Congruences satisfied by Stark units

Anthony Hayward

Ph.D. Thesis

King's College London

Abstract

"Refined abelian Stark conjectures" are special value conjectures for L-functions associated to abelian extensions of global fields at the origin. We review the conjectures of Rubin-Stark and Gross, and describe a common refinement formulated by Burns. This refined conjecture is the main object of study in this thesis.

Having formulated the conjecture, we study its behaviour with respect to variation of the data on which it depends. Combining these results with ideas of Rubin and Gross yields a complete proof in the case of extensions of degree two.

We also look at the case of base fields which have at most one infinite place, where we axiomatise the explicit Stark units known over such fields, and verify the axioms by analytic constructions in each context. This then leads to a proof of the conjecture in a wide range of cases, for example, odd-degree extensions of $\mathbb{Q}$.

The conjecture of Burns provides interpretation of conjectures of Darmon and Gross as accounting for its behaviour under quadratic extension of the base field. We state and prove these interpretations.

Acknowledgements

I would like to thank David Burns for his help and tireless encouragement, and for suggesting this topic of study. I also wish to thank Radan Ku čera, whose meticulous reading of much of this material led to a large number of corrections, and Werner Bley, Manuel Breuning, Cornelius Greither, William Hart and David Solomon, who all gave me helpful suggestions and advice.

I received funding during the work on this thesis from the Engineering and Physical Sciences Research Council, to whom I am very grateful.

Contents

Chapter 1

Introduction

An algebraic object such as an extension of number fields possesses an array of invariants, which may be crudely divided into two kinds: the analytic and the algebraic. Algebraic invariants come from (loosely-speaking) looking at the object "one bit at a time", while analytic invariants correspond to combining infinitely many of these parts via a limiting process. Many of the greatest advances in the history of number theory have come from comparing invariants of these two different natures – one striking example (amongst many possibilities) would be the original proof of the prime number theorem. The analytic invariant involved in this is the Riemann zeta-function, the beginning point for the theory of L-functions in general, which in their various guises have proved to be analytic invariants which encode information about the original object with supreme subtlety. It is surely unnecessary to argue the importance of L-functions to the history of number theory.

The objects of study of this thesis are special value conjectures (at the origin) for Dirichlet L-functions associated to abelian extensions of global fields. Two classical results give tantalising indications of relations between such analytic invariants and algebraic ones. Firstly, the analytic class number formula relates the leading term at 0 of a zeta-function to two algebraic invariants of the field: the class number and the unit group. Secondly, the value at 0 of the derivative of an L-function associated to an even Dirichlet character χ mod m may be expressed in terms of absolute values of a cyclotomic element $(1-\zeta_m)(1-\zeta_m^{-1})$. Interpreting χ as a character of the Galois group of the abelian extension $\mathbb{Q}(\zeta_m)^+/\mathbb{Q}$, we have a relation between a special value of the L-function of a Galois character at $s=0$ and an integer of restricted support ("S-unit") of the top field. That such relations should in fact be a general phenomenon is the core idea of Stark's conjectures, developed in a series of papers ([42] – [45]) in the 1970s, which led to a proliferation of special value conjectures in the following years. The S-units appearing also have applications to the problem of explicit generation of class fields (Hilbert's twelfth problem), a fascinating question which however we will not consider further, except to note that the computer system PARI [30] makes use of the assertion of Stark's conjecture for exactly this purpose. Stark also considered this application of his conjecture in [44].

The "refined abelian Stark conjecture", as it came to be known, is formulated with respect to an abelian extension K/k of global fields (with Galois group G), and a set S of places of the base field k. The set S is required to contain all infinite primes, and those ramified in K/k; in addition, the decomposition groups of elements of S control the order of vanishing of the L-functions of the characters of G at 0. Thus the fact that the conjecture concerns the first derivative of the S-truncated L-function at 0 restricts the class of K/k for which it is meaningful: for example, if k has two complex places then the first derivative, and the conjecture, are trivial. The conjecture of Rubin [39] removes this condition by allowing for any number r of totally split places in the set S, and specialises to Stark's conjecture in the case $r = 1$. However the new "Stark units" for the case $r > 1$ may no longer be taken to be S-units, but rather are combinations of them, in fact elements of (a vector space generated by) the r-th exterior power of the $\mathbb{Z}[G]$-module of S-units. At this (great) expense, Rubin produces a more flexible conjecture, which as well as recovering Stark's conjecture (and hence pertaining to the result about cyclotomic fields mentioned above), also finds a use in a special case for the analytic class number formula [39, Prop. 3.1]. Hence we see progressing conjectures capturing increasingly the analytic-algebraic relations which are to be found.

Subsequent to Rubin's conjecture, Popescu [34] formulated a slightly weaker version (still recovering Stark's conjecture) which had the advantage of a pleasant base-change property in a special case. For the purposes of the work discussed in this thesis, Rubin's conjecture will be the most applicable of the two. Rubin's conjecture makes sense also for $r = 0$, where it gives integrality properties for values of L-functions known to be true by work of Deligne, Ribet and Weil. In [18], Gross had formulated a conjecture for these values of a different kind: beginning from the integrality, he proposed a congruence in $\mathbb{Z}[G]$ between an equivariant combination of L-function values and the product of a class number by a certain "algebraic regulator". This regulator lies naturally in the $(\#S - 1)$-th power of the augmentation ideal of $\mathbb{Z}[G]$, and the congruence is modulo the next power of this ideal. Gross's conjecture was inspired in part by the work of Mazur and Tate on the arithmetic of modular curves. Most noteworthy for our present discussion is that Gross's conjecture involves a class number, and uses the S-unit group of k in its formulation of an algebraic regulator – both invariants which we noted to be related to special values by the analytic class number formula, but absent from the conjectures discussed so far. Unfortunately, the conjectures of Gross and Rubin exhibit a certain "orthogonality": passing from $r = 0$ to $r = 1$, Gross's conjecture becomes trivial (since the L-values are now all 0) while Rubin's conjecture goes from a known result to a somewhat inaccessible one (namely, Stark's conjecture). These two conjectures together therefore represent an unsatisfactory conjectural generalisation of the two classical results noted above, although each catches some aspects of them. It is clearly desirable to formulate a conjecture which captures both, and so gives a clearer picture of the analytic-algebraic relations which exist.

The conjectures of Rubin-Stark and Gross are both interesting, difficult and much studied (see e.g. [8]). But the above discussion shows that neither deserves to be seen as a satisfactory "big picture". The state-of-the-art answer to the question of what does deserve this title is the "equivariant Tamagawa number conjecture". This conjecture has its genesis in work of Bloch and Kato, was further developed by Fontaine and Perrin-Riou, and reaches its most general form in the formulation due to Burns and Flach [5]. Its intent fits neatly into the idea of relating analytic to algebraic invariants; the object of study being in general a motive, the analytic object a special value of a motivic L-function (at an integer), and the algebraic invariant a virtual object arising from motivic cohomology. In our context of abelian extensions of number fields, which correspond to "Tate motives", we recover Dirichlet L-functions, and there exists a pleasant "arithmetic" interpretation of the motivic cohomology (see [4, Prop. 3.1]). Indeed, under certain hypotheses it is possible to reformulate the equivariant Tamagawa number conjecture in terms of the existence of a set of units satisfying certain relations [3, Thm. 3.2]. But the important thing to note in the context of the present discussion is that the equivariant Tamagawa number conjecture is very general and much less ad hoc in its formulation than the conjectures mentioned previously. Its interpretation in a special case therefore carries a certain momentum behind it; indeed, it provides us with another special value conjecture which has the appealing property of being the specialisation of a much bigger philosophical framework, rather than an analogy, or generalisation of a special case. Recent work of Burns [6] seeks to explore the relationship between the specialisation of the equivariant Tamagawa number conjecture and various refined abelian Stark conjectures which have been postulated, including those explained above. The results are striking: the equivariant Tamagawa number conjecture recovers at least the essential aspects, and in many cases the whole statement, of all these conjectures. The results are given in [7], and some of them are mentioned below.

The equivariant Tamagawa number conjecture thus provides illumination and unification for the disparate collection of conjectures which constituted the field at the end of the 20th century. Its interpretation in terms of explicit units, moreover, led Burns to formulate a less "high-tech" conjecture directly unifying the conjectures of Gross and Rubin described above. This conjecture (Conjecture 3.5.1 below) arose following discussions with the author attempting to understand a conjecture of Darmon [12], a "refinement" of Gross's, in the context of Rubin's conjecture. Such an interpretation (Theorem 8.7.1 below) was subsequently proved by the author, as well as a number of other properties and special cases of Conjecture 3.5.1, in work which first appeared in [22] (although we note that Conjecture 3.5.1 is there only stated up to sign, a deficiency which is here removed). The conjecture adds to Rubin's conjecture a congruence in the style of Gross's, thereby overcoming the unfortunate "orthogonality" mentioned above. Indeed it comes close (bar a small-looking kernel) to recovering the analytic class number formula (Theorem 2.1), as well as capturing the abelian Stark conjecture. It therefore represents progress towards a theory which accounts for both of the classical phenomena noted above. The conjecture is proved in the special case of quadratic extensions below (Chapter 5); its formulation in this case gives an explanation of the power-of-two factor appearing in the formula for the Stark unit (5.4), and its proof provides a new proof of Gross's conjecture for quadratic extensions. This new proof is considerably smoother than the detailed consideration of special cases necessary in [18], due to the fact that Conjecture 3.5.1 allows S and r to be increased, which makes it possible to neuter an awkward class group. The mixture of Gross's and Rubin's ideas also sheds light on Gross's "conjecture on tori" [18, Conj. 8.8] and the conjecture of Darmon mentioned above, in that both can be interpreted as expressing the change in the statement of Conjecture 3.5.1 caused by replacing k by a quadratic extension, replacing K by its compositum with this extension, and increasing r appropriately (Theorems 8.7.1 and 8.9.2). This shows that the new conjecture provides both theoretical and practical advantages in the area.

In the second classical result mentioned at the start of this introduction, a cyclotomic element appeared as the Stark unit for a cyclotomic field. It is well-known that cyclotomic elements satisfy certain distribution properties with respect to norms, and indeed this is not restricted to this one context; in fact analogous units are known to exist in abelian extensions of two other kinds of fields: imaginary quadratic fields and global function fields. These are then all cases of global fields which have at most one archimedean place. We systematise the distribution relations and prove them in each context, the units being defined in quite different ways: via special values of elliptic functions for the imaginary quadratic fields, and division points on rank-one sign-normalised Drinfeld modules for function fields. In the case of elliptic units, we need a new result to show that the elliptic units used by Bley in [2] fit into this picture. After establishing that the special units satisfy the desired relations in all cases, and are all L-function evaluators, we proceed to use these relations to establish Conjecture 3.5.1 for a wide class of extensions of these three kinds of fields. The proof requires a study of the combinatorics of minors of matrices of zero row sum – we develop this theory in Chapter 7, §1 below – and also an integer identity dating back to Euler. This proof, as well as establishing the conjecture in new cases, gives a view of the conjecture and its various constructions in a very explicit setting. We note that this combinatorial approach was first suggested by work of Greither and Ku čera [17].

Gross's conjecture, and by extension Conjecture 3.5.1 below, involve the augmentation filtration of the group ring $\mathbb{Z}[G]$ for a finite abelian group G. For the study of these conjectures, it is helpful to understand the structure of this filtration. The structure is well understood when for each p the p-part of G is either cyclic or elementary abelian, but for other G it is rather tricky to deal with. The author carried out a computer investigation into this structure for certain small G not satisfying these simplifying conditions. The results are described in Chapter 9 below. In particular, we show that the conjectures cannot be reduced to statements only concerning cyclic subextensions of the given extension.

Chapter 2

Notation

1 Global fields

By a *global field* F we mean either a number field (i.e. a finite extension of the rational field $\mathbb{Q}$) or a global function field (a finite extension of the field of rational functions $\mathbb{F}(T)$, where $\mathbb{F}$ is a finite field). A *place* v of F is an equivalence class of absolute values on F, where two absolute values are equivalent if they define the same topology on F. We distinguish between archimedean (also called infinite) places and non-archimedean (finite) ones. Only number fields F have infinite places; we identify them with equivalence classes of embeddings $F \to \mathbb{C}$ under complex conjugation. If the image of an embedding is contained in $\mathbb{R}$, the corresponding infinite place is called *real* and the associated absolute value $|\cdot|_v$ is given by composing this embedding with the absolute value on $\mathbb{R}$; if not, the place is *complex*, and the absolute value is given by composing this with the square of the absolute value[1] on $\mathbb{C}$. The sum of the number of real places and twice the number of complex places is equal to the degree $[k : \mathbb{Q}]$ of the number field, and is therefore finite.

If v is a finite place, it is represented by an absolute value $|x|_v = \alpha^{v(x)}$, where α is any positive real number less than 1 and $x \mapsto v(x)$ is a uniquely determined surjective homomorphism $F^\times \to \mathbb{Z}$ which is a discrete valuation on F. If F is a number field, nontrivial discrete valuations v are in bijective correspondence with prime ideals $\mathfrak{p}$ of the ring of integers, and if F is a global function field, they correspond to primes $\mathfrak{p}$ of the field; we write $v_\mathfrak{p}$ for the discrete valuation associated to $\mathfrak{p}$. We choose a representative absolute value of the place by setting $|x|_v = N_v^{-v(x)}$ for all x in $F^\times$, where N_v denotes the number of elements of the residue field at v. We also write $N_\mathfrak{p} := N_{v_\mathfrak{p}}$.

Suppose S is a finite nonempty set of places of a global field F, such that S contains all infinite places. The ring of *S-integers* of F is the subset $\mathcal{O}_{F,S} = \{x \in F : v(x) \geq 0 \text{ for all } v \notin S\}$. If F is a number field and S is the set of infinite places

[1] This does not strictly give a field absolute value, due to the square. Removing this square does give an absolute value in the strict sense, which induces an equivalent metric on F.

only, this is $\mathcal{O}_F$, the ring of integers of F. The multiplicative group $\mathcal{O}_{F,S}^\times$ will be denoted $U_{F,S}$ and called the *S-units* of F. The following theorem of Dirichlet describes the abelian group structure of $U_{F,S}$:

Theorem 1.1 (Dirichlet's unit theorem). *The abelian group $U_{F,S}$ is the direct product of its torsion subgroup (a finite cyclic group) with a free subgroup of rank $\#S - 1$.*

The torsion subgroup of $U_{F,S}$ is independent of S and equal to the torsion subgroup of the multiplicative group $F^\times$; we denote it by μ_F, and its order by w_F.

The free abelian group on the finite places of F is called the divisor group of F, denoted $\mathcal{I}_F$. Those divisors all of whose coefficients are non-negative are called *effective divisors*, and these form a submonoid $\mathcal{I}_F^+$ of $\mathcal{I}_F$. A divisor is called coprime to S if no primes in S have nonzero coefficient; the group of such divisors is naturally isomorphic to the group of fractional ideals of $\mathcal{O}_{F,S}$, and denoted $\mathcal{I}_{F,S}$. There is a natural truncation map $\mathcal{I}_F \to \mathcal{I}_{F,S}$ defined by setting the coefficients of the primes which lie in S to 0. Any nonzero element x of F has an associated divisor (x) given by its valuations, and the group of these principal divisors will be denoted $\mathcal{P}_F$, with $\mathcal{P}_{F,S}$ the subgroup of the truncations at S of the principal divisors. The quotient $\mathcal{I}_{F,S}/\mathcal{P}_{F,S}$ is defined to be the *S-class group* of F, denoted $A_{F,S}$; it is the ideal class group of the ring $\mathcal{O}_{F,S}$. This group is finite since S is assumed to be nonempty. To summarise, we have an exact sequence

$$0 \longrightarrow U_{F,S} \longrightarrow F^\times \longrightarrow \mathcal{I}_{F,S} \longrightarrow A_{F,S} \longrightarrow 0. \tag{2.1}$$

Let $\mathfrak{t}$ be an ideal of $\mathcal{O}_{F,S}$, so that its support $\operatorname{Supp}(\mathfrak{t})$ is a finite collection of finite places not in S. An element $x \in k$ is said to satisfy $x \equiv 1 \pmod{\mathfrak{t}}$ if $v(x-1) \geq v(\mathfrak{t})$ for all $v \in \operatorname{Supp}(\mathfrak{t})$. We denote $U_{F,S,\mathfrak{t}} = \{x \in U_{F,S} : x \equiv 1 \pmod{\mathfrak{t}}\}$ the group of S-units congruent to 1 modulo $\mathfrak{t}$. We let $\mu_{F,\mathfrak{t}}$ be the subgroup of μ_F consisting of roots of unity congruent to 1 modulo $\mathfrak{t}$, and denote its size by $w_{F,\mathfrak{t}}$, so that $w_{F,\mathfrak{t}} = \#(U_{F,S,\mathfrak{t}})_{\mathrm{tors}}$. Let $\mathcal{P}_{F,S,\mathfrak{t}}$ denote the subgroup of $\mathcal{P}_{F,S}$ consisting of divisors (x) which have a generator x congruent to 1 modulo $\mathfrak{t}$, and note that this definition implies that $\mathcal{P}_{F,S,\mathfrak{t}}$ is contained in $\mathcal{I}_{F,S\cup\operatorname{Supp}(\mathfrak{t})}$. Define $A_{F,S,\mathfrak{t}} = \mathcal{I}_{F,S\cup\operatorname{Supp}(\mathfrak{t})}/\mathcal{P}_{F,S,\mathfrak{t}}$, the $(S,\mathfrak{t})$-class group of F.

The class groups fit into an exact sequence

$$0 \longrightarrow U_{F,S,\mathfrak{t}} \longrightarrow U_{F,S} \longrightarrow (\mathcal{O}_{F,S}/\mathfrak{t})^\times \longrightarrow A_{F,S,\mathfrak{t}} \longrightarrow A_{F,S} \longrightarrow 0, \tag{2.2}$$

The third arrow here is the reduction map, and the fourth takes a residue to the class of the principal ideal generated by an S-integer with that residue, which exists by the weak approximation theorem. The exactness is clear.

The sizes of the class groups define the S-class number $h_{F,S} = \#A_{F,S}$ and $(S,\mathfrak{t})$-class number $h_{F,S,\mathfrak{t}} = \#A_{F,S,\mathfrak{t}}$. Sequence (2.2) gives exact sequences of finite groups $0 \to U_{F,S}/U_{F,S,\mathfrak{t}} \to (\mathcal{O}_{F,S}/\mathfrak{t})^\times \to A_{F,S,\mathfrak{t}} \to A_{F,S} \to 0$ and $0 \to (\mathcal{O}_{F,S}/\mathfrak{t})^\times/\widetilde{U_{F,S}} \to A_{F,S,\mathfrak{t}} \to A_{F,S} \to 0$, where $\widetilde{U_{F,S}}$ denotes the image of $U_{F,S}$ in the residue ring. Since in such sequences the product of the sizes of the even-indexed terms is equal to that of the odd-indexed terms, we obtain the following formulas relating the class numbers:

$$h_{F,S,\mathfrak{t}} = h_{F,S}\frac{\#(\mathcal{O}_{F,S}/\mathfrak{t})^\times}{(U_{F,S} : U_{F,S,\mathfrak{t}})} = h_{F,S}\Big((\mathcal{O}_{F,S}/\mathfrak{t})^\times : \widetilde{U_{F,S}}\Big).$$

For the most part we will take $\mathfrak{t}$ to be a prime ideal or a square-free product of prime ideals. For consistency with much of the literature, when we do this we will set $T = \mathrm{Supp}(\mathfrak{t})$ and may write T in place of $\mathfrak{t}$ in the subscripts. We use the expression "x congruent to 1 modulo T" to mean that $v(x-1) > 0$ for all $v \in T$. Since for these square-free $\mathfrak{t}$ we have $\mathcal{O}_{F,S}/\mathfrak{t} \cong \prod_{v\in T}\mathbb{F}_v$, where $\mathbb{F}_v$ denotes the residue field of v, the last displayed equation gives

$$h_{F,S,T} = h_{F,S}\frac{\prod_{v\in T}(N_v - 1)}{(U_{F,S} : U_{F,S,T})}. \tag{2.3}$$

When F is a number field, we sometimes omit the subscripts S on the various objects defined in this section, on the understanding that this means S is to be taken to be the set of all archimedean places of F. Hence we write $\mathcal{O}_F$ (the ring of integers), U_F (the units), $\mathcal{I}_F$ and $\mathcal{P}_F$ (agreeing with our previous definitions), and A_F and h_F for the class group and class number.

2 Abelian extensions of global fields

Let K/k be an extension of global fields, and let S and T be sets of places of k as described in §1. Then we denote by S_K and T_K the sets of places of K lying above those in S and T respectively. We will usually denote places of k by v and places of K by w.

In this thesis we will always denote by K/k a finite abelian extension of global fields having group G. We will write the conjugate by an element g of an element x of K as x^g, and then since G is abelian we have $x^{gh} = (x^g)^h$ for all $g, h \in G$. The Galois group G acts on places w of K by the following transformation of absolute values:

$$|x|_{gw} = |x^{g^{-1}}|_w,$$

where $g \in G$ and x is any element of K. The action of G is transitive on the set of places lying above each place v of k. The stabiliser of a place w of K is the decomposition group G_w of the place, and we note that, since G is abelian, it only depends upon the place v of k induced by w and may therefore be written $G_v := G_w$.

Recall that we normalise the absolute value corresponding to a place w of K as follows:

$$|x|_w = \begin{cases} |x| & \text{if } K_w = \mathbb{R} \\ |x|^2 & \text{if } K_w = \mathbb{C} \\ N_w^{-w(x)} & \text{if } w \text{ is a finite place,} \end{cases}$$

where a finite place w is considered as a discrete valuation normalised so that its image is $\mathbb{Z}$. With these normalisations, the *product rule for absolute values* states that we have

$$\prod_{w \text{ place of } K} |x|_w = 1, \tag{2.4}$$

as in [23, Chap. V, §1].

For a finite place w of K lying over a place v of k, the inertia group I_w is defined to be the kernel of the quotient map $G_w \to \mathrm{Gal}(\mathbb{F}_w/\mathbb{F}_v)$, where $\mathbb{F}_w/\mathbb{F}_v$ is the residue field extension associated to w/v. If I_w is trivial, the place v is called unramified. Almost all places are unramified – a finite place can only ramify if it divides the discriminant of the extension K/k.

The Galois group $\mathrm{Gal}(\mathbb{F}_w/\mathbb{F}_v)$ is cyclic, generated by the *(arithmetic) Frobenius automorphism*

$$\begin{array}{rccc} \sigma_w : & \mathbb{F}_w & \longrightarrow & \mathbb{F}_w \\ & x & \longmapsto & x^{N_v}. \end{array}$$

The Frobenius may also be considered as an element of G_w/I_w. If I_w is trivial, i.e. w/v is unramified, then G_w is cyclic, generated by the Frobenius σ_w. Given v, the objects σ_w and I_w only depend on w up to conjugation in G, and so, since G is abelian, we may write σ_v and I_v instead. The choice of Frobenius also leads to the definition of the *local reciprocity map* (see [41, Ch. XIII, §4]), which is a homomorphism $(-, K_w/k_v) : k_v^\times \to G_v$ (independent of choice of w above v). This has the properties that $(x, K_w/k_v) \in I_v$ if $v(x) = 0$ and $(x, K_w/k_v) = \sigma_v^{v(x)}$ if w/v is unramified.

We may also make the definitions of the previous two paragraphs for an extension of infinite places w/v of K. If w is real or v is complex, then G_w is trivial and so $\sigma_v := 1$. Otherwise w is complex and v is real, so that G_w has order 2. The nontrivial element of this group is taken for σ_v, and I_w is taken to be trivial. We have $(x, K_w/k_v) = 1$ if x is positive under the real embedding corresponding to v, and $(x, K_w/k_v) = \sigma_v$ otherwise.

Let us consider the local reciprocity symbol $(x, K_w/k_v)$ for $x \in k^\times$ fixed and v varying, choosing for each v a place w of K above v. For almost all v, it is equal to 1 – it can only be otherwise if v is ramified, or v is infinite, or $v(x) \neq 0$. Therefore the product across all v of these symbols is finite. In fact, we have the following *product rule for local reciprocity maps*:

$$\prod_{v \text{ place of } k} (x, K_w/k_v) = 1.$$

This is a central fact of global class field theory – see e.g. [41, Ch. XIV (Appendix)].

For every finite place v of k which is unramified in K, we have defined the Frobenius element $\sigma_v \in G$. Since these places form a basis of the free abelian group $\mathcal{I}_{k,S}$, we obtain a homomorphism (Artin map)

$$\begin{array}{ccc} \mathcal{I}_{k,S} & \longrightarrow & G \\ \mathfrak{a} & \longmapsto & \sigma_{\mathfrak{a}} \end{array}$$

extending $v \mapsto \sigma_v$.

Let $Y_{S_K} = \{\sum_{w \in S_K} n_w w : n_w \in \mathbb{Z}\}$ be the free abelian group on S_K, and $X_{S_K} = \{\sum_{w \in S_K} n_w w \in Y_{S_K} : \sum_{w \in S_K} n_w = 0\}$ its augmentation subgroup. These are modules for $\mathbb{Z}[G]$, the integral group ring of G. For any commutative ring R and $\mathbb{Z}[G]$-module M, we let RM denote the $R[G]$ module $R \otimes_{\mathbb{Z}} M$ obtained by scalar extension. Then $\mathbb{R}Y_{S_K}$ is the real vector space with basis S_K and associated G-action. The abstract $\mathbb{R}[G]$ structure of $\mathbb{R}Y_{S_K}$ is easily seen to be

$$\mathbb{R}Y_{S_K} \cong \bigoplus_{v \in S} \mathbb{R}[G/G_v].$$

Using these normalisations, we may define the *Dirichlet logarithmic regulator with respect to S_K*:

$$\begin{array}{rccc} \lambda_{S_K}: & U_{K,S} & \longrightarrow & \mathbb{R}X_{S_K} \\ & x & \longmapsto & -\sum_{w \in S_K} \ln |x|_w w. \end{array}$$

The product formula (2.4) shows that the image of this map is indeed contained in the $\mathbb{R}[G]$-submodule $\mathbb{R}X_{S_K}$ of $\mathbb{R}Y_{S_K}$. The Dirichlet logarithmic regulator is easily seen to be a G-equivariant map. The map induced by λ_{S_K} on $\mathbb{R}U_{K,S}$ by scalar extension (which will be denoted by the same symbol) is an $\mathbb{R}$-vector space isomorphism. This is part of the proof of Dirichlet's unit theorem, and is proved for example as the Unit Theorem in [23, Chap. V, §1]. It follows that

$$\lambda_{S_K} : \mathbb{R}U_{K,S} \longrightarrow \mathbb{R}X_{S_K}$$

is an isomorphism of $\mathbb{R}[G]$-modules.

Note that the fact that λ_{S_K} is an $\mathbb{R}[G]$-isomorphism implies the following

Proposition 2.1. *The $\mathbb{Q}[G]$-modules $\mathbb{Q}U_{K,S} = \mathbb{Q}U_{K,S,T}$ and $\mathbb{Q}X_{S_K}$ are isomorphic.*

Proof. This is explained in Tate [46, Ch. 1, §4]. □

Finally, we look at a comparison of the maps λ_{S_K} and λ_{S_k}. We define a map

$$\begin{array}{rccc} i_{K/k}: & Y_{S_k} & \longrightarrow & Y_{S_K} \\ & v & \longmapsto & N_{K/k} w, \end{array}$$

where w is a place of K chosen arbitrarily above the place v of k, and $N_{K/k} = N_G$ is the trace element of $\mathbb{Z}[G]$. With these maps, the following diagram is commutative:

$$\begin{array}{ccc} U_{K,S,T} & \xrightarrow{\lambda_{S_K}} & \mathbb{R}X_{S_K} \\ \uparrow & & \uparrow{\scriptstyle i_{K/k}} \\ U_{k,S,T} & \xrightarrow{\lambda_{S_k}} & \mathbb{R}X_{S_k}. \end{array} \tag{2.5}$$

This follows from the relation $|x|_w = |x|_v^{\#G_v}$ between our normalised absolute values (for w/v an extension of places in K/k and $x \in k$).

3 L-functions

If G is a finite abelian group, the complex group ring $\mathbb{C}[G]$ decomposes by the irreducible characters of the group into one-dimensional submodules. More precisely, if χ is an irreducible complex character of G, define an element of $\mathbb{C}[G]$ by

$$e_\chi = \frac{1}{\#G} \sum_{g \in G} \chi(g) g^{-1}.$$

Then $\mathbb{C}[G]e_\chi$ is a representation of G with character χ, that is, a one-dimensional $\mathbb{C}$-vector space on which $g \in G$ acts by multiplication by $\chi(g)$. The elements e_χ satisfy:

$$e_\chi^2 = e_\chi; \qquad e_\chi e_{\chi'} = 0 \text{ for } \chi \neq \chi'; \qquad \chi(e_\chi) = 1; \qquad \chi'(e_\chi) = 0 \text{ for } \chi \neq \chi';$$

hence they form an orthogonal system of idempotents. We have an isomorphism of $\mathbb{C}[G]$-modules

$$\mathbb{C}[G] \cong \bigoplus_{g \in G} \mathbb{C}[G]e_\chi.$$

The submodule $\mathbb{C}[G]e_\chi$ will be referred to as the χ-component of $\mathbb{C}[G]$. It is a one-dimensional $\mathbb{C}$-vector space on which $g \in G$ acts by multiplication by $\chi(g)$.

Now let K/k be an abelian extension with Galois group G, χ a complex character of G, and S and T finite sets of places of k as in §1. Assume that S contains all primes of k which ramify in K. To this data is associated an S-truncated, T-modified *Dirichlet L-function*, which is a meromorphic function on $\mathbb{C}$. The function is defined for $s \in \mathbb{C}$ with Re $s > 1$ by the convergent Euler product

$$L_{K/k,S,T}(s,\chi) = \prod_{v \in T} (1 - N_v^{1-s} \chi(\sigma_v)) \cdot \prod_{v \notin S} (1 - N_v^{-s} \chi(\sigma_v))^{-1}. \tag{2.6}$$

For empty T we will also write $L_{K/k,S}(s,\chi) := L_{K/k,S,\emptyset}(s,\chi)$. Note that the factors for the ramified primes have been removed by the condition that these primes lie in S, so that σ_v is a well-defined element of G_v for each v. The number N_v^{-s} in the formula is the complex power of a positive real number N_v defined in the usual way, that is $N_v^{-s} := \exp(-s \ln N_v)$. Expanding the Euler product gives the usual Dirichlet series expansion

$$L_{K/k,S}(s,\chi) = \sum_{\mathfrak{a} \in \mathcal{I}_{k,S}^+} \chi(\sigma_\mathfrak{a}) N_\mathfrak{a}^{-s} \quad \text{for Re } s > 1. \tag{2.7}$$

All this generalises to the case where G is not abelian; the L functions are replaced by *Artin L-functions*, which correspond to the Dirichlet L-functions when G is abelian.

It is well known that these L-functions may be meromorphically continued to all of $\mathbb{C}$ (see for example [28, Ch. VII, Cor. 8.6]). The L-function (as defined in (2.6) above) for the trivial character χ_0 is called the S-truncated, T-modified *zeta-function* of k, written $\zeta_{k,S,T}(s)$. We may factorise the zeta-function of the top field K in terms of the L-functions of all the characters χ of G as follows:

$$\zeta_{K,S,T}(s) = \prod_{\chi} L_{K/k,S,T}(s,\chi). \tag{2.8}$$

(This follows from [46, Ch. 0 §4 (1)]).

So far we have looked at the L-function associated to a character. We now introduce a way of looking at all these L-functions at the same time, by introducing the *equivariant L-function* associated to the abelian extension K/k and the sets S and T. Let χ^{-1} denote the conjugate character to χ, so that

$$\chi^{-1}(g) = \overline{\chi(g)} = \chi(g^{-1}) \quad \text{for all } g \in G,$$

where the bar denotes complex conjugation. Then the equivariant L-function is defined by

$$\Theta_{K/k,S,T}(s) = \sum_{\chi} L_{K/k,S,T}(s,\chi^{-1})e_{\chi}.$$

Thus, if we consider a character χ as a ring homomorphism $\mathbb{C}[G] \to \mathbb{C}$ in the natural way, we have $\chi(\Theta_{K/k,S,T}(s)) = L_{K/k,S,T}(s,\chi^{-1})$. It is also possible to express the function without mentioning characters, as in [46, Ch. IV, Prop. 1.6]:

$$\Theta_{K/k,S,T}(s) = \prod_{v\in T}(1-\sigma_v^{-1}N_v^{1-s})\prod_{v\notin S}(1-\sigma_v^{-1}N_v^{-s})^{-1} \quad \text{for } s > 1.$$

This has the advantage of splitting off the dependence on T as the finite product. The value of this product at $s = 0$ will be written

$$\delta_T = \prod_{v\in T}(1-\sigma_v^{-1}N_v).$$

We will be interested in the behaviour of these L-functions at $s = 0$. We write $r_S(\chi)$ for the order of $L_{K/k,S,T}(s,\chi)$ at $s = 0$; it is clear that this depends on S but not on T. We have $r_S(\chi^{-1}) = r_S(\chi)$ because the corresponding L-functions are mutually conjugate along the real line. A formula for $r_S(\chi)$ is given in terms of S and χ in [46, Ch. 1, Prop. 3.4], and in the abelian case it gives the following result.

Proposition 3.1. *If χ is the trivial character, we have $r_S(\chi) = \#S-1$. Otherwise $r_S(\chi)$ is equal to the number of $v \in S$ such that χ is trivial on G_v.*

The result is proved by using the well-known fact that $L_{K/k,S}(s,\chi)$ has order 0 at $s = 1$ for χ nontrivial and order -1 for χ trivial, and then using the functional equation for the L-functions.

We let r_S denote the number of totally split places in S, or $r_S = \#S - 1$ if all places are totally split. That is, $r_S = \min(\#\{v \in S : G_v = 0\}, \#S - 1)$. It is clear from Proposition 3.1 that all the $L_{K/k,S,T}(s,\chi)$ vanish to order at least r_S at the point $s=0$, and hence $\Theta_{K/k,S,T}(s)$ does as well. If we consider the Taylor expansion of the L-functions at the point $s=0$, the terms in $s^0, s^1, \ldots, s^{r_S-1}$ are all identically 0. We define $L^n_{K/k,S,T}(0,\chi)$ to be the n-th term in the Taylor expansion of $L_{K/k,S,T}(s,\chi)$ at $s=0$, and $\Theta^n_{K/k,S,T}(0)$ similarly for the equivariant function, so that

$$\Theta^n_{K/k,S,T}(0) = \sum_{\chi} L^n_{K/k,S,T}(0,\chi^{-1})e_\chi,$$

where χ runs through all irreducible characters of G. Since $L_{K/k,S,T}(s,\chi^{-1})$ and $L_{K/k,S,T}(s,\chi)$ are complex conjugates for s real, each term $\Theta^n_{K/k,S,T}(0)$ is actually an element of $\mathbb{R}[G]$. We may also express it as $\Theta^n_{K/k,S,T}(0) = \frac{1}{n!}\frac{\mathrm{d}^n}{\mathrm{d}s^n}\Theta_{K/k,S,T}(s)\big|_{s=0}$.

We set $e_{r_S} := \sum_{\chi : r_S(\chi)=r_S} e_\chi$ to be the idempotent corresponding to the characters where the order of vanishing of the associated L-function is exactly r_S. Then $\Theta^{r_S}_{K/k,S,T}(0)$ lies in the subspace $\mathbb{R}[G]e_{r_S}$ and so is stable under multiplication by e_{r_S}.

We may also define $\Theta_{K/k,S}(s)$ in terms of *partial zeta-functions*. Let $\sigma \in G$. Since S contains all ramifying places, we may define

$$\zeta_{K/k,S}(s,\sigma) = \sum_{\substack{\mathfrak{a}\in\mathcal{I}^+_{k,S}:\\ \sigma_{\mathfrak{a}}=\sigma}} N_{\mathfrak{a}}^{-s} \tag{2.9}$$

for Re $s > 1$, where $\mathfrak{a}$ runs through all effective divisors of k coprime to S with Artin symbol σ. Comparing this to (2.7) and using the orthogonality properties of characters, we have the relations

$$L_{K/k,S}(s,\chi) = \sum_{\sigma\in G}\chi(\sigma)\zeta_{K/k,S}(s,\sigma); \quad \zeta_{K/k,S}(s,\sigma) = \frac{1}{\#G}\sum_{\chi}\chi(\sigma)L_{K/k,S}(s,\chi^{-1}),$$

for Re $s > 1$, and hence $\zeta_{K/k,S}(s,\sigma)$ may be meromorphically continued to the whole plane. The relations also show that

$$\Theta_{K/k,S}(s) = \sum_{\sigma\in G}\zeta_{K/k,S}(s,\sigma)\sigma^{-1}. \tag{2.10}$$

Proposition 3.2. *Let $L/K/k$ be a tower of global fields with L/k and K/k abelian. Let S be a set of places of k containing all infinite places and all places ramifying in L/k. Then*

$$\zeta_{K/k,S}(s,\sigma) = \sum_{\substack{\theta\in\mathrm{Gal}(L/k):\\ \theta=\sigma \text{ on } K}} \zeta_{L/k,S}(s,\theta).$$

Proof. This is immediate from the definition (2.9). ☐

Corollary 3.3. *The composition of $\Theta_{L/k,S,T}$ with the natural projection map $\mathbb{C}[\mathrm{Gal}(L/k)] \to \mathbb{C}[\mathrm{Gal}(K/k)]$ is $\Theta_{K/k,S,T}$.*

Proof. This follows from the proposition and (2.10). ☐

4 Torsion in unit groups

We keep the notation $K/k, G, S, T$ from the previous sections, so that S is a nonempty set of places of k containing all infinite places and those ramifying in K/k, and T is a finite disjoint set of primes. The purpose of T is the following hypothesis:

Hypothesis 4.1. *The set T is such that $U_{K,S,T}$ is torsion free.*

Another way of stating the hypothesis is that we should have $w_{K,T} = 1$. The natural exact sequence of $\mathbb{Z}[G]$-modules

$$0 \longrightarrow \mu_{K,T} \longrightarrow \mu_K \longrightarrow \prod_{v \in T} \mathbb{F}_v^\times$$

shows that, if Hypothesis 4.1 is satisfied, the element $\delta_T = \prod_{v \in T}(1 - \sigma_v^{-1} N_v) \in \mathbb{Z}[G]$ defined in §3 annihilates μ_K.

We will use the following lemma to see some possible choices for T.

Lemma 4.2. *Let K be a global field with w_K roots of unity. Let v be a discrete valuation on K. Write $w_{K,v}$ for the number of roots of unity ζ in K which satisfy $v(\zeta - 1) > 0$. Then*

1. *If K is a function field, $w_{K,v} = 1$.*

2. *If K is a number field and $w_{K,v} > 1$, then $v(w_K) > 0$ and the ramification index for v in the extension $K/\mathbb{Q}$ is at least $p - 1$, where p is the residue characteristic of v.*

3. *If K is a number field and v' another discrete valuation on K of residue characteristic coprime to that of v, then there are no nontrivial roots of unity ζ in K satisfying $v(\zeta - 1) > 0$ and $v'(\zeta - 1) > 0$.*

Proof. In the function field case, for any root of unity ζ we have that $\zeta - 1$ is a constant and so it is either a root of unity or zero. This shows the first assertion.

Now assume K is a number field. The valuation v corresponds to a nonzero prime ideal $\mathfrak{p}$ in the ring of integers $\mathcal{O}_K$ of K. If ζ is a root of unity of order n in K satisfying $v(\zeta - 1) > 0$ then $\zeta - 1 \in \mathfrak{p}$ and so $\mathfrak{p} \mid (\zeta - 1)$. If n has more than one prime factor then $\zeta - 1$ is a global unit [47, Ch. 2, Prop. 2.8] and this is a contradiction to $\mathfrak{p} \mid (\zeta - 1)$. Therefore n must be a prime power q^a; since $\mathfrak{p} \mid p$ and $(\zeta - 1) \mid q$ we must have $q = p$. Hence $n = p^a$, and ζ is a primitive p^a-th root of unity. So $p \mid w_K$, and this shows $v(w_K) > 0$ as required by the second assertion. Now $(p) = (1 - \zeta)^{p^{a-1}(p-1)}$ and so the assertion about ramification holds as well.

The third assertion is clear by this argument since $v'(p) = 0$, and so it is not possible that the prime ideal of $\mathcal{O}_K$ corresponding to v' divides $(\zeta - 1)$, since the latter ideal divides p. $\square$

If K is a global function field with constant field of size 2, Hypothesis 4.1 is satisfied for any T. For all other function fields, the lemma shows that T need only be non-empty to satisfy Hypothesis 4.1. For a number field K, we may take T containing a single prime of sufficiently large residue characteristic, or two primes of coprime residue characteristic, and Hypothesis 4.1 will be satisfied.

Hypothesis 4.1 has the following happy consequence for a quotient of (S,T)-unit groups.

Lemma 4.3. *For any $K/k, S, T$ such that K/k is Galois and $U_{K,S,T}$ is torsion free, the quotient $U_{K,S,T}/U_{k,S,T}$ is also torsion free.*

Proof. Suppose $u \in U_{K,S,T}$ is such that $u^n \in U_{k,S,T}$ for some $n > 0$. This means that for all $\sigma \in \mathrm{Gal}(K/k)$, we have $(u^n)^{\sigma-1} = 1$. But this is $(u^{\sigma-1})^n$. Hence for all $\sigma \in \mathrm{Gal}(K/k)$, $u^{\sigma-1}$ is a torsion element of $U_{K,S,T}$ and so is 1. Therefore $u \in k$ as required. $\square$

This lemma will allow us to extend a basis of the free abelian group $U_{k,S,T}$ to a basis of $U_{K,S,T}$.

5 Exterior powers

In the remainder of this chapter we deal with some algebra which will be required for the later formulation of conjectures.

