfrak{L}$ be a prime of K_m over $\mathfrak{l}$, then $\mathcal{O}_{K_m}/\mathfrak{L} \cong \mathcal{O}_K/\mathfrak{l}$. Moreover, by

$$\langle \tau|_M \rangle = \mathrm{Gal}(M/K_m) \cong \mathbb{Z}/p\mathbb{Z}\,,$$

$\mathfrak{L}$ must be inert in M. It is easily seen that $\mathcal{O}_M/\mathfrak{L}\mathcal{O}_M \cong (\mathcal{O}_{K_m}/\mathfrak{L})[\xi]$, where ξ is the class of $x^{1/p}$ modulo $\mathfrak{L}\mathcal{O}_M$. If x was a p-th power in $(\mathcal{O}_{K_m}/\mathfrak{L})^\times$, this extension would be trivial, hence the inertia degree of $\mathfrak{L}$ would be one. This is a contradiction since $\mathfrak{L}$ is inert in M, so we have shown that x cannot be a p-th power in $(\mathcal{O}_K/\mathfrak{l})^\times$.

Recall that we get $(\mathcal{O}_K/\mathfrak{l})^\times/m \cong \mathrm{Gal}(K[\mathfrak{l}]/K)$ from Artin's Reciprocity Theorem and $p \nmid w_K$. Since x is not a p-th power in $(\mathcal{O}_K/\mathfrak{l})^\times$, it clearly follows that $(x\mathcal{O}_K, K[\mathfrak{l}]/K) = (\mathfrak{q}, K[\mathfrak{l}]/K)^h$ is not a p-th power in $\mathrm{Gal}(K[\mathfrak{l}]/K)$. As $\mathrm{Gal}(K[\mathfrak{l}]/K)$ is cyclic of order m and $p \nmid h$, we obtain that $(\mathfrak{q}, K[\mathfrak{l}]/K)$ generates $\mathrm{Gal}(K[\mathfrak{l}]/K)$ and hence $\mathfrak{q}$ is inert in $K[\mathfrak{l}]$. □

Using the notation from the proof of Theorem 3.5.4 and the prime $\mathfrak{l}$ satisfying the conditions of the previous lemma, we can define the elliptic units

$$\begin{aligned}\eta_{\mathfrak{l}} &:= N_{H_{\mathfrak{l}\mathfrak{m}_I}/L[\mathfrak{l}]}(\alpha_{\mathfrak{l}\mathfrak{m}_I})\,,\\ \hat{\eta}_{\mathfrak{l}} &:= N_{H_{\mathfrak{l}\mathfrak{m}_{I'}}/L[\mathfrak{q}\mathfrak{l}]}(\alpha_{\mathfrak{l}\mathfrak{m}_{I'}})\,,\end{aligned}$$

where $L[\mathfrak{q}\mathfrak{l}]$ is the compositum of $L[\mathfrak{q}]$ and $L[\mathfrak{l}]$. Using the norm relation, we find

$$\begin{aligned}N_{L[\mathfrak{q}\mathfrak{l}]/L[\mathfrak{l}]}(\hat{\eta}_{\mathfrak{l}}) &= \eta_{\mathfrak{l}}^{1-\sigma_{\mathfrak{q}}^{-1}}\,,\\ N_{L[\mathfrak{q}\mathfrak{l}]/L[\mathfrak{q}]}(\hat{\eta}_{\mathfrak{l}}) &= \hat{\eta}^{1-\sigma_{\mathfrak{l}}^{-1}} = \hat{\eta}^{1-\sigma}\,,\\ N_{L[\mathfrak{l}]/L}(\eta_{\mathfrak{l}}) &= \eta^{1-\sigma_{\mathfrak{l}}^{-1}} = \eta^{1-\sigma}\,,\end{aligned}$$

where $\sigma_{\mathfrak{q}} = (\mathfrak{q}, L[\mathfrak{l}]/K)$ and $\sigma_{\mathfrak{l}} = (\mathfrak{l}, L[\mathfrak{q}]/K) = \sigma^{-1}$ by condition (ii).

Since $\mathfrak{q} \in \mathcal{Q}_m$, $\mathfrak{q}$ splits completely in L/K and by condition (iii), the primes of L above $\mathfrak{q}$ are inert in $L[\mathfrak{l}]/L$. Then each prime of $L[\mathfrak{q}]$ above $\mathfrak{q}$ must also be inert in $L[\mathfrak{q}\mathfrak{l}]/L[\mathfrak{q}]$. Moreover, each prime above $\mathfrak{q}$ is unramified in $L[\mathfrak{l}]/L$ and totally ramified in $L[\mathfrak{q}]/L$, therefore it is also totally ramified in $L[\mathfrak{q}\mathfrak{l}]/L[\mathfrak{l}]$ and the product of all primes of $L[\mathfrak{q}\mathfrak{l}]$ above $\mathfrak{q}$ is given by $\mathfrak{q}_{L[\mathfrak{q}]}\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}$. Therefore, we get the following isomorphism of rings

$$\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}/\mathfrak{q}_{L[\mathfrak{q}]}\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]} \cong \mathcal{O}_{L[\mathfrak{l}]}/\mathfrak{q}\mathcal{O}_{L[\mathfrak{l}]}\,.$$

Since $L[\mathfrak{q}]$ and $L[\mathfrak{l}]$ are linearly disjoint over L and $\mathfrak{q}$ splits completely in L/K, we can extend $\sigma_{\mathfrak{q}} \in \mathrm{Gal}(L[\mathfrak{l}]/K)$ to $L[\mathfrak{q}\mathfrak{l}]$ such that this extension (also denoted by $\sigma_{\mathfrak{q}}$) restricts to the identity on $L[\mathfrak{q}]$. In particular, $\sigma_{\mathfrak{q}}$ generates $\mathrm{Gal}(L[\mathfrak{q}\mathfrak{l}]/L[\mathfrak{q}])$.

From the above isomorphism, we get that $\sigma_{\mathfrak{q}}$ acts as raising to the Q-th power on $\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}/\mathfrak{q}_{L[\mathfrak{q}]}\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}$. Moreover, the group $\mathrm{Gal}(L[\mathfrak{q}\mathfrak{l}]/L[\mathfrak{l}])$ is the inertia group at $\mathfrak{q}$ and acts trivially on $\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}/\widetilde{\mathfrak{q}}\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}$. Therefore, we can express the action of the norms $N_{L[\mathfrak{q}\mathfrak{l}]/L[\mathfrak{l}]}$ and $N_{L[\mathfrak{q}\mathfrak{l}]/L[\mathfrak{q}]}$ on $\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}/\mathfrak{q}_{L[\mathfrak{q}]}\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}$ as raising to the power m respectively to the power $\sum_{i=0}^{m-1} Q^i$. As $Q \equiv 1 \mod m$, there exists an integer $r > 0$ such that $\sum_{i=0}^{m-1} Q^i = mr$. Combining our results, we get that

$$\begin{aligned}\hat{\eta}^{Q(1-\sigma)} &\equiv \hat{\eta}_{\mathfrak{l}}^{Qmr} \equiv \eta_{\mathfrak{l}}^{Qr(1-\sigma_{\mathfrak{q}}^{-1})} \equiv \eta_{\mathfrak{l}}^{r(Q-1)} \equiv (\eta_{\mathfrak{l}}^{mr})^{\frac{Q-1}{m}}\\ &\equiv \eta^{(1-\sigma)\frac{Q-1}{m}} \mod \mathfrak{q}_{L[\mathfrak{q}]}\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}\,.\end{aligned}$$

Since the natural map $\mathcal{O}_{L[\mathfrak{q}]}/\mathfrak{q}_{L[\mathfrak{q}]} \longrightarrow \mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}/\mathfrak{q}_{L[\mathfrak{q}]}\mathcal{O}_{L[\mathfrak{q}\mathfrak{l}]}$ is injective, we obtain the desired result. □

This finishes the proof of Proposition 3.5.6 and hence the proof of Theorem 3.5.4 is now complete.

3.6 Annihilating the ideal class group

Using the same notation as before, we define

$$\mu_i := n_{\max M_i} .$$

This is always a power of p and since $M_i \subseteq M_{i+1}$, we get $\mu_i \leq \mu_{i+1}$. We call an index $i \in \{1, ..., k-1\}$ a *jump* if $\mu_i < \mu_{i+1}$. Further, we declare 0 and k to be jumps and set $\mu_0 = 0$. Then we get the next

Lemma 3.6.1. *Let $0 = s_0 < s_1 < ... < s_\kappa = k$ be the ordered sequence of all jumps. Then the set*

$$\bigcup_{t=1}^{\kappa} \{\alpha_{s_t}^{\sigma^i} \mid 0 \leq i < p^{s_t} - p^{s_{t-1}}\}$$

is a $\mathbb{Z}$-basis of $\overline{\mathcal{C}_L}$.

Proof. See [CK19, Lemma 7.1]. □

With this basis, we obtain our next result:

Lemma 3.6.2. *Let r be the highest jump less than k, i.e. $\mu_r < \mu_{r+1} = n_s$. Assume that $\rho \in \mathbb{Z}[\Gamma]$ is such that $\alpha_k^\rho \in \overline{\mathcal{C}_{L_r}}$. Then*

$$(1 - \sigma^{p^r})\rho = 0 .$$

Proof. See [CK19, Lemma 7.2]. □

Now we need an additional condition on the p-power m. We already know that $(m, q) = 1$, since $p \nmid q$, so $q \in (\mathbb{Z}/m\mathbb{Z})^\times$. Let d denote its order, then there exists $i \geq 0$ and $b \in \mathbb{Z}$ with $p \nmid b$ such that

$$q^d - 1 = b \cdot p^i m.$$

If we define $m' := p^i m$, we still have $p^{ks} \mid m'$ and d is the order of q modulo m', so we can assume without loss of generality that $i = 0$. Now we can define f to be the order of q in $(\mathbb{Z}/m^2\mathbb{Z})^\times$.

Lemma 3.6.3. *We have $m \mid \frac{f}{d}$.*

Proof. We have

$$\begin{aligned} q^f &= (q^d)^{f/d} = (1 + bm)^{f/d} \\ &\equiv 1 + \frac{f}{d} bm \mod m^2 . \end{aligned}$$

Since f is the order of q in $(\mathbb{Z}/m^2\mathbb{Z})^\times$, we obtain that the left hand side is congruent to 1 modulo m^2, hence

$$m^2 \mid \frac{f}{d} bm$$

Since $p \nmid b$, this implies

$$m \mid \frac{f}{d} .$$

□

Theorem 3.6.4. *Let m be a power of p such that $m \mid \frac{f}{d}$ and let $V \subseteq L^\times/m$ be a finitely generated $\mathbb{Z}_p[\Gamma]$-submodule. Without loss of generality choose representatives of generators of V which belong to $\mathcal{O}_L$. Suppose there is a map $z\colon V \longrightarrow (\mathbb{Z}/m\mathbb{Z})[\Gamma]$ of $\mathbb{Z}_p[\Gamma]$-modules such that $z(V \cap K^\times) = 0$, where $V \cap K^\times$ means $V \cap (K^\times(L^\times)^m/(L^\times)^m)$. Then for any $\mathfrak{c} \in \mathrm{cl}(\mathcal{O}_L)_p$, there exist infinitely many primes $\mathfrak{Q}$ in L such that:*

(i) $\mathfrak{q} := \mathfrak{Q} \cap K$ *is completely split in* L/K,

(ii) $[\mathfrak{Q}] = \mathfrak{c}$, *where* $[\mathfrak{Q}]$ *is the projection of the ideal class of* $\mathfrak{Q}$ *into* $\mathrm{cl}(L)_p$,

(iii) $Q := |\mathcal{O}_L/\mathfrak{Q}| \equiv 1 + m \mod m^2$,

(iv) for each $j = 1, ..., s$, *the class of* x_j *is an* m*-th power in* $(\mathcal{O}_K/\mathfrak{q})^\times$,

(v) no prime above $\mathfrak{q}$ *is contained in the support of the generators of* V *and there is a* $\mathbb{Z}_p[\Gamma]$*-linear map* $\varphi\colon (\mathcal{O}_L/\mathfrak{q}\mathcal{O}_L)^\times/m \longrightarrow (\mathbb{Z}/m\mathbb{Z})[\Gamma]$ *such that the diagram*

$$\begin{array}{ccc} V & \xrightarrow{\quad z \quad} & (\mathbb{Z}/m\mathbb{Z})[\Gamma] \\ \downarrow{\scriptstyle \psi} & \nearrow{\scriptstyle \varphi} & \\ (\mathcal{O}_L/\mathfrak{q}\mathcal{O}_L)^\times/m & & \end{array}$$

commutes, where ψ *corresponds to the reduction map.*

Remark 3.6.5. The reduction map ψ is defined on the chosen set of generators: Let $x \in \mathcal{O}_L$ be a representative of such a generator, then $\overline{x}$ is the class of $x \in \mathcal{O}_L/\mathfrak{q}\mathcal{O}_L$. Since no prime above $\mathfrak{q}$ is contained in the support of x, we get $\overline{x} \in (\mathcal{O}_L/\mathfrak{q}\mathcal{O}_L)^\times$. Hence, we can set $\psi(x)$ to be the class of $\overline{x}$ in $(\mathcal{O}_L/\mathfrak{q}\mathcal{O}_L)^\times/m$. This yields a well-defined $\mathbb{Z}_p[\Gamma]$-homomorphism.

Proof. Let H_L be the p-Hilbert class field of L, i.e. the abelian extension such that $\mathrm{Gal}(H_L/L)$ is isomorphic to $\mathrm{cl}(\mathcal{O}_L)_p$. Define $L_m := L(\zeta_m)$ and $L_{m^2} := L(\zeta_{m^2})$, where ζ_m (resp. ζ_{m^2}) is a primitive m-th (resp. m^2-th) root of unity. Note that these are constant field extensions, in particular we obtain $L_m = L\mathbb{F}_{q^d}$ and $L_{m^2} = L\mathbb{F}_{q^f}$.

Define $L' := L_m(\ker(z)^{1/m})$, $L'' := L_m(V^{1/m})$ and $M := L_m(P^{1/m})$, where P is the subgroup of $L^\times$ (actually $K^\times$) generated by $x_1, ..., x_s$. Moreover, let $L''_{m^2} := L''L_{m^2}$, $M_{m^2} := ML_{m^2}$ and $L''' := L''_{m^2}M_{m^2}$. We first check that all these extensions are Galois over K.

Let $K_m = K\mathbb{F}_{q^d}$ and $K_{m^2} = K\mathbb{F}_{q^f}$, then $L_m = LK_m$ and $L_{m^2} = LK_{m^2}$ are Galois over K. Since $P \subseteq K$, we clearly get that $\mathrm{Gal}(L_m/K)$ acts (trivially) on P, so the Kummer extension M is Galois over K. Analogously, we need to show that $\mathrm{Gal}(L_m/K)$ acts on $\ker(z)$ (resp. V) to obtain that L' (resp. L'') is Galois over K. Since both $\ker(z)$ and V are subsets of L, it suffices to check that Γ acts on them. For V this is clear since V is a $\mathbb{Z}_p[\Gamma]$-module. Since z is a $\mathbb{Z}_p[\Gamma]$-homomorphism, Γ also acts on the kernel of z. Hence the extensions L' and L'' are Galois over K. Then also the composites with K_m^2 are Galois over K.

Note that by Kummer theory

$$M \cap L'' = L_m(P^{1/m}) \cap L_m(V^{1/m}) = L_m((P \cap V)^{1/m}).$$

Since $V \cap P \subseteq V \cap K^\times \subseteq \ker(z)$, this implies $M \cap L'' \subseteq L'$.

Lemma 3.6.6 (cf. [GK04, Lemma 18]). *(i) L_{m^2} is the maximal abelian subextension of L'''/L.*

(ii) L_m is the maximal abelian subextension of L''/L.

(iii) $L''' \cap H_L = L$.

Proof. (i) We have an exact sequence

$$1 \longrightarrow \mathrm{Gal}(L'''/L_{m^2}) \longrightarrow \mathrm{Gal}(L'''/L) \longrightarrow \mathrm{Gal}(L_{m^2}/L) \longrightarrow 1\,.$$

The group $\mathrm{Gal}(L_{m^2}/L)$ is isomorphic to the unique subgroup H of $(\mathbb{Z}/m^2\mathbb{Z})^\times$ of order f and its action is determined by

$$\sigma_a(\zeta_{m^2}) = \zeta_{m^2}^a\,,$$

where $a \in H$ and σ_a is the corresponding element in $\mathrm{Gal}(L_{m^2}/L)$ under this isomorphism.

By Kummer theory, the extension L'''/L_{m^2} is an abelian p-extension and with the above observations, the action of H on $B := \mathrm{Gal}(L'''/L_{m^2})$ is given by

$$(a, \sigma) \longmapsto \sigma^a\,.$$

Note that we can choose q as a generator of H since f is the order of q in $(\mathbb{Z}/m^2\mathbb{Z})^\times$. Then the coinvariants of B are given by

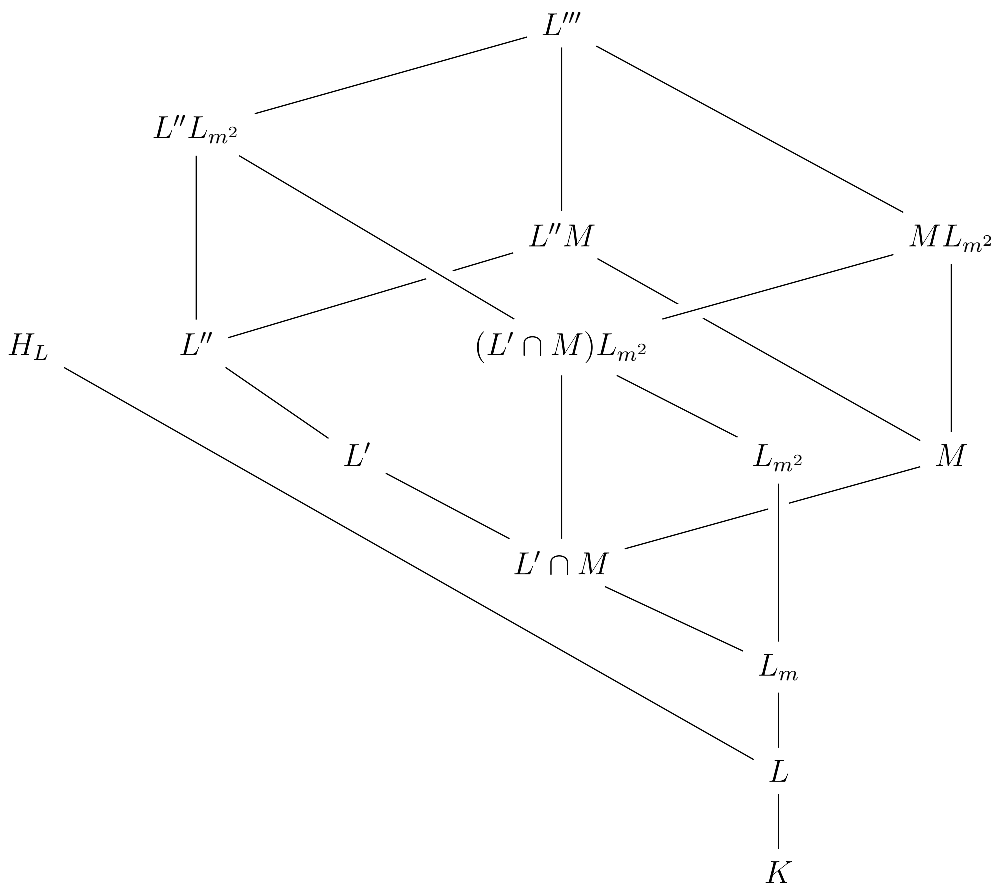
$$B_H = B/I_H B = B/(q-1)B\,.$$

As $p \nmid q - 1 = w_K$ and B is a p-group, we obtain $(q-1)B = B$ and hence the coinvariants vanish. This implies that $\mathrm{Gal}(L'''/L)/B \cong \mathrm{Gal}(L_{m^2}/L)$ is the maximal abelian quotient and hence L_{m^2}/L is the maximal abelian subextension.

(ii) Analogously to (i).

(iii) Since H_L/L is abelian, we obtain $L''' \cap H_L = L_{m^2} \cap H_L$. Since H_L is a real extension of L, this intersection must be contained in the splitting field of ∞ in L_{m^2}. By [Ros02, Prop. 8.13], the splitting field of ∞ in $L_{m^2} = L\mathbb{F}_{q^f}$ is the unique subextension of degree (f, d_∞). By $p \nmid d_\infty$, this subextension has degree prime to p and since H_L is a p-extension, we obtain $H_L \cap L_{m^2} = L$. □

The situation can be illustrated in the following diagram:



Now we want to construct a suitable element $\tau \in \mathrm{Gal}(L'''/L)$ such that the statement of Theorem 3.6.4 follows from an application of Čebotarev's Densitiy Theorem.

For the first step, let $e_0 \in \mathrm{Hom}((\mathbb{Z}/m\mathbb{Z})[\Gamma], \mu_m)$ be given by

$$e_0 \left(\sum_{i=0}^{p^k-1} a_i \sigma^i \right) = \zeta_m^{a_0} .$$

Then e_0 generates $\mathrm{Hom}((\mathbb{Z}/m\mathbb{Z})[\Gamma], \mu_m)$ as a $\mathbb{Z}[\Gamma]$-module and therefore the $\mathbb{Z}$-span of $\sigma^{-j} e_0$, $j = 1, ..., p^k$, is $\mathrm{Hom}((\mathbb{Z}/m\mathbb{Z})[\Gamma], \mu_m)$. Moreover, we obtain from Kummer theory

$$\begin{aligned} \mathrm{Gal}(L''/L') &\cong \ker(\mathrm{Hom}(V, \mu_m) \to \mathrm{Hom}(\ker(z), \mu_m)) \\ &\cong \mathrm{Hom}(\mathrm{im}(z), \mu_m) . \end{aligned}$$

From Baer's criterion (see [Wei94, 2.3.1 and Ex. 2.3.1]) we get that $\mu_m \cong \mathbb{Z}/m\mathbb{Z}$ is injective as a $\mathbb{Z}/m\mathbb{Z}$-module, therefore we get a surjective map

$$\mathrm{Hom}((\mathbb{Z}/m\mathbb{Z})[\Gamma], \mu_m) \twoheadrightarrow \mathrm{Hom}(\mathrm{im}(z), \mu_m) \cong \mathrm{Gal}(L''/L') .$$

Let τ_1 be the image of e_0 under this isomorphism, then τ_1 is a $\mathbb{Z}[\Gamma]$-generator of $\mathrm{Gal}(L''/L')$.

In the second step we want to extend τ_1 to an element $\tau_2 \in \mathrm{Gal}(L''M/L_m)$ which restricts to the identity on M. This is possible if and only if τ_1 is the identity on $M \cap L''$. We already observed that $M \cap L'' \subseteq L'$ and since $\tau_1 \in \mathrm{Gal}(L''/L')$, we clearly have $\tau_1|_{M \cap L''} = \mathrm{id}$.

