Verifying the Congruence Conjecture for Rubin-Stark Elements

X.-F. Roblot
Université de Lyon, Université Claude Bernard Lyon 1
Institut Camille Jordan, CNRS – UMR 5208
roblot@math.univ-lyon1.fr

D. Solomon
King's College, London
david.solomon@kcl.ac.uk

June 19, 2008

Abstract

The 'Congruence Conjecture' was developed by the second author in a previous paper [So3]. It provides a conjectural explicit reciprocity law for a certain element associated to an abelian extension of a totally real number field whose existence is predicted by earlier conjectures of Rubin and Stark. The aim of the present paper is to design and apply techniques to numerically investigate the Congruence Conjecture.

1 Introduction

The primary purpose of this paper is to provide numerical evidence for the 'Congruence Conjecture'. This first appeared as Conjecture 5.4 of [So2] but we shall refer here to the improved and generalised version appearing as $CC(K/k, S, p, n)$ in [So3]. Thus K/k denotes an abelian extension of number fields, S a finite set of places of k, p an *odd* prime number and n an integer, $n \geq -1$. We suppose that k is totally real of degree d and that K is of CM type and contains $\xi_{p^{n+1}} := \exp(2\pi i/p^{n+1})$. (More precise conditions on S will be explained later.) In this set-up, we can say that the CC is a conjectural, *p-adic, explicit reciprocity law for the so-called Rubin-Stark element* $\eta_{K^+/k,S}$. We recall that $\eta_{K^+/k,S}$ is a particular element of a certain dth exterior power of the global S-units of K^+ (tensored with $\mathbb{Q}$) which is predicted to exist by Stark's conjectures, as reformulated and refined by Rubin in [Ru]. It is uniquely determined by the dth derivatives at $s = 0$ of the S-truncated Artin L-functions of even characters of $\mathrm{Gal}(K/k)$.

By way of illustration, consider the simplest case $K/k = \mathbb{Q}(\xi_{p^{n+1}})/\mathbb{Q}$, $S = \{\infty, p\}$ (so $d = 1$). One can then prove that $\eta_{K^+/k,S}$ exists and equals $-\frac{1}{2} \otimes (1 - \xi_{p^{n+1}})(1 - \xi_{p^{n+1}}^{-1})$. Moreover, the CC then reduces to the explicit reciprocity law proven by Artin and Hasse in [A-H]. This is a precise formula for the Hilbert symbol $(1 - \xi_{p^{n+1}}, u)_{K_{\mathfrak{P}}, p^{n+1}}$, for any $u \in U^1(K_{\mathfrak{P}})$, which involves the p-adic logarithms of the conjugates of u over $\mathbb{Q}_p$. (Here $K_{\mathfrak{P}}$ denotes the completion of K at the unique prime $\mathfrak{P}$ dividing p and $U^1(K_{\mathfrak{P}})$ its group of principal units.)

For the general case of the CC one must replace u by an element θ of a certain dth exterior power of $U^1(K_p)$ (the principal, p-semilocal units of K). From θ and $\eta_{K^+/k,S}$ one forms a $d \times d$ determinant of (additive, group-ring-valued) Hilbert symbols. The conjectural reciprocity law takes the form of a congruence modulo p^{n+1} between this determinant and $\mathfrak{s}_{K/k,S}(\theta)$ (for any θ), where $\mathfrak{s}_{K/k,S}$ is a map defined explicitly in [So3] and [So2] using a certain p-adic regulator and the values at $s = 1$ of the S-truncated Artin L-functions of odd characters of $\mathrm{Gal}(K/k)$. More details of $\eta_{K^+/k,S}$, this determinant, the map $\mathfrak{s}_{K/k,S}$ and the precise formulation of $CC(K/k, S, p, n)$ are given in Section 2.

In the case where K is absolutely abelian, the CC was proven (with some restrictions) in [So3]: One reduces first to the case $k = \mathbb{Q}$ where $\eta_{K/k,S}$ is essentially a cyclotomic unit (as above) and the CC can be proven without restriction, replacing the Artin-Hasse law with a generalisation due to Coleman. This case of the CC (or more precisely the connection it makes between reciprocity laws and the map $\mathfrak{s}_{K/\mathbb{Q},S}$) finds applications in Iwasawa Theory related to some new annihilators of the class-groups of real abelian fields (see [So4]). This gives one motivation for studying the CC more generally.

Unfortunately, there are very few cases with K not absolutely abelian in which $CC(K/k, S, p, n)$ can be proven, even partially (see [So3, §4]). Indeed for such K, one can't even prove the *existence* of $\eta_{K^+/k,S}$ except in very special cases (see Section 2.2). On the other hand, techniques for the *numerical* computation of $\eta_{K^+/k,S}$ were developed by the authors in [R-S1]. A slight simplification of these methods is used in the present paper to identify $\eta_{K^+/k,S}$ with virtual certainty. The rest of the paper is concerned with the detailed numerical verification of 48 varied cases of the CC using the computed values of $\eta_{K^+/k,S}$.

In order to make the computations manageable we still need to restrict the parameters $(K/k, S, p, n)$: in all our test cases k is (real) quadratic, $p \leq 7$ and $n = 0$ or 1. (On the other hand, $K/\mathbb{Q}$ is always non-abelian and frequently non-Galois). The precise set-up is given at the start of Section 3. We then explain in detail how we computed the objects appearing in the CC, in order: the map $\mathfrak{s}_{K/k,S}$, economical sets of (Galois) generators for $U^1(K_p)$ and its exterior square, the element $\eta_{K^+/k,S}$ and the Hilbert-symbol-determinant $H_{K/k,n}(\eta_{K^+/k,S}, \theta)$. Some of our techniques are well known and even implemented in PARI/GP (which is also the medium of all our computations). However, we believe that the majority are innovative and may well find applications elsewhere. It is worth mentioning an important dichotomy which emerges in our examples, between the minority of cases in which p divides $[K : k]$ and the majority in which it does not. On the one hand, the former cases provide a more probing test of the conjecture. For instance, since k is quadratic, the condition $n = 1$ requires $p|[K : k]$. On the other hand, cases of the latter type are much quicker to compute.

Finally, Section 4 presents the results of the computations. One simple but characteristic example is explained in detail. Data from the remaining ones are summarised in tables at the end of the paper.

Some notations and conventions: All number fields are finite extensions of $\mathbb{Q}$ within $\bar{\mathbb{Q}}$ which is the algebraic closure of $\mathbb{Q}$ within $\mathbb{C}$. If F is any field and m any positive integer, we shall write $\mu_m(F)$ for the group of all mth roots of unity in F. We shall abbreviate $\mu_m(\mathbb{C})$ to μ_m and write ξ_m for its generator $\exp(2\pi i/m)$. Suppose L/F is a Galois extension of number fields and $\mathfrak{Q}$ a prime ideal of $\mathcal{O}_L$ with $\mathfrak{q} = F \cap \mathfrak{Q}$. We shall write $D_{\mathfrak{Q}}(L/F)$ for the decomposition subgroup of $\mathrm{Gal}(L/F)$ at $\mathfrak{Q}$ and similarly $T_{\mathfrak{Q}}(L/F)$ for the inertia subgroup. We shall identify $D_{\mathfrak{Q}}(L/F)$ with the Galois group of the completed extension $L_{\mathfrak{Q}}/F_{\mathfrak{q}}$ and $T_{\mathfrak{Q}}(L/F)$ with its inertia group in the usual way. If $\mathcal{R}$ is a commutative ring and H is a finite group, we shall write simply $\mathcal{R}H$ for the group-ring often denoted $\mathcal{R}[H]$.

The second author wishes to thank Cristian Popescu and UCSD for their hospitality during the sabbatical year in which part of this paper was written.

2 The Congruence Conjecture

2.1 The Map $\mathfrak{s}_{K/k,S}$

Given an abelian extension K/k of number fields as above, we write G for $\mathrm{Gal}(K/k)$ and $S_\infty = S_\infty(k)$ and $S_{\mathrm{ram}} = S_{\mathrm{ram}}(K/k)$ respectively for the set of infinite places of k and the set of those finite places of k which ramify in K. We always identify finite places with prime ideals so, for instance, S_{ram} consists of the prime factors of the conductor $\mathfrak{f}(K)$ of K/k. We denote by $S_p = S_p(k)$ the set of places of k dividing the prime number $p \neq 2$. The finite S appearing in the CC must satisfy the hypothesis

$$S \text{ contains } S^1 := S_\infty \cup S_{\mathrm{ram}} \cup S_p \tag{1}$$

which we assume henceforth. Recall also that we are assuming K is CM so that $[K : K^+] = 2$ where K^+ is its maximal real subfield which contains k. The extra assumption that K contains $\mu_{p^{n+1}}$, which is necessary for the CC, may be dropped until further notice.

If s is a complex number with $\mathrm{Re}(s) > 1$, we define an Euler product in the complex group ring $\mathbb{C}G$ of G by

$$\Theta_{K/k,S}(s) := \prod_{\mathfrak{q} \notin S} \left(1 - N\mathfrak{q}^{-s}\sigma_{\mathfrak{q}}^{-1}\right)^{-1} \tag{2}$$

(The prime ideal $\mathfrak{q}$ of $\mathcal{O}_k$ ranges over all those not in S and $\sigma_{\mathfrak{q}}$ denotes the corresponding Frobenius element of G.) Indeed, the condition $\mathrm{Re}(s) > 1$ implies that $(1 - N\mathfrak{q}^{-s}\sigma_{\mathfrak{q}}^{-1})$ lies in $\mathbb{C}G^\times$ and that the product converges absolutely. $\Theta_{K/k,S}(s)$ is sometimes called the *'equivariant L-function'* because, if $\hat{G}$ denotes the group of (complex, irreducible) characters of G, then one can write $\Theta_{K/k,S}(s) = \sum_{\chi \in \hat{G}} L_{K/k,S}(s,\chi) e_{\chi^{-1},G}$. Here, for any $\chi \in \hat{G}$, we write $e_{\chi,G}$ for the corresponding idempotent $\frac{1}{|G|}\sum_{g \in G} \chi(g) g^{-1}$ of $\mathbb{C}G$ and $L_{K/k,S}(s,\chi)$ for the (S-truncated Artin) L-function, *i.e.* the function whose Euler product for $\mathrm{Re}(s) > 1$ is obtained

by applying χ^{-1} termwise to the R.H.S. of (2). Since $L_{K/k,S}(s,\chi)$ extends to a meromorphic function on $\mathbb{C}$ so does $\Theta_{K/k,S}(s)$ (with values in $\mathbb{C}G$). Now let c denote the element of G determined by complex conjugation, so that $\mathrm{Gal}(K/K^+) = \{1,c\} = \langle c\rangle$. A character $\chi \in \hat{G}$ is called *odd* (*resp. even*) if and only if $\chi(c) = -1$ (*resp.* $\chi(c) = 1$). If $\mathcal{R}$ is any commutative ring in which 2 is invertible, we write $e^{\pm}$ for the two idempotents $\frac{1}{2}(1 \pm c) \in \mathcal{R}\langle c\rangle$. Any $\mathcal{R}\langle c\rangle$-module M then splits as $M^+ \oplus M^-$ where $M^+ = e^+M$ is the 'plus-submodule' and $M^- = e^-M$ is the 'minus-submodule'. Taking $\mathcal{R} = \mathbb{C}$ and $M = \mathbb{C}G$, we get a corresponding decomposition $\Theta_{K/k,S}(s) = e^+\Theta_{K/k,S}(s) + e^-\Theta_{K/k,S}(s) =: \Theta^+_{K/k,S}(s) + \Theta^-_{K/k,S}(s)$, say. Clearly, $\Theta^-_{K/k,S}(s) = \sum_{\chi \text{ odd}} L_{K/k,S}(s,\chi)e_{\chi^{-1},G}$ and since $L_{K/k,S}(s,\chi)$ is regular at $s = 1$ whenever χ is not the trivial character χ_0, it follows that $\Theta^-_{K/k,S}(s)$ is also regular there. We set

$$a^-_{K/k,S} := \left(\frac{i}{\pi}\right)^d \Theta^-_{K/k,S}(1) = \left(\frac{i}{\pi}\right)^d \sum_{\substack{\chi\in\hat{G}\\ \chi \text{ odd}}} L_{K/k,S}(1,\chi)e_{\chi^{-1},G} \tag{3}$$

In this notation, it is not hard to see that $a^-_{K/k,S}$ lies in $i^d\mathbb{R}G^-$. In fact it lies in $\bar{\mathbb{Q}}G^-$ and indeed a much finer statement will be proven in Proposition 2.

For each $\mathfrak{P} \in S_p(K)$ we write $K_{\mathfrak{P}}$ for the (abstract) completion of K at $\mathfrak{P}$ and $\iota_{\mathfrak{P}}$ for the natural embedding $K \to K_{\mathfrak{P}}$. Let K_p denote the ring $\prod_{\mathfrak{P}\in S_p(K)} K_{\mathfrak{P}}$ endowed with the product topology and the usual (continuous) G action (see *e.g.* [So3, §2.3]). Thus the diagonal embedding $\iota := \prod_{\mathfrak{P}} \iota_{\mathfrak{P}} : K \to K_p$ is dense and G-equivariant. We fix once and for all an algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ (equipped with the usual p-adic absolute value $|\cdot|_p$), an embedding $j : \bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_p$ and a set $\tau_1, \ldots, \tau_d$ of left coset representatives for $\mathrm{Gal}(\bar{\mathbb{Q}}/k)$ in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. For each $i = 1, \ldots, d$, the embedding $j \circ \tau_i|_K : K \to \bar{\mathbb{Q}}_p$ extends to a continuous embedding $K_{\mathfrak{P}_i} \to \bar{\mathbb{Q}}_p$ for a unique prime ideal $\mathfrak{P}_i \in S_p(K)$, and we define $\delta_i : K_p \to \bar{\mathbb{Q}}_p$ to be its composite with the projection $K_p \to K_{\mathfrak{P}_i}$. (In general, the map $i \mapsto \mathfrak{P}_i$ is not injective, nor surjective onto $S_p(K)$, but the map $i \mapsto \mathfrak{P}_i \cap \mathcal{O}_k$ is surjective onto $S_p(k)$.) For each $\mathfrak{P} \in S_p(K)$, we write $U^1(K_{\mathfrak{P}})$ for the group of principal units of $K_{\mathfrak{P}}$ considered as a finitely generated $\mathbb{Z}_p$-module. We write $U^1(K_p)$ for the group $\prod_{\mathfrak{P}\in S_p(K)} U^1(K_{\mathfrak{P}})$ of 'p-semilocal principal units of K' considered as a $\mathbb{Z}G$-submobule of $K_p^\times$ and hence as a f.g. multiplicative $\mathbb{Z}_pG$-module. (*Warning:* nevertheless, we shall often use an *additive* notation for the $\mathbb{Z}_pG$-action on $U^1(K_p)$.) It is clear that $|\delta_i(u) - 1|_p < 1$ for every $u \in U^1(K_p)$ and each $i \in \{1, \ldots, d\}$ so that $\log_p(\delta_i(u)) \in \bar{\mathbb{Q}}_p$ is given by the usual logarithmic series. The formula $\lambda_{i,p}(u) := \sum_{g\in G} \log_p(\delta_i(gu))g^{-1}$ then defines a $\mathbb{Z}_pG$-linear map $\lambda_{i,p} : U^1(K_p) \to \bar{\mathbb{Q}}_pG$ and letting i vary we get a unique $\mathbb{Z}_pG$-linear 'regulator' map R_p from the exterior power $\bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)$ to $\bar{\mathbb{Q}}_pG$ such that $R_p(u_1 \wedge \ldots \wedge u_d) = \det(\lambda_{i,p}(u_l))^d_{i,l=1}$. (The dependence on j of δ_i, $\lambda_{i,p}$ and R_p will be denoted by a superscript 'j' where necessary.) We can now define a map

$$\begin{array}{rcccc} \mathfrak{s}_{K/k,S} & : & \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p) & \longrightarrow & \mathbb{Q}_pG^- \\ & & \theta & \longmapsto & j(a^{-,*}_{K/k,S})R^j_p(\theta) \end{array} \tag{4}$$

Some explanations are in order. First, $x \mapsto x^*$ is the unique $\mathbb{C}$-linear involution of $\mathbb{C}G$ sending g to g^{-1} for all $g \in G$. Since $a^-_{K/k,S}$ lies in $\bar{\mathbb{Q}}G^-$, so does $a^{-,*}_{K/k,S}$ and we apply j coefficientwise to get an element of $\bar{\mathbb{Q}}_pG^-$. Multiplying the result by $R^j_p(\theta)$ in $\bar{\mathbb{Q}}_pG$ gives $\mathfrak{s}_{K/k,S}(\theta)$ which is *a priori* another element of $\bar{\mathbb{Q}}_pG^-$. However one can show that it actually lies in $\mathbb{Q}_pG^-$ and, moreover, is *independent of the choice of* j (see [So2, Prop. 3.4] and [So3, Prop. 5]). Although the map $\mathfrak{s}_{K/k,S}$ is *not* independent of the choice and ordering of the τ_i's, the dependence is simple and explicit (see [So3, Rem. 2.6] for more details).