Let R be a commutative ring with 1, and M an R-module. Then for any integer $n \geq 0$, the n-th exterior power of M over R is defined as in [24, Ch. XIX], and denoted $\wedge_R^n M$. An element $m_1 \wedge \cdots \wedge m_n$ of this will be referred to as the wedge product of $m_1, \ldots, m_n$. If $\phi : M \to R$ is a map of R-modules, it naturally induces an R-module homomorphism

$$\begin{array}{cccc} \phi: & \wedge_R^n M & \longrightarrow & \wedge_R^{n-1} M \\ & m_1 \wedge \cdots \wedge m_n & \longmapsto & \sum_{i=1}^n (-1)^{i+1} \phi(m_i) m_1 \wedge \cdots \wedge m_{i-1} \wedge m_{i+1} \wedge \cdots m_n. \end{array}$$

Iterating this process gives an R-linear map

$$\begin{array}{ccc} \wedge_R^r \mathrm{Hom}_R(M,R) & \longrightarrow & \mathrm{Hom}_R(\wedge_R^n M, \wedge_R^{n-r} M) \\ \phi_1 \wedge \cdots \wedge \phi_r & \longmapsto & \phi_1 \circ \cdots \circ \phi_r. \end{array}$$

If $\Phi = \phi_1 \wedge \cdots \wedge \phi_r$ is in the domain, and $\mathbf{m} = m_1 \wedge \cdots \wedge m_n \in \wedge_R^n M$, we have the following formula for $\Phi(\mathbf{m})$, in which S_n denotes the symmetric group on n letters:

Lemma 5.1. *We have*

$$\Phi(\mathbf{m}) = \sum_{\substack{\sigma \in S_n \\ \sigma(r+1) < \ldots < \sigma(n)}} \mathrm{sign}(\sigma) \big(\prod_{j=1}^r \phi_j(m_{\sigma(j)}) \big) m_{\sigma(r+1)} \wedge \cdots \wedge m_{\sigma(n)},$$

Proof. Necessarily by induction on r.

$r = 1$: We want to show

$$\sum_{i=1}^{n}(-1)^{i+1}\phi(m_i)m_1 \wedge \cdots \wedge \hat{m}_i \wedge \cdots \wedge m_r = \sum_{\substack{\sigma \in S_n \\ \sigma(2)<\ldots<\sigma(n)}} \operatorname{sign}(\sigma)\phi_j(m_{\sigma(1)})m_{\sigma(2)} \wedge \cdots \wedge m_{\sigma(n)},$$

where $\hat{}$ means that this part of the wedge should be omitted.

We match the i-th term on the left with the term on the right corresponding to the permutation $\sigma_i \in S_n$ which takes 1 to i and satisfies $\sigma_i(2) < \ldots < \sigma_i(n)$. The relations

$$\sigma_1 = \mathrm{id}, \sigma_{i+1} = (i \quad i+1)\sigma_i$$

show that $\operatorname{sign}(\sigma_i) = (-1)^{i+1}$ as required.

$r > 1$: By induction we have

$$\begin{aligned}\Phi(m_1 \wedge \cdots \wedge m_n) \quad = \quad & \sum_{\substack{\tau \in S_n \\ \tau(r)<\ldots<\tau(n)}} \operatorname{sign}(\tau)\Big(\prod_{j=1}^{r-1}\phi_j(m_{\tau(j)})\Big) \cdot \\ & \sum_{i=0}^{n-r}(-1)^i\phi_n(m_{\tau(r+i)})m_{\tau(r)} \wedge \cdots \wedge \widehat{m_{\tau(r+i)}} \wedge \cdots \wedge m_{\tau(n)}.\end{aligned}$$

We wish to compare this to

$$\sum_{\substack{\sigma \in S_n \\ \sigma(r+1)<\ldots<\sigma(n)}} \operatorname{sign}(\sigma)\Big(\prod_{j=1}^{r}\phi_j(m_{\sigma(j)})\Big) \cdot m_{\sigma(r+1)} \wedge \cdots \wedge m_{\sigma(n)}.$$

We match the term corresponding to a pair (τ, i) to σ, where σ satisfies

$$\sigma(r) = \tau(r+i), \sigma(r+1) = \tau(r), \sigma(r+2) = \tau(r+1), \ldots, \sigma(r+i) = \tau(r+i-1),$$

and is otherwise equal to τ. That is,

$$\sigma = \tau(r+i \quad r+i-1 \quad \ldots \quad r+1 \quad r).$$

Therefore $\operatorname{sign}(\sigma) = (-1)^i\operatorname{sign}(\tau)$, and we see the terms match up. □

Definition 5.2. *Let $r \leq n$ be nonnegative integers. Define a set of permutations*

$$\begin{bmatrix} n \\ r \end{bmatrix} := \{\sigma \in S_n : \sigma(1) < \sigma(2) < \ldots < \sigma(r) \text{ and } \sigma(r+1) < \sigma(r+2) < \ldots < \sigma(n)\}.$$

Note that the cardinality of this set is the binomial coefficient $\binom{n}{r}$. Each element corresponds to choosing a subset of r elements from $\{1, \ldots, n\}$, and associates to it a sign, $\operatorname{sign}(\sigma)$.

Lemma 5.3. *Using the notation of the previous lemma, and Definition 5.2, we have*

$$\Phi(\mathbf{m}) = \sum_{\sigma \in \left[{n \atop r}\right]} \operatorname{sign}(\sigma) \det(\phi_j(m_{\sigma(i)}))_{i,j} m_{\sigma(r+1)} \wedge \cdots \wedge m_{\sigma(n)}$$

Proof. Fix such a σ as appears in the sum in the statement of the lemma. Consider the coefficient of $m_{\sigma(r+1)} \wedge \cdots \wedge m_{\sigma(n)}$ in $\Phi(\mathbf{m})$ as expanded in the previous lemma. It is:

$$\sum_{\substack{\tau \in S_n: \\ \tau(j)=\sigma(j) \\ \text{for } j=r+1,\ldots,n}} \operatorname{sign}(\tau) \prod_{j=1}^{r} \phi_j(m_{\tau(j)})$$

which is

$$\operatorname{sign}(\sigma) \sum_{\theta \in S_r} \operatorname{sign}(\theta) \prod_{j=1}^{r} \phi_j(m_{\sigma\theta(j)}),$$

as required. □

These results show that if $r = n$, we have

$$\Phi(\mathbf{m}) = \det(\phi_j(m_i))_{i,j}.$$

6 Constructions in group rings

For any group G, we let $\operatorname{aug} : \mathbb{Z}[G] \to \mathbb{Z}$ denote the *augmentation homomorphism*, that is, the ring homomorphism which maps every $g \in G$ to $1 \in \mathbb{Z}$. The kernel of this map is called the *augmentation ideal* and denoted I_G. It is the two-sided ideal generated as an abelian group by elements of the form $g - 1$ for $g \in G$. The powers of this ideal form a decreasing chain of ideals in the group ring.

The quotient $\mathbb{Z}[G]/I_G$ is obviously isomorphic to $\mathbb{Z}$. The next quotient I_G/I_G^2 is isomorphic to the abelianisation of G, and hence to G itself if G is abelian. For a finite group, it is the case that $\#G$ annihilates each of the quotients I_G^n/I_G^{n+1} for $n > 0$, and these quotients are also finite (this follows from the surjectivity of the canonical map from the n-th symmetric power of G to I_G^n/I_G^{n+1} studied in [32]). An investigation into the structure of the filtration for several small finite abelian groups is given in Chapter 9 below.

Certain manipulations will be commonly made in these augmentation quotients. We summarise these in the following lemmas.

Lemma 6.1. *Suppose $x \in \mathbb{Z}[G]$ and $y \in I_G^n$. Then $xy \equiv \operatorname{aug}(x)y \pmod{I_G^{n+1}}$.*

Proof. This is because $x - \operatorname{aug}(x)$ has augmentation 0. □

Lemma 6.2. *The map*

$$\begin{array}{ccc} G & \longrightarrow & I_G/I_G^2 \\ g & \longmapsto & g-1 \end{array}$$

is an isomorphism. Hence, if $g \in G$ and $t \in \mathbb{Z}$, we have $g^t - 1 \equiv t(g-1) \pmod{I_G^2}$.

Proof. This is well-known. A proof may be found for example in [9, p. 190]. □

Moreover, this shows:

Corollary 6.3. *If $g \in G$, $t \in \mathbb{Z}$ and $y \in I_G^n$, then $(g^t - 1)y \equiv t(g-1)y \pmod{I_G^{n+1}}$.*

Corollary 6.4. *Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ be $2n$ elements of G, and r a positive integer. Suppose $a_i^r = b_i^r$ for all i. Then $r(a_1 - 1) \cdots (a_n - 1) \equiv r(b_1 - 1) \cdots (b_n - 1) \pmod{I_G^{n+1}}$.*

Proof. We simply apply Lemmas 6.1 and 6.2 to each factor in turn, replacing $r(a_1 - 1)$ by $r(b_1 - 1)$. □

We now turn to a discussion of group ring-linear duals. If G is a finite abelian group and M is a $\mathbb{Z}[G]$-module, the $\mathbb{Z}[G]$-dual of M is the $\mathbb{Z}[G]$-module $\mathrm{Hom}_{\mathbb{Z}[G]}(M, \mathbb{Z}[G])$, where the G-action is induced by that on M.

Lemma 6.5. *There is a canonical isomorphism of abelian groups*

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z}) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[G]}(M, \mathbb{Z}[G]) \\ \phi^1 & \longmapsto & (m \mapsto \sum_{g \in G} \phi^1(g^{-1}m)g). \end{array}$$

Proof. This is easily seen to be a homomorphism. An inverse is given by the composition with the map $\mathbb{Z}[G] \to \mathbb{Z}$ given by taking the coefficient of $1 \in G$. □

We define a $\mathbb{Z}[G]$-action on $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$ by $(g\phi^1)(m) = \phi^1(gm)$, and then the map of Lemma 6.5 is an isomorphism of $\mathbb{Z}[G]$-modules – indeed, we have defined a natural equivalence of $\mathbb{Z}[G]$-module-valued functors from $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z})$ to $\mathrm{Hom}_{\mathbb{Z}[G]}(-, \mathbb{Z}[G])$.

Corollary 6.6. *The $\mathbb{Z}[G]$-linear dual functor $\mathrm{Hom}_{\mathbb{Z}[G]}(-, \mathbb{Z}[G])$ is exact on short exact sequences of $\mathbb{Z}$-torsion free $\mathbb{Z}[G]$-modules.*

Proof. Such a sequence consists of free $\mathbb{Z}$-modules. □

We write $N_G = \sum_{g \in G} g \in \mathbb{Z}[G]$ for the *norm* (or *trace*) element of $\mathbb{Z}[G]$. It is clear that if $m \in M$ is fixed by every element of G then $\phi(m) = \phi^1(m)N_G$ for maps ϕ and ϕ^1 corresponding to each other as in Lemma 6.5.

If we now look at an element $\Phi \in \wedge^r_{\mathbb{Z}[G]}\mathrm{Hom}_{\mathbb{Z}[G]}(M, \mathbb{Z}[G])$, this corresponds by this isomorphism to a unique element of $\wedge^r_{\mathbb{Z}[G]}\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$. Then the natural inclusion $M^G \to M$ gives us an element $\tilde{\Phi} \in \wedge^r_{\mathbb{Z}}\mathrm{Hom}_{\mathbb{Z}}(M^G, \mathbb{Z})$. Hence we obtain a homomorphism

$$\tilde{} : \wedge^r_{\mathbb{Z}[G]}\mathrm{Hom}_{\mathbb{Z}[G]}(M, \mathbb{Z}[G])) \longrightarrow \wedge^r_{\mathbb{Z}}\mathrm{Hom}_{\mathbb{Z}}(M^G, \mathbb{Z}).$$

Chapter 3

Special values of L-functions

Throughout this chapter, we continue with the notation $K/k, G, S, T$ developed in Chapter 2, so K/k is an abelian extension of global fields with Galois group G, S is a finite nonempty set of places of k containing all archimedean ones and all those that ramify in K/k, and T is a finite set of places of k disjoint from S. Recall that r_S is defined to be the number of places in S which split completely in K/k, or $\#S-1$, whichever is smaller. We define nonnegative integers n and d by the equations $\#S = n+1 = r_S + d + 1$.

1 Stark units

We first consider exterior powers of the module X_{S_K} defined in Chapter 2, §2. There are r_S places in S which are totally split in K, and we choose places $w_1, \dots, w_{r_S}$ in S_K above each of these. We define an element $e_{r_S} \in \mathbb{R}[G]$ as in Chapter 2, §3. Then the following is proved by Rubin in [39, Lem. 2.6ii].

Lemma 1.1. *Let w be a place of S_K which is not conjugate to any w_i, and define $\mathbf{x} = (w_1 - w) \wedge \cdots \wedge (w_{r_S} - w) \in \wedge^{r_S}_{\mathbb{Z}[G]} X_{S_K}$. Then*

$$e_{r_S} \wedge^{r_S}_{\mathbb{Z}[G]} X_{S_K} = e_{r_S}\mathbb{Z}[G]\mathbf{x}.$$

Proof. We need to show that $e_{r_S}\mathbf{x}$ generates $e_{r_S} \wedge^{r_S}_{\mathbb{Z}[G]} X_{S_K}$ as a $\mathbb{Z}[G]$-module. Any element of X_{S_K} can be written as

$$\sum_{i=1}^{r_S} \alpha_i (w_i - w) + \beta \tag{3.1}$$

with $\alpha_i \in \mathbb{Z}[G]$ and $\beta = \sum_{w'} \beta_{w'} w'$, where the w' are not conjugate to any w_i, and $\beta_{w'}$ lies in $\mathbb{Z}[G]$. Let χ be a character of G; we will show that $e_\chi e_{r_S} \beta = 0$. If χ is nontrivial on the decomposition group $G_{w'}$ for such a w', then $e_\chi w' = 0$ (since the sum of values of a nontrivial character of $G_{w'}$ is zero). Otherwise, if χ is not the trivial character, Lemma 2.3.1 shows that $e_\chi e_{r_S} = 0$. If χ is the trivial character χ_0, the element $e_\chi e_{r_S}$ is 0 if $\#S > r_S + 1$ (by Lemma 2.3.1) and it is e_{χ_0} otherwise. Hence we have

$$e_\chi e_{r_S} w' = \begin{cases} e_{\chi_0} w' & \text{if } \chi = \chi_0 \text{ and } \#S = r_S + 1; \\ 0 & \text{otherwise.} \end{cases}$$

For a nontrivial character χ we have $e_\chi e_r \beta = 0$, and this is also true for the trivial character if $\#S > r_S + 1$. If χ is the trivial character and $\#S = r_S + 1$ then β can be written as $\beta_w w$, and must satisfy $e_{\chi_0}\beta_w = 0$ since e_{χ_0} annihilates every element of X_{S_K}. Therefore in all cases $e_\chi e_{r_S}\beta = 0$. Now an arbitrary element of $\wedge^{r_S}_{\mathbb{Z}[G]} X_{S_K}$ is a wedge product of elements of the form (3.1), and this gives the result. $\square$

Let T be a finite set of primes of k disjoint from S. We know that

$$\wedge^{r_S}\lambda_{S_K} : \wedge^{r_S}_{\mathbb{R}[G]} \mathbb{R}U_{K,S,T} \longrightarrow \wedge^{r_S}_{\mathbb{R}[G]} \mathbb{R}X_{S_K}$$

is an isomorphism, and so this restricts to an isomorphism

$$\wedge^{r_S}\lambda_{S_K} : e_{r_S} \wedge^{r_S}_{\mathbb{R}[G]} \mathbb{R}U_{K,S,T} \longrightarrow e_{r_S} \wedge^{r_S}_{\mathbb{R}[G]} \mathbb{R}X_{S_K} = e_{r_S}\mathbb{R}[G]\mathbf{x}.$$

Definition 1.2. *The preimage under this map of the special value $\Theta^{r_S}_{K/k,S,T}(0)\mathbf{x}$ will be called the* Stark unit *corresponding to the data $K/k, S, T, \mathbf{x}$, and denoted η (adorned with as many subscripts taken from the data as is necessary for clarity in each context). That is, η is the unique*

$$\eta \in e_{r_S} \wedge^{r_S}_{\mathbb{R}[G]} \mathbb{R}U_{K,S,T}$$

satisfying

$$(\wedge^{r_S}\lambda_{S_K})(\eta) = \Theta^{r_S}_{K/k,S,T}(0)\mathbf{x}.$$

Let us examine the dependence of η on $\mathbf{x} = (w_1 - w) \wedge \cdots \wedge (w_{r_S} - w)$. Note that $e_{r_S}(w^\sigma - w) = 0$ for w not conjugate to any of $w_1, \ldots, w_{r_S}$ and $\sigma \in G$, which follows from the preceding proof for the component idempotents of e_{r_S} corresponding to nontrivial characters, and is obvious for the trivial character. This shows that replacing a w_i by a Galois conjugate changes $e_{r_S}\mathbf{x}$ to a Galois conjugate of itself, and also that changing w to w^σ in $\mathbf{x}$ leaves $e_{r_S}\mathbf{x}$ unchanged. Changing w to a place which is not conjugate to w also has no effect on $e_{r_S}\mathbf{x}$, since in this case $\#S > r_S + 1$ and the preceding proof shows that $e_{r_S} w = 0$ for any allowable w. If $r_S > 1$ we may reorder the w_i and this can induce a change of sign in $e_{r_S}\mathbf{x}$. In the special case where all places in S split in K, we may also exchange w with a w_i. It is easily checked that this has the effect of negating $\mathbf{x}$.

To summarise, choosing a different $\mathbf{x}$ will change $e_{r_S}\mathbf{x}$ by a Galois element, and possibly induce a sign change if $r_S > 1$. This dependency of η on $\mathbf{x}$ is straightforward, and so we will choose $\mathbf{x}$ freely in the sequel.

In the case $r_S = 0$ we have $\mathbf{x} = 1$ and $\eta = \Theta_{K/k,S,T}(0)$ equal to the special value itself. In the case $r_S = 1$, the Stark unit η lies in $e_{r_S}\mathbb{R}U_{K,S,T}$ and so may be written in the form $x \otimes u$ where $x \in \mathbb{R}$ and $u \in U_{K,S,T}$. In fact, according to the Rubin-Stark conjecture below, it should be possible to take $x = 1$ (for almost all T), and so the Stark unit is really an element of $U_{K,S,T}$. In general, η will be a sum of wedge products of (S,T)-units with real coefficients, which it should be possible to make rational numbers with "small" denominator. The Stark unit η and its integrality and arithmetic properties will be the object of study of the conjectures which follow.

2 The analytic class number formula

We use all the notation of §1. If $K = k$ we have the classical analytic class number formula, which we now recall and translate into the language of η. We order the places of S as $v_1, \dots, v_{n+1}$, and also choose a basis $u_1, \dots, u_n$ for $U_{k,S,T}$ modulo torsion (we do not need to assume Hypothesis 2.4.1 to state the theorem). Then setting $\mathbf{x} = (v_1 - v_{n+1}) \wedge \cdots \wedge (v_n - v_{n+1})$, there is a unique nonzero $R \in \mathbb{R}$ such that

$$(\wedge^n \lambda_S)(u_1 \wedge \cdots \wedge u_n) = R \cdot \mathbf{x}.$$

Explicitly, we have

$$R = \det(-\ln |u_i|_{v_j})_{i,j=1}^n. \tag{3.2}$$

The (S,T)-*regulator* $R_{k,S,T}$ is defined to be the absolute value of R. Note that the sign of R depends upon the ordering of the elements of S and the choice of basis u_i, while $R_{k,S,T}$ is independent of these.

The analytic class number formula reads as follows (see [35, (1.2)]):

Theorem 2.1. *The zeta function $\zeta_{k,S,T} = L_{k/k,S,T}(s,\chi_0)$ has exact order of vanishing $\#S - 1$ at $s = 0$, and its leading coefficient there is*

$$\zeta_{k,S,T}^n(0) = (-1)^{\#T+1} \frac{h_{k,S,T}}{w_{k,T}} R_{k,S,T}. \tag{3.3}$$

□

Note that the factor $(-1)^{\#T}$ is missing from the statement of this theorem in [18, (1.6)]. We define a sign

$$\xi = (-1)^{\#T+1} \operatorname{sign}(R), \tag{3.4}$$

which depends upon the set T, the ordering of the set S and the choice of basis of $U_{k,S,T}$. Thus the right-hand side of (3.3) is $\xi(h_{k,S,T}/w_{k,T})R$.

We may restate Theorem 2.1 in the language of §1. Let K be an abelian extension of k in which every place in S splits, for example $K = k$. Let $G = \mathrm{Gal}(K/k)$. We have in this situation that

$$\Theta_{K/k,S,T}^n(0) = \zeta_{k,S,T}^n(0) e_{\chi_0}.$$

Hence the following proposition follows directly from the definitions.

Proposition 2.2. *[39, Prop. 3.1] Let K/k be an abelian extension with group G such that every place in S splits completely in K. Theorem 2.1 is equivalent to the statement that*

$$\eta^{\xi} = \frac{1}{\#G^n} \frac{h_{k,S,T}}{w_{k,T}} u_1 \wedge \cdots \wedge u_n.$$

□

Note that the rational coefficient of the Stark unit here may have a fairly large denominator.

3 Gross's conjecture

In [18] (1988), Gross formulated a conjecture bearing a certain resemblance to the analytic class number formula, which we now describe.

As before, we let K/k be an abelian extension of global fields with group G, and sets S and T. We assume Hypothesis 2.4.1 for the rest of this section. Then $\Theta_{K/k,S,T}(0) \in \mathbb{R}[G]$ has the following integrality property:

Theorem 3.1 (Deligne, Ribet, Weil). *We have $\Theta_{K/k,S,T}(0) \in \mathbb{Z}[G]$.*

Proof. The proof is given in [18, Prop. 3.7]. □

Gross's conjecture looks at this element relative to the augmentation filtration.

Composing the local reciprocity map for a place v of S with the natural isomorphism of Lemma 2.6.2 gives a map

$$\begin{array}{rccc} f_v : & k_v^{\times} & \longrightarrow & I_G/I_G^2 \\ & x & \longmapsto & (x, K_w/k_v) - 1. \end{array}$$

Let $v_1, \ldots, v_m$ be an ordering of a subset of S of size m. We may combine the maps f_{v_j} to obtain an *algebraic regulator homomorphism*

$$\begin{array}{rccc} \mathrm{Reg}_G^{(v_1,\ldots,v_m)} : & \wedge_{\mathbb{Z}}^m k^{\times} & \longrightarrow & I_G^m/I_G^{m+1} \\ & x_1 \wedge \cdots \wedge x_m & \longmapsto & \det(f_{v_j}(x_i))_{i,j=1}^m. \end{array}$$

Note that if any of the places v_j is totally split in the extension K/k, then G_{v_j} is trivial and hence f_{v_j} is the zero map and so is $\mathrm{Reg}_G^{(v_1,\ldots,v_m)}$.

Let us fix an ordering $v_1, \ldots, v_{\#S}$ of S. Since we are assuming Hypothesis 2.4.1, the group $U_{k,S,T}$ is a free $\mathbb{Z}$-module of rank n, and we fix a basis $u_1, \ldots, u_n$ of this module. This determines the regulator $R_{k,S,T} \in \mathbb{R}$ as defined in §2. We set $\mathrm{Reg}_G := \mathrm{Reg}_G^{(v_1,\ldots,v_{\#S-1})}$ and $\mathbf{u} := u_1 \wedge \cdots \wedge u_n$, so that $\mathrm{Reg}_G(\mathbf{u})$ is the algebraic regulator corresponding to $R_{k,S,T}$. Then [18, Conj. 4.1] states the following:

Conjecture 3.2 (Gross). *We have*

$$\Theta_{K/k,S,T}(0) \equiv \xi h_{K,S,T} \mathrm{Reg}_G(\mathbf{u}) \pmod{I_G^{\#S}}.$$

For comparison with Gross's notation in [18], we note that choosing the function "f" of loc. cit. to be the composition of the Artin reciprocity map with inversion (so that Gross's "$g(\mathfrak{p})$" is our $\sigma_{\mathfrak{p}}^{-1}$), the element "$\theta_G$" of loc. cit. is the same as our $\Theta_{K/k,S,T}(0)$. The element "$\det_G \lambda$" appearing in [18, Conj. 4.1] is congruent to $(-1)^{\#S-1}\mathrm{Reg}_G(\mathbf{u}) \pmod{I_G^{\#S}}$, due to the choice of f and using Lemma 2.6.2. On the other hand, the differing signs in [18, (1.1)] and the definition of λ_{S_K} above give that the integer "m" appearing in [18, Conj. 4.1] is equal to $(-1)^{\#S-1}\xi h_{k,S,T}$. That Conjecture 3.2 is equivalent to [18, Conj. 4.1] is now clear.

The conjecture is not altered by changing the choice or ordering of places or units. This will be proved below for a generalisation of the conjecture.

Note that Conjecture 3.2 says $0 \equiv 0$ in the case $r_S > 0$. So another way to express this conjecture is that, if $r_S = 0$, then we should have

$$\eta \equiv \xi h_{k,S,T}\mathrm{Reg}_G(\mathbf{u}) \pmod{I_G^{\#S}}.$$

4 The Rubin-Stark conjecture

We use all the notation of §1 and assume Hypothesis 2.4.1. Considering the element $\eta \in e_{r_S}\mathbb{R} \wedge_{\mathbb{Z}[G]}^{r_S} U_{K,S,T}$, Rubin first asserts a rationality conjecture [39, Conj. A′] which is equivalent to "principal Stark conjecture" [46, Conj. I.5.1] for the extension K/k and those characters χ satisfying $r(\chi) = r_S$ [39, Prop. 2.3]:

Conjecture 4.1. $\eta \in \mathbb{Q} \wedge_{\mathbb{Z}[G]}^{r_S} U_{K,S,T}$.

Stark formulated a finer conjecture in the case of abelian extensions, the "refined abelian Stark conjecture" [46, Ch. IV, §2]. In the notation developed so far, it reads as follows:

Conjecture 4.2. *If $r_S = 1$ then, for all acceptable T, we have $\eta \in U_{K,S,T}$.*

We refer to [39, Prop. 2.5] for the comparison with the formulation in [46]. In fact, it is sufficient to check this conjecture for almost all acceptable singleton sets T (by [46, Prop. IV.1.2]).

The Rubin-Stark conjecture generalises Conjecture 4.2 to allow other values of r_S. The most obvious generalisation, to expect that for all r_S we have $\eta \in \wedge_{\mathbb{Z}[G]}^{r_S} U_{K,S,T}$, does not hold. Rubin gives counterexamples in [39, §4]. Instead, the integrality property is expressed using a dual construction. By $\mathbb{R}$-linear extension, an element $\Phi \in \wedge^{r_S}\mathrm{Hom}_{\mathbb{Z}[G]}(U_{K,S,T}, \mathbb{Z}[G])$ induces an $\mathbb{R}[G]$-homomorphism $\mathbb{R}\wedge_{\mathbb{Z}[G]}^{r_S} U_{K,S,T} \to \mathbb{R}[G]$. The Rubin-Stark conjecture [39, Conj. B'] is the following statement about the image of η under such maps:

Conjecture 4.3 (Rubin). *If $\Phi \in \wedge_{\mathbb{Z}[G]}^{r_S}\mathrm{Hom}_{\mathbb{Z}[G]}(U_{K,S,T}, \mathbb{Z}[G])$, then we have*

$$\Phi(\eta) \in \mathbb{Z}[G].$$

This conjecture specialises to Conjecture 4.2 in the case $r_S = 1$ since $\{x \in \mathbb{R}U_{K,S,T} : \phi(x) \in \mathbb{Z}[G] \text{ for all } \phi \in \mathrm{Hom}_{\mathbb{Z}[G]}(U_{K,S,T}, \mathbb{Z}[G])\} = U_{K,S,T}$, as is easy to see by, for example, picking a basis of the unit group.

An alternative generalisation of Conjecture 4.2 was proposed by Popescu in [34]. His version is weaker than Rubin's in the case where the torsion μ_K is not G-cohomologically trivial, but has the advantage of a particular base-change property. However, because of its use of group rings, Conjecture 4.3 will be the object of study here.

Note that in the case $r_S = 0$, Conjecture 4.3 says that $\eta \in \mathbb{Z}[G]$, which is Theorem 3.1 above. So Rubin's conjecture is known in this case. On the other hand, for higher r_S, Rubin's conjecture is open while Gross's conjecture (Conjecture 3.2) becomes trivial. These conjectures however allow a common refinement which brings congruences in the style of Gross's conjecture to the more general context of Rubin's. This refinement, formulated by Burns, is described in the next section and will be the main object of study of this thesis.

5 Burns's conjecture

We use the notation of the preceding sections, and assume Hypothesis 2.4.1. According to Conjecture 4.3, the Stark unit η satisfies $\Phi(\eta) \in \mathbb{Z}[G]$ for all $\Phi \in \wedge^{r_S}_{\mathbb{Z}[G]} \mathrm{Hom}_{\mathbb{Z}[G]}(U_{K,S,T}, \mathbb{Z}[G])$. The conjecture which will be described, formulated by Burns, proposes that this should hold, and furthermore $\Phi(\eta)$ should satisfy a congruence with respect to the augmentation filtration of $\mathbb{Z}[G]$ in the style of Conjecture 3.2.

Order the elements of S as $v_1, \dots, v_{n+1}$ such that $v_1, \dots, v_{r_S}$ are totally split in K. We define the map $\mathrm{Reg}_G := \mathrm{Reg}_G^{(v_{r_S+1}, \dots, v_n)}$ in the notation of §3. An element $\Phi \in \wedge^{r_S}_{\mathbb{Z}[G]} \mathrm{Hom}_{\mathbb{Z}[G]}(U_{K,S,T}, \mathbb{Z}[G])$ gives us $\tilde{\Phi} \in \wedge^{r_S}_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(U_{k,S,T}, \mathbb{Z})$ as in Chapter 2, §6. Combining these gives us a map

$$\mathrm{Reg}_G \circ \tilde{\Phi} : \wedge^n_{\mathbb{Z}} U_{k,S,T} \longrightarrow \mathbb{Z}[G]/I_G^{d+1}.$$

The map may be written down explicitly as follows, using the results of Chapter 2, §5. We have

$$\begin{aligned}
&(\mathrm{Reg}_G \circ \tilde{\Phi})(u_1 \wedge \cdots \wedge u_n) \\
&\quad = \sum_{\sigma \in \left[n \atop r_S \right]} \mathrm{sign}(\sigma) \det(\phi^1_j(u_{\sigma(i)})) \mathrm{Reg}_G(u_{\sigma(r_S+1)} \wedge \cdots \wedge u_{\sigma(n)}) \\
&\quad = \begin{vmatrix} \phi^1_1(u_1) & \cdots & \phi^1_{r_S}(u_1) & f_{v_{r_S+1}}(u_1) & \cdots & f_{v_n}(u_1) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \phi^1_1(u_n) & \cdots & \phi^1_{r_S}(u_n) & f_{v_{r_S+1}}(u_n) & \cdots & f_{v_n}(u_n) \end{vmatrix}.
\end{aligned}$$

Conjecture 5.1 (Burns). *Let S be ordered $v_1, \ldots, v_{\#S}$ so that $v_1, \ldots, v_{r_S}$ are totally split in K, and choose an integral basis $u_1, \ldots, u_n$ of $U_{k,S,T}$. Conjecture 4.3 holds, and furthermore we have*

$$\Phi(\eta) \equiv \xi h_{k,S,T} \cdot (\mathrm{Reg}_G \circ \tilde{\Phi})(u_1 \wedge \cdots \wedge u_n) \pmod{I_G^{d+1}}$$

for all $\Phi \in \wedge^{r_S}_{\mathbb{Z}[G]} \mathrm{Hom}_{\mathbb{Z}[G]}(U_{K,S,T}, \mathbb{Z}[G])$, where $\xi = \pm 1$ is the sign defined in (3.4) with respect to the choices and orderings of v_j and u_i.

Note that by the form of the regulator term, this suggests that in Conjecture 4.3, the element $\Phi(\eta) \in \mathbb{Z}[G]$ actually lies in the submodule I_G^d.

It is not necessarily the case that every $\Phi \in \wedge^{r_S}_{\mathbb{Z}[G]} \mathrm{Hom}_{\mathbb{Z}[G]}(U_{K,S,T}, \mathbb{Z}[G])$ can be written as a primitive tensor $\phi_1 \wedge \cdots \wedge \phi_{r_S}$. However, by the linear form of the conjecture it is sufficient to consider only these. For $r_S = 0$ it is sufficient to consider the generator $\Phi = 1 \in \mathbb{Z}[G]$.

We will show below (Chapter 4, §1) that Conjecture 5.1 is independent of the choices made in its statement.

Proposition 5.2. *Conjecture 5.1 is a common refinement of Conjectures 4.3 and 3.2.*

Proof. It is obvious from the formulation that Conjecture 5.1 implies Conjecture 4.3.

If $r_S > 0$, taking $\Phi = 1$, Conjecture 3.2 states that $0 \equiv 0$ and so is a consequence of Conjecture 5.1. Otherwise, the statements of the conjectures are the same. □

Proposition 5.3. *If all places in S split in K, then Conjecture 5.1 is true.*

Proof. We have $r_S = n$, and use Proposition 2.2 to see that

$$\eta^{\xi} = \frac{1}{\#G^n} h_{k,S,T} \cdot u_1 \wedge \cdots \wedge u_n.$$

We apply $\Phi = \phi_1 \wedge \cdots \wedge \phi_n \in \wedge^n_{\mathbb{Z}[G]} \mathrm{Hom}_{\mathbb{Z}[G]}(U_{K,S,T}, \mathbb{Z}[G])$ to this equation. Note that, since $u_i \in k$, we have $\phi_j(u_i) = \phi_j^1(u_i) N_G$, where $N_G = \sum_{g \in G} g \in \mathbb{Z}[G]$. We obtain

$$\Phi(\eta) = \xi \frac{1}{\#G^n} h_{k,S,T} N_G^n \det(\phi_j^1(u_i)) = \xi \frac{1}{\#G} h_{k,S,T} N_G \det(\phi_j^1(u_i)).$$

Since S contains all ramifying places, the extension K/k is unramified and K is a subfield of the Hilbert class field H_k of k. The Frobenius elements for the v_i in the extension H_k/k restrict to 1 in K/k, and this shows that $\#G \mid h_{k,S} \mid h_{k,S,T}$, as noted by Rubin in [39, Prop. 3.1, proof]. Therefore reducing the equality modulo I_G gives Conjecture 5.1. □

Corollary 5.4. *If $K = k$, then Conjecture 5.1 is true.* □

We note that the proof of Proposition 5.3 shows that the statement is simply the statement of the analytic class number formula (Proposition 2.2) hit by all possible Φ and reduced modulo I_G.

Chapter 4

Properties of the conjectures

1 Well-statedness

We first show that the statement of Conjecture 3.5.1 does not depend on the various choices of bases and places. Firstly, it is clear that any change to the basis of $U_{k,S,T}$ will equally affect the signs ξ and $u_1 \wedge \cdots \wedge u_n$, so that this does not change the statement of Conjecture 3.5.1.

Let us now consider a reordering of the places $v_1, \ldots, v_{\#S}$, so that the new ordering is given by a $\sigma \in S_{\#S}$. It is either the case that all the places are split in K/k, or exactly r_S of them are. If all places are split, the conjecture is true (Proposition 5.3). Otherwise, it is necessary that σ restricts to a permutation σ_1 on $\{1, \ldots, r_S\}$. Call the restriction of σ to the complement of this set σ_2. Then in the congruence of Conjecture 3.5.1, reordering the places by σ induces sign changes by $\mathrm{sign}(\sigma_1)$ in $\Phi(\eta)$, $\mathrm{sign}(\sigma)$ in $R_{k,S,T}$ and $\mathrm{sign}(\sigma_2)$ in Reg_G. Since $\mathrm{sign}(\sigma_1) = \mathrm{sign}(\sigma)\mathrm{sign}(\sigma_2)$, this does not alter the statement. Therefore Conjecture 3.5.1 is well stated.

We now study the dependence of Conjecture 3.5.1 on the data $K/k, S, T, \mathbf{x}$ used in Chapter 3. Note that the dependence of η on $\mathbf{x}$ was dealt with after Definition 1.2. Aside from the possibility of changing the sign of η by reordering the places appearing in $\mathbf{x}$ (the effect of which on Conjecture 3.5.1 has already been considered), changes to $\mathbf{x}$ may replace η with a Galois conjugate. The form of Conjecture 3.5.1 combined with Lemma 2.6.1 shows that this does not alter the statement of the conjecture.

2 Dependence on fields and T

We next show that we may lower the top field in Conjecture 3.5.1.

Proposition 2.1. *Let $L/K/k$ be a tower of finite extensions, with L/k and K/k abelian with groups Γ and $G = \Gamma/H$ respectively. Suppose the only primes in S totally split in K/k are those totally split in L/k. Then, if Conjecture 3.5.1 holds for L/k, it also holds for K/k.*

Proof. By the commutative diagram (2.5) for the extension L/K and Proposition 2.3.3, we see that

$$(\wedge^{rs}\lambda_{S_L})(\eta_{K/k}) = (\wedge^{rs}(i_{L/K}\circ\lambda_{S_K}))(\eta_{K/k}) = \Theta^{rs}_{L/k,S,T}(0)(\wedge^{rs}N_{L/K})\mathbf{x},$$

and hence that $\eta_{K/k} = (\wedge^{rs}N_{L/K})\eta_{L/k}$.

The inclusion $U_{K,S,T}\hookrightarrow U_{L,S,T}$ and the $\mathbb{Z}[G]$-module isomorphism

$$\begin{array}{ccc} \mathbb{Z}[\Gamma]^H & \xrightarrow{\sim} & \mathbb{Z}[G] \\ N_{L/K} & \longmapsto & 1 \end{array}$$

induce a surjective map

$$\mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U_{L,S,T},\mathbb{Z}[\Gamma]) \longrightarrow \mathrm{Hom}_{\mathbb{Z}[G]}(U_{K,S,T},\mathbb{Z}[G])$$

whereby each ϕ in the second group can be lifted to a $\hat{\phi}$ in the first in such a way that the projection of $\hat{\phi}(u)$ to $\mathbb{Z}[G]$ is $\phi(N_{L/K}u)$ for all $u\in U_{L,S,T}$. To see this, we apply the functor $\mathrm{Hom}_{\mathbb{Z}[\Gamma]}(-,\mathbb{Z}[\Gamma])$ to the short exact sequence

$$0\longrightarrow U_{K,S,T}\longrightarrow U_{L,S,T}\longrightarrow U_{L,S,T}/U_{K,S,T}\longrightarrow 0,$$

which consists of torsion-free groups by Lemma 2.4.3, and note Corollary 2.6.6, to see that the restriction map $\mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U_{L,S,T},\mathbb{Z}[\Gamma])\to\mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U_{K,S,T},\mathbb{Z}[\Gamma])$ is surjective. Elements ϕ of the domain group fit into the following commutative diagram [39, (16)]:

$$\begin{array}{ccccc} U_{L,S,T} & \xrightarrow{\phi} & \mathbb{Z}[\Gamma] & = & \mathbb{Z}[\Gamma] \\ {\scriptstyle N_{L/K}}\downarrow & & {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \text{canon.}} \\ U_{K,S,T} & \xrightarrow{\phi|_K} & \mathbb{Z}[\Gamma]^H & \xrightarrow{\sim} & \mathbb{Z}[G]. \end{array}$$

This proves the claim.

Now we take $\Phi\in\wedge^{rs}_{\mathbb{Z}[G]}\mathrm{Hom}_G(U_{K,S,T},\mathbb{Z}[G])$ and apply this lifting process componentwise to obtain $\hat{\Phi}\in\wedge^{rs}_{\mathbb{Z}[\Gamma]}\mathrm{Hom}_{\mathbb{Z}[\Gamma]}(U_{L,S,T},\mathbb{Z}[\Gamma])$. We have

$$\hat{\Phi}(\eta_{L/k})\equiv\xi h_{k,S,T}\cdot\mathrm{Reg}_\Gamma(\tilde{\hat{\Phi}}(\mathbf{u}))\pmod{I_\Gamma^{d+1}},$$

where $\mathbf{u}=u_1\wedge\cdots\wedge u_n$, u_i a $\mathbb{Z}$-basis of $U_{k,S,T}$. Passing to the quotient in this congruence, and noting that $\tilde{\hat{\Phi}}=\tilde{\Phi}$, we get

$$\Phi(\eta_{K/k})\equiv\xi h_{k,S,T}\cdot\mathrm{Reg}_G(\tilde{\Phi}(\mathbf{u}))\pmod{I_G^{d+1}},$$

as required. □

We now look at what happens if we enlarge T. Recall from Chapter 2, §4 that it is always sufficient for the condition of Hypothesis 2.4.1 to take T to consist of at most two places, or one place of sufficiently large residue characteristic. The next proposition shows that these cases imply the cases for larger T.

Proposition 2.2. *Suppose Conjecture 3.5.1 holds for $K/k, S, T$, and v is a place of k not in S or T. Set $T' = T \cup \{v\}$. Then Conjecture 3.5.1 holds for $K/k, S, T'$.*

Proof. The definition of $\Theta_{K/k,S,T}$ shows that $\eta_{T'} = \eta_T^{1-N_v\sigma_v^{-1}}$.

