ACTA ARITHMETICA
162.2 (2014)

Some new maps and ideals in classical Iwasawa theory with applications

by

DAVID SOLOMON (London)

1. Introduction. Let K/k be any Galois extension of number fields and p any *odd* prime number. For each $n \geq -1$, we set $K_n = K(\mu_{p^{n+1}})$ and $G_n = \mathrm{Gal}(K_n/k)$. Let $K_\infty = \bigcup_{n\geq -1} K_n$, $G_\infty = \mathrm{Gal}(K_\infty/k)$ and $\mathfrak{X}_\infty = \mathrm{Gal}(M_\infty/K_\infty)$ where M_∞ is the maximal abelian pro-p extension of K_∞ unramified outside p. For each $n \geq 0$ we shall write Γ_n for $\mathrm{Gal}(K_\infty/K_n)$.

Now suppose that $k = \mathbb{Q}$ and $\mathrm{Gal}(K/\mathbb{Q})$ is abelian. Let K_n^+ and K_∞^+ be the maximal real subfields and let $G_n^+ = \mathrm{Gal}(K_n^+/\mathbb{Q})$. By applying Kummer theory to a particular sequence of cyclotomic 'units' $\{\varepsilon_n\}_{n\geq 0}$ of the fields K_n^+ we shall construct a pair of new G_∞-(semi)linear maps denoted $\mathfrak{d}_\infty$ and $\mathfrak{j}_\infty$, which are defined on $\mathfrak{X}_\infty$ and take values in the 'plus' and 'minus' parts respectively of the completed group ring $\mathbb{Z}_p[[G_\infty]]$. The main purpose of this paper is to explore systematically the properties of these maps and their images, the latter being ideals of $\mathbb{Z}_p[[G_\infty]]$ which we denote $\mathfrak{D}_\infty$ and $\mathfrak{J}_\infty$ respectively. In so doing, we shall establish precise links with, and/or applications to, the following areas, among others: the Galois structure of the class group and also (units)/(cyclotomic units) for a real, absolutely abelian field; Greenberg's and Vandiver's Conjectures; explicit reciprocity laws and the map '$\mathfrak{s}$' introduced in [So2, So3]; the 'Λ-torsion' submodule of $\mathfrak{X}_\infty$; the Main Conjecture over $\mathbb{Q}$. (These connections are dealt with in successive sections whose content is described in more detail below.) Thus, as well as producing new mathematics, these maps and ideals also provide a unifying approach to several significant areas of the Iwasawa theory of abelian number fields, and one that has so far been largely overlooked. (We also mention in passing a technical advantage of this approach as compared to some others, namely the way it works naturally at the group-ring level. This means

2010 *Mathematics Subject Classification*: Primary 11R18, 11R23; Secondary 11R27, 11R29, 11R42.
Key words and phrases: Iwasawa theory, Kummer theory, cyclotomic fields, abelian fields, cyclotomic units, class groups.

DOI: 10.4064/aa162-2-1

that we never need to decompose using p-adic characters of $\mathrm{Gal}(K/\mathbb{Q})$ in the present paper. Consequently no exceptions or special treatments are necessary for the 'non-semisimple' case, i.e. when p divides $[K:\mathbb{Q}]$.)

In Section 2 of this paper we consider general K/k as above and define the basic Kummer-theoretic pairing between $\mathfrak{X}_\infty$ and norm-coherent sequences of (global) p-units, taking values in $\mathbb{Z}_p[[G_\infty]]$.

In Section 3 and from there on, K is almost always taken to be an (absolutely) abelian field and $k=\mathbb{Q}$. The pairing applied to the above sequence $\{\varepsilon_n\}_{n\geq 0}$ then produces both the map $\mathfrak{d}_\infty$ and the map $\mathfrak{j}_\infty$ (which is its 'mirror-twist'), and hence the ideals $\mathfrak{D}_\infty$ and $\mathfrak{J}_\infty$. The images of the latter in $\mathbb{Z}_p[G_n]$ are ideals denoted $\mathfrak{D}_n$ and $\mathfrak{J}_n$ respectively. We give a concrete description of $\mathfrak{D}_n$ (modulo p^{n+1}) using power-residue symbols. This dovetails perfectly with Thaine's methods to show that $\mathfrak{D}_n$ annihilates the p-part of the class group $\mathrm{Cl}(K_n^+)$ (at least if K_∞/K_n is totally ramified). In this sense it can be seen as an analogue in the plus-part of $\mathbb{Z}_p[G_n]$ of the (p-adified) Stickelberger ideal in the minus-part. We also give an abstract characterisation of $\mathfrak{D}_n$ in terms of the $\mathbb{Z}_p[G_n]$-dual of p-units.

In Section 4 we study the behaviour of $\mathfrak{j}_\infty$ and $\mathfrak{d}_\infty$ when we replace K by a subfield. This contributes to the proof of the main result of this section, namely that the common kernel of $\mathfrak{d}_\infty$ and $\mathfrak{j}_\infty$ is precisely the subgroup $\mathrm{Gal}(M_\infty/N_\infty^0)$ of $\mathfrak{X}_\infty$. Here, N_∞^0 denotes the field obtained by adjoining to K_∞ all p-power roots of those units whose local absolute norms above p are trivial. If K_∞^+ has only one prime above p, this means that Greenberg's conjecture holds for K_∞^+/K^+ iff $\mathfrak{d}_\infty$ and $\mathfrak{j}_\infty$ are injective on the minus part of $\mathfrak{X}_\infty$.

Section 5 gives more precise results in the case $K=\mathbb{Q}$ i.e. $K_n=\mathbb{Q}(\mu_{p^{n+1}})$. We show that $\mathbb{Z}_p[G_n^+]/\mathfrak{D}_n$ is then naturally isomorphic to the *Pontryagin dual* of the p-part of the quotient of units by cyclotomic units in K_n^+. In particular, $\mathfrak{D}_n$ is precisely the Fitting ideal of this dual and also, by a result of Cornacchia and Greither, that of the p-part of $\mathrm{Cl}(K_n^+)$. Further links between $\mathfrak{d}_\infty$ and the Conjectures of Greenberg and Vandiver then follow naturally.

Back in the case of general abelian K, Section 6 starts by considering the restriction of $\mathfrak{j}_\infty$ to the product of inertia subgroups in $\mathfrak{X}_\infty$. An explicit reciprocity law due to Coleman connects this restriction with the projective limit $\mathfrak{s}_\infty$ of certain maps $\mathfrak{s}_n$ defined in terms of p-adic logarithms and complex L-values at $s=1$ for odd Dirichlet characters. (The latter maps were introduced and studied in a more general context in [So2, So3].) This connection has many consequences. For instance, we show that $\mathrm{Gal}(M_\infty/N_\infty^0)$ (already shown to be the common kernel of $\mathfrak{d}_\infty$ and $\mathfrak{j}_\infty$) is also precisely the torsion submodule of $\mathfrak{X}_\infty$ as a module over the Iwasawa algebra Λ. We also deduce a new 4-term exact sequence of torsion Λ-modules, involving both $\mathfrak{D}_\infty$ and $\mathfrak{S}_\infty$ (the image of $\mathfrak{s}_\infty$).

For Section 7 we return to the special case $K=\mathbb{Q}$ of Section 5 and use results of [I1] on the image of the p-adic logarithm to show that $\mathfrak{S}_\infty$ is then precisely the limit of the (p-adified) Stickelberger ideals. The above-mentioned exact sequence then shows that for a given even, non-trivial power ω^j of the Teichmüller character ω, the Main Conjecture over $\mathbb{Q}$ can be rephrased as an equality between the characteristic power series in Λ of the ω^j-components of $\ker(\mathfrak{d}_\infty)$ and $\mathrm{coker}(\mathfrak{d}_\infty)$.

A few previous papers contain constructions having something is common with our $\mathfrak{D}_\infty$, $\mathfrak{d}_\infty$ and $\mathfrak{j}_\infty$. The closest to ours in spirit seems to be [KS], whose aims are, however, much narrower than ours, relating principally to the computation of the structure of certain Iwasawa modules in the case where K is real-quadratic (and $p=3$, assumed not to split in K; see also [Sc] for different but related techniques and computations). In Remark 8 we explain how some of the results in [KS] relate to special cases of those in Sections 3 and 5. Next, if we restrict to $K=\mathbb{Q}$ and let m be an odd integer, then the value of the so-called *Soulé character* $\chi_m:\mathfrak{X}_\infty\to\mathbb{Z}_p$ at $h\in\mathfrak{X}_\infty^-$ turns out to be simply the integral of the $(1-m)$th power of the cyclotomic character with respect to $\mathfrak{d}_\infty(h)$, regarded as a $\mathbb{Z}_p$-valued measure on G_∞. See [IS, p. 54]. It might therefore be interesting to compare the results of our Section 7 with some of those mentioned in [IS, §3]. Finally, we mention that, in a different context and for different purposes, Section 6.2 of [Sh] contains the construction of a map 'ϕ_2' which is related to our $\mathfrak{j}_\infty$ for cyclotomic fields K.

Looking to the future, the first problem is to generalise to any abelian K the results obtained in Sections 5 and 7 for $K=\mathbb{Q}$. Beyond this, one might like to consider abelian extensions K/k with $r:=[k:\mathbb{Q}]>1$. For imaginary quadratic k, elliptic units might substitute for the ε_n's but, in some ways, a stronger analogy with the present case can be expected when k is totally real and the K_n's are CM. The best available substitutes for the ε_n's are then 'Rubin–Stark elements' for K_n^+/k. Unfortunately, not only do these lie *a priori* in a certain rth exterior power of S-units of K_n^+ tensored with $\mathbb{Q}$ but their existence is only conjectural. It is, however, strongly supported by computations (e.g. [RS, §3.5]) which also suggest that for $n\ge 0$ one can use p-units and tensor only with $\mathbb{Z}_{(p)}=\mathbb{Q}\cap\mathbb{Z}_p$. By assuming this, one could mimic some of Sections 2 to 5, replacing $\mathfrak{X}_\infty$ by an appropriate rth exterior power, etc. On the other hand, the map $\mathfrak{s}_n$ is already defined unconditionally in this case in [So2, So3]. To connect it with a generalised $\mathfrak{j}_\infty$, the Congruence Conjecture (formulated in [So3] and tested numerically in [RS]) would be precisely the required substitute for Coleman's reciprocity law mentioned above.

Notation. If F is any field then $\mu(F)$ denotes the group of roots of unity in $F^\times$ with the subgroup $\mu_m(F)$ (resp. $\mu_{p^\infty}(F)$) consisting of those of order dividing $m>0$ (resp. of p-power order). We write ξ_m for the generator $\exp(2\pi i/m)$ of $\mu_m := \mu_m(\mathbb{C})$, and μ_{p^∞} for $\mu_{p^\infty}(\mathbb{C})$. A 'number field' L is always a finite extension of $\mathbb{Q}$ contained it its algebraic closure $\bar{\mathbb{Q}} \subset \mathbb{C}$. We write $\mathcal{O}_L$, $E(L) = \mathcal{O}_L^\times$ and $S_r(L)$ respectively for its ring of integers, its unit group and the set of its places (or prime ideals) dividing an integer $r>1$. If F/F' is an abelian extension of number fields and $\mathfrak{q}$ is a prime ideal of $\mathcal{O}_{F'}$ unramified in F then $\sigma_{\mathfrak{q},F/F'}$ denotes the (unique) Frobenius element attached to $\mathfrak{q}$ in $\mathrm{Gal}(F/F')$.

2. A general construction. Let K/k be any Galois extension of number fields and let K_n and other notations be as above. (Thus $K = K_n$ for $n=-1$ and possibly for some $n \ge 0$.) Throughout this paper we shall write π_n^m for the natural restriction map $G_m \to G_n$ (where $m \ge n \ge -1$) or indeed for the homomorphism of group rings $\mathcal{R}[G_m] \to \mathcal{R}[G_n]$ obtained by $\mathcal{R}$-linear extension, for any commutative ring $\mathcal{R}$. We identify G_∞ with the projective limit of the G_n's with respect to the π_n^m's.

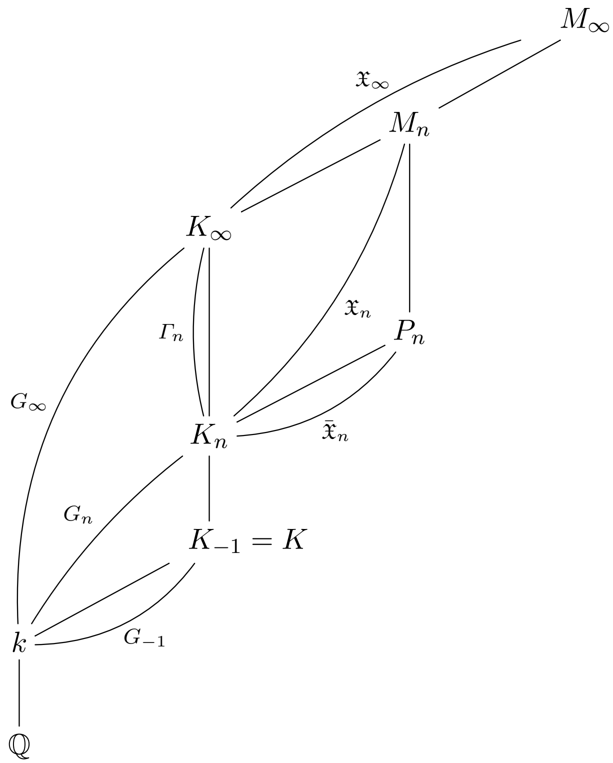
Let P_n denote the maximal abelian extension of K_n of exponent dividing p^{n+1} and unramified outside $S_p(K_n)$. (It contains K_{2n+1} and is finite over K_n.) Let M_n be the maximal abelian pro-p-extension of K_n unramified outside $S_p(K_n)$. Thus M_n contains P_nK_∞ and $M_\infty = \bigcup_{n\ge -1} M_n = \bigcup_{n\ge -1} P_n$. Both M_∞/k and M_n/k (for all n) are (infinite) Galois extensions. We write $\mathfrak{X}_n$ for the profinite group $\mathrm{Gal}(M_n/K_n)$ (so that $\mathfrak{X}_\infty = \varprojlim \mathfrak{X}_n$) and $\bar{\mathfrak{X}}_n$ for the quotient $\mathfrak{X}_n/\mathfrak{X}_n^{p^{n+1}}$ which identifies with $\mathrm{Gal}(P_n/K_n)$ and hence is finite.

Set $\mathcal{V}_n = E_{S_p}(K_n) := \mathcal{O}^\times_{K_n,S_p(K_n)}$ (the group of 'p-units' of K_n) and $\bar{\mathcal{V}}_n := \mathcal{V}_n/\mathcal{V}_n^{p^{n+1}}$. Kummer theory gives a unique, well-defined pairing $\langle\ ,\ \rangle_n : \bar{\mathcal{V}}_n \times \bar{\mathfrak{X}}_n \to \mathbb{Z}/p^{n+1}\mathbb{Z}$ satisfying

$$h(\alpha^{1/p^{n+1}})/\alpha^{1/p^{n+1}} = \zeta_n^{\langle\bar{\alpha},\bar{h}\rangle_n} \qquad \text{for all } \alpha\in\mathcal{V}_n \text{ and } h \in \mathfrak{X}_n$$

where ζ_n denotes $\xi_{p^{n+1}}$ and $\alpha^{1/p^{n+1}}$ is any of the p^{n+1}th roots of α (all lying in P_n). We abbreviate $\mathbb{Z}/p^{n+1}\mathbb{Z}$ to $\mathcal{R}_n$ so that $\langle\ ,\ \rangle_n$ is $\mathcal{R}_n$-bilinear. We shall write $\chi_{\mathrm{cyc}} : G_\infty \to \mathbb{Z}_p^\times$ for the p-cyclotomic character, determined by $g(\zeta) = \zeta^{\chi_{\mathrm{cyc}}(g)}$ for any $g \in G_\infty$ and $\zeta\in\mu_{p^\infty}$, so that $\chi_{\mathrm{cyc}}(\Gamma_n) \subset 1 + p^{n+1}\mathbb{Z}_p$ for all $n \ge 0$. Reducing χ_{cyc} modulo p^{n+1} gives a character $\chi_{\mathrm{cyc},n} : G_n \to \mathcal{R}_n^\times$ for all $n \ge 1$. For any $g\in G_n$ and $h \in \mathfrak{X}_n$ we define $g.h$ to be $\tilde{g}h\tilde{g}^{-1}$ for any lift $\tilde{g}$ of g to $\mathrm{Gal}(M_n/k)$. This determines a left G_n-action on $\mathfrak{X}_n$, hence on $\bar{\mathfrak{X}}_n$, and it follows easily from the definition that

$$(2.1) \qquad \langle g\bar{\alpha}, g.\bar{h}\rangle_n = \chi_{\mathrm{cyc},n}(g)\langle\bar{\alpha},\bar{h}\rangle_n \qquad \text{for all } \alpha\in\mathcal{V}_n,\ h\in\mathfrak{X}_n \text{ and } g \in G_n.$$



Next, $\langle\ ,\ \rangle_n$ gives rise to a group-ring-valued pairing $\{\,,\,\}_n : \bar{\mathcal{V}}_n \times \bar{\mathfrak{X}}_n \to \mathcal{R}_n[G_n]$ defined by

$$\{\bar{\alpha}, \bar{h}\}_n = \sum_{g \in G_n} \langle \bar{\alpha}, g^{-1}.\bar{h}\rangle_n g = \sum_{g \in G_n} \chi_{\mathrm{cyc},n}(g)^{-1} \langle g\bar{\alpha}, \bar{h}\rangle_n g \tag{2.2}$$

for all $\alpha \in \mathcal{V}_n$ and $h \in \mathfrak{X}_n$, which is $\mathcal{R}_n[G_n]$-linear in the second variable and $\mathcal{R}_n[G_n]$-semilinear in the first. More precisely, there is an involutive automorphism ι_n of $\mathcal{R}_n[G_n]$ sending $\sum_{g \in G_n} a_g g$ to $\sum_{g \in G_n} a_g \chi_{\mathrm{cyc},n}(g) g^{-1}$, and equations (2.1) and (2.2) show that

(2.3)

$$\{x\bar{\alpha}, y.\bar{h}\}_n = \iota_n(x) y \{\bar{\alpha}, \bar{h}\}_n \quad \text{for all } \alpha \in \mathcal{V}_n,\ h \in \mathfrak{X}_n \text{ and } x, y \in \mathcal{R}_n[G_n].$$

Clearly, $\iota_n(\{\bar{\alpha}, \bar{h}\}_n)$ is $\mathcal{R}_n[G_n]$-linear in $\bar{\alpha}$ and ι_n-semilinear in $\bar{h}$, and (2.2) gives

$$\iota_n(\{\bar{\alpha}, \bar{h}\}_n) = \sum_{g \in G_n} \langle g^{-1}\bar{\alpha}, \bar{h}\rangle_n g \tag{2.4}$$

If $m \geq n \geq -1$ then $M_m \supset M_n$ and we write ρ_n^m for the restriction $\mathfrak{X}_m \to \mathfrak{X}_n$ and $\bar{\rho}_n^m : \bar{\mathfrak{X}}_m \to \bar{\mathfrak{X}}_n$. We also write N_n^m for the norm map $K_m^\times \to K_n^\times$ inducing $\bar{N}_n^m : \bar{\mathcal{V}}_m \to \bar{\mathcal{V}}_n$, and $\bar{\pi}_n^m$ for the ring homomorphism $\mathcal{R}_m[G_m] \to \mathcal{R}_n[G_n]$

which acts as π_n^m on the elements of G_m and as the reduction $\mathcal{R}_m \to \mathcal{R}_n$ on the coefficients. From (2.1) and the fact that $\chi_{\mathrm{cyc},m}(g) \equiv 1 \pmod{p^{n+1}}$ for all $g \in \mathrm{Gal}(K_m/K_n)$, we deduce:

Proposition 1. *If $m \ge n \ge -1$ then the diagram*

$$\begin{array}{ccc} \bar{\mathcal{V}}_m \times \bar{\mathfrak{X}}_m & \xrightarrow{\{\,,\}_m} & \mathcal{R}_m[G_m] \\ \downarrow{\scriptstyle \bar{N}_n^m \times \bar{\rho}_n^m} & & \downarrow{\scriptstyle \bar{\pi}_n^m} \\ \bar{\mathcal{V}}_n \times \bar{\mathfrak{X}}_n & \xrightarrow{\{\,,\}_n} & \mathcal{R}_n[G_n] \end{array}$$

commutes. ■

Passing to projective limits with respect to $\bar{N}_n^m$, $\bar{\rho}_n^m$ and $\bar{\pi}_n^m$ for $m \ge n \ge 0$, we obtain a pairing

$$\{\,,\,\}_\infty := \varprojlim_{n\ge 0}\{\,,\,\}_n : \varprojlim_{n\ge 0} \bar{\mathcal{V}}_n \times \varprojlim_{n\ge 0} \bar{\mathfrak{X}}_n \to \varprojlim_{n\ge 0} \mathcal{R}_n[G_n].$$

Each of the last three limits above has another interpretation. The third identifies (as a compact topological ring) with the completed group-ring $\Lambda_G := \mathbb{Z}_p[[G_\infty]] = \varprojlim \mathbb{Z}_p[G_n]$. For future reference, it may help to make this identification explicit: Decompose $\bar{\pi}_n^m$ as $\beta_{m,n;n} \circ \phi_n^m$ where $\phi_k^j : \mathcal{R}_j[G_j] \to \mathcal{R}_j[G_k]$ (for $j \ge k \ge 0$) is R_j-linear, acting as π_k^j on the elements of G_j, and $\beta_{i,j;k} : \mathcal{R}_i[G_k] \to \mathcal{R}_j[G_k]$ (for $i \ge j \ge k \ge 0$) simply reduces coefficients modulo p^{j+1}. Then a sequence $(x_n)_n$ of $\varprojlim\ \mathcal{R}_n[G_n]$ gives rise to a sequence $y_k := (\phi_k^j(x_j))_j$ for each $k \ge 0$ lying in the limit $\varprojlim R_j[G_k]$ with respect to the $\beta_{i,j;k}$'s (k fixed). Thus we get a sequence

$$(y_k)_k \in \varprojlim_{k\ge 0}\Big(\varprojlim_{j\ge k}\ \mathcal{R}_j[G_k]\Big) = \varprojlim_{k\ge 0}(\mathbb{Z}_p[G_k]) = \Lambda_G.$$

Conversely, an element $(z_k)_k \in \varprojlim(\mathbb{Z}_p[G_k])$ gives rise to the element $(z_n \pmod{p^{n+1}})_n$ of $\varprojlim R_n[G_n]$. Similar decompositions of $\bar{\rho}_n^m$ and $\bar{N}_n^m$ respectively identify $\varprojlim \bar{\mathfrak{X}}_n$ with

$$\varprojlim_{k\ge 0}\Big(\varprojlim_{j\ge k}\ \mathfrak{X}_k/p^{j+1}\mathfrak{X}_k\Big) = \varprojlim_{k\ge 0}\ \mathfrak{X}_k = \mathfrak{X}_\infty$$

and $\varprojlim \bar{\mathcal{V}}_n$ with

$$\varprojlim_{k\ge 0}\Big(\varprojlim_{j\ge k}\ \mathcal{V}_k/p^{j+1}\mathcal{V}_k\Big) = \varprojlim_{k\ge 0}\ (\mathbb{Z}_p \otimes \mathcal{V}_k) =: \mathcal{V}_\infty.$$

Thus we may regard $\{\,,\,\}_\infty$ as a continuous Λ_G-valued pairing between the compact, topological Λ_G-modules $\mathcal{V}_\infty$ and $\mathfrak{X}_\infty$. If $\iota_\infty = \varprojlim\ \iota_n$ denotes the continuous, involutive automorphism of Λ_G sending $g \in G_\infty$ to $\chi_{\mathrm{cyc}}(g)g^{-1}$, then (2.3) leads to

(2.5)
$$\{x\underline{\alpha}, y.h\}_\infty = \iota_\infty(x)y\{\underline{\alpha}, h\}_\infty \quad \text{for all } \underline{\alpha} \in \mathcal{V}_\infty,\ h \in \mathfrak{X}_\infty \text{ and } x, y \in \Lambda_G.$$

Fix $n \geq -1$ and let $\mathfrak{q}$ be a prime of K_n not dividing p. Then $\mu_{p^{n+1}}$ injects into $(\mathcal{O}_{K_n}/\mathfrak{q})^\times$, so that p^{n+1} divides $N\mathfrak{q}-1$ and the image of $\mu_{p^{n+1}}$ is precisely the subgroup of $((N\mathfrak{q}-1)/p^{n+1})$th powers in $(\mathcal{O}_{K_n}/\mathfrak{q})^\times$. If $\beta \in K_n^\times$ is a local unit at $\mathfrak{q}$ we write $\left\{\frac{\beta}{\mathfrak{q}}\right\}_n$ for the additive p^{n+1}th power-residue symbol mod $\mathfrak{q}$, i.e. the unique element of $\mathcal{R}_n$ satisfying

$$\beta^{(N\mathfrak{q}-1)/p^{n+1}} \equiv \zeta_n^{\{\frac{\beta}{\mathfrak{q}}\}_n} \pmod{\mathfrak{q}}.$$

Now any $\bar{h} \in \bar{\mathfrak{X}}_n$ can be written as $\sigma_{\mathfrak{q},P_n/K_n}$ for some such ideal $\mathfrak{q}$, so the following characterises the pairing $\{\ ,\ \}_n$.

