Can. J. Math. Vol. 47 (2), 1995 pp. 302–317.

THAINE'S METHOD FOR CIRCULAR UNITS AND A CONJECTURE OF GROSS

HENRI DARMON

ABSTRACT. We formulate a conjecture analogous to Gross' refinement of the Stark conjectures on special values of abelian L-series at $s = 0$. Some evidence for the conjecture can be obtained, thanks to the fundamental ideas of F. Thaine.

1. **Introduction.** This paper formulates a refined analogue of the usual class number formula for a real quadratic extension of $\mathbf{Q}$, using circular units. The statement of this conjecture is inspired by an analogous conjecture of Gross [Gr]. Strong evidence for this conjecture can be given thanks to F. Thaine's powerful method [Th] for generating relations in ideal class groups using circular units.

The first two sections briefly recall Dirichlet's analytic class number formula and Gross's refinement of it; they are there mainly to fix notations and provide motivation. Section 4 states the new conjecture. The remaining sections are devoted to proving various results that support it.

ACKNOWLEDGEMENTS. I wish to thank Massimo Bertolini and Benedict Gross for many stimulating conversations on the topics of this paper.

NOTATIONS. If K is a number field and w is a place of K lying above a prime v of $\mathbf{Q}$, we denote by K_w the localization of K at w, and let $\mathbf{N}w$ be the order of its residue field. The w-adic norm $\| \ \|_w$ is normalized so that it is equal to $\mathbf{N}w^{-1}$ on uniformizing elements.

Given a finite abelian extension M/K, we let

$$\text{rec}_w\colon K_w^* \longrightarrow \text{Gal}(M/K) \tag{1}$$

denote the reciprocity map of local class field theory. When w is unramified in M/K, it factors through the valuation map $K_w^* \longrightarrow \mathbf{Z}$ and maps uniformizing elements to Frob_w, the Frobenius element in $\text{Gal}(M/K)$ characterized by

$$\text{Frob}_w(x) = x^{\mathbf{N}w} \pmod{\tilde{w}}, \tag{2}$$

where $\tilde{w}$ is any place of M above w.

This work was supported at different stages by a Sloan Doctoral Dissertation fellowship, an NSERC postdoctoral fellowship, and by NSF grant # DMS-8703372.A04.

Received by the editors April 6, 1993.

AMS subject classification: 11R11, 11R04, 11R18, 11R27, 11R29.

We write $\mathrm{Div}(K)$ for the free $\mathbf{Z}$-module generated by the finite places of K, and $P(K)$ for the submodule generated by the principal divisors. The class group $C(K)$ is the quotient $\mathrm{Div}(K)/P(K)$. Given a set S of places of K, let $\langle S\rangle$ be the $\mathbf{Z}$-span of the elements of S in $\mathrm{Div}(K)$, and let

(3) $$C_S(K) = \langle S\rangle \setminus \mathrm{Div}(K)/P(K).$$

2. **Dirichlet's analytic class number formula.** We recall briefly the analytic class number formula of Dirichlet relating the behavior of the L-series of a number field at $s = 0$ to the arithmetic properties of that number field. The exposition follows closely the one in [Gr].

Let K be a number field, and choose a finite set S of places of K containing all of the archimedean places. Let T be a finite set of places of K disjoint from S.

There is associated to this situation the local data which describes the splitting of the primes in K. This data is conveniently encoded in the Euler product

(4) $$L_{S,T}(K,s) = \prod_{v\notin S}(1-\mathbf{N}v^{-s})^{-1}\prod_{v\in T}(1-\mathbf{N}v^{1-s}).$$

Here the products are taken over the non-archimedean places of K. The Euler product defines the L-function $L_{S,T}(K,s)$ in some right half plane of convergence, and it is known that $L_{S,T}(K,s)$ has a meromorphic continuation to the entire complex plane.

The number field K together with the sets S and T gives rise to more subtle global invariants.

1. The group $(\mathcal{O}_S^*)_T$ of S-units which are congruent to 1 modulo the places of T. This is a finitely generated abelian group which is free when T is large enough. Let r denote the rank of this group. By Dirichlet's unit theorem, one has $r = \#(S) - 1$.

2. The torsion subgroup $[(\mathcal{O}_S^*)_T]_{\mathrm{torsion}}$ which is cyclic of order $w_{S,T}$. (Typically we will choose T so that $w_{S,T} = 1$.)

3. The Picard group $\mathrm{Pic}(\mathcal{O}_S)_T$ of invertible $\mathcal{O}_S$-modules together with a trivialization at T. It is a finite extension of $C_S(K)$. Let $h_{S,T}$ denote its order.