We will adapt Popescu's argument in [34, Prop. 5.3.1, proof]. Let $\phi'_1, \ldots, \phi'_r$ be elements of $\mathrm{Hom}_{\mathbb{Z}[G]}(U_{K,S,T'}, \mathbb{Z}[G])$ and set $\Phi' = \phi'_1 \wedge \cdots \wedge \phi'_r$. Popescu proves that there exists $\phi_0 \in \mathrm{Hom}_{\mathbb{Z}[G]}(U_{K,S,T'}, \mathbb{Z}[G])$, and (for each $i = 1, \ldots, r$) $\phi_i \in \mathrm{Hom}_{\mathbb{Z}[G]}(U_{K,S,T}, \mathbb{Z}[G])$ and $\alpha_i \in \mathbb{Z}[G]$, such that $\phi'_i = \phi_i + \alpha_i\phi_0$ for all $i = 1, \ldots, r$. Let $\delta_v = 1 - N_v\sigma_v^{-1}$; it is then clear that the map $\delta_v\phi_0 : x \mapsto \phi_0(\delta_v x)$ is in $\mathrm{Hom}_{\mathbb{Z}[G]}(U_{K,S,T}, \mathbb{Z}[G])$. Popescu shows that

$$\Phi'(\eta_{T'}) = \Psi(\eta_T), \tag{4.1}$$

where $\Psi \in \wedge^{r_S}_{\mathbb{Z}[G]}\mathrm{Hom}_{\mathbb{Z}[G]}(U_{K,S,T}, \mathbb{Z}[G])$ is given by

$$\delta_v(\phi_1 \wedge \cdots \wedge \phi_{r_S}) + \sum_{i=1}^{r_S} \alpha_i\phi_1 \wedge \cdots \wedge \phi_{i-1} \wedge \delta_v\phi_0 \wedge \phi_{i+1} \wedge \cdots \wedge \phi_{r_S}. \tag{4.2}$$

Now let $\mathbf{u} = u_1 \wedge \cdots \wedge u_n$ be the wedge of a basis of $U_{k,S,T}$ and $\mathbf{u}' = u'_1 \wedge \cdots \wedge u'_n$ similarly for $U_{k,S,T'}$. Adjusting u_1 by inversion if necessary, we have $(U_{k,S,T} : U_{k,S,T'})\mathbf{u} = \mathbf{u}'$ in $\wedge^n_{\mathbb{Z}}U_{k,S,T}$. Apply $\tilde{\Psi}$ to both sides of this equality. We note that $(\delta_v\phi_0)^1(u'_i) = \mathrm{aug}(\delta_v)\phi_0^1(u'_i)$ since $u'_i \in U_{k,S,T'}$. Note also that $\mathrm{aug}(\delta_v) = -(N_v - 1)$. By the form of (4.2), this shows that

$$(U_{k,S,T} : U_{k,S,T'})\tilde{\Psi}(\mathbf{u}) = -(N_v - 1)\widetilde{\Phi'}(\mathbf{u}') \qquad \text{in } \wedge^d_{\mathbb{Z}}U_{k,S,T}.$$

But $(U_{k,S,T} : U_{k,S,T'})$ divides $(N_v - 1)$. Since the group in which the equality holds is torsion-free, we may cancel $(U_{k,S,T} : U_{k,S,T'})$ from both sides. Furthermore, by (2.3),

$$h_{k,S,T'} = \frac{(N_v - 1)}{(U_{k,S,T} : U_{k,S,T'})} h_{k,S,T}.$$

So we have $h_{k,S,T}\tilde{\Psi}(\mathbf{u}) = -h_{k,S,T'}\widetilde{\Phi'}(\mathbf{u}')$ in $\wedge^d_{\mathbb{Z}}U_{k,S,T}$. Note that the sign corresponds to the factor $(-1)^{\#T+1}$ in (3.4). Applying Reg_G to this and using (4.1) gives the result. □

3 Changing S

We next look at changing S. We will use:

Lemma 3.1. *Let k, S, T be such that $U_{k,S,T}$ is torsion free. Suppose $u_1, \ldots, u_n$ is a $\mathbb{Z}$-basis for $U_{k,S,T}$. Let v be a place of k not in S or T. Take $u' \in U_{k,S\cup\{v\},T}$ such that $v(u')$ is minimal positive. Then $u_1, \ldots, u_n, u'$ is a basis for $U_{k,S\cup\{v\},T}$.*

Proof. Let $u \in U_{k,S\cup\{v\},T}$. Then there exists $a \in \mathbb{Z}$ such that $v(u) = av(u')$. Thus $u/u'^a \in U_{k,S,T}$, so we see $u_1, \ldots, u_n, u'$ generates $U_{k,S\cup\{v\},T}$. Linear independence follows from considering the valuations at v. □

Lemma 3.2. *Using the notation of the previous Lemma, we have*

$$h_{k,S\cup\{v\},T} \cdot v(u') = h_{k,S,T}.$$

Proof. Write $S' = S \cup \{v\}$ for short. The result follows from the analytic class number formula (Theorem 3.2.1) as follows. If $n = \#S - 1$, we have

$$\begin{aligned} \zeta_{k,S',T}(s) &\equiv (-1)^{\#T+1} h_{k,S',T} R_{k,S',T} s^{n+1} \pmod{s^{n+2}}, \\ \zeta_{k,S,T}(s) &\equiv (-1)^{\#T+1} h_{k,S,T} R_{k,S,T} s^{n} \pmod{s^{n+1}}, \end{aligned}$$

and the leading terms are related by

$$h_{k,S',T} R_{k,S',T} = \lim_{s\to 0} \frac{1 - N_v^{-s}}{s} h_{k,S,T} R_{k,S,T}.$$

Hence $h_{k,S',T} R_{k,S',T} = (\ln N_v) h_{k,S,T} R_{k,S,T}$. On the other hand, the definition of the regulator, and the fact that $v(u_i) = 0$ for $i = 1, \ldots, n$ shows that $R_{k,S',T} = \ln |u'|_v R_{k,S,T} = v(u')(\ln N_v) R_{k,S,T}$. This gives the result. ☐

Proposition 3.3. *Let v be a place of k not in S or T and which splits completely in K/k. Set $S' = S \cup \{v\}$. If Conjecture 3.5.1 holds for $K/k, S', T$, then it holds for $K/k, S, T$.*

Proof. Choose bases as in Lemma 3.1. We order the set $S' = \{v, v_1, v_2, \ldots, v_{n+1}\}$, and order the basis of $U_{k,S',T}$ as $u', u_1, \ldots, u_n$. We choose w above v to go into the definition of $\mathbf{x}'$, which corresponds to S' as $\mathbf{x}$ does to S. By [39, Prop. 5.2], we have $\eta_S = \breve{w}(\eta_{S'})$, where $\breve{w} \in \operatorname{Hom}_{\mathbb{Z}[G]}(U_{K,S',T}, \mathbb{Z}[G])$ is defined by

$$\breve{w}(u) = \sum_{g\in G} w(g^{-1}u)g.$$

Take $\Phi \in \wedge_G^{r_S} \operatorname{Hom}_{\mathbb{Z}[G]}(U_{K,S,T}, \mathbb{Z}[G])$. The inclusion map $U_{K,S,T} \to U_{K,S',T}$ is an injective map of $\mathbb{Z}$-torsion-free $\mathbb{Z}[G]$-modules with $\mathbb{Z}$-torsion-free cokernel, and therefore by Corollary 2.6.6 the map $\operatorname{Hom}_{\mathbb{Z}[G]}(U_{K,S',T}, \mathbb{Z}[G]) \to \operatorname{Hom}_{\mathbb{Z}[G]}(U_{K,S,T}, \mathbb{Z}[G])$ (restriction) is surjective. So we may lift Φ componentwise to an element $\Phi' \in \wedge_G^{r} \operatorname{Hom}_{\mathbb{Z}[G]}(U_{K,S',T}, \mathbb{Z}[G])$. Then

$$\Phi(\eta_S) = (\Phi' \circ \breve{w})(\eta_{S'}) \equiv \xi h_{k,S',T} \operatorname{Reg}_G(\tilde{\Phi}(\tilde{\breve{w}}(u' \wedge u_1 \wedge \cdots \wedge u_n))) \pmod{I_G^{d+1}},$$

and $\tilde{\breve{w}}(u' \wedge u_1 \wedge \cdots \wedge u_{n+1}) = w(u') u_1 \wedge \cdots \wedge u_n + \sum_{i=1}^{n+1} (-1)^i w(u_i) u' \wedge u_1 \wedge \cdots \wedge u_{i-1} \wedge u_{i+1} \wedge \cdots \wedge u_n$. But $u_1, \ldots, u_n$ are S-units so this collapses to $w(u') u_1 \wedge \cdots \wedge u_n$. Now because v splits completely in K/k, we have $w(u') = v(u')$. Hence

$$\Phi(\eta_S) \equiv \xi v(u') h_{k,S',T} \operatorname{Reg}_G(\tilde{\Phi}(u_1 \wedge \cdots \wedge u_n)) \pmod{I_G^{d+1}},$$

which by Lemma 3.2, and noting that ξ is unchanged, is what we want. ☐

Proposition 3.4. *Suppose Conjecture 3.5.1 holds for $K/k, S, T$. Let v be a place of k not in S or T and which does not split completely in K, and set $S' = S \cup \{v\}$. Then Conjecture 3.5.1 holds for $K/k, S', T$.*

Proof. We define $u_{n+1} = u'$, with u' as in Lemma 3.1. We note that, because S contains all places ramifying in K/k, v is unramified in K/k. Therefore the Artin symbol at v can be calculated by the formula

$$f_v(x) = (\sigma_v)^{v(x)},$$

for all x in $k^\times$. The definition of $\Theta_{K/k,S,T}$ shows that $\eta_{S'} = \eta_S^{1-\sigma_v^{-1}}$. Take $\Phi = \phi_1 \wedge \cdots \wedge \phi_{r_S} \in \wedge^{r_S}_{\mathbb{Z}[G]} \mathrm{Hom}_{\mathbb{Z}[G]}(U_{K,S',T}, \mathbb{Z}[G])$, then Conjecture 3.5.1 for S' asks for:

$$\Phi(\eta_{S'}) \equiv \xi h_{k,S',T} \mathrm{Reg}_G(\tilde{\Phi}(u_1 \wedge \cdots \wedge u_{r+d+1})) \pmod{I_G^{d+2}}.$$

We order the elements of S' as v_i', where $v_i' = v_i$ for $i = 1, \ldots, n$, $v_{n+1}' = v$ and $v_{n+2}' = v_{n+1}$. That is, we insert the new place v before the last place in S. The effect of passing from S to S' on the real number R defined in §2 is multiplication by $v(u') \ln N_v$, and hence the changes have no effect on ξ.

For the algebraic regulator, we have

$$\mathrm{Reg}_G(\tilde{\Phi}(u_1 \wedge \cdots \wedge u_{n+1})) = \sum_{\sigma \in \left[{n+1 \atop r_S}\right]} \mathrm{sign}(\sigma) \det\left(\phi_j^1(u_{\sigma(i)})\right) \det\left(f_{v_j}(u_{\sigma(r_S+i)})\right).$$

Let us consider two cases of σ. If $n+1 \in \{\sigma(1), \ldots, \sigma(r_S)\}$ then in the corresponding term, the column in the second determinant corresponding to v is all zeros, since $u_1, \ldots, u_{r+d}$ are S-units. The other possibility is that $n+1 = \sigma(n+1)$. Then this same column is all zeros apart from the bottom-right entry, which is

$$f_v(u_{n+1}) - 1 = (\sigma_v)^{v(u')} - 1 \equiv v(u')(\sigma_v - 1) \pmod{I_G^2}.$$

Hence $\mathrm{Reg}_{K/k,S'}(\tilde{\Phi}(u_1 \wedge \cdots \wedge u_{n+1})) = v(u')(\sigma_v - 1)\mathrm{Reg}_{K/k,S}(\tilde{\Phi}(u_1 \wedge \cdots \wedge u_n))$, where in the second expression we may consider Φ as being restricted to $U_{K,S,T}$. So Conjecture 3.5.1 for S' now reads, using Lemma 3.2,

$$(1 - \sigma_v^{-1})\Phi(\eta_S) \equiv \xi(\sigma_v - 1) h_{k,S,T} \mathrm{Reg}_G(\tilde{\Phi}(u_1 \wedge \cdots \wedge u_{r+d})) \pmod{I_G^{d+2}}.$$

Using Corollary 2.6.3, we may replace $(\sigma_v - 1)$ in this congruence by $(1 - \sigma_v^{-1})$. Therefore if Conjecture 3.5.1 holds for S, it holds for S'. □

On the other hand, the proof shows that we have the following, possibly weaker, implication in the other direction.

Proposition 3.5. *Suppose Conjecture 3.5.1 holds for $K/k, S \cup \{v\}, T$, where v is a place of k not in S or T. Then we have, for the data $K/k, S, T$,*

$$(1 - \sigma_v^{-1})\Phi(\eta) \equiv (1 - \sigma_v^{-1})(\xi h_{k,S,T} \mathrm{Reg}_G^{\Phi}) \pmod{I_G^{d+1}},$$

in the notation of Conjecture 3.5.1. That is, we obtain the image of the congruence in the next level of the augmentation filtration under multiplication by $(1 - \sigma_v^{-1})$.

Chapter 5

Proof in quadratic extensions

We use the notation of Chapter 3, assume that Hypothesis 2.4.1 holds, and furthermore that the abelian extension K/k is quadratic, i.e. of degree 2. Thus G is a group of order 2, generated by its nontrivial element which we call τ. The purpose of this chapter is to prove Conjecture 3.5.1 in this case. By Proposition 3.5.2, this also establishes Conjectures 3.4.3 and 3.3.2 – indeed, the calculation of η using quotients of zeta-functions is a central part of Rubin's proof of his conjecture in this case. Gross also gives a proof of Conjecture 3.3.2 for quadratic extensions in [18, §6] and, while we use ideas from this proof in Lemma 3.4 below, the proof given here is simpler and shorter than that of loc. cit., in that it avoids the technicalities and special cases which must be considered there. This is because the extra flexibility of Conjecture 3.5.1 with respect to increase of S (Propositions 4.3.3 and 4.3.5 above) make it possible to assume the strong hypothesis on a class group used in Lemma 3.4 below.

For comparison, note that §2 below corresponds to the known case "$n = 0$" of Gross's conjecture [18, (4.3)], and that in §3 below the sign of the regulator is irrelevant.

We establish the conjecture in §§1-3. Noting Proposition 3.5.3, we may assume that not all places in S split in K/k, and so there are exactly r_S places which are split and all the rest are inert or ramified. Hence $\#S_K = n + r_S + 1$. Throughout this chapter we abbreviate $N = N_{K/k}$ for the norm map, so $Nx = x^{1+\tau}$ for $x \in K$.

1 Cohomology of $U_{K,S,T}$

Let $u_1, \ldots, u_{n+r_S}$ be a basis of $U_{K,S,T}$ such that $u_1, \ldots, u_n$ is a basis of $U_{k,S,T}$, which is possible by Lemma 2.4.3. The relevant structure of this basis is closely related to the Galois cohomology of the G-module $U_{K,S,T}$. We will use Galois cohomology, and Tate's modified cohomology for finite groups, as described in [41].

Lemma 1.1. *Without assuming Hypothesis 2.4.1, we have*

$$\frac{\#\hat{H}^0(G, U_{K,S,T})}{\#H^1(G, U_{K,S,T})} = 2^d.$$

Proof. Note the left-hand side is the Herbrand quotient $h(U_{K,S,T})$ of the $\mathbb{Z}[G]$-module $U_{K,S,T}$ in the sense of [41, Ch. VIII, §4]. The composite isomorphism of $\mathbb{Q}[G]$-modules (Proposition 2.2.1)

$$\mathbb{Q}U_{K,S,T} \cong \mathbb{Q}X_{S_K} \cong \mathbb{Q}[G]^{r_S} \oplus \mathbb{Q}^d$$

implies that there is a $\mathbb{Z}[G]$-homomorphism from $U_{K,S,T}$ to $\mathbb{Z}[G]^{r_S} \oplus \mathbb{Z}^d$ with finite kernel and cokernel. Then $h(U_{K,S,T}) = h(\mathbb{Z}[G])^{r_S} h(\mathbb{Z})^d = 2^d$ as required. □

The following result appears in [39, Thm. 3.5, proof].

Lemma 1.2. *If $H^1(G, U_{K,S,T}) \neq 0$ then we can assume $N_{K/k}u_{n+1} = 1$.*

Proof. Take $u \in U_{K,S,T}$ representing a nontrivial element of $H^1(G, U_{K,S,T}) = U^-_{K,S,T}/U^{1-\tau}_{K,S,T}$, where $U^-_{K,S,T}$ is the set of (S,T)-units of norm 1. Write $u = \epsilon \prod_i u_{n+i}^{\alpha_i}$, where $\epsilon \in U_{k,S,T}$, and write ϵ_i for the norm $u_{n+i}^{1+\tau} \in U_{k,S,T}$. Then $u_{n+i}^{1-\tau} = u_{n+i}^2 \epsilon_i^{-1}$. Therefore we can assume each α_i is 0 or 1. But they cannot all be 0, since $U_{k,S,T} \cap U^-_{K,S,T} = \{1\}$. Hence u can go into a basis of $U_{K,S,T}$. □

Lemma 1.3. *If $H^1(G, U_{K,S,T}) = 0$, we can assume that $u_i = N_{K/k}u_{n+i}$ for $i = 1, \ldots, r_S$.*

Proof. Write $Nu_{n+j} = \prod_{i=1}^n u_i^{\alpha_{ji}}$ for $j = 1, \ldots, r_S$. We may perform the following operations on the $r_S \times n$ matrix (α_{ji}): elementary column operations, which correspond to swapping and multiplying the units in the basis of $U_{k,S,T}$, and elementary row operations, which correspond to swapping and multiplying the units $u_{n+1}, \ldots, u_{n+r_S}$.

Thus we can put (α_{ji}) into diagonal form with integers $a_1, \ldots, a_{r_S}$ on the diagonal. Now suppose some a_i is even, so $Nu_{n+i} = \epsilon^2$ for some ϵ in $U_{k,S,T}$. Then $u_{n+i}\epsilon^{-1}$ is a unit in $K - k$ with norm 1. But the group $U^{1-\tau}_{K,S,T} \subseteq U_{k,S,T}U^2_{K,S,T}$. So $u_{n+i}\epsilon^{-1}$ represents a nontrivial element of

$$U^-_{K,S,T}/U^{1-\tau}_{K,S,T} = H^1(G, U_{K,S,T}).$$

This is a contradiction to our assumption. We conclude that each a_i is odd. Now replacing u_{n+i} by $u_{n+i}u_i^{-[a_i/2]}$ gives us the result. □

In our situation, noting that S contains a place not splitting in K, [39, Lem. 3.4] states:

Lemma 1.4 (Rubin).
1. $h_{k,S,T} \mid h_{K,S,T}$
2. $\#H^1(G, U_{K,S,T}) \mid h_{k,S,T}$

3. *If $\hat{H}^0(G, U_{K,S,T})$ and $H^1(G, U_{K,S,T})$ are trivial then $h_{k,S,T} \equiv h_{K,S,T}/h_{k,S,T}$* (mod 2).

We write $\epsilon_- = u_{n+1} \wedge \cdots \wedge u_{n+r_S}$. In proving his conjecture for quadratic extensions [39, proof of Prop. 3.5], Rubin uses the analytic class number formula to express η in terms of this element; we make extensive use of his formulas, which are quoted below. We note that these results may also be obtained using the calculation (8.10) below.

2 The case $d = 0$

We assume $d = 0$, that is, $\#S = r_S + 1$ and $r_S = n$, and show that the congruence in Conjecture 3.5.1 holds. We require:

$$\Phi(\eta) \equiv \xi h_{k,S,T} \begin{vmatrix} \phi_1^1(u_1) & \cdots & \phi_n^1(u_1) \\ \vdots & \ddots & \vdots \\ \phi_1^1(u_n) & \cdots & \phi_n^1(u_n) \end{vmatrix} \pmod{I_G}. \tag{5.1}$$

Note that this is an equality in $\mathbb{Z}[G]/I_G \cong \mathbb{Z}$. We observe that Lemma 1.1 gives that $\#\hat{H}^0(G, U_{K,S,T}) = \#H^1(G, U_{K,S,T}) =: H$.

As in [39, proof of Prop. 3.5], we choose $\bar{u}_1, \ldots, \bar{u}_n \in U_{K,S,T}$ which are such that $N\bar{u}_1, \ldots, N\bar{u}_n$ is a basis for $NU_{K,S,T}$, and set $\boldsymbol{\varepsilon}_+ = \bar{u}_1 \wedge \cdots \wedge \bar{u}_n$. The index $[U_{k,S,T} : NU_{K,S,T}] = H$, and so, inverting $\bar{u}_1$ if necessary to get the correct sign, we have

$$(\wedge^n N)\boldsymbol{\varepsilon}_+ = H \cdot u_1 \wedge \cdots \wedge u_n \in \wedge^n_{\mathbb{Z}[G]} U_{k,S,T}. \tag{5.2}$$

Observe that, by (2.5), $\lambda_{S_K}(\boldsymbol{\varepsilon}_+)e_{\chi_0} = \lambda_S((\wedge^n N)\boldsymbol{\varepsilon}_+)$ under the natural map $\mathbb{Q}Y_S \xrightarrow{\times e_{\chi_0}} \mathbb{Q}Y_{S_K}$. Therefore, by the analytic class number formula (Chapter 2, §2), we have $e_{\chi_0}\eta = \frac{\xi}{H} h_{k,S,T} e_{\chi_0} \boldsymbol{\varepsilon}_+$. Rubin [39, proof of Prop. 3.5] calculates the part of η corresponding to the nontrivial character, and using this gives

$$\eta = \frac{\xi}{H} e_{\chi_0} h_{k,S,T} \boldsymbol{\varepsilon}_+ \pm \frac{h_{K,S,T}}{h_{k,S,T}} e_\chi \boldsymbol{\varepsilon}_-. \tag{5.3}$$

Assume first that $H = 1$. Then we may assume $u_{n+i}^{1+\tau} = u_i$ for $i = 1, \ldots, n$ by Lemma 1.3, so that $\boldsymbol{\varepsilon}_+ = \boldsymbol{\varepsilon}_-$ (inverting u_{n+1} if necessary to maintain (5.2)). Hence

$$\eta = \xi \left(h_{k,S,T} \frac{(1+\tau)}{2} \pm \frac{h_{K,S,T}}{h_{k,S,T}} \frac{(1-\tau)}{2} \right) \epsilon_-.$$

Lemma 1.4 shows the $\mathbb{Q}[G]$-factor here lies in $\mathbb{Z}[G]$, and we note its augmentation is $\xi h_{k,S,T}$. Furthermore

$$\phi(u_{n+i}) = \phi^1(u_{n+i}) - \tau\phi^1(u_{n+i}) + \tau\phi^1(u_i) \equiv \phi^1(u_i) \pmod{I_G}.$$

Hence (5.1) is satisfied in this case.

Now assume $H \neq 1$. Then by Lemma 1.2, we may assume $N_{K/k}u_{n+1} = 1$. A similar argument to the proof of Lemma 1.2, but working with $\hat{H}^0(G, U_{K,S,T})$, shows that we may also assume $\bar{u}_1 \in U_{k,S,T}$. Therefore $e_\chi \boldsymbol{\varepsilon}_+ = e_{\chi_0}\boldsymbol{\varepsilon}_- = 0$. Hence (5.3) becomes

$$\eta = \frac{\xi}{H} h_{k,S,T}\boldsymbol{\varepsilon}_+ \pm \frac{h_{K,S,T}}{h_{k,S,T}}\boldsymbol{\varepsilon}_-.$$

Note that Lemma 1.4 again gives that the $\mathbb{Q}[G]$-factors here are in $\mathbb{Z}[G]$. By the assumption on Nu_{n+1}, we have

$$\phi_j(u_{n+1}) \equiv \phi_j^1(N_{K/k}u_{n+1}) = 0 \pmod{I_G},$$

so $\Phi(\boldsymbol{\varepsilon}_-) \equiv 0 \pmod{I_G}$. Now we note that $\Phi(\boldsymbol{\varepsilon}_+) \equiv \tilde{\Phi}((\wedge^n N)\boldsymbol{\varepsilon}_+) \pmod{I_G}$, and so using (5.2) completes the proof of (5.1) in this case.

This verifies Conjecture 3.5.1 in the case $d = 0$.

3 The case $d > 0$

Now we assume $d > 0$, ie. $\#S > r_S + 1$. For $d > 0$, I_G^d/I_G^{d+1} is a group of order 2, so the congruence statement in Conjecture 3.5.1 only concerns in which power of the augmentation ideal the terms lie. We have $(1-\tau)^m = 2^{m-1}(1-\tau)$ for $m > 0$. Note that the map

$$\begin{array}{ccc} I_G^d/I_G^{d+1} & \longrightarrow & I_G^{d+1}/I_G^{d+2} \\ x & \longmapsto & (1-\tau)x \end{array}$$

is a bijection. We have the following freedom to increase S:

Lemma 3.1. *Let $[K:k] = 2$. Assume $d = \#S - r_S - 1 > 0$. Let v be a place of k not in S or T, and set $S' = S \cup \{v\}$. Then if Conjecture 3.5.1 holds for $K/k, S', T$, it also holds for $K/k, S, T$.*

Proof. The place v is either split or inert in K/k. If it is split, the result follows from Proposition 4.3.3. If v is inert, we have $\sigma_v = \tau$ and Proposition 4.3.5, combined with the stability of the augmentation quotients, shows the result. □

Rubin shows in [39, Prop. 3.5, proof] that for the case K/k quadratic and $d > 0$ we have

$$\eta = \pm 2^d \frac{h_{K,S,T}}{h_{k,S,T}} \frac{(1-\tau)}{2}\epsilon_-. \tag{5.4}$$

We note that $2^{d-1}(1-\tau) \in I_G^d$.

It turns out that we only need to consider the congruence statement under the following cohomological assumption[1].

[1] In fact it is easy to show that both sides of the congruence vanish if this assumption is not satisfied.

Lemma 3.2. *Suppose $d > 0$ and $H^1(G, U_{K,S,T}) = 0$. Then the congruence of Conjecture 3.5.1 is implied by the following statement:*

$$2^{d-1}(1-\tau)\frac{h_{K,S,T}}{h_{k,S,T}} \equiv h_{k,S,T}\mathrm{Reg}_G(u_{r_S+1} \wedge \cdots \wedge u_n) \pmod{I_G^{d+1}}. \tag{5.5}$$

Proof. We apply Lemma 1.3 to assume that $u_i = Nu_{n+i}$ for $i = 1, \ldots r_S$. Then $\phi_j(u_{n+i}) \equiv \phi_j^1(u_i) \pmod{I_G}$. Thus

$$\Phi(\eta) \equiv 2^{d-1}(1-\tau)\frac{h_{K,S,T}}{h_{k,S,T}} \begin{vmatrix} \phi_1^1(u_1) & \cdots & \phi_{r_S}^1(u_1) \\ \vdots & \ddots & \vdots \\ \phi_1^1(u_{r_S}) & \cdots & \phi_{r_S}^1(u_{r_S}) \end{vmatrix} \pmod{I_G^{d+1}}$$

For the right-hand side of the congruence in Conjecture 3.5.1, we note that if any u_i, $1 \leq i \leq r_S$, appears in the argument of Reg_G, then the corresponding term is 0 (because u_i is a norm from K, and therefore in the kernel of all the local reciprocity maps). So the right-hand side collapses to a single term:

$$\xi h_{k,S,T} \begin{vmatrix} \phi_1^1(u_1) & \cdots & \phi_{r_S}^1(u_1) \\ \vdots & \ddots & \vdots \\ \phi_1^1(u_{r_S}) & \cdots & \phi_{r_S}^1(u_{r_S}) \end{vmatrix} \mathrm{Reg}_G(u_{r_S+1} \wedge \cdots \wedge u_n).$$

This gives the result since multiplication by $\xi = \pm 1$ is the identity on I_G^d / I_G^{d+1}. □

Next we identify a condition for the non-vanishing of the regulator. We need an auxiliary lemma. For Tate's theory of the group cohomology of finite cyclic groups, we refer to [41, Ch. VIII, §4].

Lemma 3.3. *Suppose $h_{k,S} = 1$. Then there is an isomorphism*

$$\frac{U_{k,S} \cap NK^\times}{NU_{K,S}} \cong A_{K,S}^G.$$

Proof. (cf. [18, p191]) We have the exact sequence (from (2.1)):

$$0 \longrightarrow K^\times / U_{K,S} \longrightarrow \bigoplus_{\mathfrak{P} \notin S_K} \mathfrak{P}^{\mathbb{Z}} \longrightarrow A_{K,S} \longrightarrow 0.$$

Considering the decompositions of primes shows that $H^1(G, \bigoplus_{\mathfrak{P} \notin S_K} \mathfrak{P}^{\mathbb{Z}}) = 0$. Then taking cohomology gives an exact sequence

$$0 \longrightarrow H^0(G, K^\times / U_{K,S}) \longrightarrow \bigoplus_{\mathfrak{p} \notin S_k} \mathfrak{p}^{\mathbb{Z}} \xrightarrow{0} A_{K,S}^G \longrightarrow H^1(G, K^\times / U_{K,S}) \longrightarrow 0.$$

Observe that $k^\times / U_{k,S}$ injects into $H^0(G, K^\times / U_{K,S})$, and (2.1) for k shows that it surjects onto $\bigoplus_{\mathfrak{p} \notin S_k} \mathfrak{p}^{\mathbb{Z}}$, because the S-class group of k is trivial. This is why the map marked 0 is zero. Therefore we have $A_{K,S}^G \cong H^1(G, K^\times / U_{K,S})$.

On the other hand, applying Hilbert's Theorem 90 [41, Ch. X, Prop. 2] and Tate cohomology to the short exact sequence

$$0 \longrightarrow U_{K,S} \longrightarrow K^\times \longrightarrow K^\times/U_{K,S} \longrightarrow 0$$

gives an exact sequence

$$0 \longrightarrow H^1(G, K^\times/U_{K,S}) \longrightarrow \hat{H}^0(G, U_{K,S}) \longrightarrow \hat{H}^0(G, K^\times).$$

Therefore

$$H^1(G, K^\times/U_{K,S}) \cong \ker(U_{k,S}/NU_{K,S} \longrightarrow k^\times/NK^\times) = U_{k,S} \cap NK^\times/NU_{K,S}.$$

This completes the proof. □

Lemma 3.4. *Suppose $h_{K,S,T} = 1$. Then* $\mathrm{Reg}_G(u_{r_S+1} \wedge \cdots \wedge u_n) \not\equiv 0 \pmod{I_G^{d+1}}$.

Proof. By (2.3) and Lemma 1.4 (part (i)), we have that $h_{k,S} = 1$, and then [36, Cor. 2] shows that $H^1(G, U_{K,S}) = 0$. Therefore $\hat{H}^0(G, U_{K,S})$ is a 2-torsion group with 2^d elements by Lemma 1.1, and hence is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^d$.

Similarly to [18, p191], we define a homomorphism

$$f : U_{k,S} \longrightarrow G^{S-S_1} \cong (\mathbb{Z}/2\mathbb{Z})^{d+1}$$

by the local reciprocity maps f_v. Then, by the product formula,

$$\mathrm{im}\, f \subseteq V := \left\{ (g_v)_{v \in S-S_1} : \prod g_v = 1 \right\} \cong (\mathbb{Z}/2\mathbb{Z})^d.$$

Now $u \in U_{k,S}$ is in $\ker f$ if and only if u is a local norm at all the places in $S - S_1$, and we note it is automatically a norm at all other places. Since K/k is cyclic, u is a local norm everywhere if and only if it is a global norm. So $\ker f = U_{k,S} \cap NK^\times$. Since $h_{K,S,T} = 1$, we have $A_{K,S}^G = 0$ and so Lemma 3.3 shows that $\ker f = NU_{K,S}$. On the other hand, $\hat{H}^0(G, U_{K,S}) = U_{k,S}/NU_{K,S} \cong (\mathbb{Z}/2\mathbb{Z})^d$, so we have $f(U_{k,S}) = V$.

We note that the form of our regulator and the choice of our unit basis show that the non-vanishing of our regulator

$$\mathrm{Reg}_G(u_{r_S+1} \wedge \cdots \wedge u_n) \not\equiv 0 \pmod{I_G^{d+1}}$$

is equivalent to saying $f(U_{k,S,T}) = V$.

The reduction map $U_{K,S} \longrightarrow \prod_{\mathfrak{P} \in T_K} \mathbb{F}_{\mathfrak{P}}^\times$ is surjective, by (2.2) for K and the assumption that $h_{K,S,T} = 1$. Also, the norm in an extension of finite fields is surjective. Hence $\ker f = NU_{K,S}$ surjects onto $\prod_{\mathfrak{p} \in T} \mathbb{F}_{\mathfrak{p}}^\times$. The sequence (2.2) for k shows that this latter is isomorphic by the reduction map to $U_{k,S}/U_{k,S,T}$. So every element of $U_{k,S}$ can be written as the product of something in $\ker f$ by something in $U_{k,S,T}$, which gives our result. □

Now consider $A_{K,S,T}$, the S_K ray class group modulo T_K. Choose a set S'_K of primes of $\mathcal{O}_{K,S}$ coprime to T_K whose classes generate this group. Set S' to be the set of places of k lying below these. If S contains S', then $h_{K,S,T} = 1$. On the other hand:

Lemma 3.5. *If $h_{K,S,T} = 1$, then the congruence of Conjecture 3.5.1 holds.*

Proof. By Lemma 1.4 (part (i)) we have that $h_{k,S,T} = 1$, which also shows by part (ii) of the same lemma that $H^1(G, U_{K,S,T}) = 0$. So by Lemma 3.2 it is sufficient to show (5.5) holds. Lemma 3.4 shows that the right-hand side of (5.5) is not zero. On the other hand $h_{K,S,T}/h_{k,S,T} = 1$ so the left-hand side is not zero either. □

Now by Lemma 3.1, we may assume $S' \subseteq S$. Then $h_{K,S,T} = 1$, so Lemma 3.5 implies that the congruence of Conjecture 3.5.1 holds.

Therefore we have established the following theorem in all cases.

Theorem 3.6. *Suppose $[K : k] = 2$. Then Conjecture 3.5.1 holds.* □

Chapter 6

Explicit Stark units

Let k be a global field which has at most one archimedean place. This means that k is either the rational field $\mathbb{Q}$, an imaginary quadratic field, or a global function field. In the first two cases we let ∞ denote the unique archimedean place, and for k a function field we choose a place freely and call it ∞. If K/k is an abelian extension of k in which ∞ splits completely, we have explicit analytic constructions of the Stark units $\eta \in U_{K,S,T}$. It is sufficient to consider the *ray class fields totally split at* ∞, since given K and S, K is contained in such a field $H(\mathfrak{m})$, where $\mathfrak{m}$ is an ideal of the ∞-integers of k supported above the primes in S. The Stark unit for K/k is then the norm of the Stark unit for $H(\mathfrak{m})/k$, as in the proof of Proposition 4.2.1. This Proposition also shows that it is sufficient to prove Conjecture 3.5.1 for $H(\mathfrak{m})/k$ to know it for K/k. In this chapter we describe the ray class fields $H(\mathfrak{m})$ and the special elements which lie in them.

1 Systems of special units

We fix a global field k and a place ∞ of k such that all other places of k are finite. Then the ring of ∞-integers $\mathcal{O} := \mathcal{O}_{k,\infty}$ (as defined in Chapter 2, §1) is a Dedekind domain whose prime ideals correspond to the other places of k.

The *idèle group* J_k of k is the subgroup of elements $\mathbf{i} = (i_v)_v \in \prod_v k_v^\times$ (where v runs over all places of k) such that $v(i_v) = 0$ for almost all v, considered as a topological group with respect to the topology defined in [23, Ch. VII, §§1,3]. The open subgroups of J_k containing the diagonally-embedded subgroup $k^\times$ correspond to the finite abelian extensions of k via global class field theory (see e.g. [23, Ch. IX–XI]). In particular, for a nonzero ideal $\mathfrak{m}$ of $\mathcal{O}_{k,\infty}$, define $S = \mathrm{Supp}(\mathfrak{m}) \cup \{\infty\}$ and

$$\begin{aligned} U(\mathfrak{m}) = \{\mathbf{i} \in J_k \quad : \quad & v(i_v) = 0 \ \text{ if } v \notin S \\ & v(i_v - 1) \geq v(\mathfrak{m}) \ \text{ if } v \neq \infty \ \text{ and } v \mid \mathfrak{m}\}, \end{aligned}$$

the group of idèles which are local units away from $\mathrm{Supp}(\mathfrak{m})$ and ∞ and congruent to 1 modulo $\mathfrak{m}$. The group $k^\times U(\mathfrak{m})$ is then an open subgroup of J_k of finite index, and the corresponding field $H(\mathfrak{m})$ is the ray class field modulo $\mathfrak{m}$ totally split at ∞. There is a canonical identification

$$\mathrm{Gal}(H(\mathfrak{m})/k) \cong J_k/k^\times U(\mathfrak{m}) \cong A_{k,S,\mathfrak{m}}.$$

(One reference for the second isomorphism here is [23, Ch. VII, §4]). Therefore the exact sequence (2.2) with $S = \{\infty\}$ and $\mathfrak{t} = \mathfrak{m}$ becomes

$$0 \longrightarrow \mu_{k,\mathfrak{m}} \longrightarrow \mu_k \longrightarrow (\mathcal{O}/\mathfrak{m})^\times \longrightarrow \mathrm{Gal}(H(\mathfrak{m})/k) \longrightarrow A_{k,\infty} \longrightarrow 0. \tag{6.1}$$

Note that the class group $A_{k,\infty}$ of $\mathcal{O}$ is the Galois group of the subextension H/k, where H is the Hilbert class field totally split at ∞ (i.e. the maximal unramified extension of k totally split at ∞).

If $\mathfrak{a}$ and $\mathfrak{b}$ are coprime ideals of $\mathcal{O}$, the restriction map $\mathrm{Gal}(H(\mathfrak{ab})/H) \to \mathrm{Gal}(H(\mathfrak{a})/H)$ fits into the exact commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mu_{k,\mathfrak{a}}/\mu_{k,\mathfrak{ab}} \arrow[r] \arrow[d] & (\mathcal{O}/\mathfrak{b})^\times \arrow[r] \arrow[d] & \mathrm{Gal}(H(\mathfrak{ab})/H(\mathfrak{a})) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mu_k/\mu_{k,\mathfrak{ab}} \arrow[r] \arrow[d] & (\mathcal{O}/\mathfrak{ab})^\times \arrow[r] \arrow[d] & \mathrm{Gal}(H(\mathfrak{ab})/H) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mu_k/\mu_{k,\mathfrak{a}} \arrow[r] \arrow[d] & (\mathcal{O}/\mathfrak{a})^\times \arrow[r] \arrow[d] & \mathrm{Gal}(H(\mathfrak{a})/H) \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0. &
\end{tikzcd} \tag{6.2}$$

We now introduce some notation which will make it easier to talk about prime-power factors of ideals. If $\mathfrak{m}$ is an ideal of $\mathcal{O}$, it may be written in the form

$$\mathfrak{m} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_n^{e_n} \tag{6.3}$$

for primes $\mathfrak{p}_i$ of $\mathcal{O}$ and positive integers e_i. Write $B = \{1, \ldots, n\}$ for the set of indices. If $1 \le i \le n$, we write $\mathfrak{m}_i = \mathfrak{p}_i^{e_i}$, and $\mathfrak{m}_I = \prod_{i \in I} \mathfrak{m}_i$, $S_I = \{p_i : i \in I\}$ relative to a subset $I \subseteq B$. We abbreviate $w_I = w_{k,\mathfrak{m}_I}$, the number of roots of unity of k congruent to 1 modulo $\mathfrak{m}_I$.

Let us fix $\mathfrak{m}$ and also a prime $\mathfrak{t}$ of $\mathcal{O}$ which is coprime to $3\mathfrak{m}w_{H(\mathfrak{m})}$.

Proposition 1.1. *There is a system of elements $\hat{\lambda}_I$ of the maximal abelian extension of k, indexed by nonempty subsets $I \subseteq \{1, \ldots, n\}$, such that for each prime $\mathfrak{t}$ of $\mathcal{O}$ coprime to $3\mathfrak{m}w_{H(\mathfrak{m})}$, the elements $\hat{\lambda}_I^{\delta_\mathfrak{t}} =: \lambda_I$ satisfy the following properties.*

1. $\lambda_I \in U_{H(\mathfrak{m}_I),S_I,\mathfrak{t}}$.

2. *Distribution relations.*

   (a) *If* $i \notin I$, *then* $N_{H(\mathfrak{m}_{I\cup\{i\}})/H(\mathfrak{m}_I)}(\lambda_{I\cup\{i\}}^{w_I/w_{I\cup\{i\}}}) = \lambda_I^{1-\sigma_{\mathfrak{p}_i}^{-1}}$.

   (b) $N_{H(\mathfrak{m}_i)/H}(\lambda_i^{w_k/w_i}) = \alpha_i$, *where* $\alpha_i \mathcal{O}_H = \mathfrak{p}_i^{1-N_\mathfrak{t}}\mathcal{O}_H$ ($\mathcal{O}_H$ *denoting the integral closure of* $\mathcal{O}$ *in* H).

3. *L-function evaluation. There is a place* ∞' *of* $H(\mathfrak{m})$ *above* ∞ *such that we have*

$$w_I \Theta'_{H(\mathfrak{m}_I)/k,S_I,\mathfrak{t}}(0)\infty' = \lambda_{\infty'}(\lambda_I).$$

It follows from part 3 that we have

Proposition 1.2.

$$\eta_{H(\mathfrak{m})/k,S,\mathfrak{t}}^{w_I} = \lambda_I. \quad \square$$

Proposition 1.3. *To verify property 3 of Proposition 1.1, it is sufficient to check that there is a place* ∞' *of* $H(\mathfrak{m}_I)/k$ *such that*

$$w_I\big(\zeta'_{H(\mathfrak{m}_I)/k,S_I}(0,\sigma) - N_\mathfrak{t}\zeta'_{H(\mathfrak{m}_I)/k,S_I}(0,\sigma\sigma_\mathfrak{t}^{-1})\big) = -\ln|\lambda_I^\sigma|_{\infty'}$$

for all $\sigma \in \mathrm{Gal}(H(\mathfrak{m}_I)/k)$.