In the last step, we want to extend τ_2 to an element τ of $\mathrm{Gal}(L'''/L)$ such that $\tau(\zeta_{m^2}) = \zeta_{m^2}^{1+m}$. First we see that this would imply $\tau(\zeta_m) = \zeta_m$ hence we get the necessary condition $\tau_2|_{L_m} = \mathrm{id}$. This is true since $\tau_2 \in \mathrm{Gal}(L''M/L_m)$. Moreover, the order of $\tau|_{L_{m^2}} \in \mathrm{Gal}(L_{m^2}/L_m)$ must be the order of $1+m$ in $(\mathbb{Z}/m^2\mathbb{Z})^\times$, which is m. Hence $[L_{m^2} : L_m] = \frac{f}{d}$ must be divisible by m which is shown in Lemma 3.6.3. A last condition is that $L''M \cap L_{m^2} = L_m$. As L_{m^2} is abelian over L, this follows from Lemma 3.6.6 (ii).

Now since H_L/K and L'''/K are Galois, we find that $H_L L'''/K$ is Galois and we let $\sigma \in \mathrm{Gal}(H_L L'''/K)$ be an element such that $\sigma|_{L'''} = \tau$ and $\sigma|_{H_L} = \sigma_{\mathfrak{c}}$, where $\sigma_{\mathfrak{c}} \in \mathrm{Gal}(H_L/L)$ corresponds to the class $\mathfrak{c} \in \mathrm{cl}(\mathcal{O}_L)_p$. Such an element exists since $H_L \cap L''' = L$ and $\sigma_{\mathfrak{c}}|_L = \mathrm{id} = \tau|_L$. By Čebotarev's Density Theorem (cf. [Ros02, Thm. 9.13A]), there exist infinitely many primes $\mathfrak{q}$ of K such that $(\mathfrak{q}, H_L L'''/K)$ is in the conjugacy class of σ. As the support of the generators of V consists only of finitely many primes, we obtain infinitely many primes $\mathfrak{q}$ such that the primes of L above $\mathfrak{q}$ are not contained in this support. Now we are left to show that these primes satisfy the conditions (i)-(v).

Since $\sigma|_L = \tau|_L = \mathrm{id}$, we get that $\mathfrak{q}$ is completely split in L, so we obtain (i).

We get

$$(\mathfrak{Q}, H_L/L) = (\mathfrak{Q}, H_L L'''/L)|_{H_L} = (\mathfrak{q}, H_L L'''/K)|_{H_L} = \sigma|_{H_L} = \sigma_{\mathfrak{c}}\,,$$

because of (i) hence we obtain (ii).

For (iii), we use the fact that $\sigma|_{L_m} = \tau|_{L_m} = \mathrm{id}$, so $\mathfrak{Q}$ splits completely in L_m. Let $\widetilde{\mathfrak{Q}}$ be a prime of L_m above $\mathfrak{Q}$ and let $\widehat{\mathfrak{Q}}$ be a prime of L_{m^2} above $\widetilde{\mathfrak{Q}}$, then we get

$$\zeta_m^{(\widetilde{\mathfrak{Q}}, L_{m^2}/L_m)} \equiv \zeta_m^{N\widetilde{\mathfrak{Q}}} \mod \widehat{\mathfrak{Q}}$$

by the definition of the Frobenius. Since ζ_m is a constant, this implies

$$\zeta_{m^2}^{(\widetilde{\mathfrak{Q}}, L_{m^2}/L_m)} = \zeta_{m^2}^{N\widetilde{\mathfrak{Q}}}\,.$$

By the properties of the Frobenius element, we obtain

$$(\widetilde{\mathfrak{Q}}, L_{m^2}/L_m) = (\widetilde{\mathfrak{Q}}, H_L L'''/L_m)|_{L_{m^2}} = (\mathfrak{q}, H_L L'''/K)|_{L_{m^2}} = \tau|_{L_{m^2}}\,,$$

so

$$\zeta_{m^2}^{Q} = \zeta_{m^2}^{N\mathfrak{Q}} = \zeta_{m^2}^{N\widetilde{\mathfrak{Q}}} = \zeta_{m^2}^{\tau|_{L_{m^2}}} = \zeta_{m^2}^{1+m}\,.$$

Therefore, we get (iii).

We first observe that since $\mathfrak{q}$ splits completely in L_m, we get $\mathcal{O}_K/\mathfrak{q} \cong \mathcal{O}_{L_m}/\widetilde{\mathfrak{Q}}$. Let $\xi_j \in M$ be an m-th root of x_j and let $\mathfrak{Q}'$ be an ideal of M above $\widetilde{\mathfrak{Q}}$. From

$$(\widetilde{\mathfrak{Q}}, M/L_m) = (\widetilde{\mathfrak{Q}}, H_L L'''/L_m)|_M = (\mathfrak{q}, H_L L'''/K)|_M = \tau|_M = \mathrm{id}\,,$$

we obtain that $\widetilde{\mathfrak{Q}}$ splits completely in M and hence

$$[\xi_j] \in \mathcal{O}_M/\mathfrak{Q}' \cong \mathcal{O}_K/\mathfrak{q}$$

satisfies $[\xi_j]^m = [x_j]$. This is (iv).

For (v) we notice that $(\mathbb{Z}/m\mathbb{Z})[\Gamma]$ is an injective $(\mathbb{Z}/m\mathbb{Z})[\Gamma]$-module (this can be shown with [Wei94, Prop. 3.2.4]), hence it suffices to consider $\mathrm{im}(\psi)$ instead of $(\mathcal{O}_L/\mathfrak{q}\mathcal{O}_L)^\times/m$. Then we obtain the desired map φ from the homomorphism theorem if and only if $\ker(\psi) \subseteq \ker(z)$.

So let $u \in \ker(\psi)$, i.e. u is an m-th power in $(\mathcal{O}_L/\mathfrak{q}\mathcal{O}_L)^\times$. Then by the Chinese Remainder Theorem, u is also an m-th power in $(\mathcal{O}_L/\mathfrak{Q})^\times$ for each prime $\mathfrak{Q}$ of L above $\mathfrak{q}$. Since we have already seen that $\mathfrak{Q}$ splits completely in L_m, u is also an m-th power in $(\mathcal{O}_{L_m}/\widetilde{\mathfrak{Q}})^\times$ for any prime $\widetilde{\mathfrak{Q}}$ above $\mathfrak{Q}$. Considering the extension $L_m(u^{1/m})$, we find that for any prime $\mathfrak{Q}^*$ of $L_m(u^{1/m})$ above $\widetilde{\mathfrak{Q}}$, we get

$$\mathcal{O}_{L_m(u^{1/m})}/\mathfrak{Q}^* = \mathcal{O}_{L_m}/\widetilde{\mathfrak{Q}}(u^{1/m}) = \mathcal{O}_{L_m}/\widetilde{\mathfrak{Q}},$$

so each prime $\mathfrak{Q}$ is completely split in $L_m(u^{1/m})$. Then clearly $\tau|_{L_m(u^{1/m})} = \mathrm{id}$ and since we can do this for any Γ-conjugate of $\mathfrak{Q}$, we obtain the same result for any Γ-conjugate of $\tau|_{L_m(u^{1/m})}$. But by construction, the conjugates of $\tau|_{L''}$ generate $\mathrm{Gal}(L''/L')$, hence $\mathrm{Gal}(L''/L')$ acts trivially on $L_m(u^{1/m})$. Therefore, $L_m(u^{1/m}) \subseteq L'$ and hence $u \in \ker(z)$. This yields (v). □

For the desired annihilation result, we need the next

Theorem 3.6.7 (cf. [Rub87, Thm. (5.1)]). *Let $\mathfrak{q}$ be a prime of K which splits completely in L, set $Q := |\mathcal{O}_K/\mathfrak{q}|$. Let M be a finite extension of L which is abelian over K and such that in M/L, all primes above $\mathfrak{q}$ are totally tamely ramified and no other primes ramify. Write $\mathfrak{q}_M$ for the product of all primes of M above $\mathfrak{q}$ and let $\mathcal{A}$ denote the annihilator in $(\mathbb{Z}/(Q-1)\mathbb{Z})[\Gamma]$ of the cokernel of the reduction map*

$$\{\varepsilon \in \mathcal{O}_M^\times \mid N_{M/L}(\varepsilon) = 1\} \longrightarrow (\mathcal{O}_M/\mathfrak{q}_M)^\times .$$

Write $w := \frac{Q-1}{[M:L]}$. Then $\mathcal{A} \subseteq w(\mathbb{Z}/(Q-1)\mathbb{Z})[\Gamma]$ and for every prime $\mathfrak{Q}$ of L above $\mathfrak{q}$, $w^{-1}\mathcal{A}$ annihilates the ideal class of $\mathfrak{Q}$ in $\mathrm{cl}(\mathcal{O}_L)/[M:L]$.

Proof. The proof of Rubin also works for function fields. □

Now we can prove:

Theorem 3.6.8. *Let m be a power of p divisible by p^{ks} such that $m \mid \frac{f}{d}$. Assume that $\varepsilon \in \mathcal{O}_L$ is m-semispecial and let $V \subseteq L^\times/m$ be a finitely generated $\mathbb{Z}[\Gamma]$-module. Suppose that the class of ε belongs to V. Let $z\colon V \longrightarrow (\mathbb{Z}/m\mathbb{Z})[\Gamma]$ be a $\mathbb{Z}[\Gamma]$-linear map such that $z(V \cap K^\times) = 0$. Then $z(\varepsilon)$ annihilates $\mathrm{cl}(\mathcal{O}_L)_p/(m/p^{k(s-1)})$.*

Proof. Set $m' := m/p^{k(s-1)}$. We must prove that the image of any class $\mathfrak{c} \in \mathrm{cl}(\mathcal{O}_L)_p$ in $\mathrm{cl}(\mathcal{O}_L)_p/m'$ is annihilated by $z(\varepsilon)$. We can apply Theorem 3.6.4 to produce a completely split prime $\mathfrak{Q}$ of L and a prime $\mathfrak{q}$ of K below $\mathfrak{Q}$ which satisfy the properties (i)-(v). Since ε is m-semispecial and $\mathfrak{q} \in \mathcal{Q}_m$ by (iii) and (iv), there exists a unit $\varepsilon_{\mathfrak{q}}$ in $L[\mathfrak{q}]$

with $N_{L[\mathfrak{q}]/L}(\varepsilon_{\mathfrak{q}}) = 1$ and such that the elements ε and $\varepsilon_{\mathfrak{q}}$ have the same image in $(\mathcal{O}_{L[\mathfrak{q}]}/\mathfrak{q}_{L\mathfrak{q}]})^{\times}/m' \cong (\mathcal{O}_L/\mathfrak{q}\mathcal{O}_L)^{\times}/m'$. Applying Theorem 3.6.7 to $M = L[\mathfrak{q}]$, we get that the annihilator $\mathcal{A}$ of $\mathcal{B} := (\mathcal{O}_{L[\mathfrak{q}]}/\mathfrak{q}_{L[\mathfrak{q}]})^{\times}/\langle \mathrm{im}(\varepsilon_{\mathfrak{q}})\rangle$ annihilates the class of $\mathfrak{Q}$ in $\mathrm{cl}(\mathcal{O}_L)/m$. By property (iii), m is the exact p-power dividing $Q-1$, therefore the p-part of $\mathcal{B}$ is

$$\mathcal{B}/m = ((\mathcal{O}_{L[\mathfrak{q}]}/\mathfrak{q}_{L[\mathfrak{q}]})^{\times}/m)/\langle \mathrm{im}(\varepsilon_{\mathfrak{q}})\rangle$$

and the projection $\mathcal{A}_p$ of $\mathcal{A}$ to $(\mathbb{Z}/m\mathbb{Z})[\Gamma]$ is the annihilator of $\mathcal{B}/m$. So $\mathcal{A}_p$ annihilates $[\mathfrak{Q}]$ in $\mathrm{cl}(\mathcal{O}_L)_p/m$.

From this, we obtain that $\mathcal{A}'$, the projection of $\mathcal{A}_p$ to $(\mathbb{Z}/m'\mathbb{Z})[\Gamma]$, annihilates $[\mathfrak{Q}]$ in $\mathrm{cl}(\mathcal{O}_L)_p/m'$. Since $(\mathcal{O}_{L[\mathfrak{q}]}/\mathfrak{q}_{L[\mathfrak{q}]})^{\times}/m$ is free cyclic over $(\mathbb{Z}/m\mathbb{Z})[\Gamma]$, it follows that $\mathcal{A}'$ is the annihilator of $\mathcal{B}/m'$.

Therefore, we have to show that $z(\varepsilon) \in \mathcal{A}'$. Since ε and $\varepsilon_{\mathfrak{q}}$ have the same image in $(\mathcal{O}_{L[\mathfrak{q}]}/\mathfrak{q}_{L[\mathfrak{q}]})^{\times}/m'$, $\mathcal{A}'$ is also the annihilator of

$$((\mathcal{O}_{L[\mathfrak{q}]}/\mathfrak{q}_{L[\mathfrak{q}]})^{\times}/m')/\langle \mathrm{im}(\varepsilon)\rangle = ((\mathcal{O}_L/\mathfrak{q}\mathcal{O}_L)^{\times}/m')/\langle \psi(\varepsilon)\rangle\,,$$

where ψ is the reduction map from Theorem 3.6.4 considered modulo m'. Using the diagram from property (v), we get that $\varphi(\psi(\varepsilon)) \in \mathcal{A}'$, since $(\mathcal{O}_L/\mathfrak{q}\mathcal{O}_L)^{\times}/m'$ is $(\mathbb{Z}/m'\mathbb{Z})[\Gamma]$-cyclic (for more details, see the last paragraph in [GK04]).Therefore, $z(\varepsilon) \in \mathcal{A}'$ and we are done. □

The main result of this chapter is the next

Theorem 3.6.9. *Let r be the highest jump less than k. Then we have*

$$\mathrm{Ann}_{\mathbb{Z}[\Gamma]}((\mathcal{O}_L^{\times}/\overline{\mathcal{C}_L})_p) \subseteq \mathrm{Ann}_{\mathbb{Z}[\Gamma]}((1-\sigma^{p^r})\,\mathrm{cl}(\mathcal{O}_L)_p)\,.$$

The number r is determined by $p^{k-r} = \max\{t_j : j \in J\}$, where the set J is defined as $J = \{j \in \{1, ..., s\} : n_j = n_s\}$.

Proof. The proof of [CK19, Thm. 7.5] can be used without any changes. □

Chapter 4

A Solomon-type conjecture for totally real number fields

In this chapter we formulate a conjectural generalization of [Sol92, Thm. 2.1] for totally real number fields. We also prove the equivalence of this conjecture to the Iwasawa-theoretic Mazur-Rubin-Sano conjecture, which is formulated in the first section. Since the IMRS is a consequence of the eTNC (see [BKS16, Thm. 5.16]), the conjectural statements presented in Section 4.2 are also implied by the eTNC.

4.1 The Iwasawa-theoretic Mazur-Rubin-Sano conjecture

Let K be a number field, fix an odd prime p and set S_p to be the set of places of K above p. Let L_∞ be a Galois extension of K such that $\mathcal{G} := \mathrm{Gal}(L_\infty/K) = \Delta \times \Gamma$, where Δ is a finite abelian group and $\Gamma \cong \mathbb{Z}_p$. Then we define $L := L_\infty^\Gamma$, so L is a finite abelian extension of K with $G := \mathrm{Gal}(L/K) \cong \Delta$, and $K_\infty := L_\infty^\Delta$, so K_∞ is a $\mathbb{Z}_p$-extension of K and $\mathrm{Gal}(K_\infty/K) \cong \Gamma$. We denote the n-th level of this $\mathbb{Z}_p$-extension by K_n and set $L_n = LK_n$. Let $\mathcal{G}_n := \mathrm{Gal}(L_n/K)$ and $\Gamma_n := \mathrm{Gal}(L_n/L) \cong \mathbb{Z}/p^n\mathbb{Z}$, so $\mathcal{G}_n \cong \Delta \times \Gamma_n$. Define $I(\Gamma)$ (resp. $I(\Gamma_n)$) to be the augmentation ideal of $\mathbb{Z}_p[[\Gamma]]$ (resp. $\mathbb{Z}_p[\Gamma_n]$).

Let $S \supseteq S_\infty(K) \cup S_{ram}(L/K) \cup S_p$ and T be finite sets of places satisfying Hypotheses 2.2.1 and 2.3.1. Let V be the set of places in S which split completely in L_∞ and V' be the set of places in S which split completely in L. Then $V \subseteq V'$ and we set $r := |V|$, $r' := |V'|$ and $e := r' - r$. We use the ordering introduced in Section 2.4.2, i.e. $S = \{v_0, ..., v_n\}, V = \{v_0, ..., v_{r-1}\}$ and $V' = \{v_0, ..., v_{r-1}, v_r, ..., v_{r'-1}\}$. Let $W := \{w_r, ..., w_{r'-1}\}$ be the set of chosen primes of L over $V' \setminus V$ used in the formulation of the Rubin-Stark conjecture.

For the rest of this section we work under the following

Hypothesis 4.1.1. For each level n, the p-component of the Rubin-Stark conjecture $\mathrm{RS}(L_n/K, S, T, r)_p$ with S, T and r as above holds.

For the statement of the conjecture, we need to introduce three more maps.

We start with the canonical embedding from [San14, Lemma 2.11]

$$\bigcap^r U_{L,S,T} \longrightarrow \bigcap^r U_{L_n,S,T}$$

which induces an injection

$$\nu_n\colon \bigcap^r U_{L,S,T} \otimes_{\mathbb{Z}_p} I(\Gamma_n)^e/I(\Gamma_n)^{e+1} \longrightarrow \bigcap^r U_{L_n,S,T} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\Gamma_n]/I(\Gamma_n)^{e+1}\,.$$

Secondly, we define I_Γ (resp. I_{Γ_n}) to be the kernel of the map $\mathbb{Z}_p[[\mathcal{G}]] \longrightarrow \mathbb{Z}_p[G]$ (resp. $\mathbb{Z}_p[\mathcal{G}_n] \longrightarrow \mathbb{Z}_p[G]$). For any place $w \in W$, we fix a place w_∞ of L_∞ above w. Then on each level n, we can use the place w_n of L_n below w_∞ to define the local reciprocity map $\mathrm{rec}_w := \mathrm{rec}_{w_n} : L^\times \longrightarrow \Gamma_n$. This induces a map

$$\begin{aligned} \mathrm{Rec}_w\colon L^\times &\longrightarrow I_{\Gamma_n}/I_{\Gamma_n}^2 \\ x &\longmapsto \sum_{\sigma\in G}(\mathrm{rec}_w(\sigma(x)) - 1)\sigma^{-1}\,. \end{aligned}$$

Consider the isomorphism from [San14, Eq. (3)]

$$\begin{aligned} \mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p} I(\Gamma_n)/I(\Gamma_n)^2 &\xrightarrow{\cong} I_{\Gamma_n}/I_{\Gamma_n}^2 \\ \sigma \otimes \overline{a} &\longmapsto \overline{\tilde{\sigma} a}\,, \end{aligned} \tag{4.1.1}$$

where $\overline{a}$ denotes the image of $a \in I(\Gamma_n)$ modulo $I(\Gamma_n)^2$ and $\tilde{\sigma} \in \mathcal{G}_n$ is an arbitrary lift of $\sigma \in G \cong \mathcal{G}_n/\Gamma_n$. Then $\bigwedge_{w\in W} \mathrm{Rec}_w$ induces a homomorphism

$$\mathrm{Rec}_n\colon \bigcap^{r'} U_{L,S,T} \longrightarrow \bigcap^r U_{L,S,T} \otimes_{\mathbb{Z}_p} I(\Gamma_n)^e/I(\Gamma_n)^{e+1}$$

by [San14, Prop. 2.7]. Taking the limit over n we get

$$\mathrm{Rec}_W\colon \bigcap^{r'} U_{L,S,T} \longrightarrow \bigcap^r U_{L,S,T} \otimes_{\mathbb{Z}_p} \varprojlim I(\Gamma_n)^e/I(\Gamma_n)^{e+1} \cong \bigcap^r U_{L,S,T} \otimes_{\mathbb{Z}_p} I(\Gamma)^e/I(\Gamma)^{e+1}\,.$$

The third map will be

$$\begin{aligned} \mathcal{N}_n\colon \bigcap^r U_{L_n,S,T} &\longrightarrow \bigcap^r U_{L_n,S,T} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\Gamma_n]/I(\Gamma_n)^{e+1} \\ a &\longmapsto \sum_{\sigma\in\Gamma_n} \sigma a \otimes \sigma^{-1}\,. \end{aligned}$$

Now we can state

Conjecture 4.1.2 (IMRS$(L/K, S, T, r)_p$)**.** *There exists a*

$$\xi = (\xi_n)_n \in \bigcap^r U_{L,S,T} \otimes_{\mathbb{Z}_p} I(\Gamma)^e/I(\Gamma)^{e+1}$$

such that

$$\nu_n(\xi_n) = \mathcal{N}_n(\eta_{L_n,S,T})$$

for all $n \geq 1$ *and*

$$e_{S,r'}\xi = (-1)^{re} e_{S,r'} \mathrm{Rec}_W(\eta_{L,S,T}) \text{ in } e_{S,r'}\mathbb{Q}_p \bigcap^r U_{L,S,T} \otimes_{\mathbb{Z}_p} I(\Gamma)^e/I(\Gamma)^{e+1}\,.$$

Remark 4.1.3. (i) Note that the conjecture in [BKS17] is formulated for a single character. In the above formulation, the characters with $r_{S,\chi} = r'$ are combined in the idempotent $e_{S,r'}$.

(ii) If such an element ξ exists, it is unique since the maps ν_n are injective.

(iii) By [BKS17, Prop. 4.4(iv)], we can restrict ourselves to the case that $V' \setminus V \subseteq S_p$.

4.2 A Solomon-type conjecture

Now let K be a totally real number field and let L_∞ be an extension as in the previous section such that the extension K_∞/K is indeed the cyclotomic $\mathbb{Z}_p$-extension. In this case, the extension L_∞/L is also the cyclotomic extension.

Remark 4.2.1. If Leopoldt's conjecture is true for K, then the cyclotomic extension is the only $\mathbb{Z}_p$-extension of K, so the above choice is in fact no restriction in this case.

We additionally suppose that at least one place of K splits completely in L_∞, i.e. $r \geq 1$, and at least one place splits completely in L but not in L_∞, i.e. $e \geq 1$. In this section, we replace Hypothesis 4.1.1 by

Hypothesis 4.2.2. For each level n, the Stark conjecture $\mathrm{St}(L_n/K, S)$ with S as before holds.

We hence obtain a Stark unit $\varepsilon_{L_n,S} \in \mathcal{O}_{L_n,S}^\times$ for each n. Note that this is only defined up to a root of unity. Nevertheless, since L_∞ and hence L can be embedded into $\mathbb{R}$, we have $\mu(L) = \{\pm 1\}$ and since $e \geq 1$ (so $r' \geq 2$), we get $N_{L_n/L}(\varepsilon_{L_n,S}) \in \mu(L)$. Therefore, we can normalize the Stark units by requiring $N_{L_n/L}(\varepsilon_{L_n,S}) = 1$ for each n. These normalized Stark units then form a norm coherent sequence by Proposition 2.4.9.