4. The S-unit regulator $R_{S,T}$, defined as follows. Let $X = \mathrm{Div}^0(S)$ be the free abelian group generated by the formal linear combinations of places of S of degree 0,

$$X = \left\{\sum_{v\in S} n_v v, \quad \sum n_v = 0\right\}.$$

The logarithmic embedding $\log_S\colon \mathcal{O}_S^* \longrightarrow \mathbf{R}\otimes X$ of the S-units is defined by

(5) $$\log_S(u) = \sum_{v\in S}\log\|u\|_v \otimes v.$$

Both $(\mathcal{O}_S^*)_T$ and X are of rank r. Let

(6) $$\Lambda^r\log_S\colon \Lambda^r\mathcal{O}_S^* \longrightarrow \Lambda^r(\mathbf{R}\otimes X)$$

denote the map induced by $\log_S$ on the top exterior powers, and define the regulator $R_{S,T}$ by

(7) $$\Lambda^r\log_S(\gamma_1\wedge\cdots\wedge\gamma_r) = R_{S,T}\otimes(v_1\wedge\cdots\wedge v_r),$$

where $\gamma_1, \ldots, \gamma_r$ (resp. $v_1, \ldots, v_r$) are integral bases for $(O_S^*)_T$ modulo torsion (resp. X), normalized so that $R_{S,T}$ is positive.

The theorem of Dirichlet asserts that the above global invariants appear in the Taylor expansion of the L-function $L_{S,T}(K,s)$ which was constructed using purely local data. It is one of the simplest manifestations of a local global principle which is pervasive in number theory.

THEOREM 2.1 (DIRICHLET). *1. The L-series $L_{S,T}(K,s)$ vanishes to order r at $s=0$.*
2. The Taylor expansion of $L_{S,T}(K,s)$ at $s=0$ is given by:

$$L_{S,T}(K,s) = -\frac{h_{S,T}R_{S,T}}{w_{S,T}}s^r + O(s^{r+1}).$$

3. **Gross's refined class number formula.** We now turn to the refined class number formula of Gross, following closely the account given in [Gr].

Let L be a finite abelian extension of K which is unramified outside the places of S, and let $G = \mathrm{Gal}(L/K)$. Define a complex-valued function $\hat{\theta}_G$ on the dual group $\hat{G} = \hom(G, \mathbf{C}^*)$ by

$$\hat{\theta}_G(\chi) = L_{S,T}(K,\chi,0), \tag{8}$$

where, for a complex character $\chi\colon G \longrightarrow \mathbf{C}^*$ and a complex number s with $\Re s > 1$, the complex function $L_{S,T}(K,\chi,s)$ is defined by the convergent Euler product

$$L_{S,T}(K,\chi,s) = \prod_{v \notin S}\left(1 - \chi(\mathrm{Frob}_v)\mathbf{N}v^{-s}\right)^{-1}\prod_{v\in T}\left(1 - \chi(\mathrm{Frob}_v)\mathbf{N}v^{1-s}\right).$$

This function has a meromorphic continuation to the entire complex plane and is regular at $s=0$. Let $\theta_G \in \mathbf{C}[G]$ be the Fourier transform of $\hat{\theta}_G$,

$$\theta_G = \sum_{\chi\in\hat{G}}\hat{\theta}_G(\chi)e_\chi, \quad e_\chi = 1/|G|\sum_{g\in G}\chi(g)g^{-1}.$$

Thus, $\theta_G = \sum_{g\in G} a(g)g$ interpolates values of $L_{S,T}(K,\chi,0)$,

$$\sum_{g\in G} a(g)\chi(g) = L_{S,T}(K,\chi,0). \tag{9}$$

For the rest of this section, we make the following assumption on T, which forces $w_{S,T}=1$ so that the leading term in the class number formula is integral.

HYPOTHESIS 3.1. *Suppose that T contains two primes of unequal residue characteristic, or that T contains a prime whose absolute ramification index in K is strictly less that the residue field characteristic minus* 1.

Under this condition, Gross [Gr] shows that the element θ_G belongs to the integral group ring $\mathbf{Z}[G]$.

FACT 3.2 (GROSS). θ_G belongs to $\mathbf{Z}[G]$.

The order of vanishing of θ_G: Let I denote the augmentation ideal in the group ring $\mathbf{Z}[G]$. It is the kernel of the augmentation homomorphism $\epsilon: \mathbf{Z}[G] \longrightarrow \mathbf{Z}$ which sends $\sigma \in G$ to 1. The powers $I \supset I^2 \supset \cdots$ define a decreasing filtration on $\mathbf{Z}[G]$. Because of the exact sequence

$$0 \longrightarrow I \longrightarrow \mathbf{Z}[G] \xrightarrow{\epsilon} \mathbf{Z} \longrightarrow 0, \tag{10}$$

one has $\mathbf{Z}[G]/I = \mathbf{Z}$. The higher quotients in the filtration are torsion. For instance, there is a natural homomorphism $G \longrightarrow I/I^2$ which sends $\sigma \in G$ to $\sigma - 1 \pmod{I^2}$. In fact, this is an isomorphism. More generally, there is a natural surjective map

$$\mathrm{Sym}^r(G) \longrightarrow I^r/I^{r+1} \tag{11}$$

which sends $\sigma_1 \otimes \cdots \otimes \sigma_r$ to $(\sigma_1 - 1) \cdots (\sigma_r - 1) \pmod{I^{r+1}}$. (This map is not necessarily an isomorphism; for a detailed study of the map $\mathrm{Sym}(G) \longrightarrow \oplus_r I^r/I^{r+1}$, the reader may consult [Pa], [H1], [H2].)