Proof. Expanding the left-hand side of the equality in property 3 using (2.10) shows that the desired equality is

$$w_I\Big(\sum_\sigma \big(\zeta'_{H(\mathfrak{m}_I)/k,S_I}(0,\sigma) - N_\mathfrak{t}\zeta'_{H(\mathfrak{m}_I)/k,S_I}(0,\sigma\sigma_\mathfrak{t}^{-1})\big)\sigma^{-1}\Big)\infty' = \Big(-\sum_\sigma \ln|\lambda_I^\sigma|_{\infty'}\sigma^{-1}\Big)\infty'.$$

$\square$

Remark 1.4. 1. The w-factors in the distribution relations are the sizes of the kernels arising in the top row of (6.2). This shows that the relations appear more neatly when we consider norms with respect to the groups $(\mathcal{O}/\mathfrak{b})^\times$, which surject onto the relevant Galois groups. These formulations appear in Lemma 2.1 below.

2. The w-factor in the L-function evaluation property can be accounted for as follows. The partial zeta-function is defined for $\Re(s) > 1$ by

$$\zeta_{H(\mathfrak{m})/k,S}(s,\sigma) = \sum_{I\in\mathfrak{c}} N_I^{-s},$$

where I runs through all ideals of $\mathcal{O}$ in the congruence class $\mathfrak{c}$ corresponding to the automorphism σ by global class field theory. If I, I' are two elements of $\mathfrak{c}$ then $I'/I = (x)$ for some $x \in k^\times, x \equiv 1 \pmod{\mathfrak{m}}$. Thus fixing one element I of $\mathfrak{c}$ allows us to define a similar function

$$z_\mathfrak{m}(s,\mathfrak{c}) = \sum_{\substack{x \in I^{-1}: \\ x \equiv 1 (\mathrm{mod}\ \mathfrak{m})}} N_{xI}^{-s}.$$

If μ injects into $(\mathcal{O}/\mathfrak{m})^\times$ then the x and the I are in bijection, so the functions are the same. In general there are $w_\mathfrak{m}$ of the x to each one of the I. So $z_\mathfrak{m}(s,\mathfrak{c}) = w_\mathfrak{m}\zeta_\mathfrak{m}(s,\sigma)$. The more natural infinite-series form of the function $z_\mathfrak{m}(s,\mathfrak{c})$ means it is amenable to analytic methods of evaluation (see [45, §2] or [21, p236]).

3. It is interesting to contrast the approach of this chapter with that of Gross and Rosen in [19]. They consider a way of constructing special units corresponding to L-function values via Fourier analysis. The resulting units differ from those defined above due to our use of the "smoothing" factors $\delta_\mathfrak{t}$ to ensure that our units lie in the desired ray class field; by contrast, in loc. cit. this is achieved by raising to powers, with the required power possibly depending on the conductor (see [19, (7.14)]). This dependence corresponds to less satisfactory distribution relations. It is likely that their approach could be adapted to provide a more unified construction than the piecemeal approach of §§2–5 for our particular choice of elements.

The verification of the axioms will give a proof of the refined abelian Stark conjecture:

Corollary 1.5. *Let K/k be a finite abelian extension, where k is a field of the type discussed above. Let S be a set as in Chapter 2 such that $r_S = 1$ and $\infty \in S$ splits completely in K. Then Conjecture 3.4.2 is true.*

Proof. We first remark that it is sufficient to verify the conjecture for almost all $T = \{\mathfrak{t}\}$, and also sufficient to verify it for an abelian extension L/k satisfying the conditions of Proposition 4.2.1 relative to K/k. Since $\#S \geq r_S + 1 = 2$, there are $n \geq 1$ finite (i.e. different from ∞) primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ in S. By global class field theory and the finiteness of the group of roots of unity of k, there exist integers $e_1, \ldots, e_n$ such that, if $\mathfrak{m}$ is defined by (6.3), then $K \subseteq H(\mathfrak{m})$ and $w_i = 1$ for all i. Taking $L = H(\mathfrak{m})$, we see that for almost all $\mathfrak{t}$ we have the membership relation $\eta_{L/k,S,\mathfrak{t}} \in U_{L,S,\mathfrak{t}}$, as required. □

Remark 1.6. Explicit units are used to prove the refined abelian Stark conjecture in [46, Prop. 3.9] ($k = \mathbb{Q}$), [45] (k imaginary quadratic) and [21] (k a function field). We note that the use of Rubin's reformulation of Stark's conjecture produces a unified approach to this method of proof, and that in particular the use of elliptic units is somewhat neater than in [45].

In the rest of this chapter we prove Proposition 1.1 for the three different kinds of k.

2 Cyclotomic fields

We begin with the most familiar case, that of $k = \mathbb{Q}$, which is also in many ways the simplest because $\mathbb{Q}$ has class number one. We have $H = k = \mathbb{Q}$, $\mathcal{O} = \mathbb{Z}$, and write $\mathfrak{m} = (m)$, $\mathfrak{p}_i = (p_i)$ and $\mathfrak{t} = (t)$ in the notation of §1, for positive integers m, p_i, t. Here t is required to be an odd prime not dividing m. We define positive integers m_i, m_I for each $I \subseteq \{1, \ldots, n\} \ni i$ by $(m_i) = \mathfrak{m}_i, (m_I) = \mathfrak{m}_I$. For a positive integer r, let $\zeta_r = e^{2\pi i/r}$. Define

$$\hat{\lambda}_I = (1 - \zeta_{m_I}) \qquad \lambda_I = \hat{\lambda}_I^{\delta_t}.$$

Then $\hat{\lambda}_I$ generates the narrow ray class field associated to the divisor $m_I\infty$, with Galois group over $\mathbb{Q}$ equal to $(\mathbb{Z}/m_I Z)^\times \cong \mathcal{I}_{\mathbb{Q},S}/\mathcal{P}_{\mathbb{Q},S,m_I\infty}$, where $\mathcal{P}_{\mathbb{Q},S,m_I\infty}$ is the group of principal fractional ideals with a *positive* generator congruent to 1 mod m_I. The generator of the decomposition group at infinity is complex conjugation, corresponding to $-1 \in (\mathbb{Z}/m_I\mathbb{Z})^\times$. This acts on $\hat{\lambda}_I$ by multiplication by a $2m$-th root of unity. Since the $2m$-th roots of unity are annihilated by δ_t (using Lemma 2.4.2(2) to see that Hypothesis 2.4.1 is satisfied by $\mathbb{Q}(\zeta_m)/\mathbb{Q}$), this means that complex conjugation acts trivially on λ_I, which is therefore real and so lies in the ray class field $H(m_I)$. By the definition of the Frobenius map, λ_I satisfies the congruence condition at primes above $\mathfrak{t}$. So we have established Proposition 1.1 (1) for the cyclotomic elements.

Consider the factorisation in the polynomial ring $\mathbb{C}[X]$

$$X^{m_i} - 1 = \prod_{j=1}^{m_i}(X - \zeta_{m_i}^j) = \Big[\prod_{j \in (\mathbb{Z}/m_i\mathbb{Z})^\times}(X - \zeta_{m_i}^j)\Big](X^{m_i/p_i} - 1). \tag{6.4}$$

Let $i \notin I$. Choose integers a and b with $am_i + bm_I = 1$, so that $\zeta_{m_{I\cup\{i\}}} = \zeta_{m_i}^b \zeta_{m_I}^a$. Substitute $X = \zeta_{m_I}^{-a}$ into (6.4) and multiply through by $\zeta_{m_I}^{am_i}$:

$$1 - \zeta_{m_I}^{am_i} = \Big[\prod_{j \in (\mathbb{Z}/m_i\mathbb{Z})^\times}(1 - \zeta_{m_I}^a \zeta_{m_i}^j)\Big](1 - \zeta_{m_I}^{am_i/p_i})$$

Note that $\zeta_I^{\sigma(p_i)} = \zeta_I^{p_i}$ and $m_i = p_i^{e_i}$. Applying δ_t, we obtain

$$\lambda_{m_I}^{1-\sigma_{(p_i)}^{-1}} = \prod_{j \in (\mathbb{Z}/m_i\mathbb{Z})^\times} \lambda_{I\cup\{i\}}^{\sigma(r_j)},$$

where for each j, we pick an integer r_j congruent to 1 modulo m_I and to j modulo m_i. Now take $\mathfrak{a} = (m_I)$ and $\mathfrak{b} = (m_i)$ in (6.2). We note that $w_i/w_{I\cup\{i\}}$ is the size of the kernel of the map $(\mathbb{Z}/m_i\mathbb{Z})^\times \twoheadrightarrow \mathrm{Gal}(H(m_{I\cup\{i\}})/H(m_I))$, and so our calculations verify assertion (2a) of Proposition 1.1.

Now from (6.4) we obtain

$$\sum_{n=0}^{p_i-1} X^{m_i n/p_i} = \prod_{j \in (\mathbb{Z}/m_i\mathbb{Z})^\times}(X - \zeta_{m_i}^j).$$

Setting $X = 1$ in this equality gives $p_i = \prod_{j\in(\mathbb{Z}/m_i\mathbb{Z})^\times}(1-\zeta_{m_i}^j)$. Applying δ_t, we get $p_i^{1-N_t} = N_{H(m_i)/H}\lambda_i^{w_k/w_i}$. This shows assertion (2b).

As for L-function evaluation, [45, (3)] shows that we have, for σ the element of $\mathrm{Gal}(H(m_I)/\mathbb{Q})$ corresponding to $a \in \mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\}$

$$w_{\mathbb{Q},m_I}\zeta'_{H(m_I)/\mathbb{Q},S_I}(0,\sigma) = z'_{m_I}(0,a) = -\ln|\,1-e^{2\pi i a/m_I}\,|, \tag{6.5}$$

where

$$z_{m_I}(s,a) = \sum_{n\equiv a \bmod m_I} |n|^{-s}$$

is the function mentioned in Remark 1.4(2) above. Therefore, by Proposition 1.3, we obtain

$$w_I\Theta'_{H(m_I)/k,S_I,\mathfrak{t}}(0)\infty' = \lambda_{\infty'}(\lambda_I),$$

where ∞' is the place of $H(m_I)$ induced by our choice of $\zeta_{m_I} \in \mathbb{C}$. This verifies Proposition 1.1 part (3).

3 Function fields

The special units in this case will come from division points on sign-normalised rank-1 Drinfeld modules. This theory was developed by Hayes (see [20] and [21]) and is neatly exposited in [15, §7].

Let k be a global function field with finite constant field $\mathbb{F}$. The field $H(\mathfrak{m})$ in this context is that denoted $\mathbf{k}(\mathfrak{m})^+$ in [15, Defn. 7.5.10]. As in the cyclotomic case, analytically-constructed elements $\hat{\lambda}_I$, which generate "narrow" ray class fields, will map under $\delta_\mathfrak{t}$ to give the system λ_I. We may choose $\mathfrak{t}$ to be any prime of $\mathcal{O}$ not dividing $\mathfrak{m}$.

The chosen place ∞ of k is, of course, finite, and so it has a residue field $\mathbb{F}_\infty$ which is a finite extension of $\mathbb{F}$. This field $\mathbb{F}_\infty$ is also the field of constants of the completion k_∞ of k at ∞. We fix a *sign-function* sgn: $k_\infty^\times \to \mathbb{F}_\infty^\times$ as in [15, Defn. 7.2.1]. An element x of $k_\infty^\times$ will be called *positive* if $\mathrm{sgn}(x) = 1$; an idèle $\mathbf{i} \in J_k$ will be called positive if $\mathrm{sgn}(i_\infty) = 1$. By definition, a Drinfeld module with coefficients in $\mathbb{C}_\infty$, the completion of the algebraic closure of k_∞, is an $\mathbb{F}$-linear homomorphism

$$\begin{array}{cccc} \rho: & \mathcal{O} & \longrightarrow & \mathbb{C}_\infty[X]_\circ \\ & x & \longmapsto & \rho_x \end{array}$$

with values in the composition ring of additive polynomials. We will consider a sgn-normalised rank-1 Drinfeld module (also called a Hayes-module) ρ in the sense of [15, Defn. 7.2.14], so that the leading coefficient of ρ_x is $\mathrm{sgn}(x)^\sigma$ for all $x \in \mathcal{O}$-$\{0\}$ and some automorphism $\sigma \in \mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F})$. The coefficients of any such ρ generate an abelian extension H^+/k, called the normalising field with respect to sgn. This field corresponds via class field theory to the idèle subgroup $k^\times U(1)^+$, where $U(1)^+$ is the subgroup of positive idèles in $U(1)$, or equivalently to the ray class group $\mathcal{I}_{k,\infty}/\mathcal{P}_{k,\infty,\infty}$, where $\mathcal{P}_{k,\infty,\infty}$ is the subgroup of $\mathcal{P}_{k,\infty}$ of principal fractional ideals with a positive generator. The extension is ramified only at ∞, and has field of constants $\mathbb{F}_\infty$. The decomposition group of ∞ is equal to the inertia group, and isomorphic to $\mathbb{F}_\infty^\times/\mathbb{F}^\times$.

If $\mathfrak{a}$ is a proper nonzero ideal of $\mathcal{O}$, then the $\mathfrak{a}$-torsion points $\rho[\mathfrak{a}] = \{x \in \mathbb{C}_\infty : \rho_a(x) = 0 \text{ for all } a \in \mathfrak{a}\}$ of ρ are naturally made via the action of ρ into an $\mathcal{O}$-module isomorphic to $\mathcal{O}/\mathfrak{a}$. The elements of $\rho[\mathfrak{a}]$ which are generators of this cyclic $\mathcal{O}$-module are called primitive $\mathfrak{a}$-division points for ρ. Set $S = \{\infty\} \cup \mathrm{Supp}(\mathfrak{a})$. Any primitive $\mathfrak{a}$-division point $\hat{\lambda} \in \rho[\mathfrak{a}]$ is such that the extension $H^+(\hat{\lambda})/k$ is abelian, and corresponds via class field theory to idèle subgroup $k^\times U(\mathfrak{a})^+$ (where $U(\mathfrak{a})^+$ is the subgroup of positive idèles in $U(\mathfrak{a})$), or accordingly to $\mathcal{I}_{k,S}/\mathcal{P}_{k,S,\mathfrak{a}\infty}$, where $\mathcal{P}_{k,S,\mathfrak{a}\infty}$ is the group of principal fractional ideals of $\mathcal{O}$ with a positive generator x satisfying $x \equiv 1 \pmod{\mathfrak{a}}$. An $\mathfrak{a}$-division point for ρ is thus algebraic over k. Its valuations are zero outside the support of $\mathfrak{a}$ and ∞ [21, Thm. 4.17]. The decomposition group of ∞ in the extension $H^+(\hat{\lambda})/k$ is equal to the inertia group and isomorphic to $\mathbb{F}_\infty^\times$. The field $H(\mathfrak{a})$ is obtained as the fixed field with respect to this group. The constant field of both $H(\mathfrak{a})$ and $H^+(\hat{\lambda})$ is $\mathbb{F}_\infty$.

We extend the definition of ρ from elements of $\mathcal{O}$ to ideals as follows: if $\mathfrak{b}$ is a nonzero ideal of $\mathcal{O}$, then $\rho_\mathfrak{b}$ is the monic polynomial with roots $\rho[\mathfrak{b}]$. This gives an explicit class field theory; for $\mathfrak{b}$ coprime to $\mathfrak{a}$, the Artin symbol for $\mathfrak{b}$ acts on $H^+(\hat{\lambda})$ via

$$\hat{\lambda}^{\sigma_\mathfrak{b}} = \rho_\mathfrak{b}(\hat{\lambda}), \tag{6.6}$$

(see [15, Prop. 7.5.4 (3)]). The polynomials satisfy an important relation. If $\mathfrak{b}$ and $\mathfrak{c}$ are nonzero ideals of $\mathcal{O}$, then we have

$$\rho_{\mathfrak{b}\mathfrak{c}} = (\mathfrak{c} * \rho)_\mathfrak{b} \rho_\mathfrak{c} = (\mathfrak{b} * \rho)_\mathfrak{c} \rho_\mathfrak{b}, \tag{6.7}$$

where $\mathfrak{b} * \rho$ is the sgn-normalised rank one Drinfeld module obtained by letting the class of $\mathfrak{b}$ in $\mathcal{I}_{k,\infty}/\mathcal{P}_{k,\infty,\infty}$ act on the coefficients of ρ by the reciprocity map.

Note that the fields $H^+(\hat{\lambda})$ and $H(\mathfrak{a})$ are independent of the choices of the sgn-normalised rank one Drinfeld module ρ and the $\mathfrak{a}$-division point $\hat{\lambda}$. Indeed, all such Drinfeld modules can be obtained from ρ by the action "$*$" of ideals on H^+, and the union of their set of $\mathfrak{a}$-division points is permuted transitively by the Galois group of $H^+(\hat{\lambda})/k$.

We now proceed to define the system of elements λ_I required by Proposition 1.1. Fix a sgn-normalised rank one Drinfeld module ρ and a primitive $\mathfrak{m}$-division point $\hat{\lambda}$. Then for $I \subseteq \{1, \dots, n\}$ we set

$$\hat{\lambda}_I = \rho_{I'}(\hat{\lambda}).$$

Then $(\mathfrak{m}_{I'} * \rho)_{\mathfrak{m}_I}(\hat{\lambda}_I) = \rho_\mathfrak{m}(\hat{\lambda})$ by (6.7), and this is zero. Hence $\hat{\lambda}_I$ is an $\mathfrak{m}_I$-division point for the sgn-normalised rank one Drinfeld module $\mathfrak{m}_{I'} * \rho$. If $a \in \mathcal{O}$ then $(\mathfrak{m}_{I'} * \rho)_{(a)}(\hat{\lambda}_I) = \rho_{a\mathfrak{m}_{I'}}(\hat{\lambda})$ and this is zero if and only if $a \in \mathfrak{m}_I$. Therefore $\hat{\lambda}_I$ is a primitive $\mathfrak{m}_I$-division point for $\mathfrak{m}_{I'} * \rho$. The extension $H^+(\hat{\lambda}_I)/H^+$ has

Galois group isomorphic to $\Gamma_{\mathfrak{m}_I} = (\mathcal{O}/\mathfrak{m}_I)^\times$; another such field $H^+(\hat{\lambda}_J)$ is linearly disjoint over H^+ if J is disjoint from I.

There is another characterisation of $\hat{\lambda}_I$. Using these elements to choose isomorphisms $(\mathfrak{m}_{I'} * \rho)[\mathfrak{m}_I] \cong \mathcal{O}/\mathfrak{m}_I$ gives us commutative diagrams

$$\begin{array}{ccc} \rho[\mathfrak{m}] & \xrightarrow{\rho_{\mathfrak{m}_{I'}}} & (\mathfrak{m}_{I'} * \rho)[\mathfrak{m}_I] \\ \cong\downarrow & & \cong\downarrow \\ \mathcal{O}/\mathfrak{m} & \longrightarrow & \mathcal{O}/\mathfrak{m}_I, \end{array}$$

where the map at the bottom is the natural projection. Since $\mathcal{O}/\mathfrak{m} \cong \prod_i \mathcal{O}/\mathfrak{m}_i$, to know $\hat{\lambda}_I$ it is sufficient to know all its images under $\rho_{\mathfrak{m}_I/\mathfrak{m}_i}$ for each $i \in I$. We have by definition that $\rho_{\mathfrak{m}/\mathfrak{m}_i}(\hat{\lambda}) = \hat{\lambda}_i$, and so, by (6.6), we have $\hat{\lambda} = \sum_{i=1}^n \hat{\lambda}_i^{\sigma^{-1}_{\mathfrak{m}/\mathfrak{m}_i}}$. Applying $\rho_{\mathfrak{m}_{I'}}$ to this gives

$$\hat{\lambda}_I = \sum_{i \in I} \hat{\lambda}_i^{\sigma^{-1}_{\mathfrak{m}_I/\mathfrak{m}_i}}. \tag{6.8}$$

Recall that $\mathrm{Gal}(H^+(\hat{\lambda}_I)/H(\mathfrak{m}_I))$ is the decomposition group of ∞ in the extension $H^+(\hat{\lambda}_I)/k$. If σ is in this group, then σ acts on $\hat{\lambda}_I$ by multiplication by a root of unity in $\mathbb{F}_\infty^\times \subseteq H(\mathfrak{m}_I)$ (this follows from [21, Cor. 4.14]). Since $\delta_{\mathfrak{t}}$ annihilates these roots of unity (noting that there are no more roots of unity in $H^+(\hat{\lambda}_I)$ than in $H(\mathfrak{m}_I)$, since both have constant field $\mathbb{F}_\infty$), the element $\lambda_I := \hat{\lambda}_I^{\delta_{\mathfrak{t}}}$ is fixed by σ and so lies in $H(\mathfrak{m}_I)$.

As in the cyclotomic case, the congruence conditions on λ_I above $\mathfrak{t}$ follow directly from the definition, and since λ_I satisfy the valuation conditions, we have that Proposition 1.1 (1) holds for these elements. We proceed to check the other properties required by the Proposition.

Let $i \notin I \subseteq \{1, \ldots, n\}$, and set $\rho' = \mathfrak{m}_{I'\text{-}\{i\}} * \rho$. Then

$$\rho'_{\mathfrak{m}_i}(X) = \prod_{\hat{\lambda}:\rho'_{\mathfrak{m}_i}(\hat{\lambda})=0} (X - \hat{\lambda}) = \prod_{\sigma \in \mathrm{Gal}(H^+(\hat{\lambda}_{\mathfrak{m}_i})/H^+)} (X - \tilde{\lambda}^\sigma)\rho'_{\mathfrak{m}_i/\mathfrak{p}_i}(X), \tag{6.9}$$

where $\tilde{\lambda}$ is a primitive $\mathfrak{m}_i$-division point for ρ'. Since $\rho'_{\mathfrak{m}_i}(\hat{\lambda}_i^{\sigma^{-1}_{\mathfrak{m}_I}}) = \sigma^{-1}_{\mathfrak{m}_I}((\mathfrak{m}/\mathfrak{m}_i * \rho)_{\mathfrak{m}_i}(\hat{\lambda}_i)) = 0$, we see that $\tilde{\lambda} = -\hat{\lambda}_i^{\sigma^{-1}_{\mathfrak{m}_I}}$ (which it is easy to show is primitive) will do. Assuming I nonempty, we now set $X = \hat{\lambda}_I^{\sigma^{-1}_{\mathfrak{m}_i}}$, so that $X - \tilde{\lambda} = \hat{\lambda}_{I\cup\{i\}}$ by the characterisation (6.8). Then for any nonzero ideal $\mathfrak{a}$ coprime to $\mathfrak{m}_I$ we have

$$\rho'_{\mathfrak{a}}(X) = \sigma^{-1}_{\mathfrak{m}_i}((\mathfrak{m}_i * \rho')_{\mathfrak{a}}(\hat{\lambda}_I)) = \sigma^{-1}_{\mathfrak{m}_i}((\mathfrak{m}_{I'} * \rho)_{\mathfrak{a}}(\hat{\lambda}_I)) = \sigma^{-1}_{\mathfrak{m}_i}\sigma_{\mathfrak{a}}(\hat{\lambda}_I).$$

Hence we obtain from (6.9):

$$\hat{\lambda}_I^{1-\sigma^{-1}_{\mathfrak{p}_i}} = \prod_{\mathfrak{f}} \hat{\lambda}_{I\cup\{i\}}^{\sigma_{\mathfrak{f}}},$$

where $\mathfrak{f}$ runs through $\mathcal{P}_{k,\infty,\mathfrak{m}_{I\cup\{i\}}\infty}/\mathcal{P}_{k,\infty,\mathfrak{m}_I\infty}$. Therefore we have

$$\hat{\lambda}_I^{1-\sigma_{\mathfrak{p}_i}^{-1}} = N_{H^+(\hat{\lambda}_{I\cup\{i\}})/H^+(\hat{\lambda}_I)}\hat{\lambda}_{I\cup\{i\}}.$$

We now apply $\delta_{\mathfrak{t}}$ to this equation.

Lemma 3.1. *Provided I is not empty, the restriction map*

$$\mathrm{Gal}(H^+(\hat{\lambda}_{I\cup\{i\}})/H^+(\hat{\lambda}_I)) \to \mathrm{Gal}(H(\mathfrak{m}_{I\cup\{i\}})/H(\mathfrak{m}_I))$$

is an isomorphism.

Proof. Note that $\mathrm{Gal}(H^+(\hat{\lambda}_{\mathfrak{a}})/H^+) \cong (\mathcal{O}/\mathfrak{a})^\times$ for any primitive $\mathfrak{a}$ division point $\hat{\lambda}_{\mathfrak{a}}$ of ρ (see [15, Cor. 7.5.6]), so the domain of the restriction map is naturally isomorphic to $(\mathcal{O}/\mathfrak{m}_i)^\times$. In (6.2), set $\mathfrak{a} = \mathfrak{m}_I$ and $\mathfrak{b} = \mathfrak{m}_i$, then the required restriction map is $(\mathcal{O}/\mathfrak{b})^\times \to \mathrm{Gal}(H(\mathfrak{a}\mathfrak{b})/H(\mathfrak{a}))$. Lemma 4.2 shows that $w_{\mathfrak{a}} = 1$, hence the kernel of this map is trivial, and so it is an isomorphism. □

We obtain assertion (2a) of Proposition 1.1.

We turn now to the proof of assertion (2b). Note the Principal Ideal Theorem which states that for any ideal $\mathfrak{a}$ of $\mathcal{O}$, we have $\mathfrak{a}\mathcal{O}_{H^+} = D\rho_{\mathfrak{a}}\mathcal{O}_{H^+}$ ([15, Thm. 7.6.2]). Here D represents taking the coefficient of the linear term of the polynomial. Using this and comparing linear terms in (6.9) for $I = \emptyset$ gives the equality $D\rho'_{\mathfrak{m}_i} = \pm N_{H^+(\hat{\lambda}_i)/H^+}(\hat{\lambda}_i)D\rho'_{\mathfrak{m}_i/\mathfrak{p}_i}$. We have $\mathfrak{m}_i\mathcal{O}_{H^+} = D\rho'_{\mathfrak{m}_i}\mathcal{O}_{H^+}$ contained in $\mathfrak{m}_i/\mathfrak{p}_i\mathcal{O}_{H^+} = D\rho'_{\mathfrak{m}_i/\mathfrak{p}_i}\mathcal{O}_{H^+}$, and so $D\rho'_{\mathfrak{m}_i/\mathfrak{p}_i}$ divides $D\rho'_{\mathfrak{m}_i}$ and

$$N_{H^+(\hat{\lambda}_i)/H^+}(\hat{\lambda}_i)\mathcal{O}_{H^+} = \mathfrak{p}_i\mathcal{O}_{H^+}. \tag{6.10}$$

From (6.2) we obtain the exact sequence

$$0 \longrightarrow \mu_k \longrightarrow \mathrm{Gal}(H^+(\hat{\lambda}_i)/H^+) \longrightarrow \mathrm{Gal}(H(\mathfrak{m}_i)/H) \longrightarrow 0.$$

Therefore applying $\delta_{\mathfrak{t}}$ to (6.10) gives

$$N_{H(\mathfrak{m}_i)/H}\lambda_i^{w_k}\mathcal{O}_H = \mathfrak{p}_i^{1-N_{\mathfrak{t}}}\mathcal{O}_H.$$

This shows Proposition 1.1(2b).

Finally, we turn to assertion (3). Let ∞' be the place of $H^+(\hat{\lambda})$ whereby $\hat{\lambda}$ corresponds to the element $\xi(\mathfrak{m})e_{\mathfrak{m}}(1) \in \mathbb{C}_\infty$ as in [21, (5.5)] where $e_{\mathfrak{m}}$ is the exponential function associated to the lattice $\mathfrak{m}$ and $\xi(\mathfrak{m}) \in \mathbb{C}_\infty$ is such that $\xi(\mathfrak{m})\mathfrak{m}$ is a "special" lattice in the sense of [21, §5]. Then $\hat{\lambda}_I = \rho_{\mathfrak{m}_{I'}}(\hat{\lambda})$ corresponds by ∞' to the element $\xi(\mathfrak{m}_I)e_{\mathfrak{m}_I}(1)$ by [21, (5.3)].[1]

Hayes shows ([21, §6])

$$\zeta'_{H(\mathfrak{m}_I)/k,S_I}(0,\sigma) = -\ln|\rho_{\mathfrak{c}}(\hat{\lambda}_I)|_{\infty'},$$

[1]The factor $\xi(\mathfrak{m}_I)$ is only defined up to a root of unity in $\mathbb{F}_\infty^\times$. This choice does not affect the role in L-function evaluation. We simply choose a compatible system of elements $\xi(\mathfrak{m}_I)$.

where $\mathfrak{c}$ is an ideal in a narrow ideal class corresponding to σ. Therefore assertion (3) is satisfied.

We note that it is also possible to phrase the results of §2 in a similar language of polynomials. The operation $X \boxplus Y = X + Y - XY$ makes $\mathbb{C}$-$\{1\}$ into a $\mathbb{Z}$-module. Then $n \in \mathbb{Z}$ acts via $X \mapsto X^{\boxplus n} = f_n(X)$ where $f_n(X) = (1-(1-X)^n)$. The cyclotomic elements $1-\zeta_{m_I}$ are primitive m_I division points of this module. They satisfy the identities

$$1-\zeta_{m_I} = f_{m_{I'}}(1-\zeta_m); \quad (1-\zeta_{m_I})^{\sigma_a} = f_a(1-\zeta_{m_I}); \quad 1-\zeta_{m_I} = \boxplus_{i\in I}(1-\zeta_{m_i})^{\sigma^{-1}_{m_I/m_i}},$$

in close analogy with the Drinfeld module case. Finally, in each case the special elements $\lambda_I \in H(\mathfrak{m}_I)$ are obtained by "t-modifying" the division points.

4 Robert's functions

We now move on to the case where k is an imaginary quadratic field. The system of elliptic units we will use is essentially that used by Bley in [2]. One property which we require of these elements is not clear from loc. cit., namely the congruence condition modulo $\mathfrak{t}$ in Proposition 1.1 (1). To establish this, we will interpret Bley's units as another case of the $\mathfrak{t}$-modifying process we have seen in the previous two sections – that is, we will express the units as $\hat{\lambda}^{\delta_{\mathfrak{t}}}$ for some $\hat{\lambda}$ in the maximal abelian extension of k.

We first review the construction from [38] used in [2]. Let $L \subseteq \underline{L}$ be an inclusion of (full) $\mathbb{Z}$-lattices in $\mathbb{C}$ with index coprime to 6. Let $\omega = \binom{w_1}{w_2}$ be a column vector whose entries form a $\mathbb{Z}$-basis for L, positively oriented in the sense that w_2/w_1 has positive imaginary part, and $\underline{\omega} = \binom{\underline{w}_1}{\underline{w}_2}$ be a positively oriented basis for $\underline{L}$. There is a matrix $B \in \mathrm{M}_2^+(\mathbb{Z})$ (meaning 2×2 matrices over $\mathbb{Z}$ with positive determinant) such that $\omega = B\underline{\omega}$. Robert defines ([38, p237])

$$\tilde{F}(t; L; \underline{L}) := \rho(\omega, \underline{\omega})^{-1} \frac{\varphi(t;\omega)^{\det B}}{\varphi(t;\underline{\omega})}. \tag{6.11}$$

Here $\rho(\omega, \underline{\omega})$ is a twelfth root of unity depending only on B, and $\varphi = \varphi_{\mathrm{Rob}}$ is the φ-function of the lattice [38, (4)]:

$$\varphi_{\mathrm{Rob}}(t; w_1, w_2) = iq^{\frac{1}{2}B_2(u)} \alpha^{\frac{u-1}{2}}(1-\alpha q^u) \prod_{n=1}^{\infty}(1-\alpha q^{n+u})(1-\alpha^{-1}q^{n-u}), \tag{6.12}$$

where $\alpha = e^{2\pi i v}$, $q = e^{2\pi i \frac{w_2}{w_1}}$ and B_2 is the second Bernoulli polynomial $B_2(X) = X^2 - X + \frac{1}{6}$. Many authors define similar functions, and so it is useful to have a comparison between them. If w_1, w_2 and t are as above, and we write $t = uw_2 + vw_1$ for $u, v \in \mathbb{R}$, then we have

$$\varphi_{\mathrm{Rob}}(t; w_1, w_2) = \phi_{\mathrm{St}}(u, v, w_2/w_1) = -i\varphi_{\mathrm{Sch}}\left(u\frac{w_2}{w_1} + v\Big|_1^{w_2/w_1}\right) = -i\varphi_{\mathrm{Ouk}}(t; w_2, w_1), \tag{6.13}$$

where φ_{Rob} denotes Robert's function φ defined in [38], ϕ_{St} is Stark's function ϕ in [45], φ_{Sch} is the function denoted φ in Schertz's paper [40], and φ_{Ouk} is Oukhaba's function φ in [29]. The comparison is by comparing the q-expansions [45, (10)] and [40, (4.3)] to (6.12), and for φ_{Ouk} by [29, §2.2].

To calculate the twelfth root of unity $\rho(B)$, one uses a factor appearing in transformation formulas for the Dedekind η function $\eta(\tau) = e^{2\pi i\tau/24}\prod_{n=1}^{\infty}(1 - e^{2\pi i n\tau})$, where τ is an element of the upper half-plane. This function η is a certain 24th root of the usual discriminant function for the lattice $\mathbb{Z} + \tau\mathbb{Z}$. Let a matrix $\tilde{B}$ of positive determinant act on the upper half plane via the usual formula

$$\tilde{B} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow \tilde{B}\tau = \frac{a\tau + b}{c\tau + d}.$$

There is a function $\varepsilon : SL_2(\mathbb{Z}) \to \mu_{24}$ which is given by the rule

$$\eta(\tilde{B}\tau) = \varepsilon(\tilde{B})\sqrt{c\tau + d}\,\eta(\tau) \tag{6.14}$$

for $\tilde{B} \in \mathrm{SL}_2(\mathbb{Z})$, where the square root is chosen to have argument θ satisfying $-\frac{\pi}{2} \le \theta < \frac{\pi}{2}$, and so maps the upper half-plane to the first quadrant. Squaring (6.14), we see that $\tilde{B} \mapsto \varepsilon(\tilde{B})^2$ is a homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mu_{12}$ (note that this homomorphism is denoted ω in [45] and $\rho^{(2)}$ in [38]). The group $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ (see eg. [23, Ch. 2, §1, Thm. 1]) and ε^2 takes values $e^{2\pi i/12}$ and $-i$ on these matrices, respectively, by [23, Ch. 18, §5, Thm. 6]. This is sufficient to define ε^2; in fact, an explicit formula for ε is given in [48, §38, (15)].

The function ε^2 also gives the transformation formula for the various φ functions in (6.13). The formula [40, (4.2)] states, for $\tilde{B} \in \mathrm{SL}_2(\mathbb{Z})$, that

$$\varphi_{\mathrm{Sch}}\left(\begin{pmatrix} u & v \end{pmatrix}\begin{pmatrix} \tilde{B}z \\ 1 \end{pmatrix}\Big|_{1}^{\tilde{B}z}\right) = \varepsilon(\tilde{B})^2\varphi_{\mathrm{Sch}}\left(\begin{pmatrix} u & v \end{pmatrix}\tilde{B}\begin{pmatrix} z \\ 1 \end{pmatrix}\Big|_{1}^{z}\right). \tag{6.15}$$

To translate this into a statement for the function φ_{Rob}, we set $z = \underline{w}_2/\underline{w}_1$ and note that

$$\omega = B\underline{\omega}, \text{ i.e. } \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = B\begin{pmatrix} \underline{w}_1 \\ \underline{w}_2 \end{pmatrix}, \text{ implies that } \frac{w_2}{w_1} = \tilde{B}\frac{\underline{w}_2}{\underline{w}_1}, \tag{6.16}$$

where B and $\tilde{B}$ are related by

$$B = \begin{pmatrix} d & c \\ b & a \end{pmatrix} \iff \tilde{B} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} B \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{6.17}$$

This operation $B \mapsto \tilde{B}$ is an automorphism of $\mathrm{SL}_2(\mathbb{Z})$ of order 2, as can be seen by its expression in (6.17) as the restriction of conjugation in $\mathrm{GL}_2(\mathbb{Z})$ by a (self-inverse) matrix. It then follows from (6.15) that

$$\varphi_{\mathrm{Rob}}(t; B\underline{\omega}) = \varepsilon(\tilde{B})^2\varphi_{\mathrm{Rob}}(t; \underline{\omega}). \tag{6.18}$$

Since one property of $\rho(B)$ in its definition in [38, §4, Théorèm principal] is that the function (6.11) depends only on the lattices L and $\underline{L}$ and not the choice of bases, choosing $L = \underline{L}$ and using (6.18) shows that we must have $\rho(B) = \varepsilon(\tilde{B})^2$ for $B \in \mathrm{SL}_2(\mathbb{Z})$.

It is natural to ask how $\varepsilon(\tilde{B})^2$ is related to $\varepsilon(B)^2$.

Lemma 4.1. *For any $B \in \mathrm{SL}_2(\mathbb{Z})$, we have*

$$\varepsilon(\tilde{B})^2 = \varepsilon(B)^{-2}.$$

Proof. Since $\tilde{B} \mapsto B$ and ε^2 are homomorphisms, it is sufficient to check this on generators of $\mathrm{SL}_2(\mathbb{Z})$.

We have

$$\text{for } \tilde{B} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \; \varepsilon(\tilde{B})^2 = -i; \quad \varepsilon(B)^2 = \varepsilon(\tilde{B}^3)^2 = \frac{1}{-i},$$

and so it works for this generator. Then

$$\text{for } \tilde{B} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \; \varepsilon(\tilde{B})^2 = e^{2\pi i/12}; \quad \varepsilon(B)^2 = \varepsilon\left(\tilde{B}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\tilde{B}\right)^2 = e^{-2\pi i/12},$$

as required. $\square$

Hence we have $\rho(B) = \varepsilon(B)^{-2}$ for $B \in \mathrm{SL}_2(\mathbb{Z})$. We note that this is not stated correctly in [38, (16)] and [38, §11, Rem. 2], since Robert's $\rho^{(2)}(B)$ is equal to $\varepsilon(B)^2$ and not its inverse. Possibly Robert has made an error due to confusion between [38, (10)] and the similar equation before [38, (9)] – cf. (6.16) above. Another correction in this regard is that in [38, (11)], "$\beta(\bar{\omega}, \omega)$" should read "$\beta(\omega, \tilde{\omega})$".

Two further properties of ρ given in [38] suffice to give a formula for it (in terms of ε) for all elements of $\mathrm{M}_2^+(\mathbb{Z})_{(6)}$. Firstly, if $B, D \in \mathrm{M}_2^+(\mathbb{Z})_{(6)}$, then [38, (18)] shows that

$$\rho(BD) = \rho(B)^{\det D}\rho(D) \tag{6.19}$$

namely, ρ is a 1-cocycle of $\mathrm{M}_2^+(\mathbb{Z})_{(6)}$ with values in μ_{12}, where matrices act on roots of unity via their determinants. Secondly, for positive integers c, d coprime to 6, we have by [38, §10, Fait 3]

$$\rho\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} = (-1)^{\frac{d-1}{2}}.$$

Therefore we obtain the following, which is [38, §11, Rem. 2]:

Lemma 4.2. *If $B \in \mathrm{M}_2^+(\mathbb{Z})_{(6)}$ is expressed in the form*

$$B = E\begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix}F, \tag{6.20}$$

with $E, F \in \mathrm{SL}_2(\mathbb{Z})$, then

$$\rho(B) = \varepsilon(E)^{-b_1 b_2}(-1)^{\frac{b_2-1}{2}}\varepsilon(F)^{-2}. \quad \square$$

We note that by the theory of matrix diagonalisation, any B can be expressed in the form (6.20).

5 Elliptic units

We now construct the system of elliptic units from special values of φ_{Rob}, following [2]. Let k be an imaginary quadratic field, and choose an embedding $k \to \mathbb{C}$. If $\mathfrak{a}$ is an ideal of the ring of integers $\mathcal{O}$ of k, then $\mathfrak{a}$ is a lattice in $\mathbb{C}$ with complex multiplication by $\mathcal{O}$ (i.e. an $\mathcal{O}$-module). We define $f_{\mathfrak{a}}$ to be the smallest positive rational integer contained in $\mathfrak{a}$.

Let $L = \mathfrak{a}$, and choose a positively-oriented basis $\omega = (w_1, w_2)$ for L. By [29, Prop. 2(i)], the complex number $i\varphi_{\mathrm{Rob}}(1; \omega)$ lies in the ray class field $H(12f_{\mathfrak{a}}^2)$. One may check that $i \in H(12f_{\mathfrak{a}}^2)$ (using, for example, [37, Lem. 5]), and so $\varphi_{\mathrm{Rob}}(1; \omega) \in H(12f_{\mathfrak{a}}^2)$.

Choosing an ideal $\mathfrak{c}$ of k coprime to $6\mathfrak{a}$, we may ask for the effect of the automorphism corresponding to $\mathfrak{c}$ on $\varphi_{\mathrm{Rob}}(1; \omega)$. Choose a positively-oriented basis $\underline{\omega} = (\underline{w}_1, \underline{w}_2)$ for $\mathfrak{c}^{-1}\mathfrak{a}$, so that $\omega = B\underline{\omega}$ for some matrix $B \in \mathrm{M}_2^+(\mathbb{Z})_{(6)}$ with $\det B = N\mathfrak{p}$.

Proposition 5.1. *If $\mathfrak{c} = \mathfrak{p}$ is a prime ideal, $N\mathfrak{p} = p$ is a prime and p is unramified in k (i.e. p splits in k) then*

$$\varphi_{\mathrm{Rob}}(1; \omega)^{\sigma_{\mathfrak{p}}} = \rho(B)\varphi_{\mathrm{Rob}}(1; \underline{\omega}).$$

Proof. This is a consequence of a theorem of Stark [45, Thm. 3], and the main part of this proof will be to relate Robert's notation to Stark's using the transformation formulas of §4.