4.2.1 Solomon's κ-construction

Now we apply the construction of [Sol92] in our case. For this, we need

Conjecture 4.2.3. *For each n there exists an element $\beta_{L_n,S} \in L_n^\times/L^\times$ such that $\beta_{L_n,S}^{(\gamma-1)^e} = \varepsilon_{L_n,S}$.*

Remark 4.2.4. This is true for $e = 1$ by Hilbert's Theorem 90.

Lemma 4.2.5. *If such a $\beta_{L_n,S}$ exists, it is unique.*

Proof. For $e = 1$, this is again Hilbert's Theorem 90, so we assume $e > 1$. Suppose that we find $b_{L_n,S}, b'_{L_n,S} \in L_n$ satisfying

$$b_{L_n,S}^{(\gamma-1)^e} = \varepsilon_{L_n,S} = (b'_{L_n,S})^{(\gamma-1)^e} .$$

Hence, we get for $\alpha := \frac{b_{L_n,S}}{b'_{L_n,S}}$ that $\alpha^{(\gamma-1)^e} = 1$, so $\alpha^{(\gamma-1)^{e-1}} \in L^\times$. Therefore, we find

$$1 = N_{L_n/L}(\alpha^{(\gamma-1)^{e-1}}) = (\alpha^{(\gamma-1)^{e-1}})^{p^n}$$

and since $\mu(L) = \pm 1$, we get that $\alpha^{(\gamma-1)^{e-1}} = 1$. Inductively, we obtain that $\alpha^{\gamma-1} = 1$, so $\alpha \in L^\times$. $\square$

Hypothesis 4.2.6. For the rest of this section, we assume that Conjecture 4.2.3 holds.

Then we can define $\kappa_{L,S,n} := N_{L_n/L}(\beta_{L_n,S}) \in L^\times/(L^\times)^{p^n}$. By abuse of notation, we let

$$\begin{aligned} \mathrm{ord}_{\mathfrak{Q}} : L^\times/(L^\times)^{p^n} &\longrightarrow \mathbb{Z}/p^n\mathbb{Z} \\ \overline{x} &\longmapsto \overline{\mathrm{ord}_{\mathfrak{Q}}(x)} \end{aligned}$$

for any place $\mathfrak{Q}$ of L. Then we obtain the following properties:

Lemma 4.2.7. *(i)* $\kappa_{L,S,n} \equiv \kappa_{L,S,m} \mod (L^\times)^{p^m}$ *for all* $m \leq n$.

(ii) For all primes $\mathfrak{Q}$ *of* L *coprime to* p*, we have* $\mathrm{ord}_{\mathfrak{Q}}(\kappa_{L,S,n}) = 0$ *in* $\mathbb{Z}/p^n\mathbb{Z}$*.*

Proof. (i) We find with Proposition 2.4.9 and Lemma 2.4.1 (ii)

$$N_{L_n/L_m}(\beta_{L_n,S})^{(\gamma-1)^e} = N_{L_n/L_m}(\beta_{L_n,S}^{(\gamma-1)^e}) = N_{L_n/L_m}(\varepsilon_{L_n,S}) = \varepsilon_{L_m,S}\,.$$

Hence, the uniqueness from Lemma 4.2.5 implies $\beta_{L_m,S} = N_{L_n/L_m}(\beta_{L_n,S}) \in L_m^\times/L^\times$. Then by definition we get

$$\begin{aligned} \kappa_{L,S,m} &= N_{L_m/L}(\beta_{L_m,S}) = N_{L_m/L}(N_{L_n/L_m}(\beta_{L_n,S})) = N_{L_n/L}(\beta_{L_n,S}) \\ &= \kappa_{L,S,n} \in L^\times/(L^\times)^{p^m}\,. \end{aligned}$$

(ii) Define $b_n^{(d)} := \beta_{L_n,S}^{(\gamma-1)^{e-d}}$ for $d = 0, ..., e-1$, i.e. $b_n^{(0)} = \varepsilon_{L_n,S}$. Note that $b_n^{(d)} \in L_n^\times$ is independent of the choice of representative of $\beta_{L_n,S}$. We now use induction to prove that $b_n^{(d)}$ is an S_p-unit for $d = 0, ..., e-1$.

For $d = 0$, this is part (ii) of $\mathrm{St}(L/K, S)$: Since we have a completely split infinite place, either $|S| \geq 3$, hence $\varepsilon_{L_n,S} \in \mathcal{O}_{L_n}^\times$, or $S = \{\infty, \mathfrak{p}\}$, where $\mathfrak{p}$ is the unique prime of K over p. Then $\varepsilon_{L_n,S} \in \mathcal{O}_{L_n,S}^\times = \mathcal{O}_{L_n,S_p}^\times$.

So let $d > 0$ and suppose that $b_n^{(d-1)} \in \mathcal{O}_{L_n,S_p}^\times$. Using the Kolyvagin derivative $D = \sum_{i=0}^{p^n-1} i\gamma^i$, which satisfies $(\gamma-1)D = p^n - N_{L_n/L}$, we obtain

$$(b_n^{(d-1)})^D = (b_n^{(d)})^{(\gamma-1)D} = \frac{(b_n^{(d)})^{p^n}}{N_{L_n/L}(b_n^{(d)})}\,.$$

Since $d < e$, we get that

$$N_{L_n/L}(b_n^{(d)}) = N_{L_n/L}(\beta_{L_n,S}^{(\gamma-1)^{e-d}}) = 1\,.$$

So for any prime $\mathfrak{Q}_n \nmid p$ we get

$$p^n\,\mathrm{ord}_{\mathfrak{Q}_n}(b_n^{(d)}) = \mathrm{ord}_{\mathfrak{Q}_n}((b_n^{(d-1)})^D) = 0$$

as $b_n^{(d-1)} \in \mathcal{O}_{L_n,S_p}^\times$ and hence also $b_n^{(d)} \in \mathcal{O}_{L_n,S_p}^\times$.

Now let $\mathfrak{Q}$ be a prime of L coprime to p. Then $\mathfrak{Q}$ is unramified in L_n/L and we fix a prime $\mathfrak{Q}_n$ of L_n over $\mathfrak{Q}$. Now we can copy the proof of [Sol92, Prop. 2.2], i.e. we compute

$$(b_n^{(e-1)})^D = \beta_{L_n,S}^{(\gamma-1)D} = \beta_{L_n,S}^{p^n - N_{L_n/L}} = \frac{\beta_{L_n,S}^{p^n}}{N_{L_n/L}(\beta_{L_n,S})} .$$

This implies

$$\begin{aligned} \mathrm{ord}_{\mathfrak{Q}}(\kappa_{L,S,n}) &\equiv \mathrm{ord}_{\mathfrak{Q}_n}(N_{L_n/L}(\beta_{L_n,S})) \equiv -\,\mathrm{ord}_{\mathfrak{Q}_n}((b_n^{(e-1)})^D) \\ &\equiv 0 \mod p^n . \end{aligned}$$

□

The Lemma enables us to define

$$\kappa_{L,S} := (\kappa_{L,S,n})_n \in \varprojlim_n \mathcal{O}_{L,S}^\times/(\mathcal{O}_{L,S}^\times)^{p^n} \cong \mathbb{Z}_p \mathcal{O}_{L,S}^\times = U_{L,S} .$$

Remark 4.2.8. If $r \geq 2$, we clearly have $L_S'(\chi, 0) = 0$ for all characters $\chi \in \widehat{\mathcal{G}}$ and hence $\varepsilon_{L_n,S} = 1$ for all n. Therefore, we get $\beta_{L_n,S} = 1$ and also $\kappa_{L,S,n} = 1$ for all n, so $\kappa_{L,S}$ is trivial in this case. This approach can hence only be interesting if $r = 1$ and we will work under this assumption from now on.

4.2.2 Cyclotomic character

For each $n \geq 0$ let ζ_n be a primitive p^{n+1}-th root of unity. We assume that these satisfy $\zeta_{n+1}^p = \zeta_n$. We consider the local extensions $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$ and set $\mathbb{Q}_p(\zeta_\infty) = \bigcup_{n\geq 0} \mathbb{Q}_p(\zeta_n)$. Then an element $\sigma \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_\infty)/\mathbb{Q}_p)$ is uniquely determined by its action on ζ_n for all n, i.e. we find elements $a_{\sigma,n} \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ such that $\sigma(\zeta_n) = \zeta_n^{a_{\sigma,n}}$. Taking the limit over n, we then get $a_\sigma = (a_{\sigma,n})_n \in \mathbb{Z}_p^\times$, such that

$$\sigma(\zeta_n) = \zeta_n^{a_\sigma}$$

for all n. This relation defines the *cyclotomic character*

$$\begin{aligned} \chi_{cyc} \colon \mathrm{Gal}(\mathbb{Q}_p(\zeta_\infty)/\mathbb{Q}_p) &\xrightarrow{\cong} \mathbb{Z}_p^\times \\ \sigma &\longmapsto a_\sigma . \end{aligned}$$

Considering the cyclotomic extension $\mathbb{Q}_{p,\infty}/\mathbb{Q}_p$, we find that

$$\mathrm{Gal}(\mathbb{Q}_{p,\infty}/\mathbb{Q}_p) \cong \mathrm{Gal}(\mathbb{Q}_p(\zeta_\infty)/\mathbb{Q}_p(\zeta_0)) \subseteq \mathrm{Gal}(\mathbb{Q}_p(\zeta_\infty)/\mathbb{Q}_p)$$

and the cyclotomic character induces an isomorphism

$$\begin{aligned} \chi_{cyc} \colon \mathrm{Gal}(\mathbb{Q}_{p,\infty}/\mathbb{Q}_p) &\longrightarrow 1 + p\mathbb{Z}_p \\ \sigma &\longmapsto \chi_{cyc}(\widetilde{\sigma}) , \end{aligned}$$

where $\widetilde{\sigma}$ is the lift of σ obtained from the above isomorphism, i.e. $\widetilde{\sigma}|_{\mathbb{Q}_p(\zeta_0)} = \mathrm{id}$.

Considering the local reciprocity map $\mathrm{rec}_p \colon \mathbb{Z}_p^\times \longrightarrow \mathrm{Gal}(\mathbb{Q}_p(\zeta_\infty)/\mathbb{Q}_p)$, we get from [Neu11, Part II, Thm. (7.16)]

$$\chi_{cyc}(\mathrm{rec}_p(x)) = x^{-1} . \tag{4.2.1}$$

4.2.3 The valuations at the split primes above p

Returning to our number fields, recall that we assume $r = 1$ and we will denote the unique archimedean place which splits completely in L_∞ by v_0, i.e. $V = \{v_0\}$. we refine the ordering of the set $V' = \{v_0, v_1, ..., v_{e_p}, ..., v_e\}$ by assuming without loss of generality that $(V' \setminus V) \cap S_p = \{v_1, ..., v_{e_p}\}$, i.e. the first e_p places in $V' \setminus V$ lie over p. Hence, these places correspond to prime ideals $\mathfrak{p}_1, ..., \mathfrak{p}_{e_p}$ of K over p. Finally, we set $S_i := S \setminus \{v_i\}$ and $\hat{V} = \{v_{e_p+1}, ..., v_e\} = V' \setminus (V \cup S_p)$.

Then we see that $L_{\mathfrak{P}_i}$ is a finite extension of $\mathbb{Q}_p$ for each $i = 1, ..., e_p$. Completing L_∞ at the unique prime above $\mathfrak{P}_i$, we get the cyclotomic $\mathbb{Z}_p$-extension of $L_{\mathfrak{P}_i}$, i.e. the field $L_{\mathfrak{P}_i,\infty} := L_{\mathfrak{P}_i}\mathbb{Q}_{p,\infty}$. Let $k := L_{\mathfrak{P}_i} \cap \mathbb{Q}_{p,\infty}$, then we get

$$\Gamma \cong \mathrm{Gal}(L_{\mathfrak{P}_i,\infty}/L_{\mathfrak{P}_i}) \cong \mathrm{Gal}(\mathbb{Q}_{p,\infty}/k) \subseteq \mathrm{Gal}(\mathbb{Q}_{p,\infty}/\mathbb{Q}_p)\,.$$

Now fix a topological generator γ of Γ, then we can use the above identification to read γ as an element of $\mathrm{Gal}(\mathbb{Q}_{p,\infty}/\mathbb{Q}_p)$. Hence, we can apply χ_{cyc} to γ and obtain an element of $1 + p\mathbb{Z}_p$. Applying the p-adic logarithm, this defines a unique element

$$\omega := \log_p(\chi_{cyc}(\gamma)) \in p\mathbb{Z}_p\,.$$

For each $i = 1, ..., e_p$, we obtain a Stark element $\eta_{L,S_i} \in \mathbb{Q}\bigwedge^e \mathcal{O}_{L,S_i}^\times$. By (2.2.1) this must be of the form $\lambda^{(i)}u_1^{(i)} \wedge \cdots \wedge u_e^{(i)}$ for some $\lambda^{(i)} \in \mathbb{Q}$ and elements $u_1^{(i)}, ..., u_e^{(i)} \in \mathcal{O}_{L,S_i}^\times$.

Inspired by our definitions of Rec and Ord, we set for any prime $\mathfrak{P}$ of L above p

$$\begin{aligned} \mathrm{Log}_{\mathfrak{P}} \colon L^\times &\longrightarrow \mathbb{Q}_p[G] \\ x &\longmapsto \sum_{\sigma\in G} \log_p(N_{L_{\mathfrak{P}}/\mathbb{Q}_p}(\sigma(x)))\sigma^{-1}\,. \end{aligned}$$

Moreover, by abuse of notation we denote the p-adic completion of $\mathrm{Ord}_{\mathfrak{P}}$ also by $\mathrm{Ord}_{\mathfrak{P}}$ for any $\mathfrak{P}$ of L above p, i.e. we define

$$\begin{aligned} \mathrm{Ord}_{\mathfrak{P}} : U_{L,S} = \mathbb{Z}_p\mathcal{O}_{L,S}^\times &\longrightarrow \mathbb{Z}_p[G] \\ \alpha \otimes u &\longmapsto \alpha \otimes \mathrm{Ord}_{\mathfrak{P}}(u)\,. \end{aligned}$$

For a place $\mathfrak{p} \in \widehat{V}$ and the corresponding fixed place $\mathfrak{P}$ of L above $\mathfrak{p}$, the decomposition group of $\mathfrak{P}$ in Γ is generated by the Frobenius $\sigma_{\mathfrak{P}} \in \Gamma$. This is indeed a unique element of Γ since $\mathfrak{P}$ is unramified in L_∞, hence there exists an $n_{\mathfrak{P}} \in \mathbb{Z}_p$ such that $\sigma_{\mathfrak{P}} = \gamma^{n_{\mathfrak{P}}}$.

Now we can formulate our main conjecture:

Conjecture 4.2.9. *For all $i = 1, ..., e_p$, we have*

$$\mathrm{Ord}_{\mathfrak{P}_i}(\kappa_{L,S}) = (-1)^{i+e_p}\frac{2\lambda^{(i)}}{\omega^{e_p}} \det \left(\frac{\left(\mathrm{Log}_{\mathfrak{P}_\beta}(u_\alpha^{(i)})\right)_{\substack{1\le\beta\le e_p\\1\le\alpha\le e}}}{\left(n_{\mathfrak{P}_\beta}\,\mathrm{Ord}_{\mathfrak{P}_\beta}(u_\alpha^{(i)})\right)_{\substack{e_p+1\le\beta\le e\\1\le\alpha\le e}}} \right) \in \mathbb{Z}_p[G]\,.$$

In particular, if $V' \setminus V \subseteq S_p$, we get $e = e_p$ and hence for all $i = 1, ..., e$

$$\mathrm{Ord}_{\mathfrak{P}_i}(\kappa_{L,S}) = (-1)^{i+e}\frac{2\lambda^{(i)}}{\omega^{e}} \det \left(\mathrm{Log}_{\mathfrak{P}_\beta}(u_\alpha^{(i)})\right)_{\substack{1\le\beta\le e\\1\le\alpha\le e}} \in \mathbb{Z}_p[G]\,.$$

Remark 4.2.10. We will see in the next section that the right hand side is in fact the explicit computation of

$$(-1)^e e_{S,r'}(\mathrm{Ord}_{\mathfrak{P}_i} \circ \mathrm{Rec}_W)(\eta_{L,S,T}),$$

hence it is clearly independent of the choice of $\lambda^{(i)}$ and $u_\alpha^{(i)}$.

Example 4.2.11. Consider the case $K = \mathbb{Q}$, then L will be a totally real abelian extension of $\mathbb{Q}$. Suppose that p is completely split in L. Let $S = \{\infty, p\}$ and f be the conductor of L, then $L_n \subseteq \mathbb{Q}(\zeta_{fp^{(n+1)}})$ and hence $\varepsilon_{L_n,S} = N_{\mathbb{Q}(\zeta_{fp^{(n+1)}})/L_n}(1 - \zeta_{fp^{(n+1)}})$ (see Remark 2.2.7). Since $V' \setminus V = S_p = \{p\}$, we get $e = 1$ and hence Conjecture 4.2.3 is true by Hilbert's Theorem 90. Therefore, the elements $\kappa_{L,S,n}$ can be constructed as above. On the other hand $\eta_{L,S_1} = \frac{1}{2}\varepsilon_{L,S\setminus\{p\}} = \frac{1}{2}N_{\mathbb{Q}(\zeta_f)/L}(1 - \zeta_f)$, so the statement of Conjecture 4.2.9 is

$$\mathrm{ord}_{\mathfrak{P}}(\kappa_{L,S}) = -\frac{\log_p(\iota_{\mathfrak{P}}(N_{\mathbb{Q}(\zeta_f)/L}(1 - \zeta_f)))}{\log_p(\chi_{cyc}(\gamma))},$$

where $\mathfrak{P}$ is any place of L above p and $\iota_{\mathfrak{P}} : L \longrightarrow L_{\mathfrak{P}} \cong \mathbb{Q}_p$ is the embedding corresponding to $\mathfrak{P}$. This is exactly the result of Solomon (see [Sol92, Thm. 2.1]).

Remark 4.2.12. In fact, we could also formulate Conjecture 4.2.9 if K is an imaginary quadratic field. Then we still have only one completely split infinite place, so the statement will probably be non-trivial. Then L_∞ is not necessarily the cyclotomic extension. Indeed if p is split in K and L_∞ is the $\mathbb{Z}_p$-extension, which is unramified at one of the primes over p, we recover (under some additional assumptions) exactly [Ble04, Thm. 3.4]. If p is non-split, we find that L_∞ is a subfield of the ray class field $K(\mathfrak{f}\mathfrak{p}^\infty) = \bigcup_n K(\mathfrak{f}\mathfrak{p}^n)$, where $\mathfrak{f}$ is the conductor of L. In this case, the corresponding formulation of Conjecture 4.2.9 is a consequence of [BH20, Thm. 2.7] (again under additional assumptions). This, together with the case $K = \mathbb{Q}$, may be considered as a first theoretical evidence.

4.2.4 The remaining primes

So far we determined (at least conjecturally) the order of $\kappa_{L,S}$ at the primes of L, which are coprime to p and at the primes above $\mathfrak{p}_i$ for $i = 1, ..., e_p$. Hence, we are left to consider the primes of L above the primes in $S_p \setminus V'$. Fix such a prime $\mathfrak{q} \in S_p \setminus V'$ and let $\mathfrak{Q}$ be a prime of L above $\mathfrak{q}$. Let $D_\mathfrak{q} \subseteq G$ be the decomposition group of $\mathfrak{q}$. With the identification $G \cong \Delta$, we obtain a corresponding subgroup of Δ and we set $L'_\infty = L_\infty^{D_\mathfrak{q}}$ and $L' = L^{D_\mathfrak{q}}$. Then L'_∞ is the cyclotomic $\mathbb{Z}_p$-extension of L' and we let L'_n be the n-th level of this extension (so $L'_n = L_n^{D_\mathfrak{q}}$ with the canonical identification $G \cong \mathrm{Gal}(L_n/K_n)$).

Proposition 4.2.13. *If Conjecture 4.2.3 holds for L', then we get* $\mathrm{ord}_\mathfrak{Q}(\kappa_{L,S}) = 0$.

Proof. We find that Hypothesis 4.2.2 for L' is implied by the hypothesis for L, so we can assume that this hypothesis holds. Then for each n, we obtain a Stark unit $\varepsilon_{L'_n,S}$ and by Proposition 2.4.9 we get $\varepsilon_{L'_n,S} = N_{L_n/L'_n}(\varepsilon_{L_n,S})$. Hence if Conjecture 4.2.3 is true for L, then we can set $\alpha_{L'_n,S} = N_{L_n/L'_n}(\beta_{L_n,S})$ and find $\varepsilon_{L'_n,S} = \alpha_{L'_n,S}^{(\gamma-1)^e}$. Note that the sets V' and V may change when moving from L to L', hence we obtain $e' \geq e$ places in S which are completely split in L' but not in L'_∞. If we assume that Conjecture 4.2.3 holds for L', then we obtain elements $\beta_{L'_n,S} \in (L'_n)^\times/(L')^\times$ satisfying $\beta_{L'_n,S}^{(\gamma-1)^{e'}} = \varepsilon_{L'_n,S}$. Then as in the proof of Lemma 4.2.5 we get $\alpha_{L'_n,S} = \beta_{L'_n,S}^{(\gamma-1)^{e'-e}}$ in $(L'_n)^\times/(L')^\times$ and hence

$$\kappa_{L',S,n}^{(\gamma-1)^{e'-e}} \equiv N_{L'_n/L'}(\alpha_{L'_n,S}) \equiv N_{L/L'}(\kappa_{L,S,n}) \mod ((L')^\times)^{p^n} .$$

With Lemma 4.2.7, we get

$$\kappa_{L',S}^{(\gamma-1)^{e'-e}} = N_{L'/L}(\kappa_{L,S}) \in U_{L',S}$$

and from [Neu92, Ch. III, Thm. (1.2)]

$$f(\mathfrak{Q}/\mathfrak{Q}') \cdot \mathrm{ord}_{\mathfrak{Q}}(\kappa_{L,S}) = \mathrm{ord}_{\mathfrak{Q}'}(N_{L/L'}(\kappa_{L,S})) = \mathrm{ord}_{\mathfrak{Q}'}(\kappa_{L',S}^{(\gamma-1)^{e'-e}}) .$$

If there is a second place $v \in S$, which is completely split in L'_∞, we find $\kappa_{L',S} = 1$ by Remark 4.2.8, so $\mathrm{ord}_{\mathfrak{Q}}(\kappa_{L,S}) = 0$ in this case. If we still have only one place, which is completely split in L'_∞, we see that $e' > e$, since there is at least one additional prime which splits completely in L', namely the place $\mathfrak{q}$. But then

$$\kappa_{L',S}^{(\gamma-1)^{e'-e}} = 1 ,$$

so we find again $\mathrm{ord}_{\mathfrak{Q}}(\kappa_{L,S}) = 0$. □

4.2.5 A T-modified version

For a T-modified version, we use that $\mathrm{St}(L_n/K, S)$ implies $\mathrm{RS}(L_n/K, S, T, 1)$ by Corollary 2.4.2 and consider the Rubin-Stark elements $\eta_{L_n,S,T} \in \mathcal{O}_{L_n,S,T}^\times$ for $n \geq 1$. If we assume Conjecture 4.2.3, we find elements $\beta_{L_n,S,T}^2 \in L_n^\times/L^\times$ such that $(\beta_{L_n,S,T}^2)^{(\gamma-1)^e} = \eta_{L_n,S,T}^2$ by setting $\beta_{L_n,S,T}^2 = \beta_{L_n,S}^{\delta_T(0)}$. Defining $\kappa_{L,S,T,n}^2 := N_{L_n/L}(\beta_{L_n,S,T}^2)$ we find $\kappa_{L,S,T,n}^2 = \kappa_{L,S,n}^{\delta_T(0)}$ and hence $\kappa_{L,S,T,n}^2 \in \mathcal{O}_{L,S,T}^\times$ by Lemma 4.2.7 and 2.3.3 (iii). Taking the limit, we get $\kappa_{L,S,T}^2 = (\kappa_{L,S,T,n}^2)_n \in U_{L,S,T}$. Since p is odd, 2 is invertible in $\mathbb{Z}_p$ and we can define $\kappa_{L,S,T} := \frac{1}{2} \otimes \kappa_{L,S,T}^2 \in U_{L,S,T}$.