It is clear from its construction that $\mathfrak{s}_{K/k,S}$ is $\mathbb{Z}_pG$-linear. This implies in particular that it vanishes on $\bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)^+$, so one loses nothing by regarding it as a map $\bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)^- \to \mathbb{Q}_pG^-$. This was the point of view of [So3] but for the present purposes it is slightly more convenient to take the domain to be the whole of $\bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)$. In this context, the statement (and proof) of Prop. 6 of *ibid.* give

Proposition 1

(i). $\ker(\mathfrak{s}_{K/k,S}) = \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)^+ + \left(\bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)\right)_{\mathrm{tor}}$ *and the second summand is finite.*

(ii). $\mathrm{im}(\mathfrak{s}_{K/k,S})$ *spans* $\mathbb{Q}_pG^-$ *over* $\mathbb{Q}_p$. □

From now on we denote $\mathrm{im}(\mathfrak{s}_{K/k,S})$ by $\mathfrak{S}_{K/k,S}$.

The 'Integrality Conjecture' of [So3] is precisely the statement that $\mathfrak{S}_{K/k,S} \subset \mathbb{Z}_pG^-$. We shall not deal with this conjecture *per se* in the present paper because, in the cases we shall study, it can be subsumed into the stronger Congruence Conjecture.

2.2 Rubin-Stark Elements and the Pairing $H_{K/k,n}$

Now let $\bar{G} := \mathrm{Gal}(K^+/k) \cong G/\{1, c\}$. The $\mathbb{C}$-linear extension of the restriction map $G \to \bar{G}$ has kernel $\mathbb{C}G^-$ and defines an isomorphism $\mathbb{C}G^+ \cong \mathbb{C}\bar{G}$ identifying $\Theta^+_{K/k,S}(s) = \sum_{\chi \text{ even}} L_{K/k,S}(s,\chi)e_{\chi^{-1},G}$ with the function $\Theta_{K^+/k,S}(s) = \sum_{\chi\in\hat{\bar{G}}} L_{K^+/k,S}(s,\chi)e_{\chi^{-1},\bar{G}}$. Rubin-Stark elements are conjectural elements of a certain exterior power of the S-units of K^+ which are supposedly associated with the dth derivative of the Taylor series of $\Theta_{K^+/k,S}(s)$ at $s = 0$. Indeed, using the functional equation for primitive L-functions, one can show (see *e.g.* [Ta, Ch. I, §3]) that $\mathrm{ord}_{s=0}L_{K^+/k,S}(s,\chi) \geq d$ for all $\chi \in \hat{\bar{G}}$. (For $\chi = \chi_0$ one needs the fact that $|S| \geq d+1$, by Hypothesis 1.) Thus

$$\Theta_{K^+/k,S}(s) = \Theta^{(d)}_{K^+/k,S}(0)s^d + o(s^d) \quad \text{as } s \to 0$$

where $\Theta^{(d)}_{K^+/k,S}(0)$ denotes the element $\sum_{\chi\in\hat{\bar{G}}} \frac{1}{d!}\left(\frac{d}{ds}\right)^d|_{s=0}L_{K^+/k,S}(s,\chi)e_{\chi^{-1},\bar{G}}$ of $\mathbb{C}\bar{G}$. Let $e_{S,d,\bar{G}}$ be the (possibly empty) sum of the idempotents $e_{\chi^{-1},\bar{G}} \in \mathbb{C}\bar{G}$ over those $\chi \in \hat{\bar{G}}$ for which $\mathrm{ord}_{s=0}L_{K^+/k,S}(s,\chi)$ is exactly d. We refer to eq. (13) of [So3] for an explicit formula for $e_{S,d,\bar{G}}$

demonstrating that it actually lies in $\mathbb{Q}\bar{G}$. An element m of any $\mathbb{Q}\bar{G}$-module M will be said to *'satisfy the eigenspace condition (w.r.t. $(S,d,\bar{G})$)'* iff it lies in $e_{S,d,\bar{G}}M$, *i.e.* $m = e_{S,d,\bar{G}}m$. It is not hard to see that $\Theta^{(d)}_{K^+/k,S}(0)$ lies in $\mathbb{R}\bar{G}$ and satisfies the eigenspace condition. In fact, $\mathbb{R}\bar{G}\Theta^{(d)}_{K^+/k,S}(0) = e_{S,d,\bar{G}}\mathbb{R}\bar{G}$.

Let us write $U_S(K^+)$ for the group of all S-units of K^+, namely those elements of $K^{+,\times}$ which are local units at each place of K^+ above a place of k which is not in S. We consider $U_S(K^+)$ as a multiplicative $\mathbb{Z}\bar{G}$-module and the tensor product $\mathbb{Q}U_S(K^+) := \mathbb{Q}\otimes_{\mathbb{Z}} U_S(K^+)$ and its exterior power $\bigwedge^d_{\mathbb{Q}\bar{G}}\mathbb{Q}U_S(K^+)$ as natural $\mathbb{Q}\bar{G}$-modules. (*Warning:* we shall sometimes use an additive notation for these.) For each $i = 1,\dots d$ we define a $\mathbb{Z}\bar{G}$-linear map $\lambda_i : U_S(K^+) \to \mathbb{R}\bar{G}$ by setting $\lambda_i(\varepsilon) := \sum_{g\in G}\log|\tau_i(g\varepsilon)|g^{-1}$. This 'extends' $\mathbb{Q}$-linearly to a map $\mathbb{Q}U_S(K^+) \to \mathbb{R}\bar{G}$, also denoted λ_i, which in turn gives rise to a unique $\mathbb{Q}\bar{G}$-linear regulator map $R_{K^+/k}$ from $\bigwedge^d_{\mathbb{Q}\bar{G}}\mathbb{Q}U_S(K^+)$ to $\mathbb{R}\bar{G}$ such that $R_{K^+/k}(x_1\wedge\ldots\wedge x_d) = \det(\lambda_i(x_l))^d_{i,l=1}$.

We now define a *Rubin-Stark element for K^+/k and S* to be any element η of $\bigwedge^d_{\mathbb{Q}\bar{G}}\mathbb{Q}U_S(K^+)$ satisfying the eigenspace condition w.r.t. $(S,d,\bar{G})$ and such that

$$\Theta^{(d)}_{K^+/k,S}(0) = R_{K^+/k}(\eta) \tag{5}$$

One cannot currently demonstrate the existence of any $\eta \in \bigwedge^d_{\mathbb{Q}\bar{G}}\mathbb{Q}U_S(K^+)$ satisfying (5) unless either K^+ is absolutely abelian or all the characters $\chi \in \hat{\bar{G}}$ satisfying $\mathrm{ord}_{s=0}L_{K^+/k,S}(s,\chi) = d$ are of order 1 or 2. On the other hand, certain special cases of Stark's conjectures for the extension K^+/k are essentially equivalent to the existence of such an η (see [So3, Rem. 2.3]) and one can, if necessary, ensure that it simultaneously satisfies the eigenspace condition simply by replacing it by $e_{S,d,\bar{G}}\eta$. This makes η *unique* once $\tau_1,\dots,\tau_d$, and hence $R_{K^+/k}$, have been fixed (*e.g.* by [Ru, Lemma 2.7]). Henceforth we shall therefore refer to such an element as *the* Rubin-Stark element for K^+/k and S and denote it $\eta_{K^+/k,S}$. It may be thought of as a higher-order generalisation of a cyclotomic unit (or number).

From now on we shall assume that

$$K \text{ contains } \mu_{p^{n+1}} \tag{6}$$

where n is the integer of the Introduction, assumed w.l.o.g. to be ≥ 0. Thus, for each $\mathfrak{P}\in S_p(K)$, $\iota_{\mathfrak{P}}$ induces an isomorphism $\mu_{p^{n+1}}(K) \to \mu_{p^{n+1}}(K_{\mathfrak{P}})$ and the local Hilbert symbol $(\alpha,\beta)_{K_{\mathfrak{P}},p^{n+1}} \in \mu_{p^{n+1}}(K_{\mathfrak{P}})$ is defined for any $\alpha,\beta\in K^\times_{\mathfrak{P}}$. (We shall use the definition of the Hilbert symbol given in [Ne] rather than [Se] which reverses the order of α and β, thus effectively inverting $(\alpha,\beta)_{K_{\mathfrak{P}},p^{n+1}}$.) Given any $\varepsilon\in U_S(K^+)$ and $u = (u_{\mathfrak{P}})_{\mathfrak{P}} \in U^1(K_p)$ we define $[\varepsilon,u]_{K,n}\in\mathbb{Z}/p^{n+1}\mathbb{Z}$ by

$$[\varepsilon,u]_{K,n} = \sum_{\mathfrak{P}\in S_p(K)} \mathrm{Ind}_n\left(\iota_{\mathfrak{P}}^{-1}(\iota_{\mathfrak{P}}(\varepsilon),u_{\mathfrak{P}})_{K_{\mathfrak{P}},p^{n+1}}\right) \tag{7}$$

where $\mathrm{Ind}_n : \mu_{p^{n+1}}(K) \to \mathbb{Z}/p^{n+1}\mathbb{Z}$ is the isomorphism defined by $\xi_{p^{n+1}}^{\mathrm{Ind}_n(\zeta)} = \zeta$ for all $\zeta\in\mu_{p^{n+1}}(K)$. The pairing $[\cdot,\cdot]_{K,n} : U_S(K^+)\times U^1(K_p) \to \mathbb{Z}/p^{n+1}\mathbb{Z}$ is bilinear and one checks

(*cf* [So3, eq. (18)]) that

$$[g\varepsilon, gu]_{K,n} = \kappa_n(g)[\varepsilon, u]_{K,n} \quad \text{for all } \varepsilon \in U_S(K^+),\ u \in U^1(K_p) \text{ and } g \in G \tag{8}$$

where, here and henceforth, we write κ_n for the *cyclotomic character modulo* p^{n+1}. We shall regard κ_n as a homomorphism $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ whose restriction to $\mathrm{Gal}(\bar{\mathbb{Q}}/k)$ factors through G by (6) and is denoted by the same symbol. Thus, whether g lies in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ or in G, we have, by definition $g(\xi_{p^{n+1}}) = \xi_{p^{n+1}}^{\kappa_n(g)}$. Next we consider the pairing $[\cdot,\cdot]_{K,n,G}$ defined as follows

$$\begin{array}{rcccc} [\cdot,\cdot]_{K,n,G} & : & U_S(K^+) \times U^1(K_p) & \longrightarrow & (\mathbb{Z}/p^{n+1}\mathbb{Z})G \\ & & (\varepsilon, u) & \longmapsto & \sum_{g\in G}[\varepsilon, gu]_{K,n}g^{-1} \end{array}$$

If h lies in $\bar{G}$ and $\tilde{h}$ is any lift of h in G, then a short calculation using (8) shows that

$$[h\varepsilon, u]_{K,n,G} = \kappa_n(\tilde{h})\tilde{h}^{-1}[\varepsilon, u]_{K,n,G} \tag{9}$$

for any $\varepsilon \in U_S(K^+)$ and $u \in U^1(K_p)$. Taking $h = 1$, $\tilde{h} = c$ gives $[\varepsilon, u]_{K,n,G} = -c[\varepsilon, u]_{K,n,G}$ in $(\mathbb{Z}/p^{n+1}\mathbb{Z})G$. In other words, $[\cdot,\cdot]_{K,n,G}$ takes values in $(\mathbb{Z}/p^{n+1}\mathbb{Z})G^-$. Let us denote by κ_n^* the unique ring homomorphism from $\mathbb{Z}\bar{G}$ to $(\mathbb{Z}/p^{n+1}\mathbb{Z})G^-$ which sends $h \in \bar{G}$ to $\bar{2}^{-1}(\kappa_n(\tilde{h}_1)\tilde{h}_1^{-1} + \kappa_n(\tilde{h}_2)\tilde{h}_2^{-1})$, where $\tilde{h}_1$ and $\tilde{h}_2 = c\tilde{h}_1$ are the two lifts of h to G. Then equation (9) shows that the pairing $[\cdot,\cdot]_{K,n,G}$ is κ_n^*-semilinear in the first variable. On the other hand, it follows from its definition that $[\cdot,\cdot]_{K,n,G}$ is $\mathbb{Z}G$-linear, hence $\mathbb{Z}_pG$-linear, in the second variable. Consequently, we obtain a unique, well-defined pairing $\mathcal{H}_{K/k,n}$: $\bigwedge^d_{\mathbb{Z}\bar{G}} U_S(K^+) \times \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p) \to (\mathbb{Z}/p^{n+1}\mathbb{Z})G^-$ satisfying

$$\mathcal{H}_{K/k,n}(\varepsilon_1 \wedge \ldots \wedge \varepsilon_d, u_1 \wedge \ldots \wedge u_d) = \det([\varepsilon_i, u_t]_{K,n,G})_{i,t=1}^d$$

for any $\varepsilon_1, \ldots, \varepsilon_d \in U_S(K^+)$ and $u_1, \ldots, u_d \in U^1(K_p)$. By construction, $\mathcal{H}_{K/k,n}$ is κ_n^*-semilinear in the first variable and $\mathbb{Z}_pG$-linear in the second and the latter implies

$$\mathcal{H}_{K/k,n}(\eta, \theta) = 0 \quad \text{for all } \eta \in \textstyle\bigwedge^d_{\mathbb{Z}\bar{G}} U_S(K^+) \text{ and } \theta \in \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)^+ \tag{10}$$

(So, for fixed η the map $\mathcal{H}_{K/k,n}(\eta,\cdot) : \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p) \to (\mathbb{Z}/p^{n+1}\mathbb{Z})G^-$ factors through the projection on $\bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)^-$, just as $\mathfrak{s}_{K/k,S}$ does.) Finally, we can 'extend' $\mathcal{H}_{K/k,n}$ in an obvious way so that the first variable lies in the tensor product $\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \bigwedge^d_{\mathbb{Z}\bar{G}} U_S(K^+)$, where $\mathbb{Z}_{(p)}$ denotes the subring $\{a/b \in \mathbb{Q} : p \nmid b\}$ of $\mathbb{Q}$.

We now explain briefly a further 'extension' of the pairing $\mathcal{H}_{K/k,n}$ which is necessary to state the Congruence Conjecture properly but – for reasons that will become clear later – has only a limited importance for the computations of this paper. The reader may refer to [So3] for the details. Denote by α_S the natural map $\bigwedge^d_{\mathbb{Z}\bar{G}} U_S(K^+) \to \bigwedge^d_{\mathbb{Q}\bar{G}} \mathbb{Q}U_S(K^+)$. Following Rubin, we defined in *loc. cit.*, § 2.2, a $\mathbb{Z}\bar{G}$-lattice $\Lambda_{0,S}(K^+/k)$ in $\bigwedge^d_{\mathbb{Q}\bar{G}} \mathbb{Q}U_S(K^+)$

which contains the image of α_S with finite index. In *loc. cit.*, § 2.3 we defined a pairing $H_{K/k,n} : \mathbb{Z}_{(p)}\Lambda_{0,S}(K^+/k) \times \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p) \to (\mathbb{Z}/p^{n+1}\mathbb{Z})G^-$ which has the following property. If $1 \otimes \alpha_S$ denotes the $\mathbb{Z}_{(p)}$-linearly extension of α_S to $\mathbb{Z}_{(p)} \otimes \bigwedge^d_{\mathbb{Z}\bar{G}} U_S(K^+)$, then for any $\theta \in \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)$ there is a commuting diagram

$$\begin{array}{ccc} \mathbb{Z}_{(p)} \otimes \bigwedge^d_{\mathbb{Z}\bar{G}} U_S(K^+) & & \\ \Big\downarrow{\scriptstyle 1\otimes\alpha_S} & \overset{\mathcal{H}_{K/k,n}(\cdot,\theta)}{\searrow} & \\ & & (\mathbb{Z}/p^{n+1}\mathbb{Z})G^- \\ \mathbb{Z}_{(p)}\Lambda_{0,S}(K^+/k) & \underset{H_{K/k,n}(\cdot,\theta)}{\nearrow} & \end{array} \tag{11}$$

This follows easily from [So3, eq. (20)].