We have by (6.13) that $\varphi_{\mathrm{Rob}}(1; w_1, w_2) = \phi_{\mathrm{St}}(u, v, w_2/w_1)$, where $1 = uw_2 + vw_1$ with $u, v \in \mathbb{Q}$. The denominators of u and v can be taken to be equal to $f_{\mathfrak{a}}$, and so the function $\phi_{\mathrm{St}}(u, v, z)$ is a modular function in z of level $12f_{\mathfrak{a}}^2$ by [45, (19)], and the coefficients of its q-expansions lie in the cyclotomic field $\mathbb{Q}(\zeta_{12f_{\mathfrak{a}}^2})$. [45, Thm. 3] then gives

$$\phi_{\mathrm{St}}(u, v, w_2/w_1)^{\sigma_{\mathfrak{p}}} = [\phi_{\mathrm{St}}(u, v, -) \circ \tilde{B}](\underline{w}_2/\underline{w}_1),$$

where we note that, if B_{St} denotes the matrix called B in the statement of [45, Thm. 3], then $pB_{\mathrm{St}}^{-1} = \tilde{B}$. The "$\circ$" denotes a certain action of matrices on modular forms of level $N = 12f_{\mathfrak{a}}^2$ with coefficients in $\mathbb{Q}(\zeta_{12f_{\mathfrak{a}}^2})$, which is given explicitly for particular matrices in [45, (23)], as

$$(f \circ A)(z) = f(Az) \text{ for } A \in \mathrm{SL}_2(\mathbb{Z}) \ ; \quad (f \circ A)(z) = f^{\sigma_d}(z) \text{ if } A = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix},$$

where σ_d acts on the coefficients of f via $\zeta_N \mapsto \zeta_N^d$.

We write

$$\tilde{B} = E \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} F,$$

as in (6.20). Then

$$\begin{aligned}\phi_{\mathrm{St}}(u,v,w_2/w_1)^{\sigma_{\mathfrak{p}}} &= [\phi_{\mathrm{St}}(u,v,-)\circ\tilde{B}]\begin{pmatrix}\underline{w}_2\\ \underline{w}_1\end{pmatrix}\\ &= \left[\phi_{\mathrm{St}}(u,v,-)\circ E\circ\begin{pmatrix}1&0\\0&p\end{pmatrix}\circ F\right]\begin{pmatrix}\underline{w}_2\\ \underline{w}_1\end{pmatrix}.\end{aligned}$$

We have $[\phi_{\mathrm{St}}(u,v,-)\circ E](z) = \phi_{\mathrm{St}}(u,v,Ez) = \varepsilon(E)^2\phi_{\mathrm{St}}((u\quad v)E,z)$ by (6.15). Therefore

$$\begin{aligned}\phi_{\mathrm{St}}(u,v,w_2/w_1)^{\sigma_{\mathfrak{p}}} &= \left[(\varepsilon(E)^2\phi_{\mathrm{St}}((u\quad v)E,-)\circ\begin{pmatrix}1&0\\0&p\end{pmatrix})\right]\left(F\frac{\underline{w}_2}{\underline{w}_1}\right)\\ &= \left[(\varepsilon(E)^2\phi_{\mathrm{St}}((u\quad v)E,-))^{\sigma_p}\right]\left(F\frac{\underline{w}_2}{\underline{w}_1}\right). \qquad (6.21)\end{aligned}$$

Now we note that (6.13) and (6.12) give

$$-i\varphi_{\mathrm{St}}(u',v',z) = q^{\frac{1}{2}B_2(u')}\alpha^{\frac{u'-1}{2}}(1-\alpha q^{u'})\prod_{n=1}^{\infty}(1-\alpha q^{n+u'})(1-\alpha^{-1}q^{n-u'}),$$

where $\alpha = e^{2\pi i v'}$ and $q = e^{2\pi i z}$. The effect of σ_p on this expression is $\alpha\mapsto\alpha^p$, or in other words, v' gets multiplied by p, and so we have

$$-i^p\phi_{\mathrm{St}}((u\quad v)E,-)^{\sigma_p} = -i\phi_{\mathrm{St}}\left((u\quad v)E\begin{pmatrix}1&0\\0&p\end{pmatrix},-\right).$$

Therefore (6.21) becomes

$$\phi_{\mathrm{St}}(u,v,w_2/w_1)^{\sigma_{\mathfrak{p}}} = \varepsilon(E)^{2p}\varepsilon(F)^2 i^{1-p}\phi_{\mathrm{St}}((u\quad v)\tilde{B},\underline{w}_2/\underline{w}_1).$$

Calculating now $\rho(B)$, we have

$$B = \tilde{E}\begin{pmatrix}p&0\\0&1\end{pmatrix}\tilde{F} = (\tilde{E}T^3)\begin{pmatrix}1&0\\0&p\end{pmatrix}(T\tilde{F}),\quad\text{where } T = \begin{pmatrix}0&-1\\1&0\end{pmatrix}$$

and so $\rho(B) = \rho(\tilde{E}T^3)^p\rho(T\tilde{F}) = \varepsilon(E)^{2p}\varepsilon(T)^{-6p}\varepsilon(T)^{-2}\varepsilon(F)^2$. Since $\varepsilon(T)^2 = -i$, this gives $\rho(B) = i^{1-p}\varepsilon(E)^{2p}\varepsilon(F)^2$, and so

$$\phi_{\mathrm{St}}(u,v,w_2/w_1)^{\sigma_{\mathfrak{p}}} = \rho(B)\phi_{\mathrm{St}}((u\quad v)\tilde{B},\underline{w}_2/\underline{w}_1).$$

Now

$$(1) = (u\quad v)\begin{pmatrix}w_2\\w_1\end{pmatrix} = (u\quad v)\tilde{B}\begin{pmatrix}\underline{w}_2\\ \underline{w}_1\end{pmatrix}$$

and so by (6.13)

$$\varphi_{\mathrm{Rob}}(1;w_1,w_2)^{\sigma_{\mathfrak{p}}} = \rho(B)\varphi_{\mathrm{Rob}}(1;\underline{w}_1,\underline{w}_2).$$

as required. $\square$

Corollary 5.2. *For any $\mathfrak{c}$ coprime to $6\mathfrak{a}$, we have*

$$\varphi_{\mathrm{Rob}}(1;\omega)^{\sigma_{\mathfrak{c}}} = \rho(B)\varphi_{\mathrm{Rob}}(1;\underline{\omega}).$$

Proof. We may write $\mathfrak{c} = \lambda\mathfrak{p}$, where $\lambda \in k^\times$ satisfies $\lambda \equiv 1 \pmod{12f_{\mathfrak{a}}^2}$ and $\mathfrak{p}$ satisfies the hypotheses of Proposition 5.1. That is, we may choose a $\mathfrak{p}$ representing the class of $\mathfrak{c}$ in the ray class group corresponding to the ideal $(12f_{\mathfrak{a}}^2)$. This is possible by Čebotarev's density theorem. We write $\lambda = \frac{\alpha}{\beta}$ with $\alpha, \beta \in \mathcal{O}, \alpha \equiv \beta \pmod{12f_{\mathfrak{a}}^2}$ and coprime to $12f_{\mathfrak{a}}^2$.

Let $\underline{\omega}' = (\underline{w}_1', \underline{w}_2')$ be the basis for $\mathfrak{p}^{-1}\mathfrak{a}$ given by $\underline{\omega}' = \lambda\underline{\omega} = (\lambda\underline{w}_1, \lambda\underline{w}_2)$. Let $B' \in \mathrm{M}_2^+(\mathbb{Z})_{(6)}$ be the matrix given by $\omega = B'\underline{\omega}'$. Then, since $\sigma_{\mathfrak{c}} = \sigma_{\mathfrak{p}}$ on $H(12f_{\mathfrak{a}}^2)$, by the result of Proposition 5.1 it is sufficient to prove

$$\rho(B)\varphi_{\mathrm{Rob}}(1;\underline{w}_1,\underline{w}_2) = \rho(B')\varphi_{\mathrm{Rob}}(1;\underline{w}_1',\underline{w}_2').$$

Firstly we claim that $\rho(B) = \rho(B')$. We have $\omega = B\underline{\omega} = B'\underline{\omega}'$. Since $\alpha\underline{\omega} = \beta\underline{\omega}'$, this means that $B\beta\underline{\omega} = B'\alpha\underline{\omega}$. Let us write θ_x for the unique integer 2×2 matrix given by the equation $x\underline{\omega} = \theta_x\underline{\omega}$, where $x \in \mathcal{O}$. Then we have $B\theta_\beta = B'\theta_\alpha$, and hence by (6.19), $\rho(B)^{N\alpha}\rho(\theta_\alpha) = \rho(B')^{N\beta}\rho(\theta_\beta)$. Now $\beta = \alpha + 12f_{\mathfrak{a}}^2 x$ for some $x \in \mathcal{O}$, and so $\theta_\alpha \equiv \theta_\beta \pmod{12}$. Combining Lemma 4.2 with the explicit formulas for ε given in [48, §38, (15)] shows that $\rho(B)$ only depends upon the congruence classes of the entries of B modulo 12. Therefore $\rho(\theta_\alpha) = \rho(\theta_\beta)$, and we conclude that $\rho(B)^{N\alpha} = \rho(B')^{N\beta}$ and, since $N\alpha \equiv N\beta \pmod{12}$ and these are coprime to 12, finally that $\rho(B) = \rho(B')$.

It remains to show that

$$\varphi_{\mathrm{Rob}}(1;\underline{w}_1,\underline{w}_2) = \varphi_{\mathrm{Rob}}(1;\underline{w}_1',\underline{w}_2').$$

Since $\varphi_{\mathrm{Rob}}(y;y\underline{w}_1,y\underline{w}_2) = \varphi_{\mathrm{Rob}}(1;\underline{w}_1,\underline{w}_2)$ for any $y \in \mathbb{C}^\times$ (as is clear from the definition (6.12)), this is equivalent to

$$\varphi_{\mathrm{Rob}}(\lambda;\underline{w}_1',\underline{w}_2') = \varphi_{\mathrm{Rob}}(1;\underline{w}_1',\underline{w}_2'). \tag{6.22}$$

We now use [40, (4.1)], which states that, for $u, v \in \mathbb{Q}$ such that $t = u\underline{w}_2' + v\underline{w}_1'$, and $a, b \in \mathbb{Z}$, we have the transformation formula

$$\varphi_{\mathrm{Rob}}(t + a\underline{w}_2' + b\underline{w}_1';\underline{w}_1',\underline{w}_2') = (-1)^{ab+a+b}e^{\pi i(av-bu)}\varphi_{\mathrm{Rob}}(t;\underline{w}_1',\underline{w}_2'). \tag{6.23}$$

Writing $1 = u\underline{w}_2' + v\underline{w}_1'$, and remembering that $\mathbb{Z}\underline{w}_1' + \mathbb{Z}\underline{w}_2' = \mathfrak{p}^{-1}\mathfrak{a}$, we have that $f_{\mathfrak{a}}u \in \mathbb{Z}$ and $f_{\mathfrak{a}}v \in \mathbb{Z}$. Furthermore, $\lambda - 1 \in \mathfrak{p}^{-1}12f_{\mathfrak{a}}^2\mathcal{O}$ and so, writing $\lambda - 1 = a\underline{w}_2' + b\underline{w}_1'$, we have that a and b are integers divisible by $12f_{\mathfrak{a}}$. Therefore setting $t = 1$ in (6.23) shows that (6.22) holds. □

We now proceed to define a system of elliptic units, following [2]. We fix an ideal $\mathfrak{m}$ of $\mathcal{O}$ expressed as in (6.3). Let $\mathfrak{t}$ be any prime ideal coprime to $6\mathfrak{m}$ such that $\delta_{\mathfrak{t}}$ annihilates $\mu_{H(\mathfrak{m})}$. Bley [2, §2] defines

$$\psi(z;L,\mathfrak{t}) = \tilde{F}(z;L;\mathfrak{t}^{-1}L) = \rho(\omega,\underline{\omega})^{-1}\frac{\varphi_{\mathrm{Rob}}(z;\omega)^{N\mathfrak{t}}}{\varphi_{\mathrm{Rob}}(z;\underline{\omega})},$$

where $\tilde{F}$ is the function defined above in (6.11), ω and $\underline{\omega}$ are vectors of positively-oriented bases of L and $\mathfrak{t}^{-1}L$ respectively. We choose $L = \mathfrak{m}_I$ for each $I \subseteq \{1,\ldots,n\}$, and set $\hat{\lambda}_I = \varphi_{\mathrm{Rob}}(1,\omega) \in H(12f_{\mathfrak{a}}^2)$. We set

$$\lambda_I := \varphi_{\mathrm{Rob}}(1;\omega)^{1-\sigma_{\mathfrak{t}}^{-1}N_{\mathfrak{t}}} = \psi(1;\mathfrak{m}_I,\mathfrak{t})^{-\sigma_{\mathfrak{t}}^{-1}}, \tag{6.24}$$

using Corollary 5.2 for the last equality.

We now check the statements of Proposition 1.1 for these elements. The statement that $\lambda_I \in H(\mathfrak{m}_I)$ follows from [2, Prop. 2.2(2)]. That it is an $\mathfrak{m}_I$-unit is [loc. cit., Thm. 2.4] (and this also establishes property 2b of Proposition 1.1). The congruence property with respect to $\mathfrak{t}$ follows from the expression (6.24), and so we have established property 1. Property 2a follows directly from [2, Thm. 2.3].

Finally, we check the L-function evaluation property, which will follow from the Kronecker limit formula. The expression of this formula in [29, (2.4)] is easily seen to imply (via the comparison (6.13) of Oukhaba's notation to Robert's)

$$\zeta'_{\mathfrak{m}_I}(0,\sigma) = \frac{-1}{12w_I f_{\mathfrak{m}_I}} \ln \mid (\hat{\lambda}^{12f_{\mathfrak{m}_I}})^{\sigma} \mid^2,$$

where $\sigma \in \mathrm{Gal}(H(\mathfrak{m}_I)/k)$. Let ∞' be the infinite place of $H(\mathfrak{m}_I) \subseteq \mathbb{C}$ induced by the identity on $\mathbb{C}$. Then we have

$$w_I(\zeta'_{\mathfrak{m}_I}(0,\sigma) - N_{\mathfrak{t}}\zeta'_{\mathfrak{m}_I}(0,\sigma\sigma_{\mathfrak{t}}^{-1})) = \frac{-1}{12f_{\mathfrak{m}_I}} \ln|(\lambda_I^{\sigma})^{12f_{\mathfrak{m}_I}}|_{\infty'},$$

which gives Proposition 1.1 part (3).

Chapter 7

Evidence from special units

We now use the systems of special units defined in Chapter 6 to find evidence for Conjecture 3.5.1. The proof will be combinatorial, based on the distribution relations of Proposition 6.1.1. The local reciprocity symbols appearing in Conjecture 3.5.1 must be related to the global symbols appearing in the Proposition by means of local class field theory. We obtain the statement of Conjecture 3.5.1 multiplied through by an integer b, which may be taken to be w_k if $\mathcal{O}_{k,\infty}$ has class number one or a certain natural sequence of Galois groups is split.

1 Minors of matrices of zero row-sum

This section contains combinatorial preliminaries.

Given an inclusion of nonempty finite sets $J \subseteq I$, we define an *arborescence* on I with root J to be a directed graph on the vertices I which contains no loops and is such that every vertex in J has out-degree 0 and every other vertex has out-degree 1. Therefore an arborescence is a finite union of disjoint directed trees ("rooted branchings"), one each with root j for each element $j \in J$, so that each element of I-J is connected to an element of J. We say that there is a unique arborescence $T_\emptyset$ on the empty set and no arborescences on non-empty sets with empty root.

Fix a finite ordered set B, and for each pair (i, j) of elements of B with $i \neq j$, fix a_{ij} in a given commutative ring with 1. For $I \subseteq B$, let A^I be a square matrix, indexed by I, with (i, j)-th entry a_{ij} for $i \neq j$ and which has zero row-sums. Therefore the (i,i)-th entry is $-\sum_{j \in I\text{-}\{i\}} a_{ij}$. For a directed graph T on a subset of B (whose arcs each begin and end at distinct vertices) we denote by $A(T)$ the product $\prod_{(i,j)} a_{ij}$, where (i, j) runs over all pairs of elements of B such that there is an arc from i to j in T. We define $A(T_\emptyset) = 1$ for an empty product. Note that a function f from a subset of I to a disjoint subset also defines a directed graph by joining i to $f(i)$ for each i in the domain of f. We define $A(f)$ by this graph.

If $J \subseteq I$ then we write A^I_J for the determinant of the submatrix of A^I obtained by deleting the rows and columns indexed by J. If this matrix is 0×0 the determinant is taken to be 1. The following proposition shows how to use graphs to calculate these determinants, and generalises the "matrix tree theorem" of Kirchhoff-Tutte.

Proposition 1.1 (S. Chaiken and D. J. Kleitman). *Let A^I be a square matrix of zero row-sums, indexed by a finite ordered set I. Let $J \subseteq I$. Then*

$$A^I_J = (-1)^{\#I - \#J} \sum_T A(T),$$

where in the sum, T runs through all arborescences on I with root J.

Proof. This is proved in [11]. For illustrative purposes we give a proof here.

In the case $I = \emptyset$ we obtain $A^\emptyset_\emptyset = A(T_\emptyset) = 1$.

Now assume $I \neq \emptyset$. We proceed by induction on $\#I$. If $J = \emptyset$ then both sides of the desired equality are 0. So we may assume that J is nonempty.

The submatrix of A^I obtained by deleting the rows and columns indexed by J is the sum of $A^{I\text{-}J}$ and the diagonal matrix with (i,i)-th entry $-\sum_{j \in J} a_{ij}$ for I in I-J. Therefore its determinant is

$$A^I_J = \sum_{H \subseteq I\text{-}J} \Big[\prod_{i \in H} \big(- \sum_{j \in J} a_{ij} \big) A^{I\text{-}J}_H \Big]$$

Now, since $\#(I\text{-}J) < \#I$, the induction hypothesis implies that

$$A^{I\text{-}J}_H = (-1)^{\#I - \#J - \#H} \sum_{T_H} A(T_H),$$

where T_H runs through all arborescences on I-J with root H. Also,

$$\prod_{i \in H} \big(- \sum_{j \in J} a_{ij} \big) = (-1)^{\#H} \sum_{f_H : H \to J} A(f_H),$$

where f_H runs through all functions from H to J. So

$$A^I_J = (-1)^{\#I - \#J} \sum_{H \subseteq I\text{-}J} \sum_{T_H} \sum_{f_H} A(T_H) A(f_H).$$

The product $A(T_H)A(f_H)$ is $A(T)$ where T is the arborescence on I with root J obtained from T_H by adjoining the arcs from i to $f_H(i)$ for $i \in H$. On the other hand, given any tree T on I with root J, the set of arcs ending in an element of J defines a unique subset $H \subseteq I$, function $f_H : H \longrightarrow J$ and arborescence T_H on I-J such that T is the union of T_H and f. Therefore the desired expression for A^I_J is obtained. ☐

Example 1.2. The minor $A^{\{1,2,3,4\}}_{\{3,4\}}$ is the determinant of the matrix

$$\begin{pmatrix} -a_{12} - a_{13} - a_{14} & a_{12} \\ a_{21} & -a_{21} - a_{23} - a_{24} \end{pmatrix}$$

Proposition 1.1 shows that the determinant is $a_{13}a_{21} + a_{12}a_{23} + a_{13}a_{23} + a_{13}a_{24} + a_{14}a_{23} + a_{14}a_{24} + a_{12}a_{24} + a_{14}a_{21}$, corresponding to the arborescences

$$\begin{array}{cc} 2 & \\ \downarrow & \\ 1 & \\ \downarrow & \\ 3 & 4 \end{array} \quad \begin{array}{cc} 1 & \\ \downarrow & \\ 2 & \\ \downarrow & \\ 3 & 4 \end{array} \quad \begin{array}{cc} & \\ & \\ 1 & 2 \\ \downarrow\swarrow & \\ 3 & 4 \end{array} \quad \begin{array}{cc} & \\ & \\ 1 & 2 \\ \downarrow & \downarrow \\ 3 & 4 \end{array} \quad \begin{array}{cc} & \\ & \\ 2 & 1 \\ \downarrow & \downarrow \\ 3 & 4 \end{array} \quad \begin{array}{cc} & \\ & \\ 1 & 2 \\ & \searrow\downarrow \\ 3 & 4 \end{array} \quad \begin{array}{cc} & 1 \\ & \downarrow \\ & 2 \\ & \downarrow \\ 3 & 4 \end{array} \quad \begin{array}{cc} & 2 \\ & \downarrow \\ & 1 \\ & \downarrow \\ 3 & 4 \end{array}$$

We will need to use the following identity which, although it was known in the 18th century, seems to be more often rediscovered than familiar [16]. As in the binomial theorem, we interpret $0^0 = 1$.

Proposition 1.3 (Euler's formula). *Let n be a positive integer and $0 \leq t < n$. Then*

$$\sum_{r=0}^{n} (-1)^r \binom{n}{r} r^t = 0.$$

Proof. A nice proof is given in [14]. □

Corollary 1.4. *Let n be a positive integer and f be a polynomial of degree less than n. Then*

$$\sum_{r=0}^{n} (-1)^r \binom{n}{r} f(r) = 0.$$

We combine the results of this section to obtain an identity involving minors of matrices of zero row sum. Fix a finite ordered set B and fix a_{ij} in a fixed commutative ring with 1 for $i \neq j$ elements of B. For $J \subseteq I \subseteq B$ define A^I, A^I_J as above, and set $I' = B\text{-}I$.

Proposition 1.5. *Let $J \subseteq B$ and let F be a polynomial of degree less than $\#J$. Then*

$$\sum_{I \subseteq B} (-1)^{\#(I' \cap J)} F(\#I) A^I_{I \cap J} \prod_{i \in I'\text{-}J} \big(\sum_{j \in I} a_{ij} \big) = 0$$

Proof. By Proposition 1.1 we have

$$A^I_{I \cap J} = (-1)^{\#(I\text{-}J)} \sum_{T_I} A(T_I),$$

where T_I runs through all arborescences on I with root $I \cap J$. Also,

$$\prod_{i \in I' - J} \big(\sum_{j \in I} a_{ij} \big) = \sum_{f_I : I'\text{-}J \to I} A(f_I)$$

Combining these shows that the left-hand side of the desired equality is equal to

$$\sum_{I \subseteq B} (-1)^{\#I - \#J} F(\#I) \sum_{T_I, f_I} A(T_I) A(f_I).$$

Now $A(T_I)A(f_I) = A(T)$ where T is the arborescence on B with root J obtained from T_I by adding the "leaves" f_I. On the other hand, we can express any T as such a union for some I, T_I, f_I by choosing a subset V of the set $V^0(T)$ of vertices of T of in-degree 0 and then setting $I = B - V$, T_I to be T with the vertices V and adjoining arcs removed, and f_I these removed edges. This gives a bijection $(I, T_I, f_I) \leftrightarrow (T, V)$ so that the sum becomes

$$\sum_T A(T) \sum_{V \subseteq V^0(T)} (-1)^{\#B-\#J-\#V} F(\#B - \#V).$$

Let n denote $\#V^0(T)$. There are $\binom{n}{r}$ sets V of cardinality r for $r = 0, 1, \ldots, n$. We note that $\#J \le n$ since each element of J is the root of a subtree of T. So the coefficient of $A(T)$ in the sum is $(-1)^{\#B-\#J} \sum_{r=0}^{n} (-1)^r \binom{n}{r} F(\#B - r)$. Since $F(\#B - r)$ is a polynomial of degree less than n in r, Corollary 1.4 shows that the coefficient of $A(T)$ is zero. $\square$

2 First congruence

Let k be a global field and ∞ a place of k such that all other places are finite. Let $\mathcal{O} := \mathcal{O}_{k,\infty}$ be the ring of ∞-integers. Fix an ideal $\mathfrak{m} \ne 1, 0$ of $\mathcal{O}$ and set $S = \mathrm{Supp}(\mathfrak{m}) \cup \{\infty\}$.

Let $\mathfrak{t}$ be a prime ideal coprime to $3\mathfrak{m}w_{H(\mathfrak{m})}$, and write $\mathfrak{m}$ in the form (6.3). Abbreviate $B = \{1, \ldots, n\}$. Then we may fix a system $\lambda_I \in H(\mathfrak{m}_I)$ as in Proposition 6.1.1 for each $I \subseteq B$, and let $\alpha_i = N_{H(\mathfrak{m}_i)/H} \lambda_i^{w_k/w_i} \in H$, so that $\alpha_i \mathcal{O}_H = \mathfrak{p}_i^{1-N\mathfrak{t}} \mathcal{O}_H$. Set $\lambda = \lambda_B$.

For an ideal $\mathfrak{a}$ of $\mathcal{O}$, we set $\Gamma_\mathfrak{a} := (\mathcal{O}/\mathfrak{a})^\times$ and $G_\mathfrak{a} = A_{k,\mathfrak{a}\infty,\mathfrak{a}}$, which we identify with $\mathrm{Gal}(H(\mathfrak{a})/k)$ by global class field theory. If $x \in k^\times$ is coprime to $\mathfrak{a}$, we denote by $[x]_\mathfrak{a}$ the class of x modulo $\mathfrak{a}$ considered as an element of $\Gamma_\mathfrak{a}$. We write $[\mu_k]_\mathfrak{a}$ for the image in $\Gamma_\mathfrak{a}$ of the roots of unity μ_k. If $\mathfrak{a} = \mathfrak{m}_I$ for some set I, we abbreviate $\Gamma_I := \Gamma_{\mathfrak{m}_I}, G_I := G_{\mathfrak{m}_I}$ and $[x]_I = [x]_{\mathfrak{m}_I}$. The group G_1 is the class group of the ring $\mathcal{O}$. The group $\Gamma_\mathfrak{m}$ is a direct product:

$$\Gamma_\mathfrak{m} = \Gamma_1 \times \cdots \times \Gamma_n.$$

The sequence (6.1) gives an exact sequence

$$0 \longrightarrow [\mu_k]_\mathfrak{m} \longrightarrow \Gamma_\mathfrak{m} \longrightarrow G_\mathfrak{m} \longrightarrow G_1 \longrightarrow 0 \tag{7.1}$$

Let $s : G_1 \to G_\mathfrak{m}$ be a section to the projection $G_\mathfrak{m} \longrightarrow G_1$, and b be an integer such that $w_k \mid b$ and $s(x)^b s(y)^b = s(xy)^b$ for all x and y in $G_\mathfrak{t}$. Choose s such that b is minimal; the minimum possible b depends upon the structure of the sequence (7.1). If $\#\Gamma_\mathfrak{m}$ and $\#G_1 = h_{k,\infty}$ have greatest common divisor which divides w_k (which happens, for example, if $\mathcal{O}$ has class number 1, i.e. G_1 is trivial), then we may take $b = w_k$. We write $x \sim y$ to denote that two elements x and y of a group have equal b-th powers, so that $s(x)s(y) \sim s(xy)$ for all $x, y \in G_1$.

For any abelian group G, we use $G^{\times b}$ to denote the subgroup of b-th powers. The function s and the sequence (7.1) define a surjection $\Gamma_{\mathfrak{m}} \times G_1 \to G_{\mathfrak{m}}$, and the composition of this map with raising to the b-th power is a homomorphism.

If $I \subseteq B$, we have the commutative diagram

$$\begin{array}{ccc} \Gamma_{\mathfrak{m}} \times G_1 & \longrightarrow & G_{\mathfrak{m}} \\ \downarrow & & \downarrow \\ \Gamma_I \times G_1 & \longrightarrow & G_I. \end{array}$$

The natural inclusion $\Gamma_I \to \Gamma_{\mathfrak{m}}$ and the section s induce a section $t_I : G_I \to G_{\mathfrak{m}}$ such that t_I^b is multiplicative.

Now choose a group homomorphism $\phi^1 : U_{H(\mathfrak{m}),S,\mathfrak{t}} \to \mathbb{Z}$. For any quotient group $G_{\mathfrak{m}}/G'$ of $G_{\mathfrak{m}}$, let $\phi^{G_{\mathfrak{m}}/G'} \in \mathrm{Hom}_{\mathbb{Z}[G_{\mathfrak{m}}/G']}(U_{H(\mathfrak{m})^{G'},S,\mathfrak{t}}, \mathbb{Z}[G_{\mathfrak{m}}/G'])$ be the map corresponding to the restriction of ϕ^1 by Lemma 2.6.5. Let $\phi = \phi^{G_{\mathfrak{m}}}$.

Lemma 2.1. *Let Γ act on $H(\mathfrak{m})$ via (7.1). Let $I \subseteq C \subseteq \{1, \ldots, n\}$. Using the above notation, we calculate $N_{\Gamma_{C\text{-}I}}\lambda_C$ as follows.*

1. *If I is not empty, then*

$$N_{\Gamma_{C\text{-}I}}\lambda_C = \lambda_I^{\prod_{i \in C\text{-}I}(1-\sigma_{\mathfrak{p}_i}^{-1})}.$$

2. *For any $t \in C$,*

$$N_{\Gamma_C}\lambda_C = \alpha_t^{\prod_{i \neq t}(1-\sigma_{\mathfrak{p}_i}^{-1})}.$$

Proof. First assume $I \neq \emptyset$. Taking $\mathfrak{a} = \mathfrak{m}_I$ and $\mathfrak{b} = \mathfrak{m}_{C\text{-}I}$ in diagram (6.2) shows that the map $\Gamma_{\mathfrak{m}_i} \to \mathrm{Gal}(H(\mathfrak{m}_{I \cup \{i\}})/H(\mathfrak{m}_I))$ is surjective with kernel of size $w_{\mathfrak{m}_I}/w_{\mathfrak{m}_C}$. The assertion now follows from repeatedly applying Proposition 6.1.1 (2a).

Next we show (2). Choose $t \in C$. The assertion follows by applying Proposition 1.1 part (2a) for all the $i \neq t$ and then using part (2b). □

Let $i \in B$ and $i \notin I \subseteq B$. Set $\sigma_{i,I} = (\mathfrak{p}_i, H(\mathfrak{m}_I)/k)$. In $G_{\mathfrak{m}}$, we have

$$s(\mathfrak{p}_i)^{-b} t_I(\sigma_{i,I})^b = s(\mathfrak{p}_i)^{-b\#I} \prod_{j \in I} t_j(\sigma_{i,j})^b. \tag{7.2}$$

Recalling the notation of Proposition 1.5, let $a_{ij} = t_{ij}(\sigma_{i,j}^{-1}) - 1 \in \mathbb{Z}[G]$. Then there are defined certain elements $A_J^I \in \mathbb{Z}[G]$ for $J \subseteq I \subseteq B$.

For $I \subseteq B$ and an arbitrary choice of $t \in I$, we write

$$\Omega_I = \phi^1(N_{G_1}\alpha_t) \prod_{i \in I - \{t\}} (1 - s(\mathfrak{p}_i)^{-1}) \in I_{G_1}^{\#I-1}.$$

Note that $N_{G_1}\alpha_{\mathfrak{t}}$ is of the form $x^{1-N_{\mathfrak{t}}}$ for some $x \in U_{k,S}$ and that $w_k \mid (1 - N_{\mathfrak{t}})$, so $N_{G_1}\alpha_{\mathfrak{t}}$ is the w_k-th power of an element of y of $U_{k,S}$. We have that y is congruent to a root of unity ζ modulo $\mathfrak{t}$, so $\zeta^{-1}y$ is a w_k-th root of $N_{G_1}\alpha_{\mathfrak{t}}$ and lies in $U_{k,S,\mathfrak{t}}$. This implies that $w_k \mid \phi^1(N_{G_1}\alpha_{\mathfrak{t}})$ for all ϕ, and hence $w_k \mid \Omega_I$. We have $\frac{b}{w_k}\phi^{G_\emptyset}(N_{\Gamma_I}\lambda_I) \equiv \frac{b}{w_k}\Omega_I \pmod{I_{G_\emptyset}^{\#I}}$, independently of the choice of t, by Lemma 2.1(2).

Proposition 2.2. *For all ϕ^1 we have*

$$\phi^G(\lambda^{b/w_{\mathfrak{m}}}) \equiv \frac{b}{w_k} \sum_{\emptyset \neq J \subseteq B} (1-n)^{\#J-1}\Omega_J A_J^B \pmod{I_G^n}, \tag{7.3}$$

where $0^0 := 1$.

Proof. We prove this by induction on $n = \#B$. Suppose first $n = 1$. Then

$$\phi(\lambda_i^{w_k/w_i}) \equiv \phi^1(N_{G_1}N_{\Gamma_1}\lambda) \equiv \phi^1(N_{G_1}\alpha_1) \pmod{I_G}.$$

Hence the statement is true with $b = w_k$ in this case.

Now assume that $n > 1$ and the assertion has been proved for all $\mathfrak{m}_I$, $\emptyset \neq I \neq B$. Consider the equality in $\mathbb{Z}[G]$:

$$\begin{aligned}
&\sum_{\gamma\in\Gamma_{\mathfrak{m}}}\sum_{v\in G_1}\phi^1(\gamma^{-1}s(v)^{-1}\lambda)\Big(\prod_{i\in B}([\gamma]_{\mathfrak{m}_i}^b - 1)\Big)s(v)^b \\
= &\sum_{\gamma\in\Gamma_{\mathfrak{m}}}\sum_{v\in G_1}\phi^1(\gamma^{-1}s(v)^{-1}\lambda)\sum_{I\subseteq B}(-1)^{n-\#I}\prod_{i\in I}[\gamma]_{\mathfrak{m}_i}^b s(v)^b \\
= &\sum_{I\subseteq B}(-1)^{n-\#I}\sum_{\gamma\in\Gamma_I, v\in G_1}\phi^1(\gamma^{-1}s(v)^{-1}N_{\Gamma_{C\text{-}I}}\lambda)\gamma^b s(v)^b \\
= &\sum_{I\subseteq B}(-1)^{n-\#I}t_I^b(\phi^{G_I}(N_{\Gamma_{I'}}\lambda^{b/w_I})).
\end{aligned} \tag{7.4}$$

Now we apply the results of Lemma 2.1. Reducing (7.4) modulo I_G^n gives

$$\begin{aligned}
0 \equiv &\sum_{I\neq\emptyset}(-1)^{n-\#I}t_I^b(\phi^{G_I}(\lambda_I^{b/w_I}))\prod_{i\in C\text{-}I}(1-t_I(\sigma_{i,I}^{-1})^b) + \\
&(-1)^{\#C}\sum_{v\in G_1}t_\emptyset^b(\phi^{G_1}(\alpha_t)\prod_{i\neq t})(1-s(\mathfrak{p}_i)^{-b}) \pmod{I_G^n}.
\end{aligned}$$

We now apply the induction hypothesis and Corollary 2.6.3 to obtain

$$\begin{aligned}
0 \equiv\ &\phi(\lambda^{b/w_{\mathfrak{m}}}) \\
+\ &\frac{b}{w_k}\sum_{I\neq\emptyset}(-1)^{n-\#I}\Big[\sum_{\emptyset\neq J_1\subseteq I}(1-\#I)^{\#J_1-1}\Omega_{J_1}A_{J_1}^I\Big]\prod_{i\in I'}(1-t_I(\sigma_{i,I}^{-1})) \\
+\ &\frac{b}{w_k}(-1)^n\Omega_B \pmod{I_G^n}
\end{aligned}$$

Equation (7.2) shows that $b(1-t_I(\sigma_{i,I}^{-1}))$ can be replaced by

$$\begin{aligned} & b\prod_{i\in I'}\Big[\sum_{j\in I} a_{ij} + b(\#I-1)(1-s(\mathfrak{p}_i^{-1}))\Big] \\ = \;& b\sum_{J_2\subseteq I'}\Big[\prod_{i\in I'\text{-}J_2}\Big(\sum_{j\in I} a_{ij}\Big)(\#I-1)^{\#J_2}\prod_{i\in J_2}(1-s(\mathfrak{p}_i^{-1}))\Big]. \end{aligned}$$

Therefore we obtain

$$\begin{aligned} 0 \;\equiv\; & \phi(\lambda^{b/w_{\mathfrak{m}}}) \\ + \; & \frac{b}{w_k}\sum_{I\subsetneq B}\Big[\sum_{\substack{\emptyset\neq J_1\subseteq I,\\ J_2\subseteq I'}}(-1)^{\#J_2}(1-\#I)^{\#J_1+\#J_2-1}\Omega_{J_1\cup J_2}A^I_{J_1}\prod_{i\in C\text{-}I\text{-}J_2}\big(\sum_{h\in I}a_{ih}\big)\Big]. \end{aligned}$$

If we rearrange the sum over $J=J_1\cup J_2$, note that $A^I_\emptyset = 0$ for all I and use $\Omega_{J_1}\prod_{i\in J_2}(1-s(\mathfrak{p}_i^{-1})) = \Omega_J$, we get

$$\begin{aligned} 0 \;\equiv\; & \phi(\lambda^{b/w_{\mathfrak{m}}}) \\ + \; & \frac{b}{w_k}\sum_{\emptyset\neq J\subseteq B}\Omega_J\Big[\sum_{I\subsetneq B}(-1)^{\#(I'\cap J)}(1-\#I)^{\#J-1}A^I_{I\cap J}\prod_{i\in I'\text{-}J}\big(\sum_{h\in I}a_{ih}\big)\Big]. \end{aligned}$$

Finally, we apply Proposition 1.5 for $F(X)=(1-X)^{\#J-1}$. We obtain

$$\phi(\lambda^{b/w_{\mathfrak{m}}}) \equiv \frac{b}{w_k}\sum_{\emptyset\neq J\subseteq B}(1-n)^{\#J-1}\Omega_J A^B_J \pmod{I_G^n},$$

as required.

Now the case $C=B$ proves the proposition. ☐

We now give an alternative expression for the right-hand side of (7.3). First we need some linear algebra.

Lemma 2.3. *Suppose A is a square $n\times n$ matrix and $(v_i)_i, (\Omega_i)_i$ are vectors of length n. Suppose $\Omega_i v_j = \Omega_j v_i$ for all $i\neq j$. Then the determinant of the $n\times n$ matrix with (i,j)-th entry $a_{ij}+v_i$ for $j\neq 1$ and Ω_i for $j=1$ is the same as the determinant of the matrix obtained from A by replacing the first column with $(\Omega_i)_i$.*

Proof. Expanding by the first column, the coefficients of $\Omega_i v_j$ and $\Omega_j v_i$ are equal and opposite. ☐

If A is a square $n\times n$ matrix and $i,j\in B$, let A_{ij} denote the determinant of the matrix obtained from A by deleting row i and column j.

Lemma 2.4. *Let A be a square $n \times n$ matrix and A' the sum of A and the diagonal matrix with (j,j)-th entry w_j. Then:*

$$A'_{i1} = \begin{cases} (-1)^i \sum_{i \in I \subseteq B} \big(\prod_{j \in I\text{-}\{i\}} w_j \big) A_I & \text{if } i = 1, \\ (-1)^i \sum_{i \in I \subseteq B\text{-}\{1\}} \big(\prod_{j \in I\text{-}\{i\}} w_j \big) \sum_{\sigma \in S_{B\text{-}I}} \operatorname{sign}(\sigma) \prod_{j \in B\text{-}I} a_{j,(1\ i)\sigma(j)} & \text{if } i \neq 1, \end{cases}$$

where $(1\ i) \in S_n$ is the permutation swapping 1 and i.

Proof. Denote the (j,k)-th entry of A' by $a'_{jk} = a_{jk} + w_j \delta_{jk}$. Then

$$\begin{aligned} A'_{i1} &= \sum_{\sigma \in S_{B\text{-}\{i\}}} \operatorname{sign}(\sigma) \prod_{j \in B\text{-}\{i\}} a'_{j,(1\ 2\ \cdots\ i-1\ i)\sigma(j)} \\ &= (-1)^i \sum_{\sigma \in S_{B\text{-}\{i\}}} \operatorname{sign}(\sigma) \prod_{j \in B\text{-}\{i\}} a'_{j,(1\ i)\sigma(j)}. \end{aligned}$$

Now

$$\prod_{j \in B\text{-}i} a'_{j,(1\ i)\sigma(j)} = \sum_{J \subseteq B\text{-}\{i\}} \big(\prod_{j \in J} w_j \delta_{j,(1\ i)\sigma(j)} \big) \big(\prod_{j \in B\text{-}\{i\}\text{-}J} a_{j,(1\ i)\sigma(j)} \big).$$

The term for J is nonzero only if $j = (1\ i)\sigma(j)$ for $j \in J$. If $i \neq 1$ then this is impossible if $1 \in J$. So assuming $1 \notin J$ if $i \neq 1$, the condition implies that σ is any permutation of B-J-$\{i\}$. Therefore

$$A'_{i1} = (-1)^i \sum_{J \subseteq B\text{-}\{1,i\}} \big(\prod_{j \in J\text{-}\{i\}} w_j \big) \sum_{\sigma \in S_{B\text{-}J\text{-}\{i\}}} \operatorname{sign}(\sigma) \prod_{j \in B\text{-}J\text{-}\{i\}} a_{j,(1\ i)\sigma(j)}.$$

Now set $I = J \cup \{i\}$ to complete the proof. □

We now define a matrix to which to apply this theory. We set $a_{ih} = t_h(\sigma_{i,h}^{-1}) - 1 \in \mathbb{Z}[G]$ and $\upsilon_i = s(\mathfrak{p}_i)^{-1} - 1$ for $i, h \in B$. Set now

$$m_{ih} = a_{ih} + (n-1)\upsilon_i \delta_{ih} - \upsilon_i, \tag{7.5}$$

defining a matrix M. We consider the expression

$$\sum_{i=1}^{n} (-1)^{i+1} \Omega_i M_{i1}.$$

Proposition 2.5.

$$\sum_{i=1}^{n} (-1)^i \Omega_i M_{i1} = \sum_{\emptyset \neq J \subseteq B} (1-n)^{\#J-1} \Omega_J A_J^B.$$

Proof. Noting that $\Omega_i v_j = \Omega_j v_i = -\Omega_{\{i,j\}}$ for $i \neq j$ by Lemma 2.1(2), we see that Lemma 2.3 shows that M_{i1} can be replaced by A'_{i1} in the left-hand side of the equation, where A' is the $n \times n$ matrix with (i,j)-th entry $a'_{ih} = a_{ih} + (n-1)v_i\delta_{ih}$.