Proposition 2. *Let $n \geq -1$, let $\mathfrak{q}$ be a prime of K_n not dividing p and $\alpha \in \mathcal{V}_n$. Then*

$$\{\bar{\alpha}, \sigma_{\mathfrak{q},P_n/K_n}\}_n = \sum_{g \in G_n} \left\{\frac{\alpha}{g^{-1}(\mathfrak{q})}\right\}_n g, \tag{2.6}$$

$$\iota_n(\{\bar{\alpha}, \sigma_{\mathfrak{q},P_n/K_n}\}_n) = \sum_{g \in G_n} \left\{\frac{g^{-1}(\alpha)}{\mathfrak{q}}\right\}_n g. \tag{2.7}$$

Proof. A well-known argument gives $\langle \bar{\alpha}, \sigma_{\mathfrak{q},P_n/K_n}\rangle_n = \left\{\frac{\alpha}{\mathfrak{q}}\right\}_n$ so the second equation follows from (2.4). Since also $g^{-1}.\sigma_{\mathfrak{q},P_n/K_n} = \sigma_{g^{-1}(\mathfrak{q}),P_n/K_n}$ for all $g \in G_n$, the first follows from (2.2). ∎

3. Cyclotomic units and the annihilation of real classes. We shall suppose henceforth that $k = \mathbb{Q}$ and $\mathrm{Gal}(K/k)$ is abelian so that K_n is an (absolutely) abelian field for all $n \geq -1$. *We shall also suppose $n \in \mathbb{Z}$, $n \geq 0$ unless explicitly stated otherwise.* We write c for the element of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ induced by complex conjugation and also for its restriction to K_n for any n. In the notation of the Introduction, its fixed field is K_n^+, $G_n^+ \cong G_n/\{1,c\}$ and $K_\infty^+ = \bigcup_{n\geq -1} K_n^+$. If M is any module for one of the (commutative) rings $\mathcal{R}_n[G_n]$, $\mathbb{Z}_p[G_n]$, Λ_G, etc., we shall also write M^+ (resp. M^-) for the submodule of M on which c acts trivially (resp. by -1). Since $p \neq 2$, we have $M = M^+ \oplus M^-$, corresponding to the decomposition $m = m^+ + m^- := \frac{1}{2}(1+c)m + \frac{1}{2}(1-c)m$ for each $m \in M$.

For any abelian field F we shall write f_F for its conductor (i.e. the smallest integer $f \geq 1$ such that $F \subset \mathbb{Q}(\mu_f)$), so a prime number r divides f_F iff it ramifies in F. If $F \neq \mathbb{Q}$ then $f \geq 3$ and we write ε_F for the cyclotomic 'unit' attached to F, namely $N_{\mathbb{Q}(\mu_{f_F})/F}(1-\xi_{f_F}) \in \mathcal{O}_F$. We shall need the following result (see e.g. Lemma 2.1 of [So1]).

Lemma 1. *Suppose F, F' are abelian fields with $F \supset F' \supsetneq \mathbb{Q}$. Then*

$$N_{F/F'}\varepsilon_F = \varepsilon_{F'}^x$$

where $x = \prod_r (1 - \sigma_{r,F'/\mathbb{Q}}^{-1}) \in \mathbb{Z}[\mathrm{Gal}(F'/\mathbb{Q})]$, the product running over all *prime numbers r dividing f_F but not $f_{F'}$. Moreover if f_F is a power of some prime number, say r, then $N_{F/\mathbb{Q}}\varepsilon_F = r$ (so ε_F is an r-unit of F). Otherwise $N_{F/\mathbb{Q}}\varepsilon_F = 1$ (so ε_F is a unit of F).* ■

Warning: we shall sometimes be forced to use an additive notation for Galois (group-ring) actions on modules, such as class groups and S-units which are usually written multiplicatively. For instance we might write $x\varepsilon_{F'}$ for $\varepsilon_{F'}^x$ in the lemma above. For brevity, we shall write f_n for f_{K_n} for any $n \geq -1$, so f_n is the l.c.m. of p^{n+1} and f_{-1}. If $n \geq 0$ then $K_n \neq \mathbb{Q}$ and we set

$$\varepsilon_n := N_{K_n/K_n^+}\varepsilon_{K_n} = \varepsilon_{K_n}^{1+c} \in \mathcal{V}_n^+ \quad \text{and} \quad \eta_n := \frac{1}{2} \otimes \varepsilon_n \in (\mathbb{Z}_p \otimes \mathcal{V}_n)^+.$$

(Notice that ε_n coincides with $\varepsilon_{K_n^+}$ provided f_n equals $f_{K_n^+}$. Since $K_n = K_n^+(\mu_p)$, this holds iff $p \mid f_{K_n^+}$, e.g. if $p > 3$ or $n > 0$.) Let $\bar{\eta}_n$ denote the image of η_n in $(\mathbb{Z}_p \otimes \mathcal{V}_n)/p^{n+1}(\mathbb{Z}_p \otimes \mathcal{V}_n)$ which identifies canonically with $\bar{\mathcal{V}}_n$ so that $\bar{\eta}_n = \frac{1}{2}\bar{\varepsilon}_n \in \bar{\mathcal{V}}_n^+$. Taking $x = y = c$ in equation (2.3) gives $\{\bar{\eta}_n, c.\bar{h}\}_n = -\{\bar{\eta}_n, \bar{h}\}_n$ for all $h \in \mathfrak{X}_n$ and hence

$$\{\bar{\eta}_n, \bar{h}\}_n = \{\bar{\eta}_n, \bar{h}^-\}_n \in \mathcal{R}_n[G_n]^- \tag{3.1}$$

so that $\iota_n(\{\bar{\eta}_n, \bar{h}\}_n) \in \mathcal{R}_n[G_n]^+$. The $\mathcal{R}_n$-linear extension of the restriction map $G_n \to G_n^+$ identifies the $\mathcal{R}_n[G_n]^+$ with $\mathcal{R}_n[G_n^+]$ so $\mathrm{Cl}(K_n^+)/p^{n+1}\mathrm{Cl}(K_n^+)$ becomes an $\mathcal{R}_n[G_n]^+$-module.

THEOREM 1. *If $n \geq 0$ and $h \in \mathfrak{X}_n$ then $\iota_n(\{\bar{\eta}_n, \bar{h}\}_n)$ annihilates*

$$\mathrm{Cl}(K_n^+)/p^{n+1}\mathrm{Cl}(K_n^+).$$

(We shall shortly use this to construct explicit annihilators without prior knowledge of $\mathfrak{X}_n$.)

Proof. The theorem will follow from the following, apparently much weaker statement.

CLAIM 1. *Let $\mathfrak{q}$ be a prime of K_n dividing a rational prime q which splits completely in K_n. Then the element $\frac{1}{2}\sum_{g \in G_n}\left\{\frac{g^{-1}(\varepsilon_n)}{\mathfrak{q}}\right\}_n g$ of $\mathcal{R}_n[G_n]^+$ annihilates the image of the class $[\mathfrak{q}^+]$ in $\mathrm{Cl}(K_n^+)/p^{n+1}\mathrm{Cl}(K_n^+)$, where $\mathfrak{q}^+$ is the prime of K_n^+ below $\mathfrak{q}$.*

Assume this for the moment. Let H_n^+ be the maximal unramified abelian extension of K_n^+ of exponent dividing p^{n+1} so that the Artin map defines an isomorphism $\mathrm{Cl}(K_n^+)/p^{n+1}\mathrm{Cl}(K_n^+) \to \mathrm{Gal}(H_n^+/K_n^+)$ sending the class of $\mathfrak{c} \in \mathrm{Cl}(K_n^+)$ to $\sigma_{\mathfrak{c}}$, say. Since $p \neq 2 = [K_n : K_n^+]$, the restriction map $\mathrm{Gal}(K_nH_n^+/K_n) \to \mathrm{Gal}(H_n^+/K_n^+)$ is an isomorphism. Moreover, $K_nH_n^+ \subset P_n$ so the restriction map $\phi : \bar{\mathfrak{X}}_n = \mathrm{Gal}(P_n/K_n) \to \mathrm{Gal}(H_n^+/K_n^+)$ factors through the previous one and is surjective. But $K_nH_n^+/K_n^+$ is abelian so c acts trivially on $\mathrm{Gal}(K_nH_n^+/K_n)$, from which it follows that $\phi(\bar{\mathfrak{X}}_n^-) = \{0\}$ and $\phi(\bar{\mathfrak{X}}_n^+) = \mathrm{Gal}(H_n^+/K_n^+)$. Now choose any $\mathfrak{c} \in \mathrm{Cl}(K_n^+)$ and any element $h \in \mathfrak{X}_n$. Since $\bar{\mathfrak{X}}_n = \bar{\mathfrak{X}}_n^+ \oplus \bar{\mathfrak{X}}_n^-$, Chebotarev's Theorem implies the existence of $\mathfrak{q}$ satisfying the hypotheses of the Claim such that $\sigma^-_{\mathfrak{q},P_n/K_n} = \bar{h}^- \in \bar{\mathfrak{X}}_n^-$ *and* such that $\sigma^+_{\mathfrak{q},P_n/K_n} \in \bar{\mathfrak{X}}_n^+$ maps to $\sigma_{\mathfrak{c}}$ by ϕ, hence so does $\sigma_{\mathfrak{q},P_n/K_n}$. On the one hand it follows from (3.1) and Proposition 2 that

$$\iota_n(\{\bar{\eta}_n, \bar{h}\}_n) = \iota_n(\{\bar{\eta}_n, \sigma_{\mathfrak{q},P_n/K_n}\}_n) = \frac{1}{2}\sum_{g\in G_n}\left\{\frac{g^{-1}(\varepsilon_n)}{\mathfrak{q}}\right\}_n g.$$

On the other hand the properties of the Artin map (and the fact that $\mathfrak{q}^+$ splits in K_n) show that $\mathfrak{c}$ and $[\mathfrak{q}^+]$ have the same image in the quotient $\mathrm{Cl}(K_n^+)/p^{n+1}\mathrm{Cl}(K_n^+)$. Thus the claim implies that $\iota_n(\{\bar{\eta}_n, \bar{h}\}_n)$ annihilates the image of $\mathfrak{c}$ for *all* h and $\mathfrak{c}$.

Our proof of Claim 1 is close to that of Thaine's Theorem as given in [W, §15.2]. The splitting condition implies $q \nmid f_n$ and that $\mu_{p^{n+1}}$ injects into $(\mathcal{O}_{K_n}/\mathfrak{q})^\times = (\mathbb{Z}/q\mathbb{Z})^\times$. In particular, $p^{n+1} \mid (q-1)$, so we may choose a primitive root $t \in \mathbb{Z}$ modulo q such that $t^{(q-1)/p^{n+1}} \equiv \zeta_n \pmod{\mathfrak{q}}$. We denote by $K_{n,q}$ the field $K_n(\xi_q)$, which is easily seen to be unramified over $K_{n,q}^+$ at all finite primes. Since $q \neq 2$ both $K_{n,q}$ and $K_{n,q}^+$ have conductor qf_n. The extension $K_{n,q}/K_n$ is totally tamely ramified at all primes above q, hence so is $K_{n,q}^+/K_n^+$ (and $K_{n,q}/K_n$ is unramified elsewhere). Therefore $\mathbb{Q}(\mu_{f_n})$ and $K_{n,q}^+$ are linearly disjoint over K_n^+ with compositum $\mathbb{Q}(\mu_{qf_n})$. $\mathrm{Gal}(K_{n,q}/K_n)$ identifies by restriction with $\mathrm{Gal}(K_{n,q}^+/K_n^+)$ and is cyclic of degree $q-1$ generated by $\tau : \xi_q \to \xi_q^t$. Set $\varepsilon_{n,q} = N_{\mathbb{Q}(\mu_{qf_n})/K_{n,q}^+}(1 - \xi_q\xi_{f_n})$, which is clearly conjugate over $\mathbb{Q}$ to $\varepsilon_{K_{n,q}^+}$. Lemma 1 implies that it is a unit of $K_{n,q}^+$ and that $N_{K_{n,q}^+/K_n^+}(\varepsilon_{n,q}) = 1$, since $\sigma_{q,K_n^+/\mathbb{Q}} = 1$. By Hilbert's Theorem 90, we can therefore choose $\beta \in K_{n,q}^{+,\times}$ such that $\tau(\beta)/\beta = \varepsilon_{n,q}$. It follows that $\mathrm{ord}_{\mathfrak{R}^+}(\beta) = \mathrm{ord}_{\mathfrak{R}^+}(\tau^i(\beta))$ for any prime $\mathfrak{R}^+$ of $K_{n,q}^+$ and for $i = 1, \ldots, q-1$, so $\mathrm{ord}_{\mathfrak{R}^+}(N_{K_{n,q}^+/K_n^+}\beta) = (q-1)\,\mathrm{ord}_{\mathfrak{R}^+}(\beta)$.

If $\mathfrak{R}^+ \nmid q$ then $\mathfrak{R}^+$ has ramification index 1 or 2 over K_n^+ (the latter case if K_n/K_n^+ is ramified at the prime below $\mathfrak{R}^+$, which requires $\mathfrak{R}^+ \mid p$ and f_n a power of p). We deduce that the principal fractional ideal of K_n^+ generated by $N_{K_{n,q}^+/K_n^+}\beta$ is of the form $\mathfrak{a}I^{(q-1)/2}$ where I is a fractional ideal prime to q and $\mathfrak{a}$ has support above q. For each $g \in G_n$, we write $\mathfrak{Q}_g$ for the unique prime of $K_{n,q}$ dividing $g(\mathfrak{q})$ and $\mathfrak{Q}_g^+$ for the prime of $K_{n,q}^+$ below it (dividing $g(\mathfrak{q}^+)$), so $\mathfrak{Q}_g$ is split over $\mathfrak{Q}_g^+$. We set

$$a_g := \mathrm{ord}_{g(\mathfrak{q}^+)}(\mathfrak{a}) = \frac{1}{q-1}\mathrm{ord}_{\mathfrak{Q}_g^+}(N_{K_{n,q}^+/K_n^+}\beta) = \mathrm{ord}_{\mathfrak{Q}_g^+}(\beta) = \mathrm{ord}_{\mathfrak{Q}_g}(\beta) \in \mathbb{Z}.$$

The stabiliser of $\mathfrak{q}^+$ in G_n is $\{1, c\}$, so in $\mathrm{Cl}(K_n^+)$ we have $\sum_{g\in G_n} a_g g[\mathfrak{q}^+] =$

$2[\mathfrak{a}] = (1-q)[I] \in p^{n+1}\mathrm{Cl}(K_n^+)$. Thus the claim, and hence the theorem, will follow once we have proven that

$$a_g \equiv \left\{\frac{g^{-1}(\varepsilon_n)}{\mathfrak{q}}\right\}_n \pmod{p^{n+1}} \quad \text{for every } g \in G_n. \tag{3.2}$$

Since $\mathrm{ord}_{\mathfrak{Q}_g}(1-\xi_q) = 1$ we can write $\beta = (1-\xi_q)^{a_g}v$ for some $v \in K_{n,q}^\times$, a local unit at $\mathfrak{Q}_g$. Therefore $\varepsilon_{n,q} = ((1-\xi_q^t)/(1-\xi_q))^{a_g}\tau(v)/v = (1+\xi_q+\cdots+\xi_q^{t-1})^{a_g}\tau(v)/v$ and since τ acts trivially on the residue field at $\mathfrak{Q}_g$ by total ramification, we deduce $\varepsilon_{n,q} \equiv t^{a_g} \pmod{\mathfrak{Q}_g}$. On the other hand, $1-\xi_q\xi_{f_n}$ is congruent to $1-\xi_{f_n}$ modulo all primes of $\mathbb{Q}(\mu_{qf_n})$ dividing q, from which it follows easily that $\varepsilon_{n,q} \equiv \varepsilon_n \pmod{\mathfrak{Q}_g}$. Thus $\varepsilon_n \equiv t^{a_g} \pmod{g(\mathfrak{q})}$ so that $g^{-1}(\varepsilon_n)^{(q-1)/p^{n+1}} \equiv t^{a_g(q-1)/p^{n+1}} \equiv \zeta_n^{a_g} \pmod{\mathfrak{q}}$, giving (3.2). ∎

Remark 1. One can in fact deduce Theorem 1 from Theorem 1.3 of [R] (a far more general elaboration of Thaine's method). This is explained briefly below. A minor complication occurs if f_n is a power of p but the main virtue of our *ab initio* proof is its much greater simplicity and directness compared to Rubin's proof of Theorem 1.3. This is natural enough given the specialness of our situation.

In Rubin's Theorem 1.3, take 'K', 'F', 'N' and 'G' in to be $\mathbb{Q}$, K_n^+, p^{n+1} and G_n^+ respectively. Let his 'V' and 'A' be $E(K_n^+)/E(K_n^+)^{p^{n+1}}$ and $\mathrm{Cl}(K_n^+)/p^{n+1}\mathrm{Cl}(K_n^+)$ respectively. Given any $\bar{h} \in \bar{\mathfrak{X}}_n$, we may take '$\alpha$' to be the map $\alpha_{\bar{h}} : v \mapsto \iota_n(\{v,\bar{h}\}_n)$. It follows easily from [R, Lemma 1.6(ii)] that Rubin's 'A'' also equals $\mathrm{Cl}(K_n^+)/p^{n+1}\mathrm{Cl}(K_n^+)$ in this situation. So Rubin's Theorem 1.3 implies that $\iota_n(\{\bar{\varepsilon}_n,\bar{h}\}_n)$ annihilates the latter (giving our Theorem 1) provided ε_n lies in Rubin's '$\mathcal{C}$', i.e. it is a 'special' unit. If f_n is not a power of p then it is certainly a unit and the proof that it is special is similar to that of Rubin's Theorem 2.1. (Take $u := N_{\mathbb{Q}(\xi_{qf_n})/K_n^+\mathbb{Q}(\xi_q)^+}(1-\xi_q\xi_{f_n})$ for each prime $q \neq 2$ splitting in K_n^+.) If f_n is a power of p then ε_n is only a 'special number'—but see [R, Remark 2, p. 513].

Let us define a subset $\bar{\mathfrak{D}}_n$ of $\mathcal{R}_n[G_n]^+$ for $n \geq 0$ by

$$\bar{\mathfrak{D}}_n := \{\iota_n(\{\bar{\eta}_n,\bar{h}\}_n) : \bar{h} \in \bar{\mathfrak{X}}_n\} = \{\iota_n(\{\bar{\eta}_n,\bar{h}\}_n) : \bar{h} \in \bar{\mathfrak{X}}_n^-\}, \tag{3.3}$$

which is clearly an ideal since $\bar{h} \mapsto \iota_n(\{\bar{\eta}_n,\bar{h}\}_n)$ is $\mathcal{R}_n[G_n]$-semilinear with respect to ι_n. Since every $\bar{h} \in \bar{\mathfrak{X}}_n$ is a Frobenius element in P_n/K_n, we can use Proposition 2 to reformulate Theorem 1 as the following remarkable strengthening of Claim 1.

Corollary 1. *If $n \geq 0$ then*

$$\bar{\mathfrak{D}}_n = \left\{\frac{1}{2}\sum_{g\in G_n}\left\{\frac{g^{-1}(\varepsilon_n)}{\mathfrak{q}}\right\}_n g : \mathfrak{q} \textit{ a prime of } K_n \textit{ not dividing } p\right\}. \tag{3.4}$$

Moreover, $\bar{\mathfrak{D}}_n$ is an ideal of $\mathcal{R}_n[G_n]^+$ annihilating $\mathrm{Cl}(K_n^+)/p^{n+1}\mathrm{Cl}(K_n^+)$. ∎

We now pass to limits as $n \to \infty$, as explained in Section 2. If $m \geq n \geq 0$ then Lemma 1 implies $N_n^m \varepsilon_{K_m} = \varepsilon_{K_n}$, so $N_n^m \varepsilon_m = \varepsilon_n$. Thus $\underline{\eta} := (\eta_k)_{k\geq 0}$ lies in $\mathcal{V}_\infty^+$ and we may define a (continuous) Λ_G-linear map $\mathfrak{j}_\infty$ by

$$\mathfrak{j}_\infty : \mathfrak{X}_\infty \to \Lambda_G, \qquad h \mapsto \{\underline{\eta}, h\}_\infty.$$

Since $c\underline{\eta} = \underline{\eta}$, equation (2.5) shows as before that $\mathfrak{j}_\infty$ takes values in Λ_G^- and factors through the projection of $\mathfrak{X}_\infty$ on $\mathfrak{X}_\infty^-$. We write $\mathfrak{J}_\infty$ for the (closed) ideal $\mathrm{im}(\mathfrak{j}_\infty)$ of Λ_G^-.