REMARK 1 In fact, the vertical map above is an isomorphism whenever $p \nmid |\bar{G}|$. (See [So3, Remark 2.4].) If $p||G|$, then both the kernel (namely the torsion in $\mathbb{Z}_{(p)} \otimes \bigwedge^d_{\mathbb{Z}\bar{G}} U_S(K^+)$) and the cokernel may be non-trivial, though finite. As far as the present paper is concerned, the main consequence of (11) is simply that $\mathcal{H}_{K/k,n}(\cdot,\theta)$ vanishes on the kernel of $1 \otimes \alpha_S$, for all θ.

2.3 Statement of the Conjecture

With the above hypotheses the Congruence Conjecture (CC) of [So3] may be stated as follows.

Conjecture $CC(K/k, S, p, n)$ *The Rubin-Stark element $\eta_{K^+/k,S}$ exists and lies in $\mathbb{Z}_{(p)}\Lambda_{0,S}(K^+/k)$. Furthermore, if $\theta \in \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)$ then $\mathfrak{s}_{K/k,S}(\theta)$ lies in $\mathbb{Z}_pG^-$ and satisfies the following congruence modulo p^{n+1}*

$$\overline{\mathfrak{s}_{K/k,S}(\theta)} = \kappa_n(\tau_1 \dots \tau_d) H_{K/k,n}(\eta_{K^+/k,S}, \theta) \quad \textit{in } (\mathbb{Z}/p^{n+1}\mathbb{Z})G^-. \tag{12}$$

REMARK 2 The choice of $\tau_1, \dots, \tau_d$ affects both $\mathfrak{s}_{K/k,S}$ and $\eta_{K^+/k,S}$ but not the validity of $CC(K/k, S, p, n)$ thanks to the 'normalising factor' $\kappa_n(\tau_1 \dots \tau_d)$ in (12).

REMARK 3 The conjecture behaves well under changing K, S and n. More precisely, it is shown in [So3, §5] that $CC(K/k, S, p, n)$ implies $CC(F/k, S', p, n')$ for any S' containing S, any n' such that $n \geq n' \geq 0$ and any intermediate field F, $K \supset F \supset k$ provided that the norm map from $\bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)^-$ to $\bigwedge^d_{\mathbb{Z}_p\mathrm{Gal}(F/k)} U^1(F_p)^-$ is surjective. This holds, for instance, if K/F is at most tamely ramified at primes in $S_p(F)$.

REMARK 4 As already noted, the CC includes the statement $\mathfrak{S}_{K/k,S} \subset \mathbb{Z}_pG^-$ *i.e.* the Integrality Conjecture (IC). This was treated separately in [So3] since it does not require

$\mu_p \subset K$. Section 4 of *loc. cit.* contains a survey of evidence for both conjectures. The IC is known in many cases where the CC is not, *e.g.* when p splits completely in k (with a technical condition), when p is unramified in K or when $p \nmid |G|$.

REMARK 5 It is shown in [So3, Rem. 2.3] that Conjecture B' of [Ru] implies the existence of $\eta_{K^+/k,S}$ and that it lies in $\frac{1}{2}\Lambda_{0,S}(K^+/k)$, hence it implies the first statement of the CC. However, even in situations where $\eta_{K^+/k,S}$ is known as an explicit element of $\frac{1}{2}\Lambda_{0,S}(K^+/k)$ (for instance, if $k = K^+$) the congruence (12) can still be elusive. If $\theta \in \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)^+$ then (12) clearly holds trivially (*i.e.* as $0 = 0$) and the same thing happens in a couple of more interesting cases mentioned in [So3, §4]. Apart from these, the full CC is unknown whenever K is not abelian over $\mathbb{Q}$.

3 Methods of Computation

In this section we describe in detail the method we used to numerically check the CC for the 48 examples listed in Section 4.

3.1 The Set-Up

We take the field k to be a real quadratic field (so $d = 2$), and always take $S = S^1$ (so we drop it from the notation when possible). In view of Remark 3, $CC(K/k, S^1, p, n)$ implies $CC(K/k, S, p, n)$ for all other admissible S. The prime p will be small for computational reasons: large primes would lead to extensions K/k of too large a degree. Thus we shall always take $p = 3$, 5 or 7. For the same reason, we shall usually take $n = 0$, except for a few examples with $n = 1$ and $p = 3$, which were added for completeness. Since $d = 2 < p$, the latter examples necessarily have $p||G|$. The question as to whether or not p divides $|G|$ is of importance in the computation of $\mathbb{Z}_pG$-generators of $\bigwedge^2_{\mathbb{Z}_pG} U^1(K_p)$, as we shall see in Subsection 3.4. All computations take place in the number field F which is defined to be the *normal closure of K over $\mathbb{Q}$* (within $\bar{\mathbb{Q}}$). They were performed using the PARI/GP system [PARI].

3.2 Computation of $a^-_{K/k}$ and $\mathfrak{s}_{K/k}(\theta)$

Using the implementation in PARI/GP of the algorithm of [D-T], see also [Co, Section 10.3], we can compute arbitrarily good approximations of the values at $s = 1$ of the S^1-truncated Artin L-functions of odd irreducible characters of G, and thus deduce arbitrarily good approximations of $a^-_{K/k}$ as an element of $i^2\mathbb{R}G = \mathbb{R}G$, thanks to (3). In order to compute $\mathfrak{s}_{K/k}$ we must however determine $a^-_{K/k}$ exactly as an element of FG^- and to this end, we use the

Proposition 2 *Let $f(K)$ denote the positive generator of the ideal $\mathfrak{f}(K) \cap \mathbb{Z}$. Set $\delta = 1$ if $(p, f(K)) = 1$ and $\delta = 0$ otherwise, and let*

$$\tilde{a}^-_{K/k} := p^\delta |\mu(K)| \sqrt{d_k} N\mathfrak{f}(K) a^-_{K/k} = -p^\delta |\mu(K)| \sqrt{d_k} N\mathfrak{f}(K) \pi^{-2} \Theta^-_{K/k}(1) \tag{13}$$

The coefficients of $\tilde{a}^-_{K/k}$ are algebraic integers of $F \cap \mathbb{Q}(\mu_{f(K)})$ and are stable (as a set) under the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

The proof uses the following group-theoretic lemma whose (simple) verification is left to the reader.

Lemma 1 *Let $\mathcal{G}$ be a group and $\mathcal{H}$ a subgroup of finite index in $\mathcal{G}$, and let* Ver *denote the transfer homomorphism from $\mathcal{G}^{\mathrm{ab}} = \mathcal{G}/\mathcal{G}'$ to $\mathcal{H}^{\mathrm{ab}} = \mathcal{H}/\mathcal{H}'$. Suppose $\mathcal{J}$ is a normal subgroup of $\mathcal{H}$ containing $\mathcal{H}'$ and write $\tilde{\mathcal{J}}$ for the largest normal subgroup of $\mathcal{G}$ contained in $\mathcal{J}$,* i.e.*$\tilde{\mathcal{J}} = \bigcap_g g\mathcal{J}g^{-1}$ where g runs through $\mathcal{G}$ (or, indeed, through a set of left-coset representatives for $\mathcal{H}$ in $\mathcal{G}$). Then $\tilde{\mathcal{J}}$ is contained in the kernel of the composite homomorphism*

$$\mathcal{G} \longrightarrow \mathcal{G}^{\mathrm{ab}} \xrightarrow{\mathrm{Ver}} \mathcal{H}^{\mathrm{ab}} \longrightarrow \mathcal{H}/\mathcal{J}$$

□

Proof of Proposition 2 Let $\Phi_{K/k}(s)$ be the function defined in [So2, eq. (9)]. It follows from [So3, eq. (8)] (dropping e^-, since $k \neq \mathbb{Q}$) that $\tilde{a}^-_{K/k} = (\prod(N\mathfrak{p} - \sigma_\mathfrak{p}^{-1}))|\mu(K)|d_k N\mathfrak{f}(K)\Phi_{K/k}(0)$ where the product runs over the set of all primes $\mathfrak{p} \in S_p(k)$ not dividing $\mathfrak{f}(K)$. (Since K contains μ_p and $[k : \mathbb{Q}] = 2$, it is easy to see that either this set is empty – so $\delta = 0$ – or p ramifies in k and this set consists of the unique prime $\mathfrak{p} \in S_p(k)$ – so that $N\mathfrak{p} = p = p^\delta$.) Equation (27) of [So2] shows that the coefficients of $|\mu(K)|d_k N\mathfrak{f}(K)\Phi_{K/k}(0)$ are algebraic integers of $\mathbb{Q}(\mu_{f(K)})$, hence so are those of $\tilde{a}^-_{K/k}$. It remains to show that they are $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-stable and lie in F. Consider the automorphism of $\bar{\mathbb{Q}}G$ obtained by applying some $\alpha \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ to coefficients. It was shown in [So2, Prop. 3.2] that this has the same effect on $\Phi_{K/k}(0)$ as multiplying it by $\mathcal{V}_K(\alpha)$ where $\mathcal{V}_K$ is the composite homomorphism

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})^{\mathrm{ab}} \xrightarrow{\mathrm{Ver}} \mathrm{Gal}(\bar{\mathbb{Q}}/k)^{\mathrm{ab}} \longrightarrow G$$

The same is therefore true of $\tilde{a}^-_{K/k}$, hence its coefficients are $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-stable. Moreover, they are fixed by $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$ because the latter is contained in $\ker \mathcal{V}_K$, as follows from the Lemma. (Take $\mathcal{G} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, $\mathcal{H} = \mathrm{Gal}(\bar{\mathbb{Q}}/k)$ and $\mathcal{J} = \mathrm{Gal}(\bar{\mathbb{Q}}/K)$, so that $\tilde{\mathcal{J}} = \mathrm{Gal}(\bar{\mathbb{Q}}/F)$). □

Remark 6 If we define $\tilde{a}^-_{K/k}$ to be the second member in (13) with p^δ replaced by $\prod_{\mathfrak{q} \in S \setminus (S_{\mathrm{ram}} \cup S_\infty)} N\mathfrak{q}$, then both the statement of the Proposition and its proof go through essentially unchanged for any $d > 1$ and $S \supset S^1$. Since the coefficients of $\tilde{a}^-_{K/k}$ also lie in $i^d\mathbb{R}$ in general, for $d = 2$ they must actually lie in $F \cap \mathbb{Q}(\mu_{f(K)})^+$.

Let $\tilde{a}^-_{K/k,\sigma}$ denote the coefficient of $\sigma \in G$ in $\tilde{a}^-_{K/k}$. Having computed $a^-_{K/k}$ to high accuracy

in $\mathbb{R}G$ as described above, we obtain good real approximations to the values $\tilde{a}^-_{K/k,\sigma}$ for $\sigma \in G$ and hence to the coefficients of the polynomial $\prod_{\sigma\in G}(X - \tilde{a}^-_{K/k,\sigma})$. But Proposition 2 implies that this polynomial lies in $\mathbb{Z}[X]$, so we may recover it exactly. By recognising the $\tilde{a}^-_{K/k,\sigma}$ among its roots in F (embedded in $\mathbb{C}$), we then obtain $\tilde{a}^-_{K/k}$ as an element of $\mathcal{O}_F[G]$ and dividing by $p^\delta|\mu(K)|\sqrt{d_k}N\mathfrak{f}(K) \in F^\times$ gives $a^-_{K/k}$ as an element of FG.

We now explain how to compute $\mathfrak{s}_{K/k}(\theta) \in \mathbb{Q}_pG$ (for $\theta \in \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)$) to any predetermined ($p$-adic) accuracy. We shall need only the case $\theta = u_1 \wedge u_2$ with $u_1, u_2 \in U^1(K_p)$ (which suffices anyway, by linearity). For any integer $N \geq 1$ we write the power series $\log(1+X)$ as $\ell_N(X) + r_N(X)$ where $\ell_N(X) := \sum_{t=1}^{N-1}(-1)^{t-1}X^t/t \in \mathbb{Q}[X]$ and $r_N(X) := \sum_{t=N}^{\infty}(-1)^{t-1}X^t/t \in \mathbb{Q}[[X]]$. For $i = 1, 2$ and any $u \in U^1(K_p)$ we define elements $\lambda_{i,p,N}(u) = \lambda^j_{i,p,N}(u)$ and $\rho_{i,p,N}(u) = \rho^j_{i,p,N}(u)$ of $\bar{\mathbb{Q}}_pG$ by

$$\lambda_{i,p,N}(u) := \sum_{g\in G} \ell_N(\delta^j_i(g(u-1)))g^{-1} \quad \text{and} \quad \rho_{i,p,N}(u) := \sum_{g\in G} r_N(\delta^j_i(g(u-1)))g^{-1}$$

so that $\lambda_{i,p}(u) = \lambda_{i,p,N}(u) + \rho_{i,p,N}(u)$. It follows easily that $\lambda_{i,p}(u_l) = \lim_{N\to\infty}\lambda_{i,p,N}(u_l)$ for any $i, l \in \{1, 2\}$ and consequently that

$$\mathfrak{s}_{K/k}(u_1 \wedge u_2) = \lim_{N\to\infty} j(a^{-,*}_{K/k}) \det(\lambda^j_{i,p,N}(u_l))^2_{i,l=1}$$

The convergence in $\bar{\mathbb{Q}}_pG$ implied in each of these limits is coefficientwise, w.r.t. the absolute value $|\cdot|_p$ on $\bar{\mathbb{Q}}_p$. The next result gives us the explicit control we require on the rate of convergence in the second limit. First, we impose a p-adic norm $\|\cdot\|_p$ on the $\bar{\mathbb{Q}}_p$-algebra $\bar{\mathbb{Q}}_pG$ by setting

$$\|a\|_p = \max\{|a_g|_p : g \in G\} \quad \text{where } a = \textstyle\sum_{g\in G} a_g g \in \bar{\mathbb{Q}}_pG$$

It is easy to check that $\|x + y\|_p \leq \max\{\|x\|_p, \|y\|_p\}$ and $\|x.y\|_p \leq \|x\|_p.\|y\|_p$. We define a rational number $m_{K/k}$ by $p^{m_{K/k}} = \|j(a^-_{K/k})\|_p = \|j(a^{-,*}_{K/k})\|_p$. The coefficients of $a^-_{K/k}$ now being known as elements of a number field F, we may calculate $m_{K/k}$ from their valuations at the prime ideal in $S_p(F)$ determined by j. (Notice, however, that Prop. 2 gives an *a priori* upper bound for $m_{K/k}$ and also shows it to be independent of our choice of j.)

Next, for $i = 1, 2$ we set $e_i = e_{\mathfrak{P}_i}(K/\mathbb{Q})$ (recall that $\mathfrak{P}_i$ is the element of $S_p(K)$ determined by $j\tau_i$) and $h_i(x) = (\log(x)/\log(p)) - (x/e_i)$ for any real number $x > 0$. Thus the function h_i decreases monotonically to $-\infty$ on $[e_i/\log(p), \infty)$. For $i = 1, 2$, we let b_i be the smallest integer b such that $p^b(p-1) \geq e_i$. In our examples, b_i ranges from 0 to 2. Finally, we write ϵ for the transposition $(1, 2) \in \Sigma_2$.