Consider first those J containing 1. In the left-hand-side, such Ω_J are produced only by the term for $i = 1$. Now applying Lemma 2.4 for $I = J$ gives the correct coefficients for these Ω_J.

Now suppose $1 \notin J$. We have a contribution to the coefficient of Ω_J from terms on the left-hand side corresponding to i for each $i \in J$. Applying Lemma 2.4 with $I = J$, the coefficient of Ω_J on the left-hand side is

$$\begin{aligned} & -(1-n)^{\#J-1} \sum_{i \in J} \sum_{\sigma \in S_{B\text{-}J}} \operatorname{sign}(\sigma) \prod_{j \in B\text{-}J} a_{j,(1\ i)\sigma(j)} \\ = \quad & (1-n)^{\#J-1} \sum_{\sigma \in S_{B\text{-}J}} \operatorname{sign}(\sigma) \prod_{j \in B\text{-}J\text{-}\{\sigma^{-1}(1)\}} a_{j,\sigma(j)} \big(-\sum_{i \in J} a_{\sigma^{-1}(1),i} \big). \end{aligned} \tag{7.6}$$

Now we use the fact that A has zero row-sums. This gives $-\sum_{i \in J} a_{\sigma^{-1}(1),i} = \sum_{i \in B\text{-}J} a_{\sigma^{-1}(1),i}$. Substituting this into the expression (7.6) gives

$$\begin{aligned} & (1-n)^{\#J-1} \sum_{\sigma \in S_{B\text{-}J}} \operatorname{sign}(\sigma) \prod_{j \in B\text{-}J} a_{j,\sigma(j)} \\ + \quad & \sum_{i \in B\text{-}J\text{-}\{1\}} (1-n)^{\#J-1} \sum_{\sigma \in S_{B\text{-}J}} \operatorname{sign}(\sigma) \big(\prod_{j \in B\text{-}J\text{-}\{\sigma^{-1}(1)\}} a_{j,\sigma(j)} \big) a_{\sigma^{-1}(1),i}. \end{aligned}$$

In the second line, indices i, σ and $\sigma^{-1}(i), (1\ i)\sigma$ match up with opposite signs. Therefore the second term vanishes and the first term, which is $(1-n)^{\#J-1}A_J$, remains. □

Corollary 2.6. *For all* ϕ^1 *we have*

$$\phi(\lambda^{b/w_\mathfrak{m}}) \equiv \frac{b}{w_k} \sum_{i=1}^{n} (-1)^i \phi^1(N_{G_1}\alpha_i) M_{i1}.$$

Proof. This combines Propositions 2.2 and 2.5. □

3 Reciprocity symbol calculations

We continue with the hypotheses and notation of §2.

Lemma 3.1. *If* $\sigma \in \operatorname{Gal}(H(\mathfrak{m})/k)$ *restricts to the identity on* $\operatorname{Gal}(H(\mathfrak{m}_i)/k)$ *for all* i*, then* $\sigma \sim \mathrm{id}$.

Proof. We may represent σ by a principal ideal $(a) \in A_{k,\mathfrak{m}\infty,\mathfrak{m}}$. The element $a \in \mathcal{O}$ is then congruent to a root of unity modulo each $\mathfrak{m}_i$. □

Proposition 3.2. *The decomposition group of any prime of* $H(\mathfrak{m})$ *above* $\mathfrak{p}_i$ *is an extension of the subgroup of* $\mathrm{Gal}(H(\mathfrak{m}_{B\text{-}\{i\}})/k)$ *generated by the Frobenius of* $\mathfrak{p}_i$ *on* $H(\mathfrak{m}_{B\text{-}\{i\}})$ *by* $\mathrm{Gal}(H(\mathfrak{m})/H(\mathfrak{m}_{B\text{-}\{i\}}))$. *The inertia group of the same prime is* $\mathrm{Gal}(H(\mathfrak{m})/H(\mathfrak{m}_{B\text{-}\{i\}}))$.

Proof. Choose a prime of $H(\mathfrak{m})$ above $\mathfrak{p}_i$, and write D for the its decomposition group in G. The groups $\mathrm{Gal}(H(\mathfrak{m})/k)$ and $\mathrm{Gal}(H(\mathfrak{m}_{B\text{-}\{i\}})/k)$ are connected by the exact sequence on the right-hand side of (6.2) for $\mathfrak{a} = \mathfrak{m}_{B\text{-}\{i\}}$ and $\mathfrak{b} = \mathfrak{m}_i$.

The projection of D to $\mathrm{Gal}(H(\mathfrak{m}_{B\text{-}\{i\}})/k)$ is the decomposition group of a prime above $\mathfrak{p}_i$ in the unramified extension $H(\mathfrak{m}_{B\text{-}\{i\}})/k$, and so is generated by the Frobenius $\sigma_{\mathfrak{p}_i}$ on this extension.

Let us now calculate the ramification number of $\mathfrak{p}_i$ in the extension $H(\mathfrak{m})/k$. Useful formulas for this can be found in [10, Thm. 3.5.3]. These show that the ramification degree of any prime of $H(\mathfrak{m})$ over $\mathfrak{p}_i$ is $\#(\mathcal{I}_{k,S} \cap \mathcal{P}_{k,S\text{-}\{\mathfrak{p}_i\},\mathfrak{m}_{B\text{-}\{i\}}})/\mathcal{P}_{k,S}$, which is the size of $\mathrm{Gal}(H(\mathfrak{m})/H(\mathfrak{m}_{B\text{-}\{i\}}))$. On the other hand, the ramification number for the subextension $H(\mathfrak{m}_{B\text{-}\{i\}})/k$ is 1. This completes the proof. □

For each i, choose a prime $\mathfrak{q}_i$ coprime to $\mathfrak{m}$ such that

$$(\mathfrak{q}_i, H(\mathfrak{m})/k) = s(\mathfrak{p}_i), \tag{7.7}$$

and hence there is $\epsilon_i \in k^\times$ such that

$$\mathfrak{p}_i = \mathfrak{q}_i(\epsilon_i). \tag{7.8}$$

We abbreviate the local symbol $(-, H(\mathfrak{m})_{\mathfrak{P}_i}/k_{\mathfrak{p}_i})$, where $\mathfrak{P}_i$ is a prime of $H(\mathfrak{m})$ above $\mathfrak{p}_i$, to $(-, \mathfrak{p}_i)$.

Proposition 3.3. *Let* $i \in B$. *Let* $x \in k^\times$ *be coprime to* $\mathfrak{m}$, *i.e.* $v_{\mathfrak{p}_j}(x) = 0$ *for all* $j \in B$. *Then*

$$(x, \mathfrak{p}_i) \sim [x^{-1}]_{\mathfrak{m}_i}.$$

Proof. By the product rule of global class field theory, we have

$$1 = (x, H(\mathfrak{m})/k) = ((x), H(\mathfrak{m})/k) \prod_{i=1}^{n} (x, \mathfrak{p}_i) = [x]_{\mathfrak{m}} \prod_{i=1}^{n} (x, \mathfrak{p}_i).$$

We have that $(x, \mathfrak{p}_i)$ is in the inertia group of $\mathfrak{p}_i$ because x is a unit at $\mathfrak{p}_i$. Projecting to $\mathrm{Gal}(H(\mathfrak{m}_i)/k)$ and noting that the inertia groups of the other primes (Proposition 3.2) become thereby trivial, we obtain $(x, \mathfrak{p}_i) \sim [x^{-1}]_{\mathfrak{m}_i}$ (using Lemma 3.1) as required. □

Proposition 3.4. *The norm residue symbols of* ϵ_i *in the completions of* $H(\mathfrak{m})/k$ *at finite primes satisfy:*

$$(\epsilon_i, \mathfrak{p}_i) \sim (\mathfrak{q}_i, H(\mathfrak{m})/k)[\epsilon_i]_{\mathfrak{m}_{B\text{-}\{i\}}}$$

and

$$(\epsilon_i, \mathfrak{p}_j) \sim [\epsilon_i^{-1}]_{\mathfrak{m}_j}$$

for $j \neq i$.

Proof. The product formula for $H(\mathfrak{m}_{B\text{-}\{i\}})/k$ shows that

$$[\epsilon_i^{-1}]_{\mathfrak{m}_{B\text{-}\{i\}}} \sim \prod_{j\neq i}(\epsilon_i, \mathfrak{p}_j). \tag{7.9}$$

Projecting this to $\mathrm{Gal}(H(\mathfrak{m}_j)/k)$ gives the second assertion.

Now the product formula for $H(\mathfrak{m})/k$ gives

$$(\mathfrak{q}_i^{-1}, H(\mathfrak{m})/k)\prod_{j=1}^{n}(\epsilon_i, \mathfrak{p}_j) = 1.$$

Using this and (7.9) gives the first assertion. □

We are now ready to calculate the local symbols for arbitrary $x \in k^\times$.

Proposition 3.5. *If $x \in k^\times$, we have*

$$(x, \mathfrak{p}_i) \sim \Big((\mathfrak{q}_i, H(\mathfrak{m})/k)[\epsilon_i]_{\mathfrak{m}_{B\text{-}\{i\}}}\Big)^{v_{\mathfrak{p}_i}(x)}[x^{-1}\epsilon_i^{v_{\mathfrak{p}_i}(x)}]_i.$$

Proof. Let $\tilde{x} = \prod_{i=1}^n \epsilon_i^{v_{\mathfrak{p}_i}(x)}$. Proposition 3.3 shows that $(x\tilde{x}^{-1}, \mathfrak{p}_i) \sim [\tilde{x}x^{-1}]_i$. On the other hand, Proposition 3.4 calculates $(\tilde{x}, \mathfrak{p}_i)$, and the product is the stated formula for $(x, \mathfrak{p}_i)$. □

We now connect this to the elements σ_{ij}.

Proposition 3.6. *We have $\sigma_{ij} \sim s(\mathfrak{p}_i)[\epsilon_i]_j$ for $i \neq j$.*

Proof. Since the elements to compare lie in the subgroup G_I, it is sufficient by Lemma 3.1 to compare the corresponding automorphisms of $H(\mathfrak{m}_I)/k$. The result then follows from (7.8) and (7.7). □

For any $x \in U_{k,S}$, we define $\tilde{x} := \prod_{j=1}^n \epsilon_j^{v_{\mathfrak{p}_j}(x)}$.

Lemma 3.7. *For $x \in U_{k,S}$, we have*

$$[x^{-1}\tilde{x}]_{\mathfrak{m}} \sim 1.$$

Proof. The relation $(x) = \prod_{j=1}^n \mathfrak{p}_j^{v_{\mathfrak{p}_j}(x)}$ implies that $(x)^b = \prod_{j=1}^n \mathfrak{q}_j^{bv_{\mathfrak{p}_j}(x)}(\tilde{x})^b$, and by multiplicativity of s^b we have that the product of $\mathfrak{q}_j$ lies in $\mathcal{P}_{k,S,\mathfrak{m}}$. □

Corollary 3.8. *For any $I \subseteq B$,*

$$[x^{-1}\tilde{x}]_{\mathfrak{m}_I} \sim 1.$$

We obtain:

Proposition 3.9. *Let $x \in U_{k,S}$. Then*

$$(x, H(\mathfrak{m})_{\mathfrak{P}_j}/k_{\mathfrak{p}_j}) \sim \left(s(\mathfrak{p}_j)^{-(n-2)} \prod_{i \neq j} \sigma_{ji} \right)^{v_{\mathfrak{p}_j}(x)} \prod_{i \neq j} (\sigma_{ij} s(\mathfrak{p}_i)^{-1})^{v_{\mathfrak{p}_i}(x)}.$$

Proof. Using Lemma 3.7 to replace x with $\tilde{x}$ when applying Proposition 3.5, we obtain

$$(x, H(\mathfrak{m})_{\mathfrak{P}_j}/k_{\mathfrak{p}_j}) \sim \left(s(\mathfrak{p}_j)[\epsilon_j]_{\mathfrak{m}_{B\text{-}\{j\}}} \right)^{v_{\mathfrak{p}_j}(x)} [\tilde{x}^{-1} \epsilon_j^{v_{\mathfrak{p}_j}(x)}]_{\mathfrak{m}_j}.$$

Now $[\epsilon_j]_{\mathfrak{m}_{B\text{-}\{j\}}} = \prod_{i \neq j} [\epsilon_j]_{\mathfrak{m}_i} = \prod_{i \neq j} (s(\mathfrak{p}_j)^{-1} \sigma_{ji})$ by Proposition 3.6, and also $[\tilde{x}^{-1} \epsilon_j^{v_{\mathfrak{p}_j}(x)}]_{\mathfrak{m}_j} = \prod_{i \neq j} [\epsilon_i^{-v_{\mathfrak{p}_i}(x)}]_{\mathfrak{m}_j} = \prod_{i \neq j} (\sigma_{ij}^{-1} s(\mathfrak{p}_i))^{v_{\mathfrak{p}_i}(x)}$, by the same result. □

4 Relation to Burns's conjecture

We continue with all the notation of §2 and §3. The rank of the units of $\mathcal{O}$ is zero. Therefore an element $x \in k^\times$ is determined up to a root of unity in $\mathcal{O}$ by its valuations, or equivalently a principal fractional ideal has a unique generator up to multiplication by a root of unity. We use these facts repeatedly in this section.

We need to relate our results in terms of global Artin symbols to a basis of $U_{k,S,\mathfrak{t}}$. We recall the notation for ideal groups developed in Chapter 2, §1. In addition, we use the notation $\mathcal{I}_{k,\infty}\langle S \rangle$ to denote the free subgroup of $\mathcal{I}_{k,\infty}$ generated by the finite primes in S. We have the following exact commutative diagram.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & U_{k,S,\mathfrak{t}} & \longrightarrow & \mathcal{I}_{k,\infty}\langle S \rangle & \longrightarrow & \mathcal{I}_{k,\infty}\langle S \rangle / U_{k,S,\mathfrak{t}} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{P}_{k,\infty,\mathfrak{t}} & \longrightarrow & \mathcal{I}_{k,\{\mathfrak{t},\infty\}} & \longrightarrow & A_{k,\infty,\mathfrak{t}} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{P}_{k,S,\mathfrak{t}} & \longrightarrow & \mathcal{I}_{k,S\cup\{\mathfrak{t}\}} & \longrightarrow & A_{k,S,\mathfrak{t}} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0. & &
\end{array}$$

We obtain from the diagram an exact sequence

$$0 \longrightarrow \mathcal{I}_{k,\infty}\langle S \rangle / U_{k,S,\mathfrak{t}} \longrightarrow A_{k,\infty,\mathfrak{t}} \longrightarrow A_{k,S,\mathfrak{t}} \longrightarrow 0. \tag{7.10}$$

The group $A_{k,\infty,\mathfrak{t}}$ fits into the exact sequence

$$0 \longrightarrow U_{k,\infty} \longrightarrow (\mathcal{O}/\mathfrak{t})^\times \longrightarrow A_{k,\infty,\mathfrak{t}} \longrightarrow A_{k,\infty} \longrightarrow 0$$

The class group $A_{k,\infty}$ is the ideal class group of $\mathcal{O}$, with size $h_{k,\infty} = h_{\mathcal{O}}$. Therefore we have $\#A_{k,\infty,\mathfrak{t}} = h_{\mathcal{O}}(N_{\mathfrak{t}} - 1)/w_k$. If $u_1, \ldots, u_n$ is an integral basis for $U_{k,S,\mathfrak{t}}$, we write V for the matrix with (i,j)-th entry $v_{ij} = v_{\mathfrak{p}_i}(u_j)$, a nonsingular $n \times n$ matrix. Now in the notation of Chapter 3, §2, we have $R = (-1)^n V^t \cdot \operatorname{diag}(\ln N_{v_1}, \ln N_{v_2}, \ldots \ln N_{v_n})$. Since also $\#T = 1$, this implies that the sign ξ defined there is the sign of $(-1)^n \det V$. The absolute value of $\det V$ is the size of $\mathcal{I}_{k,\infty}\langle S\rangle / U_{k,S,\mathfrak{t}}$. We conclude from (7.10) that

$$\det V = (-1)^n \xi \left(\frac{N_{\mathfrak{t}} - 1}{w_k}\right) \frac{h_{\mathcal{O}}}{h_{k,S,\mathfrak{t}}}.$$

We now use the results of §3 to relate the local Artin symbols for the u_i to the global Artin symbols appearing in §2. As in the latter section, we define elements of $\mathbb{Z}[G]$

$$a_{ij} = \sigma_{i,j}^{-1} - 1, \qquad v_i = s(\mathfrak{p}_i)^{-1} - 1,$$

This defines a matrix $M = (m_{ij})$ as in (7.5). Applying the natural isomorphism $G \to I_G/I_G^2$ of Lemma 2.6.2 to the result of Proposition 3.9 and using Corollary 2.6.4 gives the following

Proposition 4.1. *Let R be the $n \times n$ matrix with (i,j)-th entry $f_{\mathfrak{p}_j}(u_i)$. We have*

$$b f_{\mathfrak{p}_j}(u_i) \equiv (-1)^n b \cdot VM \pmod{I_G^2}. \quad \square$$

We now relate this to Proposition 2.5. For the following calculations, "vector" means a length n column vector over k, $\mathbb{Z}$ or $\mathbb{Z}[G]$. Let V^{adj} represent the adjugate matrix of V, that is, the transpose of its cofactor matrix. Then

$$V^{\mathrm{adj}} V = (\det V)\mathbf{1} = (-1)^n \xi \left(\frac{N_{\mathfrak{t}} - 1}{w_k}\right) \frac{h_{\mathcal{O}}}{h_{k,S,\mathfrak{t}}} \mathbf{1},$$

where $\mathbf{1}$ denotes the identity matrix. On the other hand, $(1 - N_{\mathfrak{t}})[H : k]\mathbf{1} = (1 - N_{\mathfrak{t}}) h_{\mathcal{O}} \mathbf{1}$ is the valuation matrix of the vector $(N_{\Upsilon} \alpha_i)_i$. Therefore if Ω denotes the vector $(\phi^1(N_{\Upsilon}\alpha_i))_i$, then $\Omega = (-1)^{n+1} \xi (w_k h_{k,S,\mathfrak{t}}) V^{\mathrm{adj}} \omega$, where $\omega = (\phi^1(u_i))_i$. Note that the vector $((-1)^{i+1} M_{i1})_i$ is the first column of $(M^{\mathrm{adj}})^t$, where t denotes transpose, so we write it as $(M^{\mathrm{adj}})^t_{*1}$. Then Corollary 2.6 states that

$$\phi(\lambda_{\mathfrak{m}}^{b/w_{\mathfrak{m}}}) \equiv -\frac{b}{w_k} \Omega^t (M^{\mathrm{adj}})^t_{*1} \pmod{I_G^n}.$$

The right-hand side of this congruence is $\frac{b}{w_k}(-1)^n \xi (w_k h_{k,S,\mathfrak{t}}) \omega^t (V^{\mathrm{adj}})^t (M^{\mathrm{adj}})^t_{*1}$. By standard matrix rules,

$$b(V^{\mathrm{adj}})^t (M^{\mathrm{adj}})^t_{*1} = (-1)^n b((VM)^{\mathrm{adj}})^t_{*1} \equiv b(R^{\mathrm{adj}})^t_{*1} \pmod{I_G^2}.$$

We conclude

Theorem 4.2.

$$\phi(\lambda_{\mathfrak{m}}^{b/w_{\mathfrak{m}}}) \equiv b\xi h_{k,S,\mathfrak{t}} \sum_{i=1}^{n} (-1)^{i+1} \phi^1(u_i) R_{i1} \pmod{I_G^n}.$$

By Proposition 6.1.2, we have $\eta_{H(\mathfrak{m})/k,S,\{\mathfrak{t}\}}^{w_k} = \lambda_{\mathfrak{m}}^{w_k/w_{\mathfrak{m}}}$. Therefore, we obtain

$$b\phi(\eta) \equiv b\xi h_{k,S,\mathfrak{t}} (\mathrm{Reg}_G \circ \tilde{\phi})(u_1 \wedge \cdots \wedge u_n) \pmod{I_G^n},$$

that is, we verify Conjecture 3.5.1 after weakening by b on both sides.

Corollary 4.3. *If $h_{k,\infty} = 1$ (i.e. $\mathcal{O}$ is a principal ideal domain), or the sequence (7.1) splits, or $n = 1$, then*

$$w_k\phi(\eta) \equiv w_k\xi h_{k,S,\mathfrak{t}} (\mathrm{Reg}_G \circ \tilde{\phi})(u_1 \wedge \cdots \wedge u_n) \pmod{I_G^n},$$

Proof. In these cases we may take $b = w_k$. □

If K/k is an abelian extension in which all places other than a particular one ∞ are finite and not totally split, $h_{k,\infty} = 1$ and w_k is coprime to $[K : k]$, then this result combined with Proposition 4.2.1 proves the whole of Conjecture 3.5.1. To see this, we note that w_k is coprime to G and hence multiplication by w_k is an automorphism of the quotient I_G^{n-1}/I_G^n, which is a finite abelian group supported above the support of $\#G$. In particular, this proves the conjecture for an odd-degree extension of $\mathbb{Q}$, with the infinite place the only place that splits.

Chapter 8

Minus-unit conjectures

Suppose K/k is an abelian extension, and k' is a quadratic Galois extension of k such that $K \cap k' = k$. Set $K' = k'K$. Then we have the following diagram of fields

$$\begin{tikzcd}[column sep=small]
 & K' \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & k' \arrow[dl, dash] \\
 & k &
\end{tikzcd}$$

The Galois group $\mathrm{Gal}(K'/k)$ is the direct product

$$\mathrm{Gal}(K'/k) = \mathrm{Gal}(K/k) \times \mathrm{Gal}(k'/k).$$

Set $G = \mathrm{Gal}(K/k) \cong \mathrm{Gal}(K'/k')$ (the isomorphism being given by the natural restriction map). The group $\mathrm{Gal}(k'/k)$ is cyclic of order two, and we denote its nontrivial element by τ; by the direct product decomposition, τ may also be considered as an element of $\mathrm{Gal}(K'/k)$. Thus we naturally have an involution of K'/k in this situation. We let ω denote the nontrivial character of $\mathrm{Gal}(k'/k)$, so $\omega(\tau) = -1$.

The kernel of the norm map $1 + \tau$ on a $\mathbb{Z}[\mathrm{Gal}(K'/k)]$-module M consists of the elements x such that $x^\tau = -x$, and this subgroup will be referred to as the "minus-part" of M, written M^-. If M is 2-divisible (i.e. multiplication by 2 is an automorphism of M) then M^- is a direct summand of M. Another way to put this is that the two idempotents in $\mathbb{Z}[\frac{1}{2}][\langle\tau\rangle]$

$$e_+ = \frac{1+\tau}{2} \qquad e_- = e_\omega = \frac{1-\tau}{2}$$

split up any $\mathbb{Z}[\frac{1}{2}][\mathrm{Gal}(K'/k)]$-module M into a direct sum $M^+ \oplus M^-$, where $M^+ = e_+M = M^{\langle\tau\rangle}$ is the submodule fixed by τ and the "minus-part" M^- is equal to e_-M.

In this chapter we use the arrangement of field extensions above and apply the decompositions into plus- and minus-parts to L-functions and unit groups. This provides an interpretation of two conjectures by Darmon and Gross which roughly resemble Gross's conjecture (Conjecture 3.3.2), but formulated for minus-parts of equivariant L-functions and minus-units. The conjectures are interpreted as providing "base-change" statements for Conjecture 3.5.1 above, or more precisely giving a logical implication from the validity of the conjecture for the extension K/k to its validity for K'/k'. In fact, this only works under a certain simplifying hypothesis (Hypotheses 4.1 and 8.1 below) and the resulting statements are weakened by a power-of-two factor (mainly coming from the problem of inverting 2 for the decompositions described above). Nevertheless, these results provide interpretation for conjectures whose position had not been well understood, and were often regarded as "refinements" or "analogues" of Gross's conjecture when in fact they appear to relate to behaviour of a natural generalisation of it.

1 Quadratic extension of the base field for L-functions

In this section we assume S and T are disjoint finite sets of places of k such that S is nonempty and contains all infinite places, S contains all places ramifying in K/k and $S_{k'}$ contains all places ramifying in K'/k'. We will use stronger hypotheses in following sections. We compare the definitions of the S-truncated, T-modified L-functions defined in Chapter 2, §3 for the extensions K/k and K'/k'.

The character ω extends to a function on the set of finite places of k by setting $\omega(v) = \omega(\sigma_v)$ if v is unramified in k'/k and 0 otherwise. Then we have

Lemma 1.1. *If $v \notin S$, then*

$$\prod_{\substack{v' \text{ place of } k' \\ v' | v}} (1 - N_{v'}^s \cdot (v', K'/k')^{-1}) = (1 - N_v^s \cdot (v, K/k)^{-1})(1 - \omega(v) N_v^s \cdot (v, K/k)^{-1}).$$

Proof. By the fundamental equality for extensions of primes in Galois extensions, we have $efg = [k' : k] = 2$, where e is the ramification index of any v'/v, f is its residue extension degree and g is the number of primes in k' lying above v. Note that $N_w = N_v^f$ and $(v', K'/k')|_K = (v, K/k)^f$, the second equality holding under the restriction isomorphism $\mathrm{Gal}(K'/k') \xrightarrow{\sim} \mathrm{Gal}(K/k)$. In the case where $\omega(v) = 0$, v is ramified in k'/k and so $f = g = 1$. Each side in the equality of the lemma then has exactly one factor, and these are clearly the same.

In the case where v is split in k', i.e. $g = 2$, we have $\omega(v) = 1$ and the equality clearly has two matching factors on each side. In the case where v is inert, i.e. $f = 2$, we have $(v, k'/k) = \tau$ and so $\omega(v) = -1$ and the right-hand side of the equality is $(1 - N_v^{2s}(v, K/k)^2)$, which is equal to the left-hand side. ☐

Let S' be the union of S with the set of places of k which ramify in k'/k. Lemma 1.1 shows that the L-functions satisfy the following base-change factorisation when passing from K'/k' to K'/k:

$$\Theta_{K'/k',S,T}(s) = \Theta_{K'/k'/k,S',T}(s,\omega)\Theta_{K/k,S,T}(s), \tag{8.1}$$

where

$$\begin{aligned}\Theta_{K'/k'/k,S',T}(s,\omega) &:= \Big(\prod_{v\in T}(1-\omega(v)N_v^{1-s}\sigma_v^{-1})\Big)\sum_{\chi\in\hat{G}} L_{K'/k,S'}(s,\omega\chi^{-1})e_\chi(K/k)\\ &= \Big(\prod_{v\in T}(1-\omega(v)N_v^{1-s}\sigma_v^{-1})\Big)\cdot\\ &\quad\Big(\sum_{\sigma\in G}(\zeta_{K'/k,S'}(s,\sigma)-\zeta_{K'/k,S'}(s,\sigma\tau))\sigma^{-1}\Big) \qquad (8.2)\end{aligned}$$

is a twisted Stickelberger function (with trivial Euler factors at ramified primes). The validity of equation (8.1) follows from Lemma 1.1 in the region of convergence $\operatorname{Re} s > 1$ and then everywhere by meromorphic continuation.

We also write

$$\delta_T^\omega = \prod_{v\in T}(1-\omega(v)N_v\sigma_v^{-1}) \in \mathbb{Z}[G]$$

for the relative T-modification factor at $s=0$.

2 Unit groups in quadratic extensions

Let k'/k be a quadratic Galois extension of global fields with Galois group generated by τ. For this section we only need to assume that S is a finite, nonempty set of places of k containing all infinite places, and that T is any finite disjoint set of places of k. Let $\#S = n+1$ and let r denote the number of places in S which split in k'/k.

We will be interested in the unit group $U_{k',S,T}$ and its subgroups $U_{k,S,T}$, $U^-_{k',S,T} = \{x \in U_{k',S,T} : x^\tau = x^{-1}\}$ and $U^{1-\tau}_{k',S,T} = \{x^{1-\tau} : x \in U_{k',S,T}\}$. Obviously $U^{1-\tau}_{k',S,T} \subseteq U^-_{k',S,T}$. The quotient is a Tate cohomology group in the sense of [41, Ch. VIII]:

$$U^-_{k',S,T}/U^{1-\tau}_{k',S,T} = \hat{H}^{-1}(\langle\tau\rangle, U_{k',S,T}) \cong H^1(\langle\tau\rangle, U_{k',S,T}).$$

We first prove some lemmas calculating indices related to these unit groups.

Lemma 2.1. $(U_{k',S} : U_{k',S,T}) = (U_{k,S} : U_{k,S,T})(U^{1-\tau}_{k',S} : U^{1-\tau}_{k',S,T})$

Proof. Consider the following commutative diagram, in which the rows are exact.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_{k,S,T} & \longrightarrow & U_{k',S,T} & \xrightarrow{1-\tau} & U^{1-\tau}_{k',S,T} & \longrightarrow & 0\\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & U_{k,S} & \longrightarrow & U_{k',S} & \xrightarrow{1-\tau} & U^{1-\tau}_{k',S} & \longrightarrow & 0, \end{array}$$

The vertical arrows are inclusions. Applying the snake lemma, we obtain the exact sequence

$$0 \longrightarrow U_{k,S}/U_{k,S,T} \longrightarrow U_{k',S}/U_{k',S,T} \xrightarrow{1-\tau} U_{k',S}^{1-\tau}/U_{k',S,T}^{1-\tau} \longrightarrow 0.$$

This shows the result. □

Lemma 2.2. $(U_{k',S}^{1-\tau} : U_{k',S,T}^{1-\tau}) = (U_{k',S}^{-} : U_{k',S,T}^{-})\frac{\#H^1(\langle\tau\rangle, U_{k',S,T})}{\#H^1(\langle\tau\rangle, U_{k',S})}$.

Proof. We have $(U_{k',S}^{-} : U_{k',S,T}^{1-\tau}) = (U_{k',S}^{-} : U_{k',S}^{1-\tau})(U_{k',S}^{1-\tau} : U_{k',S,T}^{1-\tau}) = (U_{k',S}^{-} : U_{k',S,T}^{-})(U_{k',S,T}^{-} : U_{k',S,T}^{1-\tau})$. □

We next we adapt the method of [46, §II.2 and Thm. IV.5.4] to show the following.

Lemma 2.3.

$$(U_{k',S,T} : U_{k,S,T}U_{k',S,T}^{-}) = \frac{2^r\#(U_{k',S,T}^{-} \cap \{\pm 1\})}{\#H^1(\langle\tau\rangle, U_{k',S,T})}$$

Proof. The sequence

$$0 \longrightarrow U_{k,S,T}U_{k',S,T}^{-} \longrightarrow U_{k',S,T} \xrightarrow{1-\tau} \frac{U_{k',S,T}^{1-\tau}}{(U_{k',S,T}^{-})^2} \longrightarrow 0$$

is exact. This shows that $(U_{k',S,T} : U_{k,S,T}U_{k',S,T}^{-}) = (U_{k',S,T}^{1-\tau} : (U_{k',S,T}^{-})^2)$. We also have:

$$(U_{k',S,T}^{-} : (U_{k',S,T}^{-})^2) = (U_{k',S,T}^{-} : U_{k',S,T}^{1-\tau})(U_{k',S,T}^{1-\tau} : (U_{k',S,T}^{-})^2).$$

The first factor on the right is $\#H^1(\langle\tau\rangle, U_{k',S,T})$. The factor on the left can be calculated from the standard decomposition of the finitely generated abelian group $U_{k',S,T}^{-}$. The free rank of this group is r, and the cokernel of squaring on the torsion part has the same size as the kernel, which is $U_{k',S,T}^{-} \cap \{\pm 1\}$. The second factor on the right is what we want to calculate. Hence

$$2^r\#(U_{k',S,T}^{-} \cap \{\pm 1\}) = \#H^1(\langle\tau\rangle, U_{k',S,T})(U_{k',S,T} : U_{k,S,T}U_{k',S,T}^{-}),$$

as required. □

We now compare the regulators for the fields k and k', as defined in Chapter 3, §2. We let $n = \#S - 1$ and r be the number of places in S which split in k'. Thus $\#S_k = n + 1 + r = n' + 1$. We assume that at least one place in S does not split in k', i.e. $n \geq r$.

We order the places of S as

$$S = \{v_1, \dots, v_{n+1}\}, \tag{8.3}$$

where for $1 \le i \le r$ the place v_i splits into distinct places v'_i and $\overline{v'}_i$ of k' (conjugate by τ) and for $i > r$ there is a unique place v'_i of k' above v_i. The set $S_{k'}$ is ordered as follows:

$$S_{k'} = \{v'_1, \ldots, v'_r, \overline{v'}_1, \ldots, \overline{v'}_r, v'_{r+1}, \ldots, v'_{n+1}\}. \tag{8.4}$$

Let the r-tuple of S-units $\boldsymbol{\varepsilon}_- = (\varepsilon_1, \ldots, \varepsilon_r)$ be a basis for a maximal free $\mathbb{Z}$-submodule $\langle \boldsymbol{\varepsilon}_- \rangle$ of $U^-_{k',S,T}$, and $\boldsymbol{\varepsilon}_+ = (\varepsilon_{r+1}, \ldots, \varepsilon_{r+n})$ the same thing for $U_{k,S,T}$. Let $\boldsymbol{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_{r+n})$. We wish to use $\boldsymbol{\varepsilon}$ instead of a basis for a maximal free $\mathbb{Z}$-submodule of $U_{k',S,T}$ to calculate the regulator $R =: R_{k'}$ as defined in Chapter 3, §2 for the field k'. Define $R_{k'}(\boldsymbol{\varepsilon})$ as follows (using the notation of Chapter 3, §2)

$$(\wedge^{n'} \lambda_{S_{k'}})(\varepsilon_1 \wedge \cdots \wedge \varepsilon_{n'}) = R_{k'}(\boldsymbol{\varepsilon}) \cdot \mathbf{x},$$

and let $\mathbf{u} = (u_1, \ldots, u_{n+r})$ be a basis for a maximal free $\mathbb{Z}$-submodule of $U_{k',S,T}$, so that $(U_{k',S,T} : \langle \mathbf{u} \rangle) = w_{k',T}$. By inverting a unit if necessary, we may assume that

$$(U_{k',S,T} : \langle \boldsymbol{\varepsilon} \rangle) \cdot u_1 \wedge \cdots \wedge u_{n+r} = w_{k',T} \cdot \varepsilon_1 \wedge \cdots \wedge \varepsilon_{n+r} \tag{8.5}$$

in $\mathbb{Q} \wedge^{r+n}_{\mathbb{Z}} U_{k',S,T}$. Then

$$(U_{k',S,T} : \langle \boldsymbol{\varepsilon} \rangle) R_{k'} = w_{k',T} R_{k'}(\boldsymbol{\varepsilon}). \tag{8.6}$$

The sign $\xi_{k'}$ is defined to be the ξ defined in Chapter 3, §2 for the field k', so $\xi_{k'} = (-1)^{\#T_{k'}+1} \cdot \operatorname{sign}(R_{k'})$.

Now consider the exact commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & 0 \arrow[r] \arrow[d] & \langle \boldsymbol{\varepsilon}_- \rangle \times \langle \boldsymbol{\varepsilon}_+ \rangle \arrow[r] \arrow[d] & \langle \boldsymbol{\varepsilon}_- \rangle \times \langle \boldsymbol{\varepsilon}_+ \rangle \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & U^-_{k',S,T} \cap U_{k,S,T} \arrow[r, "\Delta"] & U^-_{k',S,T} \times U_{k,S,T} \arrow[r] & U^-_{k',S,T} U_{k,S,T} \arrow[r] & 0,
\end{tikzcd}$$

where $\Delta(x) = (x^{-1}, x)$. Applying the snake lemma gives an exact sequence

$$0 \longrightarrow U^-_{k',S,T} \cap U_{k,S,T} \longrightarrow U^-_{k',S,T}/\langle \boldsymbol{\varepsilon}_- \rangle \times U_{k,S,T}/\langle \boldsymbol{\varepsilon}_+ \rangle \longrightarrow U^-_{k',S,T} U_{k,S,T}/\langle \boldsymbol{\varepsilon} \rangle \longrightarrow 0,$$

and hence $\#(U^-_{k',S,T} \cap U_{k,S,T})(U^-_{k',S,T} U_{k,S,T} : \langle \boldsymbol{\varepsilon} \rangle) = (U^-_{k',S,T} : \langle \boldsymbol{\varepsilon}_- \rangle)(U_{k,S,T} : \langle \boldsymbol{\varepsilon}_+ \rangle)$. Now if $x \in U^-_{k',S,T} \cap U_{k,S,T}$ then $x^\tau = x = x^{-1}$ and so $x = \pm 1$; therefore the intersection is either $\{\pm 1\}$ or $\{1\}$. This shows that $\#(U^-_{k',S,T} \cap U_{k,S,T}) = \#(U^-_{k',S,T} \cap \{\pm 1\})$. Let $w^-_{k',T}$ denote the size of the torsion subgroup of $U^-_{k',S,T}$. Then combining these results with Lemma 2.3 gives

$$(U_{k',S,T} : \langle \boldsymbol{\varepsilon} \rangle) = \frac{2^r w^-_{k',T} w_{k,T}}{\# H^1(\langle \tau \rangle, U_{k',S,T})}. \tag{8.7}$$

The regulator $R_{k'}(\boldsymbol{\varepsilon})$ is equal to the determinant of the following block matrix:

$$\begin{array}{c||c|c|c}
 & v'_1,\dots,v'_r & \overline{v'}_1,\dots,\overline{v'}_r & v'_{r+1},\dots,v'_n \\
\hline\hline
\begin{matrix}\varepsilon_1\\ \vdots \\ \varepsilon_r\end{matrix} & -\ln|\varepsilon|_{v'} & -\ln|\varepsilon|_{\overline{v'}} & -\ln|\varepsilon|_{v'} \\
\hline
\begin{matrix}\varepsilon_{r+1}\\ \vdots \\ \varepsilon_{n'}\end{matrix} & -\ln|\varepsilon|_{v'} & -\ln|\varepsilon|_{\overline{v'}} & -\ln|\varepsilon|_{v'}\,.
\end{array}$$

Since $\varepsilon_{r+1},\dots,\varepsilon_{n'}$ are in k, the $n\times r$ blocks in the bottom-left and bottom-middle of the matrix are identical, and so subtracting columns shows that $R_{k'}(\boldsymbol{\varepsilon})$ is also the determinant of the matrix

$$\begin{array}{c||c|c|c}
 & v'_1,\dots,v'_r & \overline{v'}_1,\dots,\overline{v'}_r & v'_{r+1},\dots,v'_n \\
\hline\hline
\begin{matrix}\varepsilon_1\\ \vdots \\ \varepsilon_r\end{matrix} & -\ln|\varepsilon^{1-\tau}|_{v'} & -\ln|\varepsilon|_{\overline{v'}} & -\ln|\varepsilon|_{v'} \\
\hline
\begin{matrix}\varepsilon_{r+1}\\ \vdots \\ \varepsilon_{n'}\end{matrix} & 0 & -\ln|\varepsilon|_{\overline{v'}} & -\ln|\varepsilon|_{v'}
\end{array} \tag{8.8}$$

We denote the real numbers R and ξ calculated for the field k as in Chapter 3, §2 by R_k and ξ_k. We also define a "minus-unit regulator" R^- analogously to the R of Chapter 3, §2 but for the units $\varepsilon_1,\dots,\varepsilon_r$ and the places $v'_1,\dots,v'_r$, i.e.

$$R^- = \det(-\ln|\varepsilon_i|_{v'_j})_{i,j=1}^{r}. \tag{8.9}$$

Then the top-left $r\times r$ block of (8.8) has determinant $2^r R^-$. We let $\xi^- = (-1)^{\#T_{k'}-\#T}\operatorname{sign}(R^-)$.

If $u\in k$ and v' is a place of k' over a place v of k, then we have $|u|_{v'}=|u|_v$ if v'/v is split, and $|u|_{v'}=|u|_v^2$ otherwise. Hence the bottom-right $n\times n$ block of (8.8) has determinant $2^{n-r}R_k$. Putting this together gives

$$R_{k'}(\boldsymbol{\varepsilon}) = 2^n R^- R_k \qquad \text{and} \qquad \xi_{k'}=\xi^-\xi_k.$$

Therefore, using (8.6) and (8.7), we have

$$R_{k'} = \frac{w_{k',T}}{w_{k,T}w^-_{k',T}}2^{n-r}\#H^1(\langle\tau\rangle,U_{k',S,T})R^-R_k.$$

Now by (2.8) we have

$$\zeta_{k',S,T}(s) = L_{k'/k,S,T}(s,\omega)\zeta_{k,S,T}(s).$$

Hence, by (3.3), the coefficient of the leading term of the nontrivial L-function for k'/k is given by

$$\begin{aligned} L^r_{k'/k,S,T}(0,\omega) &= \frac{\zeta^{n+r}_{k',S,T}(0)}{\zeta^n_{k,S,T}(0)} = (-1)^{\#T_{k'}-\#T}\frac{w_{k,T}}{w_{k',T}}\frac{h_{k',S,T}}{h_{k,S,T}}\frac{\mid R_{k'}\mid}{\mid R_k\mid} \\ &= (-1)^{\#T_{k'}-\#T}\frac{1}{w^-_{k',T}}\frac{h_{k',S,T}}{h_{k,S,T}}2^{n-r}\#H^1(\langle\tau\rangle,U_{k',S,T})\mid R^-\mid. \qquad (8.10)\end{aligned}$$

3 Darmon's circular unit

We now relate the circular unit defined by Darmon in [12] to a special value of the base-change factor $\Theta_{K'/k'/k,S',T}(s,\omega)$ appearing in (8.1). For comparison with [12], we assume the following hypothesis for §§3–7.

