ACTA ARITHMETICA
143.2 (2010)

Abelian L-functions at $s = 1$ and explicit reciprocity for Rubin–Stark elements

by

D. Solomon (London)

1. Introduction. Throughout this paper k will be a number field of finite degree d over $\mathbb{Q}$ and K will be a finite, Galois extension of k such that the group $G := \mathrm{Gal}(K/k)$ is abelian. We denote by $S_\infty = S_\infty(k)$ and $S_{\mathrm{ram}} = S_{\mathrm{ram}}(K/k)$ the sets consisting respectively of the infinite places of k and those which are finite and ramify in K, and we set $S^0 = S^0(K/k) = S_{\mathrm{ram}} \cup S_\infty$. If S is any finite set of places containing S^0 and s a complex number with $\mathrm{Re}(s) > 1$, we define a convergent Euler product in the complex group ring of G (denoted simply $\mathbb{C}G$) by

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

The product ranges over those places $\mathfrak{q}$ of k which are not in S (here and henceforth, finite places are identified with prime ideals) and $\sigma_{\mathfrak{q}} = \sigma_{\mathfrak{q},K}$ denotes the Frobenius element of G for $\mathfrak{q}$. If k is totally real and K is a CM field with complex conjugation $c \in G$, it can be shown that the "minus part" $\Theta^-_{K/k,S}(s) := \frac{1}{2}(1-c)\Theta_{K/k,S}(s)$ extends to an entire function $\mathbb{C} \to \mathbb{C}G$.

This paper concerns two conjectures of a p-adic nature about the element $a^-_{K/k,S} := (i/\pi)^d \Theta^-_{K/k,S}(1)$ (whose coefficients turn out to be algebraic). For any number p we denote by $U^1(K_p)$ the p-semilocal principal units of K and define a p-adic regulator on the exterior power $\bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)$. By combining this with $a^-_{K/k,S}$ we obtain a map $\mathfrak{s}_{K/k,S} : \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p) \to \mathbb{Q}_pG$. Assuming for the rest of this Introduction that $p \neq 2$ and S contains all the places above p in k, our first conjecture (the "Integrality Conjecture" or "IC") states simply that the image $\mathfrak{S}_{K/k,S}$ of $\mathfrak{s}_{K/k,S}$ is contained in $\mathbb{Z}_pG$. Recall now that if K^+ denotes the maximal totally real subfield of K then

2010 *Mathematics Subject Classification*: Primary 11R42; Secondary 11S31.
Key words and phrases: Stark conjecture, explicit reciprocity law, Hilbert symbol, S-unit, abelian extension.

DOI: 10.4064/aa143-2-2

(the meromorphic continuation of) $\Theta_{K^+/k,S}(s)$ has a zero of order at least d at $s = 0$. Furthermore, a well-known conjecture of Stark (reformulated and refined by Rubin) states that the coefficient of s^d in the Taylor expansion of $\Theta_{K^+/k,S}(s)$ is given by evaluating an ($\mathbb{R}G$-valued) regulator map on an element of a certain exterior power of the (global) S-units of K^+. Imposing further natural conditions makes this element the unique "Rubin–Stark element" of the title, here denoted $\eta_{K^+/k,S}$.

Our second conjecture (the "Congruence Conjecture" or "CC") assumes and refines the IC, and in so doing links the minus part of $\Theta_{K/k,S}(s)$ at $s = 1$ to its plus part at $s = 0$. It says that if K contains the p^{n+1}th roots of unity for some $n \geq 0$, then, very roughly speaking, the reduction of $\mathfrak{s}_{K/k,S}$ modulo p^{n+1} gives an explicit reciprocity law for $\eta_{K^+/k,S}$.

The idea for these conjectures came from the results of [So4]. We shall not elaborate on the precise connection in the present paper beyond saying that if p splits in k then certain rather strong hypotheses considered in [So4] imply a weak form of the CC at each level in a cyclotomic $\mathbb{Z}_p$-tower containing K. The IC and the CC first appeared explicitly as Conjectures 5.2 and 5.4 at the end of [So5] in a form less general and more awkward than the present versions. That form also used twisted zeta-functions at $s = 0$ in place of the more accessible $\Theta^-_{K/k,S}(1)$.

The remainder of this paper is organised as follows. Section 2 contains the precise definitions and basic properties of the main players: the elements $a^-_{K/k,S}$ and $\eta_{K^+/k,S}$, the map $\mathfrak{s}_{K/k,S}$ and the pairing $H_{K/k,n}$ (a determinant of additive, equivariant Hilbert symbols in terms of which our conjectural reciprocity law is formulated). Section 3 contains the precise statements of the two conjectures. Section 4 surveys the current evidence in their favour—now quite considerable—and includes the statements of the three main results of this paper which were announced in [So5]: Firstly, in the case $p \nmid |G|$, we give a complete characterisation of $\mathfrak{S}_{K/k,S}$ in terms of L-functions of odd characters of G at $s = 0$. In this case the IC then follows, thanks to a result of Deligne–Ribet and P. Cassou-Noguès. Secondly, we prove the conjectures in the case $k = \mathbb{Q}$, using an explicit reciprocity law due to Coleman. Thirdly, we prove the conjectures when $K/\mathbb{Q}$ is abelian (but k is not necessarily $\mathbb{Q}$) by "base-change" from the previous result. In this case, we require a relatively mild technical hypothesis on K/k, S and p. We also discuss briefly A. Jones' recent work showing that a rather different refinement of the IC would follow from a special case of the Equivariant Tamagawa Number Conjecture (ETNC) of Burns and Flach. (On the other hand, there is currently no known connection between the ETNC and the CC.) Section 5 examines the behaviour of the conjectures as S, K and n vary. Sections 6, 7 and 8 contain the proofs of the three main results referred to above.

Jones' refinement of the IC mentioned above predicts that $\mathfrak{S}_{K/k,S}$ is contained in the Fitting ideal (as $\mathbb{Z}_pG$-module) of the minus part of the p-part of a certain ray-class group of K. It would be interesting to investigate links between $\mathfrak{S}_{K/k,S}$ and the Fitting ideal of the minus class group itself (cf. [Gr]). Another goal would be to generalise to arbitrary k the work of [So6] in the case $k = \mathbb{Q}$. The latter links (an extension of) $\mathfrak{s}_{K/\mathbb{Q},S}$ to the *plus* part of the class group via the CC (which is proven in this case) and Iwasawa Theory.

In addition to those introduced above, we use the following basic notations and conventions. If $\mathcal{R}$ is a commutative ring and H a finite abelian group, we write $\mathcal{R}H$ for the group-ring, and if M is a $\mathbb{Z}H$-module we shall sometimes abbreviate $\mathcal{R} \otimes_{\mathbb{Z}} M$ to $\mathcal{R}M$ (considered as an $\mathcal{R}H$-module in the obvious way). For any subgroup $D \subset H$, we write N_D for the norm element $\sum_{d \in D} d \in \mathcal{R}H$. If m is a positive integer, we denote by $\mu_m(\mathcal{R})$ the group of all mth roots of unity in $\mathcal{R}$ and for any prime number p we set $\mu_{p^\infty}(\mathcal{R}) = \bigcup_{i=0}^{\infty} \mu_{p^i}(\mathcal{R})$. All number fields in this paper are supposed of finite degree over $\mathbb{Q}$ and are considered as subfields of $\bar{\mathbb{Q}}$, which is the *algebraic closure of* $\mathbb{Q}$ *within* $\mathbb{C}$. We shall write ξ_m for the particular generator $\exp(2\pi i/m)$ of $\mu_m(\bar{\mathbb{Q}})$. For any number field F and any integer r we shall write $S_r(F)$ for the set of places (prime ideals) of F dividing r. If S is a set of places of F and L is any finite extension of F we shall write $S(L)$ for the set of places of L lying above those in S. If S contains $S_\infty(F)$ (see above) then the group $U_S(F)$ of S-units of F consists of those elements of $F^\times$ which are local units at every place not in S and we shall often write simply $U_S(L)$ in place of $U_{S(L)}(L)$. (*Caution*: U_S and related modules will sometimes be written additively.)

If L/F is abelian and v is any place of F we shall write $D_v(L/F)$ for the decomposition subgroup of $\mathrm{Gal}(L/F)$ at any prime dividing v in L and similarly $T_v(L/F)$ for the inertia subgroup (if v is finite). Suppose $L \supset F \supset M$ are three number fields such that L/M and F/M are Galois extensions. Then the restriction map $\mathrm{Gal}(L/M) \to \mathrm{Gal}(F/M)$ will be denoted $\pi_{L/F}$ and extended $\mathcal{R}$-linearly to a ring homomorphism $\mathcal{R}\mathrm{Gal}(L/M) \to \mathcal{R}\mathrm{Gal}(F/M)$ for any commutative ring $\mathcal{R}$. We also write $\nu_{L/M}$ for the $\mathcal{R}$-linear "corestriction" map $\mathcal{R}\mathrm{Gal}(F/M) \to \mathcal{R}\mathrm{Gal}(L/M)$ which sends $g \in \mathrm{Gal}(F/M)$ to the sum of its preimages under $\pi_{L/F}$ in $\mathrm{Gal}(L/M)$.

2. Dramatis personæ

2.1. The function $\Theta_{K/k,S}$ and the element $a^-_{K/k,S}$. Let $\hat{G}$ denote the dual group of G, namely the group of all (irreducible) complex characters $\chi : G \to \mathbb{C}^\times$ with identity element χ_0, the trivial character. For any $\chi \in \hat{G}$

we write $e_{\chi,G}$ for the associated idempotent in the complex group-ring $\mathbb{C}G$:

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

Expanding the Euler product (1), we get

$$\Theta_{K/k,S}(s) = \sum_{g\in G}\zeta_{K/k,S}(s;g)g^{-1} = \sum_{\chi\in\hat{G}} L_{K/k,S}(s,\chi)e_{\chi^{-1},G} \tag{2}$$

for $\mathrm{Re}(s) > 1$. Here, $\zeta_{K/k,S}(s;g)$ and $L_{K/k,S}(s,\chi)$ denote respectively the "S-truncations" of the partial zeta-function attached to G and the L-function attached to χ. In particular,

$$\begin{aligned} (3)\quad & L_{K/k,S}(s,\chi) \\ &= \prod_{\mathfrak{q}\notin S}(1-N\mathfrak{q}^{-s}\chi(\sigma_{\mathfrak{q}}))^{-1} = \prod_{\substack{\mathfrak{q}\in S\setminus S_\infty \\ \mathfrak{q}\nmid \mathfrak{f}_\chi}}(1-N\mathfrak{q}^{-s}\hat{\chi}([\mathfrak{q}]))L(s,\hat{\chi})\end{aligned}$$

where $\mathfrak{f}_\chi$ and $L(s,\hat{\chi})$ denote respectively the conductor of χ and the L-function of its associated primitive ray-class character $\hat{\chi}$ modulo $\mathfrak{f}_\chi$.

Remark 2.1. The second (but not the first) expression for $L_{K/k,S}(s,\chi)$ in (3) makes sense when S is any finite set of places of k, containing $S_\infty(k)$ but *not necessarily* $S_{\mathrm{ram}}(K/k)$. In fact, it agrees with the definition of the S-truncated *Artin L-function* attached to χ considered as a character of G (see for example [Ta, p. 23]).

The analytic behaviour of $L(s,\hat{\chi})$ is well-known. Its (in general) meromorphic continuation means that we may use equations (2) and (3) to continue $\Theta_{K/k,S}$ to a meromorphic, $\mathbb{C}G$-valued function on $\mathbb{C}$. These equations then hold as identities between meromorphic functions on $\mathbb{C}$. Similarly, if $S \supset S' \supset S^0$, then the obvious identity

$$\Theta_{K/k,S}(s) = \prod_{\mathfrak{q}\in S\setminus S'}(1-N\mathfrak{q}^{-s}\sigma_{\mathfrak{q}}^{-1})\Theta_{K/k,S'}(s) \tag{4}$$

for $\mathrm{Re}(s) > 1$ also holds for all s. In fact, the function $L(s,\hat{\chi})$, hence also the function $\chi(\Theta_{K/k,S}(s)) = L_{K/k,S}(s,\chi^{-1})$, is analytic on $\mathbb{C}\setminus\{1\}$ and

$$\mathrm{ord}_{s=1}\chi(\Theta_{K/k,S}(s)) = \begin{cases} 0 & \text{if } \chi\neq\chi_0, \\ -1 & \text{if } \chi=\chi_0. \end{cases} \tag{5}$$

Moreover, the residue of $\chi_0(\Theta_{K/k,S}(s)) = \prod_{\mathfrak{q}\in S\setminus S_\infty}(1-N\mathfrak{q}^{-s})\zeta_k(s)$ at $s=1$ is well-known (see e.g. [Ta, Théorème I.1.1]).

Using the well-known functional equation relating the *primitive* L-function $L(s,\hat{\chi}^{-1})$ to $L(1-s,\hat{\chi})$ one might expect to derive a natural relation between $\Theta_{K/k,S}(s)$ and $\Theta_{K/k,S}(1-s)$ by means of (2) and (3). There are however at least three obstacles to this: firstly the presence of Gauss sums in the functional equations and secondly the dependence on χ of the second product in (3) which, thirdly, forces $L_{K/k,S}(0,\chi)=0$ for certain χ. Instead, in [So5] we used these functional equations to give a precise relation between $\Theta_{K/k,S^0}(s)$ (there denoted $\Theta_{K/k}(s)$) and $\Phi_{K/k}(1-s)$, where the function $\Phi_{K/k}:\mathbb{C}\to\mathbb{C}G$ was defined by means of twisted zeta-functions and studied, together with its p-adic analogues, in [So2–So5]. For each $v\in S_\infty$, we write c_v for the unique generator of $D_v(K/k)$ so that $c_v=1$ unless v is real and one (hence every) place w of K above v is complex, in which case c_v is the complex conjugation associated to any such w.

We define an entire, $\mathbb{C}D_v(K/k)$-valued function

$$C_v(s)=\begin{cases}\exp(i\pi s).1-\exp(-i\pi s).c_v=2i\sin(\pi s).1 & \text{if } v \text{ is complex,}\\ \exp(i\pi s/2).1+\exp(-i\pi s/2).c_v & \text{if } v \text{ is real.}\end{cases}$$

Then Theorem 2.1 of [So5], combined with (4) for $S'=S_0$, gives

$$\text{(6)}\qquad i^{r_2(k)}\sqrt{|d_k|}\prod_{\mathfrak{q}\in S\setminus S^0}(1-N\mathfrak{q}^{-s}\sigma_{\mathfrak{q}}^{-1})\Phi_{K/k}(1-s) = ((2\pi)^{-s}\Gamma(s))^d\Big(\prod_{v\in S_\infty}C_v(s)\Big)\Theta_{K/k,S}(s)$$

where $r_2(k)$ denotes the number of complex places of k and d_k its absolute discriminant. Let $\Theta^{\text{n.t.}}_{K/k,S}(s)$ be the function $(1-e_{\chi_0,G})\Theta_{K/k,S}(s)$, which is regular at $s=1$ by (5). So (6) gives

$$\text{(7)}\qquad \sqrt{|d_k|}\prod_{\mathfrak{q}\in S\setminus S^0}(1-N\mathfrak{q}^{-1}\sigma_{\mathfrak{q}}^{-1})(1-e_{\chi_0,G})\Phi_{K/k}(0) = (2\pi)^{-d}i^{|S_\infty|}\Big(\prod_{v\in S_\infty}(1-c_v)\Big)\Theta^{\text{n.t.}}_{K/k,S}(1),$$

from which it follows that $(1-e_{\chi_0,G})\Phi_{K/k}(0)$ vanishes unless k is totally real and K is totally complex. On the other hand, multiplying (6) by $e_{\chi_0,G}$ and letting $s\to1$, we see that $e_{\chi_0,G}\Phi_{K/k}(0)$ vanishes unless $|S_\infty|=1$, i.e. k is $\mathbb{Q}$ or an imaginary quadratic field, in which case it may easily be calculated from $\mathrm{res}_{s=1}\,\zeta_k(s)$. Thus $\Phi_{K/k}(0)$ has little interest unless k is totally real and K is totally complex. Even then, $\prod_{v\in S_\infty}(1-c_v)$ vanishes unless there is a (unique) CM-subfield K^- of K containing k, in which case we lose little but complication by replacing K by K^-. (See Remark 3.1(i) of [So5] for further explanations.) For these reasons *we shall henceforth make the*

Hypothesis 2.2. *k is totally real and K is a CM field.*

This means that d_k is a positive integer and $c_v=c$, the unique complex conjugation in G, for all $v\in S_\infty$. Let $e^{\pm}$ denote the two idempotents $\frac{1}{2}(1\pm c)$ of $\mathbb{C}G$ and let $\Theta^-_{K/k,S}(s)$ be the entire function $e^-\Theta_{K/k,S}(s)=e^-\Theta^{\text{n.t.}}_{K/k,S}(s)$.

The above remarks, together with a simple calculation of $e_{\chi_0,G}\Phi_{K/k}(0)$ when $k=\mathbb{Q}$, show that equation (7) may be rewritten as

$$(8)\qquad a^-_{K/k,S} := \left(\frac{i}{\pi}\right)^d \Theta^-_{K/k,S}(1)$$
$$= \begin{cases} \displaystyle\prod_{\mathfrak{q}\in S\setminus S^0}(1-N\mathfrak{q}^{-1}\sigma_{\mathfrak{q}}^{-1})\sqrt{d_k}\,\Phi_{K/k}(0) & \text{if } k\neq\mathbb{Q},\\ \displaystyle\prod_{q\in S\setminus S^0}(1-q^{-1}\sigma_q^{-1})\Phi_{K/\mathbb{Q}}(0)+\frac{1}{2}\prod_{q\in S\setminus\{\infty\}}(1-q^{-1})e_{\chi_0,G} & \text{if } k=\mathbb{Q}.\end{cases}$$

If R is a commutative ring in which 2 is invertible and if M is any $R\langle c\rangle$-module then we shall write M^+ (resp. M^-) for the R-submodule e^+M (resp. e^-M), so that $M=M^+\oplus M^-$. In this notation, $a^-_{K/k,S}$ clearly lies in $\mathbb{C}G^-$ and multiplying (8) by e^- gives

$$(9)\qquad a^-_{K/k,S} = e^-a^-_{K/k,S} = e^-\prod_{\mathfrak{q}\in S\setminus S^0}(1-N\mathfrak{q}^{-1}\sigma_{\mathfrak{q}}^{-1})\sqrt{d_k}\,\Phi_{K/k}(0)$$

whether or not $k=\mathbb{Q}$, but if $k\neq\mathbb{Q}$ then the term e^- may be omitted on the R.H.S. In fact, $a^-_{K/k,S}$ has algebraic coefficients: Let $\mathfrak{f}(K)$ be the integral ideal of $\mathcal{O}_k$ which is the conductor of K/k in the sense of class-field theory and let $f(K)$ be the positive generator of the ideal $\mathfrak{f}(K)\cap\mathbb{Z}$. The product in (9) lies in $\mathbb{Q}G^\times$, therefore (9) and [So5, Prop. 3.1] show that $a^-_{K/k,S}$ has coefficients in $\sqrt{d_k}\,\mathbb{Q}(\mu_{f(K)})$ and that

$$(10)\qquad a^-_{K/k,S}\mathbb{Q}(\mu_{f(K)})G = \sqrt{d_k}\,\mathbb{Q}(\mu_{f(K)})G^-.$$

Integrality properties of the coefficients of $a^-_{K/k,S}$ are given in [R-S2] where it is shown that they also lie in the Galois closure of K over $\mathbb{Q}$ (see ibid., Proposition 2 and Remark 6).

2.2. Rubin–Stark elements for K^+/k. Let us write $\bar{G}$ for $\mathrm{Gal}(K^+/k)\cong G/\langle c\rangle$, so that $\pi_{K/K^+}:\mathbb{C}G\to\mathbb{C}\bar{G}$ induces an ring isomorphism $\mathbb{C}G^+\to\mathbb{C}\bar{G}$ sending $e^+\Theta_{K/k,S}(s)$ onto $\Theta_{K^+/k,S}(s)$. To study $\Theta_{K^+/k,S}(s)$ at $s=0$ we define an integer $r_S(\phi)$ for each $\phi\in\widehat{\bar{G}}$ by

$$(11)\qquad r_S(\phi):=\begin{cases} d+|\{\mathfrak{q}\in S\setminus S_\infty : \phi(D_{\mathfrak{q}}(K^+/k))=\{1\}\}| & \text{if } \phi \text{ is non-trivial},\\ d+|S\setminus S_\infty|-1=|S|-1 & \text{if } \phi \text{ is trivial}.\end{cases}$$

Since k and K^+ are totally real, the functional equation of $L(s,\widehat{\phi})$ for $\phi\in\widehat{\bar{G}}$ shows that, for any such ϕ, we have

$$(12)\qquad \mathrm{ord}_{s=0}\phi(\Theta_{K^+/k,S}(s)) = \mathrm{ord}_{s=0}L_{K^+/k,S}(s,\phi^{-1}) = r_S(\phi)$$

(see e.g. [Ta, Ch. I, §3]). We shall assume until further notice

Hypothesis 2.3. *$|S| \geq d+1$ (i.e. S contains at least one finite place).*

This implies that $r_S(\phi) \geq d$ for ϕ trivial hence for every $\phi \in \widehat{\bar{G}}$, so we may define

$$\Theta^{(d)}_{K^+/k,S}(0) := \lim_{s\to 0} s^{-d}\Theta_{K^+/k,S}(s)$$

(an element of $\mathbb{C}\bar{G}$ which is easily seen to lie in $\mathbb{R}\bar{G}$). Conjectures of Stark, as refined by Rubin [Ru], predict that $\Theta^{(d)}_{K^+/k,S}(0)$ is given by a certain $\mathbb{R}\bar{G}$-valued regulator of S-units of K^+ defined as follows. We fix once and for all a set $\tau_1,\ldots,\tau_d$ of left coset representatives for $\mathrm{Gal}(\bar{\mathbb{Q}}/k)$ in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and we define $\mathbb{Q}\bar{G}$-linear, real logarithmic maps for $i=1,\ldots,d$:

$$\lambda_{K^+/k,i} : \mathbb{Q}U_S(K^+) \to \mathbb{R}\bar{G}, \qquad a\otimes\varepsilon \mapsto a\sum_{g\in\bar{G}} \log|\tau_i(g\varepsilon)|\, g^{-1} \in \mathbb{R}\bar{G}.$$

The above-mentioned regulator is the $\mathbb{Q}\bar{G}$-linear map uniquely defined by

$$R_{K^+/k} : \textstyle\bigwedge^d_{\mathbb{Q}\bar{G}} \mathbb{Q}U_S(K^+) \to \mathbb{R}\bar{G}, \qquad x_1\wedge\cdots\wedge x_d \mapsto \det\left(\lambda_{K^+/k,i}(x_t)\right)_{1\leq i,t\leq d}.$$

The following definition generalises the above construction and will be useful later.

Proposition/Definition 2.4.

(i) *Suppose $\mathcal{R}$ is a commutative ring, $\mathcal{S}$ a commutative $\mathcal{R}$-algebra, and that M is any (left) $\mathcal{R}H$ module for a finite group H. There is an isomorphism from $\mathrm{Hom}_{\mathcal{R}}(M,\mathcal{S})$ to $\mathrm{Hom}_{\mathcal{R}H}(M,\mathcal{S}H)$ given by $f\mapsto f^H$ where f^H is defined to be the map $m\mapsto \sum_{h\in H} f(h^{-1}m)h$.*

(ii) *Suppose H is abelian and $l\in\mathbb{N}$. Then for every l-tuple $(f_1,\ldots,f_l)\in \mathrm{Hom}_{\mathcal{R}}(M,\mathcal{S})^l$ there is an $\mathcal{R}H$-linear determinantal map $\Delta_{f_1,\ldots,f_l}$ uniquely defined by*

$$\Delta_{f_1,\ldots,f_l} : \textstyle\bigwedge^l_{\mathcal{R}H} M \to \mathcal{S}H, \qquad m_1\wedge\cdots\wedge m_l \mapsto \det\left(f_i^H(m_t)\right)^l_{i,t=1}.$$

$\Delta_{f_1,\ldots,f_l}$ is $\mathcal{S}$-multilinear and alternating as a function of $(f_1,\ldots,f_d)$. Moreover for each $i=1,\ldots,l$ and $h\in H$ we have $\Delta_{f_1,\ldots,f_i\circ h,\ldots,f_l}(\mu) = \Delta_{f_1,\ldots,f_l}(\mu)h$ for all $\mu\in\bigwedge^l_{\mathcal{R}H} M$. ∎

For instance, taking $\mathcal{R}=\mathbb{Q}$, $\mathcal{S}=\mathbb{R}$, $M=\mathbb{Q}U_S(K^+)$ and $H=\bar{G}$ gives $R_{K^+/k}=\Delta_{f_1,\ldots,f_d}$, where f_i is the map sending $a\otimes\varepsilon\in\mathbb{Q}U_S(K^+)$ to its logarithmic embedding $a\log|\tau_i(\varepsilon)|$ in $\mathbb{R}$. If instead we take $\mathcal{R}=\mathcal{S}=\mathbb{Q}$, then any d elements $f_1,\ldots,f_d$ of $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}U_S(K^+),\mathbb{Q})$ give rise to a $\mathbb{Q}\bar{G}$-linear map $\Delta_{f_1,\ldots,f_d} : \bigwedge^d_{\mathbb{Q}\bar{G}} \mathbb{Q}U_S(K^+) \to \mathbb{Q}G$. Let us identify $\mathrm{Hom}_{\mathbb{Z}}(U_S(K^+),\mathbb{Z})$ with the lattice in $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}U_S(K^+),\mathbb{Q})$ which is its image under the map $f\to 1\otimes f$. We can then define a $\mathbb{Z}\bar{G}$ submodule $\Lambda_{0,S}=\Lambda_{0,S}(K^+/k)$ of

$\bigwedge^d_{\mathbb{Q}\bar G}\mathbb{Q}U_S(K^+)$ by

$$\Lambda_{0,S}(K^+/k):=\Big\{\eta\in\bigwedge^d_{\mathbb{Q}\bar G}\mathbb{Q}U_S(K^+):\Delta_{f_1,\dots,f_d}(\eta)\in\mathbb{Z}\bar G \quad \forall f_1,\dots,f_d\in\mathrm{Hom}_{\mathbb{Z}}(U_S(K^+),\mathbb{Z})\Big\}.$$

This coincides with "$\Lambda^d_0 U_S(K^+)$" as defined by Rubin's "double dual" construction in [Ru, §1]. It is clear that $\Lambda_{0,S}$ contains the lattice which is the natural image of $\bigwedge^d_{\mathbb{Z}\bar G}U_S(K^+)$ in $\bigwedge^d_{\mathbb{Q}\bar G}\mathbb{Q}U_S(K^+)$ (we denote this $\overline{\bigwedge^d_{\mathbb{Z}\bar G}U_S(K^+)}$) but the two are not necessarily equal. In fact, Proposition 1.2 of [Ru] implies