For each $n \geq 0$, we may also consider the composite map $\phi_n^\infty \circ \mathfrak{j}_\infty : \mathfrak{X}_\infty \to \mathbb{Z}_p[G_n]$ where ϕ_n^∞ is the natural map $\Lambda_G \to \mathbb{Z}_p[G_n]$. Clearly, this factors through the module $\mathfrak{X}_{\infty,\Gamma_n}$ of Γ_n-covariants. Now Γ_n is pro-cyclic, generated by γ_n, say, so that $\mathfrak{X}_{\infty,\Gamma_n} = \mathfrak{X}_\infty/(1-\gamma_n).\mathfrak{X}_\infty$ and a well-known argument shows that $(1-\gamma_n).\mathfrak{X}_\infty$ is the (closure of the) commutator subgroup of $\mathrm{Gal}(M_\infty/K_n)$, namely $\mathrm{Gal}(M_\infty/M_n)$. It follows that the natural map $\mathfrak{X}_{\infty,\Gamma_n} \to \mathfrak{X}_n$ is *injective* with image $\mathfrak{X}_n^0 := \mathrm{Gal}(M_n/K_\infty) \subset \mathfrak{X}_n$. Therefore, $\phi_n^\infty \circ \mathfrak{j}_\infty$ factors through a unique $\mathbb{Z}_p[G_n]$-linear map

$$\mathfrak{j}_n : \mathfrak{X}_n^0 \to \mathbb{Z}_p[G_n]$$

Unravelling the above definitions, that of $\{\,,\,\}_\infty$ and the identification of Λ_G with $\varprojlim \mathcal{R}_n[G_n]$ in Section 2, we obtain the following, more explicit description of $\mathfrak{j}_n(h)$ for any $h \in \mathfrak{X}_n^0$:

$$\mathfrak{j}_n(h) = \lim_{m\to\infty} \phi_n^m(\{\bar{\eta}_m, \bar{h}_m\}_m)$$

where, for each $m \geq n$, h_m is any lift of h to $\mathfrak{X}_m^0$ (the choice does not matter) and $\phi_n^m : \mathcal{R}_m[G_m] \to \mathcal{R}_m[G_n]$ is as in Section 2. Clearly, $\mathfrak{j}_n$ factors through the projection of $\mathfrak{X}_n^0$ on $(\mathfrak{X}_n^0)^- = \mathfrak{X}_n^-$ and $\mathrm{im}(\mathfrak{j}_n) = \phi_n^\infty(\mathfrak{J}_\infty)$ is an ideal of $\mathbb{Z}_p[G_n]^-$, which we shall denote $\mathfrak{J}_n$. We shall examine $\mathfrak{j}_\infty$, $\mathfrak{J}_\infty$, $\mathfrak{j}_n$ and $\mathfrak{J}_n$ more closely in Section 6.

Now let us write $\mathfrak{X}_\infty^\dagger$ for the module $\mathfrak{X}_\infty$ with the Λ_G-action twisted by ι_∞. The composite map $\mathfrak{d}_\infty := \iota_\infty \circ \mathfrak{j}_\infty : \mathfrak{X}_\infty^\dagger \to \Lambda_G$ (taking h to $\iota_\infty(\{\underline{\eta}, h\}_\infty)$) is then continuous and Λ_G-linear and factors through the projection on $(\mathfrak{X}_\infty^-)^\dagger = (\mathfrak{X}_\infty^\dagger)^+$. We set $\mathfrak{D}_\infty := \mathrm{im}(\mathfrak{d}_\infty) = \iota_\infty(\mathfrak{J}_\infty)$, which is a (closed) ideal of Λ_G^+, and for each $n \geq 0$ we write $\mathfrak{D}_n$ for $\mathrm{im}(\phi_n^\infty \circ \mathfrak{d}_\infty)$, i.e.

$$\mathfrak{D}_n = \phi_n^\infty(\mathfrak{D}_\infty) = \{\phi_n^\infty(\mathfrak{d}_\infty(h)) : h \in \mathfrak{X}_\infty^-\} \subset \mathbb{Z}_p[G_n]^+. \tag{3.5}$$

Clearly, $\mathfrak{D}_n$ is an ideal of $\mathbb{Z}_p[G_n]^+$ and the latter will henceforth be identified with $\mathbb{Z}_p[G_n^+]$. Since the map $h \mapsto h|_{P_n}$ sends $\mathfrak{X}_\infty^-$ *onto* $\bar{\mathfrak{X}}_n^-$, the reduction of $\mathfrak{D}_n$ modulo p^{n+1} in $\mathcal{R}_n[G_n]^+$ is the ideal previously denoted $\bar{\mathfrak{D}}_n$. If $\bar{\mathfrak{J}}_n$ denotes the corresponding reduction of $\mathfrak{J}_n$ in $\mathcal{R}_n[G_n]^-$ then clearly $\iota_n(\bar{\mathfrak{J}}_n) = \bar{\mathfrak{D}}_n$, but there appears to be no direct relation between $\mathfrak{J}_n$ and $\mathfrak{D}_n$ themselves.

We now give an abstract description of $\mathfrak{D}_n$. If $h \in \mathfrak{X}_\infty$ then

(3.6)
$$\begin{aligned}(\text{coeff. of } g \text{ in } \phi_n^\infty(\mathfrak{d}_\infty(h))) &= (\text{coeff. of } g \text{ in } \phi_n^\infty(\iota_\infty(\{\underline{\eta}, h\}_\infty))) \\ &= (\text{coeff. of } g \text{ in } \lim_{m\to\infty} \phi_n^m(\iota_m(\{\bar{\eta}_m, h|_{P_m}\}_m))) \\ &= \lim_{m\to\infty} \sum_{\pi_n^m(\tilde{g})=g} \langle \tilde{g}^{-1}\bar{\eta}_m, h|_{P_m}\rangle_m \\ &= \lim_{m\to\infty} \langle g^{-1}\bar{\eta}_n, h|_{P_m}\rangle_m\end{aligned}$$

using (2.4) and the fact $N_n^m \eta_m = \eta_n$. Of course, *any* element α of $\mathbb{Z}_p \otimes \mathcal{V}_n$ gives an element $\bar{\alpha} \in \bar{\mathcal{V}}_m$ for all $m \geq n$ and it is easy to see that for any $h \in \mathfrak{X}_\infty$ the limit

$$\lfloor \alpha, h\rceil_n^\infty := \lim_{m\to\infty} \langle \bar{\alpha}, h|_{P_m}\rangle_m$$

is a well-defined element of $\mathbb{Z}_p$ which is $\mathbb{Z}_p$-bilinear as a function of α and h. So (3.6) gives

$$\phi_n^\infty(\mathfrak{d}_\infty(h)) = \sum_{g\in G_n} \lfloor g^{-1}\eta_n, h\rceil_n^\infty g. \tag{3.7}$$

Proposition 3. *$\mathfrak{D}_n = \{F(\eta_n) : F \in \mathrm{Hom}_{\mathbb{Z}_p[G_n]}((\mathbb{Z}_p \otimes \mathcal{V}_n)^+, \mathbb{Z}_p[G_n])\}$ for all $n \geq 0$.*

Proof. For any $\mathbb{Z}_p[G_n]$-module M, there is a functorial isomorphism from $\mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p)$ to $\mathrm{Hom}_{\mathbb{Z}_p[G_n]}(M, \mathbb{Z}_p[G_n])$ sending f to the map $F : m \mapsto \sum_{g\in G_n} f(g^{-1}m)g$ for all $m \in M$. Thus by (3.5) and (3.7), it suffices to show that any element of $\mathrm{Hom}_{\mathbb{Z}_p}((\mathbb{Z}_p \otimes \mathcal{V}_n)^+, \mathbb{Z}_p)$ is of form $\alpha \mapsto \lfloor \alpha, h\rceil_n^\infty$ for some h in $\mathfrak{X}_\infty^-$. Using the compactness of $\mathfrak{X}_\infty^-$ and the definition of $\lfloor\cdot,\cdot\rceil_n^\infty$, we are reduced to showing the surjectivity of the following composite map for all $m \geq n$:

$$\mathfrak{X}_\infty^- \xrightarrow{a_m} \mathrm{Hom}_{\mathcal{R}_m}(\bar{\mathcal{V}}_m^+, \mathcal{R}_m) \xrightarrow{b_{m,n}} \mathrm{Hom}_{\mathcal{R}_m}((\mathcal{V}_n/\mathcal{V}_n^{p^{m+1}})^+, \mathcal{R}_m)$$

where $a_m(h)$ is the homomorphism $\bar{\alpha} \mapsto \langle \bar{\alpha}, h|_{P_m}\rangle_m$ and $b_{m,n}$ is induced by the restriction of the natural map $\mathcal{V}_n/\mathcal{V}_n^{p^{m+1}} \to \mathcal{V}_m/\mathcal{V}_m^{p^{m+1}} = \bar{\mathcal{V}}_m$ to plus-parts. But it is an easy exercise to see that the latter restriction is injective, and since $\mathcal{R}_m$ is injective as a module over itself, it follows that $b_{m,n}$ is surjective for all $m \geq n$. Furthermore, the surjectivity of a_m for all $m \geq n$ is an immediate consequence of that of $\mathfrak{X}_\infty^- \to \bar{\mathfrak{X}}_m^-$ and Kummer theory, taking into account the fact that $\mathcal{V}_m^{p^{m+1}} = \mathcal{V}_m \cap (K_m^\times)^{p^{m+1}}$. The result follows. ∎

Remark 2. Since $\mathbb{Z}_p \otimes E_{S_p}(K_n^+) = (\mathbb{Z}_p \otimes \mathcal{V}_n)^+$ is a $\mathbb{Z}_p[G_n]$-direct summand of $\mathbb{Z}_p \otimes \mathcal{V}_n$, we can of course replace the former by the latter in the statement of the proposition. If f_n is not a power of p then η_n actually lies in $\mathbb{Z}_p \otimes E(K_n^+)$, which is a $\mathbb{Z}_p$-direct summand of $\mathbb{Z}_p \otimes E_{S_p}(K_n^+)$. By the functoriality mentioned in the proof, it follows that in this case we can also replace $(\mathbb{Z}_p \otimes \mathcal{V}_n)^+$ by $\mathbb{Z}_p \otimes E(K_n^+)$ in the proposition.

For any abelian number field L and any prime number r we shall write $D_r(L/\mathbb{Q})$ for the common decomposition subgroup of $\mathrm{Gal}(L/\mathbb{Q})$ at primes of L above r, and $N_{D_r(K_n/\mathbb{Q})}$ for the norm element $\sum_d d \in \mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$ where d runs through $D_r(K_n/\mathbb{Q})$. If $r \mid f_n$ and f_n is not a prime power (i.e. not a power of p) then Lemma 1 implies $N_{D_r(K_n/\mathbb{Q})}\eta_n = 1$ and Proposition 3 gives

PROPOSITION 4. *Suppose $n \geq 0$ and f_n is not a power of p. Then we have $N_{D_r(K_n/\mathbb{Q})}\mathfrak{D}_n = \{0\}$ for every prime number r dividing f_n (e.g. $r = p$). In particular, $\mathbb{Z}_p[G_n^+]/\mathfrak{D}_n$ is infinite.* ■

Let n_0 be the smallest value of $n \geq 0$ such that K_∞/K_n is totally ramified at one (hence any) prime above p. Thus Γ_{n_0} is precisely the inertia subgroup of $\Gamma_0 \cong \mathbb{Z}_p$ at any prime above p. For each $n \geq -1$ we let L_n denote the maximal unramified abelian p-extension of K_n, so $L_n \subset M_n$ and we write L_∞ for $\bigcup_{n\geq -1} L_n \subset M_\infty$. Then $X_n := \mathrm{Gal}(L_n/K_n)$ and $X_\infty := \mathrm{Gal}(L_\infty/K_\infty)$ are isomorphic via the Artin maps to $A_n := \mathrm{Cl}(K_n)_p$ and $\varprojlim A_m$ (limit with respect to the norm maps N_n^m) respectively, as modules for $\mathbb{Z}_p[G_n]$ and Λ_G. We may identify A_n^+ with $\mathrm{Cl}(K_n^+)_p$ and consider it as a $\mathbb{Z}_p[G_n^+]$-module. If $\mathcal{R}[H]$ is any group-ring, we shall write $I(\mathcal{R}[H])$ for its augmentation ideal. We can now state our main annihilation result.

THEOREM 2. *Let K be as above and $n \geq 0$. Then*

(i) *$\mathfrak{D}_\infty$ annihilates $\varprojlim A_m^+$ (or, equivalently, X_∞^+).*
(ii) *If $n \geq n_0$ then $\mathfrak{D}_n$ annihilates A_n^+ (or, equivalently, X_n^+).*
(iii) *In any case $I(\mathbb{Z}_p[G_n^+])\mathfrak{D}_n$ annihilates A_n^+ (or, equivalently, X_n^+).*

Proof. Suppose $h \in \mathfrak{X}_\infty^\dagger$ and $(\mathfrak{c}_m)_m \in \varprojlim A_m^+$ and set $\mathfrak{d}_\infty(h)(\mathfrak{c}_m)_m = (\mathfrak{b}_m)_m$. By definition $\mathfrak{b}_m = \phi_m^\infty(\iota_\infty(\{\underline{\eta}, h\}_\infty))\mathfrak{c}_m$ where $\phi_m^\infty(\iota_\infty(\{\underline{\eta}, h\}_\infty)) \in \mathbb{Z}_p[G_m^+]$ is congruent modulo p^{m+1} to $\iota_m(\{\bar{\eta}_m, h|_{P_m}\}_m)$. So Theorem 1 implies $\mathfrak{b}_m \in p^{m+1}A_m^+$ for all m. Thus, for any $n \geq 0$, $\mathfrak{b}_n = N_n^m\mathfrak{b}_m \in p^{m+1}A_n^+$ for any $m \geq n$ so $\mathfrak{b}_n = 0$ for all n. This proves part (i). If $n \geq n_0$ then K_∞/K_n is totally ramified above p so the restriction $X_\infty \to X_n$ is surjective and (ii) follows from (i). Part (iii) follows similarly (for $n \leq n_0$) using the fact that the cokernel of $X_\infty \to X_n$ is $\mathrm{Gal}((K_\infty \cap L_n)/K_n) = \mathrm{Gal}(K_{n_0}/K_n)$, on which G_n clearly acts trivially. ■

REMARK 3. To clarify the picture, define integers i_0, f' and m_0 by letting $\mu_{p^\infty}(K_0) = \mu_{p^{i_0+1}}$ and $f_0 = f'p^{m_0+1}$ with $p \nmid f'$. It is easy to see that $m_0 \geq i_0 \geq 0$ and that $K_0 = K_1 = \cdots = K_{i_0}$ while $[K_n : K_0] = p^{n-i_0}$ for $n > i_0$. One shows that $\mathbb{Q}(\mu_{f_0})/K_0$ is unramified above p, hence so is K_{m_0}/K_0. On the other hand, if F is the inertia subfield of K_{m_0} at p, one can show that $K_{m_0} = F_{m_0}$, so $K_\infty/K_{m_0} = F_\infty/F_{m_0}$ is totally ramified above p.

Hence $K_{n_0} = K_{m_0}$. Thus n_0 equals m_0 or 0 according as $m_0 > i_0$ or $m_0 = i_0$, and $[K_{n_0} : K_0] = p^{m_0 - i_0}$ in both cases.

Remark 4. The module $(X_\infty^+)_{\Gamma_n} = X_\infty^+/(1-\gamma_n)X_\infty^+$ is finite since it is a quotient of $(\mathfrak{X}_\infty^+)_{\Gamma_n} \cong \mathfrak{X}_n^{0,+}$, which is finite by Leopoldt's Conjecture for K_n^+ (which holds e.g. by [W, Thm. 5.25].) Suppose for simplicity that $n \geq n_0$. Then the map $X_\infty^+ \to X_n^+$ factors through a surjection $y_n^+ : (X_\infty^+)_{\Gamma_n} \to X_n^+$. Part (i) of Theorem 2 clearly implies that $\mathfrak{D}_n$ annihilates $(X_\infty^+)_{\Gamma_n}$ as a $\mathbb{Z}_p[G_n^+]$-module, which is *a priori* a stronger statement than part (ii) whenever $\ker(y_n^+) =: Y_n^+/(1-\gamma_n)X_\infty^+$ is non-trivial. However, one can show that $\ker(y_n^+) = \{0\}$ if $|S_p(K_n^+)| = 1$ and that $Y_{n+1}^+ = (1 + \gamma_n + \gamma_n^2 + \cdots + \gamma_n^{p-1})Y_n^+$ in general (see e.g. [W, Lemma 13.15]). The latter implies that $\ker(y_{n+1}^+)$ is a quotient of $\ker(y_n^+)$ and hence that $\ker(y_i^+)$ is finite and decreasing in size as $i \to \infty$. In particular, it must stabilise.

Remark 5. If $m \geq n \geq 0$ then the following generalisation of (3.4) can be deduced from (3.6) (for example):

$$\begin{aligned}(3.8)\qquad \beta_{\infty,m;n}(\mathfrak{D}_n) &= \phi_n^m(\bar{\mathfrak{D}}_m)\\ &= \left\{\frac{1}{2}\sum_{g\in G_n}\left\{\frac{g^{-1}(\varepsilon_n))}{\mathfrak{q}}\right\}_m g : \mathfrak{q} \text{ a prime of } K_m \text{ not dividing } p\right\}.\end{aligned}$$

If also $n \geq n_0$ and p^{m+1} kills A_n^+ then the right-hand side of (3.8) above provides an explicit annihilator of A_n^+ in $\mathcal{R}_m[G_n^+]$. (If $n < n_0$ then we may have to multiply by $I(\mathcal{R}_m[G_n^+])$.) One would like to 'let m tend to infinity' and obtain a similar expression for $\mathfrak{D}_n$ itself. Unfortunately, this cannot be done, essentially because the limited splitting of finite primes in the extension K_∞/K_n means that the sequence $\{\sigma_{\mathfrak{q}_m,P_m/K_m}\}_{m\geq n}$ for a 'coherent' sequence of such primes $\mathfrak{q}_m$ (of K_m) can never cohere to give an element of $\mathfrak{X}_\infty$ as $m \to \infty$.

4. Variation of K, the kernels of $\mathfrak{j}_\infty$ and $\mathfrak{d}_\infty$, and Greenberg's Conjecture. First we compare the maps and objects defined above for an abelian field K with the corresponding ones defined identically for a subfield $F \subset K$. To distinguish them we shall sometimes need to include the field in the notation, using a subscript for maps and parentheses for objects. (If omitted, the field is K.) For each $n \geq 0$, and also 'for $n = \infty$', the fields K_n and $M_n(K)$ contain F_n and $M_n(F)$ respectively, so we get continuous restriction maps of Galois groups $\pi_{K_n/F_n} : G_n(K) \to G_n(F)$ and $\mathfrak{r}_{n,K/F} : \mathfrak{X}_n(K) \to \mathfrak{X}_n(F)$. Extending the former by $\mathbb{Z}_p$-linearity, we get ring homomorphisms $\pi_{K_n/F_n} : \mathbb{Z}_p[G_n(K)] \to \mathbb{Z}_p[G_n(F)]$ for every integer $n \geq 0$ whose limit is a continuous homomorphism $\Lambda_G(K) \to \Lambda_G(F)$ extending

π_{K_∞/F_∞} and denoted by the same symbol. The prime factors of f_{F_0} (which include p) coincide with those of f_{F_n} for all $n \geq 0$. For any other prime r, the Frobenius elements $\sigma_{r,F_n/\mathbb{Q}}$ for $n \geq 0$ cohere to give an element $\sigma_{r,F_\infty/\mathbb{Q}}$ of $G_\infty(F)$ satisfying $\chi_{\mathrm{cyc},F}(\sigma_{r,F_\infty/\mathbb{Q}}) = r \in \mathbb{Z}_p^\times$. Define elements $x_{\infty,K/F}$ and $y_{\infty,K/F}$ of $\Lambda_G(F)$ by setting

$$x_{\infty,K/F} := \prod_{\substack{r \mid f_{K_0} \\ r \nmid f_{F_0}}} (1 - \sigma_{r,F_\infty/\mathbb{Q}}^{-1}),$$

$$y_{\infty,K/F} := \iota_{\infty,F}(x_{\infty,K/F}) = \prod_{\substack{r \mid f_{K_0} \\ r \nmid f_{F_0}}} (1 - r^{-1}\sigma_{r,F_\infty/\mathbb{Q}}).$$

For any integer $n \geq 0$, their images in $\mathbb{Z}_p[G_n(F)]$ under $\phi_{n,F}^\infty$ are denoted $x_{n,K/F}$ and $y_{n,K/F}$ respectively and are given by the same products with $\sigma_{r,F_n/\mathbb{Q}}$ replacing $\sigma_{r,F_\infty/\mathbb{Q}}$.

Proposition 5. *Let K, F and notations be as above. We have the equations*

$$\begin{aligned} \pi_{K_\infty/F_\infty} \circ \mathfrak{d}_{\infty,K} &= x_{\infty,K/F}\, \mathfrak{d}_{\infty,F} \circ \mathfrak{r}_{\infty,K/F}, \\ \pi_{K_\infty/F_\infty} \circ \mathfrak{j}_{\infty,K} &= y_{\infty,K/F}\, \mathfrak{j}_{\infty,F} \circ \mathfrak{r}_{\infty,K/F}. \end{aligned} \tag{4.1}$$

Moreover, $\mathfrak{r}_{n,K/F}$ maps $\mathfrak{X}_n(K)^-$ onto $\mathfrak{X}_n(F)^-$ for any $n \geq 0$ and for $n = \infty$.