Proposition 3 *Suppose that a positive integer M is given. Then for any integer $N > \max\{e_1, e_2\}/\log(p)$ satisfying the inequalities*

$$h_{\epsilon(i)}(N) \leq -(M + m_{K/k} + (b_i - (p^{b_i}/e_i))) \quad \textit{for } i = 1 \textit{ and } 2 \tag{14}$$

we have

$$\|\mathfrak{s}_{K/k}(u_1 \wedge u_2) - j(a^{-,*}_{K/k}) \det(\lambda^j_{i,p,N}(u_l))^2_{i,l=1}\|_p \leq p^{-M} \quad \textit{for all } u_1, u_2 \in U^1(K_p) \tag{15}$$

PROOF If $t \in \mathbb{Z}_{\geq 1}$ and $i = 1$ or 2 then for any $g \in G$ and $u \in U^1(K_p)$ we clearly have

$$|(\delta_i^j(g(u-1)))^t/t|_p \leq p^{-t/e_i}|t|_p^{-1}$$

As t varies, the R.H.S. of this inequality attains an absolute maximum of $p^{b_i-(p^{b_i}/e_i)}$ (at $t = p^{b_i}$) and, on the other hand, is always at most $p^{h_i(t)}$. We deduce that for any i and u, we have $\|\lambda_{i,p,N}(u)\|_p \leq p^{b_i-(p^{b_i}/e_i)}$ and $\|\rho_{i,p,N}(u)\|_p \leq p^{b_i-(p^{b_i}/e_i)}$ for *every* positive integer N and also $\|\rho_{i,p,N}(u)\|_p \leq p^{h_i(N)}$ provided $N > e_i/\log(p)$. Therefore, writing $\mathfrak{s}_{K/k}(u_1 \wedge u_2)$ as $j(a_{K/k}^{-,*}) \det(\lambda_{i,p,N}^j(u_l) + \rho_{i,p,N}^j(u_l))_{i,l=1}^2$ and expanding the determinant, we find that for any $N > \max\{e_1, e_2\}/\log(p)$ satisfying the inequalities (14), we have

$$\text{(L.H.S. of (15))} \leq p^{m_{K/k}} \max\{p^{h_2(N)+b_1-(p^{b_1}/e_1)}, p^{h_1(N)+b_2-(p^{b_2}/e_2)}\} \leq p^{-M} \qquad \square$$

REMARK 7
(i) The two inequalities (14) coincide whenever $e_1 = e_2$ and in particular, whenever p does not split in k.

(ii) In our computations of $\mathfrak{s}_{K/k}(u_1 \wedge u_2)$, the elements u_1, u_2 will always be 'global' by which we shall mean that $u_l = \iota(v_l)$ for $l = 1, 2$ where $v_l \in K^\times$ satisfies $\mathrm{ord}_{\mathfrak{P}}(v_l - 1) \geq 1$ for each $\mathfrak{P} \in S_p(K)$. (In fact, the v_l will be constructed to lie in $\mathcal{O}_K$.) Thus, for $i = 1, 2$ we can write $\lambda_{i,p,N}^j(u_l)$ as $j(\sum_{g\in G}(\tau_i g(x_{l,N}))g^{-1})$ where $x_{l,N} = \ell_N(v_l - 1)$ lies in K for $l = 1, 2$, and so

$$j(a_{K/k}^{-,*}) \det(\lambda_{i,p,N}^j(u_l))_{i,l=1}^2 = j\left(a_{K/k}^{-,*} \det(\textstyle\sum_{g\in G}\tau_i g(x_{l,N})g^{-1})_{i,l=1}^2\right) \tag{16}$$

It follows from Proposition 2 that the quantity inside the large parentheses on the R.H.S. of (16) has coefficients in F. In fact, however, they lie in $\mathbb{Q}$. (Hints for a proof of this fact are given in Rem. 3.3(i) and Props. 3.3 and 3.4 of [So2] noting that $a_{K/k}^{-,*} = \sqrt{d_k}\Phi_{K/k}(0)^*$, by [So3, eq. (8)].) We may therefore drop the 'j' on the R.H.S. of (16) and substitute it into (15).

3.3 Generators of $U^1(K_p)$

Both sides of the congruence (12) are $\mathbb{Z}_pG$-linear in θ so it suffices to test it on a set of θ's generating $\bigwedge^2_{\mathbb{Z}_pG} U^1(K_p)$ over $\mathbb{Z}_pG$, preferably few in number since the R.H.S. is particularly computationally intensive (see Remark 11). First we explain our construction of a set V of $\mathbb{Z}_pG$-generators for $U^1(K_p)$. This is summarised in the two following Propositions which hold for any abelian extension of number fields K/k and any prime p. For the rest of this subsection, we therefore drop the assumption $[k : \mathbb{Q}] = 2$ and return to the notations of Subsection 2.1. In addition, we shall write $S_p(k)$ as $\{\mathfrak{p}(1), \ldots, \mathfrak{p}(t)\}$ where $t = |S_p(k)| \leq r$ and $\mathfrak{P}(i, 1), \ldots, \mathfrak{P}(i, h_i)$ for the distinct primes of K dividing $\mathfrak{p}(i)$, for $i = 1, \ldots, t$. For each pair (i, j) with $i = 1, \ldots, t$ and $j = 1, \ldots, h_i$ we shall abbreviate the completion $K_{\mathfrak{P}(i,j)}$ to $\hat{K}_{i,j}$ and the embedding $\iota_{\mathfrak{P}(i,j)} : K \to \hat{K}$ to $\iota_{i,j}$ so that $\iota = \prod_{i,j} \iota_{i,j}$ embeds K in $K_p = \prod_{i,j} \hat{K}_{i,j}$. We write $\hat{\mathcal{O}}_{i,j}$ for the ring of valuation integers of $\hat{K}_{i,j}$ and $\hat{\mathfrak{P}}(i, j)$ for its maximal ideal. For any

$l \geq 1$ we write $U^l_{i,j}$ for the lth term in the filtration of $\hat{\mathcal{O}}^\times_{i,j}$, *i.e.* $U^l_{i,j} = 1 + \hat{\mathfrak{P}}(i,j)^l$ considered as a finitely generated, multiplicative $\mathbb{Z}_p$-module. In particular $U^1(K_p) = \prod_{i,j} U^1_{i,j} \subset K_p^\times$. We write D_i for $D_{\mathfrak{P}(i,j)}(K/k)$ which depends only on i, since K/k is abelian. The same is true for $T_i := T_{\mathfrak{P}(i,j)}(K/k)$, $e'_i := |T_i| = e_{\mathfrak{P}(i,j)}(K/k)$, $f_i := |D_i/T_i| = f_{\mathfrak{P}(i,j)}(K/k)$ and for ϕ_i which we define to be the Frobenius element at $\mathfrak{P}(i,j)$ considered as a generator of the quotient group D_i/T_i. For each i we also define a positive integer l_i (independent of j) by

$$l_i := 1 + [pe_{\mathfrak{P}(i,j)}(K/\mathbb{Q})/(p-1)] = 1 + [pe'_i e_{\mathfrak{p}(i)}(k/\mathbb{Q})/(p-1)]$$

It follows from the standard properties of $\log_p$ and $\exp_p$ as defined by the usual power series (see [Wa, Ch. 5]) that $U^{l_i}_{i,j}$ is contained in $(U^1_{i,j})^p$ for all i,j. Indeed, $u \in U^{l_i}_{i,j}$ implies $|u-1|_p < p^{-p/(p-1)}$ so that $|\frac{1}{p}\log_p(u)|_p = p|u-1|_p < p^{-1/(p-1)}$. Hence $v := \exp_p(\frac{1}{p}\log_p(u))$ is a well-defined element of $\hat{K}_{i,j}$ satisfying $v^p = u$ and $|v-1|_p < p^{-1/(p-1)} < 1$, so that $v \in U^1_{i,j}$.

Proposition 4 *In the above notation, suppose that for each i we are given*

(i). a subset $X_i = \{x_{i,1}, \ldots, x_{i,n_i}\}$ of $\mathfrak{P}(i,1)$ such that the images of $\iota_{i,1}(1+x_{i,1}), \ldots, \iota_{i,1}(1+x_{i,n_i})$ generate the quotient $U^1_{i,1}/U^{l_i}_{i,1}$ as a module over $\mathbb{Z}_p D_i$ and

(ii). an element a_i of $\mathcal{O}_K$ such that for any $r = 1, \ldots, t$ and $j = 1, \ldots, h_r$ we have

$$a_i \equiv \begin{cases} 1 \pmod{\mathfrak{P}(r,j)^{l_r}} & \text{if } r = i \text{ and } j = 1, \text{ and} \\ 0 \pmod{\mathfrak{P}(r,j)^{l_r}} & \text{otherwise.} \end{cases}$$

Then the set $V := \{\iota(1 + a_i x_{i,s}) : i = 1, \ldots, t,\ s = 1, \ldots, n_i\}$ generates $U^1(K_p)$ over $\mathbb{Z}_p G$.

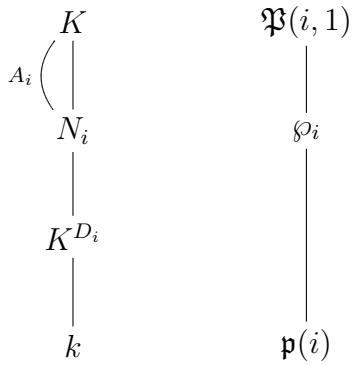
Proof By Nakayama's Lemma, it suffices to show that V generates $U^1(K_p)$ modulo $(U^1(K_p))^p$ and hence, by the preceding comments, that the images of the elements $\iota(1 + a_i x_{i,s})$ generate $U^1(K_p)/\prod_{i,j} U^{l_i}_{i,j}$. As a $\mathbb{Z}_p G$-module this is the product (over i) of the sub-modules $\prod_{j=1}^{h_i} \left(U^1_{i,j}/U^{l_i}_{i,j}\right)$ so that, by the definition of the a_i, it suffices to prove that for each i, the latter is generated over $\mathbb{Z}_p G$ by the images of the elements $\iota_{i,1}(1+a_i x_{i,t}) \times \ldots \times \iota_{i,h_i}(1+a_i x_{i,t})$ for $1 \leq t \leq n_i$. By the definition of the a_i (again) and of X_i, these images lie in the subgroup $U^1_{i,1}/U^{l_i}_{i,1}$ and generate it over $\mathbb{Z}_p D_i$. Since $\prod_j \left(U^1_{i,j}/U^{l_i}_{i,j}\right)$ is the direct product of G-translates of $U^1_{i,1}/U^{l_i}_{i,1}$, we are done. □

To find a set X_i as in part (i) of the statement of Proposition 4, one could simply ensure that the images of $\iota_{i,t}(1 + x_{i,t})$ generate the finite module $U^1_{i,1}/U^{l_i}_{i,1}$ over $\mathbb{Z}_p$ rather than $\mathbb{Z}_p D_i$. However, it is straightforward to construct a set that is generally smaller (for $f_i > 1$), provided that the exact sequence

$$1 \to T_i \longrightarrow D_i \longrightarrow D_i/T_i \to 1 \tag{17}$$

splits. This is equivalent to the existence of a lift $\tilde{\phi}_i \in D_i$ of ϕ_i which is of order f_i. A sufficient condition is that f_i be prime to e'_i or, more generally, to the cardinality of $D_i^{f_i}$ (subgroup of

f_i-th powers). Computational constraints on $[K:k]$ mean that D_i is a fairly small group in the examples considered, so it is perhaps not so surprising that the sequence (17) was found to split in *all* of them (for all i) without any pre-selection. Assuming that this occurs, we write A_i for the subgroup (of order f_i) of D_i generated by some $\tilde{\phi}_i$, N_i for K^{A_i} and $\wp_i$ for the prime of N_i below $\mathfrak{P}(i,1)$:



Thus N_i/K^{D_i} is totally ramified at $\wp_i$ (so $f_{\wp_i}(N_i/k)=1$). On the other hand, K/N_i is unramified at $\mathfrak{P}(i,1)$ and $A_i=\mathrm{Gal}(K/N_i)$ maps isomorphically onto the Galois group of the residue field $\mathcal{O}_K/\mathfrak{P}(i,1)$ over $\mathcal{O}_{N_i}/\wp_i=\mathcal{O}_k/\mathfrak{p}(i)$ (with $\tilde{\phi}_i$ acting by $N\mathfrak{p}(i)$-th powers). It follows from the Normal Basis Theorem that $\mathcal{O}_K/\mathfrak{P}(i,1)$ is freely generated over $(\mathcal{O}_k/\mathfrak{p}(i))A_i$. Moreover, a well-known criterion states that a free generator is given by the class $\bar{\alpha}_i$ modulo $\mathfrak{P}(i,1)$ of $\alpha_i\in\mathcal{O}_K$ if and only if $\det(gh(\bar{\alpha}_i))_{g,h\in A_i}\neq 0$ in $\mathcal{O}_K/\mathfrak{P}(i,1)$; in other words, iff $\det(\alpha_i^{N\mathfrak{p}(i)^{a+b}})_{a,b=0}^{f_i-1}\notin\mathfrak{P}(i,1)$. Such an α_i is easily found by trial and error.

Proposition 5 *Suppose the sequence (17) splits for some $i\in\{1,\dots,t\}$. Using the above notations, choose any $\pi_i\in\wp_i\setminus\wp_i^2$ and a subset $Y_i\subset\mathcal{O}_k$ whose images in $\mathcal{O}_k/\mathfrak{p}(i)$ form a basis over $\mathbb{Z}/p\mathbb{Z}$. Then the set $X_i:=\{\pi_i^a y\alpha_i\,:\,a=1,\dots,l_i-1,\ y\in Y_i\}$ satisfies the requirements of part (i) of the statement of Proposition 4 (and even with 'over $\mathbb{Z}_pD_i$', replaced by 'over $\mathbb{Z}_pA_i$').*

Proof The definition of α_i ensures that the classes modulo $\hat{\mathfrak{P}}(i,1)$ of the $\iota_{i,1}(y\alpha_i)$ for $y\in Y_i$ freely generate $\hat{\mathcal{O}}_{i,1}/\hat{\mathfrak{P}}(i,1)$ over $(\mathbb{Z}/p\mathbb{Z})A_i$. Now $\iota_{i,1}(\pi_i)$ is a local uniformiser for $K_{i,1}$ so for each $a=1,\dots,l_i-1$ there is a familiar isomorphism of (finite) $\mathbb{Z}_p$-modules $\hat{\mathcal{O}}_{i,1}/\hat{\mathfrak{P}}(i,1)\to U_{i,1}^a/U_{i,1}^{a+1}$ which sends the class of x to the class of $1+\iota_{i,1}(\pi_i)^a x$. *Since $\iota_{i,1}(\pi_i)$ is fixed by A_i*, this is a $\mathbb{Z}_pA_i$-isomorphism and it follows that for each $a=1,\dots,l_i-1$ the classes modulo $U_{i,1}^{a+1}$ of the $\iota_{i,1}(1+\pi_i^a y\alpha_i)$ for $y\in Y_i$ generate $U_{i,1}^a/U_{i,1}^{a+1}$ over $\mathbb{Z}_pA_i$. The result follows easily from this. □

For each example tested, we used Propositions 4 and 5 to construct a set of $\mathbb{Z}_pG$-generators for $U^1(K_p)$ which is denoted V and has cardinality $N:=\sum_{i=1}^t|X_i|=\sum_{i=1}^t(l_i-1)|Y_i|=\sum_{i=1}^t(l_i-1)f_{\mathfrak{p}(i)}(k/\mathbb{Q})\leq\frac{pd}{p-1}\max\{e_i':i=1,\dots,t\}$.

Remark 8 By construction, each $u\in V$ is of form $\iota(v)$ for some $v\in\mathcal{O}_K$ which is congruent

to 1 modulo each $\mathfrak{P} \in S_p(K)$. At certain points in the computations it can be helpful to 'perturb' one or several such v as follows

$$v \rightsquigarrow v' := v + p^{l+1}x \text{ for some } x \in \mathcal{O}_K \text{ and } l \in \mathbb{Z},\ l \geq 1$$

Clearly, $\iota(v') \in U^1(K_p)$ and previous arguments involving $\log_p$ and $\exp_p$ can be adapted to show that

$$\iota(v') \equiv \iota(v) \pmod{U^1(K_p)^{p^l}}$$

(Indeed, $\iota_{i,j}(v'/v)$ is the p^lth power of $\exp_p(p^{-l}\log_p(1+p^{l+1}\iota_{i,j}(x/v))) \in U^1(\hat{K}_{i,j})$, convergence being assured by the fact that $l+1 > l+(1/(p-1))$ since $p > 2$.) In particular, Nakayama's Lemma implies that such perturbations do not effect the generation of $U^1(K_p)$ by V. For example, taking $l = 1$, one can modify the v's corresponding to each $u \in V$ to ensure that their coefficients with respect to a given $\mathbb{Z}$-basis of $\mathcal{O}_K$ have absolute value at most $p^2/2$.