Proposition 2.5. *If $d=1$ (i.e. $k=\mathbb{Q}$) then $\Lambda_{0,S}=\overline{\bigwedge^1_{\mathbb{Z}\bar G}U_S(K^+)}=\overline{U_S(K^+)}$. In general, the index $|\Lambda_{0,S}:\overline{\bigwedge^d_{\mathbb{Z}\bar G}U_S(K^+)}|$ is finite and supported on primes dividing $|\bar G|$.* ■

Let us define an idempotent $e_{S,d,\bar G}$, *a priori* in $\mathbb{C}\bar G$, by setting $e_{S,d,\bar G}:=\sum_{\phi\in\hat{\bar G},\,r_S(\phi)=d}e_{\phi,\bar G}$. This is the unique element x of $\mathbb{C}\bar G$ such that $\phi(x)=1$ or 0 according as $r_S(\phi)=d$ or $r_S(\phi)>d$. It follows easily from this description and the formula (11) that

$$e_{S,d,\bar G}=\begin{cases}\prod_{\mathfrak{q}\in S\setminus S_\infty}\Big(1-\frac{1}{|D_{\mathfrak q}(K^+/k)|}N_{D_{\mathfrak q}(K^+/k)}\Big) & \text{if } |S|>d+1,\\ \Big(1-\frac{1}{|D_{\mathfrak q}(K^+/k)|}N_{D_{\mathfrak q}(K^+/k)}\Big)+e_{\chi_0,\bar G} & \text{if } |S|=d+1,\\ & \text{i.e. } S=\{\mathfrak q\}\cup S_\infty.\end{cases}\tag{13}$$

Thus $e_{S,d,\bar G}$ is an idempotent of $\mathbb{Q}\bar G$, so lies in $|\bar G|^{-1}\mathbb{Z}\bar G$. We also deduce easily:

Proposition 2.6. *Let M be any $\mathbb{Q}\bar G$-module and $m\in M$. The following are equivalent:*

(i) *$m\in e_{S,d,\bar G}M$.*
(ii) *$m=e_{S,d,\bar G}m$.*
(iii) *For all $\mathfrak q\in S\setminus S_\infty$,*

$$N_{D_{\mathfrak q}(K^+/k)}m\in\begin{cases}\{0\} & \text{if } |S|>d+1,\\ M^{\bar G} & \text{if } |S|=d+1,\ \text{i.e. } S=\{\mathfrak q\}\cup S_\infty.\end{cases}\tag{14}$$

(iv) *$e_{\phi,\bar G}(1\otimes m)=0$ in $\mathbb{C}\otimes_{\mathbb{Q}}M$ for all $\phi\in\hat{\bar G}$ such that $r_S(\phi)>d$.* ■

For brevity, we shall sometimes refer to any of these conditions as the *eigenspace condition* on m with respect to $(S,d,\bar G)$. Now, given any subring $\mathcal R$ of $\mathbb{Q}$, we formulate a version of the Rubin–Stark conjecture "over $\mathcal R$":

Conjecture RSC$(K^+/k,S;\mathcal R)$. *Let K/k and S be as above, satisfying Hypotheses 2.2 and 2.3. Then there exists an element $\eta\in\bigwedge^d_{\mathbb{Q}\bar G}\mathbb{Q}U_S(K^+)$*

satisfying the eigenspace condition with respect to $(S, d, \bar{G})$ *and such that*

$$\Theta^{(d)}_{K^+/k,S}(0) = R_{K^+/k}(\eta) \tag{15}$$

and

$$\eta \in \tfrac{1}{2}\mathcal{R}\Lambda_{0,S}(K^+/k). \tag{16}$$

Notice that $\Theta^{(d)}_{K^+/k,S}(0)$ lies in the ideal $e_{S,d,\bar{G}}\mathbb{R}\bar{G}$ (and in fact generates it) by equation (12). Thus if $\eta \in \bigwedge^d_{\mathbb{Q}\bar{G}} \mathbb{Q}U_S(K^+)$ is any solution of (15) then $e_{S,d,\bar{G}}\eta$ is a solution satisfying the eigenspace condition. On the other hand, it can be shown that $R_{K^+/k}$ is injective on $e_{S,d,\bar{G}} \bigwedge^d_{\mathbb{Q}\bar{G}} \mathbb{Q}U_S(K^+)$ (this follows from [Ru, Lemma 2.7]), so a solution of (15) satisfying the eigenspace condition is unique. For this reason, we call such an element the *Rubin–Stark element for* K^+/k *and* S and denote it $\eta_{K^+/k,S}$ since it is independent of $\mathcal{R}$. Of course, condition (16) is redundant if $\mathcal{R} = \mathbb{Q}$, and for any prime number p we have

$$\mathrm{RSC}(K^+/k, S; \mathbb{Z}) \;\Rightarrow\; \mathrm{RSC}(K^+/k, S; \mathbb{Z}_{(p)}) \;\Rightarrow\; \mathrm{RSC}(K^+/k, S; \mathbb{Q})$$

(where $\mathbb{Z}_{(p)}$ denotes the localisation $\{a/b \in \mathbb{Q} : p \nmid b\}$). Moreover, $\mathrm{RSC}(K^+/k, S; \mathbb{Z})$ is equivalent to the conjunction of $\mathrm{RSC}(K^+/k, S; \mathbb{Z}_{(p)})$ for all primes p. We shall mainly be interested in $\mathrm{RSC}(K^+/k, S; \mathbb{Z}_{(p)})$ when $p \neq 2$, in which case (16) reduces to $\eta \in \mathbb{Z}_{(p)}\Lambda_{0,S}$.

Remark 2.7. Since $R_{K^+/k}$ depends on the choice (and ordering) of the τ_i's, so will $\eta_{K^+/k,S}$, but in a simple way. For example, if one τ_i is replaced by $\tau_i\tau^{-1}$ for some $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/k)$ then we must replace $\eta_{K^+/k,S}$ by $\tau|_{K^+}\eta_{K^+/k,S}$ where $\tau|_{K^+} \in \bar{G}$.

Remark 2.8. $\mathrm{RSC}(K^+/k, S; \mathbb{Q})$ and $\mathrm{RSC}(K^+/k, S; \mathbb{Z})$ follow from certain special cases of Conjectures A′ and B′ of [Ru] respectively. Indeed, if we choose the extension "K/k" of Rubin's paper to be our K^+/k, his "S" to be ours, his "r" to be d and his chosen places "$w_1, \ldots, w_r$" to be the real places of K^+ defined by $\tau_1, \ldots, \tau_d$, then Rubin's Hypotheses 2.1.1–2.1.4 are satisfied. His conjectures also require an auxiliary set T of finite places of k satisfying certain conditions, although for Conjecture A′ the precise choice of such T does not affect the truth of the conjecture. For simplicity we take $T = \{\mathfrak{q}\}$ for some prime $\mathfrak{q} \notin S$ not dividing 2 and splitting in K^+ (infinitely many of these exist by Chebotarev's theorem). Then Rubin's Hypothesis 2.1.5 certainly holds since $U_S(K^+)_{\mathrm{tor}} = \{\pm 1\}$. Moreover, his "$\Theta^{(r)}_{S,T}(0)$" is our $(1 - N\mathfrak{q})\Theta^{(d)}_{K^+/k,S}(0)$ and his "$\Lambda^r_0 U_{S,T}$" is a sublattice of our $\Lambda_{0,S}(K^+/k)$ which also spans $\bigwedge^d_{\mathbb{Q}\bar{G}} \mathbb{Q}U_S(K^+)$ over $\mathbb{Q}$. It follows easily that $\mathrm{RSC}(K^+/k, S; \mathbb{Q})$ is equivalent to Rubin's Conjecture A′ with these choices and this (hence any) T. Moreover, if both hold then Rubin's "$\varepsilon_{S,T}$" equals our $(1-N\mathfrak{q})\eta_{K^+/k,S}$, by uniqueness. It follows that Rubin's Conjecture B′ with these choices amounts to the further condition that $(1-N\mathfrak{q})\eta_{K^+/k,S}$ lie in his "$\Lambda_0^r U_{S,T}$" hence in our $\Lambda_{0,S}(K^+/k)$. But as $\mathfrak{q}$ varies subject to the above conditions, Lemme IV.1.1 of [Ta] says that the g.c.d. of the corresponding integers $1-N\mathfrak{q}$ is $|\mu(K^+)|=2$. Thus the corresponding cases of Rubin's Conjecture B′ together imply $\mathrm{RSC}(K^+/k,S;\mathbb{Z})$.

The connection with Stark's original conjecture in terms of characters (see [Ta, Conjecture I.5.1]) is as follows. Propositions 2.3 and 2.4 of [Ru] show that Stark's conjecture holds for K^+/k, S and every character $\phi\in\bar{G}$ satisfying $r_S(\phi)=d$ if and only if Rubin's Conjecture A′ holds (for any T), which is equivalent to $\mathrm{RSC}(K^+/k,S;\mathbb{Q})$, by the above.

In the next section we shall be interested in determinantal maps obtained from a d-tuple $(f_1,\ldots,f_d)\in\mathrm{Hom}_{\mathbb{Z}}(U_S(K^+),\mathbb{Z}/p^{n+1}\mathbb{Z})$ for some prime p and $n\geq 0$. Taking $\mathcal{R}=\mathbb{Z}$, $\mathcal{S}=\mathbb{Z}/p^{n+1}\mathbb{Z}$ and $M=U_S(K^+)$ in Proposition/Definition 2.4 gives such a map $\Delta_{f_1,\ldots,f_d}:\bigwedge^d_{\mathbb{Z}\bar{G}}U_S(K^+)\to(\mathbb{Z}/p^{n+1}\mathbb{Z})\bar{G}$. We shall now show that *provided p is odd,* this map "extends" naturally to $\mathbb{Z}_{(p)}\Lambda_{0,S}$ in a sense to be explained below. First, we have

LEMMA 2.9. *If p is odd then the following sequence is exact:*

$$0\to\mathrm{Hom}_{\mathbb{Z}}(U_S(K^+),\mathbb{Z})\xrightarrow{p^{n+1}}\mathrm{Hom}_{\mathbb{Z}}(U_S(K^+),\mathbb{Z})\to\mathrm{Hom}_{\mathbb{Z}}(U_S(K^+),\mathbb{Z}/p^{n+1}\mathbb{Z})\to 0.$$

Proof. As K^+ is totally real, $U_S(K^+)/\{\pm1\}$ is $\mathbb{Z}$-free. Thus the sequence is exact if $U_S(K^+)$ is replaced by $U_S(K^+)/\{\pm1\}$. But since $\mathbb{Z}$ and $\mathbb{Z}/p^{n+1}\mathbb{Z}$ have no 2-torsion, we may identify

$$\mathrm{Hom}_{\mathbb{Z}}(U_S(K^+)/\{\pm1\},\mathbb{Z})\cong\mathrm{Hom}_{\mathbb{Z}}(U_S(K^+),\mathbb{Z}),$$
$$\mathrm{Hom}_{\mathbb{Z}}(U_S(K^+)/\{\pm1\},\mathbb{Z}/p^{n+1}\mathbb{Z})\cong\mathrm{Hom}_{\mathbb{Z}}(U_S(K^+),\mathbb{Z}/p^{n+1}\mathbb{Z}).\ \blacksquare$$

Thus given $f_1,\ldots,f_d$ in $\mathrm{Hom}_{\mathbb{Z}}(U_S(K^+),\mathbb{Z}/p^{n+1}\mathbb{Z})$ for p odd, we can choose lifts $\tilde{f}_1,\ldots,\tilde{f}_d$ in $\mathrm{Hom}_{\mathbb{Z}}(U_S(K^+),\mathbb{Z})$. As previously, we may regard these as elements of $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}U_S(K^+),\mathbb{Q})$ and use Proposition/Definition 2.4 to construct $\Delta_{\tilde{f}_1,\ldots,\tilde{f}_d}:\bigwedge^d_{\mathbb{Q}\bar{G}}\mathbb{Q}U_S(K^+)\to\mathbb{Q}\bar{G}$. If $\eta\in\Lambda_{0,S}$ then $\Delta_{\tilde{f}_1,\ldots,\tilde{f}_d}(\eta)$ lies in $\mathbb{Z}\bar{G}$ by definition of $\Lambda_{0,S}$ and we write $\tilde{\Delta}_{f_1,\ldots,f_d}(\eta)$ for its image in $(\mathbb{Z}/p^{n+1}\mathbb{Z})\bar{G}$. The latter is independent of the choice of each lift $\tilde{f}_i$, as one easily checks using Lemma 2.9, the linearity of $\Delta_{\tilde{f}_1,\ldots,\tilde{f}_d}$ in $\tilde{f}_i$ and the fact that $\eta\in\Lambda_{0,S}$. Consequently we have a well-defined map $\tilde{\Delta}_{f_1,\ldots,f_d}:\Lambda_{0,S}\to(\mathbb{Z}/p^{n+1}\mathbb{Z})\bar{G}$ which is linear and so extends uniquely to $\mathbb{Z}_{(p)}\Lambda_{0,S}$. It is now an easy exercise to check the following properties of $\tilde{\Delta}_{f_1,\ldots,f_d}$:

PROPOSITION 2.10. *Let p be odd and choose*

$$f_1,\ldots,f_d\in\mathrm{Hom}_{\mathbb{Z}}(U_S(K^+),\mathbb{Z}/p^{n+1}\mathbb{Z}).$$

(i) *The map* $\tilde{\Delta}_{f_1,\ldots,f_d} : \mathbb{Z}_{(p)}\Lambda_{0,S}(K^+/k) \to (\mathbb{Z}/p^{n+1}\mathbb{Z})\bar{G}$ *is* $\mathbb{Z}\bar{G}$*-linear.*

(ii) *It is also* $(\mathbb{Z}/p^{n+1}\mathbb{Z})$*-multilinear and alternating as a function of* $(f_1,\ldots,f_d)$ *and for each* $i = 1,\ldots,d$ *we have* $\tilde{\Delta}_{f_1,\ldots,f_i\circ g,\ldots,f_d}(\eta) = \tilde{\Delta}_{f_1,\ldots,f_d}(\eta)g$ *for all* $g \in \bar{G}$ *and* $\eta \in \mathbb{Z}_{(p)}\Lambda_{0,S}(K^+/k)$.

(iii) *The following diagram commutes:*

$$\begin{array}{ccc} \bigwedge^d_{\mathbb{Z}\bar{G}} U_S(K^+) & \xrightarrow{\Delta_{f_1,\ldots,f_d}} & \\ \downarrow \alpha & & (\mathbb{Z}/p^{n+1}\mathbb{Z})\bar{G} \\ \mathbb{Z}_{(p)}\Lambda_{0,S}(K^+/k) & \xrightarrow{\tilde{\Delta}_{f_1,\ldots,f_d}} & \end{array}$$

where α *is the natural map* $\bigwedge^d_{\mathbb{Z}\bar{G}} U_S(K^+) \to \bigwedge^d_{\mathbb{Q}\bar{G}} \mathbb{Q}U_S(K^+)$ *with restricted range.* ∎

Remark 2.11. This shows in particular that $\Delta_{f_1,\ldots,f_d}$ vanishes on the kernel of α in the above diagram. One can show that $\ker(\alpha)$ is always finite and supported on primes dividing $2|\bar{G}| = |G|$. Also, Proposition 2.5 implies that $\mathrm{im}(\alpha)$ spans $\mathbb{Z}_{(p)}\Lambda_{0,S}$ over $\mathbb{Z}_{(p)}$ whenever $p \nmid |G|$. So if $p \nmid |G|$ then *any* $\mathbb{Z}\bar{G}$-linear map $F : \bigwedge^d_{\mathbb{Z}\bar{G}} U_S(K^+) \to (\mathbb{Z}/p^{n+1}\mathbb{Z})\bar{G}$ vanishes on $\ker(\alpha)$ and has a *unique* "extension" $\tilde{F} : \mathbb{Z}_{(p)}\Lambda_{0,S} \to (\mathbb{Z}/p^{n+1}\mathbb{Z})\bar{G}$ satisfying $F = \tilde{F} \circ \alpha$.

2.3. Hilbert symbols and the pairing $H_{K/k,n}$. Suppose that L is a local field containing μ_m for some positive integer m coprime to the characteristic of L. We recall that the *Hilbert symbol* is the map

$$(\cdot,\cdot)_{L,m} : L^\times \times L^\times \to \mu_m \subset L^\times, \qquad (\alpha,\beta) \mapsto (\beta^{1/m})^{\sigma_{\alpha,L}-1},$$

where $\beta^{1/m}$ is any mth root of β in any abelian closure L^{ab} of L, and $\sigma_{\alpha,L}$ denotes the image of α under the reciprocity homomorphism $(\cdot, L)$ of local class-field theory from $L^\times$ to $\mathrm{Gal}(L^{\mathrm{ab}}/L)$. The Hilbert symbol is bilinear and skew-symmetric. For the general theory, see [A-T, Ch. 12], [Ne, V.3] or [Se, Ch. XIV]. (Note that our notation $(\alpha,\beta)_{L,m}$ is compatible with that of [A-T] and [Ne] but represents the element denoted (β,α) in [Se] and is similarly reversed in the notation of [Col].)

Let p be a prime number and $n \geq 0$ an integer. We shall assume until further notice that K *contains* $\mu_{p^{n+1}}$ for some $n \geq 0$. Let $\kappa_n : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ be the cyclotomic character modulo p^{n+1}, determined by $\tau(\zeta) = \zeta^{\kappa_n(\tau)}$ for all $\zeta \in \mu_{p^{n+1}}$, and $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Since K contains $\mu_{p^{n+1}}$, the restriction of κ_n to $\mathrm{Gal}(\bar{\mathbb{Q}}/k)$ factors through a homomorphism $G \to (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ which we denote by the same symbol. We also use the shorthand ζ_n for $\xi_{p^{n+1}} \in K$. If $K_\mathfrak{P}$ denotes the completion of K at some prime ideal $\mathfrak{P}$, we may define a bilinear pairing $[\cdot,\cdot]_{\mathfrak{P},n} : K_\mathfrak{P}^\times \times K_\mathfrak{P}^\times \to \mathbb{Z}/p^{n+1}\mathbb{Z}$ by setting

$$\iota_{\mathfrak{P}}(\zeta_n)^{[\alpha,\beta]_{\mathfrak{P},n}} = (\alpha,\beta)_{K_{\mathfrak{P}},p^{n+1}} \quad \text{for all } \alpha,\beta \in K_{\mathfrak{P}}^\times$$

where $\iota_{\mathfrak{P}} : K \to K_{\mathfrak{P}}$ is the natural embedding. Every $g \in G$ induces an isomorphism $K_{\mathfrak{P}} \to K_{g\mathfrak{P}}$, also denoted g and such that $g \circ \iota_{\mathfrak{P}} = \iota_{g\mathfrak{P}} \circ g$. Standard facts from local class field theory imply that $(g\alpha, g\beta)_{K_{g\mathfrak{P}},p^{n+1}} = g(\alpha,\beta)_{K_{\mathfrak{P}},p^{n+1}}$ in $K_{g\mathfrak{P}}^\times$ for any $\alpha,\beta \in K_{\mathfrak{P}}^\times$. It follows easily that

$$(17) \qquad [g\alpha, g\beta]_{g\mathfrak{P},n} = \kappa_n(g)[\alpha,\beta]_{\mathfrak{P},n} \quad \text{for all } \alpha,\beta \in K_{\mathfrak{P}}^\times,\ g \in G.$$

If $\mathfrak{P}$ divides p then $\iota_{\mathfrak{P}}$ extends to a $\mathbb{Q}_p$-algebra map from $K_p := K \otimes_{\mathbb{Q}} \mathbb{Q}_p$ to $K_{\mathfrak{P}}$. Thus we obtain a pairing

$$[\cdot,\cdot]_{K,n} : K_p^\times \times K_p^\times \to \mathbb{Z}/p^{n+1}\mathbb{Z}, \qquad (\alpha,\beta) \mapsto \sum_{\mathfrak{P}|p} [\iota_{\mathfrak{P}}(\alpha), \iota_{\mathfrak{P}}(\beta)]_{\mathfrak{P},n}.$$

Letting G act on K_p through K, we still have $\iota_{\mathfrak{P}} \circ g = g \circ \iota_{g^{-1}\mathfrak{P}}$ for any $g \in G$ and $\mathfrak{P} \,|\, p$, so (17) implies

$$(18) \qquad [g\alpha, g\beta]_{K,n} = \kappa_n(g)[\alpha,\beta]_{K,n} \quad \text{for all } \alpha,\beta \in K_p^\times,\ g \in G.$$

The product map $\prod_{\mathfrak{P}|p} \iota_{\mathfrak{P}} : K_p \to \prod_{\mathfrak{P}|p} K_{\mathfrak{P}}$ is a G-equivariant ring isomorphism (where $g((x_{\mathfrak{P}})_{\mathfrak{P}}) = (g x_{g^{-1}\mathfrak{P}})_{\mathfrak{P}}$ in $\prod_{\mathfrak{P}|p} K_{\mathfrak{P}}$). We shall regard this as an identification so that $\iota_{\mathfrak{P}}$ identifies with the projection $\prod_{\mathfrak{P}|p} K_{\mathfrak{P}} \to K_{\mathfrak{P}}$. Thus we identify the principal semilocal units $\prod_{\mathfrak{P}|p} U^1(K_{\mathfrak{P}})$ with a $\mathbb{Z}G$-submodule of $K_p^\times$ and denote it $U^1(K_p)$. Regarding each $U^1(K_{\mathfrak{P}})$ as a finitely generated $\mathbb{Z}_p$-module, $U^1(K_p)$ becomes a finitely generated $\mathbb{Z}_pG$-module.

From now on we assume that p is odd. Consider the unique ring automorphism of $(\mathbb{Z}/p^{n+1}\mathbb{Z})G$ sending $g \in G$ to $\kappa_n(g)g^{-1}$. Since $\kappa_n(c) = -1$, this restricts to a ring isomorphism from $(\mathbb{Z}/p^{n+1}\mathbb{Z})G^+$ to $(\mathbb{Z}/p^{n+1}\mathbb{Z})G^-$. Composing with $\bar{2}^{-1}\nu_{K/K^+} : (\mathbb{Z}/p^{n+1}\mathbb{Z})\bar{G} \to (\mathbb{Z}/p^{n+1}\mathbb{Z})G$, we obtain a ring isomorphism $\bar{\kappa}_n^* = \bar{\kappa}_{K,n}^* : (\mathbb{Z}/p^{n+1}\mathbb{Z})\bar{G} \to (\mathbb{Z}/p^{n+1}\mathbb{Z})G^-$. Explicitly, if $h \in \bar{G}$ and $g \in G$ then

$$(19) \quad \bar{\kappa}_n^*(h) = \bar{2}^{-1} \sum_{\substack{\tilde{h} \in G \\ \pi_{K/K^+}(\tilde{h}) = h}} \kappa_n(\tilde{h})\tilde{h}^{-1} \text{ and so } \bar{\kappa}_n^*(\pi_{K/K^+}(g)) = e^- \kappa_n(g) g^{-1}.$$

Given a set $S \supset S^0$ as in previous sections, any $u \in U^1(K_p)$ defines a homomorphism $f_u \in \mathrm{Hom}_{\mathbb{Z}}(U_S(K^+), \mathbb{Z}/p^{n+1}\mathbb{Z})$ by setting $f_u(\varepsilon) = [\varepsilon, u]_{K,n}$ (by abuse, we write ε for $\varepsilon \otimes 1 \in K_p^\times$). Using the "$\tilde{\Delta}$" notation of the last section we may now define a map

$$H_{K/k,S,n} : \mathbb{Z}_{(p)}\Lambda_{0,S}(K^+/k) \times U^1(K_p)^d \to (\mathbb{Z}/p^{n+1}\mathbb{Z})G^-,$$
$$(\eta; u_1, \ldots, u_d) \mapsto 2^d \bar{\kappa}_n^*(\tilde{\Delta}_{f_{u_1},\ldots,f_{u_d}}(\eta)).$$

PROPOSITION 2.12. *Suppose that $\eta \in \mathbb{Z}_{(p)}\Lambda_{0,S}(K^+/k)$ and $u_1, \dots, u_d \in U^1(K_p)^d$.*

(i) *For any $x \in \mathbb{Z}\bar{G}$ we have*

$$H_{K/k,S,n}(x\eta; u_1, \dots, u_d) = \bar{\kappa}_n^*(\bar{x}) H_{K/k,S,n}(\eta; u_1, \dots, u_d)$$

where $\bar{x}$ denotes the image of x in $(\mathbb{Z}/p^{n+1}\mathbb{Z})\bar{G}$.

(ii) *$H_{K/k,S,n}$ is $\mathbb{Z}G$-multilinear (hence $\mathbb{Z}_pG$-multilinear) and alternating as a function of $u_1, \dots, u_d$.*

Proof. Part (i) follows from Proposition 2.10(i). The $\mathbb{Z}$-multilinearity in part (ii) follows from Proposition 2.10(ii) so it suffices to prove that replacing u_i by gu_i (for $g \in G$) multiplies $H_{K/k,S,n}(\eta; u_1, \dots, u_d)$ by g, or indeed by e^-g since it lies in the minus part. But if we write h for $\pi_{K/K^+}(g) \in \bar{G}$ then (18) and Proposition 2.10(ii) give

$$\begin{aligned}
\bar{\kappa}_n^*(\tilde{\Delta}_{f_{u_1},\dots,f_{gu_i},\dots,f_{u_d}}(\eta)) &= \bar{\kappa}_n^*(\tilde{\Delta}_{f_{u_1},\dots,\kappa_n(g)f_{u_i}\circ h^{-1},\dots,f_{u_d}}(\eta)) \\
&= \bar{\kappa}_n^*(\tilde{\Delta}_{f_{u_1},\dots,f_{u_d}}(\eta)\kappa_n(g)h^{-1}) \\
&= \bar{\kappa}_n^*(\kappa_n(g)h^{-1})\bar{\kappa}_n^*(\tilde{\Delta}_{f_{u_1},\dots,f_{u_d}}(\eta)) \\
&= e^-g\bar{\kappa}_n^*(\tilde{\Delta}_{f_{u_1},\dots,f_{u_d}}(\eta))
\end{aligned}$$

by (19) and the result follows. ∎

By part (ii) of the proposition, $H_{K/k,S,n}$ defines a unique pairing (also denoted $H_{K/k,S,n}$) from $\mathbb{Z}_{(p)}\Lambda_{0,S} \times \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)$ to $(\mathbb{Z}/p^{n+1}\mathbb{Z})G^-$. By $\mathbb{Z}_pG$-linearity in the second variable, it factors through the projection on $\bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)^-$. An important and simple special case is when η equals $(1\otimes\varepsilon_1)\wedge\dots\wedge(1\otimes\varepsilon_d) \in \overline{\bigwedge^d_{\mathbb{Z}\bar{G}} U_S(K^+)}$. Using Proposition 2.10(iii) and equation (19) and tracing through the definitions, we find that for all $u_1, \dots, u_d$ in $U^1(K_p)$,

$$\begin{aligned}
&H_{K/k,S,n}((1\otimes\varepsilon_1)\wedge\dots\wedge(1\otimes\varepsilon_d), u_1\wedge\dots\wedge u_d) \\
&\quad = 2^d\bar{\kappa}_n^*(\Delta_{f_{u_1},\dots,f_{u_d}}(\varepsilon_1\wedge\dots\wedge\varepsilon_d)) = \bar{\kappa}_n^*\Big(\det\Big(2\sum_{h\in\bar{G}}[h^{-1}\varepsilon_i, u_t]_{K,n}h\Big)_{1\le i,t\le d}\Big) \\
&\quad = \det\Big(\bar{\kappa}_n^*\Big(\sum_{g\in G}[g^{-1}\varepsilon_i, u_t]_{K,n}\pi_{K/K^+}(g)\Big)\Big)_{1\le i,t\le d} \\
&\quad = \det\Big(e^-\sum_{g\in G}\kappa_n(g)[g^{-1}\varepsilon_i, u_t]_{K,n}g^{-1}\Big)_{1\le i,t\le d}.
\end{aligned}$$

But $\sum_{g\in G}\kappa_n(g)[g^{-1}\varepsilon_i, u_t]_{K,n}g^{-1}$ clearly lies in the minus part, and (18) allows us to rewrite it as $\sum_{g\in G}[\varepsilon_i, gu_t]_{K,n}g^{-1}$. Thus we obtain simply

$$(20)\qquad H_{K/k,S,n}((1\otimes\varepsilon_1)\wedge\cdots\wedge(1\otimes\varepsilon_d), u_1\wedge\cdots\wedge u_d) = \det\Big(\sum_{g\in G}[\varepsilon_i, gu_t]_{K,n}g^{-1}\Big)_{1\le i,t\le d}.$$

This shows in particular that, on $\bigwedge^d_{\mathbb{Z}\bar{G}} U_S(K^+)\times\bigwedge^d_{\mathbb{Z}_pG}U^1(K_p)$, the pairing $H_{K,n}(\alpha(\cdot),\cdot)$ agrees with that defined by the pairing $\mathcal{H}_{K,n}(\cdot,\cdot)$ of [So5].