Proof. For every $n \geq 0$ the norm N_{K_n/F_n} induces a map $\bar{N}_{K_n/F_n} : \bar{\mathcal{V}}_n(K) \to \bar{\mathcal{V}}_n(F)$, and it follows from Lemma 1 (written in an additive notation) that $\bar{N}_{K_n/F_n}\bar{\eta}_{n,K} = x_{n,K/F}\bar{\eta}_{n,F}$. If $h \in M_\infty(K)$ then equation (2.4) gives

$$\begin{aligned} &\pi_{K_n/F_n}(\iota_{n,K}\{\bar{\eta}_{n,K}, h|_{P_n(K)}\}_{n,K}) \\ &\qquad = \sum_{g' \in G_n(F)} \sum_{\substack{g \in G_n(K) \\ \pi_{K_n/F_n}(g) = g'}} \langle g^{-1}\bar{\eta}_{n,K}, h|_{P_n(K)}\rangle_{n,K} g' \\ &\qquad = \sum_{g' \in G_n(F)} \langle g'^{-1}\bar{N}_{K_n/F_n}\bar{\eta}_{n,K}, h|_{P_n(F)}\rangle_{n,F} g' \\ &\qquad = \iota_{n,F}\{x_{n,K/F}\bar{\eta}_{n,F}, h|_{P_n(F)}\}_{n,F}. \end{aligned}$$

Taking the inverse limit over n, using the definition of $\mathfrak{d}_{\infty,F}$ and equation (2.5) then gives

$$\begin{aligned} \pi_{K_\infty/F_\infty}(\mathfrak{d}_{\infty,K}(h)) &= \iota_{\infty,F}\{x_{\infty,K/F}\, \underline{\eta}_F, \mathfrak{r}_{\infty,K/F}(h)\}_{\infty,F} \\ &= x_{\infty,K/F}\, \mathfrak{d}_{F,\infty}(\mathfrak{r}_{\infty,K/F}(h)), \end{aligned}$$

whence the first equation in (4.1). The second follows on applying $\iota_{\infty,F}$ since $\iota_{\infty,F} \circ \pi_{K_\infty/F_\infty} = \pi_{K_\infty/F_\infty} \circ \iota_{\infty,K}$. For the final statement, use the fact that c acts trivially on $\mathrm{coker}(\mathfrak{r}_{n,K/F})$ since the latter is isomorphic to $\mathrm{Gal}((M_n(F)\cap K_n)/F_n)$ and K_n is abelian over $\mathbb{Q}$. ∎

It is a simple exercise to deduce

COROLLARY 2. *For each integer* $n \geq 0$:

(i) $\pi_{K_n/F_n}(\mathfrak{D}_n(K))$ *equals* $x_{n,K/F}\mathfrak{D}_n(F) \subset \mathbb{Z}_p[G_n(F)]^+$.
(ii) $\pi_{K_n/F_n} \circ \mathfrak{j}_{n,K}$ *equals* $y_{n,K/F}\,\mathfrak{j}_{n,F} \circ \mathfrak{r}_{n,F/K}$ *as a map* $\mathfrak{X}_n(K)^- \to \mathbb{Z}_p[G_n(F)]^-$ *and* $\pi_{K_n/F_n}(\mathfrak{J}_n(K))$ *equals* $y_{n,K/F}\mathfrak{J}_n(F) \subset \mathbb{Z}_p[G_n(F)]^-$. ∎

Note that part (i) also follows from Proposition 3 and implies Proposition 4 for $r \neq p$. (Take F to be the splitting field of r in K etc.)

REMARK 6. In contrast to Proposition 4, we shall see later (Corollary 7) that the index of $\mathfrak{J}_n(K)$ in $\mathbb{Z}_p[G_n(K)]^-$ is often (perhaps always) finite for all $n \geq 0$. Nevertheless, Corollary 2 suggests the idea of 'enlarging' both $\mathfrak{D}_n(K)$ and $\mathfrak{J}_n(K)$ by a method similar to that often used for the Stickelberger ideal (see e.g. [Gt, §2]): one should add to each of them ($\mathbb{Z}_p$-multiples of) the images under $\mathrm{cores}_{F_n}^{K_n}$ of the corresponding ideals for all subfields F of K. Here $\mathrm{cores}_{F_n}^{K_n}$ denotes the additive homomorphism from $\mathbb{Z}_p[G_n(F)]$ to $\mathbb{Z}_p[G_n(K)]$ which sends $g \in G_n(F)$ to the sum of its pre-images in $G_n(K)$ under restriction. The same can be done at the infinite level. (Indeed, if K/F is not linearly disjoint from F_∞/F, one should do this first, then get the 'enlarged' ideals at finite levels as images under ϕ_n^∞.) Annihilation statements similar to those of Theorem 2 can be proven for the enlarged versions of $\mathfrak{D}_\infty(K)$ and $\mathfrak{D}_n(K)$ by using those for the original versions for all subfields F of K.

For any number field L, we write $E^0(L)$ for the subgroup of $E(L)$ consisting of those units whose local absolute norms are trivial at all primes dividing our fixed prime p. If L is abelian, this is simply the kernel of $N_{D_p(L/\mathbb{Q})}$ acting on $E(L)$. Now let $N_\infty = N_\infty(K)$ (resp. $N_\infty^0 = N_\infty^0(K)$) denote the infinite abelian extension of K_∞ obtained by adjoining to it all p-power roots of all elements of $E(K_n^+)$ (resp. of $E^0(K_n^+)$) for all $n \geq 0$. Both N_∞^0 and N_∞ are Galois over $\mathbb{Q}$ and it is easy to see that $N_\infty^0 \subset N_\infty \subset M_\infty^-$. (Here, M_∞^- is defined by $\mathrm{Gal}(M_\infty/M_\infty^-) = \mathfrak{X}_\infty^+$ so that $\mathfrak{X}_\infty^-$ maps isomorphically onto $\mathrm{Gal}(M_\infty^-/K_\infty)$.) Since K_n is CM it is well known that $|E(K_n) : \mu(K_n)E(K_n^+)| = 1$ or 2. It follows that we could have used $E(K_n)$ in place of $E(K_n^+)$ (resp. $E^0(K_n)$ in place of $E^0(K_n^+)$) in the definition of N_∞ (resp. of N_∞^0).

THEOREM 3. $\ker(\mathfrak{d}_\infty) = \ker(\mathfrak{j}_\infty) = \mathrm{Gal}(M_\infty/N_\infty^0)$ *as subgroups of* $\mathfrak{X}_\infty$.

Before giving the proof, we deduce a first link with Greenberg's Conjecture for the extension K_∞^+/K^+, i.e. the statement that $|A_n^+|$ is bounded as $n \to \infty$ or, equivalently, that X_∞^+ is finite. Proposition 2 of [Gn] shows that this is also equivalent to the triviality of A_∞^+ where A_∞ denotes the *direct* limit of the A_n's as $n \to \infty$ with respect to the maps coming from extension of ideals. Now, Kummer theory gives a non-degenerate, Galois-equivariant pairing

$$\mathrm{Gal}(M_\infty/N_\infty) \times A_\infty \to \mu_{p^\infty}. \tag{4.2}$$

(This follows from [W, pp. 294–295]. See also [I2, Thm. 14] using roots of p-units and p-class groups instead.) Hence Greenberg's Conjecture for K_∞^+/K^+ is also equivalent to $\mathrm{Gal}(M_\infty/N_\infty)^- = \{0\}$, i.e. $M_\infty^- = N_\infty$.

Corollary 3. *Suppose* $|S_p(K_{n_0}^+)| = 1$. *Then* $N_\infty^0 = N_\infty$ *and*

$$\begin{aligned}\ker(\mathfrak{d}_\infty) \cap (\mathfrak{X}_\infty^\dagger)^+ = (\ker(\mathfrak{j}_\infty) \cap \mathfrak{X}_\infty^-)^\dagger = (\mathrm{Gal}(M_\infty/N_\infty)^-)^\dagger \\ \cong \mathrm{Hom}_{\mathbb{Z}_p}(A_\infty^+, \mathbb{Q}_p/\mathbb{Z}_p)\end{aligned}$$

as Λ_G^+-*modules. In particular, Greenberg's Conjecture holds for* K_∞^+/K^+ *if and only if* $\mathfrak{d}_\infty$ *is injective on* $(\mathfrak{X}_\infty^\dagger)^+$ (*or, equivalently,* $\mathfrak{j}_\infty$ *on* $\mathfrak{X}_\infty^-$).

Proof. By total ramification, $|S_p(K_{n_0}^+)| = 1$ is equivalent to $|S_p(K_n^+)| = 1$ for all $n \geq 0$. This implies $D_p(K_n^+/\mathbb{Q}) = G_n^+$ so that $E(K_n^+)^2 \subset E^0(K_n^+)$ for all $n \geq 0$, and hence $N_\infty^0 = N_\infty$. The second equality now follows from the theorem, as does the first (since $\mathfrak{X}_\infty^- = (\mathfrak{X}_\infty^\dagger)^+$ as groups). The isomorphism follows from the above pairing and the rest is a direct consequence. ∎

In Section 6, equation (6.12) will show that $\ker(\mathfrak{j}_\infty) \cap \mathfrak{X}_\infty^- = \mathrm{Gal}(M_\infty^-/N_\infty^0)$ contains a specific submodule which is non-trivial (and infinite) whenever $|S_p(K_{n_0}^+)| > 1$, regardless of Greenberg's Conjecture. Nevertheless, Theorem 7(iii) will show that $\ker(\mathfrak{j}_\infty)$ is still as small as it could possibly be for a map $\mathfrak{X}_\infty \to \Lambda_G$, namely it consists precisely of the 'Λ_Γ-torsion' (which includes $\mathfrak{X}_\infty^+$).

Proof of Theorem 3. The first equality follows from the injectivity of the involution ι_∞. For any abelian field F (not necessarily contained in K) we temporarily denote by $B_\infty(F)$ the fixed field of $\ker(\mathfrak{j}_{\infty,F})$ acting on $M_\infty(F)$. The second equality thus amounts to $B_\infty(K) = N_\infty^0(K)$, which we now prove.

Lemma 2. *Let* F *be any abelian field,* $n \geq 0$ *and write* $E_{S_p}(F_n^+)$ *as a left* $\mathbb{Z}[G_n(F)]$-*module* (*under multiplication*). *Then the field* $B_\infty(F)$ *is obtained by adjoining to* F_∞ *the following subset of* $M_\infty(F)^-$:

$$\mathcal{S}_\infty(F) := \{\alpha^{1/p^m} : \alpha \in I(\mathbb{Z}[G_n(F)])\varepsilon_n(F) \text{ and } m, n \geq 0\}.$$

Furthermore, $I(\mathbb{Z}[G_n(F)])\varepsilon_n(F)$ *is contained in* $E^0(F_n^+)$.

Proof. If $h \in \mathfrak{X}_{\infty,F}$, then $\mathfrak{j}_{\infty,F}(h) = 0$ iff $\{\bar\eta_n(F), h|_{P_n(F)}\}_{n,F} = 0$ for all $n \geq 0$. This is equivalent to h fixing all conjugates of $\varepsilon_n(F)^{1/p^{n+1}}$ over $\mathbb{Q}$ for all $n \geq 0$ and hence to h fixing all conjugates of $\varepsilon_n(F)^{1/p^m}$ for all $m, n \geq 0$, since $\varepsilon_n(F) = N_{\mathrm{Gal}(F_m/F_n)}\varepsilon_m(F)$ for $m \ge n$. This shows that $B_\infty(F)$ is obtained by adjoining the larger set with $I(\mathbb{Z}[G_n(F)])$ replaced by $\mathbb{Z}[G_n(F)]$ in the definition of $\mathcal{S}_\infty(F)$. The fact that this gives the same field follows from the relation $\varepsilon_n(F) \equiv (N_{\mathrm{Gal}(F_{m+n}/F_n)} - p^m)\varepsilon_{m+n}(F) \pmod{(K_{m+n}^\times)^{p^m}}$ (whenever $m \ge 0$) since $N_{\mathrm{Gal}(F_{m+n}/F_n)} - p^m \in I(\mathbb{Z}[G_{m+n}(F)])$. This proves the first statement. For the second, if f_{F_n} is a power of p then $|S_p(F_n^+)| = 1$, so the assertion follows from $\varepsilon_n(F) \in E_{S_p}(F_n^+)$. Otherwise, Lemma 1 gives $\varepsilon_{F_n} \in E(F_n)$ and easily implies $N_{D_p(F_n/\mathbb{Q})}\varepsilon_{F_n} = 1$. Hence $\varepsilon_n(F) \in E^0(F_n^+)$. ∎

The norm relations mean that the index $|E^0(K_n^+) : I(\mathbb{Z}[G_n(K)])\varepsilon_n(K)|$ is usually infinite for every $n \ge 0$. So the equality $B_\infty(K) = N_\infty^0(K)$ does not follow immediately from the above lemma. We also need the less obvious

LEMMA 3. *Suppose F is a subfield of K_n for some $n \ge 0$. Then $B_\infty(K)$ contains $B_\infty(F)$.*

Proof. First, the map $\mathfrak{j}_{\infty,K_n} : \mathfrak{X}_\infty(K_n) \to \Lambda_G(K_n)$ is formally identical to $\mathfrak{j}_{\infty,K} : \mathfrak{X}_\infty(K) \to \Lambda_G(K)$. Thus $B_\infty(K) = B_\infty(K_n)$ and, replacing K by K_n, we may reduce to the case $F \subset K$. We need to prove that $h \in \ker(\mathfrak{j}_{\infty,K})$ implies that $\mathfrak{r}_{\infty,K/F}(h)$ fixes $B_\infty(F)$, i.e. $\mathfrak{j}_{\infty,F} \circ \mathfrak{r}_{\infty,K/F}(h) = 0$. But if $h \in \ker(\mathfrak{j}_{\infty,K})$ then (4.1) implies $y_{\infty,K/F}\, \mathfrak{j}_{\infty,F} \circ \mathfrak{r}_{\infty,K/F}(h) = 0$ so it suffices to show that $y_{\infty,K/F}$ is a non-zero-divisor of $\Lambda_G(F)$. This follows from the fact that its image $y_{n,K/F}$ is a non-zero-divisor of $\mathbb{Z}_p[G_n(F)]$ for all $n \ge 0$ (e.g. because it divides $\prod_r (1 - r^{-a_{r,n}}) \in \mathbb{Z}_p \setminus \{0\}$ where $a_{r,n} \ge 1$ is the order of $\sigma_{r,F_n/\mathbb{Q}}$ in $G_n(F)$). ∎

By Lemma 2, the following defines a $\mathbb{Z}[G_n(K)]$-submodule of $E^0(K_n^+)$ for each $n \ge 0$:

$$C_n^0(K) := \sum_{F \subset K_n} I(\mathbb{Z}[G_n(F)])\varepsilon_n(F)$$

(where F ranges over the (finitely many) subfields of K_n). Now consider the subfield $K_\infty(\tilde{\mathcal{S}}_\infty(K))$ of $N_\infty^0(K)$ obtained by adjoining to K_∞ the set

$$\tilde{\mathcal{S}}_\infty(K) := \{\beta^{1/p^m} : \beta \in C_n^0(K) \text{ and } m, n \ge 0\}.$$

Lemma 2 for $F = K$ and the obvious containment $\mathcal{S}_\infty(K) \subset \tilde{\mathcal{S}}_\infty(K)$ imply $B_\infty(K) \subset K_\infty(\tilde{\mathcal{S}}_\infty(K))$. The reverse inclusion follows from the fact that every element of $\tilde{\mathcal{S}}_\infty(K)$ is a product of elements of the sets $\mathcal{S}_\infty(F) \subset B_\infty(F)$ for varying $F \subset K_n$ and n, and hence lies in $B_\infty(K)$, by Lemma 3. Thus $K_\infty(\tilde{\mathcal{S}}_\infty(K)) = B_\infty(K)$ and to prove Theorem 3 it only remains to show that the inclusion $K_\infty(\tilde{\mathcal{S}}_\infty(K)) \subset N_\infty^0(K)$ is an equality. But in view of the definitions of $\tilde{\mathcal{S}}_\infty(K)$ and $N_\infty^0(K)$, this is an easy deduction from

LEMMA 4. *The index $|E^0(K_n^+) : C_n^0(K)|$ is finite for all $n \ge 0$.*

Proof. This is a variant of the proof that the (full) group of cyclotomic units of an abelian field is of finite index in its unit group, so we leave out some details. It suffices to show that the natural inclusion of $\mathbb{C}\otimes C_n^0(K)$ in $\mathbb{C}\otimes E^0(K_n^+)$ is an equality. We consider these as nested $\mathbb{C}[G_n]$-submodules of $\mathbb{C}\otimes E(K_n^+)$ and show that $r_\chi := \dim_{\mathbb{C}}(e_\chi(\mathbb{C}\otimes C_n^0(K)))$ is at least $r'_\chi := \dim_{\mathbb{C}}(e_\chi(\mathbb{C}\otimes E^0(K_n^+)))$ for every (irreducible) complex character χ of G_n (whose idempotent in $\mathbb{C}[G_n]$ is e_χ). Dirichlet's Theorem shows that the map

$$\lambda : E(K_n^+)\to \mathbb{C}[G_n], \qquad \varepsilon \to \sum_{g\in G_n} \log|g(\varepsilon)|g^{-1},$$

extends to a $\mathbb{C}[G_n]$-isomorphism $\lambda_{\mathbb{C}} : \mathbb{C}\otimes E(K_n^+) \to I(\mathbb{C}[G_n])^+$. Since $\mathbb{C}\otimes E^0(K_n^+)$ is the kernel of $N_{D_p(K_n/\mathbb{Q})}$ acting on $\mathbb{C}\otimes E(K_n^+)$, it follows that $r'_\chi = 0$ unless $\chi(c)=1$ and $\chi(D_p(K_n/\mathbb{Q}))\neq\{1\}$, in which case $r'_\chi = 1$. So it suffices to show that $e_\chi(\mathbb{C}\otimes C_n^0(K))\neq\{0\}$ in this latter case. Fix such a χ and let F be the (real) subfield of K_n fixed by $\ker(\chi)$ so p does not split completely in F. We can also regard χ as an even, non-trivial Dirichlet character modulo its conductor $f=f_F$ such that $\chi(\bar p)\neq 1$ if $p\nmid f$. Choose also $g_0\in G_n$ such that $\chi(g_0)\neq 1$ so that $z_\chi := e_\chi(1\otimes(1-g_0)\varepsilon_n(F))$ lies in $e_\chi(\mathbb{C}\otimes C_n^0(K))$. If $p\mid f$ then Lemma 1 shows that $N_{F_n^+/F}\varepsilon_n(F)=\varepsilon_F$ and a calculation gives

$$\begin{aligned}\lambda_{\mathbb{C}}(z_\chi) &= [K_n : F_n^+](1-\chi(g_0)) \sum_{\substack{a=1\\(a,f)=1}}^{f} \log|1-\xi_f^a|\chi^{-1}(\bar a)\\ &= [K_n : F_n^+](\chi(g_0)-1)\tau(\chi^{-1})L(1,\chi)\end{aligned}$$

where $L(s,\chi)$ is the complex (primitive) L-function and $\tau(\chi^{-1})$ is the Gauss sum attached to χ^{-1}. (See, for example, Theorem 4.9 and the preceding pages in [W].) If $p\nmid f$ then $N_{F_n^+/F}\varepsilon_n(F) = (1-\sigma_{p,F/\mathbb{Q}}^{-1})\varepsilon_F$, giving an extra factor of $(1-\chi^{-1}(\bar p))$ in the second two members above. In either case the third member is a product of nonzero terms, so $z_\chi\neq 0$. ∎

This completes the proof of Theorem 3. ∎

5. The case $K=\mathbb{Q}$: the ideals $\mathfrak{D}_n$ and the map $\mathfrak{d}_\infty$. If $K=\mathbb{Q}$ then $K_n=\mathbb{Q}(\mu_{p^{n+1}})$, $f_n=p^{n+1}$, $n_0=i_0=0$ and K_n (resp. K_n^+) has a unique prime ideal dividing p, generated by $1-\zeta_n$ (resp. by ε_n). We abbreviate $E_{S_p}(K_n^+)$ and $E(K_n^+)$ to $\tilde E_n$ and E_n respectively. We write $\tilde C_n$ for the $\mathbb{Z}[G_n^+]$-submodule of $\tilde E_n$ generated by ε_n and C_n for $\tilde C_n\cap E_n$. (This is the group of cyclotomic units of K_n^+ and coincides with the group $C_n^0(K)$ defined above, in this case.) Since $\tilde E_n=\tilde C_nE_n$, the natural map $E_n/C_n\to\tilde E_n/\tilde C_n$ is an isomorphism. It follows from e.g. Theorem 8.2 of [W] that $\tilde E_n/\tilde C_n$ is finite, of cardinality a power of 2 times $|\mathrm{Cl}(K_n^+)|$. In particular, $\tilde C_n$ has the same $\mathbb{Z}$-rank as $\tilde E_n$, namely $[K_n^+:\mathbb{Q}]$, so that $\tilde C_n$ is $\mathbb{Z}[G_n^+]$-*free* with basis $\{\varepsilon_n\}$.

Since p is odd, $\mathbb{Z}_p \otimes \tilde{E}_n$ is $\mathbb{Z}_p$-torsionfree so may be regarded as a submodule of $\mathbb{Q}_p \otimes \tilde{E}_n$. We may also regard $\mathbb{Z}_p \otimes \tilde{C}_n$ as a $\mathbb{Z}_p[G_n^+]$-free submodule with basis $\{\eta_n\}$ and spanning $\mathbb{Q}_p \otimes \tilde{E}_n$ over $\mathbb{Q}_p$. It follows that there exists a (unique) fractional ideal J_n of $\mathbb{Q}_p[G_n^+]$ (by which we mean a $\mathbb{Z}_p[G_n^+]$-submodule of $\mathbb{Z}_p$-rank equal to $|G_n^+|$) such that the map $J_n \to \mathbb{Z}_p \otimes \tilde{E}_n$ sending j to $j\eta_n$ is an isomorphism. For each $x \in \mathbb{Z}_p[G_n^+]$ we let $t_{n,x} \in \mathrm{Hom}_{\mathbb{Z}_p}((\mathbb{Z}_p \otimes \tilde{E}_n)/(\mathbb{Z}_p \otimes \tilde{C}_n), \mathbb{Q}_p/\mathbb{Z}_p)$ be the homomorphism sending the class of $j\eta_n$ to that of the coefficient of 1 in xj, for all $j \in J_n$. If H is any abelian group and M any $\mathbb{Z}_p[H]$-module, we shall sometimes write the Pontryagin dual $\mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ as $M^\vee$ for brevity. We emphasise that it is always endowed with the $\mathbb{Z}_p[H]$-action for which $h.f$ is the homomorphism $f \circ h$ (*not* $f \circ h^{-1}$ as in [KS] etc.) for any $h \in H$ and $f \in M^\vee$.

THEOREM 4. *Suppose $K = \mathbb{Q}$, $n \geq 0$ and notations are as above. Then*

$$t_n : \mathbb{Z}_p[G_n^+]/\mathfrak{D}_n \to \mathrm{Hom}_{\mathbb{Z}_p}((\mathbb{Z}_p \otimes \tilde{E}_n)/(\mathbb{Z}_p \otimes \tilde{C}_n), \mathbb{Q}_p/\mathbb{Z}_p),$$
$$x \bmod \mathfrak{D}_n \mapsto t_{n,x},$$

is a well-defined isomorphism of $\mathbb{Z}_p[G_n^+]$-modules.