Remark 4.2.14. If T contains a place v with $\sigma_v = 1$, then $\delta_T(0)/2 \in \mathbb{Z}[G]$ so we can directly define $\beta_{L_n,S,T} = \beta_{L_n,S}^{\delta_T(0)/2}$ (and analogously for $\kappa_{L,S,T,n}$ and $\kappa_{L,S,T}$) in this case.

As before, we get a Rubin-Stark element $\eta_T^{(i)} := \eta_{L,S_i,T} \in \mathbb{Q} \bigwedge^e \mathcal{O}_{L,S_i,T}^\times$ for each $i = 1, ..., e$. By (2.3.1), this must be of the form $\lambda_T^{(i)} u_{1,T}^{(i)} \wedge \cdots \wedge u_{e,T}^{(i)}$ for some $\lambda_T^{(i)} \in \mathbb{Q}$ and elements $u_{1,T}^{(i)}, ..., u_{e,T}^{(i)} \in \mathcal{O}_{L,S_i,T}^\times$. Then the T-version of Conjecture 4.2.9 is

Conjecture 4.2.15. *For all $i = 1, ..., e_p$, we have*

$$\mathrm{Ord}_{\mathfrak{P}_i}(\kappa_{L,S,T}) = (-1)^{i+e_p} \frac{\lambda_T^{(i)}}{\omega^{e_p}} \det \left(\frac{\left(\mathrm{Log}_{\mathfrak{P}_\beta}(u_{\alpha,T}^{(i)})\right)_{\substack{1\leq\beta\leq e_p \\ 1\leq\alpha\leq e}}}{\left(n_{\mathfrak{P}_\beta} \mathrm{Ord}_{\mathfrak{P}_\beta}(u_{\alpha,T}^{(i)})\right)_{\substack{e_p+1\leq\beta\leq e \\ 1\leq\alpha\leq e}}} \right) \in \mathbb{Z}_p[G] .$$

In particular, if $V' \setminus V \subseteq S_p$ we get for all $i = 1, ..., e$

$$\mathrm{Ord}_{\mathfrak{P}_i}(\kappa_{L,S,T}) = (-1)^{i+e} \frac{\lambda_T^{(i)}}{\omega^e} \det \left(\mathrm{Log}_{\mathfrak{P}_\beta}(u_{\alpha,T}^{(i)})\right)_{\substack{1\leq\beta\leq e \\ 1\leq\alpha\leq e}} \in \mathbb{Z}_p[G] .$$

4.3 Relation of the conjectures

Throughout this section, we assume that Hpothesis 4.2.2 is true. We first relate Conjecture 4.2.9 with its T-version:

Lemma 4.3.1. *Conjecture 4.2.9 is equivalent to Conjecture 4.2.15 for all sets T satisfying Hypothesis 2.3.1.*

Proof. This follows directly from Lemma 2.4.1, the fact that

$$\kappa_{L,S,T} = \kappa_{L,S}^{\delta_T(0)/2}$$

and [Tat84, Ch. IV, Lemme 1.1]. □

In the rest of this section, we will prove the major theoretical evidence for Conjecture 4.2.9:

Theorem 4.3.2. *Assume that Conjecture 4.2.3 holds for any subfield of L. Then Conjecture 4.2.15 is equivalent to* $\mathrm{IMRS}(L/K, S, T, 1)_p$ *(Conjecture 4.1.2).*

For the proof of the theorem, we first state a reformulation of $\mathrm{IMRS}(L/K, S, T, 1)_p$ from [BH21]. Their approach starts with [BH21, Conj. (3.2)] for general Euler systems and arbitrary rank r. In our special case of Rubin-Stark elements and $r = 1$, this can be formulated as

Conjecture 4.3.3. *Let $\eta_{S,T} := (\eta_{L_n,S,T})_n \in \varprojlim_n U_{L_n,S,T} = U_{L_\infty,S,T}$ be the limit of the norm-coherent sequence of Rubin-Stark elements. Then*

$$\eta_{S,T} \in I_\Gamma^e U_{L_\infty,S,T}\,.$$

Remark 4.3.4. Bullach and Hofer proved the validity of the above conjecture under certain assumptions, a list can be found in [BH21, Thm. (3.5)]. In particular, Conjecture 4.3.3 is a consequence of a variant of the Iwasawa Main Conjecture (see [BH21, Remark (3.6)]).

Lemma 4.3.5. *Conjecture 4.2.3 is equivalent to Conjecture 4.3.3 for all sets T satisfying Hypothesis 2.3.1.*

Proof. First assume that Conjecture 4.2.3 holds. Then as in the proof of Lemma 4.2.7, we can show that $\beta_{L_n,S}^{\gamma-1} \in \mathcal{O}_{L_n,S}^\times$. Define $\alpha_{n,m} := N_{L_m/L_n}(\beta_{L_n,S})$ for $m \geq n$, then a similar computation as in the proof of Lemma 4.2.7 shows that $\alpha_{n,m} \in \mathcal{O}_{L_n,S}^\times$ and hence $\alpha_{n,m,T}^2 := \alpha_{n,m}^{\delta_T(0)} \in \mathcal{O}_{L_n,S,T}^\times$ by Lemma 2.3.3 (iii). Note that

$$N_{L_m/L_{m'}}(\beta_{L_m,S}) \equiv \beta_{L_{m'},S} \mod (L^\times)^{p^{m-m'}}$$

for all $m \geq m'$ and hence

$$\alpha_{n,m,T}^2 \equiv \alpha_{n,m',T}^2 \mod (\mathcal{O}_{L_n,S,T}^\times)^{p^{m-m'}}\,.$$

Therefore, we can define

$$\lambda_{n,T}^2 := (\alpha_{n,m,T}^2)_{m\geq n} \in \varprojlim_m \frac{\mathcal{O}_{L_n,S,T}^\times}{(\mathcal{O}_{L_n,S,T}^\times)^{p^{m-n}}} = U_{L_n,S,T}$$

and

$$\lambda_{n,T} := \frac{1}{2} \otimes \lambda_{n,T}^2 \in U_{L_n,S,T} .$$

By definition, the sequence $(\lambda_{n,T})_n$ is norm coherent and we get with Lemma 2.4.1

$$\begin{aligned}\lambda_{n,T}^{(\gamma-1)^e} &= \frac{1}{2} \otimes ((\alpha_{n,m,T}^2)^{(\gamma-1)^e})_{m\geq n} = \frac{1}{2} \otimes (N_{L_m/L_n}(\beta_{L_m,S}^{(\gamma-1)^e})^{\delta_T(0)})_{m\geq n} \\ &= \frac{1}{2} \otimes (N_{L_m/L_n}(\varepsilon_{L_m,S})^{\delta_T(0)})_{m\geq n} = \frac{1}{2} \otimes (\varepsilon_{L_n,S}^{\delta_T(0)})_{m\geq n} = (\eta_{L_n,S,T})_{m\geq n} .\end{aligned}$$

Therefore, $(\lambda_{n,T})_n^{(\gamma-1)^e} = \eta_{S,T}$, so Conjecture 4.3.3 holds.

For the other implication, we assume that $\eta_{S,T} \in I_\Gamma^e U_{L_\infty,S,T}$. This implies, that there exists a norm coherent sequence $(\lambda_{n,T})_n$ such that $\lambda_{n,T}^{(\gamma-1)^e} = \eta_{L_n,S,T}$ in $U_{L_n,S,T}$. With the identification already used in the first part of the proof, we find elements $\alpha_{n,m,T} \in \mathcal{O}_{L_n,S,T}^\times$ such that

$$\lambda_{n,T} = (\alpha_{n,m,T})_{m\geq n} \in \varprojlim_m \frac{\mathcal{O}_{L_n,S,T}^\times}{(\mathcal{O}_{L_n,S,T}^\times)^{p^{m-n}}} ,$$

and hence

$$\eta_{L_n,S,T} = u_{n,T}^{(0)} \alpha_{n,2n,T}^{(\gamma-1)^e}$$

for some $u_{n,T}^{(0)} \in (\mathcal{O}_{L_n,S,T}^\times)^{p^n}$. Since this holds for all sets T satisfying Hypothesis 2.3.1, we can choose $T = \{v\}$ for some $v \notin S$ such that $\sigma_v = 1$ and hence by Lemma 2.4.1, we find $\eta_{L_n,S,T} = \varepsilon_{L_n,S}^{(1-Nv)/w_{L_n}}$. With enough sets of this form, we can apply [Tat84, Ch. IV, Lemme 1.1] to write $w_{L_n} = \sum_i a_i(1 - Nv_i)$ and hence

$$\begin{aligned}\varepsilon_{L_n,S} &= \prod_i \varepsilon_{L_n,S}^{a_i \frac{1-Nv_i}{w_{L_n}}} = \prod_i \eta_{L_n,S,T_i}^{a_i} = \underbrace{\prod_i (u_{n,T_i}^{(0)})^{a_i}}_{=:u_n^{(0)}} \cdot \Big(\underbrace{\prod_i \alpha_{n,2n,T_i}^{a_i}}_{=:\alpha_{n,2n}} \Big)^{(\gamma-1)^e} \\ &= u_n^{(0)} \alpha_{n,2n}^{(\gamma-1)^e} ,\end{aligned}$$

where $\alpha_{n,2n} \in \mathcal{O}_{L_n,S}^\times$ and $u_n^{(0)} \in (\mathcal{O}_{L_n,S}^\times)^{p^n}$. Since $N_{L_n/L}(\varepsilon_{L_n,S}) = 1$, we can apply Hilbert's Theorem 90 to obtain an element $\beta_n^{(1)} \in L_n^\times/L^\times$ such that $(\beta_n^{(1)})^{\gamma-1} = \varepsilon_{L_n,S}$. Then we define $u_n^{(1)} := \frac{\beta_n^{(1)}}{\alpha_{n,2n}^{(\gamma-1)^{e-1}}} \in L_n^\times/L^\times$ and obtain

$$u_n^{(0)} = (u_n^{(1)})^{\gamma-1} .$$

Therefore, we have

$$(u_n^{(1)})^{\gamma} = u_n^{(1)} u_n^{(0)} \quad \Longrightarrow \quad (u_n^{(1)})^{\gamma^i} = u_n^{(1)} \prod_{j=0}^{i-1} (u_n^{(0)})^{\gamma^j}$$

and we compute

$$\begin{aligned} N_{L_n/L}(\beta_n^{(1)}) = N_{L_n/L}(u_n^{(1)}) = \prod_{i=0}^{p^n-1} (u_n^{(1)})^{\gamma^i} &= \prod_{i=0}^{p^n-1} u_n^{(1)} \prod_{j=0}^{i-1} (u_n^{(0)})^{\gamma^j} \\ &= (u_n^{(1)})^{p^n} \prod_{i=0}^{p^n-1} \prod_{j=0}^{i-1} (u_n^{(0)})^{\gamma^j} \in (L_n^\times)^{p^n} \cap L^\times = (L^\times)^{p^n} . \end{aligned}$$

Hence, we find a representative $b_n^{(1)}$ of $\beta_n^{(1)}$ such that $N_{L_n/L}(b_n^{(1)}) = 1$. Applying Hilbert's Theorem 90 again, we find an element $\beta_n^{(2)} \in L_n^\times$ such that $(\beta_n^{(2)})^{\gamma-1} = b_n^{(1)}$. Defining $u_n^{(2)} := \frac{\beta_n^{(2)}}{\alpha_{n,2n}^{(\gamma-1)^{e-2}}} \in L_n^\times / L^\times$, we obtain

$$u_n^{(1)} = (u_n^{(2)})^{\gamma-1} .$$

A similar computation as before shows that

$$N_{L_n/L}(\beta_n^{(2)}) \in (L_n^\times)^{p^n} \cap L^\times = (L^\times)^{p^n} ,$$

so we can choose a representative $b_n^{(2)}$ with $N_{L_n/L}(b_n^{(2)}) = 1$. This procedure can be applied until we obtain $\beta_n^{(e)} \in L_n^\times / L^\times$ satisfying $(\beta_n^{(e)})^{(\gamma-1)^e} = \varepsilon_{L_n,S}$. □

By [BH21, Prop. 3.13], $\mathrm{IMRS}(L/K, S, T, 1)_p$ is equivalent to

Conjecture 4.3.6. *Conjecture 4.3.3 holds and*

$$e_{S,r'} \cdot \lambda_{0,T} \otimes (\gamma - 1)^e = (-1)^e e_{S,r'} \operatorname{Rec}_W(\eta_{L,S,T}) \tag{4.3.1}$$

in $e_{S,r'} U_{L,S,T} \otimes_{\mathbb{Z}_p} I(\Gamma)^e / I(\Gamma)^{e+1}$*, where* $(\lambda_{n,T})_n$ *is the norm coherent sequence satisfying* $\lambda_{n,T}^{(\gamma-1)^e} = \eta_{L_n,S,T}$ *in* $U_{L_n,S,T}$ *for all* $n \geq 1$.

In fact, the equation (4.3.1) can be considered as an equality in a certain submodule of $e_{S,r'} U_{L,S,T} \otimes_{\mathbb{Z}_p} I(\Gamma)^e / I(\Gamma)^{e+1}$ related to the module of *universal norms* UN_0^1 of rank 1 and level 0 introduced in [BD21]. The universal norms of rank t and level n are defined as

$$\mathrm{UN}_n^t := \bigcap_{m \geq n} \left(\bigwedge^t N_{L_m/L_n} \right) \left(\bigcap^t U_{L_m,S,T} \right) \subseteq \bigcap^t U_{L_n,S,T} ,$$

so in our special case we obtain

$$\mathrm{UN}_0^1 = \bigcap_{m \geq 0} N_{L_m/L}(U_{L_m,S,T}) \subseteq U_{L,S,T} .$$

Lemma 4.3.7. *(i) For a character χ with $r_{S,\chi} = r'$, we get* $\dim_{\mathbb{Q}_p(\chi)}(\mathbb{Q}_p(\chi)\mathrm{UN}_0^1) = 1$.

(ii) For a character χ with $r_{S,\chi} = r'$ and any $i \in \{1, ..., e_p\}$, we get

$$e_{[\chi]}\mathbb{Q}_p[G]\mathrm{UN}_0^1 \cap e_{[\chi]} \ker(\mathrm{Ord}_{\mathfrak{P}_i}) = 0\,.$$

Proof. Part (i) is [BH21, Lemma (3.1)(c)]. For part (ii), it clearly suffices to construct a non-trivial element $x \in \mathbb{Q}_p(\chi)\mathrm{UN}_0^1$ which is not contained in $e_{[\chi]} \ker(\mathrm{Ord}_{\mathfrak{P}_i})$ (recall that $e_{[\chi]}\mathbb{Q}_p[G] \cong \mathbb{Q}_p(\chi)$). This is done in the proof of [BH21, Lemma (3.16)] and the hypothesis $e = 1$ is not used for this construction. We repeat the argument briefly: Let h_L be the class number of L and let x be a generator of $\mathfrak{P}_i^{h_L}$. Then $e_{[\chi]} \mathrm{Ord}_{\mathfrak{P}_i}(x) = h_L e_{[\chi]} \neq 0$, so it remains to proof that $x \in \mathbb{Q}_p\mathrm{UN}_0^1$. Since $\mathfrak{P}_i \mid p$ and L_∞/L is the cyclotomic $\mathbb{Z}_p$-extension, $\mathfrak{P}_i$ is totally ramified in each L_n. Denoting the unique prime ideal of L_n over $\mathfrak{P}_i$ by $\mathfrak{P}_{i,n}$, we get $\mathfrak{P}_i = N_{L_n/L}(\mathfrak{P}_{i,n})$ and hence $x \in N_{L_n/L}(\mathcal{O}_{L_n,S}^\times)$ for each n. Therefore, $x \in \mathbb{Q}_p\mathrm{UN}_0^1$ (see [BD21, Lemma 3.10]). □

We now repeat the first part of the proof of [BH21, Lemma (3.15)], to show that (4.3.1) can be considered as an equality in $e_{S,r'}\mathbb{Q}_p\mathrm{UN}_0^1 \otimes_{\mathbb{Z}_p} I(\Gamma)^e/I(\Gamma)^{e+1}$. We will see that the assumption $e = 1$ is not necessary for this part. This is clear for the left hand side since $\lambda_{0,T}$ is a universal norm by construction. The map $e_{S,r'}\mathbb{Q}_p \mathrm{Rec}_W$ on the right hand side is either the zero map, then clearly $0 \in e_{S,r'}\mathrm{UN}_0^1 \otimes_{\mathbb{Z}_p} I(\Gamma)^e/I(\Gamma)^{e+1}$. If it is not the zero map, we find at least one character χ such that $e_\chi \mathrm{Rec}_W$ (and hence $e_{[\chi]} \mathrm{Rec}_W$) is non-zero. Applying [BKS16, Lemma 4.2] to

$$\Psi := \bigoplus_{\mathfrak{P}\in W} e_{[\chi]} \mathrm{Rec}_{\mathfrak{P}} : \mathbb{Q}_p(\chi)U_{L,S,T} \longrightarrow \bigoplus_{\mathfrak{P}\in W} \mathbb{Q}_p(\chi)\,,$$

we get that Ψ is surjective and

$$\begin{aligned}\mathrm{im}&\left(e_{[\chi]} \mathrm{Rec}_W \colon \mathbb{Q}_p(\chi) \bigwedge^{r'} U_{L,S,T} \longrightarrow \mathbb{Q}_p(\chi)U_{L,S,T} \otimes_{\mathbb{Z}_p} I(\Gamma)^e/I(\Gamma)^{e+1}\right)\\ &= \ker(\Psi) \otimes I(\Gamma)^e/I(\Gamma)^{e+1}\,.\end{aligned}$$

Clearly $\mathbb{Q}_p(\chi)\mathrm{UN}_0^1 \subseteq \ker(e_{[\chi]} \mathrm{Rec}_{\mathfrak{P}})$ for all $\mathfrak{P} \in W$, i.e. $\mathbb{Q}_p(\chi)\mathrm{UN}_0^1 \subseteq \ker(\Psi)$. Since Ψ is surjective, we get

$$\dim_{\mathbb{Q}_p(\chi)}(\ker(\Psi)) = r_{S,\chi} - e = r' - (r' - r) = r = 1\,,$$

so $\ker(\Psi) = \mathbb{Q}_p(\chi)\mathrm{UN}_0^1$ and the right hand side is indeed an element of $e_{S,r'}\mathbb{Q}_p\mathrm{UN}_0^1 \otimes_{\mathbb{Z}_p} I(\Gamma)^e/I(\Gamma)^{e+1}$.

With the Lemma above, we get that $\mathrm{Ord}_{\mathfrak{P}_i}$ is injective on this module for any $i = 1, ..., e_p$, hence (4.3.1) is equivalent to

$$e_{S,r'} \mathrm{Ord}_{\mathfrak{P}_i}(\lambda_{0,T}) \otimes (\gamma - 1)^e = (-1)^e e_{S,r'}(\mathrm{Ord}_{\mathfrak{P}_i} \circ \mathrm{Rec}_W)(\eta_{L,S,T})\,.$$

Note that $\mathrm{Ord}_{\mathfrak{P}_i}$ on the left hand side is indeed the equivariant valuation map acting on elements of $L^\times$ (resp. $\mathbb{Z}_pL^\times$), whereas $\mathrm{Ord}_{\mathfrak{P}_i}$ on the right hand side is an induced map acting on elements in an exterior power (cf. Section 2.1.2).

The proof of Lemma 4.3.5 shows that $\lambda_{0,T} = \kappa_{L,S,T}$. Considering the right hand side, we get from the homomorphism (2.1.1) that

$$\mathrm{Ord}_{\mathfrak{P}_i} \circ \mathrm{Rec}_W = (-1)^e \,\mathrm{Rec}_W \circ \mathrm{Ord}_{\mathfrak{P}_i} \ .$$

Then by Proposition 2.4.7, we find

$$\mathrm{Ord}_{\mathfrak{P}_i}(\eta_{L,S,T}) = (-1)^i \eta_{L,S_i,T} = (-1)^i \eta_T^{(i)} \ .$$

Hence, we are left to compute $\mathrm{Rec}_W(\eta_T^{(i)})$. As before, let $\eta_T^{(i)} = \lambda_T^{(i)} u_{1,T}^{(i)} \wedge \cdots \wedge u_{e,T}^{(i)}$. Then by (2.1.2),

$$\mathrm{Rec}_W(\eta_T^{(i)}) = \lambda_T^{(i)} \det(\mathrm{Rec}_{\mathfrak{P}_\beta}(u_{\alpha,T}^{(i)}))_{1\le \alpha,\beta \le e} \, .$$

With the isomorphism (4.1.1), we get for any $x \in L^\times$

$$\mathrm{Rec}_{\mathfrak{P}_\beta}(x) = \sum_{\sigma\in G} (\mathrm{rec}_{\mathfrak{P}_\beta}(\sigma(x)) - 1)\sigma^{-1} = \sum_{\sigma \in G} \sigma^{-1} \otimes (\mathrm{rec}_{\mathfrak{P}_\beta}(\sigma(x)) - 1)\, .$$

Since γ is a generator of Γ, we know that $\mathrm{rec}_{\mathfrak{P}_\beta}(x)$ is a (p-adic) power of γ. Therefore, for any $x \in L^\times$ we can define $s(x) \in \mathbb{Z}_p$ by $\mathrm{rec}_{\mathfrak{P}_\beta}(x) = \gamma^{s(x)}$.