Remark 2.13. If $S\supset S'\supset S^0$, we shall always view the natural injection $\bigwedge^d_{\mathbb{Q}\bar{G}}\mathbb{Q}U_{S'}(K^+)\to\bigwedge^d_{\mathbb{Q}\bar{G}}\mathbb{Q}U_S(K^+)$ as an inclusion. It is then a simple exercise to check "compatibility of the pairings as S varies" in the sense that $\Lambda_{0,S}$ contains $\Lambda_{0,S'}$ and $H_{K/k,S,n}$ agrees with $H_{K/k,S',n}$ on $\mathbb{Z}_{(p)}\Lambda_{0,S'}\times\bigwedge^d_{\mathbb{Z}_pG}U^1(K_p)$. For this reason, we shall usually omit the reference to S and write simply $H_{K/k,n}$.

2.4. The map $\mathfrak{s}_{K/k,S}$. For the time being we drop Hypothesis 2.3 and the assumption that K contains $\mu_{p^{n+1}}$. We use the element $a^-_{K/k,S}$ to define a generalisation of the map $\mathfrak{s}_{K/k}$ of [So5] (slightly modified). Let j be any embedding of $\bar{\mathbb{Q}}$ into a fixed algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. For each $i=1,\dots,d$, the composite $j\tau_i:\bar{\mathbb{Q}}\to\bar{\mathbb{Q}}_p$ defines a prime ideal $\mathfrak{P}_i$ of $\mathcal{O}_K$ dividing p, namely $\mathfrak{P}_i=\{a\in\mathcal{O}_K : |j\tau_i(a)|_p<1\}$. (Of course, the ideals $\mathfrak{P}_1,\dots,\mathfrak{P}_d$ are not in general distinct.) So $j\tau_i$ gives rise to an isometric embedding $K_{\mathfrak{P}_i}\to\bar{\mathbb{Q}}_p$ (with the appropriately normalised $\mathfrak{P}_i$-adic metric on $K_{\mathfrak{P}_i}$) whose image is the topological closure $\overline{j\tau_i(K)}$. This embedding is also denoted $j\tau_i$, by abuse.

There is a composite homomorphism of $\mathbb{Q}_p$-algebras

$$\delta_i=\delta_i^{(j)}:=j\tau_i\circ\iota_{\mathfrak{P}_i}:K_p\to\bar{\mathbb{Q}}_p$$

where $\iota_{\mathfrak{P}_i}:K_p\to K_{\mathfrak{P}_i}$ is as in the previous section. It follows in particular that if u lies in $U^1(K_p)\subset K_p$ then $|\delta_i^{(j)}(u)-1|_p<1$ for all i, hence the element $\log_p(\delta_i^{(j)}(u))$ of $\overline{j\tau_i(K)}$ is given by the usual logarithmic series. In Proposition/Definition 2.4 we take $\mathcal{R}=\mathbb{Z}_p$, $\mathcal{S}=\bar{\mathbb{Q}}_p$, $M=U^1(K_p)$, $H=G$, $l=d$ and set $f_i(u):=\log_p(\delta_i^{(j)}(u))$ for all $u\in U^1(K_p)$ and $i\in\{1,\dots,d\}$ to get a *p-adic regulator map* $R_{K/k,p}:=\Delta_{f_1,\dots,f_d}:\bigwedge^d_{\mathbb{Z}_pG}U^1(K_p)\to\bar{\mathbb{Q}}_pG$. (We will denote it $R^{(j)}_{K/k,p}$ or $R^{(j;\tau_1,\dots,\tau_d)}_{K/k,p}$ if we need to indicate the dependence on j and/or $\tau_1,\dots,\tau_d$.) For any abelian group H and commutative ring $\mathcal{R}$ we define an involutive automorphism $(\cdot)^*$ of $\mathcal{R}H$ by setting $(\sum a_hh)^*=\sum a_hh^{-1}$. The element $a^-_{K/k,S}$ lies in $\bar{\mathbb{Q}}G^-$ by (10), hence so does $a^{-,*}_{K/k,S}$ and applying j to the coefficients we obtain an element $j(a^{-,*}_{K/k,S})$ of $\bar{\mathbb{Q}}_pG^-$.

Definition 2.14. For any $\theta \in \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)$ we define $\mathfrak{s}_{K/k,S}(\theta) = \mathfrak{s}_{K/k,S,p}(\theta)$ to be the product $j(a^{-,*}_{K/k,S})R^{(j)}_{K/k,p}(\theta)$ in $\bar{\mathbb{Q}}_pG$.

Remark 2.15. It is easy to see that permuting the τ_i can only change the sign of the regulator $R^{(j)}_{K/k,p}$ and hence of the map $\mathfrak{s}_{K/k,S}$ and that if τ_i is replaced by $\tau_i\tau$ for some $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/k)$ then both are multiplied by $\tau|_K \in G$. If clarity demands it we shall indicate this (simple) dependence on the τ_i by writing $\mathfrak{s}^{\tau_1,\dots,\tau_d}_{K/k,S}$ instead of $\mathfrak{s}_{K/k,S}$.

If $\mathfrak{s}_{K/k}$ denotes the map introduced in Definition 3.1 of [So5] then (9) gives

$$\begin{aligned}(21)\qquad \mathfrak{s}_{K/k,S}(\theta) &= e^- \prod_{\mathfrak{q}\in S\setminus S^0} (1 - N\mathfrak{q}^{-1}\sigma_{\mathfrak{q}}) j(\sqrt{d_k}\,\Phi_{K/k}(0)^*) R^{(j)}_{K/k,p}(\theta)\\ &= e^- \prod_{\mathfrak{q}\in S\setminus S^0} (1 - N\mathfrak{q}^{-1}\sigma_{\mathfrak{q}})\mathfrak{s}_{K/k}(\theta)\end{aligned}$$

and if $k \neq \mathbb{Q}$ then we can even drop the factor e^-. Equation (21) and Proposition 3.4 of [So5] imply the important

Proposition 2.16. *$\mathfrak{s}_{K/k,S}(\theta)$ lies in $\mathbb{Q}_pG^-$ for every $\theta \in \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)$. Moreover, it is independent of the choice of j.* ∎

In [So5], $\mathfrak{s}_{K/k}$ was considered as a ($\mathbb{Z}_pG$-linear) map from $\bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)$ to $\mathbb{Q}_pG$. But because of the factor e^- in (21), we now have $\mathfrak{s}_{K/k,S}(e^-\theta) = e^-\mathfrak{s}_{K/k,S}(\theta) = \mathfrak{s}_{K/k,S}(\theta)$. For this reason, we prefer to consider $\mathfrak{s}_{K/k,S}$ as a $\mathbb{Z}_pG$-linear map from $\bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)^-$ to $\mathbb{Q}_pG^-$.

Proposition 2.17. *The kernel of $\mathfrak{s}_{K/k,S}$ is precisely the ($\mathbb{Z}_p$-) torsion submodule of $\bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)^-$ which is finite. The image of $\mathfrak{s}_{K/k,S}$ is a fractional ideal of $\mathbb{Q}_pG^-$ (i.e. a finitely generated $\mathbb{Z}_pG$-submodule of $\mathbb{Q}_pG^-$ which spans it over $\mathbb{Q}_p$).*

Proof. In Remark 3.2 of [So5] it was shown that $\ker(R^{(j)}_{K/k,p})$ is finite and that $\mathrm{im}(R^{(j)}_{K/k,p})$ spans $\bar{\mathbb{Q}}_pG$ over $\bar{\mathbb{Q}}_p$. Also, equation (10) implies that $j(a^{-,*}_{K/k,S})$ is a unit of the ring $\bar{\mathbb{Q}}_pG^-$. It follows that $\ker(\mathfrak{s}_{K/k,S})$ lies in $\ker(R^{(j)}_{K/k,p})$ and hence in $(\bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)^-)_{\mathrm{tor}}$. The reverse inclusion is clear, since $\mathbb{Q}_pG^-$ is torsion-free.

For the second statement, finite generation follows from that of $U^1(K_p)$ and we have $\bar{\mathbb{Q}}_p\mathrm{im}(\mathfrak{s}_{K/k,S}) = \bar{\mathbb{Q}}_pG^-\mathrm{im}(\mathfrak{s}_{K/k,S}) = \bar{\mathbb{Q}}_pG^-\mathrm{im}(R^{(j)}_{K/k,p}) = \bar{\mathbb{Q}}_pG^-$. It follows that $\mathbb{Q}_p\mathrm{im}(\mathfrak{s}_{K/k,S}) = \mathbb{Q}_pG^-$. ∎

DEFINITION 2.18. We set $\mathfrak{S}_{K/k,S} = \mathfrak{S}_{K/k,S,p} := \operatorname{im}(\mathfrak{s}_{K/k,S,p}) \subset \mathbb{Q}_pG^-$. (Proposition 2.16 and Remark 2.15 show that $\mathfrak{S}_{K/k,S}$ is independent of j and the choice and ordering of the τ_i's.)

Thus

$$\mathfrak{S}_{K/k,S} = e^- \prod_{\mathfrak{q}\in S\setminus S^0} (1 - N\mathfrak{q}^{-1}\sigma_{\mathfrak{q}})\mathfrak{S}_{K/k} \tag{22}$$

where $\mathfrak{S}_{K/k} = \operatorname{im}(\mathfrak{s}_{K/k})$ as in [So5], and if $k \neq \mathbb{Q}$ then we can drop the factor e^-. Finally, the dependence of $\mathfrak{s}_{K/k,S}$ and $\mathfrak{S}_{K/k,S}$ on S is clear: if $S \supset S' \supset S^0$ then (4) and the definition of $a^-_{K/k,S}$ give

$$\begin{aligned} \mathfrak{s}_{K/k,S} &= \prod_{\mathfrak{q}\in S\setminus S'} (1 - N\mathfrak{q}^{-1}\sigma_{\mathfrak{q}})\mathfrak{s}_{K/k,S'}, \\ \mathfrak{S}_{K/k,S} &= \prod_{\mathfrak{q}\in S\setminus S'} (1 - N\mathfrak{q}^{-1}\sigma_{\mathfrak{q}})\mathfrak{S}_{K/k,S'}. \end{aligned} \tag{23}$$

3. Statements of the conjectures. Let us write S_p for $S_p(k)$ and $S^1 = S^1(K/k)$ for $S_p \cup S^0 = S_p \cup S_{\mathrm{ram}}(K/k) \cup S_\infty$.

HYPOTHESIS 3.1. *S contains S^1.*

Henceforth, the three conditions $p \neq 2$, Hypothesis 2.2 and Hypothesis 3.1 will be referred to as *the standard hypotheses* and *will be assumed to hold unless it is explicitly stated otherwise.* Our "Integrality Conjecture" (IC) reads:

CONJECTURE IC$(K/k, S, p)$. *$\mathfrak{S}_{K/k,S} \subset \mathbb{Z}_pG^-$.*

REMARK 3.2. By using [So5, Cor. 2.1] and estimates of $\log_p$ one can find explicit values of N such that $\mathfrak{S}_{K/k,S} \subset p^{-N}\mathbb{Z}_pG^-$ (cf. the proof of Prop. 4.2, ibid.). The conjecture says we can take $N = 0$. Fixing K/k but letting p (hence S^1) vary, one can also show that $\mathfrak{S}_{K/k,S^1,p} = \mathbb{Z}_pG^-$ for all but finitely many $p \neq 2$. In fact, this follows easily from Theorem 6.1 below.

REMARK 3.3. Equation (22) gives

$$\mathfrak{S}_{K/k,S^1} = e^- \prod_{\mathfrak{p}\in S_p\setminus S_{\mathrm{ram}}} (1 - N\mathfrak{p}^{-1}\sigma_{\mathfrak{p}})\mathfrak{S}_{K/k} = e^-\Big(\prod_{\mathfrak{p}\in S_p\setminus S_{\mathrm{ram}}} N\mathfrak{p}\Big)^{-1}\mathfrak{S}_{K/k}.$$

(For the second equality, observe that if $\mathfrak{p}$ lies in $S_p \setminus S_{\mathrm{ram}}$ then $N\mathfrak{p} - \sigma_{\mathfrak{p}}$ is a unit of $\mathbb{Z}_pG$.) If $k \neq \mathbb{Q}$ we may, as usual, drop the factor e^- in the last equation. It follows in particular that if $k \neq \mathbb{Q}$ then IC$(K/k, S^1, p)$ is equivalent to Conjecture 5.2 of [So5, §5.2]. If $k = \mathbb{Q}$ the latter conjecture was proven there. IC$(K/\mathbb{Q}, S^1, p)$ follows on applying e^- and will be reproven in Theorem 4.3.

Hypothesis 3.1 implies Hypothesis 2.3 so that the conditions of Conjecture $\mathrm{RSC}(K^+/k, S; \mathbb{Z}_{(p)})$ are met. Our "Congruence Conjecture" (CC) reads:

CONJECTURE $\mathrm{CC}(K/k, S, p, n)$ (Congruence Conjecture). *Suppose that Conjecture* $\mathrm{IC}(K/k, S, p)$ *holds and that* $\mathrm{RSC}(K^+/k, S; \mathbb{Z}_{(p)})$ *holds with solution* $\eta_{K^+/k,S}$. *If also* $K \supset \mu_{p^{n+1}}$ *for some* $n \geq 0$, *then for all* $\theta \in \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)^-$ *we have*

$$\overline{\mathfrak{s}_{K/k,S}(\theta)} = \kappa_n(\tau_1 \ldots \tau_d) H_{K/k,n}(\eta_{K^+/k,S}, \theta) \quad (\text{in } (\mathbb{Z}/p^{n+1}\mathbb{Z})G^-). \tag{24}$$

REMARK 3.4. The factor $\kappa_n(\tau_1 \ldots \tau_d)$ means that the Congruence Conjecture is independent of the choice of $\tau_1, \ldots, \tau_d$. For example, if we replace τ_i by $\tau_i\tau^{-1}$ for some $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/k)$ then Remark 2.7, Proposition 2.12(i) and (19) show that the R.H.S. is multiplied by $\tau|_K^{-1} \in G$ and the same is true for the L.H.S. by Remark 2.15.

REMARK 3.5. $\mathrm{CC}(K/k, S, p, n)$ replaces Conjecture 5.4 of [So5]. The latter is essentially the special case of the CC in which $S = S^1$ and p splits in k (so that $\mu_p \subset K$ forces $S^0 = S^1$). In fact, it is a direct consequence of this case provided one assumes (with no significant loss of generality) that K is CM, $k \neq \mathbb{Q}$ and one replaces $\bigwedge^d_{\mathbb{Z}G} K^\times$ in Conjecture 5.4 with $\bigwedge^d_{\mathbb{Z}\bar{G}} U_S(K^+)$ as here. The awkwardness in the formulation of Conjecture 5.4 (using $\mathcal{I}(\eta^+_{K/k})$, $\tilde{\eta}_x$ etc.) has been avoided in the CC thanks to our "extension" of $H_{K,n}$ to $\mathbb{Z}_{(p)}\Lambda_{0,S}$.

4. Evidence for the IC and the CC

4.1. The results of [So5]. Conjecture 5.2 of [So5] implies $\mathrm{IC}(K/k, S, p)$ for $S = S^1$ (see Remark 3.3) and hence for all S (using Proposition 5.1, see below). Therefore Proposition 4.2 of [So5] implies

THEOREM 4.1. $\mathrm{IC}(K/k, S, p)$ *holds whenever* p *is unramified in* $K/\mathbb{Q}$. ∎

By a similar argument, the main result, Theorem 4.1, of [So5] implies

THEOREM 4.2. $\mathrm{IC}(K/k, S, p)$ *holds whenever* p *splits completely in* $k/\mathbb{Q}$ *and either* $S_{\mathrm{ram}}(K/k) \not\subset S_p(k)$ *or* $\mu_p(K) = \{1\}$. ∎

4.2. The IC and the ETNC. Working on the original version of the IC in [So5], Andrew Jones has shown that a certain refinement would follow from the ETNC (see the Introduction). Let $\mathrm{Cl}_\mathfrak{m}(K)$ be the ray-class group of K corresponding to the cycle which is the formal product of the finite places of K above those in S^1 and write $\mathrm{Fitt}_{\mathbb{Z}G}(\mathrm{Cl}_\mathfrak{m}(K))$ for its (initial) Fitting ideal as a $\mathbb{Z}G$-module. In our notation, the first part of [Jo, Theorem 4.1.1] then says that the relevant case of the ETNC (namely [Bu1, Conj. 4(iv)] for the pair $(h^0\mathrm{Spec}(K)(1), e^-\mathbb{Z}G)$) implies

$$\mathfrak{S}_{K/k,S^1} \subset (\mathbb{Z}_p\mathrm{Fitt}_{\mathbb{Z}G}(\mathrm{Cl}_\mathfrak{m}(K)))^- \ (= \mathrm{Fitt}_{\mathbb{Z}_pG^-}((\mathrm{Cl}_\mathfrak{m}(K) \otimes \mathbb{Z}_p)^-)) \tag{25}$$

for all odd primes p. The inclusion (25), hence the ETNC, clearly implies $\mathrm{IC}(K/k,S,p)$ for $S=S^1$, hence for all S. Of course, it implies considerably more (for instance, that $\mathfrak{S}_{K/k,S^1}$ annihilates the p-part of $\mathrm{Cl}_{\mathfrak{m}}(K)$) and in this sense refines the IC in a different direction from the CC. We note that the relevant case of the ETNC has been proven in our set-up only when K is an absolutely abelian field (see below).

4.3. Strengthenings of the IC in the case $p\nmid|G|$. The second part of Jones' Theorem 4.1.1 states that if the above case of the ETNC holds and also $p\nmid|G|$, then we have the following strengthening of (25):

(26)
$$\mathfrak{S}_{K/k,S^1}=\begin{cases}\mathrm{Fitt}_{\mathbb{Z}_pG^-}(\mu_{p^\infty}(K_p)^-/\mu_{p^\infty}(K))\mathrm{Fitt}_{\mathbb{Z}_pG^-}((\mathrm{Cl}_{\mathfrak{m}}(K)\otimes\mathbb{Z}_p)^-) \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } S_{\mathrm{ram}}(K/k)\subset S_p,\\ \mathrm{Fitt}_{\mathbb{Z}_pG^-}(\mu_{p^\infty}(K_p)^-)\mathrm{Fitt}_{\mathbb{Z}_pG^-}((\mathrm{Cl}_{\mathfrak{m}}(K)\otimes\mathbb{Z}_p)^-) \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } S_{\mathrm{ram}}(K/k)\not\subset S_p.\end{cases}$$

Corollary 4.1.8 of [Jo] also establishes (26) when $p\nmid|G|$ *without* assuming the ETNC but imposes a mild condition on the characters of G. (The proof uses results of [Wi] and work of Bley, Burns and others on, roughly speaking, the compatibility of the ETNC with the functional equations of L-functions.)

Independently, we used the functional equations themselves and more elementary, index-type arguments to give a different (and unconditional) formula for $\mathfrak{S}_{K/k,S}$ whenever $p\nmid|G|$. This is presented as Theorem 6.1. Corollary 6.2 shows how one may quickly deduce $\mathrm{IC}(K/k,S,p)$ in this case. Of course, it would also follow immediately from Jones' formula (26). In fact, there is a direct link between the two formulae, explained in Remark 6.3.

4.4. The case $k=\mathbb{Q}$. When $k=\mathbb{Q}$, the IC follows from Corollary 4.1 of [So5] (or indeed from the work of Jones, see below). In Section 7 we shall prove the CC in this case, reproving the IC along the way:

THEOREM 4.3.

(i) *Conjecture* $\mathrm{IC}(K/\mathbb{Q},S,p)$ *holds.*
(ii) *If K contains $\mu_{p^{n+1}}$ for some $n\geq 0$, then Conjecture* $\mathrm{CC}(K/\mathbb{Q},S,p,n)$ *holds.*

4.5. The case of absolutely abelian K. As noted in [Jo, Cor. 4.1.7], the relevant case of the ETNC follows from [B-F, Cor. 1.2] whenever K is absolutely abelian and k is any totally real subfield (possibly but not necessarily equal to $\mathbb{Q}$). Thus the inclusion (25) holds and in particular

THEOREM 4.4. *If K is an abelian extension of $\mathbb{Q}$, then Conjecture* $\mathrm{IC}(K/k,S,p)$ *holds.* ∎

To state our result for the CC, in this case, we first define a set of rational primes

$$\mathrm{Bad}(S) := \{q \in S_{\mathrm{ram}}(k/\mathbb{Q}) : S_q(k) \not\subset S\}$$

and formulate

HYPOTHESIS 4.5. *$p \nmid e_q(k/\mathbb{Q})$ for all $q \in \mathrm{Bad}(S)$.*

In Section 8 we shall show

THEOREM 4.6. *If K is an abelian extension of $\mathbb{Q}$ containing $\mu_{p^{n+1}}$ for some $n \geq 0$ and Hypothesis 4.5 is satisfied, then Conjecture $\mathrm{CC}(K/k, S, p, n)$ holds.*

(At the same time we shall obtain a second proof of Theorem 4.4 which assumes Hypothesis 4.5 but is independent of the ETNC.) The proof of Theorem 4.6 uses induction formulae for L-functions to relate the situation for K/k to that of $F/\mathbb{Q}$ for various CM subfields F of K, and this in two parallel applications. The first concerns $\mathfrak{s}_{K/k,S}$ and works at $s = 1$. The second concerns $\mathrm{RSC}(K^+/k, S; \mathbb{Z}_{(p)})$ and works at $s = 0$. Popescu introduced the latter application in [Po]. (In fact, he applied it to his own variant of Rubin's Conjecture B$'$ which also implies $\mathrm{RSC}(K^+/k, S; \mathbb{Z})$.) He worked under a hypothesis which implies $\mathrm{Bad}(S) = \emptyset$. This simplifies matters (we only need to consider $F = K$) but is rather restrictive (e.g. $\mathrm{Bad}(S^1(K/k)) \neq \emptyset$ whenever a rational prime $q \neq p$ ramifies in $k/\mathbb{Q}$ but not in K/k). The elaboration of Popescu's techniques which allows us to conclude under our weaker Hypothesis 4.5 is one ingredient of Cooper's work on Popescu's Conjecture in [Coo]. Hypothesis 4.5 holds, for example, whenever $p \nmid [k : \mathbb{Q}]$ (e.g. $[k : \mathbb{Q}]$ is a power of 2). Alternatively, suppose $K = \mathbb{Q}(\xi_f)$ and $k = K^+$ where $f = p^{n+1} f' \not\equiv 2 \pmod 4$, $n \geq 0$ and $p \nmid f'$. If we take $S = S^1(K/k) = S_\infty \cup S_p$ then $\mathrm{Bad}(S) = \emptyset \Leftrightarrow f' = 1$, but Hypothesis 4.5 holds provided only $p \nmid q - 1$ for all $q \mid f'$.

4.6. Two "trivial" cases of the congruence (24). Suppose $K \supset \mu_{p^{n+1}}$ for some $n \geq 0$ and S contains at least $d + 2$ places and at least one finite place $\mathfrak{q}$ that splits completely in K^+. Equations (11) and (12) imply $\Theta^{(d)}_{K^+/k,S} = 0$ so that $\mathrm{RSC}(K^+/k, S; \mathbb{Z})$ holds with $\eta_{K^+/k,S} = 0$. The congruence (24) is thus equivalent to $\mathfrak{s}_{K/k,S}(\theta) \in p^{n+1}\mathbb{Z}_p G^-$. The extension $K/K^+ = K^+(\mu_{p^{n+1}})/K^+$ is unramified outside p, so if $\mathfrak{q}$ does not divide p then it cannot lie in S^1 (which forces $|S| \geq d + 2$). We can then apply the following result. (For a case with $\mathfrak{q} \mid p$, see the next subsection.)

PROPOSITION 4.7. *Suppose $K \supset \mu_{p^{n+1}}$ and $\mathfrak{q} \in S \setminus S^1(K/k)$ splits (completely) in K^+. If $\mathrm{IC}(K/k, S \setminus \{\mathfrak{q}\}, p)$ holds (e.g. if $p \nmid |G|$) then $\mathfrak{S}_{K/k,S} \subset p^{n+1}\mathbb{Z}_p G^-$. In particular, $\mathrm{CC}(K/k, S, p, n)$ holds.*

Proof. By (23) it clearly suffices to show that p^{n+1} divides $(N\mathfrak{q}-\sigma_{\mathfrak{q}})e^-$. Since $\mathfrak{q}$ splits in K^+, $\sigma_{\mathfrak{q}}$ is either 1 or c, and since $\mathfrak{q}\nmid p$, it acts on $\mu_{p^{n+1}}$ by $N\mathfrak{q}$. If $\sigma_{\mathfrak{q}}=1$, it also acts trivially, so p^{n+1} divides $N\mathfrak{q}-1$ hence also $(N\mathfrak{q}-1)e^-=(N\mathfrak{q}-\sigma_{\mathfrak{q}})e^-$. If $\sigma_{\mathfrak{q}}=c$, it also acts by -1, so p^{n+1} divides $N\mathfrak{q}+1$ hence also $(N\mathfrak{q}+1)e^-=(N\mathfrak{q}-\sigma_{\mathfrak{q}})e^-$. ∎

Next, suppose that θ is a $\mathbb{Z}_p$-torsion element in $\bigwedge^d_{\mathbb{Z}_pG}U^1(K_p)^-$. Then Proposition 2.17 implies that the L.H.S. of (24) vanishes, so, assuming $\mathrm{RSC}(K^+/k,S;\mathbb{Z}_{(p)})$, this congruence is equivalent to $H_{K/k,n}(\eta_{K^+/k,S},\theta)=0$. If also $p\nmid|G|$, then this is an immediate consequence of the following result, to be proved in Section 6. (The verification seems harder if $p\,|\,|G|$ (and $d\geq 2$), not least because $(\bigwedge^d_{\mathbb{Z}_pG}U^1(K_p))_{\mathrm{tor}}$ is then harder to characterise.)