Proof. The injection $(\mathbb{Z}_p \otimes \tilde{E}_n)/(\mathbb{Z}_p \otimes \tilde{C}_n) \to (\mathbb{Q}_p[G_n^+]/\mathbb{Z}_p[G_n^+])$ sending the class of $j\eta_n$ to that of j (for $j \in J_n$) induces a surjection from $(\mathbb{Q}_p[G_n^+]/\mathbb{Z}_p[G_n^+])^\vee$ to $((\mathbb{Z}_p \otimes \tilde{E}_n)/(\mathbb{Z}_p \otimes \tilde{C}_n))^\vee$. On the other hand, it is easy to see that every element of $(\mathbb{Q}_p[G_n^+]/\mathbb{Z}_p[G_n^+])^\vee$ sends the class of $y \in \mathbb{Q}_p[G_n^+]$ to that of the coefficient of 1 in xy for some fixed $x \in \mathbb{Z}_p[G_n^+]$. It follows that the map $\tilde{t}_n$ from $\mathbb{Z}_p[G_n^+]$ to $((\mathbb{Z}_p \otimes \tilde{E}_n)/(\mathbb{Z}_p \otimes \tilde{C}_n))^\vee$ sending x to $t_{n,x}$ is surjective. It is easy to check that $\tilde{t}_n$ is $\mathbb{Z}_p[G_n^+]$-linear so it only remains to prove that $\mathfrak{D}_n = \ker(\tilde{t}_n)$. But $\ker(\tilde{t}_n)$ is precisely the set $\{x \in \mathbb{Z}_p[G_n^+] : xj \in \mathbb{Z}_p[G_n^+]$ for all $j \in J_n\}$. It follows easily that $\mathrm{Hom}_{\mathbb{Z}_p[G_n^+]}(\mathbb{Z}_p \otimes \tilde{E}_n, \mathbb{Z}_p[G_n^+]) = \mathrm{Hom}_{\mathbb{Z}_p[G_n]}((\mathbb{Z}_p \otimes \mathcal{V}_n)^+, \mathbb{Z}_p[G_n])$ is precisely the set of maps $j\eta_n \mapsto xj$ for $x \in \ker(\tilde{t}_n)$. Taking $j = 1$, Proposition 3 implies $\mathfrak{D}_n = \ker(\tilde{t}_n)$, as required. ∎

From the above—and elementary properties of duals etc.—we deduce:

COROLLARY 4. *If $K = \mathbb{Q}$ and $n \geq 0$ then*

(i) $\mathbb{Z}_p[G_n^+]/\mathfrak{D}_n$ *is finite and* $|\mathbb{Z}_p[G_n^+]/\mathfrak{D}_n| = |\mathbb{Z}_p \otimes (\tilde{E}_n/\tilde{C}_n))| = |A_n^+|$.
(ii) $\mathfrak{D}_n$ *is precisely the* $\mathbb{Z}_p[G_n^+]$*-annihilator of* $(\mathbb{Z}_p \otimes (\tilde{E}_n/\tilde{C}_n))^\vee \cong (\mathbb{Z}_p \otimes (E_n/C_n))^\vee$, *hence also of* $\mathbb{Z}_p \otimes (\tilde{E}_n/\tilde{C}_n) \cong \mathbb{Z}_p \otimes (E_n/C_n)$.
(iii) $\mathfrak{D}_n$ *is precisely the* (*initial*) $\mathbb{Z}_p[G_n^+]$*-Fitting ideal of* $(\mathbb{Z}_p \otimes (\tilde{E}_n/\tilde{C}_n))^\vee \cong (\mathbb{Z}_p \otimes (E_n/C_n))^\vee$. ∎

REMARK 7. Part (ii) above combines with Theorem 2(ii) to show that

$$\mathrm{Ann}_{\mathbb{Z}_p[G_n^+]}(\mathbb{Z}_p \otimes (E_n/C_n)) \subset \mathrm{Ann}_{\mathbb{Z}_p[G_n^+]}(A_n^+). \tag{5.1}$$

This may be compared with the statement of Thaine's Theorem in [W, Thm. 15.2] (as well as the general results of [R] already cited). The former is essentially (5.1) generalised to allow any real abelian field F in place of K_n^+ *but* also restricted to p (possibly 2) not dividing $[F:\mathbb{Q}]$. Since G_n^+ is cyclic, Fitting ideals of $\mathbb{Z}_p[G_n^+]$-modules and their duals coincide (this follows from Propositions 1 and 4 of [MW, Appendix]) so we have the interesting equalities

$$\mathfrak{D}_n = \mathrm{Fitt}_{\mathbb{Z}_p[G_n^+]}(\mathbb{Z}_p \otimes (E_n/C_n)) = \mathrm{Fitt}_{\mathbb{Z}_p[G_n^+]}(A_n^+) \tag{5.2}$$

where the first follows from (iii) above and the second from [CG, Thm. 1].

It is not clear to the author whether to expect generalisations of (5.1) and/or the equalities between each pair of the three members in (5.2), when E_n is replaced by $E(F)$ for arbitrary real, abelian F and C_n by a suitably defined group of cyclotomic units $C(F)$. (Before even considering the first equality in (5.2) one would have to enlarge $\mathfrak{D}_n$, perhaps as in Remark 6.) However, our approach certainly suggests that it might be more natural to consider the *Pontryagin dual* of $\mathbb{Z}_p \otimes (E(F)/C(F))$. This might even be necessary in (5.2) when $\mathrm{Gal}(F/\mathbb{Q})$ is not p-cyclic. Note also that the case $p \nmid [F:\mathbb{Q}]$ may not be indicative here. Not only is $\mathbb{Z}_p \otimes (E(F)/C(F))$ then $\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]$-isomorphic to its dual, but its Fitting ideal and annihilator coincide since $\mathbb{Z}_p \otimes E(F)$ is cyclic over $\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]$ in this case.

It is easy to check that the following diagram commutes for all $m \ge n \ge 0$:

$$\begin{array}{ccc}
\mathbb{Z}_p[G_m^+]/\mathfrak{D}_m & \xrightarrow{\ \cong\ } & \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p \otimes (\tilde{E}_m/\tilde{C}_m), \mathbb{Q}_p/\mathbb{Z}_p) \\
\downarrow & & \downarrow \\
\mathbb{Z}_p[G_n^+]/\mathfrak{D}_n & \xrightarrow{\ \cong\ } & \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p \otimes (\tilde{E}_n/\tilde{C}_n), \mathbb{Q}_p/\mathbb{Z}_p)
\end{array}$$

Here, the horizontal isomorphisms are (essentially) t_m and t_n, the left-hand vertical map is the natural surjection and the right-hand map is induced by the natural map $(\tilde{E}_n/\tilde{C}_n) \to (\tilde{E}_m/\tilde{C}_m)$. It follows that the transition maps on the right-hand side are also surjections. (This can also be seen by the injectivity of $(\tilde{E}_n/\tilde{C}_n) \to (\tilde{E}_m/\tilde{C}_m)$, which follows in turn from the $\mathbb{Z}[G_m^+]$-freeness of $\tilde{C}_m$.) Passing to inverse limits, we obtain continuous Λ_G^+-isomorphisms

$$\Lambda_G^+/\mathfrak{D}_\infty \cong \varprojlim_{n\ge 0}(\mathbb{Z}_p[G_n^+]/\mathfrak{D}_n) \cong \varprojlim_{n\ge 0}\big((\mathbb{Z}_p \otimes (\tilde{E}_n/\tilde{C}_n))^\vee\big). \tag{5.3}$$

(The first follows from compactness arguments.) Finally, the right-hand side of (5.3) is easily seen to be isomorphic to $\mathrm{Hom}_{\mathbb{Z}}(\tilde{E}(K_\infty^+)/\tilde{C}(K_\infty^+), \mathbb{Q}_p/\mathbb{Z}_p)$ where $\tilde{E}(K_\infty^+) := \bigcup_{n\ge 0}\tilde{E}_n$ and $\tilde{C}(K_\infty^+) := \bigcup_{n\ge 0}\tilde{C}_n$.

Remark 8. We point out the connections mentioned in the Introduction between our results and those of [KS]. Let K be real quadratic so that $G_n^+ = G_0^+ \times \mathrm{Gal}(K_n^+/K_0^+)$ and let χ denote non-trivial character of $\mathrm{Gal}(K/\mathbb{Q})$ inflated to G_0^+. The aim of Kraft and Schoof is to study modules for such K which are denoted by them 'A_n' and 'C_n' and are essentially the χ-components of our A_n^+ and $\big(\mathbb{Z}_p \otimes (E(K_n^+)/C(K_n^+))\big)^\vee$ respectively. Now, using our Corollary 1, one can obtain a precise relation between the χ-component of our $\bar{\mathfrak{D}}_n$ and the denominator on the right-hand side of the last equation on p. 141 of [KS], with $k = n+1$. (Use the description of their f_r given on p. 144, not the vaguer one on p. 140.) Combining this relation with [KS, Prop. 2.5] gives a sort of mod-p^k analogue of our Proposotion 3. The above-mentioned equation itself may be compared with our Theorem 4 modulo p^k (where, of course, $K = \mathbb{Q}$), and the first statement of [KS, Theorem 2.4] with our equation (5.3). The ideal I in this statement is essentially the χ-component of our $\mathfrak{D}_\infty$. Note that the Galois action on Pontryagin duals defined in [KS] must be changed to ours to make it consistent with their own identification at the end of the proof of [KS, Thm. 2.4].

Vandiver's Conjecture for p states that $A_0^+ = \{0\}$ or, equivalently, $A_n^+ = \{0\}$ for all $n \geq 0$. (For the non-trivial implication, use [W, Thm. 10.4].) Thus, Vandiver's Conjecture strengthens Greenberg's Conjecture for K_∞^+/K^+ and each corresponds to certain properties of $\mathfrak{d}_\infty$:

Proposition 6. *Suppose* $K = \mathbb{Q}$.

(i) *The following are equivalent:*

(a) *Greenberg's Conjecture holds for* K_∞^+/K^+,
(b) $\mathfrak{d}_\infty$ *is injective on* $(\mathfrak{X}_\infty^\dagger)^+$,
(c) $\mathrm{coker}(\mathfrak{d}_\infty)$ (*i.e.* $\Lambda_G^+/\mathfrak{D}_\infty$) *is finite.*

(ii) *The following are equivalent:*

(a) *Vandiver's Conjecture holds for* p,
(b) $\mathfrak{d}_\infty$ *is an isomorphism from* $(\mathfrak{X}_\infty^\dagger)^+$ *to* Λ_G^+,
(c) $\mathfrak{d}_\infty$ *is surjective* (*i.e.* $\mathfrak{D}_\infty = \Lambda_G^+$).

Proof. In part (i), the equivalence (a)$\Leftrightarrow$(b) is from Corollary 3. For (a)$\Leftrightarrow$(c), Greenberg's Conjecture is equivalent to the boundedness of $|\mathbb{Z}_p[G_n^+]/\mathfrak{D}_n|$ by Corollary 4(i). Now use (5.3) noting that the transition maps in the limits are surjective. The equivalence (a)$\Leftrightarrow$(c) of part (ii) is proved in a similar way. The implication (b)$\Rightarrow$(c) in (ii) is trivial and (c)$\Rightarrow$(b) follows from the same implication in (i). ∎

Remark 9. The argument (a)$\Leftrightarrow$(c) in (i) shows that if Greenberg's Conjecture holds then $|\Lambda_G^+/\mathfrak{D}_\infty| = |X_\infty^+|$ (since then $X_\infty^+ \cong A_n^+$ for all $n \gg 0$).

The kernel and cokernel of $\mathfrak{d}_\infty$ can also be related without Greenberg's Conjecture, using instead the Main 'Conjecture' of Iwasawa theory over $\mathbb{Q}$ (a theorem, of course!). See Theorem 9.

6. Inertia subgroups, the map $\mathfrak{s}_\infty$ and Λ_Γ-torsion. When j_∞ is restricted to the product of inertia subgroups in $\mathfrak{X}_\infty$ we shall see that it is given by a limit of certain rather explicit p-adic maps $\mathfrak{s}_n$ as $n \to \infty$. These are specialisations of the map $\mathfrak{s}_{F/k,S}$ defined in [So3, §2.4] for any abelian extension of number fields F/k with F of CM-type and k totally real, and for any finite set S of places of k containing $S^0(F/k)$ (i.e. the infinite ones and those ramified in F). We start by giving the particularly simple definition of $\mathfrak{s}_{F/k,S}$ in the relevant case, namely $k = \mathbb{Q}$ and F any imaginary abelian field.

For each irreducible, complex character $\chi \in \widehat{\mathrm{Gal}(F/\mathbb{Q})}$ we let the S-truncated L-function $L_{F/\mathbb{Q},S}(s,\chi)$ be the function defined by the Euler product $\prod_{q \notin S}(1-q^{-s}\chi(\sigma_{q,F/\mathbb{Q}}))^{-1}$ for $\Re(s) > 1$, meromorphically continued to $\mathbb{C}$. Let

$$a^-_{F/\mathbb{Q},S} := \frac{i}{\pi} \sum_{\substack{\chi \in \widehat{\mathrm{Gal}(F/\mathbb{Q})} \\ \chi\,\mathrm{odd}}} L_{F/\mathbb{Q},S}(1,\chi) e_{\chi^{-1}} \in \mathbb{C}[\mathrm{Gal}(F/\mathbb{Q})]^-$$

where $e_{\chi^{-1}}$ denotes the idempotent $|\mathrm{Gal}(F/\mathbb{Q})|^{-1} \sum_{g \in \mathrm{Gal}(F/\mathbb{Q})} \chi^{-1}(g) g^{-1}$ of $\mathbb{C}[\mathrm{Gal}(F/\mathbb{Q})]$. We shall also write $a^{-,*}_{F/\mathbb{Q},S}$ for the image of $a^-_{F/\mathbb{Q},S}$ under the $\mathbb{C}$-linear involution of $\mathbb{C}[\mathrm{Gal}(F/\mathbb{Q})]$ sending $g \in \mathrm{Gal}(F/\mathbb{Q})$ to g^{-1}.

For *any* integer $l \geq 1$ we write $G(l)$ for $\mathrm{Gal}(\mathbb{Q}(\mu_l)/\mathbb{Q}) = \{\sigma_{a,l} : (a,l) = 1\}$ where $\sigma_{a,l}(\xi_l) = \xi_l^a$. If $l \geq 3$ we may take $F = \mathbb{Q}(\mu_l)$ and S to be $S_l := \{\infty\} \cup S_l(\mathbb{Q})$. In this case we record here (for use in Section 7) a relatively simple 'equivariant functional equation' relating $a^{-,*}_{\mathbb{Q}(\mu_l)/\mathbb{Q},S_l}$ to the Stickelberger elements defined for any integer $r > 1$ by

$$\theta_{\mathbb{Q}(\mu_r)/\mathbb{Q},S_r} := \sum_{\chi \in \widehat{G(r)}} L_{\mathbb{Q}(\mu_r)/\mathbb{Q},S_r}(0,\chi) e_{\chi^{-1}} \tag{6.1}$$

$$= -\sum_{\substack{a=1 \\ (a,r)=1}}^{r} \left(\frac{a}{r} - \frac{1}{2}\right) \sigma_{a,r}^{-1} \in \mathbb{Q}[G(r)]^-. \tag{6.2}$$

(For (6.2) see e.g. [W, p. 95].)

Proposition 7. *Suppose $l \geq 3$ and for each $r \mid l$, let $\mathrm{cores}^{\mathbb{Q}(\mu_l)}_{\mathbb{Q}(\mu_r)} : \mathbb{C}[G(r)] \to \mathbb{C}[G(l)]$ be the corestriction map defined as in Remark* 6. *Then*

$$a^{-,*}_{\mathbb{Q}(\mu_l)/\mathbb{Q},S_l} = \frac{1}{l} \sum_{\substack{r \mid l \\ r \neq 1}} \mathrm{cores}^{\mathbb{Q}(\mu_l)}_{\mathbb{Q}(\mu_r)}(\mathcal{A}_r \theta_{\mathbb{Q}(\mu_r)/\mathbb{Q},S_r}) \tag{6.3}$$

where $\mathcal{A}_r$ denotes the 'equivariant Gauss sum'

$$\sum_{g \in G(r)} g(\xi_r) g = \sum_{\substack{a=1 \\ (a,r)=1}}^{r} \xi_r^a \sigma_{a,r} \in \mathbb{C}[G(r)].$$

Proof. We sketch two alternatives. The first uses the much more general equivariant functional equation coming from Theorems 2.2 and 2.1 of [So2]: In the notations of that paper, take $k = \mathbb{Q}$ and $\mathfrak{m}$ to be the cycle $(l\mathbb{Z})\infty$. Then, equations (13) and (9) ibid., with $s = 1$ and 0 respectively, show that

$$a^{-,*}_{\mathbb{Q}(\mu_l)/\mathbb{Q},S_l} = \frac{1}{l}\,\frac{1-c}{2}\Phi_{\mathfrak{m}}(0)^*$$

(if $l = 2\tilde{l}$ with $\tilde{l}$ odd, we need also (8) ibid.). The reader may check that equation (15) ibid. with $s = 0$ then gives (6.3) above.

Alternatively, and more directly, let χ be any odd character of $G(l)$ linearly extended to $\mathbb{C}[G(l)]$, let $\hat{\chi}$ be the associated *primitive* Dirichlet character modulo f_χ (which divides l) and let T_χ denote the set of primes dividing l but not f_χ. One shows that if r is of the form $f_\chi \prod_{q\in T} q$ for some $T \subset T_\chi$ then

$$\chi(\mathrm{cores}^{\mathbb{Q}(\mu_l)}_{\mathbb{Q}(\mu_r)}(\mathcal{A}_r)) = \frac{\varphi(l)}{\varphi(r)} \prod_{q\in T}(-\hat{\chi}(q))\tau(\hat{\chi})$$

(where $\tau(\hat{\chi})$ is the usual Gauss sum and φ is Euler's function) and otherwise $\chi(\mathrm{cores}^{\mathbb{Q}(\mu_l)}_{\mathbb{Q}(\mu_r)}(\mathcal{A}_r)) = 0$. Using this fact and some further manipulation, one can evaluate χ(right-hand side of (6.3)) in terms of $L(0, \hat{\chi}^{-1})$. The usual functional equation for $L(s, \hat{\chi})$ then shows that it is precisely equal to $(i/\pi)L_{\mathbb{Q}(\mu_l)/\mathbb{Q},S_l}(1, \chi) = \chi$(left-hand side of (6.3)). Since χ was an arbitrary odd character and both sides of (6.3) lie in $\mathbb{C}[G(l)]^-$, the result follows. ∎

We now specialise to the case $F = K_n$ for $n \geq 0$ for our fixed but general abelian field K. We shall always take S to be $S^0(K_n/\mathbb{Q})$, which equals $S_{f_n} \cup \{\infty\}$ and contains p. It is independent of $n \geq 0$ so we drop it from the notation. It follows easily from the definition that $a^-_{K_n/\mathbb{Q}}$ is the image of $a^-_{\mathbb{Q}(\mu_{f_n})/\mathbb{Q}}$ under the restriction map $\mathbb{C}[\mathrm{Gal}(\mathbb{Q}(\mu_{f_n})/\mathbb{Q})] \to \mathbb{C}[G_n]$ coming from the inclusion $K_n \subset \mathbb{Q}(\mu_{f_n})$. In principle, a rather complicated formula for $a^-_{K_n/\mathbb{Q}}$ then follows from (6.3). A much simpler one—which is also better suited to present purposes—is easily obtained by the same process from a different formula for $a^-_{\mathbb{Q}(\mu_{f_n})/\mathbb{Q}}$ proved in [So3, Lemma 7.1(ii)]. (Note: $a^-_{\mathbb{Q}(\mu_{f_n})/\mathbb{Q}}$ would there be denoted $a^-_{K_{f_n}/\mathbb{Q},S}$.) The reader may check that this results in the following expression, which shows in particular that $a^-_{K_n/\mathbb{Q}}$ lies in $K_n[G_n]^-$:

$$(6.4)\qquad a^-_{K_n/\mathbb{Q}} = \frac{1}{2f_n}(1-c)\sum_{g\in G_n} g\Big(\mathrm{Tr}_{\mathbb{Q}(\mu_{f_n})/K_n}\Big(\frac{\xi_{f_n}}{1-\xi_{f_n}}\Big)\Big)g^{-1}.$$

For each $\mathfrak{P} \in S_p(K_n)$ we shall write $K_{n,\mathfrak{P}}$ for the (abstract) completion of K_n at $\mathfrak{P}$. We shall usually regard the canonical embedding $i_{\mathfrak{P}} : K_n \to K_{n,\mathfrak{P}}$

as an inclusion. We write $K_{n,p}$ for the product $\prod_{\mathfrak{P}\in S_p(K_n)} K_{n,\mathfrak{P}}$ in which we shall usually consider K_n to be diagonally embedded (via $\prod_{\mathfrak{P}} i_{\mathfrak{P}}$). Let $\pi_{\mathfrak{P}}$ denote the projection from $K_{n,p}$ to $K_{n,\mathfrak{P}}$ and $U^1(K_{n,p})$ the group of 'principal p-semilocal units of K_n', i.e. $\prod_{\mathfrak{P}\in S_p(K_n)} U^1(K_{n,\mathfrak{P}}) \subset K_{n,p}$. It is a multiplicative pro-p group under the product topology. (*Warning:* we shall sometimes write it additively.) $K_{n,p}$ is equipped with a natural G_n-action extending that on K_n (see e.g. [So3, §2.3]) and such that $U^1(K_{n,p})$ identifies as a finitely generated, topological $\mathbb{Z}_p[G_n]$-module with the Sylow pro-p subgroup of $(\mathcal{O}_{K_n} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times$.

We fix once and for all an algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and an embedding $j : \bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_p$ whose restriction to K_n extends to an embedding $j : K_{n,\mathfrak{P}^0} \to \bar{\mathbb{Q}}_p$ for some $\mathfrak{P}^0 \in S_p(K_n)$. We shall also write j for the composite $j \circ \pi_{\mathfrak{P}^0}$ taking $K_{n,p}$ onto $\overline{j(K_n)}$ (topological closure). We write $\log_p$ for the p-adic logarithm defined by the usual convergent series on $U^1(\overline{j(K_n)})$ and on $U^1(K_{n,\mathfrak{P}})$ for any $\mathfrak{P}$.