Lemma 4.3.8. *For $x \in L^\times$, we have*

$$s(x) = \begin{cases} -\frac{1}{\omega}\log_p(N_{L_{\mathfrak{P}_\beta}/\mathbb{Q}_p}(x)), & 1 \le \beta \le e_p, \\ n_{\mathfrak{P}_\beta}\,\mathrm{ord}_{\mathfrak{P}_\beta}(x) & e_p + 1 \le \beta \le e. \end{cases}$$

Proof. First consider the case that $e_p + 1 \le \beta \le e$, then $\mathfrak{P}_\beta$ is unramified in L_∞/L, hence the local reciprocity map is determined by the Frobenius $\sigma_{\mathfrak{P}_\beta} = \gamma^{n_{\mathfrak{P}_\beta}}$ associated to $\mathfrak{P}_\beta$ and the valuation of x. We hence get

$$\mathrm{rec}_{\mathfrak{P}_\beta}(x) = \gamma^{n_{\mathfrak{P}_\beta}\,\mathrm{ord}_{\mathfrak{P}_\beta}(x)} \, .$$

Now let $1 \le \beta \le e_p$. From local class field theory, we know that the local reciprocity map is a surjection $L_{\mathfrak{P}_\beta}^\times \twoheadrightarrow \mathrm{Gal}(L_{\mathfrak{P}_\beta,\infty}/L_{\mathfrak{P}_\beta})$ and we denote its kernel by $V_{\mathfrak{P}_\beta}$. Since $L_{\mathfrak{P}_\beta,\infty}$ is a totally ramified p-extension, it suffices to consider principal units, i.e. we even get a surjection $1+\mathfrak{P}_\beta\mathcal{O}_{L_{\mathfrak{P}_\beta}} \twoheadrightarrow \mathrm{Gal}(L_{\mathfrak{P}_\beta,\infty}/L_{\mathfrak{P}_\beta})$ with kernel $V_{\mathfrak{P}_\beta}^{(1)} := V_{\mathfrak{P}_\beta} \cap 1 + \mathfrak{P}_\beta\mathcal{O}_{L_{\mathfrak{P}_\beta}}$. Analogously, we obtain for each level n surjections $L_{\mathfrak{P}_\beta}^\times \twoheadrightarrow \mathrm{Gal}(L_{\mathfrak{P}_\beta,n}/L_{\mathfrak{P}_\beta})$ with kernel $V_{\mathfrak{P}_\beta,n}$ and $1 + \mathfrak{P}_\beta\mathcal{O}_{L_{\mathfrak{P}_\beta}} \twoheadrightarrow \mathrm{Gal}(L_{\mathfrak{P}_\beta,n}/L_{\mathfrak{P}_\beta})$ with kernel $V_{\mathfrak{P}_\beta,n}^{(1)} := V_{\mathfrak{P}_\beta,n} \cap 1 + \mathfrak{P}_\beta\mathcal{O}_{L_{\mathfrak{P}_\beta}}$. As we have seen in Section 4.2.2, the local reciprocity map for $\mathbb{Q}_p$ is an isomorphism $1 + p\mathbb{Z}_p \longrightarrow \mathrm{Gal}(\mathbb{Q}_{p,\infty}/\mathbb{Q}_p)$, whose inverse is related to the cyclotomic character (see (4.2.1)). On the n-th level, this isomorphism restricts to $\frac{1+p\mathbb{Z}_p}{1+p^{n+1}\mathbb{Z}_p} \longrightarrow \mathrm{Gal}(\mathbb{Q}_{p,n}/\mathbb{Q}_p)$. By [Neu11, Part II, Thm. (5.10)], we hence obtain for each n the following commutative diagram:

$$\begin{array}{ccccccc}
\Gamma_n & \xrightarrow{\ \cong\ } & \mathrm{Gal}(L_{\mathfrak{P}_\beta,n}/L_{\mathfrak{P}_\beta}) & \hookrightarrow & \mathrm{Gal}(\mathbb{Q}_{p,n}/\mathbb{Q}_p) & & \\
\Big\uparrow & & {\scriptstyle \mathrm{rec}_{\mathfrak{P}_\beta}}\Big\uparrow{\scriptstyle\cong} & & {\scriptstyle\cong}\Big\downarrow{\scriptstyle (-)^{-1}\circ\chi_{cyc}} & & \\
{\scriptstyle \mathrm{rec}_{\mathfrak{P}_\beta}} & & 1+\mathfrak{P}_\beta\mathcal{O}_{L_{\mathfrak{P}_\beta}}/V_{\mathfrak{P}_\beta,n}^{(1)} & \xrightarrow{N_{L_{\mathfrak{P}_\beta}/\mathbb{Q}_p}} & \frac{1+p\mathbb{Z}_p}{1+p^{n+1}\mathbb{Z}_p} & \xrightarrow[\cong]{\log_p} & \frac{p\mathbb{Z}_p}{p^{n+1}\mathbb{Z}_p} \\
\Big| & & {\scriptstyle\cong}\Big\uparrow & & {\scriptstyle\cong}\Big\uparrow & & \\
L^\times & \longrightarrow & L_{\mathfrak{P}_\beta}^\times/V_{\mathfrak{P}_\beta,n} & \xrightarrow{N_{L_{\mathfrak{P}_\beta}/\mathbb{Q}_p}} & \mathbb{Q}_p/\langle p^{\mathbb{Z}}\rangle \times \mu_{p-1} \times (1+p^{n+1}\mathbb{Z}_p) & &
\end{array}$$

Note that the extension $L_{\mathfrak{P}_\beta}/\mathbb{Q}_p$ (and hence $L_{\mathfrak{P}_\beta,n}/\mathbb{Q}_p$) might not be normal. In this case, one can consider the normal closure of $L_{\mathfrak{P}_\beta}$ (resp. $L_{\mathfrak{P}_\beta,n}$) to apply [Neu11, Part II, Thm. (5.10)]. However, we still end up with a diagram as above. Now we can take inverse limits and since this is left exact, we obtain

$$\begin{array}{ccccccc}
\Gamma & \xrightarrow{\cong} & \mathrm{Gal}(L_{\mathfrak{P}_\beta,\infty}/L_{\mathfrak{P}_\beta}) & \hookrightarrow & \mathrm{Gal}(\mathbb{Q}_{p,\infty}/\mathbb{Q}_p) & & \\
\Big\uparrow & & {\scriptstyle \mathrm{rec}_{\mathfrak{P}_\beta}}\Big\uparrow{\scriptstyle \cong} & & {\scriptstyle \cong}\Big\downarrow{\scriptstyle (-)^{-1}\circ\chi_{cyc}} & & \\
{\scriptstyle \mathrm{rec}_{\mathfrak{P}_\beta}} & & 1+\mathfrak{P}_\beta\mathcal{O}_{L_{\mathfrak{P}_\beta}}/V^{(1)}_{\mathfrak{P}_\beta} & \xrightarrow{N_{L_{\mathfrak{P}_\beta}/\mathbb{Q}_p}} & 1+p\mathbb{Z}_p & \xrightarrow[\cong]{\log_p} & p\mathbb{Z}_p \\
\Big| & & {\scriptstyle \cong}\Big\uparrow & & {\scriptstyle \cong}\Big\uparrow & & \\
L^\times & \longrightarrow & L^\times_{\mathfrak{P}_\beta}/V_{\mathfrak{P}_\beta} & \xrightarrow{N_{L_{\mathfrak{P}_\beta}/\mathbb{Q}_p}} & \mathbb{Q}_p/\langle p^{\mathbb{Z}}\rangle \times \mu_{p-1} & &
\end{array} \tag{4.3.2}$$

We immediately see that the norm maps in the middle and bottom line must be injective. Recall that for any $x \in L^\times$ we defined $s(x) \in \mathbb{Z}_p$ by $\mathrm{rec}_{\mathfrak{P}_\beta}(x) = \gamma^{s(x)}$. Then x can be embedded into $L^\times_{\mathfrak{P}_\beta}$ and there exists $y \in 1+\mathfrak{P}_\beta\mathcal{O}_{L_{\mathfrak{P}_\beta}}$ such that

$$\mathrm{rec}_{\mathfrak{P}_\beta}(y) = \mathrm{rec}_{\mathfrak{P}_\beta}(x) = \gamma^{s(x)}\,.$$

From the above diagram, we get that this is equivalent to

$$\log_p(N_{L_{\mathfrak{P}_\beta}/\mathbb{Q}_p}(y)) = \log_p(\chi_{cyc}(\gamma^{s(x)})^{-1}) = -s(x)\omega\,.$$

So we are left to show that

$$\log_p(N_{L_{\mathfrak{P}_\beta}/\mathbb{Q}_p}(y)) = \log_p(N_{L_{\mathfrak{P}_\beta}/\mathbb{Q}_p}(x))\,.$$

But from the above diagram, we see that $N_{L_{\mathfrak{P}_\beta}/\mathbb{Q}_p}(y)$ and $N_{L_{\mathfrak{P}_\beta}/\mathbb{Q}_p}(x)$ differ by an element of $\langle p^{\mathbb{Z}}\rangle \times \mu_{p-1} = \ker(\log_p)$. □

With the above Lemma, we get for $1 \le \beta \le e_p$

$$\begin{aligned}
\mathrm{Rec}_{\mathfrak{P}_\beta}(x) &= \sum_{\sigma\in G} \sigma^{-1} \otimes (\gamma^{s(\sigma(x))} - 1) \\
&= \sum_{\sigma\in G} s(\sigma(x))\sigma^{-1} \otimes (\gamma - 1) \\
&= -\frac{1}{\omega}\sum_{\sigma\in G} \log_p(N_{L_{\mathfrak{P}_\beta}/\mathbb{Q}_p}(\sigma(x)))\sigma^{-1} \otimes (\gamma - 1) \\
&= -\frac{1}{\omega}\,\mathrm{Log}_{\mathfrak{P}_\beta}(x) \otimes (\gamma - 1)
\end{aligned}$$

and analogously for $e_p + 1 \le \beta \le e$

$$\mathrm{Rec}_{\mathfrak{P}_\beta}(x) = n_{\mathfrak{P}_\beta}\,\mathrm{Ord}_{\mathfrak{P}_\beta}(x) \otimes (\gamma - 1)\,.$$

In our case, we hence get

$$\mathrm{Rec}_{\mathfrak{P}_\beta}(u^{(i)}_{\alpha,T}) = \begin{cases} -\frac{1}{\omega}\,\mathrm{Log}_{\mathfrak{P}_\beta}(u^{(i)}_{\alpha,T}) \otimes (\gamma - 1), & 1 \le \beta \le e_p, \\ n_{\mathfrak{P}_\beta}\,\mathrm{Ord}_{\mathfrak{P}_\beta}(u^{(i)}_{\alpha,T}) \otimes (\gamma - 1), & e_p + 1 \le \beta \le e. \end{cases}$$

Inserting this yields

$$\begin{aligned}
e_{S,r'} \operatorname{Ord}_{\mathfrak{P}_i}(\kappa_{L,S,T}) \otimes (\gamma-1)^e &= e_{S,r'} \operatorname{Rec}_W((-1)^i \eta_T^{(i)}) \\
&= e_{S,r'} (-1)^i \lambda_T^{(i)} \det \left(\frac{-\left(\frac{1}{\omega} \operatorname{Log}_{\mathfrak{P}_\beta}(u_{\alpha,T}^{(i)}) \otimes (\gamma-1)\right)_{\substack{1\le\beta\le e_p \\ 1\le\alpha\le e}}}{\left(n_{\mathfrak{P}_\beta} \operatorname{Ord}_{\mathfrak{P}_\beta}(u_{\alpha,T}^{(i)}) \otimes (\gamma-1)\right)_{\substack{e_p+1\le\beta\le e \\ 1\le\alpha\le e}}} \right) \\
&= e_{S,r'} (-1)^{i+e_p} \frac{\lambda_T^{(i)}}{\omega^{e_p}} \det \left(\frac{\left(\operatorname{Log}_{\mathfrak{P}_\beta}(u_{\alpha,T}^{(i)})\right)_{\substack{1\le\beta\le e_p \\ 1\le\alpha\le e}}}{\left(n_{\mathfrak{P}_\beta} \operatorname{Ord}_{\mathfrak{P}_\beta}(u_{\alpha,T}^{(i)})\right)_{\substack{e_p+1\le\beta\le e \\ 1\le\alpha\le e}}} \right) \otimes (\gamma-1)^e .
\end{aligned}$$

Since $I(\Gamma)^e/I(\Gamma)^{e+1} \cong \Gamma \cong \mathbb{Z}_p$ and $(\gamma-1)^e$ is a generator, it follows that

$$e_{S,r'} \operatorname{Ord}_{\mathfrak{P}_i}(\kappa_{L,S,T}) = e_{S,r'} (-1)^{i+e_p} \frac{\lambda_T^{(i)}}{\omega^{e_p}} \det \left(\frac{\left(\operatorname{Log}_{\mathfrak{P}_\beta}(u_{\alpha,T}^{(i)})\right)_{\substack{1\le\beta\le e_p \\ 1\le\alpha\le e}}}{\left(n_{\mathfrak{P}_\beta} \operatorname{Ord}_{\mathfrak{P}_\beta}(u_{\alpha,T}^{(i)})\right)_{\substack{e_p+1\le\beta\le e \\ 1\le\alpha\le e}}} \right) .$$

and hence, we are left to consider the characters χ with $r_{S,\chi} > r'$. Since $e_{[\chi]}\eta_{L,S_i,T} = 0$ for such a character, we also find that the right hand side vanishes for these characters. If we can show that $e_{[\chi]} \operatorname{Ord}_{\mathfrak{P}_i}(\kappa_{L,S,T}) = 0$ for these characters, then Conjecture 4.2.15 follows.

For this we consider the extensions $L_\chi := L^{\ker(\chi)}$ resp. $L_{\chi,n} = L_n^{\ker(\chi)}$. Since $r_{S,\chi} > r'$, we have at least one place $v \in S \setminus V'$ such that $G_v \subseteq \ker(\chi)$, i.e. v splits completely in L_χ. If there is such a place which is not only completely split in L_χ but also in $L_{\chi,\infty}$, we find for each n that

$$N_{L_n/L_{\chi,n}}(\eta_{L_n,S,T}) = \eta_{L_{\chi,n},S,T} = \eta_{L_{\chi,n},S,T}^{1-\sigma_v} = 1 .$$

In this case, we also find $\beta_{L_{\chi,n},S,T} = N_{L_n/L_{\chi,n}}(\beta_{L,n}) \in L_{\chi,n}^\times/L^\times$ satisfying $\beta_{L_{\chi,n},S,T}^{(\gamma-1)^e} = 1$. Indeed, this implies $\beta_{L_{\chi,n},S,T} \in L^\times$ and hence

$$\kappa_{L_\chi,S,T,n} = N_{L_{\chi,n}/L_\chi}(\beta_{L_{\chi,n},S,T}) = N_{L/L_\chi}(\kappa_{L,S,T,n}) \in (L_\chi^\times)^{p^n} .$$

Therefore, we get that

$$\begin{aligned}
e_\chi \operatorname{Ord}_{\mathfrak{P}_i}(\kappa_{L,S,T,n}) &= e_\chi \sum_{\sigma\in G} \operatorname{ord}_{\mathfrak{P}_i}(\sigma(\kappa_{L,S,T,n}))\sigma^{-1} \\
&= \sum_{\sigma\in G} \operatorname{ord}_{\mathfrak{P}_i}(\sigma(\kappa_{L,S,T,n}))\chi(\sigma^{-1})e_\chi \\
&= \sum_{\sigma\in \operatorname{Gal}(L_\chi/K)} \operatorname{ord}_{\mathfrak{P}_i}(\sigma(\kappa_{L_\chi,S,T,n}))\chi(\sigma^{-1})e_\chi \\
&\equiv 0 \mod p^n .
\end{aligned}$$

Since for $\psi \sim \chi$, we have $\ker(\chi) = \ker(\psi)$, this holds for all $\psi \in [\chi]$ and hence $e_{[\chi]} \operatorname{Ord}_{\mathfrak{P}_i}(\kappa_{L,S,T,n}) \equiv 0 \mod p^n$ for all n. Taking the limit, we get

$$e_{[\chi]} \operatorname{Ord}_{\mathfrak{P}_i}(\kappa_{L,S,T}) = 0 \in e_{[\chi]}\mathbb{Z}_p[G] .$$

Last but not least, we have to consider the case that S contains no additional place which is completely split in $L_{\chi,\infty}$. In this case, the difference e increases when moving from L and L_∞ to L_χ and $L_{\chi,\infty}$. Indeed, Conjecture 4.3.3 then implies that there exists an $\alpha_{L_n,S,T} \in L_{\chi,n}^\times/L^\times$ such that $\alpha_{L_n,S,T}^{\gamma-1} = N_{L_n/L_{\chi,n}}(\beta_{L_n,S,T})$ (maybe we could take even some powers of $\gamma - 1$). But then we find that

$$N_{L/L_\chi}(\kappa_{L,S,T,n}) = N_{L_{\chi,n}/L}(\alpha_{L_n,S,T})^{\gamma-1} = 1$$

and hence a similar computation as above shows that

$$e_{[\chi]} \operatorname{Ord}_{\mathfrak{P}_i}(\kappa_{L,S,T}) = 0 \in e_{[\chi]}\mathbb{Z}_p[G]$$

in this case.

This finishes the proof of Theorem 4.3.2. We can deduce the following

Corollary 4.3.9. *(i) If Conjecture 4.2.15 holds for $L/K, S$ and T and $v \notin S$ is a place of K, which is completely split in L_∞, then Conjecture 4.2.15 also holds for $L/K, S \cup \{v\}$ and T.*

(ii) If the equation in Conjecture 4.2.15 holds for any $1 \leq i \leq e_p$, then it holds for all $i = 1, ..., e_p$.

(iii) The validity of Conjecture 4.2.15 does not depend on the choice of γ.

Proof. (i) From Theorem 4.3.2 we get that $\mathrm{IMRS}(L/K, S, T, 1)_p$ holds by assumption, hence we obtain $\mathrm{IMRS}(L/K, S \cup \{v\}, T, 1)_p$ from [BKS17, Prop. 4.4(iv)] and therefore Conjecture 4.2.15 also holds for this data.

(ii) We have seen before that the equation in Conjecture 4.2.15 for any $1 \leq i \leq e_p$ is equivalent to (4.3.1), hence the other equations follow from an application of $\operatorname{Ord}_{\mathfrak{P}_j}$ for $j \neq i$.

(iii) It is clear that $\kappa_{L,S,T}$ and hence the statement of Conjecture 4.2.15 depend on the generator γ. However, if the conjecture is true for a certain choice of γ, this implies $\mathrm{IMRS}(L/K, S, T, 1)_p$. Since this is independent of γ, we hence obtain Conjecture 4.2.15 for any other choice of γ. □

Remark 4.3.10. Part (i) of the above corollary indeed proves that we can restrict to the simpler formulation under the assumption $V' \setminus V \subseteq S_p$.

Chapter 5

An algorithmic study of the Mazur-Rubin-Sano conjecture

In this chapter, we want to use our reformulation of $\mathrm{IMRS}(L/K, S, T, 1)_p$ to numerically verify the conjecture up to some level n. We use the notation and assumptions from the last chapter, in particular K is a totally real field, L_∞ is an abelian extension containing the cyclotomic $\mathbb{Z}_p$-extension K_∞/K and $L = L_\infty^\Gamma$. We assume that Stark's conjecture and Conjecture 4.2.3 hold for each level n (Hypotheses 4.2.2 and 4.2.6) and that $r = 1$ (Remark 4.2.8).

We first present an algorithm to compute Rubin-Stark elements (for arbitrary r). In the second part, we consider the computation of Stark units in the case when K is a real quadratic field. Then we combine the presented algorithms to compute all the necessary values for testing Conjecture 4.2.15 up to level n. In the last section, we construct examples L/K, where Conjecture 4.2.15 is not implied by any theoretical results known to the author and present the computational results for these examples.

5.1 The computation of Rubin-Stark elements

In order to verify Conjecture 4.2.9, we need to compute Rubin-Stark elements in the field L. The basis for this computation was developed in the author's master thesis. We will start with a short presentation of this approach. The rounding method from the master's thesis is replaced by an improved version described in Section 5.1.4.

5.1.1 Computing the (S, T)-units

The algorithm for the computation of the (S, T)-units was provided by Werner Bley.

We assume that we are able to compute $\mathcal{O}_{L,S}^\times$ as an abstract abelian group $O_{L,S}$ together with an embedding $\iota_{L,S}$ into the field L. An algorithm for this can be found in [Coh93, §6.5]. We sort the generators $b_1, ..., b_{|S_L|}$ of $O_{L,S}$ such that $b_{|S_L|}$ generates the torsion part, i.e. $\iota_{L,S}(b_{|S_L|})$ generates $\mu(L)$. Now let $T_L = \{t_1, ..., t_l\}$ and choose a generator π_i of $(\mathcal{O}_L/t_i)^\times$ for each i. Then $\iota_{L,S}(b_j) \notin t_i$ for all i and j, hence we obtain integers α_{ij} such that $\iota_{L,S}(b_j) \equiv \pi_i^{\alpha_{ij}} \mod t_i$. Defining the matrices

$$A_1 = (\alpha_{ij})_{\substack{1\le i\le l\\ 1\le j\le |S_L|}}, \quad A_2 = \begin{pmatrix} Nt_1 - 1 & & 0 \\ & \ddots & \\ 0 & & Nt_l - 1 \end{pmatrix}$$

and

$$A = (A_1|A_2) \in \mathbb{Z}^{l\times(|S_L|+l)},$$

we find

Proposition 5.1.1. *Consider the map*

$$\varphi\colon \mathbb{Z}^{|S_L|+l} \longrightarrow O_{L,S}$$
$$(z_1, ..., z_{|S_L|+l}) \longmapsto \sum_{j=1}^{|S_L|} z_j b_j$$

and set $O_{L,S,T} := \varphi(\ker(A))$. *Then* $\iota_{L,S}(O_{L,S,T}) = \mathcal{O}_{L,S,T}^\times$.

Proof. Let $z = (z_1, ..., z_{|S_L|+l}) \in \ker(A)$, then $\sum_{j=1}^{|S_L|} \alpha_{ij} z_j = -z_{|S_L|+i}(N_{t_i} - 1)$ for each $i = 1, ..., l$. Hence

$$\iota_{L,S}(\varphi(z)) \equiv \pi_i^{\sum_{j=1}^{|S_L|}\alpha_{ij}z_j} \equiv \pi_i^{-z_{|S_L|+i}(N_{t_i}-1)} \equiv 1 \mod t_i$$

for all i, so $\iota_{L,S}(O_{L,S,T}) \subseteq \mathcal{O}_{L,S,T}^\times$.

Now suppose that $x \in \mathcal{O}_{L,S,T}^\times$. Since the $\iota_{L,S}(b_j), j = 1, ..., |S_L|$ generate $\mathcal{O}_{L,S}^\times$, there exist integers $z_1, ..., z_{|S_L|}$ such that $x = \iota_{L,S}(\sum_{j=1}^{|S_L|} z_j b_j)$. Choosing

$$z_{|S_L|+i} = -\frac{1}{N_{t_i} - 1} \sum_{j=1}^{|S_L|} \alpha_{ij} z_j$$

for $i = 1, ..., l$, we obtain and element $z \in \mathbb{Z}^{|S_L|+l}$ such that $x = \iota_{L,S}(\varphi(z))$ and the above computation shows that $z \in \ker(A)$. □

Hence, the computation of $\mathcal{O}_{L,S,T}^\times$ can be reduced to compute the kernel of A. The result of this computation is the abstract subgroup $O_{L,S,T}$ of $O_{L,S}$ and the generators of this subgroup define a $\mathbb{Q}$-basis $\{u_1, ..., u_{|S_L|-1}\}$ of $\mathbb{Q}\mathcal{O}_{L,S,T}^\times$ via $\iota_{L,S}$. Set $m := |S_L| - 1$.