PROPOSITION 4.8. *Suppose $p\nmid|G|$, $K\supset\mu_{p^{n+1}}$ and η is any element of $\mathbb{Z}_{(p)}\Lambda_{0,S}(K^+/k)$ satisfying the eigenspace condition with respect to $(S,d,\bar{G})$. Then $H_{K/k,n}(\eta,\theta)=0$ for all $\theta\in(\bigwedge^d_{\mathbb{Z}_pG}U^1(K_p))_{\mathrm{tor}}$.*

4.7. The case $k=K^+$. In this case $G=\{1,c\}$ so $p\nmid|G|$ and the IC holds for all admissible S. For the CC, we assume $K\supset\mu_{p^{n+1}}$ with $n\geq 0$ so that $K=k(\mu_{p^{n+1}})$ and $S^1=S_\infty\cup S_p$. All places of k split in K^+ so if $S\neq S^1$ then $\mathrm{CC}(K/k,S,p,n)$ holds by Proposition 4.7. Also, if $|S_p(k)|\geq 2$ then $|S|\geq d+2$ so once again $\mathrm{CC}(K/k,S^1,p,n)$ is equivalent to $\mathfrak{S}_{K/k,S}\subset p^{n+1}\mathbb{Z}_pG^-$ (see above). But this will follow from equation (32) in Section 6 (for the unique odd character ϕ; indeed, the first term on the R.H.S. of (32) is clearly divisible by $(p^{n+1})^{|S_p|-1}$). This leaves only the case $S=S_\infty\cup S_p$ with $|S_p(k)|=1$. Then $\eta_{k/k,S^1}$ is non-zero and can be written explicitly in terms of a $\mathbb{Z}$-basis $\varepsilon_1,\ldots,\varepsilon_d$ for $U_{S^1}(k)/\{\pm1\}$ and the S_p-classnumber of k. Furthermore, $a^-_{K/k,S}$ can be calculated explicitly. Thus $\mathrm{CC}(K/k,S^1,p,n)$ reduces to a new and unproven identity in $\mathbb{Z}/p^{n+1}\mathbb{Z}$, relating a p-adic regulator of elements of $U^1(K_p)^-$ to a determinant of their Hilbert symbols with the ε_i. This was studied in [Bo]. Results include a proof of a weaker divisibility statement, a proposed analogous identity for $p=2$ and full numerical verification of these identities in more than 100 varied cases.

4.8. Other computational results. $\mathrm{RSC}(K^+/k,S;\mathbb{Q})$ is not currently known to hold non-trivially for any S 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. However, if d is not too large, high-precision computation can identify $\eta_{K^+/k,S}$ with virtual certainty as the unique solution of (15) in $e_{S,d,\bar{G}}\bigwedge^d_{\mathbb{Q}\bar{G}}\mathbb{Q}U_S(K^+)$. (This was done in [R-S1].) This makes it possible to check the CC (and simultaneously the IC) on a computer. In [R-S2] we give details of such numerical verifications for nearly 50 cases of $\mathrm{CC}(K/k,S^1,p,n)$ with k real quadratic, $n=0$ or 1 and varying K and p.

5. Changing S, K and n. If $\mathfrak{q}$ is a prime ideal of k not in S_p then $(1 - N\mathfrak{q}^{-1}\sigma_{\mathfrak{q}})$ lies in $\mathbb{Z}_pG$. Hence (23) gives

PROPOSITION 5.1. *If $S \supset S' \supset S^1$ then the conjecture* $\mathrm{IC}(K/k, S', p)$ *implies* $\mathrm{IC}(K/k, S, p)$. ∎

REMARK 5.2. For the converse one would need $e^-(1 - N\mathfrak{q}^{-1}\sigma_{\mathfrak{q}})$ to be invertible in $\mathbb{Z}_pG^-$ for each $\mathfrak{q} \in S \setminus S'$. But for any such $\mathfrak{q}$ one has an isomorphism of $\mathbb{Z}_pG$-modules

$$(27)\qquad \mathbb{Z}_pG/(1 - N\mathfrak{q}^{-1}\sigma_{\mathfrak{q}}) \cong (\mathcal{O}_K/\mathfrak{q}\mathcal{O}_K)^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \bigoplus_{\mathfrak{Q}} (\mathbb{F}_{\mathfrak{Q}}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p)$$

where $\mathfrak{Q}$ runs through the primes dividing $\mathfrak{q}$ in K and $\mathbb{F}_{\mathfrak{Q}}$ denotes $\mathcal{O}_K/\mathfrak{Q}$. Hence, if $c \notin D_{\mathfrak{q}}(K/k)$ (respectively, $c \in D_{\mathfrak{q}}(K/k)$) then $e^-(1 - N\mathfrak{q}^{-1}\sigma_{\mathfrak{q}})$ lies in $(\mathbb{Z}_pG^-)^\times$ if and only if $p \nmid |\mathbb{F}_{\mathfrak{Q}}^\times|$ (respectively, $p \nmid |\mathbb{F}_{\mathfrak{Q}}^\times/(1+c)\mathbb{F}_{\mathfrak{Q}}^\times|$) for one, hence any $\mathfrak{Q}$. This fails in particular if $\mu_p \subset K$, in which case $\mathrm{IC}(K/k, S, p)$ does not by itself imply $\mathrm{IC}(K/k, S', p)$ for any $S \supsetneq S'$.

PROPOSITION 5.3. *Suppose $S \supset S' \supset S^1$ and* $\mathrm{RSC}(K^+/k, S'; \mathbb{Z}_{(p)})$ *holds with solution $\eta_{K^+/k,S'}$. Then* $\mathrm{RSC}(K^+/k, S; \mathbb{Z}_{(p)})$ *holds with solution* $\eta_{K^+/k,S} = \prod_{\mathfrak{q} \in S \setminus S'} (1 - \sigma_{\mathfrak{q},K^+}^{-1}) \eta_{K^+/k,S'}$.

Proof. It follows easily from (4) and Proposition 2.6(iii) that the product $\prod_{\mathfrak{q}} (1 - \sigma_{\mathfrak{q},K^+}^{-1}) \eta_{K^+/k,S'}$ is a solution of $\mathrm{RSC}(K^+/k, S; \mathbb{Q})$. The result follows since $\mathbb{Z}_{(p)}\Lambda_{0,S'}$ is a $\mathbb{Z}\bar{G}$-submodule of $\mathbb{Z}_{(p)}\Lambda_{0,S}$. ∎

PROPOSITION 5.4. *If $K \supset \mu_{p^{n+1}}$ for some $n \geq 0$ and $S \supset S' \supset S^1$ then* $\mathrm{CC}(K/k, S', p, n)$ *implies* $\mathrm{CC}(K/k, S, p, n)$.

Proof. We assume that $\mathrm{CC}(K/k, S', p, n)$ holds so also $\mathrm{IC}(K/k, S', p)$ and $\mathrm{RSC}(K^+/k, S'; \mathbb{Z}_{(p)})$. Thus $\mathrm{IC}(K/k, S, p)$ and $\mathrm{RSC}(K^+/k, S; \mathbb{Z}_{(p)})$ hold by Propositions 5.1 and 5.3. Using the latter and Proposition 2.12(i) we find that, for any $\theta \in \bigwedge_{\mathbb{Z}_pG}^d U^1(K_p)^-$,

$$(28)\qquad \begin{aligned} &\kappa_n(\tau_1 \ldots \tau_d) H_{K/k,n}(\eta_{K^+/k,S}, \theta) \\ &\quad = \prod_{\mathfrak{q} \in S \setminus S'} (1 - \bar{\kappa}_n^*(\sigma_{\mathfrak{q},K^+}^{-1})) \kappa_n(\tau_1 \ldots \tau_d) H_{K/k,n}(\eta_{K^+/k,S'}, \theta) \\ &\quad = \prod_{\mathfrak{q} \in S \setminus S'} (1 - \bar{\kappa}_n^*(\sigma_{\mathfrak{q},K^+}^{-1})) \overline{\mathfrak{s}_{K/k,S'}(\theta)} \quad \text{in } (\mathbb{Z}/p^{n+1}\mathbb{Z})G^-. \end{aligned}$$

For each $\mathfrak{q} \in S \setminus S'$, equation (19) with $g = \sigma_{\mathfrak{q}}^{-1} = \sigma_{\mathfrak{q},K}^{-1}$ gives $\bar{\kappa}_n^*(\sigma_{\mathfrak{q},K^+}^{-1}) = e^-\kappa_n(\sigma_{\mathfrak{q}})^{-1}\sigma_{\mathfrak{q}}$, and since $\mathfrak{q} \nmid p$ it follows that $\kappa_n(\sigma_{\mathfrak{q}}) = \overline{N\mathfrak{q}}$ in $\mathbb{Z}/p^{n+1}\mathbb{Z}$. Thus $1 - \bar{\kappa}_n^*(\sigma_{\mathfrak{q},K^+}^{-1})$ acts as $1 - N\mathfrak{q}^{-1}\sigma_{\mathfrak{q}}$ on $(\mathbb{Z}/p^{n+1}\mathbb{Z})G^-$ and combining (28) with (23) gives (24), as required. ∎

Now suppose that F is any CM subfield of K containing k. Then p, F and S satisfy the standard hypotheses. We write G_F for $\mathrm{Gal}(F/k)$ and $N_{K/F}$

for the norm map $K_p \to F_p$. (If we identify K_p with $\prod_{\mathfrak{P}|p} K_{\mathfrak{P}}$ and F_p with $\prod_{\mathfrak{p}|p} F_{\mathfrak{p}}$, then $N_{K/F}$ sends $(x_{\mathfrak{P}})_{\mathfrak{P}}$ to $(y_{\mathfrak{p}})_{\mathfrak{p}}$, where $y_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} N_{K_{\mathfrak{P}}/F_{\mathfrak{p}}} x_{\mathfrak{P}}$.) We shall also write $N_{K/F}$ for the $\mathbb{Z}_p$-linear map $\bigwedge^d_{\mathbb{Z}_pG} U^1(K_p) \to \bigwedge^d_{\mathbb{Z}_pG_F} U^1(F_p)$ sending $u_1 \wedge \cdots \wedge u_d$ to $N_{K/F}u_1 \wedge \cdots \wedge N_{K/F}u_d$. One checks easily that $\pi_{K/F} \circ R^{(j)}_{K/k,p} = R^{(j)}_{F/k,p} \circ N_{K/F}$ and also that $\pi_{K/F} \circ \Theta_{K/k,S} = \Theta_{F/k,S}$ (as meromorphic functions $\mathbb{C} \to \mathbb{C}G_F$) so that $\pi_{K/F}(a^-_{K/k,S}) = a^-_{F/k,S}$. We deduce easily

PROPOSITION 5.5. *If $K \supset F \supset k$ are as above then $\pi_{K/F} \circ \mathfrak{s}_{K/k,S} = \mathfrak{s}_{F/k,S} \circ N_{K/F}$. In particular, if $N_{K/F} : \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)^- \to \bigwedge^d_{\mathbb{Z}_pG_F} U^1(F_p)^-$ is surjective then $\pi_{K/F}(\mathfrak{S}_{K/k,S}) = \mathfrak{S}_{F/k,S}$, so the conjecture* IC$(K/k,S,p)$ *implies* IC$(F/k,S,p)$. ∎

REMARK 5.6. The surjectivity condition i s certainly satisfied whenever $N_{K/F}(U^1(K_p)) = U^1(F_p)$, which in turn holds iff K/F is at most tamely ramified at each prime in $S_p(F)$ (by local class field theory). Of course, it actually suffices that $N_{K/F}(U^1(K_p)^-) = U^1(F_p)^-$, which can be shown to be equivalent to the following statement: *K/F^+ is at most tamely ramified at each prime in $S_p(F^+)$ which splits in F.* Also, it is not hard to see that $\nu_{K/F} \circ \mathfrak{s}_{F/k,S} = [K : F]^{1-d}\mathfrak{s}_{K/k,S} \circ i_{K/F}$ where $i_{K/F}$ is the natural map $\bigwedge^d_{\mathbb{Z}_pG_F} U^1(F_p)^- \to \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)^-$, but for present purposes this is only helpful when $p \nmid [K : F]$ or $d = 1$.

Let $\bar{G}_F = \mathrm{Gal}(F^+/k)$. The norm N_{K^+/F^+} maps $U_S(K^+)$ into $U_S(F^+)$. The symbol "N_{K^+/F^+}" will denote both the map $1 \otimes N_{K^+/F^+} : \mathbb{Q}U_S(K^+) \to \mathbb{Q}U_S(F^+)$ and the $\mathbb{Q}$-linear map $\bigwedge^d_{\mathbb{Q}\bar{G}} \mathbb{Q}U_S(K^+) \to \bigwedge^d_{\mathbb{Q}\bar{G}_F} \mathbb{Q}U_S(F^+)$ sending $x_1 \wedge \cdots \wedge x_d$ to $N_{K^+/F^+}x_1 \wedge \cdots \wedge N_{K^+/F^+}x_d$.

PROPOSITION 5.7. *Suppose $K \supset F \supset k$ as above and* RSC$(K^+/k,S;\mathbb{Q})$ *holds with solution $\eta_{K^+/k,S}$. Then* RSC$(F^+/k,S;\mathbb{Q})$ *holds with solution $\eta_{F^+/k,S} = N_{K^+/F^+}\eta_{K^+/k,S}$.*

Proof. $\pi_{K^+/F^+}(N_{D_{\mathfrak{q}}(K^+/k)})$ is a $\mathbb{Z}$-multiple of $N_{D_{\mathfrak{q}}(F^+/k)}$ for all $\mathfrak{q} \in S \setminus S_\infty$. From this it follows easily that the form (iii) of the eigenspace condition on $\eta_{K^+/k,S}$ (with respect to $(S,d,\bar{G})$) implies the same on $N_{K^+/F^+}\eta_{K^+/k,S}$ (with respect to $(S,d,\bar{G}_F)$). Similarly, since $\pi_{K^+/F^+} \circ \Theta_{K^+/k,S} = \Theta_{F^+/k,S}$ and $\pi_{K^+/F^+} \circ R_{K^+/k} = R_{F^+/k} \circ N_{K^+/F^+}$, if we apply π_{K^+/F^+} to condition (15) for $\eta_{K^+/k,S}$ then we get the equivalent condition on $N_{K^+/F^+}\eta_{K^+/k,S}$. ∎

Before attacking the Congruence Conjecture in this context, we need two lemmas.

LEMMA 5.8. *If $d = 1$ then $N_{K^+/F^+}(\Lambda_{0,S}(K^+/k)) \subset \Lambda_{0,S}(F^+/k)$. If $d > 1$, then $N_{K^+/F^+}(\Lambda_{0,S}(K^+/k))$ is contained in $e^{-d}\Lambda_{0,S}(F^+/k)$ where $e = \exp((U_S(K^+)/U_S(F^+))_{\mathrm{tor}}) = 1$ or 2.*

Proof. The first statement follows from that of Proposition 2.5. Next, by sending $[\varepsilon]$ to the map $g \mapsto g(\varepsilon)/\varepsilon$, we see that $(U_S(K^+)/U_S(F^+))_{\mathrm{tor}}$ injects into

$$\mathrm{Hom}(\mathrm{Gal}(K^+/F^+), \mu(K^+)) = \mathrm{Hom}(\mathrm{Gal}(K^+/F^+), \{\pm 1\})$$

so $e = 1$ or 2. Let $(U_S(K^+)/U_S(F^+))_{\mathrm{tor}} = V/U_S(F^+)$ where $U_S(K^+) \supset V \supset U_S(F^+)$. Since $U_S(K^+)/V$ is torsion-free, $U_S(K^+)$ splits over $\mathbb{Z}$ as $V \oplus V'$. The sum $U_S(F^+) + V'$ is also direct and contains $U_S(K^+)^e$. Therefore, any $f_1, \ldots, f_d$ lying in $\mathrm{Hom}_{\mathbb{Z}}(U_S(F^+), \mathbb{Z})$ (considered as a subset of $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}U_S(F^+), \mathbb{Q})$) extend to $\hat{f}_1, \ldots, \hat{f}_d$ in $\mathrm{Hom}_{\mathbb{Z}}(U_S(F^+) + V', \mathbb{Z})$ considered as a subset of $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}U_S(K^+), \mathbb{Q})$ and $e\hat{f}_i \in \mathrm{Hom}_{\mathbb{Z}}(U_S(K^+), \mathbb{Z})$ for all i. It is easy to see from the definitions that

$$\pi_{K^+/F^+}(\varDelta_{\hat{f}_1,\ldots,\hat{f}_d}(\eta)) = \varDelta_{f_1,\ldots,f_d}(N_{K^+/F^+}\eta) \quad \text{for all } \eta \in \textstyle\bigwedge^d_{\mathbb{Q}\bar{G}} \mathbb{Q}U_S(K^+). \tag{29}$$

Hence, if $\eta \in \varLambda_{0,S}(K^+/k)$ then

$$\varDelta_{f_1,\ldots,f_d}(e^d N_{K^+/F^+}\eta) = \pi_{K^+/F^+}(\varDelta_{e\hat{f}_1,\ldots,e\hat{f}_d}(\eta))$$

lies in $\mathbb{Z}\bar{G}_F$. Letting the f_i vary shows that $N_{K^+/F^+}\eta$ lies in $e^{-d}\varLambda_{0,S}(F^+/k)$. ∎

The proof shows that $e = 1$ if, for instance, $|\mathrm{Gal}(K^+/F^+)| = [K : F]$ is odd. *Suppose now that* $\mu_{p^{n+1}} \subset F$ *for some* $n \geq 0$ and that $\mathfrak{P} \in S_p(K)$ lies above $\mathfrak{p} \in S_p(F)$, so we may regard $F_{\mathfrak{p}}$ as a subfield of $K_{\mathfrak{P}}$. Basic properties of the Hilbert symbol show that $(a, b)_{K_{\mathfrak{P}}, p^{n+1}} = (a, N_{K_{\mathfrak{P}}/F_{\mathfrak{p}}} b)_{F_{\mathfrak{p}}, p^{n+1}}$ for all $a \in F_{\mathfrak{p}}^\times$ and $b \in K_{\mathfrak{P}}^\times$. Regarding F as a subset of K_p, we easily see that

$$[\alpha, \beta]_{K,n} = [\alpha, N_{K/F}\beta]_{F,n} \quad \text{for all } \alpha \in F^\times \text{ and } \beta \in K_p^\times. \tag{30}$$

Lemma 5.9. *Let* $\eta \in \mathbb{Z}_{(p)}\varLambda_{0,S}(K^+/k)$ *and* $\theta \in \bigwedge^d_{\mathbb{Z}_p G} U^1(K_p)$. *Then* $N_{K^+/F^+}\eta$ *lies in* $\mathbb{Z}_{(p)}\varLambda_{0,S}(F^+/k)$ *and*

$$\pi_{K/F}(H_{K/k,n}(\eta, \theta)) = H_{F/k,n}(N_{K^+/F^+}\eta, N_{K/F}\theta).$$

Proof. By $\mathbb{Z}_{(p)}$-linearity in η and the fact that $p \neq 2$, we may assume $\eta \in e\varLambda_{0,S}(K^+/k)$ with e as in Lemma 5.8. The latter then shows that $N_{K^+/F^+}(\eta)$ lies in $\varLambda_{0,S}(F^+/k) \subset \mathbb{Z}_{(p)}\varLambda_{0,S}(F^+/k)$. Similarly, we may assume that $\theta = u_1 \wedge \cdots \wedge u_d$ with $u_i \in U^1(K_p)^-$ for all i. We let f_i be the map $[\,\cdot\,, u_i]_{K,n} \in \mathrm{Hom}_{\mathbb{Z}}(U_S(K^+), \mathbb{Z}/p^{n+1}\mathbb{Z})$ and choose a lift $\tilde{f}_i \in \mathrm{Hom}_{\mathbb{Z}}(U_S(K^+), \mathbb{Z})$ for each i. If $\tilde{g}_i$ denotes the restriction of $\tilde{f}_i$ to $U_S(F^+)$ then (30) says that $\tilde{g}_i$ lifts the map $g_i := [\,\cdot\,, N_{K/F}u_i]_{F,n} \in \mathrm{Hom}_{\mathbb{Z}}(U_S(F^+), \mathbb{Z}/p^{n+1}\mathbb{Z})$. Just as for (29) we find $\pi_{K^+/F^+}(\varDelta_{\tilde{f}_1,\ldots,\tilde{f}_d}(\eta)) = \varDelta_{\tilde{g}_1,\ldots,\tilde{g}_d}(N_{K^+/F^+}\eta)$, and since both sides lie in $\mathbb{Z}G_F$, we can reduce modulo p^{n+1} to get $\pi_{K^+/F^+}(\tilde{\varDelta}_{f_1,\ldots,f_d}(\eta)) = \tilde{\varDelta}_{g_1,\ldots,g_d}(N_{K^+/F^+}\eta)$. We conclude by applying $2^d\bar{\kappa}^*_{F,n}$ to both sides and using $\bar{\kappa}^*_{F,n} \circ \pi_{K^+/F^+} = \pi_{K/F} \circ \bar{\kappa}^*_{K,n}$. ∎

PROPOSITION 5.10. *Suppose* $K \supset F \supset k$ *as above and that* $N_{K/F}: \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)^- \to \bigwedge^d_{\mathbb{Z}_pG} U^1(F_p)^-$ *is surjective. If* $F \supset \mu_{p^{n+1}}$ *for some* $n \geq 0$ *then* $\mathrm{CC}(K/k, S, p, n)$ *implies* $\mathrm{CC}(F/k, S, p, n)$.

Proof. We assume that $\mathrm{CC}(K/k, S, p, n)$ holds, so also $\mathrm{IC}(F/k, S, p)$ holds and $\mathrm{RSC}(F^+/k, S; \mathbb{Z}_{(p)})$ holds with solution $\eta_{K^+/k,S}$, say. Proposition 5.5 implies $\mathrm{IC}(F/k, S, p)$. Moreover, Proposition 5.7 and Lemma 5.9 imply $\mathrm{RSC}(F^+/k, S; \mathbb{Z}_{(p)})$ and that for any $\theta \in \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)^-$ we have

$$\begin{aligned}
&\kappa_n(\tau_1 \ldots \tau_d) H_{F/k,n}(\eta_{F^+/k,S}, N_{K/F}\theta) \\
&\qquad = \kappa_n(\tau_1 \ldots \tau_d) H_{F/k,n}(N_{K^+/F^+}\eta_{K^+/k,S}, N_{K/F}\theta) \\
&\qquad = \pi_{K/F}(\kappa_n(\tau_1 \ldots \tau_d) H_{K/k,n}(\eta_{K^+/k,S}, \theta)) \\
&\qquad = \pi_{K/F}(\overline{\mathfrak{s}_{K/k,S}(\theta)}) = \overline{\mathfrak{s}_{F/k,S}(N_{K/F}\theta)}.
\end{aligned}$$

The result now follows from the surjectivity condition. ∎

Finally, if $n \geq n' \geq 0$ then $H_{K,n}(\eta, \theta) \equiv H_{K,n'}(\eta, \theta) \pmod{p^{n'+1}}$ for all $\eta \in \mathbb{Z}_{(p)}\Lambda_{0,S}(K^+/k)$ and $\theta \in \bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)^-$. (The proof is an exercise using the definitions of the Hilbert symbol, $[\cdot,\cdot]_{K,n}$, $\tilde{\Delta}$, $H_{k,n}$, κ_n etc. and the fact that $\zeta_n^{p^{n-n'}} = \zeta_{n'}$!) One deduces easily

PROPOSITION 5.11. *If* $K \supset \mu_{p^{n+1}}$ *for some* $n \geq 0$ *then* $\mathrm{CC}(K/k, S, p, n)$ *implies* $\mathrm{CC}(K/k, S, p, n')$ *for all* n' *with* $n \geq n' \geq 0$. ∎

6. The case $p \nmid |G|$. Let $\mathcal{X}_{\mathbb{Q}_p}$ denote the set of irreducible $\mathbb{Q}_p$-valued characters of G which is in natural bijection with $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$-conjugacy classes of absolutely irreducible characters $\phi \in \mathrm{Hom}(G, \bar{\mathbb{Q}}_p^\times)$. (Precisely, if Φ lies in $\mathcal{X}_{\mathbb{Q}_p}$ then its idempotent $e_\Phi \in \mathbb{Q}_pG$ splits in $\bar{\mathbb{Q}}_pG$ as the sum of the idempotents e_ϕ where ϕ runs once through the conjugacy class corresponding to Φ.) We shall say that the characters ϕ in this conjugacy class *belong* to Φ and we shall call Φ *odd* if one—hence any—such ϕ is odd (i.e. $\phi(c) = -1$). Henceforth we set $\mathfrak{a} := \mathbb{Z}_pG$ and $\mathfrak{a}_\Phi := e_\Phi\mathbb{Z}_pG$. Any ϕ belonging to Φ extends $\mathbb{Q}_p$-linearly to a homomorphism $\mathbb{Q}_pG \to F_\phi := \mathbb{Q}_p(\phi)$, which in turn restricts to *iso*morphisms from $e_\Phi\mathbb{Q}_pG$ to F_ϕ and from $\mathfrak{a}_\Phi$ to $\mathcal{O}_\phi := \mathbb{Z}_p[\phi]$, the ring of valuation integers of F_ϕ. In particular, $\mathfrak{a}_\Phi$ is a complete d.v.r., hence a p.i.d.

For the rest of this section we suppose that *the prime p does not divide* $|G|$. This means that the idempotent e_Φ lies in $\mathbb{Z}_pG$ for each $\Phi \in \mathcal{X}_{\mathbb{Q}_p}$ so that $\mathfrak{a}$ is a product $\prod_{\Phi \in \mathcal{X}_{\mathbb{Q}_p}} \mathfrak{a}_\Phi$. Any $\mathfrak{a}$-module M splits as a corresponding direct sum $\bigoplus_{\Phi \in \mathcal{X}_{\mathbb{Q}_p}} M_\Phi$, where M_Φ denotes the $\mathfrak{a}_\Phi$-module $e_\Phi M$, and $M \mapsto M_\Phi$ is an exact functor. Since any ϕ belonging to Φ has order prime to p, a uniformiser of $\mathcal{O}_\phi$—hence of $\mathfrak{a}_\Phi$—is given by p. The $\mathfrak{a}_\Phi$-*order ideal* $[N]_{\mathfrak{a}_\Phi}$ of any finite (= finite length) $\mathfrak{a}_\Phi$-module N is therefore $p^l\mathfrak{a}_\Phi$ where l is the length of any $\mathfrak{a}_\Phi$-composition series for N. We shall assume the usual properties of the order ideal, such as multiplicativity in exact sequences. Each p-adic-valued character $\phi \in \mathrm{Hom}(G, \bar{\mathbb{Q}}_p^\times)$ corresponds to a unique complex character $\chi \in \hat{G}$ such that $\phi = j \circ \chi$ where j is the fixed embedding $\bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_p$. We write $\hat{\chi}$ and $\hat{\phi} = j \circ \hat{\chi}$ respectively for the associated complex and p-adic *primitive* ray-class characters, $\mathfrak{f}_\phi$ for $\mathfrak{f}_\chi$ and K^ϕ for the field $K^{\ker(\phi)} = K^{\ker(\chi)}$ cut out by ϕ, so that χ and ϕ factor through $G_\phi := \mathrm{Gal}(K^\phi/k)$. Work of Siegel [Si] and Klingen (see also Shintani [Sh, Cor. to Thm. 1]) implies that $\Theta_{K^\phi/k,S_\infty}(0)$ lies in $\mathbb{Q}G_\phi$ so that $L(0,\hat{\chi}^{-1}) = \chi(\Theta_{K^\phi/k,S^0(K^\phi/k)}(0))$ lies in $\mathbb{Q}(\chi)$. Thus $j(L(0,\hat{\chi}^{-1})) = \phi(\Theta_{K^\phi/k,S^0(K^\phi/k)}(0))$ lies in F_ϕ and is independent of j so, by a slight abuse of notation, we write it simply as $L(0,\hat{\phi}^{-1})$.