Given any $u \in U^1(K_{n,p})$ we set

$$\lambda_{p,n}(u) := \sum_{g\in G_n} \log_p(j(gu))g^{-1} \in \overline{j(K_n)}[G_n].$$

Applying j coefficientwise to $a^{-,*}_{K_n/\mathbb{Q}}$, we get an element $j(a^{-,*}_{K_n/\mathbb{Q}})$ of $j(K_n)[G_n]^-$ and a map

$$\mathfrak{s}_n : U^1(K_{n,p}) \to \mathbb{Q}_p[G_n]^-, \qquad u \mapsto j(a^{-,*}_{K_n/\mathbb{Q}})\lambda_{p,n}(u).$$

This is the map $\mathfrak{s}_{K_n/\mathbb{Q},S^0(K_n/\mathbb{Q})}$ of [So3] (taking 'τ_1' to be $1 \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$). The fact that $\mathfrak{s}_n(u)$ has coefficients in $\mathbb{Q}_p$ and is independent of j therefore follows from [So3, Prop. 2.16] (or, in our special case, from (6.5) below). It clearly is $\mathbb{Z}_p[G_n]$-linear on $U^1(K_{n,p})$ and so factors through the projection on $U^1(K_{n,p})^-$. Assuming u lies in $U^1(K_{n,p})^-$, the formula (6.4) gives

$$\text{(6.5)}\quad \mathfrak{s}_n(u) = \sum_{g\in G_n}\sum_{\mathfrak{P}\in S_p(K_n)} \frac{1}{f_n}\mathrm{Tr}_{K_{n,\mathfrak{P}}/\mathbb{Q}_p}\left(\mathrm{Tr}_{\mathbb{Q}(\mu_{f_n})/K_n}\left(\frac{\xi_{f_n}}{1-\xi_{f_n}}\right)\log_p(\pi_{\mathfrak{P}}(g^{-1}u))\right)g.$$

The next result gives the properties of $\mathfrak{s}_n$ that are crucial to the present paper. For each $\mathfrak{P} \in S_p(K_n)$ we write $(\cdot,\cdot)_{K_{n,\mathfrak{P}},p^{n+1}}$ for the Hilbert symbol on $K^\times_{n,\mathfrak{P}} \times K^\times_{n,\mathfrak{P}}$ with values in $\mu_{p^{n+1}}$ (regarded as a subgroup of $K^\times_{n,\mathfrak{P}}$) defined as in [Ne]. This gives rise to an $\mathcal{R}_n$-valued pairing $[\cdot,\cdot]_{\mathfrak{P},n}$ on $K^\times_{n,\mathfrak{P}} \times K^\times_{n,\mathfrak{P}}$ defined by

$$\zeta_n^{[\alpha,\beta]_{\mathfrak{P},n}} = (\alpha,\beta)_{K_{n,\mathfrak{P}},p^{n+1}}$$

and hence, letting $\mathfrak{P}$ vary, to a pairing

$$[\cdot,\cdot]_n : K_{n,p}^\times \times K_{n,p}^\times \to \mathcal{R}_n, \qquad (\alpha,\beta) \mapsto \sum_{\mathfrak{P}\in S_p(K_n)} [\pi_{\mathfrak{P}}(\alpha), \pi_{\mathfrak{P}}(\beta)]_{\mathfrak{P},n}.$$

Properties of the Hilbert symbol give the following (see [So3, eq. (18)]):

$$[g\alpha, g\beta]_n = \chi_{\mathrm{cyc},n}(g)[\alpha,\beta]_n \quad \text{for all } \alpha,\beta \in K_{n,p}^\times \text{ and } g \in G_n. \tag{6.6}$$

Now write $\mu_{p^\infty}(K_{n,p})$ for $\prod_{\mathfrak{P}\in S_p(K_n)} \mu_{p^\infty}(K_{n,\mathfrak{P}}) = \mathrm{tor}_{\mathbb{Z}_p}(U^1(K_{n,p}))$, and $\mathfrak{S}_n$ for the image of $\mathfrak{s}_n$ in $\mathbb{Q}_p[G_n]^-$ (denoted $\mathfrak{S}_{K_n/k,S^0(K_n/\mathbb{Q})}$ in [So3]).

Proposition 8. *For all $n \geq 0$ we have*

(i) $\ker(\mathfrak{s}_n|_{U^1(K_{n,p})^-}) = \mu_{p^\infty}(K_{n,p})^-$.

(ii) $\mathfrak{S}_n$ *is contained in* $\mathbb{Z}_p[G_n]^-$ *with finite index and*

$$\mathfrak{s}_n(u) \equiv -\frac{1}{2}\sum_{g\in G_n} [\varepsilon_n, g^{-1}u]_n g \pmod{p^{n+1}} \quad \textit{for all } u \in U^1(K_{n,p})^-. \tag{6.7}$$

Proof. Part (i) follows easily from the fact that that $a^{-,*}_{K_n/\mathbb{Q}}$ is a unit of $\bar{\mathbb{Q}}[G_n]^-$ (since $\chi(a^{-,*}_{K_n/\mathbb{Q}}) = (i/\pi)L_{K_n/\mathbb{Q}}(1,\chi) \neq 0$ for all odd $\chi \in \hat{G}_n$) or as a special case of [So3, Prop. 2.17] with $d = [k:\mathbb{Q}] = 1$. The latter also shows $\mathbb{Q}_p\mathfrak{S}_n = \mathbb{Q}_p[G_n]^-$. It remains to show $\mathfrak{S}_n \subset \mathbb{Z}_p[G_n]^-$ and (6.7). But it is easy to see that these amount precisely to the case of the 'Congruence Conjecture' of [So3, §3] with data $K_n/\mathbb{Q}$, $S = S^0(K_n/\mathbb{Q}) = S^1(K_n/\mathbb{Q})$, p and n, which was proven in [So3, Theorem 4.3]. In particular, (6.7) follows from equations (24) and (20) of [So3], taking $d = 1$ and $\tau_1 = 1$ and noting that '$\eta_{K_n^+/\mathbb{Q},S^1(K_n/\mathbb{Q})}$' equals our $-\frac{1}{2}\otimes\varepsilon_n$. (This last equation is established in the case $K_n = \mathbb{Q}(\mu_{f_n})$ during the course of the proof of Theorem 4.3 in [So3, pp. 177–178]. The general case follows on applying $N_{\mathbb{Q}(\mu_{f_n})^+/K_n^+}$ to both sides and using [So3, Prop. 5.7].) ∎

Remark 10. For those unfamiliar with [So3], the following may shed some light on (6.7).

(i) The right-hand side is G_n-equivariant in $u \in U^1(K_{n,p})$ and lies in the *minus*-part of $\mathcal{R}_n[G_n]$. (Use (6.6) with $g = c$.) Thus (6.7) would read '$0 \equiv 0$' for $u \in U^1(K_{n,p})^+$.

(ii) If $K = \mathbb{Q}$ then $K_n = \mathbb{Q}(\mu_{p^{n+1}})$ and $\varepsilon_n = (1-\zeta_n)(1-\zeta_n^{-1})$. In this case the reader can easily check that (6.7) follows immediately from (6.5) and the explicit reciprocity law of Artin and Hasse [AH]. Coleman's generalisation of this law in [C] is an essential ingredient in the proof of Theorem 4.3 of [So3] which establishes (6.7) in the general case.

For each $m \geq n \geq 0$, the norm $N_n^m : K_m^\times \to K_n^\times$ is the restriction of the map $K_{m,p}^\times \to K_{n,p}^\times$ which is given by the products of local norms (and also denoted N_n^m). Proposition 5.5 of [So3] gives a commuting diagram

$$\begin{array}{ccc} U^1(K_{m,p}) & \xrightarrow{\mathfrak{s}_m} & \mathbb{Z}_p[G_m]^- \\ {\scriptstyle N_n^m}\downarrow & & \downarrow{\scriptstyle \pi_n^m} \\ U^1(K_{n,p}) & \xrightarrow{\mathfrak{s}_n} & \mathbb{Z}_p[G_n]^- \end{array}$$

We write U^1_∞ for the projective limit of the groups $U^1(K_{n,p})$ for all $n \geq 0$ with respect to the maps N_n^m, considered as a natural Λ_G-module. The maps $(\mathfrak{s}_n)_{n\geq 0}$ give rise to a Λ_G-linear map $\mathfrak{s}_\infty : U^1_\infty \to \Lambda_G^-$ factoring through $U^{1,-}_\infty$. The image of $\mathfrak{s}_\infty$ is precisely $\mathfrak{S}_\infty := \varprojlim \mathfrak{S}_n$ considered as a submodule of Λ_G^-. (This follows from the finiteness of $\mu_{p^\infty}(K_{n,p})$ and Lemma 15.16 of [W] or the fact that $N_n^m : \mu_{p^\infty}(K_{m,p}) \to \mu_{p^\infty}(K_{n,p})$ is surjective for all $m \geq n \geq 0$.) So, by Proposition 8(i) we obtain an exact sequence of Λ_G-modules

$$0 \to \mu^-_{\mathrm{local},\infty} \hookrightarrow U^{1,-}_\infty \xrightarrow{\mathfrak{s}_\infty} \Lambda_G^- \to \Lambda_G^-/\mathfrak{S}_\infty \to 0 \tag{6.8}$$

where $\mu_{\mathrm{local},\infty}$ denotes the projective limit of $\mu_{p^\infty}(K_{n,p})$ with respect to N_n^m for all $m \geq n \geq 0$.

On the other hand, for each $\mathfrak{P} \in S_p(K_n)$ the reciprocity map of local class field theory restricts to a map $\psi_{n,\mathfrak{P}}$ from $U^1(K_\mathfrak{P})$ onto the inertia subgroup above $\mathfrak{P}$ in $\mathfrak{X}_n$, so that the product $\prod_{\mathfrak{P}\in S_p(K_n)} \psi_{n,\mathfrak{P}}$ defines a $\mathbb{Z}_p[G_n]$-*equivariant* map $\psi_n : U^1(K_{n,p}) \to \mathfrak{X}_n$ with image $\mathrm{Gal}(M_n/L_n)$. Global class field theory (and the fact that K_n is CM) show that $\ker(\psi_n|_{U^1(K_{n,p})^-}) = \mu_{p^\infty}(K_n) \subset \mu_{p^\infty}(K_{n,p})^-$ so we get an exact sequence of $\mathbb{Z}_p[G_n]$-modules

$$0 \to \mu_{p^\infty}(K_n) \hookrightarrow U^1(K_{n,p})^- \xrightarrow{\psi_n} \mathfrak{X}_n^- \to X_n^- \to 0$$

for each $n \geq 0$. Furthermore, if $m \geq n$, one has $\rho_n^m \circ \psi_m = \psi_n \circ N_n^m$ so, on passing to limits, we obtain a Λ_G-linear map $\psi_\infty : U^1_\infty \to \mathfrak{X}_\infty$. It is easy to see that $\psi_\infty(U^{1,-}_\infty) = \mathrm{Gal}(M_\infty/L_\infty)^-$, so we get an exact sequence of Λ_G-modules

$$0 \to \mu_{\mathrm{global},\infty} \hookrightarrow U^{1,-}_\infty \xrightarrow{\psi_\infty} \mathfrak{X}^-_\infty \to X^-_\infty \to 0 \tag{6.9}$$

where $\mu_{\mathrm{global},\infty}$ denotes the projective limit of $\mu_{p^\infty}(K_n)$ with respect to N_n^m for all $m \geq n \geq 0$.

THEOREM 5. *The following diagram commutes:*

$$\begin{array}{ccc} U^1_\infty & & \\ & \searrow^{\mathfrak{s}_\infty} & \\ {\scriptstyle \psi_\infty}\downarrow & & \Lambda_G^- \\ & \nearrow_{\mathfrak{j}_\infty} & \\ \mathfrak{X}_\infty & & \end{array}$$

Proof. Suppose $m \geq 0$ and let $v = (v_{\mathfrak{P}})_{\mathfrak{P}\in S_p(K_m)}$ be an element of $U^1(K_{m,p})$. Then

$$\begin{aligned}\zeta_m^{\langle\bar\varepsilon_m,\overline{\psi_m(v)}\rangle_m} &= \psi_m(v)(\varepsilon_m^{1/p^{m+1}})/\varepsilon_m^{1/p^{m+1}}\\ &= \prod_{\mathfrak{P}\in S_p(K_m)} \big(\psi_{m,\mathfrak{P}}(v_{\mathfrak{P}})(\varepsilon_m^{1/p^{m+1}})/\varepsilon_m^{1/p^{m+1}}\big)\\ &= \prod_{\mathfrak{P}\in S_p(K_m)} (v_{\mathfrak{P}},\varepsilon_m)_{K_{m,\mathfrak{P}},p^{m+1}}\\ &= \prod_{\mathfrak{P}\in S_p(K_m)} (\varepsilon_m, v_{\mathfrak{P}})^{-1}_{K_{m,\mathfrak{P}},p^{m+1}} = \zeta_m^{-[\varepsilon_m,v]_m}\end{aligned}$$

(where the third equality comes from the definition of the Hilbert symbol $(\cdot,\cdot)_{K_{m,\mathfrak{P}},p^{m+1}}$ that we are using and the fourth from one of its basic properties). Thus $\frac{1}{2}\langle\bar\varepsilon_m,\overline{\psi_m(v)}\rangle_m \equiv -\frac{1}{2}[\varepsilon_m,v]_m$ modulo p^{m+1} and it follows from (2.2) and (6.7) that

$$\{\bar\eta_m,\overline{\psi_m(u)}\}_m \equiv \mathfrak{s}_m(u) \pmod{p^{m+1}} \quad \forall u\in U^1(K_{m,p})^-. \tag{6.10}$$

Hence if $\underline{u} = (u_m)_{m\geq 0}$ lies in $U_\infty^{1,-}$, we find

$$\begin{aligned}\phi_n^m(\{\bar\eta_m,\overline{\psi_m(u_m)}\}_m) &\equiv \pi_n^m(\mathfrak{s}_m(u_m))\\ &\equiv \mathfrak{s}_n(u_n) \pmod{p^{m+1}} \quad \text{for all } m\geq n\geq 0.\end{aligned}$$

Fixing n and letting $m\to\infty$ gives $\phi_n^\infty(\mathfrak{j}_\infty\circ\psi_\infty(\underline{u})) = \mathfrak{s}_n(u_n) = \phi_n^\infty(\mathfrak{s}_\infty(\underline{u}))$ in $\mathbb{Z}_p[G_n]^-$. Since n is arbitrary and both $\mathfrak{j}_\infty\circ\psi_\infty$ and $\mathfrak{s}_\infty$ factor through $U_\infty^{1,-}$, the result follows. ∎

Considering images and using $\mathfrak{d}_\infty = \iota_\infty\circ\mathfrak{j}_\infty$ and Theorem 2(i), we deduce:

COROLLARY 5.

(i) $\mathfrak{J}_\infty \supset \mathfrak{S}_\infty$ *and* $\mathfrak{D}_\infty \supset \iota_\infty(\mathfrak{S}_\infty)$.

(ii) $\iota_\infty(\mathfrak{S}_\infty)$ *annihilates* $\varprojlim A_m^+$ *(or, equivalently,* X_∞^+*).* ∎

(For comments on part (ii) in the case $K=\mathbb{Q}$, see Remark 17.) Let $U^1(K_{n,p})^0 := \bigcap_{m\geq n} N_n^m(U^1(K_{m,p})) \subset U^1(K_{n,p})$. For any $u\in U^1(K_{n,p})^- \cap U^1(K_{n,p})^0$ a compactness argument shows that we can find $\underline{u} = (u_m)_m \in U_\infty^{1,-}$ with $u_n = u$. Then $\mathfrak{s}_n(u) = \phi_n^\infty(\mathfrak{s}_\infty(\underline{u})) = \phi_n^\infty\big(\mathfrak{j}_\infty(\psi_\infty(\underline{u}))\big)$ by the theorem. Using the definition of $\mathfrak{j}_n$ we deduce:

COROLLARY 6. $\mathfrak{j}_n(\psi_n(u)) = \mathfrak{s}_n(u)$ *for any* $n\geq 0$ *and* $u\in U^1(K_{n,p})^-\cap U^1(K_{n,p})^0$. ∎

One might ask whether $\mathfrak{j}_n\circ\psi_n = \mathfrak{s}_n$ on the whole of $U^1(K_{n,p})^-$ and in particular whether $\mathfrak{J}_n\supset\mathfrak{S}_n$. (In general, (6.10) yields only the congruence $\mathfrak{j}_n\circ\psi_n\equiv\mathfrak{s}_n \pmod{p^{n+1}}$ on $U^1(K_{n,p})^-$.) A sufficient (but possibly unnecessary) condition is that $U^1(K_{n,p})^-\subset U^1(K_{n,p})^0$. This clearly also guarantees that $\phi_n^\infty(\mathfrak{S}_\infty) = \mathfrak{S}_n$.

Lemma 5. *Suppose $m > n \geq 0$. Then $N_n^m : U^1(K_{m,p})^- \to U^1(K_{n,p})^-$ is surjective iff $m \leq n_0$ or $c \in D_p(K_0/\mathbb{Q})$.*

Proof. Let T_n^m denote the (wild) inertia subgroup of $\mathrm{Gal}(K_m/K_n)$ at primes of K_n above p, on which $D_n := D_p(K_n/\mathbb{Q})$ acts trivially. By local class field theory there is an isomorphism of $\mathbb{Z}_p[G_n]$-modules between $U^1(K_{n,p})/N_n^m U^1(K_{m,p})$ and $T_n^m \otimes_{\mathbb{Z}_p[D_n]} \mathbb{Z}_p[G_n] \cong T_n^m \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G_n/D_n]$ with G_n acting via the second factor. If $m \leq n_0$ then $T_n^m = \{0\}$. Otherwise $T_n^m \neq \{0\}$ and $\mathbb{Z}_p[G_n/D_n]^- = \{0\} \Leftrightarrow c \in D_n \Leftrightarrow c \in D_0$ (since $[K_n : K_0]$ is a power of $p \neq 2$). ■

So $U^1(K_{n,p})^- \subset U^1(K_{n,p})^0$ for some $n \geq 0$ if and only if $c \in D_p(K_0/\mathbb{Q})$, which implies in turn that $U^1(K_{n,p})^- \subset U^1(K_{n,p})^0$ for all $n \geq 0$. From the above arguments, we deduce:

Corollary 7. *Suppose $c \in D_p(K_0/\mathbb{Q})$, i.e. the primes of K_0^+ above p do not split in K_0. Then $\mathfrak{S}_n$ equals $\phi_n^\infty(\mathfrak{S}_\infty)$ and is contained in $\mathfrak{J}_n$. In particular, $\mathfrak{J}_n$ is of finite index in $\mathbb{Z}_p[G_n]^-$.* ■

Next, passing to the quotient in the exact sequences (6.8) and (6.9) gives injective maps $U_\infty^{1,-}/\mu_{\mathrm{local},\infty}^- \to \Lambda_G^-$ and $U_\infty^{1,-}/\mu_{\mathrm{global},\infty} \to \mathfrak{X}_\infty^-$, which we denote $\bar{\mathfrak{s}}_\infty$ and $\bar{\psi}_\infty$ respectively.

Theorem 6. *There is a commuting diagram of Λ_G-modules with exact rows and columns:*

(6.11)

$$
\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \mu_{\mathrm{local},\infty}^-/\mu_{\mathrm{global},\infty} & \to & U_\infty^{1,-}/\mu_{\mathrm{global},\infty} & \to & U_\infty^{1,-}/\mu_{\mathrm{local},\infty}^- & \to & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \bar{\psi}_\infty} & & \downarrow{\scriptstyle \bar{\mathfrak{s}}_\infty} & & \downarrow \\
0 & \to & \mathrm{Gal}(M_\infty/N_\infty^0)^- & \to & \mathfrak{X}_\infty^- & \xrightarrow{\mathfrak{j}_\infty} & \Lambda_G^- & \to & \Lambda_G^-/\mathfrak{J}_\infty \to 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \| \\
0 & \to & \mathrm{Gal}(L_\infty/L_\infty \cap N_\infty^0)^- & \to & X_\infty^- & \xrightarrow{\mathfrak{j}'_\infty} & \Lambda_G^-/\mathfrak{S}_\infty & \to & \Lambda_G^-/\mathfrak{J}_\infty \to 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0 & & 0
\end{array}
$$

Proof. The exactness of the second and third columns follows from (6.9) and (6.8) respectively. The commutativity of the top middle square is Theorem 5. There is therefore a unique map $\mathfrak{j}'_\infty : X_\infty^- \to \Lambda_G^-/\mathfrak{S}_\infty$ making the bottom middle square commute. The exactness of the top row is tautologous and that of the middle row follows from Theorem 3. A diagram chase then shows that the isomorphism $U_\infty^{1,-}/\mu_{\mathrm{global},\infty} \to \mathrm{Gal}(M_\infty/L_\infty)^-$ induced by $\bar{\psi}_\infty$ takes $\mu^-_{\mathrm{local},\infty}/\mu_{\mathrm{global},\infty}$ *onto* $\mathrm{Gal}(M_\infty/L_\infty)^- \cap \mathrm{Gal}(M_\infty/N^0_\infty)^- = \mathrm{Gal}(M_\infty/L_\infty N^0_\infty)^-$. The rest follows easily. ∎

Let M^-_∞ be as in Section 4. Similarly, let L^-_∞ denote the fixed field of $\mathrm{Gal}(L_\infty/K_\infty)^+$ acting on L_∞, so that $\mathrm{Gal}(M_\infty/L_\infty N^0_\infty)^-$ maps isomorphically onto $\mathrm{Gal}(M^-_\infty/L^-_\infty N^0_\infty)$. The above proof then gives the following (implicit in (6.11)).

Corollary 8. *$\bar{\psi}_\infty$ induces a Λ_G-isomorphism*

$$\mu^-_{\mathrm{local},\infty}/\mu_{\mathrm{global},\infty} \cong \mathrm{Gal}(M^-_\infty/L^-_\infty N^0_\infty). \ \blacksquare$$

We now give an explicit description of $\mu^-_{\mathrm{local},\infty}/\mu_{\mathrm{global},\infty}$ as a Λ_G-module. Recall that $K_{n_0} = K_{m_0} = F_{m_0}$ for an integer $m_0 \geq n_0$ and an abelian field F unramified over $\mathbb{Q}$ above p. (See Remark 3.) Suppose that $n \geq m_0$. It follows that $K_n = F_n$, $\mu_{p^\infty}(K_n) = \mu_{p^{n+1}}$ and also $\mu_{p^\infty}(K_{n,\mathfrak{P}}) = i_{\mathfrak{P}}(\mu_{p^{n+1}})$ for all $\mathfrak{P} \in S_p(K_n)$. Hence we have an isomorphism of $\mathbb{Z}_p[G_n]$-modules

$$\nu_n : \mathbb{Z}_p[S_p(K_n)] \otimes_{\mathbb{Z}_p} \mu_{p^{n+1}} \to \mu_{p^\infty}(K_{n,p}),$$
$$\sum_{\mathfrak{P}\in S_p(K_n)} a_{\mathfrak{P}}\mathfrak{P} \otimes \zeta_{\mathfrak{P}} \mapsto (i_{\mathfrak{P}}(\zeta_{\mathfrak{P}})^{a_{\mathfrak{P}}})_{\mathfrak{P}}$$

(where $g(\sum_{\mathfrak{P}} a_{\mathfrak{P}}\mathfrak{P} \otimes \zeta_{\mathfrak{P}}) = \sum_{\mathfrak{P}} a_{\mathfrak{P}} g(\mathfrak{P}) \otimes g(\zeta_{\mathfrak{P}})$ for all $g \in G_n$). Note that $\mu_{p^\infty}(K_n)$ is the image of $\mathbb{Z}_p(\sum_{\mathfrak{P}} \mathfrak{P}) \otimes \mu_{p^{n+1}}$ under ν_n, and $\mu_{p^\infty}(K_{n,p})^-$ is that of $(\mathbb{Z}_p[S_p(K_n)] \otimes \mu_{p^{n+1}})^- = ((1+c)\mathbb{Z}_p[S_p(K_n)]) \otimes \mu_{p^{n+1}}$. Since K_∞/K_{n_0} is totally ramified above p, we can identify $\mathbb{Z}_p[S_p(K_n)]$ with $\mathbb{Z}_p[S_p(K_{n_0})]$ and, hence, $(1+c)\mathbb{Z}_p[S_p(K_n)]$ with $\mathbb{Z}_p[S_p(K^+_{n_0})]$ for any $n \geq m_0$. Moreover, if $m \geq n \geq m_0$ then $N^m_n : \mu_{p^\infty}(K_{m,p}) \to \mu_{p^\infty}(K_{n,p})$ is simply the p^{m-n}th power map. Passing to the limit and then the quotient we find easily

$$\left(\frac{\mathbb{Z}_p[S_p(K^+_{n_0})]}{\mathbb{Z}_p(\sum_{\mathfrak{P}} \mathfrak{P})}\right) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1) \cong \mu^-_{\mathrm{local},\infty}/\mu_{\mathrm{global},\infty} \cong \mathrm{Gal}(M^-_\infty/L^-_\infty N^0_\infty) \tag{6.12}$$

as Λ_G-modules, where $\mathbb{Z}_p(1)$ is a rank-1 $\mathbb{Z}_p$-module with G_∞ acting through χ_{cyc}. Using also Corollary 3 we deduce:

Corollary 9.