Hypothesis 3.1 (Darmon's setup). *Let N and S be coprime integers with $N>2$ and $S>1$. Let ω be a primitive, quadratic, even Dirichlet character defined modulo N. Set $k'=\mathbb{Q}(\zeta_N)^{\ker\omega}$, a real quadratic field, and call its non-trivial automorphism τ. Let K be a real subfield of $\mathbb{Q}(\zeta_S)$, normal over $\mathbb{Q}$ and of conductor S. Write $K'=k'K$.*

Note that our notation N and S agrees with [12], but the fields denoted L and K in loc. cit. are respectively called K' and k' here.

We are in the situation of §1 with the further assumptions that $k=\mathbb{Q}$ and that K and k' are totally real and have coprime conductors. We define the set $S=S_\mathbb{Q}$ from the integer S in the obvious way: $S_\mathbb{Q}=\mathrm{Supp}(S)\cup\{\infty\}$. We assume all primes dividing S ramify in $K/\mathbb{Q}$, so that there is a unique place $\infty\in S_\mathbb{Q}$ splitting completely in $K/\mathbb{Q}$, and exactly two places of k' splitting completely in K', namely the two places above ∞ (which are mutually conjugate under τ).

All the characters of these extensions come from even Dirichlet characters because the fields are totally real. Since L-functions of even characters vanish at $s=0$ by Proposition 2.3.1, differentiating (8.1) twice shows that we have the following equality in $\mathbb{C}[G]$

$$\Theta^2_{K'/k',S,T}(0)=\frac{1}{2}\Theta''_{K'/k',S,T}(0)=\Theta'_{K'/k'/\mathbb{Q},S',T}(0,\omega)\Theta'_{K/\mathbb{Q},S,T}(0). \qquad (8.11)$$

We now relate the base-change factor $\Theta'_{K'/k'/\mathbb{Q},S',T}(0,\omega)$ to the circular unit defined in [12, §4]. The circular unit is the following element of $k'(\zeta_S)$.

$$\alpha_S:=\prod_{\sigma\in\mathrm{Gal}(\mathbb{Q}(\zeta_{NS})/\mathbb{Q}(\zeta_S))}\sigma(\zeta_{NS}-1)^{\omega(\sigma)}=(N_{\mathbb{Q}(\zeta_{NS})/k'(\zeta_S)}(\zeta_{NS}-1))^{1-\tau}.$$

Write ∞' for the place of K' corresponding to the embedding of K' into $\mathbb{R}$ induced by $\zeta_{NS}\mapsto e^{2\pi i/NS}$, and $\overline{\infty}'$ its conjugate by τ.

Lemma 3.2. $\Theta'_{K'/k'/\mathbb{Q},S'}(0,\omega)\cdot(\infty'-\overline{\infty}')=\frac{1}{2}\lambda_{S_{K'}}(N_{k'(\zeta_S)/K'}\alpha_S)$.

Proof. Let S' denote the union of $S_{\mathbb{Q}}$ and the set of primes dividing N. By (6.5) we have

$$\zeta'_{\mathbb{Q}(\zeta_{NS})^+/\mathbb{Q},S'}(0,\sigma) = -\ln \mid 1-\zeta_{NS}^a \mid,$$

where a is a representative of the class in $(\mathbb{Z}/NS\mathbb{Z})^\times/\{\pm 1\}$ corresponding to σ. Hence by Proposition 2.3.2 we have

$$\zeta'_{K'/k,S'}(0,\sigma) = -\frac{1}{2}\ln |N_{\mathbb{Q}(\zeta_{NS})/K'}(1-\zeta_{NS})^\sigma|_{\infty'}.$$

Therefore, for $\sigma \in G$,

$$\begin{aligned} & \zeta'_{K'/k,S'}(0,\sigma) - \zeta'_{K'/k,S'}(0,\sigma\tau) \\ = \quad & -\frac{1}{2}\ln |N_{k'(\zeta_S)/K'}N_{\mathbb{Q}(\zeta_{NS})/k'(\zeta_S)}(1-\zeta_{NS})^{(1-\tau)\sigma}|_{\infty'} \\ = \quad & -\frac{1}{2}\ln |N_{k'(\zeta_S)/K'}\alpha_S^\sigma|_{\infty'}. \end{aligned}$$

Write for brevity $\beta = N_{k'(\zeta_S)/K'}\alpha_S$. Then

$$\lambda_S(\beta) = -\sum_{\sigma\in G}\ln|\beta^\sigma|_{\infty'}\sigma^{-1}\infty' - \sum_{\sigma\in G}\ln|\beta^{\tau\sigma}|_{\infty'}\sigma^{-1}\overline{\infty}',$$

using the fact that $(1-\zeta_{NS})$ is a global unit to see that the absolute values at finite places are trivial. But since $\alpha_S^\tau = \alpha_S^{-1}$, i.e. α_S is a minus-unit, this is the same as

$$\lambda_S(\beta) = \Big(-\sum_{\sigma\in G}\ln|\beta^\sigma|_{\infty'}\sigma^{-1}\Big)(\infty - \overline{\infty}').$$

Putting all this together and using the definition (8.2) gives the claimed result. □

Definition 3.3. *We set* $\eta_\omega := \delta_T^\omega N_{k'(\zeta_S)/K'}\alpha_S$.

Then

$$\Theta'_{K'/k'/\mathbb{Q},S',T}(0,\omega)\cdot(\infty-\overline{\infty}') = \frac{1}{2}\lambda_{S_{K'}}(\eta_\omega). \tag{8.12}$$

4 Calculation of η

We wish to compare the Stark units of Chapter 2, §1 corresponding to the two sets of data $K/k, S, T$ and $K'/k', S_{k'}, T_{k'}$, where T is some set of primes such that $U_{K',S,T}$ is torsion free (Hypothesis 4.1). The connection will be given by Darmon's circular unit as defined in the preceding section. We first review our notation and the definition of the Stark units involved.

Consider the extension $K/\mathbb{Q}$. The set $S = S_{\mathbb{Q}}$ consists of the infinite place of $\mathbb{Q}$ and the finite places corresponding to the primes dividing the integer S. These finite primes may be divided into two kinds: those which split in $k'/\mathbb{Q}$ and those which are inert (they are all unramified by the assumption of coprimality of conductors in Hypothesis 3.1). We write n_s for the number of split primes, n_i for the number of inert ones, and n for the total. Since the infinite place is the only place in S splitting in K, we have $r_S = 1$ and $n = n_s + n_i = 1 + d$, using the notation r_S (Chapter 2, §3) and d (Chapter 3) for the extension K/k. We denote the n_s primes in S splitting in $k'/\mathbb{Q}$ by $p_1, \ldots, p_{n_s}$, and the inert primes by $q_1, \ldots, q_{n_i}$. Thus we have

$$S = S_{\mathbb{Q}} = \{\infty, p_1, \ldots, p_{n_s}, q_1, \ldots, q_{n_i}\}. \tag{8.13}$$

The Stark unit $\eta_{K/k} \in \mathbb{R}U_{K,S,T}e_1$ is the unique element satisfying

$$\Theta^1_{K/k,S,T}(0)(\infty' - w_0) = \lambda_S(\eta_{K/k}),$$

where ∞' is the infinite place of K induced by the place ∞' defined in §3, and v_0 is any finite place of K.

We turn now to the definition of the Stark unit for the data $K'/k', S_{k'}, T_{k'}$. Here we have $r_{S_{k'}} = 2$, corresponding to the two places ∞' and $\overline{\infty}'$ of k' lying above the infinite place of $\mathbb{Q}$. Each prime $p_i \in S$ splits into two primes of k', which we write as $\mathfrak{p}_i$ and $\bar{\mathfrak{p}}_i$. These are mutually conjugate under the action of τ. The primes q_i remain prime in k', and we denote $\mathfrak{q}_i = q_i\mathcal{O}_{k'}$. Hence we have

$$S_{k'} = \{\infty', \overline{\infty}', \mathfrak{p}_1, \ldots, \mathfrak{p}_{n_s}, \bar{\mathfrak{p}}_1, \ldots \bar{\mathfrak{p}}_{n_s}, \mathfrak{q}_1, \ldots, \mathfrak{q}_{n_i}\}. \tag{8.14}$$

We add dashes to distinguish the integers n and d (as defined at the beginning of Chapter 3) for the set $S_{k'}$, so that $\#S_{k'} = r_{S_{k'}} + d' + 1 = n' + 1$. Then, since $\#S_{k'} = 2 + 2n_s + n_i$, we have $n' = 1 + 2n_s + n_i$ and $d' = 2n_s + n_i - 1$. The Stark unit $\eta_{K'/k'} \in \mathbb{R} \wedge^2_{\mathbb{Z}[G]} U_{K',S,T}e_2$ is defined by

$$\Theta^2_{K'/k',S,T}(0)(\infty' - w_0') \wedge (\overline{\infty}' - w_0') = (\wedge^2\lambda_{S_{K'}})(\eta_{K'/k'})$$

for a finite place w_0' of K'.

The results of §3 allow us to express $\eta_{K'/k'}$ in terms of η_ω and $\eta_{K/k}$. We have

$$\begin{aligned} &2\Theta^2_{K'/k,S,T}(0)(\infty' - w_0') \wedge (\overline{\infty}' - w_0') = \\ &\qquad \Theta'_{K'/k'/\mathbb{Q},S',T}(0,\omega)(\infty' - \overline{\infty}') \wedge \Theta'_{K/\mathbb{Q},S,T}(0)(\infty' + \overline{\infty}' - 2w_0'). \end{aligned} \tag{8.15}$$

Recall that $\lambda_{S_{K'}}(\eta_\omega)$ was calculated in (8.12) above. We will now calculate $\lambda_{S_{K'}}(\eta_{K/\mathbb{Q}})$. We note the commutative diagram (2.5) for the extension K'/K, so that $\lambda_{S_{K'}}(x) = i_{K'/K}(\lambda_{S_K}(x))$ for $x \in U_{k,S,T}$, where $i_{K'/K}(w) = w' + \overline{w'}$ for any choice of place w' of K' above a place w of K. Hence $\lambda_{S_{K'}}(\eta_{K/\mathbb{Q}}) = \Theta'_{K/\mathbb{Q},S,T}(0)(\infty' + \overline{\infty}' - w_0' - \overline{w_0'})$, where w_0' is a place of K' chosen above w_0. If we assume $n_i \neq 0$, we can choose w_0 such that $w_0' = \overline{w_0'}$. Using this choice of w_0' in (8.15) shows that

$$(\wedge^2\lambda_{S_{K'}})(\eta_\omega \wedge \eta_{K/\mathbb{Q}}) = 4\Theta^2_{K'/k',S,T}(0)(\infty' - w_0') \wedge (\overline{\infty}' - w_0'),$$

and hence

$$4\eta_{K'/k'} = \eta_\omega \wedge \eta_{K/\mathbb{Q}}. \tag{8.16}$$

In [12], Darmon makes a congruence conjecture for his circular unit. We propose to interpret this as a base-change statement for Conjecture 3.5.1, under the following assumptions:

Hypothesis 4.1. *1. $n_i > 0$*

2. For every place v in $T_{\mathbb{Q}}$, we have $\omega(v) = 1$ (i.e. v splits in $k'/\mathbb{Q}$).

Proposition 4.2. *Assuming Hypothesis 4.1, $\delta_T^\omega(U^-_{K',S}) \subseteq U^-_{K',S,T}$. Therefore $\eta_\omega \in U^-_{K',S,T}$.*

Proof. Let $x \in U^-_{K',S}$ and $y = x^{\delta_T^\omega}$. Let $v \in T$ split into $v', \overline{v'}$ in k', let w' be any place of K' above v', and $\overline{w'}$ its conjugate by τ. There is a factor of $(1 - N_{v'}\sigma_{v'}^{-1})$ in δ_T^ω by Lemma 1.1. Hence $w'(y-1) > 0$. But we also have $\overline{w'}(y-1) = w'(y^{-1}-1) = w'((1-y)/y) = w'(1-y) > 0$. Therefore $y \equiv 1 \pmod{w'}$ for all $w' \in T_{K'}$ as required. Setting $x = N_{k'(\zeta_S)/K'}\alpha_S$ proves the second assertion. □

5 Darmon's conjecture

We continue with the notation of §3, and the assumption of Hypotheses 3.1 and 4.1. We will state Darmon's conjecture and deduce a modified version involving T.

The free rank of the $\mathbb{Z}$-module $U^-_{k',S}$ is $n_s + 1$ (the number of primes of S splitting in k'), as may be seen for example by interpreting it as the kernel of the norm map to $U_{k,S,T}$. However $U^-_{k',S}$ is not free as a $\mathbb{Z}$-module since its torsion subgroup is $\{\pm 1\}$. The reader is warned that this appears to have been overlooked in [12, §4]. Accordingly, we assume that either T is empty or $U^-_{k',S,T}$ is torsion free, and we choose a basis $\varepsilon_1, \ldots, \varepsilon_{n_s+1}$ for a maximal free $\mathbb{Z}$-submodule of $U^-_{k',S,T}$, which will have index 2 if $T = \emptyset$. Let $\Gamma := \mathrm{Gal}(k'(\zeta_S)/k') \cong (\mathbb{Z}/S\mathbb{Z})^\times$. Following Darmon, we define a regulator

$$R_{S,T} := \sum_{i=1}^{n_s+1} (-1)^{i+1} \varepsilon_i \otimes \det(f_{\mathfrak{p}_k}(\varepsilon_j))_{k,j} \in U_{k',S,T} \otimes \frac{I_\Gamma^{n_s}}{I_\Gamma^{n_s+1}}, \tag{8.17}$$

where, in the matrix, k runs from 1 to n_s and j runs from 1 to $n_s + 1$, omitting i. Note that $2R_{S,\emptyset}$ is independent of the choice of maximal free subgroup of $U^-_{k',S,T}$.

Relative to the basis $\varepsilon_1, \ldots, \varepsilon_{n_s+1}$ and the ordered list of places $\infty', \mathfrak{p}_1, \ldots, \mathfrak{p}_{n_s}$, we may define a minus-unit regulator $R^- \in \mathbb{R}$ as in (8.9). Note that $(-1)^{\#T}\xi^-$ is the sign of R^- by Hypothesis 4.1 (2). Due to the fact that the logarithmic regulators Darmon uses are the negatives of ours, his assumption [12, (20)] that a regulator be positive corresponds in our notation to the statement that for $T = \emptyset$, we have $\xi^- = (-1)^{n_s+1}$. Instead of assuming this, we will introduce an appropriate sign depending on ξ^- into statements in the style of Chapter 3, §3.

We define a number m_T by $L^{n_s+1}_{k'/k,S,T}(0,\omega) = \xi^- m_T R^-$. The calculation (8.10) shows that in the current setup

$$m_T = \frac{1}{w^-_{k',T}} \frac{h_{k',S,T}}{h_{\mathbb{Q},S,T}} 2^{n_i-1} \# H^1(\langle\tau\rangle, U_{k',S,T}). \tag{8.18}$$

Therefore for $T = \emptyset$ we have

$$m_\emptyset = \frac{1}{w^-_{k',T}} h_{k',S} 2^{n_i-1} \# H^1(\langle\tau\rangle, U_{k',S,T}). \tag{8.19}$$

We study the cohomological factor in this expression.

Lemma 5.1. *Suppose k' is a real quadratic field, and S a set of places of $\mathbb{Q}$ not ramifying in $k'/\mathbb{Q}$. Then $\# H^1(\langle\tau\rangle, U_{k',S}) = 2^{a+b}$, where*

- *$a = 2$ if the fundamental unit of k' has norm 1 and $a = 1$ if it has norm -1;*
- *If C denotes the subgroup of $A_{k'}$ generated by the classes of the primes which ramify in $k'/\mathbb{Q}$, then the kernel of the quotient map $C \to A_{k',S}$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^b$.*

Proof. We abbreviate $H_S = \# H^1(\langle\tau\rangle, U_{k',S})$. Firstly we consider the case where S only consists of the archimedean place. Let u denote the fundamental unit of the real quadratic field k, so that $U_{k'} = \{\pm 1\} \times u^{\mathbb{Z}}$. If the norm of u is 1, then $U^-_{k'} = U_{k'}$ and $U^{1-\tau}_{k'} = u^{2\mathbb{Z}}$, and so $H^1(\langle\tau\rangle, U_{k'}) = U^-_{k'}/U^{1-\tau}_{k'} \cong (\mathbb{Z}/2\mathbb{Z})^2$ and $H_\emptyset = 4$. On the other hand, if the norm of u is -1 then $U^-_{k'} = \{\pm 1\} \times u^{2\mathbb{Z}}$ and $U^{1-\tau}_{k'} = (-u^2)^{\mathbb{Z}}$, so $H_\emptyset = 2$.

We now proceed to consider the integer H_S when S is not empty. There is a natural map $i : \mathcal{I}_{\mathbb{Q}} \to \mathcal{I}_{k'}$ given by $v_p \to e_p \sum_{\mathfrak{p}|p} v_{\mathfrak{p}}$, with e_p the ramification index of the prime p in $k'/\mathbb{Q}$. Considering the quotient $\mathcal{I}^{\langle\tau\rangle}_{k',S}/\mathcal{I}_{\mathbb{Q},S}$, we see that it is a direct product of cyclic groups of order 2, with each cyclic component generated by the class of a prime which ramifies in $k'/\mathbb{Q}$ but does not lie in S. Let C_S denote the image of these ramified $\mathfrak{p}$ in the S-class group $A_{k',S}$, so that $C = C_\emptyset$. Note that C_S is always an elementary abelian 2-group. [36, Thm.] gives a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1(\langle\tau\rangle, U_{k'}) & \longrightarrow & \mathcal{I}^{\langle\tau\rangle}_{k'}/\mathcal{I}_{\mathbb{Q}} & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H^1(\langle\tau\rangle, U_{k',S}) & \longrightarrow & \mathcal{I}^{\langle\tau\rangle}_{k',S}/\mathcal{I}_{\mathbb{Q},S} & \longrightarrow & C_S & \longrightarrow & 0 \end{array}$$

From this we see firstly that if $k'/\mathbb{Q}$ were unramified outside S then we would have $H_S = 1$ (note that this is stated in [22, Lem. 6.7(i)] erroneously because the assumption on S is missing). Since S contains none of the places which ramify in $k'/\mathbb{Q}$, the central vertical arrow of the above diagram is an isomorphism. Therefore, the snake lemma gives that $H^1(\langle\tau\rangle, U_{k',S})/H^1(\langle\tau\rangle, U_{k'}) \cong \ker(C \to C_S)$, which is the intersection of C with the subgroup of $A_{k'}$ generated by classes of primes in $S_{k'}$. Therefore $H_S = H_\emptyset 2^b$. We note that if $h_{k'} = 1$ then $H_S = H_\emptyset = 2^a$. □

This calculation seems to contradict Darmon's assertion [12, (22)], which states (in our notation) that $m_\emptyset = 2^{n_i+1} h_{k',S}$. Noting that [12, §4] wrongly states that $U^-_{k',S}$ is torsion free (i.e. $w^-_{k',S} = 1$), we observe that replacing $w^-_{k',S}$ by 1 in (8.19) gives the same value as [12, (22)] in the case where k' has class number one and the norm of its fundamental unit is 1, or half that value if the norm of the fundamental unit is -1.

Noting the relation [12, Thm. 4.1] of Darmon's element α_S to double the values of derivatives of L-functions, it seems reasonable that the integer factor in Darmon's conjecture should be $2m_\emptyset$, and so that is the value which we use in our statement of the conjecture. This may differ by a power of 2 from the statement in [12]. By the above discussion, our formulation agrees with [12] when k' has class number one and fundamental unit of norm 1. We note that $2m_\emptyset$ is an integer (and $m_\emptyset$ is as well, since we assume Hypothesis 4.1).

Define $\Gamma = \mathrm{Gal}(k'(\zeta_S)/k') \cong (\mathbb{Z}/S\mathbb{Z})^\times$. We state Darmon's conjecture under the ring automorphism involution of $\mathbb{Z}[\Gamma]$ induced by inversion on Γ. Note that the effect of this involution on an element of $I_\Gamma^{n_s}/I_\Gamma^{n_s+1}$ is the same as multiplication by $(-1)^{n_s}$, by repeated application of Corollary 2.6.3. Then Darmon's conjecture [12, Conj. 4.3] states that

Conjecture 5.2 (Darmon). *Let $T = \emptyset$. We have the following equality in $U_{k'(\zeta_S),S} \otimes_{\mathbb{Z}} I_\Gamma^{n_s}/I_\Gamma^{n_s+1}$:*

$$\sum_{\sigma\in\Gamma} \sigma^{-1}\alpha_S \otimes \sigma = \xi^- 2m_\emptyset R_{S,\emptyset}.$$

We consider a T-modified version. This will fit with our general framework, and avoids the problem of torsion in the unit group.

Lemma 5.3. *Under Hypothesis 4.1, m_T is an integer.*

Proof. By Hypothesis 4.1 (2), each v in T splits into w and $\overline{w}$ in k', with $N_w = N_v$. Then by (2.3), we have the following:

$$h_{\mathbb{Q},S,T} = h_{\mathbb{Q},S} \cdot \frac{\prod_{v\in T}(N_v - 1)}{(U_{\mathbb{Q},S} : U_{\mathbb{Q},S,T})}, \qquad h_{k',S,T} = h_{k',S} \cdot \frac{\prod_{v\in T}(N_v - 1)^2}{(U_{k',S} : U_{k',S,T})},$$

where we note $h_{\mathbb{Q},S} = 1$. The quotient is

$$\frac{h_{k',S,T}}{h_{\mathbb{Q},S,T}} = h_{k',S} \cdot \frac{\prod_{v\in T}(N_v - 1)}{(U^{1-\tau}_{k',S} : U^{1-\tau}_{k',S,T})} = h_{k',S} \cdot \frac{\prod_{v\in T}(N_v - 1)}{(U^-_{k',S} : U^-_{k',S,T})} \frac{\#H^1(\langle\tau\rangle, U_{k',S})}{\#H^1(\langle\tau\rangle, U_{k',S,T})},$$

using Lemmas 2.1 and 2.2. Therefore, by (8.18) we have

$$m_T = \frac{1}{w^-_{k',T}} h_{k',S} \cdot \frac{\prod_{v\in T}(N_v - 1)}{(U^-_{k',S} : U^-_{k',S,T})} 2^{n_i - 1} \# H^1(\langle\tau\rangle, U_{k',S}).$$

We have $w^-_{k',T} = 1$ or 2, $n_i - 1 \geq 0$ (by Hypothesis 4.1 (1)) and $2 \mid \# H^1(\langle\tau\rangle, U_{k',S})$ (by Lemma 5.1). Therefore it is sufficient to show that $(U^-_{k',S} : U^-_{k',S,T})$ divides $\prod_{v\in T}(N_v - 1)$.

The natural sequence

$$0 \longrightarrow U^-_{k',S,T} \longrightarrow U^-_{k',S} \longrightarrow \bigoplus_{v\in T} \mathbb{F}^\times_{v'}$$

is exact, where for each v, we choose a place v' of k' arbitrarily above v. To see the exactness, we note that if $u \in U^-_{k',S}$ reduces to 1 modulo each v', then $\overline{v'}(u-1) = v'(\bar{u}-1) = v'((1-u)/u) = v'(1-u) > 0$, as in Proposition 4.2. Hence $u \in U_{k',S,T} \cap U^-_{k',S} = U^-_{k',S,T}$. This shows that $(U^-_{k',S} : U^-_{k',S,T}) \mid \prod_{v\in T}(N_v - 1)$, as required. ☐

We propose the following generalisation of Darmon's conjecture:

Conjecture 5.4. *We have the following equality in $U_{k'(\zeta_S),S,T} \otimes I^{n_s}_\Gamma / I^{n_s+1}_\Gamma$:*

$$\sum_{\sigma\in\Gamma} \sigma^{-1} \alpha_S^{\delta^\omega_T} \otimes \sigma = \xi^- 2 m_T R_{S,T}. \tag{8.20}$$

If we put $T = \emptyset$ in this statement, then we recover Conjecture 5.2. On the other hand, let us look at how Conjecture 5.4 varies when we replace T by $T \cup \{v\}$. If T is empty, then for the comparison statement we will have to assume that the regulator in Conjecture 5.2 is calculated with respect to a maximal free subgroup of $U_{k',S}$ which contains $U_{k',S,\{v\}}$.

Passing from T to $T \cup \{v\}$ has the effect of multiplying the left-hand side of (8.20) by $1 \otimes (1 - N_v \sigma_v^{-1})$, or equivalently its augmentation $1 - N_v$. On the other side, the index of a maximal free $\mathbb{Z}$-submodule of $U_{k',S,T\cup\{v\}}$ in a maximal free $\mathbb{Z}$-submodule of $U_{k',S,T}$ is $y := \frac{(U^-_{k',S,T} : U^-_{k',S,T\cup\{v\}})}{w_{k',T}}$. We have $(1 - N_v)\xi^-_T m_T R^-_T = \xi^-_{T\cup\{v\}} m_{T\cup\{v\}} y R^-_T$, and $R_{S,T\cup\{v\}} = y R_{S,T}$. This shows that equality (8.20) is preserved by enlarging T.

The consequence of Darmon's conjecture that we wish to use is the following.

Proposition 5.5. *Assume the setup of Hypothesis 3.1 and let T satisfy Hypothesis 4.1 (2) with $U_{K',S,T}$ torsion-free. Then Conjecture 5.4 implies that for each $\phi \in \mathrm{Hom}_{\mathbb{Z}[G]}(U_{K',S,T}, \mathbb{Z}[G])$, we have*

$$\phi(\eta_\omega) \equiv \xi^- 2 m_T \phi^1(R_{S,T}) \pmod{I_G^{n_s+1}}.$$

Proof. We apply the natural projection $U_{k'(\zeta_S),S} \otimes \mathbb{Z}[\Gamma] \longrightarrow U_{k'(\zeta_S),S} \otimes \mathbb{Z}[G]$, which maps the left-hand side of (8.20) to $\sum_{\sigma \in G} \sigma^{-1}(\delta_T^\omega N_{k'(\zeta_S)/K'} \alpha_S) \otimes \sigma$ in $U_{K',S} \otimes \mathbb{Z}[G]$. Then Conjecture 5.4 implies the following equality in $U_{K',S} \otimes I_G^{n_s}/I_G^{n_s+1}$:

$$\sum_{\sigma \in G} \sigma^{-1} \eta_\omega \otimes \sigma = \xi^- 2 m_T R_{S,T},$$

with η_ω from Definition 3.3.

We define a homomorphism ϕ^1 corresponding to ϕ as in Lemma 2.6.5. Applying the homomorphism

$$\phi^1 \otimes \mathrm{id} : U_{K',S,T} \otimes I_G^{n_s}/I_G^{n_s+1} \longrightarrow I_G^{n_s}/I_G^{n_s+1}$$

gives the stated result. □

6 Factorisation of the regulator

We assume T is such that $U_{K',S,T}$ is torsion free, and that Hypothesis 4.1 is satisfied. We let $\varepsilon_1, \ldots, \varepsilon_{n_s+1}$ be a basis for $U^-_{k',S,T}$ and $\varepsilon_{n_s+2}, \ldots, \varepsilon_{n'}$ be a basis for $U_{\mathbb{Q},S,T}$. Then these ε_i form a basis for $U_{\mathbb{Q},S,T} U^-_{k',S,T}$. The index of this group in $U_{k',S,T}$ was calculated in Lemma 2.3. We calculate the regulator from Conjecture 3.5.1 for these ε_i. Let $\Phi = \phi_1 \wedge \phi_2 \in \wedge^2_{\mathbb{Z}[G]} \mathrm{Hom}_{\mathbb{Z}[G]}(U_{K',S,T}, \mathbb{Z}[G])$. Let $R_{S,T}$ be the regulator defined in §5 in terms of the ε_i. Write $\boldsymbol{\varepsilon}_{\mathbb{Q}} = \varepsilon_{n_s+2} \wedge \cdots \wedge \varepsilon_{n'}$. We refer to §4 above for the definitions and orderings of the sets S and $S_{k'}$, and the definition of the integers n_s, n_i, n, d, n' and d'.

Proposition 6.1. *We have the following equality in $\mathbb{Z}[G]/I_G^{d'+1}$:*

$$\mathrm{Reg}_{K'/k'}(\tilde{\Phi}(\varepsilon_1 \wedge \cdots \wedge \varepsilon_{n'})) = (-2)^{n_s} \begin{vmatrix} 2^{n_i-1}\phi_1^1(R_{S,T}) & 2^{n_i-1}\phi_2^1(R_{S,T}) \\ \mathrm{Reg}_{K/\mathbb{Q}}(\tilde{\phi}_1(\boldsymbol{\varepsilon}_{\mathbb{Q}})) & \mathrm{Reg}_{K/\mathbb{Q}}(\tilde{\phi}_2(\boldsymbol{\varepsilon}_{\mathbb{Q}})) \end{vmatrix}.$$

Proof. We saw in Lemma 2.5.3 that

$$\tilde{\Phi}(\varepsilon_1 \wedge \cdots \wedge \varepsilon_{n'}) = \sum_{\sigma \in \left[{n' \atop 2}\right]} \mathrm{sign}(\sigma) \begin{vmatrix} \phi_1^1(\varepsilon_{\sigma(1)}) & \phi_2^1(\varepsilon_{\sigma(1)}) \\ \phi_1^1(\varepsilon_{\sigma(2)}) & \phi_2^1(\varepsilon_{\sigma(2)}) \end{vmatrix} \varepsilon_{\sigma(3)} \wedge \cdots \wedge \varepsilon_{\sigma(n')}. \quad (8.21)$$

The terms $\varepsilon_{\sigma(3)} \wedge \cdots \wedge \varepsilon_{\sigma(n')}$ are made by choosing two of the ε_i for the integer determinant. So each σ excludes 0, 1 or 2 units of the $U^-_{k',S,T}$ basis from the wedge of units. Let $m_\sigma = \#(\sigma(\{3, 4, \ldots, n'\}) \cap \{1, \ldots, n_s + 1\})$ be the number of minus-units included in $\varepsilon_{\sigma(3)} \wedge \cdots \wedge \varepsilon_{\sigma(n')}$ in the term corresponding to σ, so $m_\sigma = n_s - 1, n_s$ or $n_s + 1$.

We calculate the matrix determining the map $\mathrm{Reg}_{K'/k'}$ (see Chapter 3, §3) with respect to the following places of k', using Hypothesis 4.1 to exclude $\mathfrak{q}_{n_i}$:

$$\mathfrak{p}_1, \ldots, \mathfrak{p}_{n_s}, \bar{\mathfrak{p}}_1, \ldots, \bar{\mathfrak{p}}_{n_s}, \mathfrak{q}_1, \ldots, \mathfrak{q}_{n_i-1}.$$

This means we have the determinant of the following $d' \times d'$ matrix to calculate for $\mathrm{Reg}_{K'/k'}(\varepsilon_{\sigma(3)} \wedge \cdots \wedge \varepsilon_{\sigma(n')})$:

$$
\begin{array}{c||c|c|c}
 & \mathfrak{p}_1,\ldots,\mathfrak{p}_{n_s} & \bar{\mathfrak{p}}_1,\ldots,\bar{\mathfrak{p}}_{n_s} & \mathfrak{q}_1,\ldots,\mathfrak{q}_{n_i-1} \\
\hline\hline
\begin{matrix}\varepsilon_{\sigma(3)} \\ \vdots \\ \varepsilon_{\sigma(m_\sigma+2)}\end{matrix} & f_{\mathfrak{p}_j}(\varepsilon_i) & f_{\bar{\mathfrak{p}}_j}(\varepsilon_i) & f_{\mathfrak{q}_j}(\varepsilon_i) \\
\hline
\begin{matrix}\varepsilon_{\sigma(m_\sigma+3)} \\ \vdots \\ \varepsilon_{\sigma(n')}\end{matrix} & f_{\mathfrak{p}_j}(\varepsilon_i) & f_{\bar{\mathfrak{p}}_j}(\varepsilon_i) & f_{\mathfrak{q}_j}(\varepsilon_i)
\end{array}
\tag{8.22}
$$

where the units at the top are in $U^-_{k',S,T}$ and the units at the bottom are in $U_{\mathbb{Q},S,T}$. We will distinguish between the cases where m_σ takes the different values.

First consider the case $m_\sigma = n_s + 1$. We may add the column for $\mathfrak{p}_j$ to the column for $\bar{\mathfrak{p}}_j$ for $j = 1, \ldots, n_s$ without altering the value of the determinant. The (i,j)-th entry in the top-centre $(n_s + 1) \times (n_s)$ block is then congruent mod I_G^2 to $f_{\mathfrak{p}_j}(\bar{\varepsilon}_i \varepsilon_i) = 0$. On the other hand, $f_{\mathfrak{q}_j}(\varepsilon_i) = f_{q_j}(\varepsilon_i^{1+\tau})$ under the natural restriction map corresponding to $\mathrm{Gal}(K'/k') \to \mathrm{Gal}(K/\mathbb{Q})$, and so $f_{\mathfrak{q}_j}(\varepsilon_i) = 0$ for these ε_i. Therefore the entire top-right $(n_s + 1) \times (n - 1)$ block is zero. Hence there are at most n_s columns which are nonzero in their first n_s rows. Therefore the determinant is zero.

Now in (8.22) we subtract the $\bar{\mathfrak{p}}_j$ column from the $\mathfrak{p}_j$ column for $j = 1, \ldots, n_s$ to show the determinant is the same as the determinant of the following matrix.

$$
\begin{array}{c||c|c|c}
 & \mathfrak{p}_1,\ldots,\mathfrak{p}_{n_s} & \bar{\mathfrak{p}}_1,\ldots,\bar{\mathfrak{p}}_{n_s} & \mathfrak{q}_1,\ldots,\mathfrak{q}_{n_i-1} \\
\hline\hline
\begin{matrix}\varepsilon_{\sigma(3)} \\ \vdots \\ \varepsilon_{\sigma(m_\sigma+2)}\end{matrix} & f_{\mathfrak{p}_j}(\varepsilon_i) - f_{\bar{\mathfrak{p}}_j}(\varepsilon_i) & f_{\bar{\mathfrak{p}}_j}(\varepsilon_i) & f_{\mathfrak{q}_j}(\varepsilon_i) \\
\hline
\begin{matrix}\varepsilon_{\sigma(m_\sigma+3)} \\ \vdots \\ \varepsilon_{\sigma(n')}\end{matrix} & 0 & f_{\bar{\mathfrak{p}}_j}(\varepsilon_i) & f_{\mathfrak{q}_j}(\varepsilon_i)
\end{array}
\tag{8.23}
$$

If $m_\sigma = n_s - 1$, the first n_s columns have all zeros except perhaps in the first $n_s - 1$ rows. Therefore the determinant is again zero.

We are left with the case $m_\sigma = n_s$. In this case the matrix (8.23) is block-upper-triangular. Let us consider the top-left $n_s \times n_s$ block first. We note that $f_{\mathfrak{p}_j}(\varepsilon_{\sigma(i)}) - f_{\bar{\mathfrak{p}}_j}(\varepsilon_{\sigma(i)}) \equiv 2 f_{\mathfrak{p}_j}(\varepsilon_{\sigma(i)}) \pmod{I_G^2}$. So the top-left block has determinant $2^{n_s} \det(f_{\mathfrak{p}_j}(\varepsilon_{\sigma(i)}))_{i,j}$. Note the relation to the regulator $R_{S,T}$ of (8.17).

Now we calculate the determinant of the bottom-right block. We have $f_{\bar{\mathfrak{p}}_j}(\varepsilon) = f_{p_j}(\varepsilon)$, $f_{\mathfrak{q}_j}(\varepsilon) = f_{q_j}(\varepsilon^2)$ for each j and each ε appearing. So the bottom-right block is $2^{n_i-1}\mathrm{Reg}_{K/\mathbb{Q}}(\varepsilon_{\sigma(m_\sigma+3)} \wedge \cdots \wedge \varepsilon_{\sigma(n')})$.

Referring back to (8.21), the only terms which appear in the sum after applying $\mathrm{Reg}_{K'/k'}$ are those for σ such that $\sigma(1) \leq n_s + 1$ and $\sigma(2) > n_s + 1$. We put this in correspondence with a pair $(i,j), 1 \leq i \leq n_s+1, 1 \leq j \leq d+1$ such that $\sigma(1) = i, \sigma(2) = n_s+1+j$. Then one may check that $\mathrm{sign}(\sigma) = (-1)^{n_s}(-1)^{i+1}(-1)^{j+1}$.

Putting all this together with (8.21) gives the stated result. ☐

7 Base change for the congruence

We are now ready to show the base change statement for Conjecture 3.5.1.

We choose a basis $\varepsilon_1, \ldots, \varepsilon_{n'}$ as in §6. We also choose a basis $u_1, \ldots, u_{n'}$ for $U_{k',S,T}$ such that $u_i = \varepsilon_i$ for $i \geq n_s+2$ (which is possible by Lemma 2.4.3) and, if we write $\mathbf{u} = u_1 \wedge \cdots \wedge u_{n'}$ and $\boldsymbol{\varepsilon} = \varepsilon_1 \wedge \cdots \wedge \varepsilon_{n'}$, that these are similarly oriented in the sense that (8.5) is satisfied. Set $\mathbf{u}_{\mathbb{Q}} = u_{n_s+2} \wedge \cdots \wedge u_{n'}$.

Theorem 7.1. *We use the setup of Hypothesis 3.1 and assume Hypothesis 4.1.*

Assume Conjecture 3.5.1 holds for the extension $K/\mathbb{Q}$, ie. that

$$\phi(\eta_{K/\mathbb{Q}}) \equiv \xi_{\mathbb{Q}} h_{\mathbb{Q},S,T} \mathrm{Reg}_{K/\mathbb{Q}}(\tilde{\phi}(\mathbf{u}_{\mathbb{Q}})) \pmod{I_G^{d+1}},$$

for all $\phi \in \mathrm{Hom}_G(U_{K,S,T}, \mathbb{Z}[G])$. Assume also that the modified Darmon conjecture 5.4 holds. Then Conjecture 3.5.1 holds for the extension K'/k' up to a power of 2. Explicitly, for all $\Phi \in \wedge^2_{\mathbb{Z}[G]} \mathrm{Hom}_{\mathbb{Z}[G]}(U_{K',S,T}, \mathbb{Z}[G])$, we have

$$4 \cdot 2^{n_s} \Phi(\eta_{K'/k'}) \equiv \xi_{k'} 4 \cdot 2^{n_s} h_{k',S,T} \mathrm{Reg}_{K'/k'}(\tilde{\Phi}(\mathbf{u})) \pmod{I_G^{d'+1}}.$$

Proof. Recall from §4 that $4\eta_{K'/k'} = \eta_\omega \wedge \eta_{K/\mathbb{Q}}$. Set (as in Chapter 5) $H := \#H^1(\langle\tau\rangle, U_{k',S,T})$. The conjectures tell us, using Proposition 5.5,

$$\begin{aligned} 4\Phi(\eta_{K'/k'}) &= \begin{vmatrix} \phi_1(\eta_\omega) & \phi_2(\eta_\omega) \\ \phi_1(\eta_{K/\mathbb{Q}}) & \phi_2(\eta_{K/\mathbb{Q}}) \end{vmatrix} \\ &\equiv \begin{vmatrix} \xi^- 2m_T \phi_1^1(R_{S,T}) & \xi^- 2m_T \phi_2^1(R_{S,T}) \\ \xi_{\mathbb{Q}} h_{\mathbb{Q},S,T} \mathrm{Reg}_{K/\mathbb{Q}}(\tilde{\phi_1}(\mathbf{u}_{\mathbb{Q}})) & \xi_{\mathbb{Q}} h_{\mathbb{Q},S,T} \mathrm{Reg}_{K/\mathbb{Q}}(\tilde{\phi_2}(\mathbf{u}_{\mathbb{Q}})) \end{vmatrix} \end{aligned}$$

modulo $I_G^{d+n_s+1}$, where $R_{S,T}$ is calculated with respect to the $\mathbb{Z}$-basis $\varepsilon_1, \ldots, \varepsilon_{n_s+1}$ of $U^-_{k',S,T}$. Noting that $d' = d + n_s$, this is

$$\equiv \xi^- \xi_{\mathbb{Q}} 2m_T h_{\mathbb{Q},S,T} \begin{vmatrix} \phi_1^1(R_{S,T}) & \phi_2^1(R_{S,T}) \\ \mathrm{Reg}_{K/\mathbb{Q}}(\tilde{\phi_1}(\mathbf{u}_{\mathbb{Q}})) & \mathrm{Reg}_{K/\mathbb{Q}}(\tilde{\phi_2}(\mathbf{u}_{\mathbb{Q}})) \end{vmatrix} \pmod{I_G^{d'+1}}.$$

By (8.18), $2m_T h_{\mathbb{Q},S,T} = 2^{n_i} h_{k',S,T} H$. Hence by Proposition 6.1, we have

$$4 \cdot 2^{n_s} \Phi(\eta_{K'/k'}) \equiv \xi^- \xi_{\mathbb{Q}} (-1)^{n_s} h_{k',S,T} \cdot 2H \mathrm{Reg}(\tilde{\Phi}(\boldsymbol{\varepsilon})) \pmod{I_G^{d'+1}}.$$

Now we know from Lemma 2.3 that $(U_{k',S,T} : U_{\mathbb{Q},S,T} U^-_{k',S,T}) = 2^{n_s+1}/H$, so $\boldsymbol{\varepsilon} = (2^{n_s+1}/H)\mathbf{u}$. Therefore

$$4 \cdot 2^{n_s} \Phi(\eta_{K'/k'}) \equiv \xi^- \xi_{\mathbb{Q}} (-1)^{n_s} h_{k',S,T} \cdot 2^{n_s+2} \mathrm{Reg}_{K'/k'}(\tilde{\Phi}(\mathbf{u}_{\mathbb{Q}})) \pmod{I_G^{d'+1}}.$$

Concerning the signs, we note that we may use the results of §2 to compare $\xi_{\mathbb{Q}}, \xi^-$ and $\xi_{k'}$ if we permute the ordering (8.14) of $S_{k'}$ so that it relates to the ordering (8.13) of S in the same way that (8.4) relates to (8.3). This may be achieved by applying a cycle of length n_s+1 to transform the sequence $\overline{\infty}', \mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ into $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n, \overline{\infty}'$, which is a permutation which has sign $(-1)^{n_s}$, corresponding to multiplication by this sign of the regulator $R_{k'}$. Thus, using the results of §2 and noting Hypothesis 4.1, we have $\xi_{k'} = \xi^- \xi_{\mathbb{Q}}(-1)^{n_s}$.