THEOREM 6.1. *If $p \nmid |G|$ then, for any odd $\Phi \in \mathcal{X}_{\mathbb{Q}_p}$ and $\phi \in \mathrm{Hom}(G, \bar{\mathbb{Q}}_p^\times)$ belonging to Φ, we have*

$$\phi(\mathfrak{S}_{K/k,S}) = \phi([(U^1(K_p)_{\mathrm{tor}})_\Phi]_{\mathfrak{a}_\Phi}) \prod_{\substack{\mathfrak{q}\in S\setminus S_\infty \\ \mathfrak{q}\nmid p\mathfrak{f}_\phi}} (1 - N\mathfrak{q}^{-1}\hat{\phi}([\mathfrak{q}]))L(0,\hat{\phi}^{-1}) \tag{31}$$

(an equality of fractional ideals of F_ϕ) where $L(0,\hat{\phi}^{-1})$ is as defined above.

Equation (31) for each Φ clearly determines $\mathfrak{S}_{K/k,S}$. Before giving the proof, we reformulate it and deduce some consequences. Firstly, $U^1(K_p)_{\mathrm{tor}}$ is nothing but $\mu_{p^\infty}(K_p) = \prod_{\mathfrak{P}|p} \mu_{p^\infty}(K_\mathfrak{P})$. Next, for given ϕ as above we define a $\mathbb{Z}_pG_\phi$-submodule of $\mathbb{Q}_pG_\phi$ by

$$J_\phi := \mathrm{ann}_{\mathbb{Z}_pG_\phi}(\mu_{p^\infty}(K^\phi))\Theta_{K^\phi/k,S^0(K^\phi/k)}(0).$$

Since $p \nmid [K : K^\phi]$, we have

$$\begin{aligned}
\phi(\nu_{K/K^\phi}(J_\phi)) &= \phi(\mathrm{ann}_\mathfrak{a}(\mu_{p^\infty}(K^\phi))\nu_{K/K^\phi}(\Theta_{K^\phi/k,S^0(K^\phi/k)}(0))) \\
&= \phi(\mathrm{ann}_\mathfrak{a}(\mu_{p^\infty}(K^\phi)))[K : K^\phi]L(0,\hat{\phi}^{-1}) \\
&= \phi(\mathrm{ann}_{\mathfrak{a}_\Phi}(\mu_{p^\infty}(K^\phi)_\Phi))L(0,\hat{\phi}^{-1}) \\
&= \phi(\mathrm{ann}_{\mathfrak{a}_\Phi}(\mu_{p^\infty}(K)_\Phi))L(0,\hat{\phi}^{-1}) \\
&= \phi([\mu_{p^\infty}(K)_\Phi]_{\mathfrak{a}_\Phi})L(0,\hat{\phi}^{-1})
\end{aligned}$$

(the last equation because $\mu_{p^\infty}(K^\phi)_\Phi$ is cyclic over $\mathbb{Z}$, so over $\mathfrak{a}_\Phi$). Thus we may reformulate (31) as

$$\begin{aligned}
\phi(\mathfrak{S}_{K/k,S}) &= \phi([(\mu_{p^\infty}(K_p)/\mu_{p^\infty}(K))_\Phi]_{\mathfrak{a}_\Phi}) \\
&\quad \times \prod_{\substack{\mathfrak{q}\in S\setminus S_\infty \\ \mathfrak{q}\nmid p\mathfrak{f}_\phi}} (1 - N\mathfrak{q}^{-1}\hat{\phi}([\mathfrak{q}]))\phi(\nu_{K/K^\phi}(J_\phi)).
\end{aligned} \tag{32}$$

But J_ϕ is spanned over $\mathbb{Z}_p$ by $\mathrm{ann}_{\mathbb{Z}G_\phi}(\mu(K^\phi))\Theta_{K^\phi/k,S^0(K^\phi/k)}(0)$, which lies in $\mathbb{Z}G_\phi$ by the well-known result of Deligne–Ribet and (independently)

P. Cassou-Noguès (see Théorème 6.1 of [Ta, p. 107]). Hence $J_\phi \subset \mathbb{Z}_p G_\phi$ and so (32) implies that $\phi(\mathfrak{S}_{K/k,S}) \subset \mathcal{O}_\phi$ for all odd $\phi \in \mathrm{Hom}(G, \bar{\mathbb{Q}}_p^\times)$. Consequently,

Corollary 6.2. *If* $p \nmid |G|$ *then* $\mathrm{IC}(K/k,S,p)$ *holds.*

Remark 6.3. We explain the relation between Jones' formula (26) and our Theorem 6.1, recast as equation (32) for all odd ϕ: The ray-class group $\mathrm{Cl}_{\mathfrak{m}}(K)$ appearing in (26) fits into an exact sequence of $\mathbb{Z}G$-modules:

$$0 \to \overline{\mathcal{O}_K^\times} \to \prod_{\mathfrak{q} \in S^1 \setminus S_\infty} \prod_{\mathfrak{Q} | \mathfrak{q}} (\mathcal{O}_K/\mathfrak{Q})^\times \to \mathrm{Cl}_{\mathfrak{m}}(K) \to \mathrm{Cl}(K) \to 0$$

(where the first non-zero term is simply the image of $\mathcal{O}_K^\times$ in the second). Now tensor this sequence with $\mathbb{Z}_p$ and take minus parts. Using the fact that $(\mathcal{O}_K^\times \otimes \mathbb{Z}_p)^- = \mu_{p^\infty}(K)$ and isomorphisms similar to (27) one finds with a little work that (26) is equivalent to the following for each odd ϕ as in Theorem 6.1:

$$\phi(\mathfrak{S}_{K/k,S^1}) = \phi([(\mu_{p^\infty}(K_p)/\mu_{p^\infty}(K))_\Phi]_{\mathfrak{a}_\Phi}) \times \prod_{\substack{\mathfrak{q} \in S^1 \setminus S_\infty \\ \mathfrak{q} \nmid p\mathfrak{f}_\phi}} (1 - N\mathfrak{q}^{-1} \hat{\phi}([\mathfrak{q}])) \phi([(\mathrm{Cl}(K) \otimes \mathbb{Z}_p)_\Phi]_{\mathfrak{a}_\Phi}).$$

Since $p \nmid [K : K^\phi]$, one sees that this in turn is equivalent to our (32) (with $S = S^1$) *if and only if* $\phi(J_\phi) = \phi([(\mathrm{Cl}(K^\phi) \otimes \mathbb{Z}_p)_\Phi]_{\mathfrak{a}_\Phi})$ (where Φ and ϕ are now considered as odd characters of G_ϕ). But Theorem 3 of [Wi] establishes the latter equality subject to a rather mild condition ("$S_{\phi,p} = 0$") on the character ϕ.

Proof of Theorem 6.1. For each $i = 1, \ldots, d$, we write $\mathfrak{p}_i$ for $\mathfrak{P}_i \cap k$ (the prime ideal in $S_p(k)$ which is defined by the embedding $j\tau_i : \bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_p$). The map $\{1, \ldots, d\} \to S_p(k)$ sending i to $\mathfrak{p}_i$ is clearly surjective so for any $\mathfrak{p} \in S_p(k)$ we write $I(\mathfrak{p})$ for its fibre over $\mathfrak{p}$ and choose an element $i(\mathfrak{p}) \in I(\mathfrak{p})$. Thus $\mathfrak{P}_{i(\mathfrak{p})} \cap k = \mathfrak{p}_{i(\mathfrak{p})} = \mathfrak{p}$ for all $\mathfrak{p} \in S_p(k)$, and the extension $K_{\mathfrak{P}_{i(\mathfrak{p})}}/k_{\mathfrak{p}}$ is Galois with group $D_{\mathfrak{p}}(K/k)$ of order prime to p. It follows (e.g. by a theorem of E. Noether, since $K_{\mathfrak{P}_{i(\mathfrak{p})}}/k_{\mathfrak{p}}$ is tame) that we may choose an element $b_{\mathfrak{p}} \in \mathcal{O}_{K_{\mathfrak{P}_{i(\mathfrak{p})}}}$ freely generating $\mathcal{O}_{K_{\mathfrak{P}_{i(\mathfrak{p})}}}$ over $\mathcal{O}_{k_{\mathfrak{p}}} D_{\mathfrak{p}}(K/k)$. Let b be the element of $\mathcal{O}_{K_p} := \prod_{\mathfrak{P} \in S_p(K)} \mathcal{O}_{K_{\mathfrak{P}}}$ whose component in $\mathcal{O}_{K_{\mathfrak{P}}}$ is $b_{\mathfrak{p}}$ whenever $\mathfrak{P} = \mathfrak{P}_{i(\mathfrak{p})}$ for some $\mathfrak{p} \in S_p(k)$ and is 0 otherwise. Then b is a free generator for $\mathcal{O}_{K_p}$ over $\mathcal{O}_{k_p} G$, where $\mathcal{O}_{k_p}$ denotes the ring $\prod_{\mathfrak{p} \in S_p(k)} \mathcal{O}_{k_{\mathfrak{p}}}$, which we identify with $\mathcal{O}_k \otimes_{\mathbb{Z}} \mathbb{Z}_p$. So if $c_1, \ldots, c_d$ is a $\mathbb{Z}$-basis of $\mathcal{O}_k$ then $c_1 \otimes 1, \ldots, c_d \otimes 1$ is a $\mathbb{Z}_p$-basis of $\mathcal{O}_{k_p}$ and $a_1 := b(c_1 \otimes 1), \ldots, a_d := b(c_d \otimes 1)$ is a free basis for $\mathcal{O}_{K_p}$ over $\mathbb{Z}_p G = \mathfrak{a}$.

For any $\mathfrak{P} \in S_p(K)$ let $\hat{\mathfrak{P}}$ and $e_{\mathfrak{P}}$ denote respectively the maximal ideal and the ramification index of $K_{\mathfrak{P}}/\mathbb{Q}_p$. Clearly, $e_{\mathfrak{P}}$ depends only on $\mathfrak{p}$, the prime lying below $\mathfrak{P}$ in K. The exponential series converges on $p\mathcal{O}_{K_\mathfrak{P}} = \hat{\mathfrak{P}}^{e_\mathfrak{P}}$ for each $\mathfrak{P} \in S_p(K)$ and defines a $\mathbb{Z}_p D_\mathfrak{p}(K/k)$-isomorphism to $U^{e_\mathfrak{P}}(K_\mathfrak{P})$. To shorten notation, we write U^1 for $U^1(K_p)$ and $U^{\underline{e}}$ for $\prod_{\mathfrak{P}\in S_p(K)} U^{e_\mathfrak{P}}(K_\mathfrak{P}) \subset U^1$. It follows from the above that the map $\mathrm{Exp}_p = \prod_{\mathfrak{P}\in S_p(K)} \exp_p : p\mathcal{O}_{K_p} \to U^{\underline{e}}$ is an $\mathfrak{a}$-isomorphism and hence that $U^{\underline{e}}$ is free over $\mathfrak{a}$ with basis $w_1 := \mathrm{Exp}_p(pa_1), \dots, w_d := \mathrm{Exp}_p(pa_d)$. It is also of finite index in U^1, and since $\mathfrak{a}$ is a product of the p.i.d.'s $\mathfrak{a}_\Phi$, it follows that U^1/U^1_{tor} must also be $\mathfrak{a}$-free of rank d, so, in an additive notation, we get

$$(33)\qquad U^1 = U^1_{\mathrm{tor}} \oplus \bigoplus_{i=1}^{d} \mathfrak{a} u_i \qquad \text{where } \bar{u}_1, \dots, \bar{u}_d \text{ is any free } \mathfrak{a}\text{-basis of } U^1/U^1_{\mathrm{tor}}.$$

Now let ϕ and Φ be as in the statement of the theorem and let $M \in M_d(\mathfrak{a}_\Phi)$ be the matrix representing $e_\Phi\bar{w}_1, \dots, e_\Phi\bar{w}_d$ in terms of the $\mathfrak{a}_\Phi$-basis $e_\Phi\bar{u}_1, \dots, e_\Phi\bar{u}_d$ of $(U^1/U^1_{\mathrm{tor}})_\Phi$. The determinant of M has two different interpretations. On the one hand, if we write $\overline{U^{\underline{e}}}$ for the isomorphic image of $U^{\underline{e}}$ in U^1/U^1_{tor} then the general theory of p.i.d.'s and order ideals gives

$$\det(M)\mathfrak{a}_\Phi = [(U^1/U^1_{\mathrm{tor}})_\Phi/(\overline{U^{\underline{e}}})_\Phi]_{\mathfrak{a}_\Phi} = [U^1_\Phi/U^{\underline{e}}_\Phi]_{\mathfrak{a}_\Phi}[(U^1_{\mathrm{tor}})_\Phi]^{-1}_{\mathfrak{a}_\Phi}.$$

Now, for all $\mathfrak{p} \in S_p(k)$, $\mathfrak{P} \in S_p(K)$ above $\mathfrak{p}$ and $l \geq 1$, there is a well-known $\mathbb{Z}_p D_\mathfrak{p}(K/k)$-isomorphism $U^l(K_\mathfrak{P})/U^{l+1}(K_\mathfrak{P}) \to \hat{\mathfrak{P}}^l/\hat{\mathfrak{P}}^{l+1}$ induced by $x \mapsto x - 1$. This gives an $\mathfrak{a}$-isomorphism after taking products of both sides over the $\mathfrak{P}$ above $\mathfrak{p}$. Applying e_Φ and letting $\mathfrak{p}$ and l vary, a simple argument with exact sequences shows that $U^1_\Phi/U^{\underline{e}}_\Phi$ has the same $\mathfrak{a}_\Phi$-order ideal as $\mathfrak{M}_\Phi/(p\mathcal{O}_{K_p})_\Phi$ where $\mathfrak{M}$ denotes $\prod_{\mathfrak{P}\in S_p(K)} \hat{\mathfrak{P}} \subset K_p$. Therefore

$$\begin{aligned}(34)\qquad \det(M)\mathfrak{a}_\Phi &= [\mathfrak{M}_\Phi/(p\mathcal{O}_{K_p})_\Phi]_{\mathfrak{a}_\Phi}[(U^1_{\mathrm{tor}})_\Phi]^{-1}_{\mathfrak{a}_\Phi} \\ &= [(\mathcal{O}_{K_p})_\Phi/(p\mathcal{O}_{K_p})_\Phi]_{\mathfrak{a}_\Phi}[(\mathcal{O}_{K_p})_\Phi/\mathfrak{M}_\Phi]^{-1}_{\mathfrak{a}_\Phi}[(U^1_{\mathrm{tor}})_\Phi]^{-1}_{\mathfrak{a}_\Phi} \\ &= p^d[(\mathcal{O}_{K_p})_\Phi/\mathfrak{M}_\Phi]^{-1}_{\mathfrak{a}_\Phi}[(U^1_{\mathrm{tor}})_\Phi]^{-1}_{\mathfrak{a}_\Phi}\end{aligned}$$

since $\mathcal{O}_{K_p}$ is free of rank d over $\mathfrak{a}$. On the other hand, Proposition 2.17, equation (33) and the definition of $\mathfrak{s}_{K/k,S}$ give

$$\begin{aligned}(35)\qquad \phi(\det(M))\phi(\mathfrak{S}_{K/k,S}) &= \phi(\det(M))\phi(e_\Phi\mathfrak{s}_{K/k,S}(u_1 \wedge \dots \wedge u_d)\mathfrak{a}) \\ &= \phi(\det(M)\mathfrak{s}_{K/k,S}(e_\Phi u_1 \wedge \dots \wedge e_\Phi u_d))\mathcal{O}_\phi \\ &= \phi(\mathfrak{s}_{K/k,S}(e_\Phi w_1 \wedge \dots \wedge e_\Phi w_d))\mathcal{O}_\phi \\ &= j(\chi(a^{-,*}_{K/k,S}))\phi(R^{(j)}_{K/k,p}(w_1 \wedge \dots \wedge w_d))\mathcal{O}_\phi\end{aligned}$$

where $\phi = j \circ \chi$. But tracing through the definitions we have

$$R^{(j)}_{K/k,p}(w_1 \wedge \dots \wedge w_d) = \det\Big(\sum_{g\in G} \log_p(\delta^{(j)}_i(g^{-1}\mathrm{Exp}_p(pa_t)))g\Big)_{1\leq i,t\leq d}$$

and

$$\begin{aligned}\log_p(\delta_i^{(j)}(g^{-1}\mathrm{Exp}_p(pa_t))) &= \log_p(j\tau_i \circ \iota_{\mathfrak{P}_i}\mathrm{Exp}_p(g^{-1}pa_t))\\ &= \log_p(j\tau_i \exp_p(\iota_{\mathfrak{P}_i} g^{-1}pa_t)) = \delta_i^{(j)}(g^{-1}pa_t)\\ &= p\delta_i^{(j)}(g^{-1}b)j\tau_i(c_t),\end{aligned}$$

so that

$$\begin{aligned}R^{(j)}_{K/k,p}(w_1 \wedge \cdots \wedge w_d) &= p^d \prod_{i=1}^d \Big(\sum_{g\in G} \delta_i^{(j)}(g^{-1}b)g\Big) \det\,(j\tau_i(c_t))_{1\le i,t\le d} \\ &= \pm p^d j(\sqrt{d_k}) \prod_{i=1}^d \delta_i^{(j),G}(b).\end{aligned} \tag{36}$$

Applying ϕ to (34) and (36) and combining them with (35) gives

$$\begin{aligned}\phi(\mathfrak{S}_{K/k,S}) &= \phi([(\mathcal{O}_{K_p})_\Phi/\mathfrak{M}_\Phi]_{\mathfrak{a}_\Phi})\phi([(U^1_{\mathrm{tor}})_\Phi]_{\mathfrak{a}_\Phi})\\ &\quad\times j(\sqrt{d_k}\,\chi(a^{-,*}_{K/k,S}))\prod_{i=1}^d \phi(\delta_i^{(j),G}(b)).\end{aligned} \tag{37}$$

Now fix $\mathfrak{p} \in S_p(k)$ and write $D_\mathfrak{p}$ for $D_\mathfrak{p}(K/k)$ and $T_\mathfrak{p}$ for $T_\mathfrak{p}(K/k)$. Considering $\prod_{\mathfrak{P}|\mathfrak{p}}(\mathcal{O}_{K_\mathfrak{P}}/\hat{\mathfrak{P}})$ as an $\mathfrak{a}$-submodule of $\mathcal{O}_{K_p}/\mathfrak{M}$, we have natural $\mathfrak{a}$-isomorphisms

$$\begin{aligned}\prod_{\mathfrak{P}|\mathfrak{p}}(\mathcal{O}_{K_\mathfrak{P}}/\hat{\mathfrak{P}}) &\cong \mathfrak{a} \otimes_{\mathbb{Z}_p D_\mathfrak{p}} (\mathcal{O}_{K_{\mathfrak{P}_{i(\mathfrak{p})}}}/\hat{\mathfrak{P}}_{i(\mathfrak{p})})\\ &\cong \mathfrak{a} \otimes_{\mathbb{Z}_p D_\mathfrak{p}} (\mathbb{Z}_p D_\mathfrak{p} \otimes_{\mathbb{Z}_p T_\mathfrak{p}} (\mathcal{O}_k/\mathfrak{p})) \cong \mathfrak{a} \otimes_{\mathbb{Z}_p T_\mathfrak{p}} (\mathcal{O}_k/\mathfrak{p})\end{aligned}$$

(where the action on $\mathcal{O}_k/\mathfrak{p}$ is trivial and the second isomorphism is from the normal basis theorem in the *residue field* extension of $K_{\mathfrak{P}_{i(\mathfrak{p})}}/k_\mathfrak{p}$). It follows easily that $(\prod_{\mathfrak{P}|\mathfrak{p}}(\mathcal{O}_{K_\mathfrak{P}}/\hat{\mathfrak{P}}))_\Phi$ is trivial unless $T_\mathfrak{p} \subset \ker(\phi)$ (i.e. $\mathfrak{p} \nmid \mathfrak{f}_\phi$), in which case it has order ideal $(N\mathfrak{p})\mathfrak{a}_\Phi$. Taking the product over all $\mathfrak{p} \in S_p(k)$ yields

$$\phi([(\mathcal{O}_{K_p})_\Phi/\mathfrak{M}_\Phi]_{\mathfrak{a}_\Phi}) = \Big(\prod_{\substack{\mathfrak{p}\in S_p(k)\\ \mathfrak{p}\nmid\mathfrak{f}_\phi}} N\mathfrak{p}\Big)\mathcal{O}_\phi. \tag{38}$$

Furthermore, equations (8), (2) and (3) give

$$\begin{aligned}\sqrt{d_k}\,\chi(a^{-,*}_{K/k,S}) &= \prod_{\substack{\mathfrak{q}\in S\setminus S_\infty\\ \mathfrak{q}\nmid\mathfrak{f}_\chi}} (1 - N\mathfrak{q}^{-1}\hat{\chi}([\mathfrak{q}]))\sqrt{d_k}\,(i/\pi)^d L(1,\hat{\chi})\\ &= \prod_{\substack{\mathfrak{q}\in S\setminus S_\infty\\ \mathfrak{q}\nmid\mathfrak{f}_\chi}} (1 - N\mathfrak{q}^{-1}\hat{\chi}([\mathfrak{q}]))(-1)^d\tau(\chi)^{-1}L(0,\hat{\chi}^{-1}).\end{aligned} \tag{39}$$

The second equality follows from Hecke's functional equation for the L-function. To be precise, we are using the version stated on p. 36 of [Fr], taking $s = 0$ and taking Fröhlich's complex character "$\bar{\theta}$" on $\mathrm{Id}(k)$—the idèle group of k—to be the one obtained by composing χ with the map $\mathrm{Id}(k) \to G$ coming from class-field theory. Thus $\tau(\chi)$ denotes the Gauss sum associated to this character whose definition we shall recall below.

Applying j to (39) and combining with (37) and (38) gives

$$\begin{aligned}\phi(\mathfrak{S}_{K/k,S}) &= \phi([(U^1_{\mathrm{tor}})_\Phi]_{\mathfrak{a}_\Phi}) \prod_{\substack{\mathfrak{p}\in S_p(k)\\ \mathfrak{p}\nmid \mathfrak{f}_\phi}} N\mathfrak{p} \prod_{\substack{\mathfrak{q}\in S\setminus S_\infty\\ \mathfrak{q}\nmid \mathfrak{f}_\phi}} (1 - N\mathfrak{q}^{-1}\hat{\phi}([\mathfrak{q}])) \\ &\qquad \times L(0,\hat{\phi}^{-1}) j(\tau(\chi))^{-1} \prod_{i=1}^{d} \phi(\delta_i^{(j),G}(b)) \\ &= \phi([(U^1_{\mathrm{tor}})_\Phi]_{\mathfrak{a}_\Phi}) \prod_{\substack{\mathfrak{q}\in S\setminus S_\infty\\ \mathfrak{q}\nmid p\mathfrak{f}_\phi}} (1 - N\mathfrak{q}^{-1}\hat{\phi}([\mathfrak{q}])) \\ &\qquad \times L(0,\hat{\phi}^{-1}) j(\tau(\chi))^{-1} \prod_{i=1}^{d} \phi(\delta_i^{(j),G}(b))\end{aligned}$$

where we have used the facts that every prime ideal $\mathfrak{p}$ in $S_p(k)$ is contained in S and that if, in addition, it does not divide $\mathfrak{f}_\phi$ then $N\mathfrak{p}(1-N\mathfrak{p}^{-1}\hat{\phi}([\mathfrak{q}])) = (N\mathfrak{p} - \hat{\phi}([\mathfrak{q}]))$ lies in $\mathcal{O}_\phi^\times$.