The element θ_G which interpolates special values at $s = 0$ of the twisted L-function $L_{S,T}(K, \chi, s)$ is what plays the role of the L-function in Gross's refined class number formula. To say that this element vanishes to order r is to say that it belongs to the r-th power of the augmentation ideal.

CONJECTURE 3.3 (GROSS). *The element θ_G belongs to I^r.*

The leading coefficient $\tilde{\theta}_G$ in the refined class number formula is defined to be the projection of θ_G to I^r/I^{r+1}. It is natural to search for an interpretation of $\tilde{\theta}_G$ which is analogous to the analytic result of Dirichlet.

To do this, it suffices to change the definition of the regulator term $R_{S,T}$ defined in the previous section. Consider the homomorphism

$$\mathrm{rec}_S \colon O_S^* \longrightarrow (I/I^2) \otimes_{\mathbf{Z}} X \tag{12}$$

defined by

$$\mathrm{rec}_S(u) = \sum_{v \in S} \left(\mathrm{rec}_v(u_v) - 1\right) \otimes v, \tag{13}$$

where $u_v \in K_v^*$ is the natural image of u. Let $\Lambda^r \,\mathrm{rec}_S$ denote the induced map on the top exterior powers:

$$\Lambda^r \,\mathrm{rec}_S \colon \Lambda^r O_S^* \longrightarrow \Lambda^r(I/I^2 \otimes X) \longrightarrow (I^r/I^{r+1}) \otimes \Lambda^r X,$$

and define the regulator $R_{S,T}$ in I^r/I^{r+1} by

$$\Lambda^r \,\mathrm{rec}_S(\gamma_1 \wedge \cdots \wedge \gamma_r) = R_{S,T} \otimes (v_1 \wedge \cdots \wedge v_r), \tag{14}$$

where $\gamma_1, \ldots, \gamma_r$ and $v_1, \ldots, v_r$ are the integral bases chosen in Section 2.

CONJECTURE 3.4 (GROSS).

$$\tilde{\theta}_G = -h_{S,T} R_{S,T}.$$

REMARKS. 1. If K has a complex place v, then the Γ-factors in the functional equation force a zero at $s = 0$ in the twisted L-function $L_{S,T}(K, \chi, s)$ for all χ. Hence $\theta_G = 0$. But rec_v is trivial, so that $R_{S,T} = 0$ as well. Therefore the conjecture is trivially verified. It is only interesting when K is a totally real field.

2. Because of the presence of the archimedean places, one has $2R_{S,T} = 0$ in I^r/I^{r+1}. (Also one can show that $2\tilde{\theta}_G \doteq 0$.) Thus Gross's conjecture for number fields is really a parity statement—it was proved by Gross when S contains only the archimedean places by using the 2-adic congruences of Deligne-Ribet for totally real fields [DR].

4. **A refined conjecture for circular units.** Let ω be an even primitive Dirichlet character of conductor N. In order to simplify the exposition, we assume that ω is quadratic, and let K denote the corresponding real quadratic field. Choose an auxiliary real abelian extension M of $\mathbf{Q}$ with conductor prime to N, and let G denote its Galois group. For all χ in $\hat{G}$, the Dirichlet L-series

$$L_S(s, \omega\chi) = \sum_{(n,S)=1}^{\infty} \omega\chi(n)n^{-s} = \prod_{p \nmid S} \left(1 - \omega\chi(p)p^{-s}\right)^{-1} \tag{15}$$

vanishes at $s = 0$, because of the pole in the factor $\Gamma(\frac{1}{2}s)$ in the functional equation. One might be tempted to define a function $\hat{\theta}'_G$ on $\hat{G}$ by $\hat{\theta}'_G(\chi) = L'_S(0, \omega\chi)$, and letting $\theta'_G \in \mathbf{C}[G]$ be its Fourier transform as in Section 3. However, the coefficients of θ'_G are not integral, or even algebraic. This leads to the problem of finding an appropriate substitute for θ'_G, and formulating a conjecture analogous to conjectures 3.3 and 3.4 for it.

Fix a choice of primitive n-th roots of unity $\zeta_n \in \bar{\mathbf{Q}}$ for each n, satisfying the compatibilities

$$\zeta_{nm}^m = \zeta_n. \tag{16}$$

This choice determines a complex embedding Ψ of $\mathbf{Q}^{ab}$, sending ζ_n to $e^{2\pi i/n}$.