For our computation of Rubin-Stark elements we want to use the decomposition by the rational idempotents $e_{[\chi]}$. Since $e_{[\chi]} \cdot \mathbb{Q}\mathcal{O}_{L,S,T}^\times$ is a free $e_{[\chi]} \cdot \mathbb{Q}[G]$-module of rank r, i.e. an r-dimensional $\mathbb{Q}(\chi)$-vector space, there exists indices $i_1(\chi), ..., i_r(\chi) \in \{1, ..., m\}$ such that $\{e_{[\chi]}u_{i_1(\chi)}, ..., e[\chi]u_{i_r(\chi)}\}$ is a $\mathbb{Q}(\chi)$-basis of $e_{[\chi]} \cdot \mathbb{Q}\mathcal{O}_{L,S,T}^\times$. Note that these indices depend on the equivalence class $[\chi]$ but not on the character χ. For determining these indices, we use the following lemma from the author's master thesis:

Lemma 5.1.2. *A family of elements* $\{v_1, ..., v_l\} \in e_{[\chi]} \cdot \mathbb{Q}\mathcal{O}_{L,S,T}^\times$ *is linearly independent over* $\mathbb{Q}(\chi)$ *if and only if the family* $\{\sigma v_j \,|\, \sigma \in G, 1 \le j \le l\}$ *spans a* $\mathbb{Q}$*-vector space of dimension* $l \cdot [\mathbb{Q}(\chi) : \mathbb{Q}]$.

Hence, we can apply the

Algorithm 5.1.3. Input: $u_1, ..., u_m$ together with the G-action, $[\mathbb{Q}(\chi) : \mathbb{Q}]$ and $e_{[\chi]}$.

(1) Search an index $i_1(\chi)$ such that $e_{[\chi]} u_{i_1(\chi)} \neq 0$.

(2) Let d be the number of already computed indices. If $d = r$, return the indices $i_1(\chi), ..., i_r(\chi)$.

(3) Test the family $e_{[\chi]} u_{i_1(\chi)}, ..., e_{[\chi]} u_{i_d(\chi)}, e_{[\chi]} u_j$ on linear independence over $\mathbb{Q}(\chi)$ for some index $j > i_d(\chi)$.

(4) If the family is linear independent, set $i_{d+1}(\chi) = j$ and go to step (2), else go to step (3) with the new index $j + 1$.

Remark 5.1.4. Computing $\sigma(u_i)$ as a linear combination of the $u_1, ..., u_m$ can be quite time consuming. Here it is helpful to compute the action of G on the abstract abelian group $O_{L,S,T}$ and then reduce the computation to a simple matrix multiplication.

Since $e_{[\chi]} u_{i_1(\chi)}, ..., e_{[\chi]} u_{i_r(\chi)}$ is a $\mathbb{Q}(\chi)$-basis of $e_{[\chi]} \cdot \mathbb{Q}\mathcal{O}_{L,S,T}^{\times} \cong \mathbb{Q}(\chi)\mathcal{O}_{L,S,T}^{\times}$, we can represent $e_{[\chi]} u_s$ for all $s = 1, ..., m$ in this basis, i.e.

$$e_{[\chi]} u_s = \sum_{\alpha=1}^{r} \mu_{s\alpha}([\chi]) e_{[\chi]} u_{i_\alpha(\chi)}$$

for some $\mu_{s\alpha}([\chi]) \in \mathbb{Q}[G]$ (note that $\mu_{s\alpha}([\chi]) e_{[\chi]}$ is unique, whereas $\mu_{s\alpha}([\chi])$ is not). These coefficients still depend on $[\chi]$, but we will only use them in the context of a fixed equivalence class, hence we will simply write $\mu_{s\alpha}$ from now on. For the rounding process, it will be necessary to determine (a choice of) these coefficients $\mu_{s\alpha}$. For this, we use the following

Algorithm 5.1.5. Input: $u_1, ..., u_m$ together with the G-action, $i_1(\chi), ..., i_r(\chi)$ and $e_{[\chi]}$.

(1) Compute $a_{st} \in \mathbb{Q}, t = 1, ..., m$ such that $e_{[\chi]} u_s = \sum_{t=1}^{m} a_{st} u_t$ for each $s = 1, ..., m$.

(2) Use the G-action on $O_{L,S,T}$ to compute $b_{\alpha t}(\sigma) \in \mathbb{Q}, t = 1, ..., m, \sigma \in G$ such that $\sigma e_{[\chi]} u_{i_\alpha(\chi)} = \sum_{t=1}^{m} b_{\alpha t}(\sigma) u_t$ for each $\alpha = 1, ..., r$.

(3) Solve the system of linear equations $a_{st} = \sum_{\alpha=1}^{r} \sum_{\sigma \in G} c_{s\alpha}(\sigma) b_{\alpha t}(\sigma)$ over $\mathbb{Q}$.

(4) Return $\mu_{s\alpha} = \sum_{\sigma \in G} c_{s\alpha}(\sigma)\sigma \in \mathbb{Q}[G]$.

Indeed we see that with this choice of $\mu_{s\alpha}$, we get

$$\begin{aligned} \sum_{\alpha=1}^{r} \mu_{s\alpha} e_{[\chi]} u_{i_\alpha(\chi)} &= \sum_{\alpha=1}^{r} \sum_{\sigma \in G} c_{s\alpha}(\sigma) \sigma e_{[\chi]} u_{i_\alpha(\chi)} = \sum_{\alpha=1}^{r} \sum_{\sigma \in G} c_{s\alpha}(\sigma) \sum_{t=1}^{m} b_{\alpha t}(\sigma) u_t \\ &= \sum_{t=1}^{m} a_{st} u_t = e_{[\chi]} u_s. \end{aligned}$$

5.1.2 Computing the L-values

The Rubin-Stark element is determined by the values of the S-truncated T-modified L-functions. So we need to determine the value $L_{S,T}^{(r)}(\chi, 0)$ for each character χ with $r_{S,\chi} = r$. There exist algorithms for the computation $L^{(d)}(\chi, 0)$ for an arbitrary d-th derivative of the L-function associated to a Hecke character (see e.g. [Dok04]), so all we have to do is to identify our given character χ with a Hecke character and compute the additional factors caused by the sets S and T. In particular, we may have to adjust the order of the computed derivative, since in general $r_{S,\chi} \neq r_{S_\infty,\chi}$. As the algorithm described in this chapter is implemented in MAGMA, we use the built-in intrinsic for the computation of $L^{(d)}(\chi, 0)$. Although the identifications in MAGMA may be a bit tricky, the involved operations are elementary and can be retraced directly in the implementation.

Also note that we distinguish the case $\chi = \mathbf{1}$, since we know the leading term of the Dedekind ζ-function from the analytic class number formula.

5.1.3 Determine the real coefficients

As mentioned before, we decompose the Rubin-Stark element by rational idempotents, i.e.

$$\eta_{L,S,T} = \sum_{[\chi] \subseteq \widehat{G}_{S,r}} e_{[\chi]} \eta_{L,S,T} \,.$$

Note that $\eta_{L,S,T}$ lies in the $e_{S,r}$-component (cf. Remark 2.2.2). With the basis computed in Section 5.1.1, we obtain

$$\eta_{L,S,T} = \sum_{[\chi] \subseteq \widehat{G}_{S,r}} e_{[\chi]} \lambda_{[\chi]} u_{i_1([\chi])} \wedge \cdots \wedge u_{i_r([\chi])} = \sum_{[\chi] \subseteq \widehat{G}_{S,r}} \left(\sum_{\psi \in [\chi]} e_\psi \lambda_\psi \right) u_{i_1([\chi])} \wedge \cdots \wedge u_{i_r([\chi])} \,,$$

where $\lambda_\psi \in \mathbb{C}$ such that $\sum_{\psi \in [\chi]} e_\psi \lambda_\psi = e_{[\chi]} \lambda_{[\chi]} \in \mathbb{R}[G]$. Applying

$$(w_0 - w')^* \wedge \cdots \wedge (w_{r-1} - w')^* \in \operatorname{Hom}_{\mathbb{R}[G]}(\wedge^r \mathbb{R}\mathcal{O}_{L,S,T}^\times, \mathbb{R}[G])$$

(where we use the identification (2.1.1)) to the definition of $\eta_{L,S,T}$, we obtain

$$\lambda_\psi \det\Big(-\sum_{\sigma \in G} \log \big|\sigma(u_{i_\alpha([\chi])})\big|_{w_\beta} \psi(\sigma^{-1})\Big)_{1 \leq \alpha,\beta \leq r} = L_{S,T}^{(r)}(\psi^{-1}, 0) \in \mathbb{C} \tag{5.1.1}$$

for each $\psi \in [\chi]$.

Hence, we can compute $\eta_{L,S,T}$ with the following

Algorithm 5.1.6. Input: L, K, S and T.

(1) Determine r as the number of the completely split primes $v_0, ..., v_{r-1}$ in S.

(2) Choose places w_β of L for $\beta = 0, ..., r-1$ such that $w_\beta \mid v_\beta$.

(3) Compute the (S,T)-units as the abstract group $O_{L,S,T}$ together with its G-action.

(4) Determine the characters $\chi \in \widehat{G}_{S,r}$ and compute the rational idempotents $e_{[\chi]}$

(5) For each $[\chi] \in \widehat{G}_{S,r}$:

  (5.1) Use Algorithm 5.1.3 to determine the indices $i_1(\chi), ..., i_r(\chi)$.

  (5.2) For each $\psi \in [\chi]$ compute $L_{S,T}^{(r)}(\psi^{-1}, 0)$ as described in Section 5.1.2.

  (5.3) Directly compute the determinant on the left hand side of (5.1.1) and determine λ_ψ.

(6) Combine the $e_\psi \lambda_\psi$ to $e_{[\chi]}\lambda_{[\chi]} \in \mathbb{R}[G]$.

(7) Return $\eta_{L,S,T}$ as a list of tuples consisting of the coefficient $e_{[\chi]}\lambda_{[\chi]}$ and the units $u_{i_1(\chi)}, ..., u_{i_r(\chi)}$.

5.1.4 Determine the rational coefficients

Now $\mathrm{St}(L/K,S,T,r)$ is equivalent to $e_{[\chi]}\lambda_{[\chi]} \in \mathbb{Q}[G]$ for all equivalence classes $[\chi]$ and we want to determine these rational coefficients. In order to do this, we assume that the Rubin-Stark conjecture holds. If this is true, the procedure described below will determine the rational coefficients $\lambda_{[\chi]}e_{[\chi]}$, hence if the procedure fails, we get a counter example for the Rubin-Stark conjecture. Conjecture $\mathrm{RS}(L/K,S,T,r)$ implies that for any $\varphi_1, ..., \varphi_r \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathcal{O}_{L,S,T}^\times, \mathbb{Z}[G])$, we get

$$(\varphi_1 \wedge \cdots \wedge \varphi_r)(\eta_{L,S,T}) \in \mathbb{Z}[G] \,.$$

Since $|G|\, e_{[\chi]} \in \mathbb{Z}[G]$, this implies

$$(\varphi_1 \wedge \cdots \wedge \varphi_r)(|G|\, e_{[\chi]}\eta_{L,S,T}) = |G|\, e_{[\chi]}\lambda_{[\chi]} \det(\varphi_\alpha(u_{i_\beta([\chi])}))_{1\le\alpha,\beta\le r} \in \mathbb{Z}[G] \qquad (5.1.2)$$

for all $[\chi]$. Fix an equivalence class $[\chi]$ and let $e_{[\chi]}u^*_{i_\alpha([\chi])} \in \mathrm{Hom}_{\mathbb{Q}(\chi)}(\mathbb{Q}(\chi)\mathcal{O}_{L,S,T}^\times, \mathbb{Q}(\chi))$ be the dual map, i.e.

$$e_{[\chi]}u^*_{i_\alpha([\chi])}(e_{[\chi]}u_{i_\beta([\chi])}) = \delta_{\alpha\beta} \,.$$

Then we obtain the following

Lemma 5.1.7. *Let N be the least common multiple of the denominators of the coefficients $\mu_{s\alpha} \in \mathbb{Q}[G]$, i.e. $N\mu_{s\alpha} \in \mathbb{Z}[G]$ for all $s = 1, ..., m, \alpha = 1, ..., r$. Then*

$$\begin{aligned}\varphi_\alpha \colon \mathcal{O}_{L,S,T}^\times &\longrightarrow \mathbb{Z}[G] \\ u &\longmapsto N \cdot |G|\, e_{[\chi]}u^*_{i_\alpha([\chi])}(e_{[\chi]}u)\end{aligned}$$

is a well-defined $\mathbb{Z}[G]$-homomorphism.

Proof. By definition, we obtain for each $s = 1, ..., m$

$$\varphi_\alpha(u_s) = N \cdot |G|\, e_{[\chi]}\mu_{s\alpha} \in \mathbb{Z}[G]\,.$$

For the linearity, let $\lambda \in \mathbb{Z}[G]$. Then $e_{[\chi]}\lambda \in e_{[\chi]}\mathbb{Q}[G] \cong \mathbb{Q}(\chi)$ and since $e_{[\chi]}u^*_{i_\alpha([\chi])}$ is $\mathbb{Q}(\chi)$-linear, we obtain

$$\begin{aligned}\varphi_\alpha(\lambda u) &= N \cdot |G|\, e_{[\chi]}u^*_{i_\alpha([\chi])}(e_{[\chi]}\lambda u) = e_{[\chi]}\lambda \cdot N \cdot |G|\, e_{[\chi]}u^*_{i_\alpha([\chi])}(e_{[\chi]}u)\\ &= \lambda\varphi_\alpha(u)\,.\end{aligned}$$

□

Using these maps, we get from (5.1.2) that

$$|G|^{r+1}\, N^r e_{[\chi]}\lambda_{[\chi]} \in \mathbb{Z}[G]$$

Therefore, we obtain the Rubin-Stark element with rational coefficients from

Algorithm 5.1.8. Input: L,K,S and T.

(1) Use Algorithm 5.1.6 to compute $e_{[\chi]}\lambda_{[\chi]} \in \mathbb{R}[G]$ and the units $u_{i_1(\chi)}, ..., u_{i_r(\chi)}$. Also store the abstract group $O_{L,S,T}$ together with the G-action.

(2) For each equivalence class $[\chi]$ do:

(2.1) Use Algorithm 5.1.5 to compute the $\mu_{s\alpha} \in \mathbb{Q}[G]$ and determine the integer N.

(2.2) Compute the coefficients of $|G|^{r+1}\, N^r e_{[\chi]}\lambda_{[\chi]}$ as real numbers and round these to integers $a_\sigma \in \mathbb{Z}$.

(2.3) Set $\lambda_{[\chi],\mathbb{Q}} := \sum_{\sigma\in G} \frac{a_\sigma}{|G|^{r+1}N^r}\sigma \in \mathbb{Q}[G]$ as the new coefficient for the $[\chi]$-component.

(3) Return $\eta_{L,S,T}$ as a list of tuples consisting of the coefficient $\lambda_{[\chi],\mathbb{Q}}$ and the units $u_{i_1(\chi)}, ..., u_{i_r(\chi)}$.

Remark 5.1.9. (i) The L-values and the logarithms in the above algorithm can only be determined up to a certain precision, hence we always obtain an error term in our computation. We determine the error term by comparing our resulting real coefficients before the rounding process with the rational coefficients determined by the rounding process.

(ii) As already mentioned above, the described procedure was already part of the author's master thesis. The main difference is the new rounding process which allows to round real numbers to integers instead of finding approximations of rational numbers.

(iii) There exists also an algorithm for computing Rubin-Stark units by K. McGown, J. Sands and D. Vallières in [MSV19]. Their approach is formulated in the language of Artin systems but is quite similar to the one presented in the author's master thesis. In particular, they also round real numbers to rational values to a high precision.

5.2 Computing Stark units over real quadratic fields

The algorithm for the Rubin-Stark elements described in the previous section can theoretically be applied to arbitrary fields L/K. The main problem is, that we have to compute the ring of integers and the units of the top field L, which limits the computations to fields of low degree (many fields L with $[L:\mathbb{Q}] < 30$ and small discriminant can be handled in reasonable time). When examining Conjecture 4.2.15, we have to compute the Rubin-Stark elements in L/K (which is possible in the considered cases), but we also need the Stark units in the extensions L_n/K. For this purpose, we have to improve the algorithm exploiting the specialization to the case $r = 1$ and by restricting to real quadratic base fields K. These improvements are based on [Rob97] and will be described in the following sections.

5.2.1 The real values of the conjugates of the Stark unit

We use the notation from the last chapter and we assume from now on that K is a real quadratic field. Moreover, we restrict to the case that $S = S_\infty \cup S_{ram}(L/K) \cup S_p$. In particular, we assume that Stark's conjecture is true, i.e. we work under Hypothesis 4.2.2. Set $m := [L_n : K]$. In the case $r = 1$, we know that $\mathrm{RS}(L/K, S, T, 1)$ for all T is equivalent to $\mathrm{St}(L/K, S)$ (see Corollary 2.4.2) and instead of computing $\eta_{L_n,S,T}$, we compute all the conjugates $\varepsilon^\sigma_{L_n,S}$ for $\sigma \in \mathcal{G}_n$. These are determined by the polynomial

$$f = \prod_{\sigma\in\mathcal{G}_n} (X - \varepsilon^\sigma_{L_n,S}) = \sum_{k=0}^{m} b_k X^k \in K[X]\,.$$

So it suffices to determine the coefficients $b_k \in K$. These are uniquely determined by their embeddings $\tau_1(b_k)$ and $\tau_2(b_k)$, where $\tau_i\colon K \longrightarrow \mathbb{R}$ corresponds to the infinite place ∞_i of K for $i = 1, 2$. Without loss of generality, we can assume that ∞_1 is the unique place which splits completely in L_∞ (as assumed in the beginning of Section 4.2 and Remark 4.2.8). We start determining $\tau_1(b_k)$ by computing $\tau(\varepsilon^\sigma_{L_n,S})$ for all $\sigma \in \mathcal{G}_n$, where $\tau\colon L_n \longrightarrow \mathbb{R}$ is the embedding corresponding to the chosen place w of L_n above ∞_1.

The defining equations

$$L'_S(\chi, 0) = -\frac{1}{2}\sum_{\sigma\in\mathcal{G}_n} \log\left|\varepsilon^\sigma_{L_n,S}\right|_w \chi(\sigma)$$

for all $\chi \in \widehat{\mathcal{G}_n}$ can be transformed into

$$(\log\left|\varepsilon^\sigma_{L_n,S}\right|_w)_{\sigma\in\mathcal{G}_n} = A^{-1}(-2L'_S(\chi,0))_{\chi\in\widehat{\mathcal{G}_n}}\,,$$

where A is the matrix with rows $(\chi(\sigma))_{\sigma\in\mathcal{G}_n}$.

Hence, we can compute (an approximation of) $\left|\varepsilon^\sigma_{L_n,S}\right|_w = \left|\tau(\varepsilon^\sigma_{L_n,S})\right|$ by computing the values of the L-series (see Section 5.1.2). We then obtain $\tau(\varepsilon^\sigma_{L_n,S}) > 0$ and hence $\tau(\varepsilon^\sigma_{L_n,S}) = \left|\tau(\varepsilon^\sigma_{L_n,S})\right|$ from [Rob97, Cor. 2.13]. So we can (approximately) compute

$$\tau_1(f) = \sum_{k=0}^{m} \tau_1(b_k) X^k = \prod_{\sigma\in\mathcal{G}_n} (X - \tau(\varepsilon^\sigma_{L_n,S})) \in \mathbb{R}[X]\,.$$

For the values $\tau_2(b_k)$, we use that $|S| \geq 3$ in our case, hence by part (ii) of $\mathrm{St}(L/K, S)$ we get that $|\varepsilon_{L_n,S}|_{w'} = 1$ for all $w' \nmid \infty_1$.

In particular, this holds for the places above ∞_2 and we hence obtain

$$|\tau_2(b_k)| \leq \binom{m}{k}.$$

Since $|\varepsilon_{L_n,S}|_{w'} = 1$ for all finite places w' of L_n, we know that $\varepsilon_{L_n,S} \in \mathcal{O}_{L_n}^{\times}$ and hence $b_k \in \mathcal{O}_K$ for all k. This information will be sufficient to uniquely determine the b_k and hence $\varepsilon_{L_n,S}^{\sigma}$ for all σ. This process will be described in the next section.

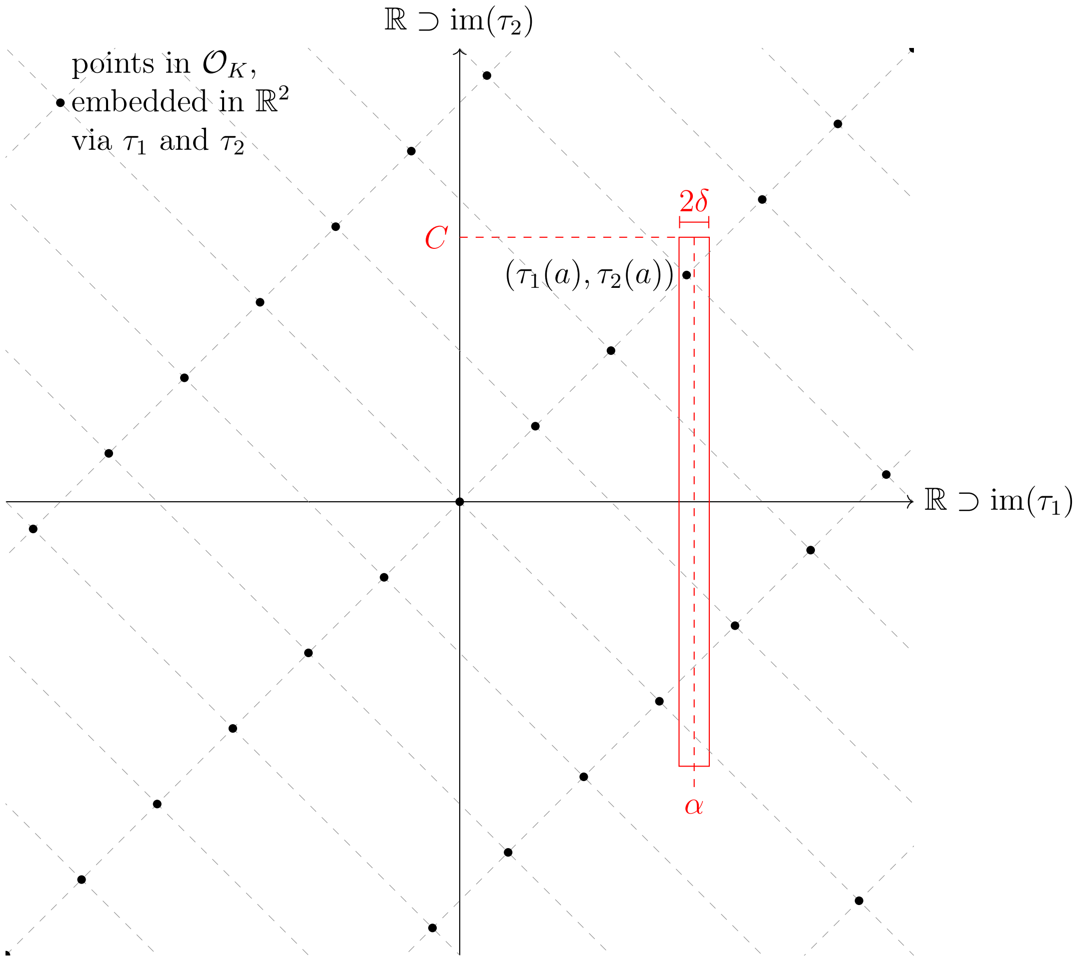
5.2.2 Rounding process

We want to determine an element $a \in \mathcal{O}_K$ from an approximation $\alpha \in \mathbb{R}$ of $\tau_1(a)$ and an upper bound C for the absolute value of $\tau_2(a)$, i.e. we search $a \in \mathcal{O}_K$ satisfying

$$\begin{aligned} |\alpha - \tau_1(a)| &\leq \delta\,, \\ |\tau_2(a)| &\leq C\,, \end{aligned}$$

where δ is the maximal error of the approximation α (in our concrete case, this is determined by the precision used in the computations of the L-values and will be examined in some detail in the next section). We assume that the upper bound C is fixed, whereas the precision of the approximation can be adjusted, i.e. we are able to make δ as small as necessary.