The argument so far shows that $j(\tau(\chi))^{-1}\prod_{i=1}^{d}\phi(\delta_i^{(j),G}(b))$ lies in F_ϕ. The theorem will follow if we can prove that it too lies in $\mathcal{O}_\phi^\times$, i.e. that

$$j(\tau(\chi)) \sim \prod_{i=1}^{d} \phi(\delta_i^{(j),G}(b))$$

where "$a \sim b$" means that $a, b \in \bar{\mathbb{Q}}_p^\times$ have the same p-adic absolute value. Recall that Fröhlich defines $\tau(\chi)$ as the product $\prod_{\mathfrak{q}\notin S_\infty}\tau(\chi_\mathfrak{q})$ where $\chi_\mathfrak{q} : k_\mathfrak{q}^\times \to \bar{\mathbb{Q}}^\times$ is the $\mathfrak{q}$-component of the complex idèle character associated to χ and $\tau(\chi_\mathfrak{q})$ is the "local Gauss sum" (which equals 1 unless $\mathfrak{q} \mid \mathfrak{f}_\chi$, so the product is finite). For definitions and basic properties of the algebraic integers $\tau(\chi_\mathfrak{q})$ see [Fr, pp. 34–35] or [Ma, II-§2]. In particular, [Fr, eq. (5.7), p. 34] shows that $j(\tau(\chi)) \sim 1$ unless $\mathfrak{q} \in S_p(k)$. Hence $j(\tau(\chi)) \sim \prod_{\mathfrak{p}\in S_p(k)} j(\tau(\chi_\mathfrak{p}))$ and since $\{1,\ldots,d\}$ is the disjoint union $\bigcup_{\mathfrak{p}\in S_p(k)} I(\mathfrak{p})$ it suffices to show that

$$j(\tau(\chi_\mathfrak{p})) \sim \prod_{i\in I(\mathfrak{p})} \phi(\delta_i^{(j),G}(b)) \quad \text{for any } \mathfrak{p} \text{ in } S_p(k). \tag{40}$$

But this is essentially (a special case of) Theorem 23 of [Fr]: Take $F := \overline{j\tau_{i(\mathfrak{p})}(k)}$, $L := \overline{j\tau_{i(\mathfrak{p})}(K)}$ as subfields of $\bar{\mathbb{Q}}_p$, isomorphic via $j\tau_{i(\mathfrak{p})}$ to $k_\mathfrak{p}$ and

$K_{\mathfrak{P}_{i(\mathfrak{p})}}$ respectively. The extension L/F is thus abelian with Galois group Γ which we identify via $j\tau_{i(\mathfrak{p})}$ with $D_{\mathfrak{p}}$. We take Fröhlich's character "χ" to be our $\chi_{\mathfrak{p}} : k_{\mathfrak{p}}^{\times} \to \bar{\mathbb{Q}}^{\times}$, which factors through the local reciprocity map $k_{\mathfrak{p}}^{\times} \to D_{\mathfrak{p}}$ and so may also be regarded as χ restricted to $D_{\mathfrak{p}} = \Gamma$. Thus Fröhlich's "$\chi^j$" may similarly be identified with our ϕ restricted to Γ. Since Γ has order prime to p, L/F is *tame* so Theorem 23 of [Fr] applies to give (with these identifications)

$$j(\tau(\chi_{\mathfrak{p}})) \sim \mathcal{N}_{F/\mathbb{Q}_p}(j\tau_{i(\mathfrak{p})}(b_{\mathfrak{p}})|\phi)$$

where the R.H.S. is the *norm resolvent* (see below) associated to the free generator $j\tau_{i(\mathfrak{p})}(b_{\mathfrak{p}})$ of $\mathcal{O}_L$ over $\mathcal{O}_F\Gamma$. Thus (40) and hence our theorem will follow from

$$\prod_{i\in I(\mathfrak{p})} \phi(\delta_i^{(j),G}(b)) \sim \mathcal{N}_{F/\mathbb{Q}_p}(j\tau_{i(\mathfrak{p})}(b_{\mathfrak{p}})|\phi). \tag{41}$$

The proof of (41) is largely a matter of unravelling our definitions and comparing with Fröhlich's, so we only sketch it. For any $i \in I(\mathfrak{p})$ we can choose $g_i \in G$ such that $g_i\mathfrak{P}_i = \mathfrak{P}_{i(\mathfrak{p})}$ and then $\sigma_i \in \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ such that $\sigma_i j\tau_{i(\mathfrak{p})}(x) = j\tau_i g_i^{-1}(x)$ for any $x \in K_{\mathfrak{P}_{i(\mathfrak{p})}}$. Then

$$\begin{aligned}\phi(\delta_i^{(j),G}(b)) &= \sum_{g\in G} j\tau_i\iota_{\mathfrak{P}_i}(g^{-1}b)\phi(g) = \sum_{h\in D_{\mathfrak{p}}} j\tau_i g_i^{-1}h^{-1}(b_{\mathfrak{p}})\phi(hg_i)\\ &= \phi(g_i)\sigma_i\Big(\sum_{\gamma\in\Gamma}\gamma^{-1}(j\tau_{i(\mathfrak{p})}(b_{\mathfrak{p}}))\sigma_i^{-1}(\phi(\gamma))\Big) \sim \sigma_i(j\tau_{i(\mathfrak{p})}(b_{\mathfrak{p}}) \,|\, \sigma_i^{-1}\circ\phi)\end{aligned}$$

where $(j\tau_{i(\mathfrak{p})}(b_{\mathfrak{p}}) \,|\, \sigma_i^{-1}\circ\phi)$ denotes the *resolvent* defined for example in [Fr, eq. (4.4), p. 29]. Equation (41) now follows on taking the product over $i \in I(\mathfrak{p})$, using the definition of the norm resolvent in [Fr, eq. (1.4), p. 107] and the fact (which the reader can easily check) that as i runs through $I(\mathfrak{p})$, σ_i runs once through a set of left coset representatives for $\mathrm{Gal}(\bar{\mathbb{Q}}_p/F)$ in $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. (Fröhlich uses right cosets because of his exponential notation for Galois action.) This completes the proof of Theorem 6.1. ∎

Some of the facts used in the above proof will also be useful in the

Proof of Proposition 4.8. Since $p\nmid|G|$, we can use (33) to show that any $\theta \in \bigwedge_{\mathbb{Z}_pG}^d U^1$ may be expressed as the sum of $xu_1\wedge\cdots\wedge u_d$ (for some $x \in \mathfrak{a}$) and finitely many terms of form $z\wedge v_2\wedge\cdots\wedge v_d$ with $z \in U^1_{\mathrm{tor}}$ and $v_i \in U^1$ for $i = 2,\ldots,d$. Since we are assuming that θ is $\mathbb{Z}_p$-torsion, so also is its image $x(\bar{u}_1\wedge\cdots\wedge\bar{u}_d)$ in $\bigwedge_{\mathbb{Z}_pG}^d(U^1/U^1_{\mathrm{tor}})$ and since $\bar{u}_1\wedge\cdots\wedge\bar{u}_d$ freely generates the latter over $\mathfrak{a}$, it follows that $x = 0$. Thus, by linearity, we may assume that $\theta = z\wedge v_2\wedge\cdots\wedge v_d$. On the other hand, $p\nmid|G|$ also implies $\mathbb{Z}_{(p)}\Lambda_{0,S} = \mathbb{Z}_{(p)}\overline{\bigwedge_{\mathbb{Z}\bar{G}}^d U_S(K^+)}$ by Proposition 2.5. If we write $\tilde{e}$ for $|\bar{G}|e_{S,d,\bar{G}} \in \mathbb{Z}\bar{G}$ then it follows from the eigenspace condition on η that it equals $|G|^{-d}(2\tilde{e})^d\eta$ and so may be written as a $\mathbb{Z}_{(p)}$-linear combination of terms of form $(1 \otimes \tilde{e}\varepsilon_1) \wedge \cdots \wedge (1 \otimes \tilde{e}\varepsilon_d)$ with $\varepsilon_i \in U_S(K^+)^2$ for all i. By $\mathbb{Z}_{(p)}$-linearity and (20), it therefore suffices to show that $[\tilde{e}\varepsilon, z]_{K,n} = 0$ for any $\varepsilon \in U_S(K^+)^2$ and any $z \in U^1_{\mathrm{tor}} = \mu_{p^\infty}(K_p)$, say $z = (z_{\mathfrak{P}})_{\mathfrak{P}}$ with $z_{\mathfrak{P}} \in \mu_{p^\infty}(K_{\mathfrak{P}})$ for each $\mathfrak{P} \in S_p(K)$. By the definitions of $[\cdot,\cdot]_{K,n}$, $[\cdot,\cdot]_{\mathfrak{P},n}$ and $(\cdot,\cdot)_{K_{\mathfrak{P}},p^{n+1}}$ this reduces further to the statement that $\sigma_{\iota_{\mathfrak{P}}(\tilde{e}\varepsilon),K_{\mathfrak{P}}}(\zeta_{\mathfrak{P}}) = \zeta_{\mathfrak{P}}$ for each $\mathfrak{P}$, where $\zeta_{\mathfrak{P}} := z_{\mathfrak{P}}^{1/p^{n+1}}$ is a p-power root of unity in $(K_{\mathfrak{P}})^{\mathrm{ab}}$. But $\zeta_{\mathfrak{P}}$ actually lies in $\mathbb{Q}_p^{\mathrm{ab}}$, so local class field theory tells us that $\sigma_{\iota_{\mathfrak{P}}(\tilde{e}\varepsilon),K_{\mathfrak{P}}}(\zeta_{\mathfrak{P}}) = \sigma_{a_{\mathfrak{P}},\mathbb{Q}_p}(\zeta_{\mathfrak{P}})$ where $a_{\mathfrak{P}} := N_{K_{\mathfrak{P}}/\mathbb{Q}_p}\iota_{\mathfrak{P}}(\tilde{e}\varepsilon) = N_{k_{\mathfrak{p}}/\mathbb{Q}_p}\iota_{\mathfrak{P}}(N_{D_{\mathfrak{p}}(K/k)}\tilde{e}\varepsilon)$ and $\mathfrak{p} \in S_p(k)$ lies below $\mathfrak{P}$. But the image of $N_{D_{\mathfrak{p}}(K/k)}$ in $\mathbb{Z}\bar{G}$ is $N_{D_{\mathfrak{p}}(K^+/k)}$ or $2N_{D_{\mathfrak{p}}(K^+/k)}$. If $|S| > d+1$ then, since $\mathfrak{p}$ lies in S, formula (13) shows that $N_{D_{\mathfrak{p}}(K^+/k)}\tilde{e} = 0$ in $\mathbb{Z}\bar{G}$, so $a_{\mathfrak{P}} = 1$ for all $\mathfrak{P}$ and the result follows. Finally, if $|S| = d+1$ then we must have $S = S_\infty(k) \cup S_p(k) = S_\infty(k) \cup \{\mathfrak{p}\}$ and (13) now implies $N_{D_{\mathfrak{p}}(K^+/k)}\tilde{e} = |D_{\mathfrak{p}}(K^+/k)|N_{\bar{G}}$. Hence $a_{\mathfrak{P}}$ is a power of $N_{k_{\mathfrak{p}}/\mathbb{Q}_p}\iota_{\mathfrak{P}}(N_{K^+/k}\varepsilon)$ which equals $\iota_{\mathfrak{P}}(N_{k/\mathbb{Q}}N_{K^+/k}\varepsilon) = N_{K^+/\mathbb{Q}}\varepsilon$ since $S_p(k) = \{\mathfrak{p}\}$. But $\varepsilon \in U_S(K^+)^2$ implies that $N_{K^+/\mathbb{Q}}\varepsilon$, hence also $a_{\mathfrak{P}}$, is a power of p and the result follows from the well-known fact that $\sigma_{p,\mathbb{Q}_p}(\zeta_{\mathfrak{P}}) = \zeta_{\mathfrak{P}}$. (Indeed, $p = N_{\mathbb{Q}_p(\zeta_{\mathfrak{P}})/\mathbb{Q}_p}(1-\zeta_{\mathfrak{P}})$ implies that $\sigma_{p,\mathbb{Q}_p}$ restricts to the identity on $\mathbb{Q}_p(\zeta_{\mathfrak{P}})$.) ∎

7. The case $k = \mathbb{Q}$. The following lemmas will be used in the proof of Theorem 4.3. Let p be an odd prime and f a positive integer. We write f as $f'p^{m+1}$ for some $m \geq -1$ and f' prime to p. We shall abbreviate $\mathbb{Q}(\xi_f)$ to K_f, $\mathrm{Gal}(\mathbb{Q}(\xi_f)/\mathbb{Q})$ to G_f and $\mathrm{Gal}(\mathbb{Q}(\xi_f)^+/\mathbb{Q})$ to $\bar{G}_f$. For any $\bar{a} \in (\mathbb{Z}/f\mathbb{Z})^\times$ we write σ_a for the element of G_f sending ξ_f to ξ_f^a.

Lemma 7.1. *Let $S = \{\infty\} \cup S_f(\mathbb{Q})$, which contains $S^0(K_f/\mathbb{Q})$. Then, with the above notations,*

(i) $$\Theta^{(1)}_{K_f^+/\mathbb{Q},S}(0) = -\frac{1}{2}\sum_{\bar{g}\in\bar{G}_f} \log|\bar{g}((1-\xi_f)(1-\xi_f^{-1}))|\bar{g}^{-1},$$

(ii) $$a^-_{K_f/\mathbb{Q},S} = e^-.\frac{1}{f}\sum_{g\in G_f} g(\xi_f/(1-\xi_f))g^{-1}.$$

Proof. For part (i), see e.g. [St, p. 203]. A rather indirect proof of the equation in (ii) uses [Sh, Prop. 1] to calculate $\Phi_{K_f/\mathbb{Q}}(0)$ as outlined in [So5, Example 3.1] and returns to $s = 1$ with (9). In principle, one can also work "χ-by-χ", calculating χ(L.H.S.) in (ii) from the usual formula for $L(1,\phi)$ when ϕ is an odd *primitive* Dirichlet character. (See e.g. [F-T, Theorem 67(b)].) However, the imprimitivity of our χ and presence of a Gauss sum in the formula make the relation to χ(R.H.S.) surprisingly difficult. We therefore sketch a direct and very elementary proof of (ii), similar in some respects to that of [F-T, Theorem 67]: Equation (2) shows that $\Theta^-_{K_f/\mathbb{Q},S}(1) = \sum_{a=1,\,(a,f)=1}^{f-1} t_a\sigma_a^{-1}$ where $t_a = \frac{1}{2}\lim_{s\to 1}(\zeta_{K_f/\mathbb{Q},S}(s,\sigma_a) - \zeta_{K_f/\mathbb{Q},S}(s,\sigma_{-a}))$ and $\zeta_{K_f/\mathbb{Q},S}(s,\sigma_a) = \sum_{n\ge 1,\, n\equiv a\,(f)} n^{-s}$ for $\mathrm{Re}(s) > 1$. For any $1 \le c \le f-1$ the function $Z(s,c) := \sum_{n\ge 1}\xi_f^{cn} n^{-s}$ converges (conditionally) to a continuous function of $s \in (0,\infty]$. For each $1 \le a \le f-1$ with $(a,f) = 1$ and any $s \in (1,\infty]$ we find easily that

$$\zeta_{K_f/\mathbb{Q},S}(s,\sigma_a) - \zeta_{K_f/\mathbb{Q},S}(s,\sigma_{-a}) = \frac{1}{f}\sum_{b=1}^{f-1}(\xi_f^{-ab} - \xi_f^{ab})Z(s,b) = \frac{1}{2f}\sum_{b=1}^{f-1}(\xi_f^{-ab} - \xi_f^{ab})(Z(s,b) - Z(s,f-b)). \tag{42}$$

But if log denotes the principal branch of logarithm, then Abel's lemma and some Euclidean geometry show that $Z(1,c) = -\log(1-\xi_f^c) = -\log|1-\xi_f^c| + i\pi(1/2 - c/f)$. So, letting $s \to 1+$ in (42), substituting for $Z(1,b)$, $Z(1,f-b)$ and using the identity

$$\sum_{b=1}^{f-1} b\xi_f^{ab} = -\frac{f}{1-\xi_f^a} \quad \text{for } (a,f) = 1,$$

we find after rearranging that

$$t_a = -\frac{i\pi}{2f}\left(\frac{\xi_f^a}{1-\xi_f^a} - \frac{\xi_f^{-a}}{1-\xi_f^{-a}}\right),$$

which implies (ii). ∎

Let us write $\hat{K}_f$ for the field $\mathbb{Q}_p(\mu_f) \subset \bar{\mathbb{Q}}_p$. The proof of Theorem 4.3 depends crucially on the following cyclotomic explicit reciprocity law due to Coleman. (The case $f' = 1$ was proved much earlier by Artin and Hasse in [A-H].)

Lemma 7.2. *Let $\hat{\xi}_f$ be any primitive fth root of unity in $\hat{K}_f$ and let $v \in U^1(\hat{K}_f)$. Then*

$$b(\hat{\xi}_f, v) := \frac{1}{f}\,\mathrm{Tr}_{\hat{K}_f/\mathbb{Q}_p}((\hat{\xi}_f/(1-\hat{\xi}_f))\log_p(v))$$

lies in $\mathbb{Z}_p$. Furthermore,

$$(1-\hat{\xi}_f, v)_{\hat{K}_f,p^{m+1}} = (\hat{\xi}_f^{f'})^{-b(\hat{\xi}_f,v)}$$

(the R.H.S. makes sense because $\hat{\xi}_f^{f'}$ is a primitive p^{m+1}th root of unity).

Proof. This follows from Corollary 15 of [Col]. We first write $\hat{\xi}_f$ uniquely as $\hat{\xi}_f = \hat{\zeta}_{p^{m+1}}\hat{\zeta}_{f'}$ where $\hat{\zeta}_{p^{m+1}}$ and $\hat{\zeta}_{f'}$ are generators respectively of $\mu_{p^{m+1}}$ and $\mu_{f'}$ in $\hat{K}_f$. We also write H for $\hat{K}_{f'}$, an unramified extension of $\mathbb{Q}_p$, and $\mathcal{O}_H$ for its ring of integers. Now $1-\hat{\xi}_f = h(u_m)$ where $h(T)$ denotes the linear polynomial $1-\hat{\zeta}_{f'}(1-T)\in\mathcal{O}_H[T]$ and $u_m := 1-\hat{\zeta}_{p^{m+1}}$. The Frobenius element φ of $\mathrm{Gal}(H/\mathbb{Q}_p)$ may be extended to an automorphism of $\mathcal{O}_H[T]$ (resp. of $H(\mu_{p^\infty})\subset\bar{\mathbb{Q}}_p$) by acting trivially on T (resp. on μ_{p^∞}). Suppose $l\ge 1$ and $l\ge i\ge 0$. Since $\varphi(\hat{\zeta}_{f'})=\hat{\zeta}_{f'}^p$, one verifies easily that

$$\varphi^{l-i}h(1-(1-T)^{p^{l-i}}) = \prod_{\hat{\zeta}\in\mu_{p^{l-i}}}(1-\hat{\zeta}_{f'}\hat{\zeta}(1-T)).$$

Substituting $T=u_l=(1-\hat{\zeta}_{p^{l+1}})$ for any generator $\hat{\zeta}_{p^{l+1}}$ of $\mu_{p^{l+1}}$, it is easy to see that the R.H.S. becomes the norm from $H(\mu_{p^{l+1}})$ to $H(\mu_{p^{l-i+1}})$ of $h(u_l)$. Thus $h(T)$ lies in the subgroup of $\mathcal{O}_H((T))^\times$ denoted $\mathcal{M}^{(l)}$ by Coleman, and this for *any* $l\ge 1$. Indeed, this follows from the equation at the foot of p. 376 of [Col] after correcting the misprint "ϕ^{n-i}" to read "ϕ^{i-n}" (which is necessary for consistency with Coleman's equation (1) on p. 377). Now we can apply Coleman's Corollary 15, p. 396, after first correcting another obvious misprint: the meaningless "$\lambda(\alpha)$" in the main equation should be replaced by $\lambda(1-\alpha)$ $(=-\log_p(\alpha))$. If we take Coleman's "n" to be our m, his "u" to be our u_m (so that his "H_n" is our $\hat{K}_f$), his "α" to be our v and his "g" to be our h (so that $\delta h(T)=(1-T)h(T)^{-1}dh(T)/dT = \hat{\zeta}_{f'}(1-T)/(1-\hat{\zeta}_{f'}(1-T)))$ then the R.H.S. of the main equation in his Corollary 15 equals $-f'b(\hat{\xi}_f,v)$. The corollary implies that this lies in $\mathbb{Z}_p$, and (taking into account Coleman's definitions of "Ind_{u_m}" and of "$(x,y)_m$", the latter agreeing with our $(y,x)_{\hat{K}_f,p^{m+1}}$) it also implies that $(1-\hat{\xi}_f,v)_{\hat{K}_f,p^{m+1}} = (1-u_m)^{-f'b(\hat{\xi}_f,v)}$, from which our lemma follows immediately. ∎

Proof of Theorem 4.3. Let K be an absolutely abelian CM field and suppose that $f=f'p^{m+1}$ is the conductor of K, i.e. the smallest positive integer such that $K\subset K_f$. Then $S_{\mathrm{ram}}(K/\mathbb{Q})=S_{\mathrm{ram}}(K_f/\mathbb{Q})=S_f(\mathbb{Q})$. Since p is odd, $\mu_{p^{n+1}}\subset K$ implies (e.g. by ramification) that $n\le m$. Therefore, if $m=-1$ then the Congruence Conjecture does not apply and $\mathrm{IC}(K/\mathbb{Q},S,p)$ follows from Theorem 4.1. So we may assume $m\ge 0$. By Propositions 5.1 and 5.4 we may further assume that $S=S^1(K/\mathbb{Q})=\{\infty\}\cup S_f(\mathbb{Q})$ (which is also equal to $S^0(K/\mathbb{Q})$ and to $S^1=S^0(K_f/\mathbb{Q})$). If $m=0$ then $K_f/\mathbb{Q}$ is tamely ramified at p. If $m\ge 1$ then (since $p\ne 2$) the ramification group $T_p(K_f/\mathbb{Q})=\mathrm{Gal}(K_f/\mathbb{Q}(\xi_{f'}))$ has a unique minimal subgroup of order p, namely $\mathrm{Gal}(K_f/\mathbb{Q}(\xi_{f/p}))$. This cannot be contained in $\mathrm{Gal}(K_f/K)$ by minimality of the conductor f. Thus, in any case, K_f/K is at most tamely ramified above p. So by Remark 5.6 it suffices to prove $\mathrm{CC}(K_f/\mathbb{Q},S^1,p,m)$ and apply Propositions 5.11 and 5.10.

We start with $\mathrm{RSC}(K_f^+/\mathbb{Q},S^1;\mathbb{Z}_{(p)})$ (see also [Ta, p. 79]). The algebraic integer $(1-\xi_f)(1-\xi_f^{-1})=(1-\xi_f)^{1+c}$ lies in K_f^+ and the norm relations for cyclotomic numbers (see for example [So1, Lemma 2.1]) show that, for any

$q \in S_f(\mathbb{Q})$, the number $N_{D_q(K_f/\mathbb{Q})}(1-\xi_f)$ equals p or 1 according as $f'=1$ or $f' \neq 1$. It follows firstly that $(1-\xi_f)^{1+c}$ lies in $U_{S^1}(K_f^+)$ (and even in $U_{S_\infty}(K_f^+)$ for $f' \neq 1$) and secondly, using Proposition 2.6, that $\eta_f := -\frac{1}{2} \otimes (1-\xi_f)^{1+c} \in \frac{1}{2}\overline{\bigwedge^1_{\mathbb{Z}\bar{G}_f} U_{S^1}(K_f^+)} = \frac{1}{2}\overline{U_{S^1}(K_f^+)}$ satisfies the eigenspace condition with respect to $(S^1, 1, \bar{G}_f)$. Moreover, $R_{K_f^+/\mathbb{Q}} = \lambda_{K_f^+/\mathbb{Q},1}$, so *taking* τ_1 *to be the identity*, Lemma 7.1(i) shows that η_f is the unique solution $\eta_{K_f^+/\mathbb{Q},S^1}$ of $\mathrm{RSC}(K_f^+/\mathbb{Q}, S^1; \mathbb{Z})$. For any $u \in \bigwedge^1_{\mathbb{Z}_pG_f} U^1(K_{f,p})^- = U^1(K_{f,p})^-$, it follows from (20) and (18) that

$$(43)\qquad \begin{aligned} H_{K_f/\mathbb{Q},m}(\eta_f, u) &= -\bar{2}^{-1} \sum_{g\in G_f} [(1-\xi_f)^{(1+c)}, gu]_{K_f,m} g^{-1} \\ &= -\bar{2}^{-1} \sum_{g\in G_f} [1-\xi_f, gu^{(1-c)}]_{K_f,m} g^{-1} \\ &= -\sum_{g\in G_f} [1-\xi_f, gu]_{K_f,m} g^{-1} \\ &= \sum_{g\in G_f} \Big(\sum_{\mathfrak{P}\in S_p(K_f)} -[1-\xi_f, \iota_{\mathfrak{P}}(gu)]_{\mathfrak{P},m} \Big) g^{-1} \end{aligned}$$

(where $1-\xi_f$ is identified with its natural images $(1-\xi_f)\otimes 1$ and $\iota_{\mathfrak{P}}(1-\xi_f)$ in K_p and $K_{\mathfrak{P}}$ respectively). Next we need to calculate the map $\mathfrak{s}_{K_f/\mathbb{Q},S^1}$. Fix a choice of $j : \bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_p$. It follows easily from the definitions of $R^{(j)}_{K_f/\mathbb{Q},p}$ and $\mathfrak{s}_{K_f/\mathbb{Q},S^1}$ and from Lemma 7.1(ii) that for any $u \in U^1(K_{f,p})^-$,

$$(44)\qquad \mathfrak{s}_{K_f/\mathbb{Q},S^1}(u) = \sum_{g\in G_f} a_g(u) g^{-1} \quad \text{where}$$
$$a_g(u) = \frac{1}{f} \sum_{h\in G_f} jh(\xi_f/(1-\xi_f)) \log_p(\delta_1^{(j)}(hgu)).$$

Let D denote $D_p(K_f/\mathbb{Q})$, identified with $\mathrm{Gal}(K_{f,\mathfrak{P}}/\mathbb{Q}_p)$ for every $\mathfrak{P} \in S_p(K_f)$. Recall that $\mathfrak{P}_1 \in S_p(K_f)$ is the ideal defined by the embedding $j = j\tau_1$, which therefore gives rise to an isomorphism (also denoted j) from $K_{f,\mathfrak{P}_1}$ to $\overline{j(K_f)} = \hat{K}_f$. This in turn induces an isomorphism from D to $\hat{D} := \mathrm{Gal}(\hat{K}_f/\mathbb{Q}_p)$ sending $d \in D$ to $\hat{d}$ say, where $jd = \hat{d}j$. For each $\mathfrak{P} \in S_p(K_f)$ we choose $h_{\mathfrak{P}} \in G_f$ such that $h_{\mathfrak{P}}(\mathfrak{P}) = \mathfrak{P}_1$ so that $h_{\mathfrak{P}}$ extends to an isomorphism from $K_{f,\mathfrak{P}}$ to $K_{f,\mathfrak{P}_1}$. Thus $G = \bigcup_{\mathfrak{P}} h_{\mathfrak{P}} D$ and for any d in D, $jh_{\mathfrak{P}}d = \hat{d}jh_{\mathfrak{P}}$ defines an isomorphism from $K_{f,\mathfrak{P}}$ to $\hat{K}_f$. It follows that if $u \in U^1(K_{f,p})^-$ and $g \in G$, then $\log_p(\delta_1^{(j)}(h_{\mathfrak{P}}dgu)) = \log_p(j\iota_{\mathfrak{P}_1}(h_{\mathfrak{P}}dgu)) =$

$\log_p(jh_{\mathfrak{P}}d\iota_{\mathfrak{P}}(gu)) = \hat{d}\log_p(jh_{\mathfrak{P}}\iota_{\mathfrak{P}}(gu))$. Consequently, we find

$$
\begin{aligned}
(45)\qquad a_g(u) &= \sum_{\mathfrak{P}\in S_p(K_f)} \frac{1}{f}\sum_{d\in D} jh_{\mathfrak{P}}d(\xi_f/(1-\xi_f))\log_p(\delta_1^{(j)}(h_{\mathfrak{P}}dgu))\\
&= \sum_{\mathfrak{P}\in S_p(K_f)} \frac{1}{f}\operatorname{Tr}_{\hat{K}_f/\mathbb{Q}_p}(jh_{\mathfrak{P}}(\xi_f/(1-\xi_f))\log_p(jh_{\mathfrak{P}}\iota_{\mathfrak{P}}(gu)))\\
&= \sum_{\mathfrak{P}\in S_p(K_f)} b(\hat{\xi}_{f,\mathfrak{P}}, v_{g,\mathfrak{P}})
\end{aligned}
$$

where, for each $\mathfrak{P} \in S_p(K_f)$, we have set $\hat{\xi}_{f,\mathfrak{P}} := jh_{\mathfrak{P}}(\xi_f)$ and $v_{g,\mathfrak{P}} := jh_{\mathfrak{P}}\iota_{\mathfrak{P}}(gu)$ and where $b(\hat{\xi}_{f,\mathfrak{P}}, v_{g,\mathfrak{P}})$ is as defined in Lemma 7.2. The first statement of this lemma therefore shows that $a_g(u) \in \mathbb{Z}_p$ for all $u \in U^1(K_{f,p})^-$ and $g \in G$, i.e. $\mathrm{IC}(K_f/\mathbb{Q}, S^1, p)$ holds. Also, the definition of the pairing $[\cdot,\cdot]_{\mathfrak{P},m+1}$ gives

$$\iota_{\mathfrak{P}}(\xi_f^{f'})^{[1-\xi_f,\iota_{\mathfrak{P}}(gu)]_{\mathfrak{P},m+1}} = (1-\xi_f, \iota_{\mathfrak{P}}(gu))_{K_{\mathfrak{P}},p^{m+1}}.$$

Applying $jh_{\mathfrak{P}}$ to both sides and using the second statement of Lemma 7.2, we get

$$(\hat{\xi}_{f,\mathfrak{P}}^{f'})^{[1-\xi_f,\iota_{\mathfrak{P}}(gu)]_{\mathfrak{P},m+1}} = (1-\hat{\xi}_{f,\mathfrak{P}}, v_{g,\mathfrak{P}})_{\hat{K}_f,p^{m+1}} = (\hat{\xi}_{f,\mathfrak{P}}^{f'})^{-b(\hat{\xi}_{f,\mathfrak{P}},v_{g,\mathfrak{P}})},$$

which implies that $b(\hat{\xi}_{f,\mathfrak{P}}, v_{g,\mathfrak{P}}) \equiv -[1-\xi_f,\iota_{\mathfrak{P}}(gu)]_{\mathfrak{P},m+1} \pmod{p^{m+1}}$. Summing this congruence over all $\mathfrak{P} \in S_p(K_f)$ and combining with (45), (44) and (43), we obtain $\mathfrak{s}_{K_f/\mathbb{Q},S^1}(u) \equiv H_{K_f/\mathbb{Q},m}(\eta_f, u) \pmod{p^{m+1}}$ for any $u \in U^1(K_{f,p})^-$, giving $\mathrm{CC}(K_f/\mathbb{Q}, S^1, p, m)$. ∎

8. The case of K absolutely abelian. If L/M is any Galois extension of number fields and ϕ any complex character of $\mathrm{Gal}(L/M)$, then the *T-truncated Artin L-function* $L_{L/M,T}(s,\phi)$ is defined for any finite set T of places of M containing $S_\infty(M)$ but *not necessarily* $S_{\mathrm{ram}}(L/M)$. If $\mathrm{Gal}(L/M)$ is abelian and ϕ is irreducible (i.e. $\phi \in \widehat{\mathrm{Gal}(L/M)}$) then, as noted in Remark 2.1, the definition agrees with the third member in (3). In particular, there is no conflict with previous notation in the case $T \supset S_{\mathrm{ram}}(L/M)$ and we always have

$$
\begin{aligned}
(46)\qquad L_{L/M,T}(s,\phi) &= \prod_{\substack{\mathfrak{q}\in T\setminus S_\infty(M)\\ \mathfrak{q}\nmid\mathfrak{f}_\phi}} (1-N\mathfrak{q}^{-s}\hat{\phi}([\mathfrak{q}]))L(s,\hat{\phi})\\
&= \prod_{\mathfrak{q}\notin T\cup S_{\mathrm{ram}}(L^\phi/M)} (1-N\mathfrak{q}^{-s}\hat{\phi}(\mathfrak{q}))^{-1}
\end{aligned}
$$

where $\hat{\phi}$ denotes the associated primitive ray-class character modulo $\mathfrak{f}_\phi$, $L^\phi = L^{\ker(\phi)}$ and the infinite product converges only for $\mathrm{Re}(s) > 1$.