Putting all this together gives the result. □

Note that if $\#G$ is odd, this last congruence is the full statement of Conjecture 3.5.1.

Remark 7.2. Using the method of [12, Lem. 8.1], it is possible to prove that $\phi(N_{k'(\zeta_S)/K'}\alpha_S) \in I_G^{n_s}$ for all $\phi \in \mathrm{Hom}_G(U^-_{k',S}, \mathbb{Z}[G])$, without assuming the validity of Darmon's conjecture. It then follows that $\phi'(\eta_\omega) \in I_G^{n_s}$ for all $\phi' \in \mathrm{Hom}_G(U_{K,S,T}, \mathbb{Z}[G])$. Thus if Conjecture 3.5.1 holds for $K/\mathbb{Q}$, then for K'/k' we have $4\Phi(\eta_{K'/k'}) \in I_G^{d'}$, for all $\Phi \in \wedge^2_{\mathbb{Z}[G]}\mathrm{Hom}_{\mathbb{Z}[G]}(U_{K',S,T}, \mathbb{Z}[G])$, consistent with the "order of vanishing" implied by Conjecture 3.5.1.

8 Gross's conjecture on the L-functions of tori

In [18, §8], Gross makes a conjecture motivated by considering algebraic tori. Similarly to Darmon's later conjecture, this involves a quadratic extension of the base field and consideration of the "minus-units" in this extension. It also involves a "Θ" element which is twisted by the nontrivial character of the extension. In the previous section we saw that Darmon's conjecture, which was related to the first derivative of the relative factor in (8.11), gave us a base change property for Conjecture 3.5.1 where the order of vanishing, r_S, increased by 1. Gross's conjecture, by contrast, concerns the value (zero-th derivative) of the relative factor and correspondingly it gives us a base change property where r_S doesn't change.

Our setup is as follows. Let k be a global field and K/k and k'/k linearly disjoint abelian extensions, with $[k' : k] = 2$. Setting $K' = k'K$, we are in the situation of §1, and we use the notation G, τ, ω from that section. Let $S = S_k$ be a set of places of k containing all infinite places and all places ramifying in K'/k. That is, both K/k *and* k'/k are unramified outside S (and so, in the notation of §1, we have $S' = S$). Take $T = T_k$ such that $U_{K',S,T}$ is torsion free. We assume that $r_S = r_{S'}$, that is, the places splitting completely in K/k do not split in k'/k. We define n_s to be the number of places in S splitting in the quadratic extension k'/k, and refer to the other $\#S - n_s$ inert or ramified places as nonsplit. This is the setup of [18, §8], with slightly different notation in that the objects denoted L, σ, χ and n there are respectively called k', τ, ω and n_s here.

We may order S as follows:

$$S = \{\ \overbrace{v_1, \ldots, v_{r_S},}^{r_S \text{ nonsplit in } k'}\ \overbrace{v_{r_S+1}, \ldots, v_{r_S+n_s},}^{n_s \text{ split in } k'}\ \overbrace{v_{r_S+n_s+1}, \ldots, v_{n+1}}^{d-n_s+1 \text{ nonsplit in } k'}\ \}, \tag{8.24}$$

and then, with v_i' denoting a place of k' above v_i and $\overline{v'}_i := \tau v_i'$, we order

$$S_{k'} = \{v_1', \ldots, v'_{r_S}, v'_{r_S+1}, \ldots, v'_{r_S+n_s}, \overline{v'}_{r_S+1}, \ldots, \overline{v'}_{r_S+n_s}, v'_{r_S+n_s+1}, \ldots, v'_{n+1}\}. \tag{8.25}$$

We impose the following assumption, which is the same as Hypothesis 4.1 (i).

Hypothesis 8.1. *There is a place in S which is nonsplit in k'/k and does not split completely in K/k. That is, $d \geq n_s$.*

We fix a basis $u_1, \ldots, u_{n'}$ of $U_{k',S,T}$ such that $u_{n_s+1}, \ldots, u_{n'}$ is a basis of $U_{k,S,T}$, which is possible by Lemma 2.4.3. Then this basis together with the orderings (8.24) and (8.25) define regulators R_k and $R_{k'}$ as in (3.2). Also, choosing a basis $\varepsilon_1, \ldots, \varepsilon_{n_s}$ for $U^-_{k',S,T}$ such that (8.5) is satisfied defines a minus-unit regulator R^- as in §2.

We wish to apply the results of §2 to compare $R_{k'}$, R_k and R^-. However, we note that the orderings of sets (8.24) and (8.25) are those required for use in Chapter 3, §5 and are not of the form required by §2. Such a form may be achieved by rotating the first $r_S + n_s$ terms of sequence (8.24) left r_S times, and rotating the first $r_S + 2n_s$ terms of sequence (8.25) left r_S times, permutations which have signs $(-1)^{(r_S+n_s+1)r_S}$ and $(-1)^{(r_S+2n_s+1)r_S}$ respectively. Then the results of §2 show that, for $R_{k'}$ and R_k calculated with respect to (8.24) and (8.25), we have $(-1)^{(r_S+2n_s+1)r_S} R_{k'} = (-1)^{(r_S+n_s+1)r_S} 2^{n-n_s} (U_{k',S,T} : U_{k,S,T}) R_k R^-$, where R^- is the minus-unit regulator calculated relative to $\{v'_{r_S+1}, \ldots, v'_{r_S+n_s}\}$. Hence

$$\xi_{k'} = (-1)^{n_s r_S} \xi_k \xi^-. \tag{8.26}$$

By (8.10), the leading term at $s = 0$ of the L-function of the nontrivial character ω of k'/k is

$$L^{n_s}_{k'/k,S,T}(0, \omega) = \xi^- \frac{h_{k',S,T}}{h_{k,S,T}} 2^{n-n_s} R^- \# H^1(\langle\tau\rangle, U_{k',S,T}).$$

The reader is warned that the factor 2^{n-n_s} is missing in [18, (8.5)]. Writing the leading term as $L^{n_s}_{k'/k,S,T}(0,\omega) = \xi^- m_\omega R^-$, so that $(-1)^{n_s} \xi^- m_\omega$ is the number denoted m_τ in [18, (8.4)] (the sign $(-1)^{n_s}$ coming from the differing signs in logarithmic regulators), we have

$$m_\omega = \frac{h_{k',S,T}}{h_{k,S,T}} 2^{n-n_s} \# H^1(\langle\tau\rangle, U_{k',S,T}).$$

Lemma 8.2. *Assuming Hypothesis 8.1, m_ω is an integer.*

Proof. The hypothesis shows that $n - n_S \geq 0$. Also k'/k is a quadratic extension unramified outside S such that at least one place in S is inert. Therefore Lemma 1.4 (i) shows that $h_{k,S,T}$ divides $h_{k',S,T}$. This gives the result. □

We define an algebraic minus-unit regulator $R_G^- \in \mathbb{Z}[G]/I_G^{n_s+1}$ by the determinant of the $n_s \times n_s$ matrix with (i,j)-th entry $f_{v'_{r_S+j}}(\varepsilon_i)$ for $1 \leq i,j \leq n_s$, where the ε_i correspond to the u_i as in (8.5). This R_G^- corresponds to $(-1)^{n_s} \det_G(\lambda_\tau)$ in the notation of [18] (with sign change for the same reason as noted in the discussion following the statement of Conjecture 3.3.2 above).

We can now state Gross's tori conjecture [18, Conj. 8.8], which in our setup, assuming Hypothesis 8.1 in order to have the conclusion of Lemma 8.2, states the following

Conjecture 8.3 (Gross). *We have*

$$\Theta_{K'/k'/k,S,T}(0,\omega) \equiv \xi^- m_\omega R_G^- \pmod{I_G^{n_s+1}}.$$

We now show how the term $\Theta_{K'/k'/k,S,T}(0,\omega)$ appearing in Gross's conjecture relates the Stark units $\eta_{K'/k'}$ and $\eta_{K/k}$. Differentiating the base-change factorisation of the L-functions (8.1) r_S times and evaluating at $s=0$ gives

$$\Theta^{r_S}_{K'/k',S,T}(0) = \Theta_{K'/k'/k,S,T}(0,\omega)\Theta^{r_S}_{K/k,S,T}(0). \tag{8.27}$$

The base-change factor $\Theta_{K'/k'/k,S,T}(0,\omega)$ lies in $\mathbb{Z}[G]$ by the argument following [18, (8.7)], where the corresponding element is denoted $\theta_G(\chi)$. The argument is essentially that, since no places in S split completely in K' by our assumptions, the integrality follows from the integrality of $\Theta_{K'/k,S,T}(0)$ given by Theorem 3.3.1. Gross's tori conjecture concerns $\Theta_{K'/k'/k,S,T}(0,\omega)$, and we will show that its validity would imply that Conjecture 3.5.1 for $K'/k', S_{k'}, T_{k'}$ (weakened by powers of 2, similarly to the case of Darmon's conjecture) follows from the conjecture for $K/k, S, T$.

The place v_{n+1} is inert in k' by Hypothesis 8.1. Choose w'_i a place of K' above v_i for $i = 1, \ldots, n+1$. Set $\mathbf{x}' = (w'_1 - w'_{n+1}) \wedge \cdots \wedge (w'_{r_S} - w'_{n+1})$. Write w_i for the place of K induced by w'_i for $i = 0, \ldots, r_S$, and set $\mathbf{x} = (w_1 - w_{n+1}) \wedge \cdots \wedge (w_{r_S} - w_{n+1})$. Then according to Chapter 2, §1 we have that $\eta_{K/k} \in \mathbb{C} \wedge^{r_S}_{\mathbb{Z}[G]} U_{K,S,T}$ is defined by the equation

$$\lambda_{S_K}(\eta_{K/k}) = \Theta^{r_S}_{K/k,S,T}(0)\mathbf{x}.$$

The commutative diagram (2.5) holds here for the extension K'/K. Since the places $v_1, \ldots, v_{r_S}$ and v_{n+1} are all nonsplit in k'/k, there is a unique w'_i over w_i for $i = 1, \ldots, r_S$ and $i = n+1$. Hence

$$\lambda_{K'}(\eta_{K/k}) = \Theta^{r_S}_{K/k,S,T}(0)\big((2w'_1 - 2w'_{n+1}) \wedge \cdots \wedge (2w'_{r_S} - 2w'_{n+1})\big) = 2^{r_S}\Theta^{r_S}_{K/k,S,T}(0)\mathbf{x}'.$$

Therefore we have, using (8.27), $\lambda_{K'}(\eta_{K/k}^{\Theta_{K'/k'/k,S,T}(0,\omega)}) = 2^{r_S}\Theta^{r_S}_{K'/k',S,T}(0)\mathbf{x}'$. It follows that

$$\eta_{K'/k'} = \frac{1}{2^{r_S}}\eta_{K/k}^{\Theta_{K'/k'/k,S,T}(0,\omega)}. \tag{8.28}$$

9 Base change via the tori conjecture

Keeping the assumptions and notation of the previous section, we now go on to study the regulators involved in the various conjectures.

The analogue of Proposition 6.1 in this situation is the following.

Proposition 9.1. *We have the following in* $\mathbb{Z}[G]/I_G^{d+n_s+1}$*:*

$$\begin{aligned}&\mathrm{Reg}_{K'/k'}(\tilde{\Phi}(u_1 \wedge \cdots \wedge u_{n'})) = \\ &\qquad (-1)^{r_S n_s} 2^{d-n_s} R_G^- \mathrm{Reg}_{K/k}(\tilde{\Phi}(u_{1+n_s} \wedge \cdots \wedge u_{n'})) \# H^1(\langle\tau\rangle, U_{k',S,T}).\end{aligned}$$

Proof. The regulator on the left is

$$\sum_{\sigma \in \left[{n' \atop r_S}\right]} \mathrm{sign}(\sigma) \det\left(\phi_j^1(u_{\sigma(i)})\right)_{1 \le i,j \le r_S} \mathrm{Reg}_{K'/k'}(u_{\sigma(r_S+1)} \wedge \cdots \wedge u_{\sigma(n')}), \tag{8.29}$$

where, after manipulations as in the proof of Proposition 6.1, $\mathrm{Reg}_{K'/k'}(u_{\sigma(r_S+1)} \wedge \cdots \wedge u_{\sigma(n')})$ is seen to be the determinant in $\mathbb{Z}[G]/I_G^{d+n_s+1}$ of the matrix

	$v'_{r_S+1},\dots,v'_{r_S+n}$	$\overline{v'}_{r_S+1},\dots,\overline{v'}_{r_S+n}$	$v'_{r_S+n+1},\dots,v'_{r_S+n+d}$
$u_{\sigma(r_S+1)}$ $\vdots$ $u_{\sigma(r_S+m_\sigma)}$	$f_{v'_j}(u_i^{1-\tau})$	$f_{\overline{v'_j}}(u_i)$	$f_{v'_j}(u_i)$
$u_{\sigma(r_S+m_\sigma+1)}$ $\vdots$ $u_{\sigma(r_S+d+n)}$	0	$f_{v_j}(u_i)$	$2(f_{v_j}(u_i))$

in which $m_\sigma = \#[\sigma(\{r_S+1,\dots,n'\}) \cap \{1,\dots,n_s\}]$. Now if $m_\sigma < n_s$ then this determinant is clearly 0. So for nonzero terms in the sum (8.29) we must have $m_\sigma = n_s$, ie. $\sigma(r_S+1) = 1, \dots, \sigma(r_S+n_s) = n_s$. The determinant of the top left $n_s \times n_s$ block is $(U^-_{k',S,T} : U^{1-\tau}_{k',S,T})R_G^-$ (where the sign has been fixed by (8.5)). The determinant of the bottom-right $d \times d$ block is $2^{d-n_s}\mathrm{Reg}_{K/k}(u_{\sigma(r_S+n_s+1)} \wedge \cdots \wedge u_{\sigma(n')})$.

Note that for such σ, the map $\sigma \circ (1 \quad 2 \quad \dots \quad r_S+n_s)^{r_S}$ is a permutation of $\{n_s+1,\dots,n'\}$ of the form $n_s+k \mapsto n_s+\sigma'(k)$ for $\sigma' \in \left[{n \atop r_S}\right]$. Thus $\mathrm{sign}(\sigma) = (-1)^{r_S(r_S+n_s+1)}\mathrm{sign}(\sigma') = (-1)^{r_S n_s}\mathrm{sign}(\sigma')$, since $(-1)^{r_S(r_S+1)} = 1$. We have

$$\begin{aligned}\mathrm{Reg}_{K'/k'}(\tilde{\Phi}(u_1 \wedge \cdots \wedge u_{n'})) &= 2^{d-n_s}(U^-_{k',S,T} : U^{1-\tau}_{k',S,T})R_G^- \sum_{\sigma'}\Big((-1)^{r_S n_s}\mathrm{sign}(\sigma') \\ &\det\left(\phi_j^1(u_{n_s+\sigma'(i)})\right)_{1\le i,j\le r_S} \mathrm{Reg}_{K/k}(u_{n_s+\sigma'(r_S+1)} \wedge \cdots \wedge u_{n_s+\sigma'(r_S+d)})\Big),\end{aligned}$$

which gives the result. □

We may now give the base-change theorem.

Theorem 9.2. *Let $K/k, k'/k$ be finite linearly disjoint abelian extensions of a global field k, with $[k' : k] = 2$. Set $K' = k'K$. Assume $S = S_k$, $T = T_k$ are such that K'/k is unramified outside S and $U_{K',S,T}$ is torsion-free. Assume that $r_{S_{k'}} = r_S$, and that Hypothesis 8.1 holds for these data.*

Assume that Conjecture 3.5.1 holds for $K/k, S, T$ and that Conjecture 8.3 holds. Then for all $\Phi \in \wedge^{r_S}_{\mathbb{Z}[G]} \mathrm{Hom}_{\mathbb{Z}[G]}(U_{K',S,T}, \mathbb{Z}[G])$ we have

$$2^{r_S}\Phi(\eta_{K'/k'}) \equiv \xi_{k'} 2^{r_S} h_{k',S,T}(\mathrm{Reg}_G \circ \tilde{\Phi}) \pmod{I_G^{d'+1}}.$$

That is, the conclusion of Conjecture 3.5.1 for $K'/k', S_{k'}, T_{k'}$ holds with a factor of 2^{r_S} on each side.

Proof. By (8.28) we have $2^{r_S}\Phi(\eta_{K'/k'}) = \Theta_{K'/k'/k,S,T}(0,\omega)\Phi(\eta_{K/k})$. Multiplying the congruences of Conjecture 8.3 and Conjecture 3.5.1 gives

$$\begin{aligned} 2^{r_S}\Phi(\eta_{K'/k'}) &\equiv \xi^- \frac{h_{k',S,T}}{h_{k,S,T}} 2^{n-n_s}(U^-_{k',S,T} : U^{1-\tau}_{k',S,T}) R^-_G \cdot \\ &\qquad \xi_k h_{k,S,T} \mathrm{Reg}_{K/k}(\tilde{\Phi}(u_{1+n_s} \wedge \cdots \wedge u_{n'})) \pmod{I_G^{d+n_s+1}} \\ &\equiv \xi_{k'} 2^{r_S} h_{k',S,T} \mathrm{Reg}_{K'/k'}(\tilde{\Phi}(u_1 \wedge \cdots \wedge u_{n'})) \pmod{I_G^{d'+1}}, \end{aligned}$$

by the regulator calculation in Proposition 9.1. Note that for the last congruence we have used (8.26). ☐

Note that if $r_S = 0$ then this shows that, under Hypothesis 8.1, Gross's conjecture on tori actually gives a base-change property with no weakening factor for [18, Conj. 4.1].

Chapter 9

The augmentation filtration

Let G be a finite abelian group, and $\mathbb{Z}[G]$ its integral group ring. Recall from Chapter 2, §6 that the augmentation ideal $I_G \subseteq \mathbb{Z}[G]$ is the kernel of the augmentation map $\mathrm{aug} : \mathbb{Z}[G] \to \mathbb{Z}$. The powers I_G^d form a filtration of $\mathbb{Z}[G]$ by ideals. We note that Conjecture 3.3.2 and its generalisation, Conjecture 3.5.1, predict that a certain element of $\mathbb{Z}[G]$ should belong to some I_G^d and satisfy a congruence modulo the ideal I_G^{d+1}. The latter is equivalent to giving a value for its projection to the quotient I_G^d/I_G^{d+1}. In Chapter 5, §3, we make use of the fact that for G a group with two elements, I_G^d/I_G^{d+1} is a group with two elements; this is one example where it is useful to know about the structure of the quotients I_G^d/I_G^{d+1}. In this chapter we summarise some facts about this structure and give the results of a computer investigation which determined this structure for some small groups G.

By [31, Prop. 3.25 (ii)], the quotients I_G^d/I_G^{d+1} decompose as

$$I_G^d/I_G^{d+1} \cong \bigoplus_p I_{G_p}^d/I_{G_p}^{d+1}$$

where G_p is the Sylow p-subgroup of G, so to address questions of structure it is sufficient to assume that G is a p-group. We assume this from now on. For p-groups, useful structural results are known when G is cyclic (e.g. [31, Thm. 3.1]), where we have $I_G^d/I_G^{d+1} \cong G$ for all $d > 0$, and if G is elementary (i.e. exponent p) there is a useful and fairly explicit description in terms of quotients of polynomial rings given by [33, §3]. Therefore we will consider the case where G is not cyclic and has exponent bigger than p.

If H is a subgroup of G, there is a natural surjective homomorphism $\mathbb{Z}[G] \longrightarrow \mathbb{Z}[G/H]$. One might hope that it is sufficient in our case to study the image of I_G^d in those quotient rings for which G/H is cyclic, where the structure is well understood. David Burns and Joongul Lee have asked (in private correspondence) whether

$$I_G^d/I_G^{d+1} \longrightarrow \prod_H I_{G/H}^d/I_{G/H}^{d+1} \tag{9.1}$$

is an injection, which is the same as saying that if $x \in \mathbb{Z}[G]$ is in $I_{G/H}^{d+1}$ after projection to each $\mathbb{Z}[G/H]$, then it is in I^{d+1}. This is known to be true in the elementary case [25, Cor. 5] and obviously in the cyclic case. In fact, it turns out not to be true in general. We will study an example where it fails. This means that, in studying Conjectures 3.3.2 and 3.5.1, it is not sufficient to consider only cyclic subextensions L/k of K/k.

The calculations were carried out on a computer, using the matrix manipulation provided by the PARI system [30].

1 Method

Let f be the number of cyclic factors of G and fix a generator $a_i \in G$ for the i-th factor.

Fix an ordering of the elements of G, $g_1, \ldots, g_{\#G}$. Such an ordering gives us an obvious isomorphism of $\mathbb{Z}$-modules

$$\begin{array}{ccc} \mathbb{Z}[G] & \longrightarrow & \mathbb{Z}^{\#G} \\ \sum_i n_i g_i & \longmapsto & (n_i)_i. \end{array}$$

Via this isomorphism we can use linear algebra to study the structure of the augmentation filtrations. Multiplication by an element $x \in \mathbb{Z}[G]$ induces a $\mathbb{Z}$-endomorphism of $\mathbb{Z}[G]$ by $x \sum_i n_i g_i = \sum_i (\sum_j m_{ij} n_j) g_i$, that is, $xy = A_x y$ where $(A_x)_{ij} = m_{ij}$ and y is considered as a vector in $\mathbb{Z}^{\#G}$. On the other hand, for an integer $d \geq 1$, the d-th power I_G^d of the augmentation ideal is generated over $\mathbb{Z}[G]$ by the finite set

$$S = \{(a_1 - 1)^{r_1}(a_2 - 1)^{r_2} \cdots (a_f - 1)^{r_f} : \, r_i \geq 0, \; r_1 + \ldots + r_f = d\}.$$

Therefore the $\mathbb{Z}$-submodule $I_G^d \subseteq \mathbb{Z}[G]$ is equal to the $\mathbb{Z}$-span of the columns of the matrix $A' = (A_{x_1} | \cdots | A_{x_{\#S}})$ where x_i runs through the elements of S. Given A', there exists a unique matrix $M_{I_G^d}$ in *Hermite Normal Form* [10, §2.4.2] whose column span over $\mathbb{Z}$ is the same as that of A'. The columns of $M_{I_G^d}$ form a basis for the free $\mathbb{Z}$-module I_G^d. We observe that the rank of $M_{I_G^d}$ is always $\#G - 1$, since this may easily be seen to be the rank of I_G^1, and the quotients I_G^d / I_G^{d+1} are finite.

For any $d \geq 1$, the $\mathbb{Z}$-module I_G^{d+1} is a submodule of I_G^d with finite index. Thus it is possible to express the basis $M_{I_G^{d+1}}$ of I_G^{d+1} in terms of the basis $M_{I_G^d}$ of I_G^d as $M_{I_G^{d+1}} = M_{I_G^d} B$, where B is some $(\#G - 1)$-square matrix with integer entries. B may now be reduced to Smith normal form by elementary row and column operations. If U, V are square invertible matrices over $\mathbb{Z}$ such that $UBV = \mathrm{diag}(d_1, \ldots, d_{\#G-1})$ with $d_1 \mid d_2 \mid \ldots \mid d_{\#G-1}$, d_i positive integers, then $I_G^d / I_G^{d+1} \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_{\#G-1}\mathbb{Z}$ and the columns of $M_{I_G^d} U^{-1}$ are generators of each cyclic factor. In this way the structure of the I_G^d / I_G^{d+1} and a minimal set of representatives in $\mathbb{Z}[G]$ were determined.

We now do some simple manipulations useful for studying the augmentation filtrations, relating to cyclic groups or subgroups. Let $g \in G$ have order n and write $N_g = \sum_{i=0}^{n-1} g^i$. Then the following equalities are easy to check:

$$(g-1)N_g = 0 \tag{9.2}$$

$$(g-1)(-g^{n-2} - 2g^{n-3} - 3g^{n-4} - \ldots - (n-2)g - (n-1)) = n - N_g \tag{9.3}$$

$$(g-1)(n - N_g) = n(g-1) \tag{9.4}$$

This shows that $n(g-1) \in I_G^2$, and in particular it proves that I_G^d/I_G^{d+1} is annihilated by the exponent of G for $d \geq 1$.

It is easy to "divide" by the augmentation element $(g-1)$ in $I_{\langle g \rangle}$. If $y = \sum_{i=0}^{n-1} y_i g^i$ is an element with augmentation 0, then $y = (g-1)x$ where $x = -(y_0) - (y_0 + y_1)g - \ldots - (y_0 + \ldots + y_{n-2})g^{n-2}$. Also, by (9.2) we may add multiples of N_g to x until its augmentation is in the range $0 \leq \operatorname{aug} x < n$. This is then uniquely determined by y, and it tells us whether y is in I_G^2 by the next result.

Proposition 1.1. *Let Γ be a cyclic group of order p^m generated by γ. Then every $x \in \mathbb{Z}[\Gamma]$ has a unique expression*

$$x = \sum_{i=0}^{\infty} x_i(\gamma - 1)^i$$

with $0 \leq x_i < p^m$ for $i > 0$.

Proof. Such an expression exists, with $x_0 = \operatorname{aug}(x)$, by the "division" process described above. Suppose $\sum x_i'(\gamma-1)^i$ is a different expression for x. Let r be the first i where $x_i' \neq x_i$ and assume (without loss of generality) that $0 < t := x_i' - x_i$. Then $t(\gamma-1)^r \in I_\Gamma^{r+1}$. But multiplication by $\gamma - 1$ induces an isomorphism $I_\Gamma^d \longrightarrow I_\Gamma^{d+1}$ for all $d \geq 1$ (see eg. [26, Lem. 3]). Hence $t(\gamma - 1) \in I_\Gamma^2$. But this means $\gamma^t = 1$ in G, which is impossible since $0 < t < p^m$. Hence the expression for x is unique. ☐

Thus we see that by iterating the above process we can find the highest power of the augmentation ideal containing a given element of $\mathbb{Z}[\langle g \rangle]$. This method is used to determine the kernel of the map (9.1).

2 Results

We first show that the map (9.1) is not always injective.

Let $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ be the smallest odd, non-elementary, non-cyclic p-group. Write $a = (1,0)$ and $b = (0,1)$ for the generators of the first and second cyclic factors respectively. We will first determine all the nontrivial cyclic quotients of G. The subgroups H such that G/H is cyclic are easily seen to be the kernels of the characters $\chi : G \longrightarrow \mathbb{C}^\times$. Since G has exponent 9, the image of any χ is contained in the group of ninth roots of unity, which is isomorphic to $\mathbb{Z}/9\mathbb{Z}$. So we consider all homomorphisms $\omega : G \longrightarrow \mathbb{Z}/9\mathbb{Z}$.

We have either $\omega(a) = 0$, 3 or 6. Firstly assume $\omega(a) = 0$, so $b \in H := \ker \omega$. The order of $\omega(b)$ is either 1, 3 or 9. If $\omega(b) = 0$ then $H = G$ gives the trivial quotient, which we denote by Γ_0. If $\omega(b)$ has order 3 then $H = \langle a, b^3 \rangle$ giving quotient Γ_1. Otherwise $H = \langle a \rangle$, giving quotient Γ_2.

Note that the Galois group $\mathfrak{G} = (\mathbb{Z}/9\mathbb{Z})^\times$ acts on $\mathbb{Z}/9\mathbb{Z}$ and permutes the ω, the kernel H being an invariant of the orbit. Every character with $\omega(a) = 6$ is in the same orbit as a character with $\omega(a) = 3$ by the action of $-1 \in \mathfrak{G}$. So we may assume $\omega(a) = 3$ to find the rest of the kernels. Now the possible $\mathfrak{G}$-orbits of $\omega(b)$ are $\{0\}$, $\{1, 4, 7\}$, $\{2, 5, 8\}$,$\{3\}$ and $\{6\}$, giving subgroups as follows:

$\omega(b)$	0	1	2	3	6
H	$\langle b \rangle$	$\langle a^2 b^3 \rangle$	$\langle a b^3 \rangle$	$\langle a^2 b \rangle$	$\langle ab \rangle$
G/H name	Γ_3	Γ_4	Γ_5	Γ_6	Γ_7

Thus there are 7 nontrivial cyclic quotients $\Gamma_1, \ldots, \Gamma_7$.

We now present an element which shows that the map (9.1) is not injective for $d = 5$. Let

$$x := 2(a-1)^2(b-1)^3 + (a-1)^4(b-1).$$

Then $x \in I_G^5$ is clear. It is also clear that x projects to 0 in $\mathbb{Z}[\Gamma_1], \mathbb{Z}[\Gamma_2]$ and $\mathbb{Z}[\Gamma_3]$ since the corresponding H contains a or b. So we wish to show it projects to an element of $I_{\Gamma_i}^6$ in $\mathbb{Z}[\Gamma_i]$ for $i = 4, 5, 6, 7$. In the following table, $\bar{x}$ denotes the projection of x in $\mathbb{Z}[\Gamma_i]$ in terms of a chosen generator σ of Γ_i, the choice of which is also indicated in the table.

Quotient	σ	$\#\Gamma_i$	$\bar{x}$
Γ_4	$\bar{b}$	9	$(\sigma-1)^6(12 + 15\sigma + 10\sigma^2 + \sigma^3 - 9\sigma^4$ $-14\sigma^5 - 13\sigma^6 - 6\sigma^7 + 4\sigma^8)$
Γ_5	$\bar{b}$	9	$(\sigma-1)^6(5 - 3\sigma - 8\sigma^2 - 9\sigma^3 - 6\sigma^4$ $-2\sigma^5 + 4\sigma^6 + 9\sigma^7 + 10\sigma^8)$
Γ_6	$\bar{a}$	3	$(\sigma-1)^6(-1 + \sigma^2)$
Γ_7	$\bar{a}^2$	3	$(\sigma-1)^6$

Therefore x is in the kernel of the map (9.1). On the other hand, x is not in I_G^6. This is proved as follows: the matrix $M_{I_G^6}$ whose columns form a Hermite normal form basis for the $\mathbb{Z}$-module $I^6 \subseteq \mathbb{Z}[G]$ has top-right entry -51. But reducing the matrix $(M_{I_G^6}|x)$ to Hermite normal form produces a matrix with top-right entry -53. Because the Hermite normal form is an invariant of the $\mathbb{Z}$-span of the columns of the matrix, this shows that $x \notin I_G^6$. Therefore x is a nontrivial element of the kernel of the map (9.1).

We remark furthermore that all the proper quotients of G are cyclic or elementary. Since the map (9.1) is known to be injective for G elementary, this shows that $x \in I_{G/H}^6$ for *all* proper subgroups H.

The following table shows the structure of the first few augmentation quotients for some small p-groups. The notation $C_a^b C_c^d$ is short for $(\mathbb{Z}/a\mathbb{Z})^b \times (\mathbb{Z}/c\mathbb{Z})^d$. K denotes the kernel of the map (9.1). Where the size of K is not recorded it is equal to 1.

We observe that it is proved in [1] that the structure of the quotients I_G^d/I_G^{d+1} is eventually constant. This can be seen in the following table for the smaller groups.

G	$\#G$	I_G^2/I_G^3	I_G^3/I_G^4	I_G^4/I_G^5	I_G^5/I_G^6	I_G^6/I_G^7	I_G^7/I_G^8
C_2C_4	8	$C_2^2C_4$	$C_2^3C_4$	$C_2^3C_4$	$C_2^3C_4$	$C_2^3C_4$	$C_2^3C_4$
C_4C_4	16	C_4^3	$C_2C_4^3$	$C_2^2C_4^3$	$C_2^3C_4^3$	$C_2^3C_4^3$	$C_2^3C_4^3$
C_2C_8	16	$C_2^2C_8$	$C_2^3C_8$	$C_2^4C_8$ $\#K=2$	$C_2^4C_8$ $\#K=2$	$C_2^4C_8$ $\#K=2$	$C_2^4C_8$ $\#K=2$
$C_2C_2C_4$	16	$C_2^5C_4$	$C_2^8C_4$	$C_2^9C_4$ $\#K=2$	$C_2^9C_4$ $\#K=2$	$C_2^9C_4$ $\#K=2$	$C_2^9C_4$ $\#K=2$
C_4C_8	32	$C_4^2C_8$	$C_4^3C_8$	$C_2C_4^3C_8$	$C_2^2C_4^3C_8$	$C_2^3C_4^3C_8$ $\#K=2$	$C_2^4C_4^3C_8$ $\#K=4$
$C_2C_4C_4$	32	$C_2^3C_4^3$	$C_2^7C_4^3$	$C_2^{10}C_4^3$ $\#K=2$	$C_2^{12}C_4^3$ $\#K=4$	$C_2^{13}C_4^3$ $\#K=8$	$C_2^{13}C_4^3$ $\#K=8$
C_8C_8	64	C_8^3	$C_4C_8^3$	$C_4^2C_8^3$	$C_4^3C_8^3$	$C_2C_4^3C_8^3$ $\#K=2$	$C_2^2C_4^3C_8^3$ $\#K=4$
C_3C_9	27	$C_3^2C_9$	$C_3^3C_9$	$C_3^4C_9$	$C_3^5C_9$ $\#K=3$	$C_3^5C_9$ $\#K=3$	$C_3^5C_9$ $\#K=3$
C_9C_9	81	C_9^3	C_9^4	$C_3C_9^4$	$C_3^2C_9^4$	$C_3^3C_9^4$	$C_3^4C_9^4$
C_3C_{27}	81	$C_3^2C_{27}$	$C_3^3C_{27}$	$C_3^4C_{27}$	$C_3^5C_{27}$ $\#K=3$	$C_3^6C_{27}$ $\#K=9$	$C_3^7C_{27}$ $\#K=27$
C_9C_{27}	243	$C_9^2C_{27}$	$C_9^3C_{27}$	$C_9^4C_{27}$	$C_9^5C_{27}$ $\#K=3$	$C_3C_9^5C_{27}$ $\#K=3$	$C_3^2C_9^5C_{27}$ $\#K=3$
C_5C_{25}	125	$C_5^2C_{25}$	$C_5^3C_{25}$	$C_5^4C_{25}$	$C_5^5C_{25}$	$C_5^6C_{25}$	$C_5^7C_{25}$ $\#K=5$

We see that K may in general be nontrivial but tends to be very small compared to the size of the group.

Bibliography

[1] F. Bachmann and L. Grünenfelder, *The periodicity in the graded ring associated with an integral group ring*, J. Pure and Applied Algebra **5** (1974), 253–264.

[2] W. Bley, *Wild Euler systems of elliptic units and the equivariant Tamagawa number conjecture*, to appear in J. Reine Angew. Math. (2004).

[3] W. Bley and D. Burns, *Explicit units and the equivariant Tamagawa number conjecture*, Amer. J. Math. **123** (2001), 931–949.

[4] D. Burns and M. Flach, *On Galois structure invariants associated to Tate motives*, Amer. J. Math. **120** (1998), no. 6, 1343–1397.

[5] D. Burns and M. Flach, *Tamagawa numbers for motives with (non-commutative) coefficients*, Doc. Math. **6** (2001), 501–570.

[6] D. Burns, *Equivariant Tamagawa numbers and refined abelian Stark conjectures*, J. Math. Soc. Univ. Tokyo **10** (2003), 225–259.

[7] D. Burns, *Congruences between derivatives of abelian L-functions at $s = 0$*, Preprint (2004).

[8] D. Burns, C. Popescu, J. Sands, D. Solomon (eds.), *Proceedings of the conference on Stark's conjecture and related topics*, Contemporary Math., American Mathematical Society (2004).

[9] H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton Math. Ser. **19**, Princeton (1956).

[10] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics **193**, Springer Verlag (2000).

[11] S. Chaiken and D. J. Kleitman, *Matrix tree theorems*, J. Combinatorial Theory (Ser. A) **24** (1978), 377–381.

[12] H. Darmon, *Thaine's method for circular units and a conjecture of Gross*, Canadian J. Math. **47** (1995) 302–317.

[13] P. Deligne and K. Ribet, *Values of abelian L-functions at negative integers over totally real fields*, Invent. Math. **59** (1980), 227–286.

[14] F. Gerrish, *Surjections from an m-set to an n-set*, Mathl. Gaz. **63** (1979), No. 426, 259–260.

[15] D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihre Grenzgebiete, 3. Folge, Bd 35, Springer Verlag (1996).

[16] H. W. Gould, *Euler's formula for nth differences of powers*, Amer. Mathl. Monthly **85** (1978), 450–467.

[17] C. Greither and R. Kučera, *The lifted root number conjecture for fields of prime degree over the rationals: an approach via trees and Euler systems*, Ann. Inst. Fourier **53** (2002), no. 3, 735–777.

[18] B. H. Gross, *On the values of abelian L-functions at s=0*, J. Fac. Sci. Univ. Tokyo, Sect 1A, Math. **35** (1988) 177–197.

[19] B. H. Gross and M. Rosen, *Fourier series and the special values of L-functions*, Adv. Math. **69** (1988), 1–31.

[20] D. Hayes, *Explicit class field theory in global function fields*, Adv. in Math. Suppl. Stud. **6**, Academic Press (1979), 173–217.

[21] D. Hayes, *Stickelberger elements in function fields*, Compos. Math. **55** (1985), 209–239.

[22] A. Hayward, *A class number formula for higher derivatives of abelian L-functions*, Compos. Math. **140** (2004) 99–129.

[23] S. Lang, *Algebraic Number Theory*, Second Edition, Graduate Texts in Mathematics **110**, Springer Verlag (1994).

[24] S. Lang, *Algebra* (revised 3rd ed.), Graduate Texts in Mathematics **211**, Springer Verlag (2002).

[25] J. Lee, *On Gross's refined class number formula for elementary abelian extensions*, J. Math. Sci. Univ. Tokyo **4** (1997), 373–383.

[26] J. Lee, *Stickelberger element for cyclic extensions and the order of vanishing of abelian L-functions at $s = 0$*, Compos. Math. **138** (2003), no. 2, 157–163.

[27] J. Martinet, *Character theory and Artin L-functions*, in *Algebraic Number Fields*, ed. A. Fröhlich, Academic Press (1977).

[28] J. Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften **322**, Springer Verlag (1999).

[29] H. Oukhaba, *Index formulas for ramified elliptic units*, Compos. Math. **137** (2003), 1–22.

[30] The PARI Group, *PARI, Version 2.1.4*, Bordeaux (2002), (available from `http://pari.math.u-bordeaux.fr/`).

[31] I. B. S. Passi, *Polynomial maps on groups*, J. Algebra **9** (1968), 121–151.

[32] I. B. S. Passi, *Polynomial functors*, Proc. Cambridge Philos. Soc. **66** (1972), 25–32.

[33] I. B. S. Passi and L. R. Vermani, *The associated graded ring of an integral group ring*, Math. Proc. Camb. Phil. Soc. **82** (1977), 25–33.

[34] C. D. Popescu, *Base change for Stark-type conjectures "Over $\mathbb{Z}$"*, J. Reine und Angew. Math. **542** (2002) 85–111.

[35] M. Reid, *Gross' conjecture for extensions ramified over three points of* $\mathbb{P}^1$, J. Math. Sci. Univ. Tokyo **10** (2003), no. 1, 119–138.

[36] D. S. Rim, *An exact sequence in Galois cohomology*, Proc. Amer. Math. Soc. **16** (1965), 837–840.

[37] G. Robert, *Concernant la relation de distribution satisfaite par la fonction φ associée à un réseau complexe*, Invent. Math. **100** (1990) 231–357.

[38] G. Robert, *Concernant la relation de distribution satisfaite par la fonction φ associée à un réseau complexe*, Invent. Math. **100** (1990) 231–357.

[39] K. Rubin, *A Stark conjecture "over $\mathbb{Z}$" for abelian L-functions with multiple zeros*, Ann. Inst. Fourier **46** (1996) 33–62.

[40] R. Schertz, *Galoismodulstruktur und elliptische Funktionen*, J. Number Theory **39** (1991), no. 3, 285–326.

[41] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics **67**, Springer Verlag (1979).

[42] H. M. Stark, *Values of L-functions at $s = 1$. I. L-functions for quadratic forms*, Adv. Math. **7** (1971), 301–343.

[43] H. M. Stark, *L-functions at $s = 1$. II. Artin L-functions with rational characters*, Adv. Math. **17** (1975), no. 1, 60–92.

[44] H. M. Stark, *L-functions at $s = 1$. III. Totally real fields and Hilbert's twelfth problem*, Adv. Math. **22** (1976), no. 1, 64–84.

[45] H. M. Stark, *L-functions at $s = 1$. IV. First derivatives at $s = 0$*, Adv. Math. **35** (1980), 197–235.

[46] J. T. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en s=0*, Progress in Mathematics **47**, Birkhäuser (1984).

[47] L. C. Washington, *Introduction to cyclotomic fields*, Second Edition, Graduate Texts in Mathematics **83**, Springer Verlag (1997).

[48] H. Weber, *Lehrbuch der Algebra*, 2. Auflage, 3. Band, Vieweg und Sohn (1908).

[49] A. Weil, *Basic Number Theory*, Grundlehren der mathematischen Wissenschaften **144**, Springer Verlag (1967).