Let S be a square-free integer which is relatively prime to the conductor of ω. Let $K_S = K(\mu_S)$. The circular unit α_S in K_S is defined by

$$\alpha_S = \prod_{\sigma \in \mathrm{Gal}(\mathbf{Q}(\mu_{SN})/\mathbf{Q}(\mu_S))} \sigma(\zeta_{NS} - 1)^{\omega(\sigma)}. \tag{17}$$

Let $\Gamma_S = \mathrm{Gal}(K_S/K)$, and let I denote the augmentation ideal in the group ring $\mathbf{Z}[\Gamma_S]$. The theta-element $\theta'(\omega, S)$ is given by the formula

$$\theta'(\omega, S) = \sum_{\sigma \in \Gamma_S} \sigma\alpha_S \otimes \sigma \in K_S^* \otimes \mathbf{Z}[\Gamma_S]. \tag{18}$$

Relation between $\theta'(\omega, S)$ and $L'_S(0, \omega\chi)$: Let $\log: K_S^* \longrightarrow \mathbf{C}$ be a principal branch of the logarithm map induced by the complex embedding Ψ of K_S. Extending a character $\chi \in \hat{\Gamma}_S$ by linearity to the group ring $\mathbf{Z}[\Gamma_S]$, one combines the maps log and χ to give a linear map

$$\log \otimes \chi: K_S^* \otimes \mathbf{Z}[\Gamma_S] \longrightarrow \mathbf{C}.$$

We call a character χ of Γ_S *primitive* if it does not factor through the natural homomorphism $\Gamma_S \longrightarrow \Gamma_T$ for any proper divisor T of S. The following theorem which describes the interpolation property of the circular units is due to Kummer.

THEOREM 4.1. *Assume that χ is primitive. Then*

$$\log \otimes \chi\big(\theta'(\omega, S)\big) = \sum_{\sigma \in \Gamma_S} \chi(\sigma) \log |\sigma\alpha_S| = -2L'_S(0, \omega\chi).$$

Thus $\theta'(\omega, S)$ can be viewed as an analogue of $L'_S(s, \omega)$.

Let

$$S_{\text{split}} = \{l | S, \omega(l) = 1\}$$
$$S_{\text{inert}} = \{l | S, \omega(l) = -1\}.$$

Let X^- be the group of divisors of K of degree 0 lying above S or ∞ on which the generator of $\mathrm{Gal}(K/\mathbf{Q})$ acts by -1. It is a free $\mathbf{Z}$-module of rank r, where

(19) $$r = \#(S_{\text{split}}) + 1.$$

Let $v_\infty = \lambda_\infty - \bar{\lambda}_\infty$ be the difference of the two conjugate real places of K, and let $v_i = \lambda_i - \bar{\lambda}_i$, where $\lambda_i, \bar{\lambda}_i$ denote conjugate primes of K lying above $l_i \in S_{\text{split}}$. Then $\{v_\infty, v_1, \ldots, v_{r-1}\}$ forms a basis for X^-. Let $(\mathcal{O}_S^*)^-$ be the group of S-units of K on which the generator of $\mathrm{Gal}(K/\mathbf{Q})$ acts by -1. This is also a free $\mathbf{Z}$-module of rank r. Choose a basis $\omega_1, \ldots, \omega_r$ for $(\mathcal{O}_S^*)^-$ in such a way that the regulator R_S for the logarithmic embedding

(20) $$(\mathcal{O}_S^*)^- \longrightarrow X^- \otimes \mathbf{R}$$

relative to the bases $\{\omega_1, \ldots, \omega_r\}$ and $\{v_\infty, v_1, \ldots, v_{r-1}\}$ is positive.

From the non-vanishing of the classical Dirichlet L-series at $s = 1$ combined with the functional equation for these L-series, one knows that

(21) $$\mathrm{ord}_{s=0} L'_S(s, \omega) = r - 1,$$

and that

(22) $$\lim_{s \to 0} L'_S(s, \omega)/(s^{r-1}) = -2^{\#S_{\text{inert}}+1} r h_S R_S.$$

In the next section, we will show that a similar statement is true for the element $\theta'(\omega, S)$:

THEOREM 4.2 (ORDER OF VANISHING). *The element $\theta'(\omega, S)$ belongs to the group $K_S^* \otimes I^{r-1}$.*

The leading coefficient $\tilde{\theta}'(\omega, S)$ is defined to be the natural projection of $\theta'(\omega, S)$ to the group $K_S^* \otimes (I^{r-1}/I^r)$. One can interpret $\theta'(\omega, S)$ by means of a kind of S-unit regulator belonging to $\mathcal{O}_S^* \otimes (I^{r-1}/I^r)$.

The regulator: Let Y^- denote the group of divisors of K of degree 0 lying above S on which $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ acts via the character ω. This is a free module of rank $r-1$ with basis $\{v_1, \ldots, v_{r-1}\}$. One defines the map

$$\text{(23)} \qquad \mathrm{rec}_S\colon (O_S^*)^- \longrightarrow I_S \otimes Y^-$$

using the reciprocity law of local class field theory as in Section 3. Define the *partial regulators* $R_i \in I_S^{r-1}/I_S^r$ by the formula

$$\text{(24)} \qquad \mathrm{rec}_S(\gamma_1 \wedge \cdots \wedge \gamma_{i-1} \wedge \gamma_{i+1} \wedge \cdots \wedge \gamma_r) = R_i \otimes (v_1 \wedge \cdots \wedge v_{r-1}).$$

The regulator $R_S \in O_S^* \otimes (I^{r-1}/I^r)$ is given by

$$\text{(25)} \qquad R_S = \sum_{i=1}^{r} (-1)^{i+1} \gamma_i \otimes R_i.$$

CONJECTURE 4.3.