LEMMA 8.1. *Suppose L/M and T are as above, with $\mathrm{Gal}(L/M)$ abelian, and suppose l is any intermediate field, $L \supset l \supset M$. Then for any $\chi \in \widehat{\mathrm{Gal}(L/l)}$, we have an identity of meromorphic functions on $\mathbb{C}$:*

$$L_{L/l,T(l)}(s,\chi) = \prod_{\substack{\phi \in \widehat{\mathrm{Gal}(L/M)} \\ \phi|_{\mathrm{Gal}(L/l)} = \chi}} L_{L/M,T}(s,\phi).$$

Proof. This follows from the usual induction and "additivity" properties for Artin L-functions (see [Ta, p. 15]) and the fact (e.g. by Frobenius reciprocity) that $\mathrm{Ind}_{\mathrm{Gal}(L/l)}^{\mathrm{Gal}(L/M)} \chi = \sum_{\substack{\phi \in \widehat{\mathrm{Gal}(L/M)} \\ \phi|_{\mathrm{Gal}(L/l)} = \chi}} \phi$. ■

LEMMA 8.2. *Let B be a finite abelian group, C any subgroup of B and x any element of $\mathbb{C}B$. We write $x|\mathbb{C}B$ for the endomorphism of $\mathbb{C}B$, considered as a free $\mathbb{C}C$-module, determined by multiplication by x. For any $\chi \in \hat{C}$, we have*

$$\chi(\det_{\mathbb{C}C}(x|\mathbb{C}B)) = \prod_{\substack{\phi \in \hat{B} \\ \phi|_C = \chi}} \phi(x)$$

(all characters extended linearly to homomorphisms from the complex group-rings to $\mathbb{C}$).

Proof. Choose any $\mathbb{C}C$-basis $\mathcal{B} = \{y_1, \ldots, y_n\}$ for $\mathbb{C}B$ (where $n = |B : C|$) and let $T = (t_{ij})_{i,j} \in M_n(\mathbb{C}C)$ be the matrix of $x|\mathbb{C}B$ with respect to $\mathcal{B}$. If $e_{\chi,C}$ denotes the idempotent attached to χ in $\mathbb{C}C$, then $x|\mathbb{C}B$ acts on the submodule $e_{\chi,C}\mathbb{C}B$, and its matrix with respect to the $\mathbb{C}$-basis $\{e_{\chi,C}y_1, \ldots, e_{\chi,C}y_n\}$ of the latter is clearly $\chi(T) := (\chi(t_{ij}))_{i,j} \in M_n(\mathbb{C})$. Hence $\chi(\det_{\mathbb{C}C}(x|\mathbb{C}B)) = \chi(\det(T)) = \det(\chi(T)) = \det_{\mathbb{C}}(x|e_{\chi,C}\mathbb{C}B)$. On the other hand, $e_{\chi,C}\mathbb{C}B$ also has a $\mathbb{C}$-basis consisting of the $\mathbb{C}B$-idempotents $e_{\phi,B}$ for the characters $\phi \in \hat{B}$ such that $\phi|_C = \chi$. (This follows easily from the fact that $e_{\chi,C}$ is the sum of the corresponding $e_{\phi,B}$'s.) The result follows, since $xe_{\phi,B} = \phi(x)e_{\phi,B}$. ■

For the rest of this section, we fix K/k, S and p satisfying the standard hypotheses with K absolutely abelian. Thus $G = \mathrm{Gal}(K/k)$ is a subgroup of the abelian group $\Gamma := \mathrm{Gal}(K/\mathbb{Q})$. We define a set of places $S_{\mathbb{Q}}$ of $\mathbb{Q}$ by

$$S_{\mathbb{Q}} = \{\infty\} \cup \{q \text{ prime such that } S_q(k) \subset S\}.$$

Thus $p \in S_{\mathbb{Q}}$ and $S_{\mathbb{Q}}(k)$ is the maximal $\mathrm{Gal}(k/\mathbb{Q})$-stable subset of S. The definition of $\mathrm{Bad}(S)$ in Subsection 4.5 gives

$$S_{\mathrm{ram}}(K/\mathbb{Q}) = \mathrm{Bad}(S) \mathbin{\dot\cup} (S_{\mathrm{ram}}(K/\mathbb{Q}) \cap S_{\mathbb{Q}})$$

(disjoint union). Let us write A for the subgroup $\prod_{q\in\mathrm{Bad}(S)} T_q(K/\mathbb{Q})$ of Γ (trivial if $\mathrm{Bad}(S)=\emptyset$). If F is any subfield of K, it follows that

$$F\subset K^A \Leftrightarrow \text{ all primes } q\in\mathrm{Bad}(S) \text{ are unramified in } F \Leftrightarrow S_{\mathrm{ram}}(F/\mathbb{Q})\subset S_{\mathbb{Q}}. \tag{47}$$

We denote by $\mathcal{X}_{\mathbb{Q}}(A)$ the set of irreducible $\mathbb{Q}$-valued characters of A. Each $\mathcal{A}\in\mathcal{X}_{\mathbb{Q}}(A)$ corresponds to a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-conjugacy class of characters $\alpha\in\hat{A}$ which "belong" to $\mathcal{A}$. We set $\ker(\mathcal{A}):=\ker(\alpha)$ for one (hence any) such α and $K^{\mathcal{A}}:=K^{\ker(\mathcal{A})}\supset K^A$. We define

$$S_{\mathcal{A}}=S_{\mathbb{Q}}\cup S_{\mathrm{ram}}(K^{\mathcal{A}}/\mathbb{Q})\supset S^1(K^{\mathcal{A}}/\mathbb{Q})$$

and write $\tilde{\nu}_{\mathcal{A}}$ for the "averaged corestriction" map $|\ker(\mathcal{A})|^{-1}\nu_{K/K^{\mathcal{A}}}$, which is a (non-unital) homomorphism from $\mathbb{C}\mathrm{Gal}(K^{\mathcal{A}}/\mathbb{Q})$ to $\mathbb{C}\Gamma$. Finally, let $e_{\mathcal{A}}$ denote the idempotent of $\mathbb{Q}A$ corresponding to $\mathcal{A}$. With these notations, we define a meromorphic function

$$x_{K/k,S}:\mathbb{C}\to\mathbb{C}\Gamma,\qquad s\mapsto\sum_{\mathcal{A}\in\mathcal{X}_{\mathbb{Q}}(A)} e_{\mathcal{A}}\tilde{\nu}_{\mathcal{A}}(\Theta_{K^{\mathcal{A}}/\mathbb{Q},S_{\mathcal{A}}}(s)).$$

Proposition 8.3. *With the above hypotheses and notations,*

$$\Theta_{K/k,S_{\mathbb{Q}}(k)}(s)=\det_{\mathbb{C}G}(x_{K/k,S}(s)\,|\,\mathbb{C}\Gamma) \tag{48}$$

(*as* $\mathbb{C}G$*-valued meromorphic functions of* $s\in\mathbb{C}$).

Proof. By meromorphic continuation, it suffices to prove $\chi(\text{L.H.S.})=\chi(\text{R.H.S.})$ in (48), for $\mathrm{Re}(s)>1$ and for all $\chi\in\hat{G}$. Equation (2) and Lemma 8.1 give

$$\chi(\text{L.H.S. of (48)})=L_{K/k,S_{\mathbb{Q}}(k)}(s,\chi^{-1})=\prod_{\substack{\phi\in\hat{\Gamma}\\ \phi|_G=\chi}} L_{K/\mathbb{Q},S_{\mathbb{Q}}}(s,\phi^{-1}),$$

and evaluating $\chi(\text{R.H.S. of (48)})$ via Lemma 8.2, it suffices to show that $L_{K/\mathbb{Q},S_{\mathbb{Q}}}(s,\phi^{-1})=\phi(x_{K/k,S}(s))$ for any $\phi\in\hat{\Gamma}$. Suppose $\alpha_\phi:=\phi|_A$ belongs to $\mathcal{A}_\phi\in\mathcal{X}_{\mathbb{Q}}(A)$, so that $\ker(\alpha_\phi)=A\cap\ker(\phi)$ and $K^{\mathcal{A}_\phi}=K^AK^\phi$. On the one hand, this means that ϕ factors through $\mathrm{Gal}(K^{\mathcal{A}_\phi}/\mathbb{Q})$ and $\phi(e_{\mathcal{A}_\phi}\tilde{\nu}_{\mathcal{A}_\phi}(y))=\phi(y)$ for all $y\in\mathbb{C}\mathrm{Gal}(K^{\mathcal{A}_\phi}/\mathbb{Q})$, while $\phi(e_{\mathcal{A}})=0$ for any $\mathcal{A}\neq\mathcal{A}_\phi$. On the other hand, the equality $K^{\mathcal{A}_\phi}=K^AK^\phi$ implies that $S_{\mathrm{ram}}(K^{\mathcal{A}_\phi}/\mathbb{Q})=S_{\mathrm{ram}}(K^A/\mathbb{Q})\cup S_{\mathrm{ram}}(K^\phi/\mathbb{Q})$. Now, crucially for our argument, (47) implies that $S_{\mathrm{ram}}(K^A/\mathbb{Q})\subset S_{\mathbb{Q}}$ so $S_{\mathcal{A}_\phi}=S_{\mathbb{Q}}\cup S_{\mathrm{ram}}(K^\phi/\mathbb{Q})$. Putting this together, (2), (3) and (46) give, for $\mathrm{Re}(s)>1$,

$$\begin{aligned}\phi(x_{K/k,S}(s))&=\phi(e_{\mathcal{A}_\phi}\tilde{\nu}_{\mathcal{A}_\phi}(\Theta_{K^{\mathcal{A}_\phi}/\mathbb{Q},S_{\mathcal{A}_\phi}}(s)))=L_{K^{\mathcal{A}_\phi}/\mathbb{Q},S_{\mathcal{A}_\phi}}(s,\phi^{-1})\\ &=\prod_{q\notin S_{\mathbb{Q}}\cup S_{\mathrm{ram}}(K^\phi/\mathbb{Q})}(1-q^{-s}\hat{\phi}^{-1}(q))=L_{K/\mathbb{Q},S_{\mathbb{Q}}}(s,\phi^{-1}).\ \blacksquare\end{aligned}$$

Let us write $\mathcal{X}_{\mathbb{Q}}^-(A)$ for the set $\{\mathcal{A}\in\mathcal{X}_{\mathbb{Q}}(A): c\notin\ker(\mathcal{A})\}$ ($=\mathcal{X}_{\mathbb{Q}}(A)$ if $c\notin A$) and $x^-_{K/k,S}$ for the function $e^-x_{K/k,S}:\mathbb{C}\to\mathbb{C}\Gamma^-$. If $\mathcal{A}\in\mathcal{X}_{\mathbb{Q}}(A)$ lies in $\mathcal{X}_{\mathbb{Q}}^-(A)$ then $K^{\mathcal{A}}$ is CM. Otherwise $e^-e_{\mathcal{A}}=0$. Therefore $x^-_{K/k,S}(s)$ equals $\sum_{\mathcal{A}\in\mathcal{X}_{\mathbb{Q}}^-(A)}e_{\mathcal{A}}\tilde\nu_{\mathcal{A}}(\Theta^-_{K^{\mathcal{A}}/\mathbb{Q},S_{\mathcal{A}}}(s))$ and is entire as a function of s. Now take $s=1$, multiply by i/π and apply the involution $(\cdot)^*:\mathbb{C}\Gamma\to\mathbb{C}\Gamma$ (which fixes each $e_{\mathcal{A}}$) to get

$$\left(\frac{i}{\pi}\right)x^-_{K/k,S}(1)^*=\sum_{\mathcal{A}\in\mathcal{X}_{\mathbb{Q}}^-(A)}e_{\mathcal{A}}\tilde\nu_{\mathcal{A}}(a^{-,*}_{K^{\mathcal{A}}/\mathbb{Q},S_{\mathcal{A}}}),\tag{49}$$

which lies in $\bar{\mathbb{Q}}\Gamma$ by (10). On the other hand, multiplying $\Theta_{K/k,S_{\mathbb{Q}}(k)}(s)$ by $(i/\pi)^de^-=((i/\pi)e^-)^{|\Gamma:G|}$ in the previous proposition and letting $s\to1$ implies that $a^-_{K/k,S_{\mathbb{Q}}(k)}$ is the $\mathbb{C}G$-determinant of $(i/\pi)x^-_{K/k,S}(1)$ acting on $\mathbb{C}\Gamma$. It follows easily from this that

$$a^{-,*}_{K/k,S_{\mathbb{Q}}(k)}=\det\nolimits_{\bar{\mathbb{Q}}G}\left(\left(\frac{i}{\pi}\right)x^-_{K/k,S}(1)^*|\bar{\mathbb{Q}}\Gamma\right).\tag{50}$$

For each $\mathcal{A}\in\mathcal{X}_{\mathbb{Q}}^-(A)$ the data $K^{\mathcal{A}}/\mathbb{Q}$, $S_{\mathcal{A}}$ and p satisfy the standard hypotheses. In particular, we have a well-defined $\mathbb{Z}_p\mathrm{Gal}(K^{\mathcal{A}}/\mathbb{Q})$-linear map $\mathfrak{s}^{\mathrm{id}}_{K^{\mathcal{A}}/\mathbb{Q},S_{\mathcal{A}}}$ from $U^1(K_p^{\mathcal{A}})^-$ to $\mathbb{Q}_p\mathrm{Gal}(K^{\mathcal{A}}/\mathbb{Q})^-$ (where "id" denotes the identity element of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$). Both the norm map $N_{K/K^{\mathcal{A}}}:U^1(K_p)\to U^1(K_p^{\mathcal{A}})$ and the averaged corestriction $\tilde\nu_{\mathcal{A}}:\mathbb{Q}_p\mathrm{Gal}(K^{\mathcal{A}}/\mathbb{Q})\to\mathbb{Q}_p\Gamma$ take minus parts to minus parts. The automorphism $\tau_i\in\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ restricts to an element $\gamma_i:=\tau_i|_K$ of Γ for $i=1,\dots,d$ such that $\{\gamma_1^{-1},\dots,\gamma_d^{-1}\}$ is a set of coset representatives for G in Γ, hence also a basis for $\mathcal{R}\Gamma$ over $\mathcal{R}G$, for any commutative ring $\mathcal{R}$. We can now state:

Theorem 8.4. *With the above hypotheses and notations, suppose that $u_1,\dots,u_d$ are any elements of $U^1(K_p)^-$. Then*

$$\mathfrak{s}^{\tau_1,\dots,\tau_d}_{K/k,S_{\mathbb{Q}}(k)}(u_1\wedge\dots\wedge u_d)=\det(c_{i,l})_{1\le i,l\le d}$$

where $c_{i,l}\in\mathbb{Q}_pG^-$ is the coefficient of γ_i^{-1} when the element

$$\sum_{\mathcal{A}\in\mathcal{X}_{\mathbb{Q}}^-(A)}e_{\mathcal{A}}\tilde\nu_{\mathcal{A}}(\mathfrak{s}^{\mathrm{id}}_{K^{\mathcal{A}}/\mathbb{Q},S_{\mathcal{A}}}(N_{K/K^{\mathcal{A}}}u_l))$$

of $\mathbb{Q}_p\Gamma^-$ is expressed in the $\mathbb{Q}_pG$-basis $\{\gamma_1^{-1},\dots,\gamma_d^{-1}\}$ of $\mathbb{Q}_p\Gamma$.

Proof. Choose an embedding $j:\bar{\mathbb{Q}}\to\bar{\mathbb{Q}}_p$ inducing a prime ideal $\mathfrak{P}\in S_p(K)$, say, and write λ_p for the (1×1) regulator $R^{(j;\mathrm{id})}_{K/\mathbb{Q},p}:U^1(K_p)\to\bar{\mathbb{Q}}_p\Gamma$.

If $u \in U^1(K_p)$ then, by definition,

$$\begin{aligned}\lambda_p(u) &= \sum_{i=1}^{d}\sum_{g\in G}\log_p(j\circ\iota_{\mathfrak{P}}(\gamma_i g^{-1}u))(g\gamma_i^{-1})\\ &= \sum_{i=1}^{d}\Big(\sum_{g\in G}\log_p(j\tau_i\circ\iota_{\mathfrak{P}_i}(g^{-1}u))g\Big)\gamma_i^{-1}\end{aligned}$$

where $j\tau_i$ induces $\mathfrak{P}_i \in S_p(K)$. Now $\bigwedge^d_{\bar{\mathbb{Q}}_pG}\bar{\mathbb{Q}}_p\Gamma$ is $\bar{\mathbb{Q}}_pG$-free of rank one on $\gamma_1^{-1}\wedge\cdots\wedge\gamma_d^{-1}$ and it follows easily from the last equation and the definition of $R^{(j;\tau_1,\ldots,\tau_d)}_{K/k,p}$ that

$$\begin{aligned}(51)\qquad &\lambda_p(u_1)\wedge\cdots\wedge\lambda_p(u_d)\\ &\quad= R^{(j;\tau_1,\ldots,\tau_d)}_{K/k,p}(u_1\wedge\cdots\wedge u_d)\gamma_1^{-1}\wedge\cdots\wedge\gamma_d^{-1}\quad\text{ in } \textstyle\bigwedge^d_{\bar{\mathbb{Q}}_pG}\bar{\mathbb{Q}}_p\Gamma.\end{aligned}$$

On the other hand, $R^{(j;\mathrm{id})}_{K^{\mathcal{A}}/\mathbb{Q},p}\circ N_{K/K^{\mathcal{A}}} = \pi_{K/K^{\mathcal{A}}}\circ\lambda_p$ for each $\mathcal{A}\in\mathcal{X}^-_{\mathbb{Q}}(A)$ so that $\mathfrak{s}^{\mathrm{id}}_{K^{\mathcal{A}}/\mathbb{Q},S_{\mathcal{A}}}(N_{K/K^{\mathcal{A}}}u_l) = j(a^{-,*}_{K^{\mathcal{A}}/\mathbb{Q},S_{\mathcal{A}}})\pi_{K/K^{\mathcal{A}}}(\lambda_p(u_l))$ for each $\mathcal{A}$ and l. It follows that

$$\begin{aligned}\sum_{i=1}^{d}c_{i,l}\gamma_i^{-1} &= \Big(\sum_{\mathcal{A}\in\mathcal{X}^-_{\mathbb{Q}}(A)} e_{\mathcal{A}}\tilde{\nu}_{\mathcal{A}}(j(a^{-,*}_{K^{\mathcal{A}}/\mathbb{Q},S_{\mathcal{A}}}))\Big)\lambda_p(u_l)\\ &= j((i/\pi)x^-_{K/k,S}(1)^*)\lambda_p(u_l)\end{aligned}$$

by (49). Using (50), we deduce easily that

$$\begin{aligned}&\det(c_{i,l})_{1\le i,l\le d}\,\gamma_1^{-1}\wedge\cdots\wedge\gamma_d^{-1}\\ &\quad= (j((i/\pi)x^-_{K/k,S}(1)^*)\lambda_p(u_1))\wedge\cdots\wedge(j((i/\pi)x^-_{K/k,S}(1)^*)\lambda_p(u_l))\\ &\quad= j(a^{-,*}_{K/k,S_{\mathbb{Q}}(k)})\lambda_p(u_1)\wedge\cdots\wedge\lambda_p(u_l)\end{aligned}$$

and combining this with (51), the result follows from the definition of $\mathfrak{s}^{\tau_1,\ldots,\tau_d}_{K/k,S_{\mathbb{Q}}(k)}$. ■

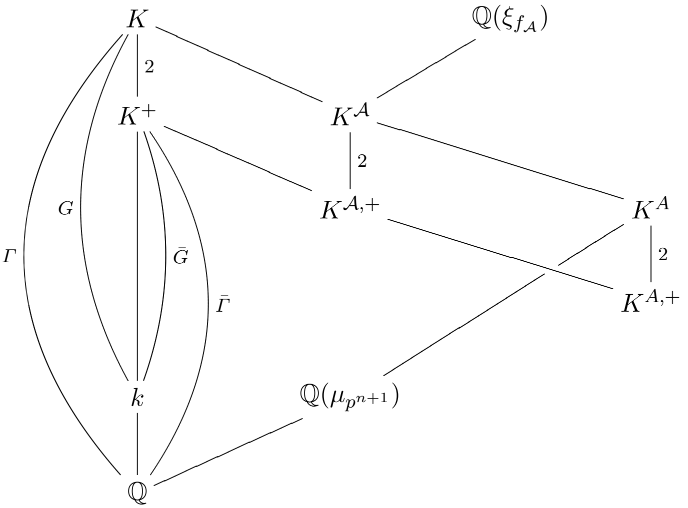
Proof of Theorem 4.4 under Hypothesis 4.5. By Proposition 5.1 it suffices to prove $\mathrm{IC}(K/k,S_{\mathbb{Q}}(k),p)$, i.e. that $\mathfrak{s}_{K/k,S_{\mathbb{Q}}(k)}(u_1\wedge\cdots\wedge u_d)$ lies in $\mathbb{Z}_pG$ for all $u_i,\ldots,u_d\in U^1(K_p)^-$ and this will clearly follow from Theorem 8.4 provided we can show

$$(52)\qquad e_{\mathcal{A}}\tilde{\nu}_{\mathcal{A}}(\mathfrak{s}_{K^{\mathcal{A}}/\mathbb{Q},S_{\mathcal{A}}}(N_{K/K^{\mathcal{A}}}u_l))\in\mathbb{Z}_p\Gamma,\qquad \forall l,\ \forall\mathcal{A}\in\mathcal{X}^-_{\mathbb{Q}}(A).$$

But Theorem 4.3(i) implies that $\mathfrak{s}_{K^{\mathcal{A}}/\mathbb{Q},S_{\mathcal{A}}}(N_{K/K^{\mathcal{A}}}u_l)$ lies in $\mathbb{Z}_p\mathrm{Gal}(K^{\mathcal{A}}/\mathbb{Q})$. Furthermore, if $q\in\mathrm{Bad}(S)$ then $|T_q(K/\mathbb{Q})| = e_q(k/\mathbb{Q})$ and Hypothesis 4.5 implies that this is prime to p for all such q, hence that $p\nmid|A|$. Consequently,

$p\nmid [K:K^{\mathcal{A}}]$ for every $\mathcal{A}$ so that $e_{\mathcal{A}}\in \mathbb{Z}_{(p)}A$ and $\tilde{\nu}_{\mathcal{A}}(\mathfrak{s}_{K^{\mathcal{A}}/\mathbb{Q},S_{\mathcal{A}}}(N_{K/K^{\mathcal{A}}}u_l))$ $\in \mathbb{Z}_p\Gamma$, establishing (52). ∎

Turning to the Congruence Conjecture, we suppose from now on that *K contains $\mu_{p^{n+1}}$ for some $n\geq 0$*. Since $S_{\rm ram}(\mathbb{Q}(\mu_{p^{n+1}})/\mathbb{Q})=\{p\}\subset S_{\mathbb{Q}}$, it follows from (47) that K^A contains $\mathbb{Q}(\mu_{p^{n+1}})$, so is CM and $\mathcal{X}^-_{\mathbb{Q}}(A)=\mathcal{X}_{\mathbb{Q}}(A)$. We write $\bar{\Gamma}$ for $\mathrm{Gal}(K^+/\mathbb{Q})$.