3.4 Generators of $\bigwedge^2_{\mathbb{Z}_pG} U^1(K_p)$

Proposition 1(i) and Equation (10) show that both sides of (12) vanish for $\theta \in \bigwedge^2_{\mathbb{Z}_pG} U^1(K_p)^+$, so we only need a set of generators modulo this submodule. For the L.H.S. of (12), Proposition 1(i) shows that the same is true for $\theta \in \left(\bigwedge^2_{\mathbb{Z}_pG} U^1(K_p)\right)_{\text{tor}}$. However for the R.H.S. we have only managed to prove this under the assumption $p \nmid |G|$ (see [So3, Proposition 8]), so we proceed as follows. For the minority of examples considered where p divides $|G|$, we simply test (12) for all θ in the $\frac{1}{2}N(N-1)$-element set $W := \{v_s \wedge v_r : 1 \leq s < r \leq N\}$, with $V = \{v_1, \ldots, v_N\}$, which clearly generates all of $\bigwedge^2_{\mathbb{Z}_pG} U^1(K_p)$ over $\mathbb{Z}_pG$. For the rest of this subsection we will assume $p \nmid |G|$ and describe a second procedure to construct a subset $W' \subset W$ generating $\bigwedge^2_{\mathbb{Z}_pG} U^1(K_p)$ modulo $\bigwedge^2_{\mathbb{Z}_pG} U^1(K_p)^+ + \left(\bigwedge^2_{\mathbb{Z}_pG} U^1(K_p)\right)_{\text{tor}}$ and such that $|W'|$ is much smaller than $|W|$ (see below). By the above remarks, it will then suffice to test (12) for all θ in W'. A generic element of W will be denoted θ. Even for integers M somewhat greater than $n+1$, the computation of $\mathfrak{s}_{K/k}(\theta)$ modulo $p^M\mathbb{Z}_pG^-$ is relatively quick compared with that of $H_{K/k,n}(\eta_{K^+/k,S}, \theta)$ in $(\mathbb{Z}/p^{n+1}\mathbb{Z})G^-$. We turn this fact to our advantage by using $\mathfrak{s}_{K/k}$ itself to determine W'. Indeed, it is obvious from Proposition 1(i) that W' will have the required property if and only if $\mathfrak{S}_{K/k}$ equals the $\mathbb{Z}_pG^-$-submodule $\langle \mathfrak{s}_{K/k}(\theta) : \theta \in W' \rangle_{\mathbb{Z}_pG^-}$ of $\mathbb{Q}_pG^-$. We construct such a W' by means of an explicit isomorphism from $\mathbb{Q}_pG^-$ to a product of fields which we now describe.

Since G is small, it is easy to compute a set R^- of representatives of the orbits of the odd, irreducible characters $\chi : G \to \bar{\mathbb{Q}}^\times$ under the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. The $\mathbb{Q}$-linear extension of each such character χ defines a homomorphism from $\mathbb{Q}G^-$ to $F_\chi := \mathbb{Q}(\chi)$ such that the product over $\chi \in R^-$ is a ring isomorphism $X^- : \mathbb{Q}G^- \to \prod_{\chi \in R^-} F_\chi$. Tensoring over $\mathbb{Q}$ with $\mathbb{Q}_p$ we get the first isomorphism, X_p^-, below.

$$\mathbb{Q}_pG^- \xrightarrow{X_p^-} \prod_{\chi \in R^-} (F\chi \otimes \mathbb{Q}_p) \xrightarrow{Z_p^-} \prod_{\chi \in R^-} \prod_{\mathfrak{P} \in S_p(F_\chi)} F_{\chi,\mathfrak{P}} \tag{18}$$

The second, Z_p^-, is the product over $\chi \in R^-$ of the isomorphisms from $F_\chi \otimes \mathbb{Q}_p$ to the product of the completions of F_χ at primes above p, the latter taking $a \otimes x$ to the vector $(x\iota_{\mathfrak{P}}(a))_{\mathfrak{P}}$. Let us write the composite isomorphism $Z_p^- \circ X_p^-$ as $\alpha = \prod_\chi \prod_{\mathfrak{P}} \alpha_{\chi,\mathfrak{P}}$. We identify $\mathbb{Z}_pG^-$ with $((1-c)\mathbb{Z}G) \otimes \mathbb{Z}_p$ considered as a subring of $\mathbb{Q}G^- \otimes \mathbb{Q}_p$ which we are identifying with $\mathbb{Q}_pG^-$. It is clear that X_p^- sends $\mathbb{Z}_pG^-$ into $\prod_{\chi \in R^-}(\mathcal{O}_\chi \otimes \mathbb{Z}_p)$ where $\mathcal{O}_\chi := \mathbb{Z}[\chi] = \mathcal{O}_{F_\chi}$ and that the image surjects onto each component (since $p \neq 2$). For a given $\chi \in R^-$, let us write $e(\chi)$ for the sum of the idempotents in $\bar{\mathbb{Q}}G$ belonging to the irreducible characters in the $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-orbit of χ. It is easy to see that $e(\chi)$ lies in $(1-c)|G|^{-1}\mathbb{Z}G$ inside $\mathbb{Q}G^-$ and hence that $e(\chi) \otimes 1$ lies in $\mathbb{Z}_pG^-$ (since $p \nmid |G|$). The orthogonality relations imply that $X_p^-(e(\chi) \otimes 1)$ has component 1 at χ and 0 elsewhere. It follows that $\mathbb{Z}_pG^-$ is sent isomorphically onto $\prod_{\chi \in R^-}(\mathcal{O}_\chi \otimes \mathbb{Z}_p)$ by X_p^-. Hence α maps it isomorphically onto the image of the latter under Z_p^- which, by standard facts, is $\prod_{\chi \in R^-}\prod_{\mathfrak{P} \in S_p(F_\chi)} \mathcal{O}_{\chi,\mathfrak{P}}$, where $\mathcal{O}_{\chi,\mathfrak{P}}$ denotes the ring of integers of $F_{\chi,\mathfrak{P}}$. The values of χ are roots of unity of order prime to p. It follows that $F_\chi/\mathbb{Q}$ is unramified at p so that each $\mathcal{O}_{\chi,\mathfrak{P}}$ is a complete d.v.r. with maximal ideal $p\mathcal{O}_{\chi,\mathfrak{P}}$.

Both $\mathfrak{S}_{K/k}$ and $\mathbb{Z}_pG^-\mathfrak{s}_{K/k}(\theta)$ (for any $\theta \in W$) are $\mathbb{Z}_pG^-$ submodules of $\mathbb{Q}_pG^-$. Hence, for each pair $(\chi, \mathfrak{P})$ and each $\theta \in W$ there exist $m(\chi,\mathfrak{P})$ and $m(\chi,\mathfrak{P};\theta)$ in $\mathbb{Z} \cup \{\infty\}$ such that (taking $p^\infty = 0$):

$$\alpha(\mathfrak{S}_{K/k}) = \prod_{\chi \in R^-}\prod_{\mathfrak{P} \in S_p(F_\chi)} p^{m(\chi,\mathfrak{P})}\mathcal{O}_{\chi,\mathfrak{P}} \quad \text{and} \quad \alpha(\mathbb{Z}_pG^-\mathfrak{s}_{K/k}(\theta)) = \prod_{\chi \in R^-}\prod_{\mathfrak{P} \in S_p(F_\chi)} p^{m(\chi,\mathfrak{P};\theta)}\mathcal{O}_{\chi,\mathfrak{P}}$$

Of course, $m(\chi,\mathfrak{P};\theta)$ is just $\mathrm{ord}_p(\alpha_{\chi,\mathfrak{P}}(\mathfrak{s}_{K/k}(\theta)))$, while $m(\chi,\mathfrak{P}) < \infty$ by Proposition 1(ii) and $m(\chi,\mathfrak{P}) \geq 0$ since the Integrality Conjecture is known for $p \nmid |G|$ by [So3, Cor. 1]. The properties of d.v.r.'s give the equivalence

$$\mathfrak{S}_{K/k} = \langle \mathfrak{s}_{K/k}(\theta) : \theta \in W \rangle_{\mathbb{Z}_pG^-} \iff m(\chi,\mathfrak{P}) = \min\{m(\chi,\mathfrak{P};\theta) : \theta \in W\} \text{ for all } (\chi,\mathfrak{P}) \tag{19}$$

Since the first equality holds by construction of W, so must the second and in particular $m(\chi,\mathfrak{P};\theta) \geq 0$ $\forall \chi,\mathfrak{P},\theta$. For each pair $(\chi,\mathfrak{P})$ we define $W_{\min}(\chi,\mathfrak{P})$ to be the non-empty subset of W on which $m(\chi,\mathfrak{P};\theta)$ attains its minimum. By the above, $W_{\min}(\chi,\mathfrak{P}) = \{\theta \in W : m(\chi,\mathfrak{P};\theta) = m(\chi,\mathfrak{P})\}$.

The construction of W' begins by using Proposition 3 to compute an approximation to $\mathfrak{s}_{K/k}(\theta)$ for each $\theta \in W$, with a guaranteed p-adic precision of p^{-M} for a moderate value of $M \geq n+1$, *e.g.* $M = n+3$. Since each θ is already expressed as $u_1 \wedge u_2$ for 'global' elements u_1 and u_2 in the sense of Remark 7(ii)), the latter and Proposition 3 naturally give rise to an approximation in $\mathbb{Q}G^-$, which we somewhat abusively write as $\mathfrak{s}_{K/k}(\theta;M)$, such that $\mathfrak{s}_{K/k}(\theta) - \mathfrak{s}(\theta;M) \in p^M\mathbb{Z}_pG^-$. Now, fixing $\chi \in R^-$ and $\mathfrak{P} \in S_p(F_\chi)$, we may compute the values $\mathrm{ord}_p(\alpha_{\chi,\mathfrak{P}}(\mathfrak{s}(\theta;M)))$ one by one for each $\theta \in W$, since these are just $\mathrm{ord}_{\mathfrak{P}}(\chi(\mathfrak{s}(\theta;M)))$, by construction of α. Suppose $W_{<M}(\chi,\mathfrak{P},M)$ is the subset of those θ in W for which we find $\mathrm{ord}_p(\alpha_{\chi,\mathfrak{P}}(\mathfrak{s}(\theta;M))) < M$. By the ultrametric inequality, if θ lies in $W_{<M}(\chi,\mathfrak{P},M)$ then we must have $m(\chi,\mathfrak{P};\theta) = \mathrm{ord}_p(\alpha_{\chi,\mathfrak{P}}(\mathfrak{s}(\theta;M)))$. Otherwise we know only that $m(\chi,\mathfrak{P};\theta) \geq M$. This means that if $W_{<M}(\chi,\mathfrak{P},M)$ is non-empty, we may compute $W_{\min}(\chi,\mathfrak{P})$ as the subset

of $W_{<M}(\chi,\mathfrak{P},M)$ on which $\mathrm{ord}_p(\alpha_{\chi,\mathfrak{P}}(\mathfrak{s}(\theta;M)))$ attains its minimum, and then pass to the next pair $(\chi,\mathfrak{P})$. However, in a very small number of examples we encountered a pair $(\chi,\mathfrak{P})$ for which $W_{<M}(\chi,\mathfrak{P},M)=\varnothing$ for the initial value of M. In this case we simply recalculated the $\mathfrak{s}(\theta;M)$'s with a larger value of M until $W_{<M}(\chi,\mathfrak{P},M)\neq\varnothing$ for that pair and then continued with the increased value of M. This simple hit-and-miss procedure terminated rapidly enough: in all cases we were able to determine $W_{\min}(\chi,\mathfrak{P})$ for all pairs $(\chi,\mathfrak{P})$ without ever taking $M>n+5$.

The equivalence obtained by replacing W by W' in (19) shows that a subset $W'\subset W$ will have the required property iff $W'\cap W_{\min}(\chi,\mathfrak{P})\neq\varnothing$ for all pairs $(\chi,\mathfrak{P})$. Picking an element at random from each $W_{\min}(\chi,\mathfrak{P})$ would give a subset W' whose cardinality could not exceed the number of pairs $(\chi,\mathfrak{P})$ which in turn is at most $\dim_{\mathbb{Q}_p}\mathbb{Q}_pG^-=\frac{1}{2}|G|$, by (18). This is already much smaller than $|W|$ in most cases. In practice, however, there was a tendency for $\bigcap_{\chi,\mathfrak{P}}W_{\min}(\chi,\mathfrak{P})$ to be non-empty, so we could simply take $W'=\{\theta_0\}$ for any θ_0 in this intersection. This tendency is explained by the fact that, as a submodule of finite index in $\mathbb{Z}_pG^-$ (which is a product of d.v.r.'s), $\mathfrak{S}_{K/k}$ is automatically free over $\mathbb{Z}_pG^-$ with one generator. While there is no guarantee that W contains such a generator, it is not surprising that it often does. In fact, if this failed for our initial choice of W, the best practical solution was simply to randomly modify W once or twice until it did (*e.g.* by changing the elements a_i and $x_{i,j}$ used in Prop. 4 to construct V). We thus achieved $|W'|=1$ in all cases without too much difficulty.

Remark 9 The procedure described above for $p\nmid|G|$ determines the values $m(\chi,\mathfrak{P})$ for all $(\chi,\mathfrak{P})$ as a by-product. However, they are also given explicitly by 'index formula' (31) of [So3] (see also (32) of *ibid.*). One should take 'ϕ' to be the composition of χ with any embedding $\bar{\mathbb{Q}}\to\bar{\mathbb{Q}}_p$ inducing $\mathfrak{P}$. Using this formula, one could in principle select the initial value of M to be greater than the maximum of the $m(\chi,\mathfrak{P})$'s, thereby ensuring that $W_{<M}(\chi,\mathfrak{P},M)\neq\varnothing$ for all $(\chi,\mathfrak{P})$.

3.5 Computation of $\eta_{K^+/k,S^1}$

We need to determine the Rubin-Stark element $\eta_{K^+/k,S^1}$, that is, the unique (conjectural) element of $\bigwedge^2_{\mathbb{Q}\bar{G}}\mathbb{Q}U_{S^1}(K^+)$ that satifies the eigenspace condition w.r.t. $(S^1,d,\bar{G})$ and Equation (5). The first statement in the Congruence Conjecture tells us to expect $\eta_{K^+/k,S}$ to lie in $\mathbb{Z}_{(p)}\Lambda_{0,S}(K^+/k)$. (As noted in Remark 5, this is also predicted by Conjecture B' of [Ru].) Assuming this *and also* $p\nmid|\bar{G}|$, we shall now sketch a proof that $\eta_{K^+/k,S^1}$ must in fact be of the rather more precise form

$$\eta_{K^+/k,S^1}=(1\otimes\alpha_{S^1})\left(\frac{1}{a}\otimes(\varepsilon_1\wedge\varepsilon_2)\right)\quad\text{for some }\varepsilon_1,\varepsilon_2\in U_{S(p)}(K^+)\text{ and }a\in\mathbb{Z},\ p\nmid a\quad(20)$$

where $S(p):=S_\infty\cup S_p$. First, by Remark 1, these hypotheses imply $\eta_{K^+/k,S^1}=(1\otimes\alpha_{S^1})(\tilde{\eta})$ for a (unique) $\tilde{\eta}\in\mathbb{Z}_{(p)}\otimes\bigwedge^d_{\mathbb{Z}\bar{G}}U_{S^1}(K^+)$. Identifying the latter module with $\bigwedge^d_{\mathbb{Z}_{(p)}\bar{G}}\mathbb{Z}_{(p)}\otimes U_{S^1}(K^+)$, we may write $\tilde{\eta}=\sum_{i=1}^N x_{1,i}\wedge x_{2,i}$ where $x_{1,i},x_{2,i}\in\mathbb{Z}_{(p)}\otimes U_{S^1}(K^+)$. Writing e_{S^1}

for the idempotent $e_{S^1,2,\bar{G}} \in |\bar{G}|^{-1}\mathbb{Z}\bar{G} \subset \mathbb{Z}_{(p)}\bar{G}$, the eigenspace condition gives

$$\eta_{K^+/k,S^1} = e_{S^1}(1 \otimes \alpha_{S^1})(\tilde{\eta}) = (1 \otimes \alpha_{S^1})(e_{S^1}\tilde{\eta}) = (1 \otimes \alpha_{S^1})(\sum_{i=1}^{N} e_{S^1}x_{1,i} \wedge e_{S^1}x_{2,i})$$

Now consider $A_{S^1} := e_{S^1}(\mathbb{Z}_{(p)} \otimes U_{S^1}(K^+))$ as a module over the ring $e_{S^1}\mathbb{Z}_{(p)}\bar{G}$ which is a product of p.i.d.'s (again because $p \nmid |\bar{G}|$). Since $p \neq 2$, A_{S^1} is $\mathbb{Z}$-torsionfree. Moreover $\mathbb{Q}A_{S^1}$ is free of rank 2 over $e_{S^1}\mathbb{Q}\bar{G}$. (This follows from the definition of $e_{S^1,2,\bar{G}}$ and the fact that $\dim_{\mathbb{C}}(e_{\chi^{-1},\bar{G}}\mathbb{C}U_{S^1}(K^+)) = \mathrm{ord}_{s=0}L_{K^+/k,S^1}(s,\chi)$ for all $\chi \in \hat{\bar{G}}$.) It follows easily that A_{S^1} is free of rank 2 over $e_{S^1}\mathbb{Z}_{(p)}\bar{G}$ and it is not hard to see that any pair of basis elements can be written $\frac{1}{a_1} \otimes \alpha_1$, $\frac{1}{a_2} \otimes \alpha_2$ where $p \nmid a_1, a_2 \in \mathbb{Z}$ and and α_1, α_2 lie in $(|\bar{G}|e_{S^1})U_{S^1}(K^+)$. Writing each $e_{S^1}x_{1,i}$ and $e_{S^1}x_{2,i}$ in such a basis, we conclude that $\tilde{\eta}$ is a $\mathbb{Z}_{(p)}\bar{G}$-multiple of $1 \otimes (\alpha_1 \wedge \alpha_2)$. Equation (20) will clearly follow if we can show $(|\bar{G}|e_{S^1})U_{S^1}(K^+) \subset U_{S(p)}(K^+)$. If $S^1 = S(p)$, this is immediate. Otherwise $|S^1| > d+1$ and [So3, eq. (13)] shows that $N_{D_\mathfrak{q}}e_{S^1} = 0$ where $N_{D_\mathfrak{q}} \in \mathbb{Z}\bar{G}$ is the norm element of the decomposition subgroup $D_\mathfrak{q} \subset \bar{G}$ for any prime $\mathfrak{q} \in S^1 \setminus S_\infty$. Thus every element of $(|\bar{G}|e_{S^1})U_{S^1}(K^+)$ is killed by every such $N_{D_\mathfrak{q}}$ which implies that, in fact, $(|\bar{G}|e_{S^1})U_{S^1}(K^+) \subset U_{S_\infty}(K^+)$ *i.e.* in this case, we can actually take $\varepsilon_1, \varepsilon_2 \in \mathcal{O}_{K^+}^\times$ in (20).