$$\tilde{\theta}'(\omega, S) = -2^{\#(S_{\mathrm{inert}})+1} h_S R_S.$$

We now give some evidence for Conjecture 4.3. Let $\tilde{\theta}'(\omega, S)_2$ denote the projection of $\tilde{\theta}'(\omega, S)$ in the group $K_S^* \otimes (I_2^{r-1}/I_2^r)$, where I_2 denotes the augmentation ideal in the group ring $\mathbf{Z}[\frac{1}{2}][\Gamma_S]$. The tensoring with the ring $\mathbf{Z}[\frac{1}{2}]$ has been made to avoid some technical complications associated with the prime 2: observe that $(I_2^{r-1}/I_2^r) = (I^{r-1}/I^r) \otimes \mathbf{Z}[\frac{1}{2}]$ is a finite abelian group of odd order, when $r > 1$.

FACT 4.4. The natural map $K^* \otimes (I_2^{r-1}/I_2^r) \longrightarrow K_S^* \otimes (I_2^{r-1}/I_2^r)$ is an injection.

The proof for this standard fact will be given in Section 9.

Let $n(S)$ be the greatest odd divisor of $\gcd_{l|S}(l-1)$. The following theorem gives some evidence for Conjecture 4.3:

THEOREM 4.5. *1. Conjecture 4.3 is true when* $r = 1$.

2. $\tilde{\theta}'(\omega, S)_2$ *belongs to* $K^* \otimes I_2^{r-1}/I_2^r$.

3. If $\gcd\big(h_S(K), n(T)\big) = 1$ *for all* $T|S$, *then* $\tilde{\theta}'(\omega, S)_2$ *belongs to* $O_s^* \otimes (I_2^{r-1}/I_2^r)$.

4. $h_S(K)$ *divides* $\tilde{\theta}'(\omega, S)_2$.

5. Suppose that $\Gamma_S = \Gamma_l$ *is cyclic, and that* l *is split in* $K/\mathbf{Q}$ *so that* $r = 2$. *Let* λ *be a prime of* K *above* l, *and let* $k_\lambda \simeq \mathbf{F}_l$ *denote the residue field at* λ. *If the fundamental unit of* $K/\mathbf{Q}$ *is a generator for* k_λ^*, *and* $\gcd\big(h(K), n(l)\big) = 1$, *then*

$$\tilde{\theta}'(\omega, l)_2 = \pm 2 h_l R_l \pmod{I_2^2}.$$

The proof of this theorem, which uses the methods of Thaine [Th] in an essential way, will be given in Section 9.

5. **The Euler system of circular units.** Let $\mathcal{S}$ be the set of square-free integers prime to the conductor of K. For all $S \in \mathcal{S}$ we are given the following data:

1. An abelian extension $K_S = K(\mu_S)$ of K with Galois group $\Gamma_S = (\mathbf{Z}/S\mathbf{Z})^*$.
2. The circular unit $\alpha(S)$ in K_S, given by the formula

$$\alpha(S) = \prod_{\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_{SN})/\mathbf{Q}(\zeta_S))} \sigma(\zeta_{SN} - 1)^{\omega(\sigma)}. \tag{26}$$

Writing $S = l_1 \cdots l_s$, the extension K_S is a compositum of the fields K_{l_i} which are linearly disjoint over K. Hence there is a canonical direct product decomposition

$$\Gamma_S = \Gamma_{l_1} \times \cdots \times \Gamma_{l_s} \tag{27}$$

which gives inclusions $\Gamma_T \subset \Gamma_S$ for all divisors T of S. We will implicitly identify elements of Γ_T with their images in Γ_S. For any T dividing S, the partial norm operator $\mathbf{N}_T$ in the group ring $\mathbf{Z}[\Gamma_S]$ is defined by

$$\mathbf{N}_T = \sum_{\sigma \in \Gamma_T} \sigma. \tag{28}$$

These operators act on the field K_S in the natural way. Given $T \in \mathcal{S}$ and l a prime in $\mathcal{S}$ which is prime to T, let $\sigma_{l,T} \in \mathrm{Gal}(K_T/\mathbf{Q})$ be the automorphism sending the roots of unity to their l-th powers.

PROPOSITION 5.1.

$$N_l\big(\alpha(Tl)\big) = (1 - \sigma_{l,T}^{-1})\alpha(T).$$

PROOF. We can write

$$\zeta_{Tl} = \zeta_T^a \zeta_l^b, \tag{29}$$

where $al + bT = 1$. Hence

$$N_l(1 - \zeta_{Tl}) = (1 - \zeta_T^{al})/(1 - \zeta_T^a) = (1 - \sigma_{l,T}^{-1})(1 - \zeta_T),$$

and the proposition follows from the definition of the circular units $\alpha(T)$ and $\alpha(Tl)$.

PROPOSITION 5.2. $\alpha(Tl) \equiv \sigma_{l,T}^{-1}\alpha(T) \pmod{\lambda}$, *where λ is any prime of K_{Tl} above l.*

PROOF. This follows from equation (29) together with the fact that a is an inverse for l in $(\mathbf{Z}/T\mathbf{Z})^*$ and that $\zeta_l \equiv 1 \pmod{\lambda}$.