(i) $|S_p(K^+_{n_0})| = 1 \Leftrightarrow M^-_\infty = L^-_\infty N^0_\infty$.
(ii) *Suppose* $|S_p(K^+_{n_0})| = 1$. *Then* $N^0_\infty = N_\infty$, $M^-_\infty = L^-_\infty N_\infty$ *and*

$$(\mathrm{Gal}(L_\infty/L_\infty \cap N_\infty)^-)^\dagger \cong (\mathrm{Gal}(M_\infty/N_\infty)^-)^\dagger \cong \mathrm{Hom}_{\mathbb{Z}_p}(A^+_\infty, \mathbb{Q}_p/\mathbb{Z}_p) \tag{6.13}$$

as Λ^+_G-modules. In particular, Greenberg's Conjecture holds in K^+_∞/K^+ if and only if $L^-_\infty \subset N_\infty$. ∎

Note that the equality $M^-_\infty = L^-_\infty N^-_\infty$ appears to be known already in certain cases, even without the condition $|S_p(K^+_{n_0})| = 1$.

We write Λ_Γ for $\mathbb{Z}_p[[\Gamma_0]]$, which is isomorphic to $\mathbb{Z}_p[[\mathbb{Z}_p]] \cong \mathbb{Z}_p[[X]]$ and so is a noetherian integral domain (often denoted Λ). Clearly, Λ_G is a Λ_Γ-algebra and it is easy to see that Λ_G^- is free of rank $\frac{1}{2}[K_0 : \mathbb{Q}]$ over Λ_Γ. We may consider (6.11) and (6.12) over Λ_Γ by restriction of scalars. Using also some 'classical' results from Iwasawa theory, this yields:

THEOREM 7.

(i) *All the modules in diagram* (6.11) *are finitely generated over* Λ_Γ.
(ii) *Those in the left-hand column and the bottom row are* Λ_Γ*-torsion.*
(iii) $\mathrm{Gal}(M_\infty/N^0_\infty) = \ker(\mathfrak{j}_\infty)$ *is precisely* $\mathrm{tor}_{\Lambda_\Gamma}(\mathfrak{X}_\infty)$ (*the* Λ_Γ*-torsion submodule of* $\mathfrak{X}_\infty$).

Proof. Recall that a Λ_Γ-module A is said to be *pseudo-isomorphic* to another, B (written $A \sim B$), if there exists a Λ_Γ-homomorphism $A \to B$ with finite kernel and cokernel. It is shown in [W, pp. 292–293 and Theorem 13.31] that $\mathfrak{X}_\infty$ is finitely generated over Λ_Γ and that

$$\mathfrak{X}_\infty \sim \Lambda_\Gamma^{\frac{1}{2}[K_0:\mathbb{Q}]} \oplus C$$

for some finitely generated torsion Λ_Γ-module C. Thus both $\mathfrak{X}^-_\infty$ and Λ^-_G are finitely generated and (i) follows.

Next, it is well known that X_∞ is finitely generated and torsion over Λ_Γ (see e.g. [W, §13.3]). Furthermore, we have

$$X_\infty \sim \mathrm{Hom}_{\mathbb{Z}_p}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathrm{Gal}(M_\infty/N_\infty)^\dagger \tag{6.14}$$

as Λ_Γ-modules, where the isomorphism follows from (4.2) and the pseudo-isomorphism from [W, Prop. 15.34]. (*Note:* Washington's '$\tilde{X}$' instead of 'X' comes about because of his different action on Hom's.) Since N_∞ is contained in M^-_∞ we have $\mathfrak{X}^+_\infty \subset \mathrm{Gal}(M_\infty/N_\infty)$ and it follows from (6.14) that $\mathfrak{X}^+_\infty$ is also Λ_Γ-torsion. Finally, (6.12) shows that $\mu^-_{\mathrm{local},\infty}/\mu_{\mathrm{global},\infty}$ is killed by $(\gamma_{n_0} - \chi_{\mathrm{cyc}}(\gamma_{n_0})) \in \Lambda_\Gamma$. It follows from the above facts that X^-_∞ and all the modules in the left-hand column of (6.11) are Λ_Γ-torsion, so part (ii) will follow if we can show that $\Lambda^-_G/\mathfrak{J}_\infty$ is too, i.e. that $(\Lambda^-_G/\mathfrak{J}_\infty) \otimes_{\Lambda_\Gamma} \mathcal{F}_\Gamma = \{0\}$ where $\mathcal{F}_\Gamma$ denotes the field of fractions of Λ_Γ. Consider the exact sequence obtained by applying $\bigotimes_{\Lambda_\Gamma} \mathcal{F}_\Gamma$ to the middle row of of (6.11). From the torsion results proved so far, the first term of this sequence vanishes and so does $\mathfrak{X}^+_\infty \otimes_{\Lambda_\Gamma} \mathcal{F}_\Gamma$. Thus $\mathfrak{j}_\infty \otimes 1$ is injective and

$$\begin{aligned}
&\dim_{\mathcal{F}_\Gamma}(\mathfrak{X}^-_\infty \otimes_{\Lambda_\Gamma} \mathcal{F}_\Gamma) \\
&\qquad = \dim_{\mathcal{F}_\Gamma}(\mathfrak{X}^-_\infty \otimes_{\Lambda_\Gamma} \mathcal{F}_\Gamma) + \dim_{\mathcal{F}_\Gamma}(\mathfrak{X}^+_\infty \otimes_{\Lambda_\Gamma} \mathcal{F}_\Gamma) \\
&\qquad = \dim_{\mathcal{F}_\Gamma}(\mathfrak{X}_\infty \otimes_{\Lambda_\Gamma} \mathcal{F}_\Gamma) = \tfrac{1}{2}[K_0 : \mathbb{Q}] = \dim_{\mathcal{F}_\Gamma}(\Lambda^-_G \otimes_{\Lambda_\Gamma} \mathcal{F}_\Gamma).
\end{aligned}$$

Hence $\mathfrak{j}_\infty \otimes 1$ is also surjective and (ii) follows.

For (iii), we already know that $\mathrm{Gal}(M_\infty/N^0_\infty)^+ = \mathfrak{X}^+_\infty$ and $\mathrm{Gal}(M_\infty/N^0_\infty)^-$ are Λ_Γ-torsion, so $\ker(\mathfrak{j}_\infty) = \mathrm{Gal}(M_\infty/N^0_\infty) \subset \mathrm{tor}_{\Lambda_\Gamma}(\mathfrak{X}_\infty)$. The reverse inclusion, $\mathrm{tor}_{\Lambda_\Gamma}(\mathfrak{X}_\infty) \subset \ker(\mathfrak{j}_\infty)$, is clear, since Λ^-_G is Λ_Γ-torsionfree. ∎

Remark 11. Since Λ_G is Λ_Γ-torsionfree and $\ker(\mathfrak{j}_\infty) = \mathrm{Gal}(M_\infty/N^0_\infty)$ is Λ_Γ-torsion (by Theorem 7(iii)) it is in the right kernel of the pairing $\{\,,\,\}_\infty$. The reverse inclusion is obvious. Thus, if $h \in \mathfrak{X}_\infty$ then $\{\underline{\alpha}, h\}_\infty = 0$ holds for all $\underline{\alpha} \in \mathcal{V}_\infty$ iff $\{\underline{\eta}, h\}_\infty = 0$.

Remark 12. If K is *any* number field, we can define M_∞, $\mathfrak{X}_\infty$, $K_{n,p}$, Λ_Γ etc. as above and a field T_∞ with $K_\infty \subset T_\infty \subset M_\infty$ by $\mathrm{Gal}(M_\infty/T_\infty) = \mathrm{tor}_{\Lambda_\Gamma}(\mathfrak{X}_\infty)$. Theorem 7(iii) says that if $K/\mathbb{Q}$ is *abelian* then T_∞ equals N^0_∞, i.e. it has Kummer radical $\varinjlim E^0(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ over K_∞. On the other hand, for *general* K, Theorem 3.1 of [LMN], attributed to Kuz'min and Kolster, states that whenever K satisfies Gross' Conjecture (e.g. $K/\mathbb{Q}$ is abelian) then the Kummer radical of T_∞ is $\varinjlim \bar{\mathcal{U}}^0(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ where $\bar{\mathcal{U}}^0(K_n)$ consists of those elements of $E_{S_p}(K_n) \otimes \mathbb{Z}_p$ whose images in $K^\times_{n,p}$ are norms from $K^\times_{m,p}$ for all $m \ge n$. I am grateful to Thong Nguyen Quang Do for drawing my attention to this result and a possible way to deduce Theorem 7(iii) from it. When $K/\mathbb{Q}$ is abelian one can certainly replace $E^0(K^+_n)$ in our definition of N^0_∞ by the larger set of $u \in E_{S_p}(K_n)$ satisfying $N_{D_p(K_n/\mathbb{Q})} u \in p^{\mathbb{Z}}$. (Use the norm properties of the $\varepsilon_t(\mathbb{Q})$'s.) Furthermore, by local class field theory, the latter condition amounts to the image of u in $K^\times_{n,p}$ being a norm from $K^\times_{m,p}$ for all $m \ge n$ (and, by Hasse's theorem, to u being a global norm from $K^\times_m$ for all $m \ge n$).

Remark 13. Still in the case of general K, the subfield of M_∞ fixed by $\bar{\psi}_\infty(\mu_{\mathrm{local},\infty}/\mu_{\mathrm{global},\infty})$ is the *field of Bertrandias–Payan* denoted K^{BP}_∞ (see e.g. [Ng]). For K abelian, Corollary 8 and Theorem 7(iii) give respectively

$$K^{\mathrm{BP}}_\infty \cap M^-_\infty = L^-_\infty N^0_\infty = L^-_\infty T_\infty$$

with T_∞ as above. If K is only CM, the equality of the first and last terms is clearly equivalent to the Λ_Γ-torsionfreeness of $U^{1,-}_\infty/\mu^-_{\mathrm{local},\infty}$. The latter follows (at least in certain cases) from work of Coleman. If K is abelian, then of course it is a consequence of the injectivity of $\bar{\mathfrak{s}}_\infty$ in (6.11) which was also crucial to Corollary 8 etc. We stress that this injectivity was in turn deduced from Proposition 8(i) and hence, at base, from the non-vanishing of *complex* L-functions at $s = 1$.

Finally, we can apply $(-)^\dagger$ to the bottom row of (6.11). Since ι_∞ induces Λ_G-isomorphisms $(\Lambda^-_G/\mathfrak{S}_\infty)^\dagger \to \Lambda^+_G/\iota_\infty(\mathfrak{S}_\infty)$ and $(\Lambda^-_G/\mathfrak{J}_\infty)^\dagger \to \Lambda^+_G/\mathfrak{D}_\infty$, we deduce:

Corollary 10. *There is an exact sequence of Λ_G^+-modules which are f.g. and torsion over Λ_Γ:*

$$(6.15)\qquad 0 \to (\mathrm{Gal}(L_\infty/L_\infty \cap N_\infty^0)^-)^\dagger \to (X_\infty^-)^\dagger \xrightarrow{\iota_\infty \circ \mathrm{j}'_\infty} \Lambda_G^+/\iota_\infty(\mathfrak{S}_\infty) \to \Lambda_G^+/\mathfrak{D}_\infty \to 0. \ \blacksquare$$

In the next section we shall analyse this sequence under the assumption $K = \mathbb{Q}$, which eliminates at a stroke many of the complicating (but also interesting) phenomena of the general case. The weaker assumption $p \nmid [K : \mathbb{Q}]$ would allow us to decompose (6.11) and (6.15) using (p-adic) characters of G_0 and hence 'isolate' these phenomena—e.g. the possible non-triviality of $\mu^-_{\mathrm{local},\infty}/\mu_{\mathrm{global},\infty}$ and/or $\mathrm{Gal}(N_\infty/N_\infty^0)$—at certain 'troublesome' characters.

7. The case $K = \mathbb{Q}$: computation of $\mathfrak{S}_n$ and $\mathfrak{S}_\infty$, and the Main Conjecture. We return to the situation and notations of Section 5, so $K_n = \mathbb{Q}(\mu_{p^{n+1}})$. We start by determining $\mathfrak{S}_n$ for $n \geq 0$, showing that in this case it is exactly the $\mathbb{Z}_p$-span of the Stickelberger ideal. First, $K_{n,p}$ is the completion of K_n at its unique prime above p, so the embedding j induces an isomorphism from $K_{n,p}$ to $\hat{K}_n := \mathbb{Q}_p(j(\zeta_n))$. We regard this as an identification and suppress j from the notation. Thus, $G_n = D_p(K_n/\mathbb{Q})$ identifies with $\mathrm{Gal}(\hat{K}_n/\mathbb{Q}_p)$, whose action commutes with $\log_p$, giving

$$(7.1)\qquad \mathfrak{s}_n(u) = a^{-,*}_{K_n/\mathbb{Q}} \sum_{g \in G_n} g(\log_p(u))g^{-1} \quad \text{for all } u \in U^1(\hat{K}_n).$$

Let us write simply θ_n for the element $\theta_{\mathbb{Q}(\mu_{p^{n+1}})/\mathbb{Q},S_{p^{n+1}}}$ of $\mathbb{Q}[G_n]^-$, b_n for the element $\frac{1}{p^{n+1}}\sum_{i=0}^n \zeta_n$ of $K_n \subset \hat{K}_n$ and $\mathbf{T}_n$ for the trace pairing $\hat{K}_n \times \hat{K}_n \to \mathbb{Q}_p$, that is, $\mathbf{T}_n(v,w) := \mathrm{Tr}_{\hat{K}_n/\mathbb{Q}_p}(vw)$ for all $v, w \in \hat{K}_n$. Observe that $\mathbf{T}_n$ is symmetric, non-degenerate and clearly satisfies

$$(7.2)\qquad T_n(xv, yw) = \mathbf{T}_n(y^*xv, w) = \mathbf{T}_n(v, x^*yw) \quad \text{for all } v, w \in \hat{K}_n \text{ and } x, y \in \mathbb{Q}_p[G_n].$$

We define a $\mathbb{Z}_p[G_n]$-equivariant map $\mathfrak{w}_n$ by

$$\mathfrak{w}_n : U^1(\hat{K}_n) \to \mathbb{Q}_p[G_n], \quad u \mapsto \sum_{g \in G_n} \mathbf{T}_n(b_n, g(\log_p(u)))g^{-1}.$$

Proposition 9. $\mathfrak{s}_n(u) = \theta_n \mathfrak{w}_n(u)$ *for all* $u \in U^1(\hat{K}_n)$.

Proof. Equation (6.1) (together with the fact $S_{p^{i+1}} = S_p$ fo rall i) implies

$$(7.3)\qquad \pi^i_j(\theta_i) = \theta_j \quad \text{for each } i > j \geq 0.$$

It follows easily from this, equation (6.3) with $l = p^{n+1}$ and the definition of $\mathcal{A}_{p^{i+1}}$ that

$$a^{-,*}_{K_n/\mathbb{Q}} = \frac{1}{p^{n+1}} \sum_{i=0}^{n} \mathrm{cores}^{K_n}_{K_i}(\mathcal{A}_{p^{i+1}}\theta_i) = \theta_n \frac{1}{p^{n+1}} \sum_{i=0}^{n} \mathrm{cores}^{K_n}_{K_i}(\mathcal{A}_{p^{i+1}})$$
$$= \theta_n \sum_{h\in G_n} h(b_n)h.$$

Substituting this in (7.1) and rearranging gives the result. ∎

The determination of the image of $\mathfrak{w}_n$ is a formal consequence of a 'classical' result from [I1]: Let $\mathcal{L}_n$ denote $\log_p(U^1(\hat{K}_n))$. This is easily seen to be a $\mathbb{Z}_p[G_n]$-submodule of $\hat{K}_n$ of $\mathbb{Z}_p$-rank equal to $[\hat{K}_n : \mathbb{Q}_p] = |G_n|$. Let $\mathcal{L}^\star_n$ denote the $\mathbb{Z}_p$-dual of $\mathcal{L}_n$ with respect to $\mathbf{T}_n$, namely the set $\{v \in \hat{K}_n : \mathbf{T}_n(v,w) \in \mathbb{Z}_p \text{ for all } w \in \mathcal{L}\}$. To determine $\mathcal{L}^\star_n$ (which he denotes '$\mathfrak{X}_n$') Iwasawa defines a fractional ideal $\mathfrak{A}_n$ of $\mathbb{Q}_p[G_n]$ which, in our notation, is given by

$$\mathfrak{A}_n := \mathbb{Z}_p[G_n]\Big(-\theta^*_n + \frac{2}{p^n}\sum_{g\in G_n} g\Big) + I(\mathbb{Z}_p[G_n]). \tag{7.4}$$

(See [I1, p. 44]. The element in large parentheses coincides with that denoted 'ξ_n' by Iwasawa.) He also shows that there is a $\mathbb{Q}_p[G_n]$-isomorphism $\mathbb{Q}_p[G_n] \to \hat{K}_n$ which he denotes 'φ_n' and which sends x to xcb_n in our notation. (See the start of §1.6 ibid., noting that Iwasawa's 'θ_n' is our $c(b_n)$.) Theorem 1 of [I1] thus amounts in our notation to the equation

$$\mathcal{L}^\star_n = \mathfrak{A}_n b_n. \tag{7.5}$$

For any fractional ideal $\mathfrak{C}$ of $\mathbb{Q}_p[G_n]$, we define another fractional ideal $\mathfrak{C}^\star$ by

$$\mathfrak{C}^\star := \{y \in \mathbb{Q}_p[G_n] : x^*y \in \mathbb{Z}_p[G_n]\ \forall x \in \mathfrak{C}\}.$$

The reason for the similarity of notation is that $\mathfrak{C}^\star$ is easily seen to be the $\mathbb{Z}_p$-dual of $\mathfrak{C}$ with respect to the symmetric, non-degenerate pairing $\mathbf{B}_n : \mathbb{Q}_p[G_n]\times\mathbb{Q}_p[G_n] \to \mathbb{Q}_p$ taking $(\sum_{g\in G_n} a_g g, \sum_{g\in G_n} b_g g)$ to $\sum_{g\in G_n} a_g b_g$, i.e. the coefficient of 1 in $(\sum_{g\in G_n} a_g g)^*(\sum_{g\in G_n} b_g g)$. We can now prove

Proposition 10. $\mathrm{im}(\mathfrak{w}_n) = \mathfrak{A}^\star_n$.

Proof. Equation (7.5) shows that $\{gb_n : g \in G_n\}$ is a $\mathbb{Q}_p$-basis of $\hat{K}_n$ and it follows from (7.2) that the dual basis with respect to $\mathbf{T}_n$ is of form $\{hb'_n : h \in G_n\}$ for some $b'_n \in \hat{K}_n$. More precisely $\mathbf{T}_n(gb_n, hb'_n) = \delta_{g,h}$ so that $\mathbf{T}_n(xb_n, yb'_n) = \mathbf{B}_n(x,y)$ for all $x, y \in \mathbb{Q}_p[G_n]$. Now, clearly, $\mathcal{L}_n$ must be of form $\mathfrak{C}b'_n$ for some fractional ideal $\mathfrak{C}$ of $\mathbb{Q}_p[G_n]$. Since also $\mathcal{L}_n$ is the $\mathbb{Z}_p$-dual of $\mathcal{L}^\star_n$ with respect to $\mathbf{T}_n$, equation (7.5) gives, for any

$y \in \mathbb{Q}_p[G_n]$,

$$y \in \mathfrak{C} \Leftrightarrow yb'_n \in \mathcal{L}_n \Leftrightarrow \mathbf{T}_n(xb_n, yb'_n) \in \mathbb{Z}_p \ \forall x \in \mathfrak{A}_n$$
$$\Leftrightarrow \mathbf{B}_n(x,y) \in \mathbb{Z}_p \ \forall x \in \mathfrak{A}_n \Leftrightarrow y \in \mathfrak{A}_n^\star.$$

Thus $\mathcal{L}_n = \mathfrak{A}_n^\star b'_n$. Finally, the map $\alpha : \hat{K}_n \to \mathbb{Q}_p[G_n]$ sending v to the element $\sum_{g\in G_n} \mathbf{T}_n(b_n, g(v))g^{-1}$ is clearly $\mathbb{Q}_p[G_n]$-equivariant, so $\mathrm{im}(\mathfrak{w}_n) = \alpha(\mathcal{L}_n) = \alpha(\mathfrak{A}_n^\star b'_n) = \mathfrak{A}_n^\star \alpha(b'_n) = \mathfrak{A}_n^\star.1 = \mathfrak{A}_n^\star$. ∎

Propositions 9 and 10 imply $\mathfrak{S}_n = \mathrm{im}(\mathfrak{s}_n) = \theta_n \mathrm{im}(\mathfrak{w}_n) = \theta_n \mathfrak{A}_n^\star$. Now definition (7.4) shows that $\mathfrak{A}_n$ and $\mathbb{Z}_p[G_n]\theta_n^* + \mathbb{Z}_p[G_n]$ have the same minus parts, hence so do $\mathfrak{A}_n^\star$ and $(\mathbb{Z}_p[G_n]\theta_n^* + \mathbb{Z}_p[G_n])^\star = (\mathbb{Z}_p[G_n]\theta_n^*)^\star \cap \mathbb{Z}_p[G_n]^\star$. Since also θ_n lies in $\mathbb{Q}_p[G_n]^-$, we deduce

$$\mathfrak{S}_n = \theta_n(\mathbb{Z}_p[G_n]\theta_n^* + \mathbb{Z}_p[G_n])^\star = \theta_n\{y \in \mathbb{Z}_p[G_n] : \theta_n y \in \mathbb{Z}_p[G_n]\}. \tag{7.6}$$

(Incidentally, this proves $\mathfrak{S}_n \subset \mathbb{Z}_p[G_n]^-$ independently of Proposition 8.) Since $\chi_{\mathrm{cyc}} : G_\infty \to \mathbb{Z}_p^\times$ is an isomorphism, G_∞ is pro-cyclic and we fix henceforth a topological generator g_∞ whose image g_n in G_n generates the latter.