Let us write $\mathcal{U}(p)$ for $\mathbb{Q} \otimes \bigwedge^2_{\mathbb{Z}\bar{G}} U_{S(p)}(K^+)$ considered as a $\mathbb{Q}\bar{G}$-submodule of $\bigwedge^2_{\mathbb{Q}\bar{G}} \mathbb{Q}U_{S^1}(K^+)$. If $p \nmid |\bar{G}|$, we have just shown that the Congruence Conjecture implies (20) or, equivalently,

$$\eta_{K^+/k,S^1} = \frac{1}{a} \otimes (\varepsilon_1 \wedge \varepsilon_2) \in e_{S^1}\mathcal{U}(p) \quad \text{for some } \varepsilon_1, \varepsilon_2 \in U_{S(p)}(K^+) \text{ and } a \in \mathbb{Z},\ p \nmid a \tag{21}$$

If $p||\bar{G}|$ and we assume only that the Rubin-Stark element $\eta_{K^+/k,S^1}$ exists, then similar but simpler arguments (replacing $\mathbb{Z}_{(p)}$ by $\mathbb{Q}$) still show that

$$\eta_{K^+/k,S^1} = \frac{1}{a} \otimes (\varepsilon_1 \wedge \varepsilon_2) \in e_{S^1}\mathcal{U}(p) \quad \text{for some } \varepsilon_1, \varepsilon_2 \in U_{S(p)}(K^+) \tag{22}$$

and also that $e_{S^1}\mathcal{U}(p)$ is free of rank 1 over $e_{S^1}\mathbb{Q}\bar{G}$. These observations motivate the following procedure for determining $\eta_{K^+/k,S^1}$ which is much simpler than the one used in [R-S1] but still sufficient for present purposes. First we compute an $e_{S^1}\mathbb{Q}\bar{G}$-generator of $e_{S^1}\mathcal{U}(p)$ in the form $1 \otimes (\gamma_1 \wedge \gamma_2)$. For this, we compute a $\mathbb{Z}$-basis modulo $\{\pm 1\}$ of the f.g. multiplicative abelian group $U_{S(p)}(K^+)$. (Note that functions to perform this computation are implemented in PARI/GP.) Once a basis is known, we use it to construct two random elements γ_1, γ_2 in $U_{S(p)}(K^+)$. If $1 \otimes (\gamma_1 \wedge \gamma_2)$ does not lie in $e_{S^1}\mathcal{U}(p)$ we replace, say, γ_1 by $(|G|e_{S^1})\gamma_1$ so that it does. Then $1 \otimes (\gamma_1 \wedge \gamma_2)$ will generate $e_{S^1}\mathcal{U}(p)$ if (and, in fact, only if) $\chi(R_{K^+/k,S(p)}((1 \otimes \gamma_1) \wedge (1 \otimes \gamma_1)))$ is non-zero for all characters $\chi \in \hat{\bar{G}}$ such that $\mathrm{ord}_{s=0}L_{K^+/k,S}(s,\chi) = 2$. These conditions can be unconditionally tested using a good enough approximation to $R_{K^+/k,S(p)}((1 \otimes \gamma_1) \wedge (1 \otimes \gamma_1))$, calculated as a group-ring determinant involving real logarithms of (absolute values of) conjugates of γ_1 and γ_2. If they are not satisfied, we recommence with two new random elements γ_1 and γ_2. (For our initial 'random'

choices of γ_1 and γ_2 we actually took pairs of distinct elements of the computed $\mathbb{Z}$-basis of $U_{S(p)}(K^+)$. In the few cases where this did not provide a generator, we then looked at pairs consisting of 'simple' random linear combinations of these basis elements.)

We now know that the unique element $\eta_{K^+/k,S^1}$ – if it exists – will be equal to $A(1 \otimes (\gamma_1 \wedge \gamma_2))$ for any $A \in \mathbb{Q}\bar{G}$ satisfying

$$A\, R_{K^+/k,S^1}((1 \otimes \gamma_1) \wedge (1 \otimes \gamma_1)) = \Theta^{(d)}_{K^+/k,S^1}(0) \tag{23}$$

(by (5)). We compute an approximation of $\Theta^{(d)}_{K^+/k,S^1}(0)$ in $\mathbb{R}\bar{G}$ using its expression in terms of Artin L-functions (see the beginning of Section 2.2), once again using the methods of [D-T], or [Co, Section 10.3]. Then we can find a solution $\tilde{A} \in \mathbb{R}\bar{G}$ of Equation (23) to a high precision. Standard methods allow us to compute an element $A_0 \in \mathbb{Q}\bar{G}$ very close to $\tilde{A}$ and with coefficients of small height. We then write A_0 as $\frac{1}{a}B_0$ where $a \in \mathbb{Z}_{>0}$ and B_0 is an element of $\mathbb{Z}\bar{G}$, the g.c.d. of whose coefficients is prime to a. Assuming that A_0 is in fact an *exact* solution of Equation (23) (see below) we now have the desired expression (22) with $\varepsilon_1 = \gamma_1$, $\varepsilon_2 = B_0\,\gamma_2$. However, we shall see in the next section that the computations of $H_{K/k,n}(\eta_{K^+/k,S^1}, \theta)$ are *much* easier if (21) holds. Thus if p divides a we find a new generator $1 \otimes (\gamma_1 \wedge \gamma_2)$ and repeat the process. We have justified above the expectation that (21) is possible whenever $p \nmid |\bar{G}|$ and indeed the above process terminated with such an expression in all our examples of this type. More surprisingly, perhaps, it also terminated with a solution of (21) in all our examples with $p||\bar{G}|$. Very similar behaviour was observed in [R-S1] (see also [So1, Rem. 3.4]). Thus it seems, experimentally at least, that Rubin-Stark elements are 'usually' better-behaved in this sense than the various conjectures predict, although no convincing sharpening has yet been proposed along these lines.

Remark 10 We need to convince ourselves that this is indeed the Rubin-Stark element and not some *ad hoc* element of $e_{S^1}\mathcal{U}_p$ constructed simply to satisfy Equation (5) to the working precision. A first significant fact is that while we are working with a large precision – usually of 100 digits – the coefficients of A_0 are of very small height. In almost all examples numerators and denominators of the coefficients of A_0 are less than 10 in absolute value, the largest ones being in example `E5` where they have up to 6 digits. However this is still considerably smaller than one would expect if $\tilde{A}$ were a random element of $\mathbb{R}\bar{G}$. A second and even more convincing way to reassure ourselves that we really have the Rubin-Stark element is as follows. Once we have calculated an element $\hat{\eta} = \frac{1}{a} \otimes (\varepsilon_1 \wedge \varepsilon_2)$, say, of $e_{S^1}\mathcal{U}(p)$ as a candidate for $\eta_{K^+/k,S^1}$, we significantly increase the working precision, say from 100 to 150 digits. We then recompute $R_{K^+/k}(\hat{\eta})$ and $\Theta^{(d)}_{K^+/k,S^1}(0)$ to the new precision and check whether they still agree. If $\hat{\eta}$ were an *ad hoc* element, constructed to satisfy Equation (5) to a precision of 100 digits, then there would be no reason for it to satisfy it to 150 digits. The fact that it always did so, without readjustment, was, we felt, convincing enough evidence to take $\eta_{K^+/k,S^1} = \hat{\eta}$.

3.6 Computation of $H_{K/k,n}$ and Verification of the Conjecture

To complete the verification of the Congruence Conjecture, it suffices to check that $\mathfrak{s}_{K/k}(\theta)$ lies in $\mathbb{Z}_pG^-$ and that the two sides of (12) agree, for all θ in an appropriate subset of $\bigwedge^2_{\mathbb{Z}_pG} U^1(K_p)$. The determination of this subset, as well as the treatment of the L.H.S., is divided into three cases. In Case 1 (*i.e.* examples `B6`, `C8`, `D7`, `D9` and `D11`) $\eta_{K^+/k,S^1} = 0$ because $e_{S^1} = 0$. It then suffices to calculate an approximation to $\mathfrak{s}_{K/k}(\theta)$ up to an element of $p^{n+1}\mathbb{Z}_pG^-$ for each θ in W, the initial $\mathbb{Z}_pG$-generating set for $\bigwedge^2_{\mathbb{Z}_pG} U^1(K_p)$ constructed in Section 3.4. These approximations are calculated using Proposition 3 with $M = n+1$ and the conjecture is verified if and only if each actually lies in $p^{n+1}\mathbb{Z}_pG^-$. In the remainder of our examples, $\eta_{K^+/k,S^1}$ is *non-zero* and the computation of the R.H.S. of (12) is usually lengthy. In Case 2, $p \nmid |G|$ and we explained at the beginning of Subsection 3.4 why it is sufficient to check (12) for each θ in the much smaller set W' generating modulo $\bigwedge^2_{\mathbb{Z}_pG} U^1(K_p)^+ + \left(\bigwedge^2_{\mathbb{Z}_pG} U^1(K_p)\right)_{\text{tor}}$ constructed there. This very construction included the computation of an element of $\mathbb{Q}G^-$ approximating $\mathfrak{s}_{K/k,S}(\theta)$ up to an element of $p^{n+1}\mathbb{Z}_pG^-$ (at least) for all $\theta \in W'$. In Case 3, $p||G|$ and we are unable to reduce W. So, once again we use Proposition 3 to calculate an approximation to $\mathfrak{s}_{K/k}(\theta)$ up to an element of $p^{n+1}\mathbb{Z}_pG^-$ for each θ in the full set W.

It remains to explain the computation of the R.H.S. of (12) in the second and third cases above, where $\eta_{K^+/k} := \eta_{K^+/k,S^1} \neq 0$. The τ_i are realised as elements of $\mathrm{Gal}(F/\mathbb{Q})$ and since F contains K and hence $\mu_{p^{n+1}}$, the quantity $\kappa_n(\tau_1\tau_2)$ may be determined directly by calculating $\xi_{p^{n+1}}^{\tau_1\tau_2}$. The computation of $H_{K/k,n}(\eta_{K^+/k},\theta)$ is greatly facilitated by the fact that Equation (21) – hence also (20) – holds in every case, as already noted. Indeed, from diagram (11) it follows that

$$H_{K/k,n}(\eta_{K^+/k},\theta) = \bar{a}^{-1}\mathcal{H}_{K/k,n}(\varepsilon_1 \wedge \varepsilon_2,\theta) \quad \text{for all } \theta \in \textstyle\bigwedge^2_{\mathbb{Z}_pG} U^1(K_p) \tag{24}$$

where $\bar{a}$ is the reduction of a modulo p^{n+1}. Recall that every $\theta \in W$ is 'global' by construction, *i.e.* of the form $\iota(v_1) \wedge \iota(v_2)$ for some $v_1, v_2 \in K^\times$. Therefore, using (24), the conditions satisfied by the ε_i and the definitions of $\mathcal{H}_{K/k,n}$ and $[\cdot,\cdot]_{K,n,G}$, it suffices to be able to calculate $[\varepsilon,\iota(v)]_{K,n}$ for any $v \in K^\times$ and $\varepsilon \in U_{S(p)}(K^+)$. The next Proposition shows how we did this. (The basic idea is well-known, see *e.g.* [Gr, § II.7.5].) Let $\mathfrak{Q}$ be any prime ideal of $\mathcal{O}_K$. If $\mathfrak{Q} \notin S_p(K)$ then reduction modulo $\mathfrak{Q}$ gives an injection $\mu_{p^{n+1}}(K) \to (\mathcal{O}_K/\mathfrak{Q})^\times$ so that $p^{n+1}|(N\mathfrak{Q}-1)$ and the image is the subgroup of $(N\mathfrak{Q}-1)/p^{n+1}$-th powers in $(\mathcal{O}_K/\mathfrak{Q})^\times$. Thus, for each such $\mathfrak{Q}$ there is a homomorphism $\mathrm{apr}_{\mathfrak{Q},n} : (\mathcal{O}_K/\mathfrak{Q})^\times \to \mathbb{Z}/p^{n+1}\mathbb{Z}$ (the *additive, p^{n+1}-th power residue symbol modulo* $\mathfrak{Q}$) uniquely defined by $\bar{\xi}_{p^{n+1}}^{\mathrm{apr}_{\mathfrak{Q},n}(\bar{b})} = \bar{b}^{(N\mathfrak{Q}-1)/p^{n+1}}$ for all $\bar{b} \in (\mathcal{O}_K/\mathfrak{Q})^\times$. For the small values of p^{n+1} occurring here, $\mathrm{apr}_{\mathfrak{Q},n}$ is quick to calculate directly and we have:

Proposition 6 *If $\varepsilon \in U_{S(p)}(K^+)$ and $v \in K^\times$, then*

$$[\varepsilon,\iota(v)]_{K,n} = \sum_{\mathfrak{Q} \notin S_p(K)} \mathrm{ord}_{\mathfrak{Q}}(v)\mathrm{apr}_{\mathfrak{Q},n}(\bar{\varepsilon})$$

where $\mathfrak{Q}$ runs over the (finite) set of prime ideals $\mathfrak{Q}$ of $\mathcal{O}_K$ not dividing p (and such that $\mathrm{ord}_{\mathfrak{Q}}(v) \neq 0$).