Propositions 5.1 and 5.2 make up the axioms of an Euler system in the sense of Kolyvagin [Ko].

6. **Divisibility properties of the circular units.** In addition to the norm operator $\mathbf{N}_l$ defined in the previous section, the following derivative operators in the group ring $\mathbf{Z}[\Gamma_S]$ are a key ingredient in Kolyvagin and Thaine's method. For each prime l in $\mathcal{S}$, choose a generator γ_l for Γ_l and let

$$\mathrm{D}_l = \sum_{i=1}^{l-2} i\gamma_l^i, \quad \mathrm{D}_T = \prod_{l|T} \mathrm{D}_l, \tag{30}$$

the product being taken in the group ring $\mathbf{Z}[\Gamma_T]$.

LEMMA 6.1. $(\gamma_l - 1)\mathrm{D}_l = (l - 1) - \mathbf{N}_l$.

PROOF. A direct computation.

The group ring $\mathbf{Z}[\Gamma_T]$ operates on the group K_T^* in a natural way. Let

$$\beta(T) = \mathrm{D}_T\alpha(T) \in K_T^*, \tag{31}$$

and let $n(T)$ be the largest odd divisor of $\gcd_{l|T}(l-1)$.

From now on, we will assume that T is a product of primes which are split in $K/\mathbf{Q}$. Although $\beta(T)$, unlike $\mathbf{N}_T\alpha(T)$, need not be invariant under the action of Γ_T, it is invariant modulo $n(T)$-th powers.

LEMMA 6.2. *$\beta(T)$ belongs to $(K_T^*/K_T^{*n(T)})^{\Gamma_T}$.*

PROOF. By induction on the number of primes dividing T. Assume the lemma for all proper divisors of T, and write $T = lQ$. Modulo $n(T)$, one has:

$$\begin{aligned}(\gamma_l - 1)\mathrm{D}_T\alpha(T) &= (l-1-\mathbf{N}_l)\mathrm{D}_Q\alpha(T) \quad \text{(Lemma 6.1)}\\ &= (\sigma_{l,Q}^{-1} - 1)\mathrm{D}_Q\alpha(Q) \quad \text{(Proposition 5.1)}\\ &= 0 \quad \text{by the induction hypothesis.}\end{aligned}$$

In the last step we use the fact that $\sigma_{l,Q} = 1$ in $\mathrm{Gal}(K/Q)$, so that $\sigma_{l,Q}$ belongs to Γ_Q.

LEMMA 6.3. *The natural map $K^*/K^{*n(T)} \longrightarrow (K_T^*/K_T^{*n(T)})^{\Gamma_T}$ is an isomorphism.*

PROOF. The group of $n(T)$-th roots of unity in K_T is trivial. Hence the sequence

$$1 \longrightarrow K_T^* \xrightarrow{n(T)} K_T^* \longrightarrow K_T^*/K_T^{*n_T} \longrightarrow 1 \tag{32}$$

is exact. Taking Γ_T-invariants gives rise to the cohomology exact sequence

$$1 \longrightarrow K^*/K^{*n(T)} \longrightarrow (K_T^*/K_T^{*n(T)})^{\Gamma_T} \longrightarrow H^1(\Gamma_T, K_T^*)_{n(T)} \longrightarrow 1, \tag{33}$$

and the lemma follows from Hilbert's Theorem 90 ($H^1(\Gamma_T, K_T^*) = 0$).

Let $\kappa(T)$ denote the preimage of $\beta(T)$ by this isomorphism. For each prime l in S, choose a place λ of K above it. Write

$$v_\lambda : K^* \longrightarrow \mathbf{Z} \tag{34}$$

for the valuation map at λ, and $\tilde{v}_\lambda$ for the induced map on $K^*/K^{*n(T)}$, making the following diagram commute:

$$\begin{array}{ccc} K^* & \xrightarrow{v_\lambda} & \mathbf{Z} \\ \downarrow & & \downarrow \\ K^*/K^{*n(T)} & \xrightarrow{\tilde{v}_\lambda} & \mathbf{Z}/n(t)\mathbf{Z} \end{array}.$$

Let u_l denote the image of γ_l by the isomorphism $\Gamma_l \longrightarrow (\mathbf{Z}/l\mathbf{Z})^*$. Given κ in K^*, let $\mathrm{red}_\lambda(\kappa) \in k_\lambda^*$ be the reduction of κ mod λ, in the residue field $k_\lambda = \mathbf{Z}/l\mathbf{Z}$. Finally, let

$$\log_{u_l} : k_\lambda^* \longrightarrow \mathbf{Z}/(l-1)\mathbf{Z} \tag{35}$$

be the logarithm map to the base u_l. The following proposition contains the information that we will need on the ideal factorization of the $\kappa(T)$.