Visualizing the situation in $\mathbb{R}^2$, we obtain the following picture:



If δ is small enough, we only obtain exactly one lattice point in the red rectangle and this point must hence be our desired $a \in \mathcal{O}_K$. So we need a method to determine all the lattice points in a rectangle with corners $(x_1, y_1), (x_2, y_1), (x_2, y_2)$ and (x_1, y_2).

We know that $\mathcal{O}_K = \langle 1, d \rangle_{\mathbb{Z}}$, where d is determined by the discriminant of K. We set $d_i := \tau_i(d)$ and hence the lattice consists of the points

$$\{(\lambda + \mu d_1, \lambda + \mu d_2) \in \mathbb{R}^2 : \lambda, \mu \in \mathbb{Z}\}.$$

Then a lattice point is contained in the rectangle if and only if

$$\begin{aligned} x_1 \leq \lambda + \mu d_1 \leq x_2, \\ y_1 \leq \lambda + \mu d_2 \leq y_2. \end{aligned}$$

The second line implies $y_1 - \mu d_2 \leq \lambda \leq y_2 - \mu d_2$. Inserting this into the first line yields the inequalities

$$\begin{aligned} x_1 \leq y_2 + \mu(d_1 - d_2), \\ x_2 \geq y_1 + \mu(d_1 - d_2), \end{aligned}$$

i.e.

$$x_1 - y_2 \leq \mu(d_1 - d_2) \leq x_2 - y_1.$$

Once we fix $x_1, x_2, y_1, y_2 \in \mathbb{R}$, we can hence compute all possible values for $\mu \in \mathbb{Z}$. These are only finitely many and hence for each of these values, we can then compute the possible values for λ. Then we obtain a complete list of elements $a_{\lambda,\mu} = \lambda + \mu d \in \mathcal{O}_K$ such that $(\tau_1(a_{\lambda,\mu}), \tau_2(a_{\lambda,\mu}))$ is contained in the given rectangle.

Remark 5.2.1. This approach is a simplification of the procedure described in [Rob97, §2.3]. It is only possible since K is real quadratic, whereas Roblot's method works for an arbitrary totally real base field.

5.2.3 Error computation

In this section, we describe how we can choose the precision for the calculation of the L-values such that the resulting rectangle contains exactly one lattice point a. We first assume that we consider a rectangle whose lower border is centered around $(0, 0)$. This rectangle obviously contains the lattice point $(0, 0)$. The height of the rectangle is fixed, hence we need to determine the maximal width 4δ of a rectangle of this height h containing only one lattice point. We will apply this only on rectangles of height $h \geq 1$ and since $1 \in \mathcal{O}_K$, we see that a rectangle of width 2 and height h contains at least two lattice points, i.e. we already have an upper bound $4\delta < 2$. Now we can use the procedure described in the previous section to determine all the (finitely many) lattice points in the rectangle with corners $(-1, 0), (1, 0), (1, h)$ and $(-1, h)$. Let (x, y) be the lattice point in this rectangle with minimal $|x|$, then for any $2\delta < x$, the rectangle of width 4δ and height h only contains the lattice point $(0, 0)$. If we place a rectangle with height h and width 2δ at any point in $\mathbb{R}^2$, the resulting rectangle will contain at most one lattice point. Therefore, if our approximation α of a satisfies $|\tau_1(a) - \alpha| \leq \delta < \frac{x}{2}$, a can be uniquely determined.

So we have to choose our precision P for the computation of the L-values such that the resulting error is less than our given δ. We compute

$$L'_S(\chi,0) = L_\chi + \Lambda_\chi\,,$$

where $L_\chi \in \mathbb{C}$ is our approximation and $\Lambda_\chi \in \mathbb{C}$ is the error term.

Remember that if A is the matrix with the rows $(\chi(\sigma))_{\sigma\in\mathcal{G}_n}$, then we can compute A^{-1} exactly over $\mathbb{Q}(\chi)$. In order to combine this with the L-values, we have to embed the matrix entries into $\mathbb{C}$ and hence obtain

$$a_{\sigma,\chi} + \alpha_{\sigma,\chi}\,,$$

where $a_{\sigma,\chi}$ is the complex value from the embedding and $\alpha_{\sigma,\chi}$ is the error term.

We hence obtain

$$\begin{aligned}\log\left|\varepsilon^\sigma_{L_n,S}\right|_w &= -2\sum_{\chi\in\widehat{\mathcal{G}}_n}(a_{\sigma,\chi}+\alpha_{\sigma,\chi})(L_\chi+\Lambda_\chi)\\ &= \underbrace{-2\sum_{\chi\in\widehat{\mathcal{G}}_n} a_{\sigma,\chi}L_\chi}_{=:x_{\sigma,\log}} + \underbrace{\Big(-2\sum_{\chi\in\widehat{\mathcal{G}}_n}(a_{\sigma,\chi}\Lambda_\chi+\alpha_{\sigma,\chi}L_\chi+\alpha_{\sigma,\chi}\Lambda_\chi)\Big)}_{=:\xi_{\sigma,\log}}\,,\end{aligned}$$

where $x_{\sigma,\log}$ is the approximation of $\log\left|\varepsilon^\sigma_{L,S}\right|$ and $\xi_{\sigma,\log}$ is the error term.

Therefore, we obtain

$$\tau(\varepsilon^\sigma_{L_n,S}) = \exp(x_{\sigma,\log}+\xi_{\sigma,\log}) = \underbrace{\exp(x_{\sigma,\log})}_{=:x_\sigma} + \underbrace{\exp(x_{\sigma,\log})(\exp(\xi_{\sigma,\log})-1)}_{=:\xi_\sigma}$$

with the approximation x_σ and error term ξ_σ. For an expression for the coefficients b_k of the polynomial $f = \prod_{\sigma\in\mathcal{G}_n}(X-\varepsilon^\sigma_{L_n,S})$, we set $m := |\mathcal{G}_n|$ and fix an ordering $\{\sigma_1,...,\sigma_m\}$ of $\mathcal{G}_n$ and define

$$I_{k,m} = \{(i_1,...,i_k) : 1 \le i_1 < \cdots < i_k \le m\}$$

to be the set of all ordered k-tuples over $\{1,...,m\}$. Set $x_i := x_{\sigma_i}$ and $\xi_i := \xi_{\sigma_i}$. Then we compute

$$\tau_1(f) = \prod_{j=1}^m (X-(x_{\sigma_j}+\xi_{\sigma_j})) = \sum_{k=0}^m (-1)^k X^{m-k} \sum_{(i_1,...,i_k)\in I_{k,m}} \prod_{j=1}^k (x_{i_j}+\xi_{i_j})\,.$$

Hence, we get

$$\begin{aligned}
\tau_1(b_{m-k}) &= (-1)^k \sum_{(i_1,\dots,i_k)\in I_{k,m}} \prod_{j=1}^{k} (x_{i_j} + \xi_{i_j}) \\
&= (-1)^k \sum_{(i_1,\dots,i_k)\in I_{k,m}} \sum_{r=0}^{k} \sum_{(j_1,\dots,j_r)\in I_{r,k}} \prod_{s=1}^{r} x_{i_{j_s}} \prod_{\substack{j\in\{1,\dots,k\}\\ j\notin(j_1,\dots,j_r)}} \xi_{i_j} \\
&= \underbrace{(-1)^k \sum_{(i_1,\dots,i_k)\in I_{k,m}} \prod_{j=1}^{k} x_{i_j}}_{=:d_{m-k}} \\
&\quad + \underbrace{(-1)^k \sum_{(i_1,\dots,i_k)\in I_{k,m}} \sum_{r=0}^{k-1} \sum_{(j_1,\dots,j_r)\in I_{r,k}} \prod_{s=1}^{r} x_{i_{j_s}} \prod_{\substack{j\in\{1,\dots,k\}\\ j\notin(j_1,\dots,j_r)}} \xi_{i_j}}_{\delta_{m-k}} \,,
\end{aligned}$$

where d_{m-k} is our approximation of $\tau_1(b_{m-k})$ and δ_{m-k} is the resulting error. We want to determine a computation precision P such that $\max_{1\le k\le m-1} |\delta_k| \le \delta$, where δ is the bound fixed in the beginning of this section such that the resulting rectangle contains only one lattice point. Note that f is always normed with constant term 1, i.e. it is not necessary to consider the indices 0 and m. Set

$$L := \max_{\chi} |L_\chi| \,, \qquad a := \max_{\sigma,\chi} |a_{\sigma,\chi}| \,,$$
$$x_{\log} := \max_{\sigma} |x_{\sigma,\log}| \,, \qquad x := \max_{\sigma} |x_\sigma| \,,$$

and analogously for the error terms. Then we get

$$\begin{aligned}
|\delta_{m-k}| &\le \sum_{(i_1,\dots,i_k)\in I_{k,m}} \sum_{r=0}^{k-1} \sum_{(j_1,\dots,j_r)\in I_{r,k}} \prod_{s=1}^{r} |x_{i_{j_s}}| \prod_{\substack{j\in\{1,\dots,k\}\\ j\notin(j_1,\dots,j_r)}} |\xi_{i_j}| \\
&\le \sum_{(i_1,\dots,i_k)\in I_{k,m}} \sum_{r=0}^{k-1} \sum_{(j_1,\dots,j_r)\in I_{r,k}} \prod_{s=1}^{r} x \prod_{\substack{j\in\{1,\dots,k\}\\ j\notin(j_1,\dots,j_r)}} \xi \\
&= \sum_{(i_1,\dots,i_k)\in I_{k,m}} \sum_{r=0}^{k-1} \sum_{(j_1,\dots,j_r)\in I_{r,k}} x^r \xi^{k-r} \\
&= \binom{m}{k} \sum_{r=0}^{k-1} \binom{k}{r} x^r \xi^{k-r} \\
&= \binom{m}{k} \left((x+\xi)^k - x^k \right) .
\end{aligned}$$

The definition of ξ_σ yields $\xi \le x \cdot \max_\sigma |\exp(\xi_{\sigma,\log}) - 1|$. For the next steps, we assume that the error term $\xi_{\sigma,\log}$ is small. More precisely, we demand

$$\xi_{\log} = \max_{\sigma} |\xi_{\sigma,\log}| \leq \frac{1}{4m^2} . \tag{5.2.1}$$

In particular, $|\xi_{\sigma,\log}| < 1$ for all σ and hence we can use the error estimate of the exponential function to obtain

$$\xi \leq x \max_{\sigma} |2\xi_{\sigma,\log}| = 2x\xi_{\log} .$$

We hence obtain

$$\begin{aligned}
|\delta_{m-k}| &\leq \binom{m}{k} x^k ((1 + 2\xi_{\log})^k - 1) \\
&= \binom{m}{k} x^k \sum_{i=1}^{k} \binom{k}{i} 2^i \xi_{\log}^i \\
&\leq \binom{m}{k} x^k \left(2k\xi_{\log} + \sum_{i=2}^{k} \binom{k}{i} 2^i \frac{1}{(2m)^i} \xi_{\log}^{i/2} \right) \\
&\leq 3 \binom{m}{k} x^k k \xi_{\log} .
\end{aligned}$$

We can estimate

$$\xi_{\log} \leq 2m(a\Lambda + \alpha L + \alpha\Lambda)$$

and hence

$$|\delta_{m-k}| \leq 6 \binom{m}{k} x^k km(a\Lambda + \alpha L + \alpha\Lambda) .$$

Now suppose that we start our computation with a precision P, i.e. we compute P digits of the L-values and the matrix entries. Let $s, t, u \in \mathbb{N}$ be defined as

$$s := \lceil \log_{10}(a) \rceil , \qquad t := \lceil \log_{10}(L) \rceil , \qquad u := \max_{1 \leq k \leq m-1} \lceil |\log_{10}(|d_k|)| \rceil . \tag{5.2.2}$$

Then we get $\alpha \leq 10^{s-P}$, $\Lambda \leq 10^{t-P}$ and hence

$$\begin{aligned}
|\delta_{m-k}| &\leq 6 \binom{m}{k} x^k km(10^{s+t-P} + 10^{s+t-P} + 10^{s+t-2P}) \\
&\leq 18 \binom{m}{k} x^k km \cdot 10^{s+t-P} .
\end{aligned}$$

Let P' be the necessary precision of the result, i.e. $10^{-P'} \leq \delta$, then we find

$$\begin{aligned}
& 10^{-P'} \geq \max_{1 \leq k \leq m-1} |\delta_{m-k}| \\
\Longleftarrow \quad & 10^{-P'} \geq \max_{1 \leq k \leq m-1} \left(18 \binom{m}{k} x^k km \cdot 10^{s+t-P} \right) \\
\Longleftarrow \quad & -P' \geq \max_{1 \leq k \leq m-1} \left(\lceil \log_{10}(18 \binom{m}{k} x^k km) \rceil \right) + s + t - P \\
\Longleftrightarrow \quad & P \geq \max_{1 \leq k \leq m-1} \left(\lceil \log_{10}(18 \binom{m}{k} x^k km) \rceil \right) + s + t + P' .
\end{aligned}$$

In order to satisfy the estimate (5.2.1), we also need

$$\begin{aligned} && 2m(a\Lambda + \alpha L + \alpha\Lambda) &\leq \frac{1}{4m^2} \\ \Longleftarrow && 6m \cdot 10^{s+t-P} &\leq \frac{1}{4m^2} \\ \Longleftrightarrow && s+t-P &\leq -\lceil \log_{10}(24m^3) \rceil \\ \Longleftrightarrow && P &\geq s+t+\lceil \log_{10}(24m^3) \rceil . \end{aligned}$$

Note that we also have to compute at least as many digits as necessary for the maximal (or minimal) coefficient, i.e. we also get an inequality $P \geq u + P'$. Hence, we choose the computation precision as

$$P = \max\left(u + P', s + t + \lceil \log_{10}(24m^3) \rceil, \max_{1 \leq k \leq m-1} \left(\lceil \log_{10}(18\binom{m}{k} x^k k m) \rceil \right) + s + t + P' \right) . \tag{5.2.3}$$

In our computations, we first compute the L-values with a low precision to determine s, t, u and x, then we define the correct precision as above and recompute the L-values with this new precision.

We summarize the computation of the conjugates $\varepsilon_{L_n,S}^{\sigma}$ in the

Algorithm 5.2.2. Input: L_n and K.

(1) Use the description in the beginning of Section 5.2.3 to determine the maximal accepted error δ.

(2) Determine the set S.

(3) Determine the necessary precision to obtain an exact result:

  (2.1) Compute $L_S'(\chi, 0)$ with low precision as described in Section 5.1.2.

  (2.2) Compute the matrix A and its inverse.

  (2.3) Compute the polynomial $\tau_1(f) \in \mathbb{R}[X]$.

  (2.4) Compute s, t and u as defined in (5.2.2) and determine the necessary precision P with (5.2.3).

(4) Compute $L_S'(\chi, 0)$, the matrix A^{-1} and $\tau_1(f)$ with the new precision.

(5) Use the procedure described in Section 5.2.2 to determine the coefficients b_k from the approximations $\tau_1(b_k)$ and the bounds for $\tau_2(b_k)$.

(6) Return the roots of f as elements of L_n, these are the conjugates $\varepsilon_{L_n,S}^{\sigma}$, together with a $\mathcal{G}_n$-action on these conjugates.

Remark 5.2.3. If we chose δ small enough, we will obtain exactly one lattice point for each coefficient b_k in step (5), i.e. the resulting Stark unit will be uniquely determined by this algorithm.

5.3 Examining Conjecture 4.2.9

By Corollary 4.3.9 (i), we can restrict ourselves to the case $S = S_\infty \cup S_{ram}(L/K) \cup S_p$. This implies that $V' \setminus V \subseteq S_p$, i.e. we can consider the simpler formulation given in Conjecture 4.2.9. Moreover, since K is real quadratic, we have $e \leq 2$. If $e = 0$, we get $\beta_{L_n,S} = \varepsilon_{L_n,S}$ and hence $\kappa_{L,S,n} = 1$ for all n, so there is nothing to check.

5.3.1 The case $e = 1$

This is either the case if p is non-split in K or $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ where $\mathfrak{p}$ is completely split in L and $\mathfrak{p}'$ not. Then we can simplify the statement of Conjecture 4.2.9 considerably. First of all, we only consider $i = 1$ (since there are no other completely split primes over p) and we get $\eta_{L,S\setminus\{\mathfrak{p}\}} \in \mathbb{Q} \bigcap^1 \mathcal{O}_{L,S\setminus\{\mathfrak{p}\}}$. In fact, we can even determine the coefficient due to Lemma 2.4.1 (ii), namely we get

$$\eta_{L,S\setminus\{\mathfrak{p}\}} = \varepsilon_{L,S\setminus\{\mathfrak{p}\}}^{1/2} .$$

Then Conjecture 4.2.9 simplifies to

$$\mathrm{Ord}_{\mathfrak{P}}(\kappa_{L,S}) = \frac{1}{\omega} \mathrm{Log}_{\mathfrak{P}}(\varepsilon_{L,S\setminus\{\mathfrak{p}\}}) .$$

Inserting the definitions of $\mathrm{Ord}_{\mathfrak{P}}$ and $\mathrm{Log}_{\mathfrak{P}}$ and comparing coefficients then yields

$$\mathrm{ord}_{\sigma\mathfrak{P}}(\kappa_{L,S}) = \frac{1}{\omega} \log_p(N_{L_{\mathfrak{P}}/\mathbb{Q}_p}(\varepsilon^{\sigma}_{L,S\setminus\{\mathfrak{p}\}})) \tag{5.3.1}$$

for all $\sigma \in G$.

To check these equalities on a level n, we apply the following

Algorithm 5.3.1. Input: L, K, n and p.

(1) Generate the field L_n.

(2) Apply Algorithm 5.2.2 to compute the conjugates $\varepsilon^{\sigma}_{L_n,S}$ for $\sigma \in \mathcal{G}_n$.

(3) Determine the topological generator $\gamma := \mathrm{rec}_{\mathfrak{P}}(1+p)^{-1}$ as an element of Γ_n and compute ω.

(4) Apply Hilbert's Theorem 90 to compute the conjugates $\beta^{\sigma}_{L_n,S}$ for $\sigma \in \mathcal{G}_n$.

(5) Compute $\kappa_{L,S,n} = \prod_{\sigma\in\Gamma_n} \beta^{\sigma}_{L_n,S}$ and its conjugates (as elements of L_n).

(6) Identify $\kappa^{\sigma}_{L,S,n}$ with the corresponding element in L.

(7) Compute $\mathrm{ord}_{\sigma\mathfrak{P}}(\kappa_{L,S,n}) \mod p^n$.

(8) Apply Algorithm 5.2.2 to compute $\varepsilon^{\sigma}_{L,S\setminus\{\mathfrak{p}\}}$ for $\sigma \in G$.

(9) Compute $\log_p(N_{L_{\mathfrak{P}}/\mathbb{Q}_p}(\varepsilon^{\sigma}_{L,S\setminus\{\mathfrak{p}\}}))$ and compare both sides of (5.3.1).

For the computation of $\mathrm{rec}_{\mathfrak{P}}(1+p)^{-1}$ in step (3) we use the algorithm described in [Ble03, §3.2]. By the diagram (4.3.2), we get that the cyclotomic character sends the resulting element to

$$N_{L_{\mathfrak{P}}/\mathbb{Q}_p}(1+p) = \begin{cases} 1+2p+p^2, & p \text{ non-split}, \\ 1+p, & p \text{ split}. \end{cases}$$

In both cases, we see that the result generates $1+p\mathbb{Z}_p$, i.e. we find that $\gamma := \mathrm{rec}_{\mathfrak{P}}(1+p)^{-1}$ is indeed a topological generator of Γ. By Corollary 4.3.9 (iii), we can use this choice for the desired verification.

For step (4), we use the constructive proof of Hilbert's Theorem 90, given in [Neu92, Ch. IV, Thm. (3.5)]. The algorithm for this was provided by W. Bley.

For the identification in step (6), we use the minimal polynomial of $\kappa_{L,S,n}$ over K, which we can compute since we know all the conjugates of $\kappa_{L,S,n}$.

For the local computations in step (9), we use the identification

$$\mathcal{O}_L/\mathfrak{P}^t \cong \mathcal{O}_{L_{\mathfrak{P}}}/\mathfrak{P}^t\mathcal{O}_{L_{\mathfrak{P}}} \cong \mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p}^t\mathcal{O}_{K_{\mathfrak{p}}} \cong \mathcal{O}_K/\mathfrak{p}^t$$

for any $t \geq 1$. If we want to compute $\log_p(N_{L_{\mathfrak{P}}/\mathbb{Q}_p}(x))$ for some $x \in \mathcal{O}_L$, we can hence find an element $x_K \in \mathcal{O}_K$ such that $x_K \equiv x \mod \mathfrak{P}^t$. Now if p is split in K, we can use the same method to find an element $x_{\mathbb{Z}} \in \mathbb{Z}$ such that $x_{\mathbb{Z}} \equiv x_K \mod \mathfrak{p}^t$ and indeed, $x_{\mathbb{Z}} \equiv N_{L_{\mathfrak{P}}/\mathbb{Q}_p}(x) \mod p^t$ in this case. If p is non-split, we find that

$$N_{L_{\mathfrak{P}}/\mathbb{Q}_p}(x) \equiv N_{K_{\mathfrak{p}}/\mathbb{Q}_p}(x_K) \equiv N_{K/\mathbb{Q}}(x_K) \mod p^t.$$

Hence, we can reduce the local computations to the described global computations if we restrict to a p-adic precision t. Since we can only compare both sides of (5.3.1) up to level n anyway, it suffices to take $t > n$ big enough such that the p-adic logarithm can be computed up to precision n.