PROOF Let L^ε be the Kummer extension $K(\varepsilon^{1/p^{n+1}})$ and write h_ε for the isomorphism $\mathrm{Gal}(L^\varepsilon/K) \to \mathbb{Z}/p^{n+1}\mathbb{Z}$ given by $h_\varepsilon(g) = \mathrm{Ind}_n(g(\varepsilon^{1/p^{n+1}})/\varepsilon^{1/p^{n+1}})$. (Everything is independent of the choice of root $\varepsilon^{1/p^{n+1}}$.) For each prime ideal $\mathfrak{Q}$ of $\mathcal{O}_K$ we choose a prime ideal $\tilde{\mathfrak{Q}}$ dividing $\mathfrak{Q}$ in $\mathcal{O}_{L^\varepsilon}$ and write $\mathrm{rec}_{\mathfrak{Q}}$ for the composite homomorphism

$$K^\times \xrightarrow{\iota_{\mathfrak{Q}}} K_{\mathfrak{Q}}^\times \longrightarrow D_{\tilde{\mathfrak{Q}}}(L^\varepsilon/K) \hookrightarrow \mathrm{Gal}(L^\varepsilon/K)$$

where the second homomorphism is the local reciprocity map. (This is independent of the choice of $\tilde{\mathfrak{Q}}$.) It follows easily from the definition and alternating property of the local Hilbert symbol $(\cdot,\cdot)_{K_{\mathfrak{P}},p^{n+1}}$ (see [Ne, Prop. 3.2]) for $\mathfrak{P} \in S_p(K)$ that

$$h_\varepsilon(\mathrm{rec}_{\mathfrak{P}}(v)) = \mathrm{Ind}_n(\iota_{\mathfrak{P}}^{-1}(\iota_{\mathfrak{P}}(v), \iota_{\mathfrak{P}}(\varepsilon))) = -\mathrm{Ind}_n(\iota_{\mathfrak{P}}^{-1}(\iota_{\mathfrak{P}}(\varepsilon), \iota_{\mathfrak{P}}(v))_{K_{\mathfrak{P}},p^{n+1}}) \quad \text{for all } \mathfrak{P} \in S_p(K) \tag{25}$$

On the other hand, if $\mathfrak{Q} \notin S_p(K)$ then the extension L^ε/K is unramified at $\mathfrak{Q}$ (since $\varepsilon \in U_{S(p)}(K^+)$) and so $\mathrm{rec}_{\mathfrak{Q}}(v) = \sigma_{\mathfrak{Q},L^\varepsilon/K}^{\mathrm{ord}_{\mathfrak{Q}}(v)}$ where $\sigma_{\mathfrak{Q},L^\varepsilon/K}$ denotes the Frobenius element. Since $\varepsilon^{1/p^{n+1}}$ is a local unit at $\tilde{\mathfrak{Q}}$, the definition of $\sigma_{\mathfrak{Q},L^\varepsilon/K}$ tells us that the image of the p^{n+1}th root of unity $\sigma_{\mathfrak{Q},L^\varepsilon/K}(\varepsilon^{1/p^{n+1}})/\varepsilon^{1/p^{n+1}}$ in $(\mathcal{O}_K/\mathfrak{Q})^\times \subset (\mathcal{O}_{L^\varepsilon}/\tilde{\mathfrak{Q}})^\times$ is equal to that of $\varepsilon^{(N\mathfrak{Q}-1)/p^{n+1}}$. It follows that

$$h_\varepsilon(\mathrm{rec}_{\mathfrak{Q}}(v)) = \mathrm{ord}_{\mathfrak{Q}}(v) h_\varepsilon(\sigma_{\mathfrak{Q},L^\varepsilon/K}) = \mathrm{ord}_{\mathfrak{Q}}(v)\mathrm{apr}_{\mathfrak{Q},n}(\bar{\varepsilon}) \quad \text{for all } \mathfrak{Q} \notin S_p(K) \tag{26}$$

In particular $h_\varepsilon(\mathrm{rec}_{\mathfrak{Q}}(v))$, and therefore $\mathrm{rec}_{\mathfrak{Q}}(v)$, is trivial for almost all $\mathfrak{Q}$. Finally, global class-field theory tells us that the product of $\mathrm{rec}_{\mathfrak{Q}}(v)$ over all prime ideals is equal to $1 \in \mathrm{Gal}(L^\varepsilon/K)$. (Since K is totally complex the local reciprocity map is trivial at archimedean places.) Using this and equations (7), (25) and (26), we get

$$[\varepsilon, \iota(v)]_{K,n} = -\sum_{\mathfrak{P}\in S_p(K)} h_\varepsilon(\mathrm{rec}_{\mathfrak{P}}(v)) = \sum_{\mathfrak{Q}\notin S_p(K)} h_\varepsilon(\mathrm{rec}_{\mathfrak{Q}}(v)) = \sum_{\mathfrak{Q}\notin S_p(K)} \mathrm{ord}_{\mathfrak{Q}}(v)\mathrm{apr}_{\mathfrak{Q},n}(\bar{\varepsilon})$$

as required. □

REMARK 11 In order to compute $H_{K/k,n}(\eta_{K^+/k}, \theta)$ for θ in W (or W') using the Proposition, one needs to compute the prime-ideal factorisation of (v_1) and (v_2) in K where $\theta = \iota(v_1) \wedge \iota(v_2)$. Since, moreover, the v_i's lie in $\mathcal{O}_K$, the first step is to factor the absolute norm of v_i, $i = 1, 2$. Unfortunately, the v_i's constructed by the method of Propositions 4 and 5 tend to have very large norms which can be divisible by more than one large prime number and hence virtually impossible to factor. We get around this problem by perturbing one or more of the v_i's, *i.e.* replacing v_i by $v_i' := v_i + p^{n+2}x_i$ for a random element $x_i \in \mathcal{O}_K$ for $i = 1, 2$. Remark 8 (with $l = n+1$) implies that $\iota(v_1') \wedge \iota(v_2') \equiv \theta$ modulo $p^{n+1}\bigwedge^2_{\mathbb{Z}_p G} U^1(K_p)$ and so $H_{K/k,n}(\eta_{K^+/k}, \theta) = H_{K/k,n}(\eta_{K^+/k}, \iota(v_1') \wedge \iota(v_2'))$. Thus we may proceed as follows. We set some time limit, say two minutes during which we try to factor the norm of of each v_i. If

we fail, we just perturb one or more of the v_i's as above and try again. Indeed, although v_i''s usually have norms of about the same size as those of the v_i's, it usually happens that after several tries, we find norms that are (relatively) easy to factor, allowing us to calculate $H_{K/k,n}(\eta_{K^+/k}, \iota(v_1') \wedge \iota(v_2'))$ *i.e.* $H_{K/k,n}(\eta_{K^+/k}, \theta)$.

4 Results of the Computations

4.1 An Example

We illustrate the numerical computations with example `B1` (see next subsection). We have $p = 3$ and $n = 0$, k is the real quadratic field $\mathbb{Q}(\sqrt{6})$ (thus p ramifies in $k/\mathbb{Q}$), K^+ is the ray-class field of k of conductor $4\mathfrak{p}$ where $\mathfrak{p}$ is the unique prime ideal of k dividing 3, and $K = K^+(\xi_3)$. The extension K^+/k is of degree 4 with Galois group $\bar{G}$ isomorphic to C_2^2, and the extension K/k has degree 8 and its Galois group G is isomorphic to C_2^3. In particular, p does not divide $|G|$.

The extension $K/\mathbb{Q}$ is a Galois extension, but is not abelian, and we have $K = \mathbb{Q}(\nu)$ where ν is a root of the irreducible polynomial

$$X^{16} - 8X^{15} + 48X^{14} - 196X^{13} + 642X^{12} - 1668X^{11} + 3580X^{10} - 6328X^9 + 9297X^8 \\ - 11276X^7 + 11224X^6 - 9024X^5 + 5736X^4 - 2780X^3 + 972X^2 - 220X + 25$$

We find $\mathfrak{p}\mathcal{O}_{K^+} = \mathfrak{P}_+^2$ (so that $e_{\mathfrak{P}_+}(K^+/k) = f_{\mathfrak{P}_+}(K^+/k) = 2$) and $\mathfrak{P}_+\mathcal{O}_K = \mathfrak{P}\mathfrak{P}'$. Finally, we have $S = S^1 = \{\infty_1, \infty_2, \mathfrak{p}, \mathfrak{q}_2\}$ where $2\mathcal{O}_k = \mathfrak{q}_2^2$.

Let $\sigma_1, \sigma_2, \sigma_3$ be three distinct k-automorphisms of K of order 2 such that $G = \langle \sigma_1, \sigma_2, \sigma_3 \rangle$, with the convention that $\sigma_3 : \nu \mapsto 1 - \nu$ is the complex conjugation of the CM field K. Using the method of Subsection 3.2, we find that

$$a_{K/k}^- = \frac{1}{2^6\,3^2}(\sigma_3 - 1)\left(3 + 2\sqrt{3} + \sigma_1 + \sigma_1\sigma_2 + \left(3 - 2\sqrt{3}\right)\sigma_2\right)$$

With the notations of Subsection 3.3, we have $t = 1$, $h_1 = 2$ (with $\mathfrak{p}(1) = \mathfrak{p}$, $\mathfrak{P}(1,1) = \mathfrak{P}$, $\mathfrak{P}(1,2) = \mathfrak{P}'$) and $e_{\mathfrak{P}(1,j)}(K/\mathbb{Q}) = 4$ for $j = 1, 2$. Thus $l_1 = 7$, and Propositions 4 and 5 enable us to construct 6 elements such that the set W of wedge product of two of these generate $\bigwedge^2_{\mathbb{Z}_pG} U^1(K_p)$ over $\mathbb{Z}_pG$. We now use the method (and the notations) of Subsection 3.4 to find a smaller generating subset. Let χ_i, $i = 1, 2, 3$, be the character of G defined by $\chi_i(\sigma_i) = -1$ and $\chi_i(\sigma_j) = 1$ for $j \neq i$. It is easy to see that the set $R^- := \{\chi_3, \chi_1\chi_3, \chi_2\chi_3, \chi_1\chi_2\chi_3\}$ is a system of representatives of the orbits of the odd, irreducible characters of G under the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Thus, we have $F_\chi = \mathbb{Q}$ for all χ in Equation (18), and the equation gives

$$\mathbb{Q}_pG^- \simeq \mathbb{Q}_p^4$$

We compute that

$$m(\chi_3, (p)) = m(\chi_2\chi_3, (p)) = m(\chi_1\chi_2\chi_3, (p)) = 0 \quad \text{and} \quad m(\chi_1\chi_3, (p)) = 1$$

and after several tries, we find a set W such that $\bigcap_{\chi\in R^-} W_{\min}(\chi,p)$ is non-empty and we take in this set the element $\theta_0=\iota(v_1)\wedge\iota(v_2)$ where

$$\begin{aligned}v_1=\frac{1}{17095}\big(&1058221\nu^{15}-7915486\nu^{14}+46551510\nu^{13}-182313497\nu^{12}+579396826\nu^{11}\\&-1444318673\nu^{10}+2976716004\nu^9-5002660697\nu^8+6945207975\nu^7\\&-7851102425\nu^6+7170233086\nu^5-5155280183\nu^4+2822456537\nu^3\\&-1105885714\nu^2+278328786\nu-33994775\big)\end{aligned}$$

and

$$\begin{aligned}v_2=\frac{1}{17095}\big(&-383541\nu^{15}+2749923\nu^{14}-16006808\nu^{13}+61029582\nu^{12}-190600453\nu^{11}\\&+462662235\nu^{10}-930346920\nu^9+1513004524\nu^8-2026236417\nu^7\\&+2184191092\nu^6-1881836887\nu^5+1247007651\nu^4-609767073\nu^3\\&+198580288\nu^2-36118966\nu+1344335\big)\end{aligned}$$

By the result of Subsection 3.4, we know that θ_0 generates $\bigwedge^2_{\mathbb{Z}_pG}U^1(K_p)$ over $\mathbb{Z}_pG$ modulo $\bigwedge^2_{\mathbb{Z}_pG}U^1(K_p)^+ + \left(\bigwedge^2_{\mathbb{Z}_pG}U^1(K_p)\right)_{\text{tor}}$ so to prove $CC(K/k,S^1,p,n)$ it suffices to establish (12) with $\theta=\theta_0$. Note that the L.H.S. of (12) has already been computed. For the R.H.S., the field K^+ is generated over $\mathbb{Q}$ by a root λ of the irreducible polynomial

$$P_\lambda(X)=X^8-4X^7-4X^6+20X^5+4X^4-20X^3-4X^2+4X+1$$

Using the methods described in Subsection 3.5, we find that the Rubin-Stark element is given by

$$\eta_{K^+/k}=\frac{1}{16}(\varepsilon_1\wedge\varepsilon_2)$$

where

$$\varepsilon_1=\frac{1}{5}\big(6\lambda^7-22\lambda^6-33\lambda^5+119\lambda^4+52\lambda^3-121\lambda^2-31\lambda+7\big)$$

and

$$\begin{aligned}\varepsilon_2=\frac{1}{25}\big(&-102282\lambda^7+463929\lambda^6+152556\lambda^5-2073598\lambda^4\\&+604836\lambda^3+1722767\lambda^2-413178\lambda-221449\big).\end{aligned}$$

Note that ε_1 and ε_2 lie in $\mathcal{O}_{K^+}^\times$, and not just in $U_{S(p)}(K^+)$.

We now compute by Subsection 3.6[1]

$$H_{K/k,0}(\eta_{K^+/k},\theta_0)=(\sigma_3-\bar{1})(\sigma_1-\sigma_2-\bar{1})\in(\mathbb{Z}/3\mathbb{Z})G.$$

[1]As mentioned in Remark 11, one needs to factor the norm of v_1 and v_2 to do this computation, but since these are of about 17 digits, it is easy in this case.

Finally, we can check that

$$\mathfrak{s}_{K/k}(\theta_0) \equiv H_{K/k,0}(\eta_{K^+/k}, \theta_0) \pmod 3$$

and therefore $CC(K/k, S^1, p, n)$ is satisfied (since we compute that our choice of τ_1 and τ_2 implies that $\kappa_0(\tau_1\tau_2) \equiv 1 \pmod 3$).

4.2 Tables

We have numerically verified that the conjecture CC is satisfied in 48 examples. These examples are divided into 4 types[2] of differing significance.

- 12 examples of type `B`: $p = 3$, 5 or 7, $n = 0$, p does not divide $|G|$, $K/\mathbb{Q}$ is Galois but not abelian;
- 16 examples of type `C`: $p = 3$, 5 or 7, $n = 0$, p does not divide $|G|$, $K/\mathbb{Q}$ is non-Galois;
- 14 examples of type `D`: $p = 3$ or 5, $n = 0$, p divides $|G|$, $K/\mathbb{Q}$ non-Galois (resp. Galois but not abelian) if $p = 3$ (resp. $p = 5$);
- 6 examples of type `E`: $p = 3$, $n = 1$, p necessarily divides $|G|$, $K/\mathbb{Q}$ not abelian but possibly Galois.

The examples are summarized in four tables, with one table for each type. The columns of the tables have the following meaning:

- the number of the example,
- the value of p (it is either 3, 5 or 7),
- the discriminant d_k of the real quadratic base field k (thus $k = \mathbb{Q}(\sqrt{d_k})$),
- 'R', 'S' or 'I' according to whether p is ramified, split or inert in k,
- the conductor $\mathfrak{f}(K)$ of K/k with the following notations: $\mathfrak{p} = \mathfrak{p}(1)$, and $\mathfrak{p}' = \mathfrak{p}(2)$ if p is split in k, $\mathfrak{q}_q$ is a prime ideal of k above a primer number q, and $\mathfrak{q}'_q$ is the other prime ideal of k above q if q is split in k,[3]
- the structure of the Galois group G as a product of cyclic groups,
- the structure of the Galois group $\bar{G}$ as a product of cyclic groups,
- the minimal polynomial P_λ of a generating element λ of K^+ over $\mathbb{Q}$, so $K^+ = \mathbb{Q}(\lambda)$ and $K = \mathbb{Q}(\lambda, \xi_p)$,

[2] A fifth, type `A`, for which the extension $K/\mathbb{Q}$ is abelian, was used for testing purposes only. It is not included because the CC then follows from [So3, Thm. 5]. (Hypothesis 4, *ibid.* holds since $p \nmid 2 = [k : \mathbb{Q}]$).

[3] Note that the examples `B8` and `B9` differ only by the prime ideal in k above 7 dividing the conductor.

- the decomposition in K/k of the primes ideals above p given as $(e_{\mathfrak{P}(i,1)}(K/k), f_{\mathfrak{P}(i,1)}(K/k), h_i)$ for $i = 1, \ldots, t$ (see Subsection 3.3 for the notations),
- the cardinality of S^1,
- the value of a (see Equation (21)),
- the nature of the Rubin-Stark element: a '0' means that it is trivial, a 'U' means that we found a representation as in (21) with $\varepsilon_i \in \mathcal{O}_{K^+}^{\times}$ for $i = 1, 2$. Recall from Subsection 3.5 that this is to be expected in examples where $p \nmid |G|$ and $|S^1| \geq 4$. Interestingly, it turned out to be possible in most of our other examples as well. In the remainder, indicated by a 'p' in this column, we were only able to satisfy (21) with $\varepsilon_1 \in \mathcal{O}_{K^+}^{\times}$ and $\varepsilon_2 \in U_{S(p)}(K^+)$.

References

[A-H] E. Artin and H. Hasse, 'Die Beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n-ten Potenzreste im Körper der l^n-ten Einheitswurzeln', Abh. Math. Sem. Univ. Hamburg, **6**, (1928), p. 146-162.

[Co] H. Cohen, 'Advanced topics in computational number theory', Graduate Texts in Math. **193**, Springer-Verlag, New York, 2000.

[D-T] D. Dummit and B. Tangedal, 'Computing the lead term of an abelian L-function', Algorithmic number theory symposium (Portland, OR, 1998), Lecture Notes in Comput. Sci. **1423**, p .400–411, Springer, Berlin, 1998.