PROPOSITION 6.4. *1. If l does not divide T, then $\tilde{v}_\lambda\big(\kappa(T)\big) = 0$.*
2. If l is split in $K_T/\mathbf{Q}$, then

$$\tilde{v}_\lambda\big(\kappa(Tl)\big) = -\log_{u_l}\Big(\mathrm{red}_\lambda\big(\kappa(T)\big)\Big)\big(\mathrm{mod}\, n(Tl)\big).$$

PROOF. 1. If l does not divide T, then λ is unramified in K_T/K, and hence the valuation map $\tilde{v}_\lambda$ extends from $K^*/K^{*n(T)}$ to $K_T^*/K_T^{*n(T)}$. But clearly $\tilde{v}_\lambda\big(\beta(T)\big) = 0$, since $\beta(T)$ is a unit in K_T^*.

2. Let λ' be a prime of K_T above λ, and let λ'' be the prime of K_{Tl} above λ'. Let $v_{\lambda'}$ (resp. $v_{\lambda''}$) be the valuations on K_T (resp K_{Tl}) normalized to be 1 on uniformizing elements, so that

$$v_{\lambda'}(\kappa) = \frac{1}{l-1} v_{\lambda''}(\kappa), \qquad \kappa \in K_T^*. \tag{36}$$

Writing

$$\kappa(Tl) = \beta(Tl)\rho^{-n(Tl)}, \qquad \rho \in K_{Tl}, \tag{37}$$

and using the fact that $\beta(Tl)$ is a unit, one finds

$$v_\lambda\big(\kappa(Tl)\big) = -\frac{n(Tl)}{l-1} v_{\lambda''}(\rho). \tag{38}$$

By definition of u_l, one has

$$v_{\lambda''}(\rho) = \log_{u_l}\Big(\mathrm{red}_{\lambda''}\big((\gamma_l - 1)\rho\big)\Big) \pmod{l-1}. \tag{39}$$

But

$$\begin{aligned}(\gamma_l - 1)\rho &= \frac{1}{n(Tl)}[(\gamma_l - 1)\beta(Tl)] \\ &= \frac{1}{n(Tl)}[(l-1)\mathrm{D}_T\alpha(Tl) + (1 - \sigma_{l,T}^{-1})\mathrm{D}_T\alpha(T)] \\ &= \frac{l-1}{n(Tl)}\mathrm{D}_T\alpha(Tl), \qquad \text{since } \sigma_{l,T} = 1.\end{aligned}$$

Hence by Proposition 5.2,

$$\mathrm{red}_{\lambda''}\big((\gamma_l - 1)\rho\big) = \mathrm{red}_{\lambda'}\left(\frac{l-1}{n(Tl)}\mathrm{D}_T\alpha(T)\right), \tag{40}$$

and hence

$$\log_{u_l}\mathrm{red}_{\lambda''}\big((\gamma_l - 1)\rho\big) \equiv \log_{u_l}\mathrm{red}_{\lambda'}\left(\frac{l-1)}{n(Tl)}\beta(T)\right) \pmod{l-1}. \tag{41}$$

Combining equations (38), (39) and (41), one obtains

$$\tilde{v}_\lambda\big(\kappa(Tl)\big) \equiv -\log_{u_l}\big(\mathrm{red}_\lambda\, \kappa(T)\big)\big(\mathrm{mod}\, n(Tl)\big) \tag{42}$$

as desired.

If M is a $\mathbf{Z}$-module and m belongs to M, we say that $n \in \mathbf{Z}$ divides m if there exists $m' \in M$ with $n \cdot m' = m$. Given a rational prime p, one defines $\operatorname{ord}_p(m)$ to be the integer M such that p^M divides m, but p^{M+1} does not. (If this integer does not exist one sets $\operatorname{ord}_p(m) = \infty$.) Recall that $C_S(K)$ is defined to be the quotient of the ideal class group of K by the subgroup generated by the prime ideals lying above S, and that $h_S(K)$ denotes its order. The main result of Thaine and Kolyvagin gives a bound on the order of $C_S(K)$ in terms of the divisibilty of the elements $\kappa(S)$.

THEOREM 6.5 (THAINE, KOLYVAGIN). *The greatest common divisor of $n(S)$ and $h_S(K)$ divides $\kappa(S)$.*

PROOF. We prove this by induction on $h_S(K)$. If $h_S(K) = 1$, then the theorem is trivially true. Otherwise, choose a prime p dividing $h_S(K)$. Suppose that $\operatorname{ord}_p\big(\kappa(S)\big) = M_0 < \infty$, and let $M = M_0 + 1$. We must show that p^M does not divide $\gcd\big(n(S), h_S(K)\big)$. If p^M does not divide $n(S)$, we are done. Hence, suppose that p^M divides $n(S)$. (So that in particular, p is odd). Now, choose a prime l in $\mathcal{S}$ not dividing S, such that

1. l splits in $K/\mathbf{Q}$; let λ denote a prime of K lying above it.
2. $l \equiv 1 \pmod{P^M}$ (*i.e.*, l splits in $\mathbf{Q}(\mu_{p^M})/\mathbf{Q}$).
3. $\operatorname{ord}_p\Big(\operatorname{red}_\lambda\big(\kappa(S)\big)\Big) = M_0$.
4. The image of λ in $C_S(K) \otimes \mathbf{Z}_p$ is non trivial, and the exact sequence
$$0 \longrightarrow \langle\lambda\rangle \longrightarrow C_S(K) \otimes \mathbf{Z}_p \longrightarrow C_{Sl}(K) \otimes \mathbf{Z}_p \longrightarrow 0$$
is split (and hence in particular $\operatorname{ord}_p(\lambda) = 0$).