For the computation of $\log_p$, we now decompose $x_{\mathbb{Z}}$ into $\zeta \in \mu_{p-1}$ and $b \in 1+p\mathbb{Z}_p$. This decomposition can again be done with the global elements and we use a variant of an algorithm provided by W. Bley. Then $\log_p(x_{\mathbb{Z}}) = \log_p(b)$ can be explicitly calculated with the power series from [Neu92, Ch. II, Thm. (5.4)].

5.3.2 The case $e = 2$

This can only be the case when p is split in K and both primes $\mathfrak{p}$ and $\mathfrak{p}'$ above p are completely split in L, i.e. p is completely split in L. So we have to compute $\eta_{L,S\setminus\{\mathfrak{p}\}} \in \mathbb{Q}\bigwedge^2 \mathcal{O}_{L,S\setminus\{\mathfrak{p}\}}^\times$ and $\eta_{L,S\setminus\{\mathfrak{p}'\}} \in \mathbb{Q}\bigwedge^2 \mathcal{O}_{L,S\setminus\{\mathfrak{p}'\}}^\times$. For the computations in exterior powers, it is convenient to use the T-modified version. Then we can apply Algorithm 5.1.8 and we obtain

$$\eta_{L,S\setminus\{\mathfrak{p}\},T} = \lambda_T u_{1,T} \wedge u_{2,T} = \sum_{[\chi]} e_{[\chi]}\lambda_{[\chi],\mathbb{Q}} u_{i_1([\chi])} \wedge u_{i_2([\chi])}\,,$$

$$\eta_{L,S\setminus\{\mathfrak{p}'\},T} = \lambda'_T u'_{1,T} \wedge u'_{2,T} = \sum_{[\chi]} e_{[\chi]}\lambda'_{[\chi],\mathbb{Q}} u'_{i_1([\chi])} \wedge u'_{i_2([\chi])}\,.$$

Then Conjecture 4.2.15 is equivalent to

$$\mathrm{Ord}_{\mathfrak{P}}(\kappa_{L,S,T}) = -\sum_{[\chi]} \frac{e_{[\chi]}\lambda_{[\chi],\mathbb{Q}}}{\omega^2} \det \begin{pmatrix} \mathrm{Log}_{\mathfrak{P}}(u_{i_1([\chi])}) & \mathrm{Log}_{\mathfrak{P}'}(u_{i_1([\chi])}) \\ \mathrm{Log}_{\mathfrak{P}}(u_{i_2([\chi])}) & \mathrm{Log}_{\mathfrak{P}'}(u_{i_2([\chi])}) \end{pmatrix},$$

$$\mathrm{Ord}_{\mathfrak{P}'}(\kappa_{L,S,T}) = \sum_{[\chi]} \frac{e_{[\chi]}\lambda'_{[\chi],\mathbb{Q}}}{\omega^2} \det \begin{pmatrix} \mathrm{Log}_{\mathfrak{P}}(u'_{i_1([\chi])}) & \mathrm{Log}_{\mathfrak{P}'}(u'_{i_1([\chi])}) \\ \mathrm{Log}_{\mathfrak{P}}(u'_{i_2([\chi])}) & \mathrm{Log}_{\mathfrak{P}'}(u'_{i_2([\chi])}) \end{pmatrix}.$$

By Corollary 4.3.9 (ii), it suffices to check one of the above equations. We first apply the steps (1)-(4) of Algorithm 5.3.1. Note the element $\alpha_{L_n,S}$, obtained from Hilbert's Theorem 90, is not the desired $\beta_{L_n,S}$. Now we can check whether $N_{L_n/L}(\alpha_{L_n,S})$ is a p^n-th power in L by determining the roots of the polynomial $x^{p^n} - N_{L_n/L}(\alpha_{L_n,S})$ in L. If we find such a root, we can divide by this root to obtain $\alpha'_{L_n,S}$ such that $N_{L_n/L}(\alpha'_{L_n,S}) = 1$, hence we can apply Hilbert's Theorem 90 a second time to obtain $\beta_{L_n,S}$. This proves Conjecture 4.2.3 in this setting up to level n under the assumption that Stark's conjecture holds for level n. Then we can compute $\kappa^{\sigma}_{L,S,n}$ for $\sigma \in G$ as in the previous section. So the left hand side can be directly computed as

$$\mathrm{Ord}_{\mathfrak{P}}(\kappa_{L,S,T,n}) = \frac{\delta_T(0)}{2}\,\mathrm{Ord}_{\mathfrak{P}}(\kappa_{L,S,n}),$$

in $\mathbb{Z}/p^n\mathbb{Z}[G]$. For the right hand side, we use Algorithm 5.1.8 for the Rubin-Stark elements. We can again choose $\gamma = \mathrm{rec}_{\mathfrak{P}}(1+p)^{-1}$ and hence we can perform the local computations analogously to the $e = 1$-case to obtain the matrix entries as elements of $\mathbb{Z}/p^t\mathbb{Z}[G]$, where t is the precision of the local computations. Then we can clearly compute the right hand side and if we chose t big enough, we can again compare both sides modulo p^n.

By Theorem 4.3.2, the procedure described above gives an algorithm to verify $\mathrm{IMRS}(L/K, S, T, 1)_p$ up to level n under the assumption that the Rubin-Stark conjecture holds for the extension L/K and that Stark's conjecture holds for level n.

5.4 Computational results

The algorithms described above can in fact be applied to an arbitrary extension L of a real quadratic number field K. However, the computation of the unit groups (which are necessary to compute Rubin-Stark elements) are very expensive and should only be applied to extension of low degree (the author experienced that for fields with $[L : \mathbb{Q}] > 30$ the computation may take more than 24 hours or fail completely). Another limiting factor is the computation of L-values with high precision. As we have seen in Section 5.2.3, the necessary precision grows logarithmically with the absolute value of the L-values and the resulting polynomial coefficients. The computations show that these values can be very large even in rather small extensions, so the resulting necessary precision and hence the computation costs also grow fast. Moreover, the computation of the exact roots in the number field L_n as well as determining the maximal accepted error δ may be very time consuming and need a lot of memory. The author successfully tested the computation of Stark units in a field of degree $[L : \mathbb{Q}] = 56$ with a necessary precision of 167. The computation needed about 48 hours on a laptop with 1.80 GHz and 8 GB RAM.

After these introductory remarks on the limitations, we will now see how to construct non-trivial examples for the computations. For simplicity, we restrict to the case of cyclic extensions L/K. We start by fixing a degree, e.g. $deg = 4$, and an upper (resp. lower) bound $d_{\max}$ (resp. $d_{\min}$) for d, where $K = \mathbb{Q}(\sqrt{d})$. Moreover, we choose an upper (resp. lower) bound $f_{\max}$ (resp. $f_{\min}$) for the minimal integer contained in the conductor of our desired extension L. The author always used the natural lower bounds $d_{\min} = 2$ and $f_{\min} = 1$, but it would be possible to restrict the considered cases by these bounds even further. We also fix a list of primes which will be considered, e.g. 3 and 5.

For each square-free d, we then construct the real quadratic field $K = \mathbb{Q}(\sqrt{d})$ and compute a list of all ideals $\mathfrak{f}$ up to $f_{\max}$ of $\mathcal{O}_K$. We can reduce this list by requiring that the norm of $\mathfrak{f}$ is greater than $f_{\min}$ and also greater than $f_{\max}/m$, where m is the smallest non-trivial norm of ideals in the list (i.e. $m \leq 4$). For the remaining candidates $\mathfrak{f}$, we compute the ray class group $G_{\mathfrak{f}\infty_1\infty_2}$ and all subgroups H of $G_{\mathfrak{f}\infty_1\infty_2}$ such that the quotient $Q := G_{\mathfrak{f}\infty_1\infty_2}/H$ has exactly deg elements. If this quotient is cyclic, we construct the abelian extension L/K with Galois group Q. In the next step, we iterate through our chosen primes and check for each $\mathfrak{p} \subseteq \mathcal{O}_K$ if $\mathfrak{p}$ splits completely in L. If one of the infinite places of K splits completely in L while the other one does not, we find that L satisfies all the necessary assumptions and we store L, p and e in a list of cases which should be investigated.

With this procedure, we also obtain fields with smaller conductors, since these can be obtained by quotients with a suitable subgroup H. However, if we choose the lower bound such that $f_{\min} > f_{\max}/m$, we will skip some conductors which are too small to have norm greater than $f_{\min}$, but too big to correspond to such a quotient.

The author used this method with $deg = 4$, $d_{\max} = 70$ and $f_{\max} = 60$. We hence covered the cases

$$d \in \{2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 33, 34, 35, 37, 38, 39, 41, 42, 43, 46, 47, 51, 53, 55, 57, 58, 59, 61, 62, 65, 66, 67, 69, 70\}$$

for the primes 3 and 5. This results in 170 cases of interest distributed as seen in Table 5.1:

p \ e	1		2
	split	non-split	
3	4	52	2
5	16	88	8

Table 5.1: Number of cases for p and e with the chosen bounds

The relevant base fields for these cases correspond to

$$d \in \{13, 14, 21, 22, 26, 30, 35, 38, 39, 41, 42, 43, 53, 55, 58, 61, 65, 66, 69, 70\}.$$

Choosing $n = 1$, the author checked Conjecture 4.2.15 in all these cases on the first level with a positive result. The author was also able to compute several singular cases for $p = 7$ and $n = 1$ with a positive result. These results are again based on the assumption that the Rubin-Stark conjecture holds for L/K and Stark's conjecture holds for L_1/K.

Bibliography

[BO01] Jean-Robert Belliard and Hassan Oukhaba. “Sur la torsion de la distribution ordinaire universelle attachée à un corps de nombres”. In: *Manuscripta Math.* 106.1 (2001), pp. 117–130.

[Ble03] Werner Bley. “Numerical evidence for a conjectural generalization of Hilbert’s Theorem 132”. In: *LMS J. Comput. Math.* 6 (2003), pp. 68–88.

[Ble04] Werner Bley. “Wild Euler systems of elliptic units and the equivariant Tamagawa number conjecture”. In: *J. Reine Angew. Math.* 577 (2004), pp. 117–146.

[Ble06] Werner Bley. “Equivariant Tamagawa number conjecture for abelian extensions of a quadratic imaginary field”. In: *Doc. Math.* 11 (2006), pp. 73–118.

[BH20] Werner Bley and Martin Hofer. “Construction of elliptic $\mathfrak{p}$-units”. In: *Development of Iwasawa Theory - the Centennial of K. Iwasawa’s Birth*. Advanced Studies in Pure Mathematics 86. 2020, pp. 79–111.

[BD21] Dominik Bullach and Alexandre Daoud. *On Universal Norms for p-adic Representations in Higher Rank Iwasawa Theory*. To appear in Acta Arith. 2021. arXiv: `2007.07454 [math.NT]`.

[BH21] Dominik Bullach and Martin Hofer. *On trivial zeroes of Euler systems for $\mathbb{G}_m$*. 2021. arXiv: `2102.01545 [math.NT]`.

[Bur07] David Burns. “Congruences between derivatives of abelian L-functions at $s = 0$”. In: *Invent. Math.* 169.3 (2007), pp. 451–499.

[Bur11] David Burns. “Congruences between derivatives of geometric L-functions”. In: *Invent. Math.* 184.2 (2011), pp. 221–256.

[BG03] David Burns and Cornelius Greither. “On the equivariant Tamagawa number conjecture for Tate motives”. In: *Invent. Math.* 153.2 (2003), pp. 303–359.

[BKS16] David Burns, Masato Kurihara, and Takamichi Sano. “On zeta elements for $\mathbb{G}_m$”. In: *Doc. Math.* 21 (2016), pp. 555–626.

[BKS17] David Burns, Masato Kurihara, and Takamichi Sano. “On Iwasawa theory, zeta elements for $\mathbb{G}_m$, and the equivariant Tamagawa number conjecture”. In: *Algebra Number Theory* 11.7 (2017), pp. 1527–1571.

[CK19] Hugo Chapdelaine and Radan Kučera. “Annihilators of the ideal class group of a cyclic extension of an imaginary quadratic field”. In: *Canad. J. Math.* 71.6 (2019), pp. 1395–1419.

[Coh93] Henri Cohen. *A course in computational algebraic number theory*. Vol. 138. Graduate Texts in Mathematics. Springer-Verlag, Berlin, 1993.

[DK20] Samit Dasgupta and Mahesh Kakde. *On the Brumer-Stark Conjecture*. 2020. arXiv: `2010.00657 [math.NT]`.

[DR80] Pierre Deligne and Kenneth A. Ribet. “Values of abelian L-functions at negative integers over totally real fields”. In: *Invent. Math.* 59.3 (1980), pp. 227–286.

[Dok04] Tim Dokchitser. “Computing special values of motivic L-functions”. In: *Experiment. Math.* 13.2 (2004), pp. 137–149.

[Dri74] Vladimir G. Drinfel’d. “Elliptic modules”. In: *Mat. Sb. (N.S.)* 94(136) (1974), pp. 594–627, 656.

[DST97] David S. Dummit, Jonathan W. Sands, and Brett A. Tangedal. “Computing Stark units for totally real cubic fields”. In: *Math. Comp.* 66.219 (1997), pp. 1239–1267.

[FX96] Keqin Feng and Fei Xu. “Kolyvagin’s “Euler systems” in cyclotomic function fields”. In: *J. Number Theory* 57.1 (1996), pp. 114–121.

[Fla11] Matthias Flach. “On the cyclotomic main conjecture for the prime 2”. In: *J. Reine Angew. Math.* 661 (2011), pp. 1–36.

[Fra20] Pavel Francírek. “Annihilators of the ideal class group of an imaginary cyclic field”. In: *J. Number Theory* 213 (2020), pp. 187–220.

[Gra77] Georges Gras. “Classes d’idéaux des corps abéliens et nombres de Bernoulli généralisés”. In: *Ann. Inst. Fourier (Grenoble)* 27.1 (1977), pp. ix, 1–66.

[GK04] Cornelius Greither and Radan Kučera. “Annihilators for the class group of a cyclic field of prime power degree”. In: *Acta Arith.* 112.2 (2004), pp. 177–198.

[GK06] Cornelius Greither and Radan Kučera. “Annihilators for the class group of a cyclic field of prime power degree. II”. In: *Canad. J. Math.* 58.3 (2006), pp. 580–599.

[GK14a] Cornelius Greither and Radan Kučera. “Eigenspaces of the ideal class group”. In: *Ann. Inst. Fourier (Grenoble)* 64.5 (2014), pp. 2165–2203.

[GK14b] Cornelius Greither and Radan Kučera. “Linear forms on Sinnott’s module”. In: *J. Number Theory* 141 (2014), pp. 324–342.

[GK15] Cornelius Greither and Radan Kučera. “Annihilators for the class group of a cyclic field of prime power degree III”. In: *Publ. Math. Debrecen* 86.3-4 (2015), pp. 401–421.

[GK20a] Cornelius Greither and Radan Kučera. “On the compositum of orthogonal cyclic fields of the same odd prime degree”. In: *Canad. J. Math.* (2020), pp. 1–25.

[GK20b] Cornelius Greither and Radan Kučera. “Washington units, semispecial units, and annihilation of class groups”. In: *Manuscripta Math.* (2020).

[Hay74] David R. Hayes. “Explicit class field theory for rational function fields”. In: *Trans. Amer. Math. Soc.* 189 (1974), pp. 77–91.

[Hay79] David R. Hayes. “Explicit class field theory in global function fields”. In: *Studies in algebra and number theory*. Vol. 6. Adv. in Math. Suppl. Stud. Academic Press, New York-London, 1979, pp. 173–217.

[Hay85] David R. Hayes. “Stickelberger elements in function fields”. In: *Compositio Math.* 55.2 (1985), pp. 209–239.

[Hof18] Hofer, Martin. “Elliptic $\mathfrak{p}$-units and the equivariant Tamagawa Number Conjecture”. PhD thesis. Ludwig-Maximilians-Universität München, 2018.

[Kol88] Victor A. Kolyvagin. “Finiteness of $E(\mathbf{Q})$ and $Ш(E, \mathbf{Q})$ for a subclass of Weil curves”. In: *Izv. Akad. Nauk SSSR Ser. Mat.* 52.3 (1988), pp. 522–540, 670–671.

[Kol90] Victor A. Kolyvagin. “Euler systems”. In: *The Grothendieck Festschrift, Vol. II*. Vol. 87. Progr. Math. Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.

[MR11] Barry Mazur and Karl Rubin. “Refined class number formulas and Kolyvagin systems”. In: *Compos. Math.* 147.1 (2011), pp. 56–74.

[MW84] Barry Mazur and Andrew Wiles. “Class fields of abelian extensions of $\mathbf{Q}$”. In: *Invent. Math.* 76.2 (1984), pp. 179–330.

[MSV19] Kevin J. McGown, Jonathan W. Sands, and Daniel Vallières. “Numerical evidence for higher order Stark-type conjectures”. In: *Math. Comp.* 88.315 (2019), pp. 389–420.

[Neu92] Jürgen Neukirch. *Algebraische Zahlentheorie*. Springer-Verlag, Berlin, 1992.

[Neu11] Jürgen Neukirch. *Klassenkörpertheorie*. Springer-Lehrbuch. [Springer Textbook]. Newly edited and with a foreword by Alexander Schmidt. Springer, Heidelberg, 2011.

[Ouk92] Hassan Oukhaba. “Groups of elliptic units in global function fields”. In: *The arithmetic of function fields (Columbus, OH, 1991)*. Vol. 2. Ohio State Univ. Math. Res. Inst. Publ. de Gruyter, Berlin, 1992, pp. 87–102.

[Ouk95] Hassan Oukhaba. “Construction of elliptic units in function fields”. In: *Number theory (Paris, 1992–1993)*. Vol. 215. London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 1995, pp. 187–208.

[Ouk97] Hassan Oukhaba. “Groups of elliptic units and torsion points of Drinfeld modules”. In: *Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996)*. World Sci. Publ., River Edge, NJ, 1997, pp. 298–310.

[Ouk03] Hassan Oukhaba. “Index formulas for ramified elliptic units”. In: *Compositio Math.* 137.1 (2003), pp. 1–22.

[Pop99] Cristian D. Popescu. “Gras-type conjectures for function fields”. In: *Compositio Math.* 118.3 (1999), pp. 263–290.

[Pop02] Cristian D. Popescu. “Base change for Stark-type conjectures “over $\mathbb{Z}$””. In: *J. Reine Angew. Math.* 542 (2002), pp. 85–111.

[Pop11] Cristian D. Popescu. “Integral and p-adic refinements of the abelian Stark conjecture”. In: *Arithmetic of L-functions*. Vol. 18. IAS/Park City Math. Ser. Amer. Math. Soc., Providence, RI, 2011, pp. 45–101.

[Rob97] Xavier-François Roblot. “Algorithmes de factorisation dans les extensions relatives et applications de la conjecture de Stark à la construction des corps de classes de rayon”. PhD thesis. Université Bordeaux I, 1997.

[Ros02] Michael Rosen. *Number theory in function fields.* Vol. 210. Graduate Texts in Mathematics. Springer-Verlag, New York, 2002.

[Rub87] Karl Rubin. “Global units and ideal class groups”. In: *Invent. Math.* 89.3 (1987), pp. 511–526.

[Rub96] Karl Rubin. “A Stark conjecture “over **Z**” for abelian L-functions with multiple zeros”. In: *Ann. Inst. Fourier (Grenoble)* 46.1 (1996), pp. 33–62.

[Rub00] Karl Rubin. *Euler systems.* Vol. 147. Annals of Mathematics Studies. Hermann Weyl Lectures. The Institute for Advanced Study. Princeton University Press, Princeton, NJ, 2000, pp. xii+227.

[San14] Takamichi Sano. “Refined abelian Stark conjectures and the equivariant leading term conjecture of Burns”. In: *Compos. Math.* 150.11 (2014), pp. 1809–1835.

[Sie70] Carl L. Siegel. “Über die Fourierschen Koeffizienten von Modulformen”. In: *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II* 1970 (1970), pp. 15–56.

[Sin80] Warren Sinnott. “On the Stickelberger ideal and the circular units of an abelian field”. In: *Invent. Math.* 62.2 (1980), pp. 181–234.

[Sol92] David Solomon. “On a construction of p-units in abelian fields”. In: *Invent. Math.* 109.2 (1992), pp. 329–350.

[Sta71] Harold M. Stark. “Values of L-functions at $s = 1$. I. L-functions for quadratic forms”. In: *Advances in Math.* 7 (1971), pp. 301–343.

[Sta75] Harold M. Stark. “L-functions at $s = 1$. II. Artin L-functions with rational characters”. In: *Advances in Math.* 17.1 (1975), pp. 60–92.

[Sta76] Harold M. Stark. “L-functions at $s = 1$. III. Totally real fields and Hilbert’s twelfth problem”. In: *Advances in Math.* 22.1 (1976), pp. 64–84.

[Sta80] Harold M. Stark. “L-functions at $s = 1$. IV. First derivatives at $s = 0$”. In: *Adv. in Math.* 35.3 (1980), pp. 197–235.

[Sti90] Ludwig Stickelberger. “Ueber eine Verallgemeinerung der Kreistheilung”. In: *Math. Ann.* 37.3 (1890), pp. 321–367.

[Stu20] Pascal Stucky. “Annihilators of the ideal class group of a cyclic extension of a global function field”. In: (2020). To appear in Acta Arith. arXiv: `2011.08776 [math.NT]`.

[Tat81a] John Tate. “Brumer-Stark-Stickelberger”. In: *Seminar on Number Theory, 1980–1981 (Talence, 1980–1981).* Univ. Bordeaux I, Talence, 1981, Exp. No. 24, 16.

[Tat81b] John Tate. “On Stark’s conjectures on the behavior of $L(s, \chi)$ at $s = 0$”. In: *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 28.3 (1981), 963–978 (1982).

[Tat84] John Tate. *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$*. Vol. 47. Progress in Mathematics. Lecture notes edited by Dominique Bernardi and Norbert Schappacher. Birkhäuser Boston, Inc., Boston, MA, 1984.

[Tha88] Francisco Thaine. "On the ideal class groups of real abelian number fields". In: *Ann. of Math. (2)* 128.1 (1988), pp. 1–18.

[Wei94] Charles A. Weibel. *An introduction to homological algebra*. Vol. 38. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1994.

[XZ01] Fei Xu and Jianqiang Zhao. "Euler systems in global function fields". In: *Israel J. Math.* 124 (2001), pp. 367–379.

[Yin97] Linsheng Yin. "On the index of cyclotomic units in characteristic p and its applications". In: *J. Number Theory* 63.2 (1997), pp. 302–324.

Eidesstattliche Versicherung

(Siehe Promotionsordnung vom 12.07.11, § 8, Abs. 2 Pkt. .5.)

Hiermit erkläre ich an Eidesstatt, dass die Dissertation von mir selbstständig, ohne unerlaubte Beihilfe angefertigt ist.

Stucky, Pascal

Name, Vorname

München, 14.12.2021

Ort, Datum

Pascal Stucky

Unterschrift Doktorand/in

Formular 3.2