LEMMA 6.

$$\begin{aligned}\mathbb{Z}_p[G_n](g_n - \chi_{\mathrm{cyc}}(g_\infty)) &= \langle \sigma_{a,p^{n+1}} - a : (a,2p) = 1\rangle_{\mathbb{Z}_p[G_n]} \\ &= \{y \in \mathbb{Z}_p[G_n] : \theta_n y \in \mathbb{Z}_p[G_n]\}.\end{aligned} \tag{7.7}$$

Proof (sketch). Denote the three sets by (1), (2) and (3) respectively. One checks directly that (2) $\subset$ (3) and that (3)/(2) is represented by elements of (3) lying in $\mathbb{Z}_p$, which must clearly be divisible by p^{n+1}. Since $-2p^{n+1} = \sigma_{1+2p^{n+1},p^{n+1}} - (1+2p^{n+1})$, we deduce $p^{n+1} \in (2)$ so (3) = (2). Clearly, (1) is generated over $\mathbb{Z}_p[G_n]$ by the elements $g_n^l - \chi_{\mathrm{cyc}}(g_\infty^l)$ for $l \geq 1$. Taking $l = (p-1)p^n$ we find easily $p^{n+1} \in (1)$ so it suffices to show (1) $\equiv$ (2) mod p^{n+1}. But $g_n^l = \sigma_{a,p^{n+1}}$ implies $\chi_{\mathrm{cyc}}(g_\infty^l) \equiv a \bmod p^{n+1}$ so the generators are the same mod p^{n+1}. ∎

REMARK 14. In fact, if $G(r)$ denotes $\mathrm{Gal}(\mathbb{Q}(\mu_r)/\mathbb{Q})$ for some $r > 1$, it is well known that

$$\begin{aligned}\mathrm{ann}_{\mathbb{Z}[G(r)]}(\mu(\mathbb{Q}(\mu_r))) &= \langle \sigma_{a,r} - a : (a,2r) = 1\rangle_{\mathbb{Z}[G(r)]} \\ &= \{y \in \mathbb{Z}[G(r)] : \theta_{\mathbb{Q}(\mu_r)/\mathbb{Q},S_r} y \in \mathbb{Z}[G(r)]\}.\end{aligned}$$

The argument for the second equality above is similar to that for the second equality of (7.7). For more details, see [W, Lemma 6.9] but note that the element 'θ' there is our $-\theta_{\mathbb{Q}(\mu_r)/\mathbb{Q},S_r} + \frac{1}{2}\sum_{g\in G(r)} g$. The Stickelberger ideal $\mathrm{St}_{\mathbb{Q}(\mu_r)}$ of $\mathbb{Z}[G(r)]$ is $\theta_{\mathbb{Q}(\mu_r)/\mathbb{Q},S_r} \mathrm{ann}_{\mathbb{Z}[G(r)]}(\mu(\mathbb{Q}(\mu_r)))$. (This is the 'unenlarged' ideal, but for $r = p^{n+1}$ it makes no difference.) Thus (7.6), the second equality in (7.7) and the first equality in the last equation imply $\mathfrak{S}_n = \mathbb{Z}_p \mathrm{St}_{\mathbb{Q}(\mu_{p^{n+1}})}$.

Let $\tilde{\theta}_n = (g_n - \chi_{\mathrm{cyc}}(g_\infty))\theta_n$. Then $\tilde{\theta}_n \in \mathbb{Z}_p[G_n]^-$ by (7.7) and the sequence $(\tilde{\theta}_n)_n$ defines an element $\tilde{\theta}_\infty$ of Λ_G^- by (7.3). Equations (7.7) and (7.6) give

THEOREM 8. *If $K = \mathbb{Q}$ then $\mathfrak{S}_n$ (for any $n \geq 0$) and $\mathfrak{S}_\infty$ are the principal ideals of $\mathbb{Z}_p[G_n]^-$ and Λ_G^- generated by $\tilde{\theta}_n$ and $\tilde{\theta}_\infty$ respectively.* ∎

REMARK 15. It is worth noting that a similarly simple description of $\mathfrak{S}_n$ cannot be expected for general abelian K. Indeed, if θ_{K_n} denotes the Stickelberger element of $\mathbb{Q}_p[G_n]^-$ generalising θ_n then the phenomenon of 'trivial zeroes' means that $\mathbb{Z}_p[G_n]^- \cap \mathbb{Z}_p[G_n]^-\theta_{K_n}$ is frequently of infinite index in $\mathbb{Z}_p[G_n]^-$ and so cannot contain $\mathfrak{S}_n$, which is always of finite index.

Our assumption $K = \mathbb{Q}$ implies $|S_p(K_0^+)| = 1$ so, using Corollary 9 and Theorem 8, the sequence (6.15) can be rewritten as

$$0 \to A_\infty^{+,\vee} \to (X_\infty^-)^\dagger \to \Lambda_G^+/(\iota_\infty(\tilde{\theta}_\infty)) \to \Lambda_G^+/\mathfrak{D}_\infty \to 0. \tag{7.8}$$

Since $p \nmid |G_0| = p-1$, there is a unique splitting $G_\infty = G_0 \times \Gamma_0$ and we can decompose (7.8) using (even) characters of G_0. Let $\omega : G_0 \to \mathbb{Z}_p^\times$ be the Teichmüller character (the restriction of χ_{cyc}) and let e_j be the idempotent of $\mathbb{Z}_p[G_0]$ associated to ω^j for $j \in \mathbb{Z}$. Any $\mathbb{Z}_p[G_0]$-module M is the direct sum of its components $M^{(j)} := e_jM$ for $j = 0, \ldots, p-2$. For $\mathbb{Z}_p[G_0^+]$-modules, we restrict to j even. It follows that (7.8) is the direct sum of the exact sequences

$$0 \to A_\infty^{(j),\vee} \to (X_\infty^{(1-j)})^\dagger \to \Lambda_G^{(j)}/(\iota_\infty(\tilde{\theta}_\infty))^{(j)} \to \Lambda_G^{(j)}/\mathfrak{D}_\infty^{(j)} \to 0 \tag{7.9}$$

of f.g. torsion Λ_Γ-modules for $j = 0, 2, 4, \ldots, p-3$. The fact that the generalised Bernoulli number $B_{1,\omega^{-1}}$ lies in $p^{-1}\mathbb{Z}_p^\times$ implies that the image of $e_0\iota_\infty(\tilde{\theta}_\infty)$ in $e_0\mathbb{Z}_p[G_0] = \mathbb{Z}_p e_0$ lies in $\mathbb{Z}_p^\times e_0$. It follows easily that $\Lambda_G^{(0)}/(\iota_\infty(\tilde{\theta}_\infty))^{(0)}$ vanishes; but the same fact also implies that $A_0^{(1)} \cong (X_\infty^{(1)})_{\Gamma_0}$ vanishes (by Stickelberger's Theorem), hence so does $X_\infty^{(1)}$. Thus (7.9) is trivial for $j = 0$ and we suppose henceforth $j \neq 0$ unless otherwise stated.

To analyse the third non-zero term in (7.9) we first write $g_\infty = g_0\gamma$ so that γ and $\kappa := \chi_{\mathrm{cyc}}(\gamma)$ topologically generate Γ_0 and $1 + p\mathbb{Z}_p$ respectively. Similarly $g_n = g_0\gamma(n)$ where $\gamma(n)$ is the image of γ in $\Gamma(n) := \mathrm{Gal}(K_n/K_0) \cong \Gamma_0/\Gamma_n$ and $G_n = G_0 \times \Gamma(n)$. Define $\tilde{\theta}_{n,j}$, $\theta_{n,j}$ and $v_{n,j} \in \mathbb{Q}_p[\Gamma(n)]$ by

$$e_{1-j}\tilde{\theta}_n = \tilde{\theta}_{n,j}e_{1-j}, \quad e_{1-j}\theta_n = \theta_{n,j}e_{1-j}, \quad e_{1-j}(g_n - \chi_{\mathrm{cyc}}(g_\infty)) = v_{n,j}e_{1-j},$$

so that $\tilde{\theta}_{n,j} \in \mathbb{Z}_p[\Gamma(n)]$ and $\tilde{\theta}_{n,j} = v_{n,j}\theta_{n,j}$. Since $j \neq 0$, the augmentation of $v_{n,j} = \omega(g_0)(\omega^{-j}(g_0)\gamma(n) - \kappa)$ lies in $\mathbb{Z}_p^\times$ so that $v_{n,j} \in \mathbb{Z}_p[\Gamma(n)]^\times$ and $\theta_{n,j} \in \mathbb{Z}_p[\Gamma(n)]$. Thus $e_{1-j}\tilde{\theta}_\infty = v_{\infty,j}\theta_{\infty,j}e_{1-j}$ where $v_{\infty,j} := \varprojlim v_{n,j} \in \Lambda_\Gamma^\times$ and $\theta_{\infty,j} := \varprojlim \theta_{n,j} \in \Lambda_\Gamma$. It follows that $\Lambda_G^{(j)}/(\iota_\infty(\tilde{\theta}_\infty))^{(j)}$ can be written as $\Lambda_\Gamma e_j/\iota_\infty(\theta_{\infty,j})\Lambda_\Gamma e_j$. Next, we identify Λ_Γ as usual with $\Lambda := \mathbb{Z}_p[[T]]$ by sending γ to $1+T$. Then $\theta_{\infty,j}$ goes to the unique power series $f_j(T) \in \Lambda$ such that

$$L_p(s,\omega^j\psi) = f_j(\psi(\gamma(n))^{-1}\kappa^s - 1) \tag{7.10}$$

for all $s \in \mathbb{Z}_p$ and any character $\psi : \Gamma(n) \to \bar{\mathbb{Q}}_p^\times$ for any $n \geq 0$, where $L_p(s,\omega^j\psi)$ denotes the p-adic L-function. (See [W, pp. 119 and 122–123]: take $\gamma(n)$ to be '$\gamma_n(1+q_0)$' for all n so that $\psi(\gamma(n))^{-1}$ equals 'ζ_ψ' and check that $\theta_{n,j}$ equals '$\xi_n(\omega^j)$' by (6.2).)

Thus $\Lambda_G^{(j)}/(\iota_\infty(\tilde\theta_\infty))^{(j)} \cong \Lambda/(f_j(\kappa(1+T)^{-1}-1))$. But the 'Main Conjecture' states in this case that $f_j(T)$ also equals $\mathrm{char}_\Lambda(X_\infty^{(1-j)})$ (the characteristic power series of $X_\infty^{(1-j)}$ as a f.g. torsion Λ-module, defined up to a unit of Λ). This is clearly equivalent to the two middle terms of (7.9) having the same characteristic power series (up to a unit). The Main Conjecture is, of course, proven (see e.g. [W, Thm. 15.14], where characteristic *polynomials* are used, for unicity). From the multiplicativity of characteristic power series in exact sequences we deduce

THEOREM 9. *If* $K = \mathbb{Q}$ *then*

$$\mathrm{char}_\Lambda((A_\infty^{(j)})^\vee) = \mathrm{char}_\Lambda(\Lambda_G^{(j)}/\mathfrak{D}_\infty^{(j)}) \quad (\textit{up to a unit of } \Lambda) \tag{7.11}$$

for all j *even,* $0 \leq j \leq p-3$. ∎

Note that both sides of (7.11) are units for $j=0$ and Greenberg's Conjecture is equivalent to the same for all even j. (See also Proposition 6(i) for the right-hand side)

REMARK 16. Let $\mathfrak{D}_{\infty,j}$ be the ideal of Λ_Γ determined by $\mathfrak{D}_\infty^{(j)} = \mathfrak{D}_{\infty,j}e_j$. Identifying Λ_Γ with Λ (a noetherian unique factorization domain) we find that $\mathrm{char}_\Lambda(\Lambda_G^{(j)}/\mathfrak{D}_\infty^{(j)})$ is simply the h.c.f. of any set of Λ-generators of $\mathfrak{D}_{\infty,j}$. Equation (7.11) is equivalent to the statement that $\mathfrak{D}_{\infty,j}$ is contained with finite index in the principal ideal generated by $\mathrm{char}_\Lambda((A_\infty^{(j)})^\vee)$, and the Main Conjecture for $K=\mathbb{Q}$ would follow by converse arguments if we could give an independent proof of this statement for all even j. Consider the extra hypothesis that $(A_\infty^{(j)})^\vee$ is pseudo-isomorphic to a *cyclic* Λ-module $\Lambda/(c_j)$, so $c_j = \mathrm{char}_\Lambda((A_\infty^{(j)})^\vee)$. The inclusion $\mathfrak{D}_{\infty,j} \subset (c_j)$ then follows from Theorem 2, and the finiteness of the index should follow from Corollary 4. Without this hypothesis however, a new ingredient would probably be required to reprove the Main Conjecture by this route, perhaps an 'Euler systems'-type elaboration of Theorem 1.

REMARK 17. By Theorem 8 and the foregoing calculations, $\iota_\infty(\mathfrak{S}_\infty)e_j$ equals $\iota_\infty(\theta_{\infty,j})\Lambda_\Gamma e_j$ for each $j \neq 0$, so $\iota_\infty(\theta_{\infty,j})$ annihilates $X_\infty^{(j)}$ by Corollary 5(ii). For $n \geq 0$, let $d_{n,j}$ denote the image of $\iota_\infty(\theta_{\infty,j})$ in $\mathbb{Z}_p[\Gamma(n)]$. Since $\theta_{\infty,j}$ corresponds to $f_j(T)$ we find $\psi(d_{n,j}) = f_j\big(\kappa\psi(\gamma(n))^{-1} - 1\big) = L_p(1, \omega^j\psi)$ for every character $\psi : \Gamma(n) \to \bar{\mathbb{Q}}_p^\times$, giving the formula $d_{n,j} = \sum_\psi L_p(1, \omega^j\psi)e_\psi$ (where ψ ranges over all such characters and e_ψ is the corresponding idempotent in $\bar{\mathbb{Q}}_p[\Gamma(n)]$). Clearly, $d_{n,j}$ annihilates $(X_\infty^{(j)})_{\Gamma(n)}$, which is isomorphic to $X_n^{(j)} \cong A_n^{(j)}$ (see Remark 4, using $K = \mathbb{Q}$). This is a weakening of the annihilation results of Gras and Oriat (see [O]). The latter hold for more general real abelian fields and even in the present case they amount (more or less) to the annihilation by $d_{n,j}$ of the much *bigger module* $\mathfrak{X}_n^{(j)}$. (Indeed, if p divides the numerator of the jth Bernoulli number, one can show that $|\mathfrak{X}_n^{(j)}|$ is finite but unbounded as $n \to \infty$, whereas $A_n^{(j)} = \{0\}$ in all known cases.) This, of course, corresponds to the fact that $\iota_\infty(\mathfrak{S}_\infty)$ is usually a much *smaller ideal* than $\mathfrak{D}_\infty$. Considerable generalisations of Gras' and Oriat's annihilation results appear in [BB]. See also [BN].

Remark 18. There is a more familiar exact sequence featuring both in a formulation of the Main Conjecture essentially due to Iwasawa in [I1] and in its proof by Rubin (see e.g. [W, §§15.4–7]). Still in the case $K = \mathbb{Q}$ it reads (for each even j)

$$0 \to (\hat{E}_\infty^1/\hat{C}_\infty^1)^{(j)} \to (U_\infty^1/\hat{C}_\infty^1)^{(j)} \to \mathfrak{X}_\infty^{(j)} \to X_\infty^{(j)} \to 0. \tag{7.12}$$

Recall that $\hat{E}_n^1$ (resp. $\hat{C}_n^1$) denotes the *closure* in $U^1(K_n)^+$ of the group E_n^1 (resp. C_n^1), which in turn consists of the embeddings of those elements of E_n (resp. of C_n, see Section 5) which are congruent to 1 modulo the unique prime above p in K_n^+. Then $\hat{E}_\infty^1$ (resp. $\hat{C}_\infty^1$) is obtained by taking the projective limit with respect to norms. The middle map comes from the map ψ_∞ used in Section 6 (but here in the *plus* part). We assume for simplicity that $j \neq 0$ and compare the non-zero terms of this sequence with those of (7.9). First, Iwasawa proved that $(U_\infty^1/\hat{C}_\infty^1)^{(j)}$ is Λ-isomorphic to $\Lambda/(f_j(\kappa(1+T)^{-1} - 1))$. Hence

$$(U_\infty^1/\hat{C}_\infty^1)^{(j)} \cong \Lambda_G^{(j)}/(\iota_\infty(\tilde{\theta}_\infty))^{(j)}.$$

For the remaining terms we use the notion of the *adjoint* $\alpha(M)$ of a torsion Λ-module M (see [W, §15.5]). In the special case where M_{Γ_n} is *finite* for all $n \geq 0$ we have $\alpha(M) \cong \varprojlim (M_{\Gamma_n})^\vee$, where the map $(M_{\Gamma_{n+1}})^\vee \to (M_{\Gamma_n})^\vee$ is dual to the map $M_{\Gamma_n} \to M_{\Gamma_{n+1}}$ given by multiplication by $1 + \gamma_n + \gamma_n^2 + \cdots + \gamma_n^{p-1}$. (See [I2].) From the isomorphism $(X_\infty)_{\Gamma_n} \to X_n$ we deduce $\alpha(X_\infty^{(i)}) \cong A_\infty^{(i),\vee}$ for all i. Also, α commutes with $\dagger$, and (6.14) gives $A_\infty^{(1-j),\vee} \cong (\mathfrak{X}_\infty^{(j)})^\dagger$ for j even. Therefore

$$\alpha(X_\infty^{(j)}) \cong A_\infty^{(j),\vee} \quad \text{and} \quad \alpha((X_\infty^{(1-j)})^\dagger) \cong \mathfrak{X}_\infty^{(j)}.$$

Finally, from $(\Lambda_G^{(j)}/\mathfrak{D}_\infty^{(j)})_{\Gamma_n} \cong (\mathbb{Z}_p[G_n]/\mathfrak{D}_n)^{(j)}$ and Theorem 4 one deduces that $\alpha(\Lambda_G^{(j)}/\mathfrak{D}_\infty^{(j)})$ is the projective limit of the groups $\mathbb{Z}_p \otimes (\tilde{E}_n/\tilde{C}_n) \cong (\mathbb{Z}_p \otimes E_n^1)/(\mathbb{Z}_p \otimes C_n^1)$ with respect to the norm maps. Now, since Leopoldt's Conjecture holds for K_n, there is an isomorphism $\mathbb{Z}_p \otimes E_n^1 \to \hat{E}_n^1$ taking $\mathbb{Z}_p \otimes C_n^1$ to $\hat{C}_n^1$. Hence $(\mathbb{Z}_p \otimes E_n^1)/(\mathbb{Z}_p \otimes C_n^1) \cong \hat{E}_n^1/\hat{C}_n^1$ and the compactness of $\hat{E}_n^1$ gives

$$\alpha(\Lambda_G^{(j)}/\mathfrak{D}_\infty^{(j)}) \cong (\hat{E}_\infty^1/\hat{C}_\infty^1)^{(j)}.$$

Despite these relations between the terms of (7.12) and (7.9), it is not obvious to the author that one sequence follows directly from the other, or even whether such neat relations are to be expected between the terms of appropriately generalised sequences for any abelian K.

Acknowledgments. My thanks are due to Jean-Robert Belliard, Ralph Greenberg and Romyar Sharifi for their comments, and particularly to Thong Nguyen Quang Do for helpful discussions and for drawing my attention to [KS], [IS] and the possibility of some connection with [NN], yet to be determined. I am also very grateful to an anonymous referee for useful comments on an earlier version of this paper.

References

[AH] 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.

[BB] D. Burns and J. Barrett, *Annihilating Selmer modules*, J. Reine Angew. Math. 675 (2013), 191–222.

[BN] J.-R. Belliard and T. Nguyen Quang Do, *On modified circular units and annihilation of real classes*, Nagoya Math. J. 177 (2005), 77–115.

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

[CG] P. Cornacchia and C. Greither, *Fitting ideals of class groups of real fields with prime power conductor*, J. Number Theory 73 (1998), 459–471.

[Gn] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. 98 (1976), 263–284.

[Gt] C. Greither, *Determining Fitting ideals of minus class groups via the equivariant Tamagawa number conjecture*, Compos. Math. 143 (2007), 1399–1426.

[IS] H. Ichimura and K. Sakaguchi, *The non-vanishing of a certain Kummer character χ_m (after C. Soulé), and some related topics*, in: Galois Representations and Arithmetic Algebraic Geometry, Y. Ihara (ed.), Adv. Stud. Pure Math. 12, Kinokuniya, 1987, 53–64.

[I1] K. Iwasawa, *On some modules in the theory of cyclotomic fields*, J. Math. Soc. Japan 20 (1964), 42–82.

[I2] K. Iwasawa, *On $\mathbb{Z}_l$-extensions of algebraic number fields*, Ann. of Math. 98 (1973), 246–326.

[KS] J. S. Kraft and R. Schoof, *Computing Iwasawa modules of real quadratic number fields*, Compos. Math. 97 (1995), 135–155; Erratum, ibid. 103 (1996), 241.

[LMN] M. Le Floc'h, A. Movahhedi and T. Nguyen Quang Do, *On capitulation cokernels in Iwasawa theory*, Amer. J. Math. 127 (2005), 851–877.

[MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$, Invent. Math. 76 (1984), 179–330.

[Ne] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, 1999.

[Ng] T. Nguyen Quang Do, *Sur la torsion de certains modules galoisiens II*, in: Séminaire de Théorie des Nombres, Paris, 1986–87, Progr. Math. 75, Birkhäuser, 1988, 271–297.

[NN] T. Nguyen Quang Do et V. Nicolas, *Nombres de Weil, sommes de Gauss et annulateurs galoisiens*, Amer. J. Math. 133 (2011), 1533–1571.

[O] B. Oriat, *Annulation de groupes de classes réelles*, Nagoya Math. J. 81 (1981), 45–56.

[RS] X.-F. Roblot and D. Solomon, *Testing the Congruence Conjecture for Rubin–Stark elements*, J. Number Theory 130 (2010), 1374–1398.

[R] K. Rubin, *Global units and ideal class groups*, Invent. Math. 89 (1987), 511–526.

[Sc] R. Schoof, *Class numbers of real cyclotomic fields of prime conductor*, Math. Comp. 72 (2003), 913–937.

[Sh] R. Sharifi, *A reciprocity map and the two-variable* p*-adic* L*-function*, Ann. of Math. 173 (2011), 251–300.

[So1] D. Solomon, *Galois relations for cyclotomic numbers and* p*-units*, J. Number Theory 46 (1994), 158–178.

[So2] D. Solomon, *On twisted zeta-functions at* $s = 0$ *and partial zeta-functions at* $s = 1$, J. Number Theory 128 (2008), 105–143.

[So3] D. Solomon, *Abelian* L*-functions at* $s = 1$ *and explicit reciprocity for Rubin–Stark elements*, Acta Arith. 143 (2010), 145–189.

[W] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, 1997.

David Solomon
132 Hillfield Ave.
London N8 7DJ, United Kingdom
E-mail: david.solomon314@gmail.com

Received on 26.12.2011
and in revised form on 14.4.2013 (6919)