Now $\mathrm{RSC}(K^{\mathcal{A},+}/\mathbb{Q},S_{\mathcal{A}};\mathbb{Q})$ holds for each $\mathcal{A}\in\mathcal{X}_{\mathbb{Q}}(A)$. Indeed, let us write $f_{\mathcal{A}}$ for the conductor of $K^{\mathcal{A}}$ so that $p^{n+1}\mid f_{\mathcal{A}}$ and $S^1(K^{\mathcal{A}}/\mathbb{Q})=S^1(\mathbb{Q}(\xi_{f_{\mathcal{A}}})/\mathbb{Q})$ $=\{\infty\}\cup S_{f_{\mathcal{A}}}(\mathbb{Q})$. Then the determination of $\eta_{\mathbb{Q}(\xi_{f_{\mathcal{A}}})^+/\mathbb{Q},S^1(\mathbb{Q}(\xi_{f_{\mathcal{A}}})/\mathbb{Q})}$ in the proof of Theorem 4.3, together with Propositions 5.7 and 5.3, implies that the solution $\eta_{K^{\mathcal{A},+}/\mathbb{Q},S_{\mathcal{A}}}$ of $\mathrm{RSC}(K^{\mathcal{A},+}/\mathbb{Q},S_{\mathcal{A}};\mathbb{Q})$ (with $\tau_1=\mathrm{id}$) is

$$\begin{aligned}\eta_{\mathcal{A}}&:=\Big(\prod_{q\in S_{\mathcal{A}}\setminus S^1(K^{\mathcal{A}}/\mathbb{Q})}(1-\sigma^{-1}_{q,K^{\mathcal{A},+}/\mathbb{Q}})\Big)N_{\mathbb{Q}(\xi_{f_{\mathcal{A}}})^+/K^{\mathcal{A},+}}(\eta_{\mathbb{Q}(\xi_{f_{\mathcal{A}}})^+/\mathbb{Q},S^1(\mathbb{Q}(\xi_{f_{\mathcal{A}}})/\mathbb{Q})})\\&=\Big(\prod_{q\in S_{\mathcal{A}}\setminus S^1(K^{\mathcal{A}}/\mathbb{Q})}(1-\sigma^{-1}_{q,K^{\mathcal{A},+}/\mathbb{Q}})\Big)N_{\mathbb{Q}(\xi_{f_{\mathcal{A}}})^+/K^{\mathcal{A},+}}\Big(\frac{1}{2}\otimes(1-\xi_{f_{\mathcal{A}}})^{1+c}\Big).\end{aligned}$$

In fact, $1-\xi_{f_{\mathcal{A}}}$ lies in $U_{\{\infty\}}(\mathbb{Q}(\xi_{f_{\mathcal{A}}}))$ unless $f_{\mathcal{A}}$ is a power of a prime, necessarily p, in which case it lies in $U_{\{\infty,p\}}(\mathbb{Q}(\xi_{f_{\mathcal{A}}}))$. Thus for all $\mathcal{A}\in\mathcal{X}_{\mathbb{Q}}(A)$, the element $\eta_{\mathcal{A}}$ lies in $\frac{1}{2}\overline{U_{\{\infty,p\}}(K^{\mathcal{A},+})}\subset\mathbb{Q}U_{\{\infty,p\}}(K^{\mathcal{A},+})$. Let us write $i_{\mathcal{A}}$ for the natural injection $\mathbb{Q}U_{\{\infty,p\}}(K^{\mathcal{A},+})\to\mathbb{Q}U_{\{\infty,p\}}(K^+)$ and $\tilde{i}_{\mathcal{A}}$ for $|\ker(\mathcal{A})|^{-1}i_{\mathcal{A}}$. We define

$$\alpha_{S_{\mathbb{Q}}(k)}:=\sum_{\mathcal{A}\in\mathcal{X}_{\mathbb{Q}}(A)}e_{\mathcal{A}}\tilde{i}_{\mathcal{A}}(\eta_{\mathcal{A}}),$$

$$\eta_{S_{\mathbb{Q}}(k)}:=\gamma_1^{-1}\alpha_{S_{\mathbb{Q}}(k)}\wedge\cdots\wedge\gamma_d^{-1}\alpha_{S_{\mathbb{Q}}(k)},$$

from which it is clear that $\alpha_{S_{\mathbb{Q}}(k)}$ lies in $|A|^{-2}\frac{1}{2}\overline{U_{\{\infty,p\}}(K^+)}$ and $\eta_{S_{\mathbb{Q}}(k)}$ in $\left(|A|^{-2}\frac{1}{2}\right)^d\overline{\bigwedge^d_{\mathbb{Z}\bar{G}} U_{\{\infty,p\}}(K^+)}$.

Proposition 8.5. *With the above hypotheses,* $\mathrm{RSC}(K^+/k, S_{\mathbb{Q}}(k); \mathbb{Q})$ *holds with solution* $\eta_{K^+/k,S_{\mathbb{Q}}(k)} = \eta_{S_{\mathbb{Q}}(k)}$.

We defer the proof. The final ingredient in the proof of Theorem 4.6 is

Lemma 8.6. *Suppose* α *is an element of* $\overline{U_{\{\infty,p\}}(K^+)}$ *so that* $\gamma_1^{-1}\alpha \wedge \cdots \wedge \gamma_d^{-1}\alpha$ *lies in the subset* $\overline{\bigwedge^d_{\mathbb{Z}\bar{G}} U_{S_{\mathbb{Q}}(k)}(K^+)}$ *of* $\bigwedge^d_{\mathbb{Q}\bar{G}} \mathbb{Q}U_{S_{\mathbb{Q}}(k)}(K^+)$. *Then, for any* $u_1,\ldots,u_d \in U^1(K_p)^-$, *we have*

$$\kappa_n(\tau_1\ldots\tau_d)H_{K/k,n}(\gamma_1^{-1}\alpha\wedge\cdots\wedge\gamma_d^{-1}\alpha, u_1\wedge\cdots\wedge u_d) = \det(d_{i,l})_{1\le i,l\le d}$$

where $d_{i,l} \in (\mathbb{Z}/p^{n+1}\mathbb{Z})G^-$ *is the coefficient of* γ_i^{-1} *when* $H_{K/\mathbb{Q},n}(\alpha,u_l) \in (\mathbb{Z}/p^{n+1}\mathbb{Z})\Gamma^-$ *is expressed in the* $(\mathbb{Z}/p^{n+1}\mathbb{Z})G$*-basis* $\{\gamma_1^{-1},\ldots,\gamma_d^{-1}\}$ *of* $(\mathbb{Z}/p^{n+1}\mathbb{Z})\Gamma$.

Proof. If $\alpha = 1\otimes\varepsilon$ for some $\varepsilon \in U_{\{\infty,p\}}(K^+)$ then $\gamma_i^{-1}\alpha = 1\otimes\gamma_i^{-1}\varepsilon$ with $\gamma_i^{-1}\varepsilon \in U_{\{\infty,p\}}(K^+) \subset U_S(K^+)$ for all i. Equations (20) and (18) applied to $K/\mathbb{Q}$ give

$$\begin{aligned} H_{K/\mathbb{Q},n}(\alpha,u_l) &= \sum_{i=1}^d \Big(\sum_{g\in G}[\varepsilon,\gamma_i g u_l]_{K,n} g^{-1}\Big)\gamma_i^{-1} \\ &= \sum_{i=1}^d \Big(\kappa_n(\tau_i)\sum_{g\in G}[\gamma_i^{-1}\varepsilon, g u_l]_{K,n} g^{-1}\Big)\gamma_i^{-1} \end{aligned}$$

since $\gamma_i = \tau_i|_K$. Thus $d_{i,l} = \kappa_n(\tau_i)\sum_{g\in G}[\gamma_i^{-1}\varepsilon, g u_l]_{K,n} g^{-1}$. Now use (20) for K/k. ∎

Proof of Theorem 4.6. By Proposition 5.4 it suffices to establish $\mathrm{CC}(K/k, S_{\mathbb{Q}}(k), p, n)$ under Hypothesis 4.5. But the latter has already been shown to imply $\mathrm{IC}(K/k, S_{\mathbb{Q}}(k), p)$ and $p\nmid|A|$. In particular, $\eta_{S_{\mathbb{Q}}(k)}$ lies in

$$\mathbb{Z}_{(p)}\overline{\bigwedge^d_{\mathbb{Z}\bar{G}} U_{\{\infty,p\}}(K^+)} \subset \mathbb{Z}_{(p)}\Lambda_{0,S_{\mathbb{Q}}(k)}$$

and so is the solution of $\mathrm{RSC}(K^+/k, S_{\mathbb{Q}}(k); \mathbb{Z}_{(p)})$ by Proposition 8.5. It remains to prove that the congruence (24) holds with $\eta_{K^+/k,S} = \eta_{S_{\mathbb{Q}}(k)}$ and $\theta = u_1\wedge\cdots\wedge u_d$ with $u_i \in U^1(K_p)^-$ for all i. (Such θ generate $\bigwedge^d_{\mathbb{Z}_pG} U^1(K_p)^-$.) For each $\mathcal{A} \in \mathcal{X}_{\mathbb{Q}}(\mathcal{A})$ we may write $2\eta_{\mathcal{A}}$ as $1\otimes\varepsilon_{\mathcal{A}}$ where $\varepsilon_{\mathcal{A}}$ lies in $U_{\{\infty,p\}}(K^{\mathcal{A},+})$. From (30) with $F = K^{\mathcal{A}}$ and (20) (with $d=1$!) it follows easily that

$$H_{K/\mathbb{Q},n}(i_{\mathcal{A}}(2\eta_{\mathcal{A}}), u_l) = \nu_{K/K^{\mathcal{A}}}(H_{K^{\mathcal{A}}/\mathbb{Q},n}(2\eta_{\mathcal{A}}, N_{K/K^{\mathcal{A}}}u_l)).$$

Therefore, using the $\mathbb{Z}\Gamma$-linearity of $H_{K/\mathbb{Q},n}(\cdot,\cdot)$ in the first variable and the fact that $|A|e_{\mathcal{A}}\in\mathbb{Z}\Gamma$, we have, for each l,

$$\begin{aligned}
H_{K/\mathbb{Q},n}(2|A|^2\alpha_{S_{\mathbb{Q}}(k)},u_l) &= \sum_{\mathcal{A}\in\mathcal{X}_{\mathbb{Q}}(A)}(|A|\,|A:\ker(\mathcal{A})|e_{\mathcal{A}})H_{K/\mathbb{Q},n}(i_{\mathcal{A}}(2\eta_{\mathcal{A}}),u_l)\\
&= \sum_{\mathcal{A}\in\mathcal{X}_{\mathbb{Q}}(A)}(|A|\,|A:\ker(\mathcal{A})|e_{\mathcal{A}})\nu_{K/K^{\mathcal{A}}}(H_{K^{\mathcal{A}}/\mathbb{Q},n}(2\eta_{\mathcal{A}},N_{K/K^{\mathcal{A}}}u_l))\\
&\equiv \sum_{\mathcal{A}\in\mathcal{X}_{\mathbb{Q}}(A)}2(|A|\,|A:\ker(\mathcal{A})|e_{\mathcal{A}})\nu_{K/K^{\mathcal{A}}}(\mathfrak{s}^{\mathrm{id}}_{K^{\mathcal{A}}/\mathbb{Q},S_{\mathcal{A}}}(N_{K/K^{\mathcal{A}}}u_l))\\
&\equiv \sum_{\mathcal{A}\in\mathcal{X}_{\mathbb{Q}}(A)}2|A|^2e_{\mathcal{A}}\tilde{\nu}_{\mathcal{A}}(\mathfrak{s}^{\mathrm{id}}_{K^{\mathcal{A}}/\mathbb{Q},S_{\mathcal{A}}}(N_{K/K^{\mathcal{A}}}u_l))\equiv\sum_{i=1}^{d}2|A|^2c_{i,l}\gamma_i^{-1}\pmod{p^{n+1}}
\end{aligned}$$

where $c_{i,l}$ is precisely as defined in Theorem 8.4. Note that the first congruence above comes from Theorem 4.3, which also shows that the last three expressions lie in $\mathbb{Z}_p\Gamma$. It follows from Lemma 8.6 and the above that

$$\begin{aligned}
&\overline{(2|A|^2)^d}\kappa_n(\tau_1\ldots\tau_d)H_{K/k,n}(\eta_{S_{\mathbb{Q}}(k)},u_1\wedge\cdots\wedge u_d)\\
&\quad=\kappa_n(\tau_1\ldots\tau_d)H_{K/k,n}(\gamma_1^{-1}(2|A|^2\alpha_{S_{\mathbb{Q}}(k)})\wedge\cdots\wedge\gamma_d^{-1}(2|A|^2\alpha_{S_{\mathbb{Q}}(k)}),u_1\wedge\cdots\wedge u_d)\\
&\quad=\det(\overline{2|A|^2c_{i,l}})_{1\le i,l\le d}
\end{aligned}$$

in $(\mathbb{Z}/p^{n+1}\mathbb{Z})G$. As $p\nmid 2|A|$, we may cancel the factor $\overline{(2|A|^2)^d}\in(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ on both sides above and combining with Theorem 8.4 we obtain the required equation

$$\begin{aligned}
\overline{\mathfrak{s}^{\tau_1,\ldots,\tau_d}_{K/k,S_{\mathbb{Q}}(k)}(u_1\wedge\cdots\wedge u_d)} &= \det(\overline{c_{i,l}})_{1\le i,l\le d}\\
&=\kappa_n(\tau_1\ldots\tau_d)H_{K/k,n}(\eta_{S_{\mathbb{Q}}(k)},u_1\wedge\cdots\wedge u_d). \quad\blacksquare
\end{aligned}$$

Remark 8.7. Burns has proven Conjecture B′ of [Ru] whenever K is absolutely abelian (see [Bu2, Theorem A]). It follows from Remark 2.8 that $\eta_{S_{\mathbb{Q}}(k)}=\eta_{K^+/k,S_{\mathbb{Q}}(k)}$ must also lie in $\frac{1}{2}\Lambda_{0,S_{\mathbb{Q}}(k)}(K^+/k)$, although this is not obvious from our expression for $\eta_{S_{\mathbb{Q}}(k)}$ and Burns' results do not appear to provide an explicit expression. On the other hand, Cooper obtains essentially our expression $\gamma_1^{-1}\alpha_{S_{\mathbb{Q}}(k)}\wedge\cdots\wedge\gamma_d^{-1}\alpha_{S_{\mathbb{Q}}(k)}$ in [Coo]. (Indeed, we adapt his methods in the proof of Proposition 8.5 below.) By manipulating it cleverly and using the norm relations for cyclotomic numbers, he shows explicitly that if A is cyclic and of odd order, then $\eta_{S_{\mathbb{Q}}(k)}$ lies in $2^{-d}\overline{\bigwedge^d_{\mathbb{Z}\bar{G}}U_{\{\infty,p\}}(K^+)}$. (This follows from [Coo, Theorem 5.2.2].)

Proof of Proposition 8.5. The arguments are mostly familiar by now: Applying e^+ to (48) one deduces that $\Theta_{K^+/k,S_{\mathbb{Q}}(k)}(s)$ is the $\mathbb{C}\bar{G}$-determinant of $\sum_{\mathcal{A}}e_{\mathcal{A}}|\ker(\mathcal{A})|^{-1}\nu_{K^+/K^{\mathcal{A},+}}(\Theta_{K^{\mathcal{A},+}/\mathbb{Q},S_{\mathcal{A}}}(s))$ acting on $\mathbb{C}\bar{\Gamma}$, where we are identifying A with $\mathrm{Gal}(K^+/K^{A,+})$ by restriction. Now $\Theta_{K^{\mathcal{A},+}/\mathbb{Q},S_{\mathcal{A}}}(0) = 0$ and $\Theta^{(1)}_{K^{\mathcal{A},+}/\mathbb{Q},S_{\mathcal{A}}}(0)$ has real coefficients for each $\mathcal{A}$, so

$$(53)\quad \Theta^{(r)}_{K^+/k,S_{\mathbb{Q}}(k)}(0) = \det{}_{\mathbb{R}\bar{G}}\Big(\sum_{\mathcal{A}} e_{\mathcal{A}}|\ker(\mathcal{A})|^{-1}\nu_{K^+/K^{\mathcal{A},+}}(\Theta^{(1)}_{K^{\mathcal{A},+}/\mathbb{Q},S_{\mathcal{A}}}(0))\Big|\mathbb{R}\bar{\Gamma}\Big) = \det\,(e_{i,l})_{1\le i,l\le d}$$

say, where $(e_{i,l})_{i,l=1}^d$ is the matrix of multiplication by $\sum_{\mathcal{A}}\dots$ on $\mathbb{R}\bar{\Gamma}$ with respect to the $\mathbb{R}\bar{G}$-basis $\bar{\gamma}_l^{-1}$, $i = 1,\dots,d$ (where $\bar{\gamma}_l := \gamma_l|_{K^+} = \tau_l|_{K^+}$). Fix l and take $\tau_1 = \mathrm{id}$. Using (15) for each extension $K^{\mathcal{A},+}/\mathbb{Q}$ and the relation $\nu_{K^+/K^{\mathcal{A},+}}\circ\lambda_{K^{\mathcal{A},+}/\mathbb{Q},1} = \lambda_{K^+/\mathbb{Q},1}\circ i_{K^+/K^{\mathcal{A},+}}$, we get

$$\sum_{\mathcal{A}} e_{\mathcal{A}}|\ker(\mathcal{A})|^{-1}\nu_{K^+/K^{\mathcal{A},+}}(\Theta^{(1)}_{K^{\mathcal{A},+}/\mathbb{Q},S_{\mathcal{A}}}(0))\bar{\gamma}_l^{-1} = \sum_{\mathcal{A}} e_{\mathcal{A}}|\ker(\mathcal{A})|^{-1}\nu_{K^+/K^{\mathcal{A},+}}(\lambda_{K^{\mathcal{A},+}/\mathbb{Q},1}(\eta_{\mathcal{A}}))\bar{\gamma}_l^{-1} = \lambda_{K^+/\mathbb{Q},1}(\alpha_{S_{\mathbb{Q}}(k)})\bar{\gamma}_l^{-1}.$$

But for any element $\alpha = a\otimes\varepsilon$ of $\mathbb{Q}U_S(K^+)$ (with $a\in\mathbb{Q}$) we have

$$\lambda_{K^+/\mathbb{Q},1}(\alpha)\bar{\gamma}_l^{-1} = \lambda_{K^+/\mathbb{Q},1}(\bar{\gamma}_l^{-1}\alpha) = a\sum_{i=1}^d\Big(\sum_{\bar{g}\in\bar{G}}\log|\bar{\gamma}_i\bar{g}\bar{\gamma}_l^{-1}\varepsilon|\bar{g}^{-1}\Big)\bar{\gamma}_i^{-1} = \sum_{i=1}^d \lambda_{K^+/k,i}(\bar{\gamma}_l^{-1}\alpha)\bar{\gamma}_i^{-1}$$

and combining with the previous equation, we find $e_{i,l} = \lambda_{K^+/k,i}(\bar{\gamma}_l^{-1}\alpha_{S_{\mathbb{Q}}(k)})$. Substituting this in (53), it follows that $\eta_{S_{\mathbb{Q}}(k)}$ satisfies condition (15) for K/k^+ and $S_{\mathbb{Q}}(k)$.

To show that $\eta_{S_{\mathbb{Q}}(k)}$ satisfies the eigenspace condition with respect to $(S_{\mathbb{Q}}(k), d, \bar{G})$, one could adapt the argument of [Coo] (based on [Po, Proposition 3.1.2]) using condition (iv) of Proposition 2.6. We sketch a more "algebraic" argument based on the equivalent condition (iii): Suppose $\mathfrak{q}\in S_{\mathbb{Q}}(k)\setminus S_\infty(k)$ lies above $q\in S_{\mathbb{Q}}\setminus\{\infty\}$, write D for $D_q(K/\mathbb{Q})$ and $\mathfrak{D}$ for $D_{\mathfrak{q}}(K/k) = D\cap G$. Let $\rho_1,\dots,\rho_t$ be a set of representatives for D mod $\mathfrak{D}$, hence for DG mod G, and let $\sigma_1,\dots,\sigma_m$ be a set of representatives for Γ mod DG. Then $d = mt$ and both $\{\sigma_a\rho_b\}_{a,b}$ and $\{\gamma_i^{-1}\}_i$ are sets of representatives for Γ mod G. Writing also η and α for $\eta_{S_{\mathbb{Q}}(k)}$ and $\alpha_{S_{\mathbb{Q}}(k)}$ respectively, it follows that $\eta = \pm g\bigwedge_{a=1}^m\bigwedge_{b=1}^t\sigma_a\rho_b\alpha$ for some $g\in G$. (The unordered "wedge product" (over $\mathbb{Q}\bar{G}$) on the R.H.S. is defined only up to sign.) Since $N_{D_{\mathfrak{q}}(K^+/k)}\eta$ equals $\frac{1}{2}N_{\mathfrak{D}}\eta$ or $N_{\mathfrak{D}}\eta$, condition (iii) for $m=\eta$ and $S = S_{\mathbb{Q}}(k)$ will follow if we can show that $N_{\mathfrak{D}}\eta$ is fixed by G (hence by $\bar{G}$) and is zero if $|S_{\mathbb{Q}}(k)| > d+1$. But

$$(54)\qquad N_{\mathfrak{D}}\eta = \pm|\mathfrak{D}|^{1-d} g \bigwedge_{a=1}^{m} \bigwedge_{b=1}^{t} \sigma_a N_{\mathfrak{D}} \rho_b \alpha$$
$$= \pm|\mathfrak{D}|^{1-d} g \bigwedge_{a=1}^{m} (\sigma_a N_D \alpha \wedge \sigma_a N_{\mathfrak{D}} \rho_2 \alpha \wedge \cdots \wedge \sigma_a N_{\mathfrak{D}} \rho_t \alpha)$$

(the second equality since $\sigma_a N_D \alpha = \sum_{b=1}^{t} \sigma_a N_{\mathfrak{D}} \rho_b \alpha$ for each a). If $|S_{\mathbb{Q}}| > 2$ then $|S_{\mathcal{A}}| > 2$ for each $\mathcal{A} \in \mathcal{X}_{\mathbb{Q}}(A)$ so the eigenspace condition on $\eta_{\mathcal{A}}$ as a solution of $\mathrm{RSC}(K^{\mathcal{A},+}/\mathbb{Q}, S_{\mathcal{A}}; \mathbb{Q})$ implies that it is annihilated by $N_{D_q(K^{\mathcal{A},+}/\mathbb{Q})}$, hence by N_D. It follows that $N_D \alpha = 0$ hence $N_{\mathfrak{D}}\eta = 0$ by (54). Otherwise, $|S_{\mathbb{Q}}| = 2$, $S_{\mathbb{Q}} = \{\infty, q\}$ (so $q = p$) and $|S_{\mathbb{Q}}(k)|$ is precisely $d+m$. In this case, the eigenspace condition on $\eta_{\mathcal{A}}$ still shows that $N_{D_q(K^{\mathcal{A},+}/\mathbb{Q})}\eta_{\mathcal{A}}$ is fixed by $\mathrm{Gal}(K^{\mathcal{A},+}/\mathbb{Q})$ for all $\mathcal{A}$ and it follows as above that $N_D\alpha$ is fixed by G. So (54) implies that $N_{\mathfrak{D}}\eta$ is fixed by G and, if $m > 1$, that it is zero, since then $\sigma_1 N_D \alpha = \sigma_2 N_D \alpha$. ■

Acknowledgments. It is my pleasure to thank Andrew Jones, Radan Kučera, Cristian Popescu and Jonathan Sands for useful discussions about the contents of this paper. I wish also to thank Cristian and UCSD for their hospitality during the sabbatical year in which the majority of this paper was written.

References

[A-H] E. Artin und 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), 146–162.

[A-T] E. Artin and J. Tate, *Class Field Theory*, Benjamin, New York, 1967.

[Bo] M. Bovey, *Explicit reciprocity for p-units and a special case of the Rubin–Stark conjecture*, PhD thesis, King's College London, 2009.

[Bu1] D. Burns, *Equivariant Tamagawa numbers and refined abelian Stark conjectures*, J. Math. Sci. Univ. Tokyo 10 (2003), 225–259.

[Bu2] —, *Congruences between derivatives of abelian L-functions at $s = 0$*, Invent. Math. 169 (2007), 451–499.

[B-F] D. Burns and M. Flach, *On the equivariant Tamagawa number conjecture for Tate motives, II*, Doc. Math., Extra Volume for John H. Coates' Sixtieth Birthday, 2006, 133–163.

[Col] R. Coleman, *The dilogarithm and the norm residue symbol*, Bull. Soc. Math. France 109 (1981), 373–402.

[Coo] A. Cooper, *Some explicit solutions of the Abelian Stark conjecture*, PhD thesis, King's College London, 2005.

[Fr] A. Fröhlich, *Galois Module Structure of Algebraic Integers*, Springer, Berlin, 1983.

[F-T] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge Univ. Press, Cambridge, 1991.

[Gr] C. Greither, *Determining Fitting ideals of minus class groups via the equivariant Tamagawa number conjecture*, Compos. Math. 143 (2007), 1399–1426.
[Jo] A. Jones, *Dirichlet L-functions at $s = 1$*, PhD thesis, King's College London, 2007.
[Ma] J. Martinet, *Character theory and Artin L-functions*, in: Algebraic Number Fields, A. Fröhlich (ed.), Academic Press, New York, 1977, 1–87.
[Ne] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, Berlin, 1999.
[Po] C. Popescu, *Base change for Stark-type conjectures "over $\mathbb{Z}$"*, J. Reine Angew. Math. 542 (2002), 85–111.
[R-S1] X.-F. Roblot and D. Solomon, *Verifying a p-adic abelian Stark conjecture at $s = 1$*, J. Number Theory 107 (2004), 168–206.
[R-S2] —, —, *Testing the congruence conjecture for Rubin–Stark elements*, ibid., in press.
[Ru] K. Rubin, *A Stark conjecture "over $\mathbf{Z}$" for abelian L-functions with multiple zeros*, Ann. Inst. Fourier (Grenoble) 46 (1996), 33–62.
[Se] J.-P. Serre, *Local Fields*, Springer, New York, 1979.
[Sh] T. Shintani, *On evaluation of zeta functions of totally real algebraic number fields at non-positive integers*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 23 (1976), 393–417.
[Si] C. L. Siegel, *Über die Fourierschen Koeffizienten von Modulformen*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II 1970, 15–56.
[So1] D. Solomon, *Galois relations for cyclotomic numbers and p-units*, J. Number Theory 46 (1994), 158–178.
[So2] —, *Twisted zeta-functions and abelian Stark conjectures*, ibid. 94 (2002), 10–48.
[So3] —, *On p-adic abelian Stark conjectures at $s = 1$*, Ann. Inst. Fourier (Grenoble) 52 (2002), 379–417.
[So4] —, *Abelian conjectures of Stark type in $\mathbb{Z}_p$-extensions of totally real fields*, in: Stark's Conjectures: Recent Work and New Directions, D. Burns et al. (eds.), Contemp. Math. 358, Amer. Math. Soc., Providence, RI, 2004, 143–178.
[So5] —, *On twisted zeta-functions at $s = 0$ and partial zeta-functions at $s = 1$*, J. Number Theory 128 (2008), 105–143.
[So6] —, *Some new ideals in classical Iwasawa theory*, preprint, 2009, http://arxiv.org/abs/0905.4336.
[St] H. Stark, *L-functions at $s = 1$. IV*, Adv. Math. 35 (1980), 197–235.
[Ta] J. T. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$*, Birkhäuser, Boston, 1984.
[Wi] A. Wiles, *On a conjecture of Brumer*, Ann. of Math. 131 (1990), 555–565.

D. Solomon
Department of Mathematics
King's College
Strand, London
WC2R 2LS, U.K.
E-mail: david.solomon@kcl.ac.uk

Received on 1.7.2009
and in revised form on 9.9.2009 (6075)