[Gr] G. Gras, 'Class Field Theory: From Theory to Practice', Monographs in Mathematics, Springer, 2005.

[Ne] J. Neukirch, 'Algebraic Number Theory', Grundlehren der mathematischen Wissenschaften 322, Springer-Verlag, 1999

[PARI] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, PARI/GP System, available at `http://pari.math.u-bordeaux.fr`

[R-S1] X.-F. Roblot and D. Solomon, 'Verifying a p-adic Abelian Stark Conjecture at $s = 1$', Journal of Number Theory **107**, (2004), pp. 168-206.

[Ru] K. Rubin, 'A Stark Conjecture "Over $\mathbf{Z}$" for Abelian L-Functions with Multiple Zeros', Annales de l'Institut Fourier **46**, No. 1, (1996), p. 33-62.

[Se] J.-P. Serre, 'Local Fields', Springer-Verlag, New York, 1979.

[So1] D. Solomon, 'On p-Adic Abelian Stark Conjectures at $s = 1$', Annales de l'Institut Fourier **52**, No. 2, (2002), p. 379-417.

[So2] D. Solomon, 'On Twisted Zeta-Functions at $s = 0$ and Partial Zeta-Functions at $s = 1$', Journal of Number Theory **128**, (2008), p. 105-143.

[So3] D. Solomon, 'Abelian L-Functions at $s = 1$ and Explicit Reciprocity for Rubin-Stark Elements', preprint, http://arxiv.org/abs/math.NT/0702387

[So4] D. Solomon, 'Some New Ideals in Classical Iwasawa Theory', in preparation.

[Ta] J. T. Tate, 'Les Conjectures de Stark sur les Fonctions L d'Artin en $s = 0$', Birkhäuser, Boston, 1984.

[Wa] L. Washington, 'Introduction to Cyclotomic Fields', 2nd Ed., Graduate Texts in Math. 83, Springer-Verlag, New York, 1996.

Table 1: Examples of type B ($n = 0$, $p \nmid |G|$, $K/\mathbb{Q}$ Galois but not abelian)

#	p	d_k	p in k	$\mathfrak{f}(K)$	G	$\bar{G}$	$P_\lambda(X)$	p in K/k	$\lvert S^1\rvert$	a	$\eta_{K^+/k}$
1	3	24	R	$4\mathfrak{p}$	C_2^3	C_2^2	$X^8-4X^7-4X^6+20X^5+4X^4-20X^3-4X^2+4X+1$	$(2,2,2)$	4	16	U
2	3	28	S	$3\mathfrak{q}_2^5$	C_2^3	C_2^2	$X^8-4X^7-8X^6+24X^5+30X^4-16X^3-20X^2+2$	$(2,2,2)(2,2,2)$	5	2	U
3	3	29	I	$15\mathcal{O}_k$	C_2^3	C_2^2	$X^8-2X^7-12X^6+26X^5+17X^4-36X^3-5X^2+11X-1$	$(2,2,2)$	5	1	U
4	3	33	R	$4\mathfrak{p}$	C_2^3	C_2^2	$X^8-11X^6+24X^4-11X^2+1$	$(2,2,2)$	5	4	U
5	3	40	S	$3\mathfrak{q}_2^3\mathfrak{q}_5$	$C_8\times C_2$	C_8	$X^{16}-4X^{15}-16X^{14}+76X^{13}+46X^{12}-392X^{11}$ $-24X^{10}+928X^9-23X^8-1128X^7-44X^6+672X^5$ $+96X^4-156X^3-36X^2+4X+1$	$(2,8,1)(2,8,1)$	6	2	U
6	3	41	I	$15\mathcal{O}_k$	$C_4\times C_2$	C_4	$X^8-19X^6+41X^4-19X^2+1$	$(2,1,4)$	5	1	0
7	3	44	I	$3\mathcal{O}_k$	$C_4\times C_2$	C_4	$X^8-11X^6+24X^4-11X^2+1$	$(4,1,2)$	3	80	p
8	3	505	S	$3\mathcal{O}_k$	$C_8\times C_2$	C_8	$X^{16}-3X^{15}-50X^{14}+157X^{13}+800X^{12}-3014X^{11}-4242X^{10}$ $+25193X^9-6314X^8-82099X^7+99216X^6+38525X^5$ $-125349X^4+50387X^3+19768X^2-14926X+2029$	$(2,8,1)(2,8,1)$	4	16	U
9	5	29	S	$5\mathcal{O}_k$	$C_4\times C_2$	$C_2\times C_2$	$X^8-2X^7-12X^6+26X^5+17X^4-36X^3-5X^2+11X-1$	$(4,2,1)(4,2,1)$	4	1	U
10	5	41	S	$5\mathcal{O}_k$	$C_4\times C_2$	C_4	$X^8-19X^6+41X^4-19X^2+1$	$(4,1,2)(4,1,2)$	4	4	U
11	5	44	S	$15\mathcal{O}_k$	C_4^2	$C_4\times C_2$	$X^{16}-33X^{14}+289X^{12}-990X^{10}+1470X^8-990X^6+289X^4-33X^2+1$	$(4,4,1)(4,4,1)$	5	1	U
12	7	29	S	$35\mathcal{O}_k$	$C_6\times C_2^2$	$C_6\times C_2$	$X^{24}-8X^{23}-22X^{22}+308X^{21}-94X^{20}-4452X^{19}+5808X^{18}+31789X^{17}$ $-59220X^{16}-122740X^{15}+288660X^{14}+258142X^{13}-781464X^{12}$ $-270957X^{11}+1221211X^{10}+92820X^9-1092490X^8+34676X^7$ $+537022X^6-9659X^5-133103X^4-11639X^3+12521X^2+2860X+169$	$(6,2,2)(6,2,2)$	6	3	U

Table 2: Examples of type C ($n = 0$, $p \nmid |G|$, $K/\mathbb{Q}$ not Galois)

#	p	d_k	p in k	$\mathfrak{f}(K)$	G	$\bar{G}$	$P_\lambda(X)$	p in K/k	$\lvert S^1\rvert$	a	$\eta_{K^+/k}$
1	3	5	I	$3\mathfrak{q}_{29}$	C_2^2	C_2	$X^4 - X^3 - 3X^2 + X + 1$	$(2,2,1)$	4	1	U
2	3	8	I	$3\mathfrak{q}_{41}$	C_2^2	C_2	$X^4 - 2X^3 - 3X^2 + 2X + 1$	$(2,2,1)$	4	1	U
3	3	12	R	$\mathfrak{p}\mathfrak{q}_{11}$	C_2^2	C_2	$X^4 - 2X^3 - 3X^2 + 4X + 1$	$(2,2,1)$	4	2	U
4	3	13	S	$12\mathcal{O}_k$	C_2^2	C_2	$X^4 - 5X^2 + 3$	$(2,1,2)(2,2,1)$	5	1	U
5	3	17	I	$3\mathfrak{q}_2^3\mathfrak{q}_2'^2$	C_2^2	C_2	$X^4 - 5X^2 + 2$	$(2,2,1)$	5	1	U
6	3	21	R	$\mathfrak{q}_{37}$	C_2^2	C_2	$X^4 - 2X^3 - 4X^2 + 5X + 1$	$(1,2,2)$	4	1	U
7	3	24	R	$4\mathfrak{p}$	C_2^2	C_2	$X^4 - 6X^2 + 3$	$(2,1,2)$	4	2	U
8	3	28	S	$3\mathfrak{q}_2^5$	C_2^2	C_2	$X^4 - 6X^2 + 2$	$(2,2,1)(2,1,2)$	5	1	0
9	3	29	I	$3\mathfrak{q}_5$	C_2^2	C_2	$X^4 - X^3 - 5X^2 - X + 1$	$(2,2,1)$	4	2	U
10	5	5	R	$\mathfrak{p}\mathfrak{q}_{29}$	C_2^2	C_2	$X^4 - X^3 - 3X^2 + X + 1$	$(2,2,1)$	4	1	U
11	5	8	I	$5\mathfrak{q}_{41}$	$C_4 \times C_2$	$C_2 \times C_2$	$X^8 - 14X^6 - 4X^5 + 43X^4 + 8X^3 - 34X^2 - 8X + 4$	$(4,1,2)$	4	1	U
12	5	12	I	$5\mathfrak{q}_3\mathfrak{q}_{11}$	$C_4 \times C_2$	$C_2 \times C_2$	$X^8 - 14X^6 + 45X^4 - 32X^2 + 4$	$(4,2,1)$	5	1	U
13	5	17	I	$5\mathfrak{q}_2^3\mathfrak{q}_2'^2$	$C_4 \times C_2$	$C_2 \times C_2$	$X^8 - 15X^6 + 39X^4 - 30X^2 + 4$	$(4,2,1)$	5	1	U
14	7	5	I	$\mathfrak{p}\mathfrak{q}_{29}$	$C_6 \times C_2$	C_6	$X^{12} - X^{11} - 17X^{10} + 8X^9 + 79X^8 - 32X^7 - 126X^6 + 37X^5 + 81X^4 - 15X^3 - 19X^2 + 2X + 1$	$(6,1,2)$	4	1	U
15	7	8	S	$\mathfrak{p}\mathfrak{q}_{41}$	$C_6 \times C_2$	C_6	$X^{12} - 2X^{11} - 21X^{10} + 30X^9 + 142X^8 - 146X^7 - 383X^6 + 276X^5 + 385X^4 - 214X^3 - 124X^2 + 56X - 1$	$(6,2,1)(6,2,1)$	5	1	U
16	7	28	R	$\mathfrak{p}\mathfrak{q}_2^5$	$C_6 \times C_2$	C_6	$X^{12} - 16X^{10} + 88X^8 - 204X^6 + 212X^4 - 88X^2 + 8$	$(3,2,2)$	4	6	U

Table 3: Examples of type D ($n = 0$, $p \mid \lvert G\rvert$, $K/\mathbb{Q}$ not Galois if $p = 3$ and $K/\mathbb{Q}$ Galois but not abelian if $p = 5$)											
#	p	d_k	p in k	$\mathfrak{f}(K)$	G	$\bar{G}$	$P_\lambda(X)$	p in K/k	$\lvert S^1\rvert$	a	$\eta_{K^+/k}$
1	3	5	I	$6\mathfrak{q}_{19}$	C_6	C_3	$X^6 - X^5 - 6X^4 + 7X^3 + 4X^2 - 5X + 1$	$(2,3,1)$	5	1	U
2	3	8	I	$3\mathfrak{q}_{79}$	C_6	C_3	$X^6 - 2X^5 - 5X^4 + 10X^3 - 4X + 1$	$(2,3,1)$	4	1	U
3	3	12	R	$15\mathcal{O}_k$	C_6	C_3	$X^6 - 21X^4 - 10X^3 + 42X^2 - 8$	$(3,2,1)$	4	1	p
4	3	29	I	$6\mathfrak{q}_7$	C_6	C_3	$X^6 - 3X^5 - 8X^4 + 19X^3 + 24X^2 - 29X - 29$	$(2,3,1)$	5	1	U
5	3	29	I	$6\mathfrak{q}_{13}$	C_6	C_3	$X^6 - X^5 - 14X^4 - 13X^3 + 6X^2 + 7X + 1$	$(2,3,1)$	5	1	U
6	3	29	I	$3\mathfrak{q}_7\mathfrak{q}_{13}$	C_6	C_3	$X^6 - 2X^5 - 15X^4 + 6X^3 + 45X^2 + 22X - 4$	$(2,3,2)$	5	1	U
7	3	29	I	$3\mathfrak{q}_7\mathfrak{q}_{13}$	C_6	C_3	$X^6 - 2X^5 - 16X^4 + 6X^3 + 76X^2 + 79X + 23$	$(2,1,3)$	5	1	0
8	3	37	S	$\mathfrak{p}\mathfrak{p}'^2\mathfrak{q}_7$	C_6	C_3	$X^6 - X^5 - 16X^4 + 9X^3 + 65X^2 - 10X - 4$	$(2,3,1)(6,1,1)$	5	1	U
9	3	37	S	$\mathfrak{p}\mathfrak{p}'^2\mathfrak{q}_7'$	C_6	C_3	$X^6 - X^5 - 14X^4 + 20X^3 + 16X^2 - 16X - 9$	$(2,1,3)(6,1,1)$	5	1	0
10	3	37	S	$\mathfrak{p}\mathfrak{q}_{73}$	C_6	C_3	$X^6 - 2X^5 - 15X^4 + 13X^3 + 30X^2 - 13X - 7$	$(2,3,1)(2,3,1)$	5	1	U
11	3	40	S	$\mathfrak{p}\mathfrak{q}_{37}$	C_6	C_3	$X^6 - 2X^5 - 9X^4 + 18X^3 + 12X^2 - 20X - 9$	$(2,3,1)(2,1,3)$	5	1	0
12	3	40	S	$3\mathfrak{q}_{67}$	C_6	C_3	$X^6 - 2X^5 - 19X^4 + 10X^3 + 100X^2 + 100X + 25$	$(2,3,1)(2,3,1)$	5	1	U
13	3	44	I	$3\mathfrak{q}_{19}$	C_6	C_3	$X^6 - 2X^5 - 10X^4 + 14X^3 + 19X^2 - 22X + 5$	$(2,3,1)$	4	1	U
14	5	5	R	$55\mathcal{O}_k$	C_{10}	C_5	$X^{10} - 45X^8 + 700X^6 - 4265X^4 + 7725X^2 - 980$	$(10,1,1)$	5	1	U

Table 4: Examples of type E ($n = 1$ so $p \mid |G|$, $K/\mathbb{Q}$ not Galois or Galois but not abelian)

#	p	d_k	p in k	$\mathfrak{f}(K)$	G	$\bar{G}$	$P_\lambda(X)$	p in K/k	$\lvert S^1\rvert$	a	$\eta_{K^+/k}$
1	3	13	S	$90\mathcal{O}_k$	$C_6 \times C_3$	C_3^2	$X^{18} - 9X^{17} - 3X^{16} + 222X^{15} - 387X^{14} - 1701X^{13} + 4637X^{12} + 4659X^{11} - 19920X^{10} - 2160X^9 + 37413X^8 - 5949X^7 - 32755X^6 + 5439X^5 + 12117X^4 - 441X^3 - 813X^2 - 60X - 1$	$(6,3,1)(6,3,1)$	6	7	U
2	3	29	I	$9\mathfrak{q}_5$	$C_6 \times C_2$	C_6	$X^{12} - 3X^{11} - 24X^{10} + 52X^9 + 195X^8 - 306X^7 - 680X^6 + 744X^5 + 999X^4 - 727X^3 - 516X^2 + 213X - 1$	$(6,2,1)$	4	1	U
3	3	37	S	$18\mathcal{O}_k$	$C_6 \times C_3$	C_3^2	$X^{18} - 9X^{17} + 3X^{16} + 174X^{15} - 357X^{14} - 1083X^{13} + 3463X^{12} + 2001X^{11} - 13218X^{10} + 3150X^9 + 22479X^8 - 14883X^7 - 15063X^6 + 16155X^5 + 741X^4 - 5073X^3 + 1557X^2 - 37$	$(6,3,1)(6,3,1)$	5	2	U
4	3	37	S	$18\mathcal{O}_k$	$C_6 \times C_3$	C_3^2	$X^{18} - 9X^{17} + 3X^{16} + 174X^{15} - 357X^{14} - 1083X^{13} + 3463X^{12} + 2001X^{11} - 13218X^{10} + 3150X^9 + 22479X^8 - 14883X^7 - 15063X^6 + 16155X^5 + 741X^4 - 5073X^3 + 1557X^2 - 37$	$(6,3,1)(6,3,1)$	5	2	U
5	3	44	I	$9\mathcal{O}_k$	$C_{12} \times C_2$	C_{12}	$X^{24} - 45X^{22} + 801X^{20} - 7460X^{18} + 40758X^{16} - 137607X^{14} + 291465X^{12} - 381516X^{10} + 294180X^8 - 122240X^6 + 24288X^4 - 2112X^2 + 64$	$(12,1,2)$	3	38 480	p
6	3	53	I	$90\mathcal{O}_k$	$C_6 \times C_3$	$C_3 \times C_3$	$X^{18} - 9X^{17} - 33X^{16} + 462X^{15} - 147X^{14} - 7521X^{13} + 11377X^{12} + 47199X^{11} - 92040X^{10} - 144180X^9 + 293583X^8 + 245031X^7 - 406925X^6 - 245451X^5 + 209247X^4 + 118989X^3 - 21813X^2 - 14520X - 1331$	$(6,1,3)$	5	1	U