Let $F = K\big(\mu_{p^M}, \kappa(S)^{1/p^M}\big)$. Conditions 2 and 3 are equivalent to the condition that $\operatorname{Frob}_\lambda$ in $\operatorname{Gal}(F/K)$ belongs to the subgroup $\operatorname{Gal}\big(F/K(\mu_{p^M})\big)$ and is non-trivial. Condition 4 is equivalent to a condition on $\operatorname{Frob}_\lambda$ in $\operatorname{Gal}(H_S/K)$ where H_S is a non-trivial subfield of the Hilbert class field H of K. Since F and H are linearly disjoint over K (as can be seen for example by ramification considerations), it follows from the Chebotarev density theorem that conditions 1–4 can be imposed simultaneously.

Let $m = \operatorname{ord}_p\big(\kappa(Sl)\big)$. By combining Proposition 6.4 with condition 3 satisfied by l, one has

$$\operatorname{ord}_p\Big(\tilde{v}_\lambda\big(\kappa(Sl)\big)\Big) = M_0, \tag{43}$$

and hence a *fortiori* $m \leq M_0$. Moreover, since p^M divides $l - 1$, it also divides $n(Sl)$. Let ρ be the natural projection of $\kappa(Sl)$ to K^*/K^{*p^M}, and let $\kappa'(Sl) = \rho^{1/p^m}$ which is well defined in $K^*/K^{*p^{M-m}}$. By equation 43 and condition 3, one has

$$\tilde{v}_\lambda\big(\kappa'(Sl)\big) = u \cdot p^{M_0 - m}, \tag{44}$$

where u is a unit in $\mathbf{Z}/p^{M-m}\mathbf{Z}$. Hence p^{M_0-m} annihilates the class of λ in $C(S) \otimes \mathbf{Z}/p^{M-m}\mathbf{Z}$. Because of condition 4, we have

$$\#\langle\lambda\rangle \leq p^{M_0-m}. \tag{45}$$

In particular, $m < M_0$, and by the induction hypothesis,

$$\#C_{Sl}(K) \otimes \mathbf{Z}_p \leq p^m. \tag{46}$$

Combining the inequalities (45) and (46) gives

$$\#C_S(K) \otimes \mathbf{Z}_p \leq p^{M_0}, \tag{47}$$

so that p^M does not divide $h_S(K)$, as was to be shown.

7. **Formal properties of $\theta'(\omega, S)$.** We now turn to the study of the element $\theta'(\omega, S)$ defined by

$$\theta'(\omega, S) = \sum_{\sigma \in \Gamma_S} \sigma\alpha(S) \otimes \sigma \in K_S^* \otimes \mathbf{Z}[\Gamma_S]. \tag{48}$$

Given

$$\gamma \in \mathrm{Gal}(K_S/\mathbf{Q}) = \Gamma_S \times \mathrm{Gal}(K/\mathbf{Q}),$$

let $\gamma(T)$ denote its natural projection in Γ_T.

The group $\mathrm{Gal}(K_S/\mathbf{Q})$ acts on the left of $K_S^* \otimes \mathbf{Z}[\Gamma_S]$ by the Galois action, and Γ_S acts on the right by multiplication in the group ring.

LEMMA 7.1. $\gamma\theta'(\omega, S) = \omega(\gamma) \cdot \theta'(\omega, S) \cdot \gamma(S)^{-1}$.

PROOF. A change of variable argument.

Given a divisor T of S, let $P_{S,T}\colon K_S^* \otimes \mathbf{Z}[\Gamma_S] \longrightarrow K_S^* \otimes \mathbf{Z}[\Gamma_S]$ be the map induced by the projection $\Gamma_S \longrightarrow \Gamma_T \subset \Gamma_S$.

LEMMA 7.2.

$$P_{S,T}\big(\theta'(\omega, S)\big) = \theta'(\omega, T) \cdot \prod_{l \mid S/T} \big(1 - \omega(l) \cdot \sigma_{l,T}\big).$$

PROOF. One has

$$P_{S,T}\big(\theta'(\omega, S)\big) = \sum_{\sigma \in \Gamma_T} (\mathbf{N}_{S/T} \cdot \sigma\alpha_S \otimes \sigma). \tag{49}$$

Hence by Proposition 5.1

$$P_{S,T}\big(\theta'(\omega, S)\big) = \Big(\prod_{l \mid S/T} (1 - \sigma_{l,T}^{-1})\Big)\theta'(\omega, T), \tag{50}$$

which is equal to $\theta'(\omega, T) \cdot \prod\big(1 - \omega(l)\sigma_{l,T}\big)$ by Lemma 7.1.

8. **The order of vanishing of** $\theta'(\omega, S)$**.** Let us write S as $S = PQ$, where $P = l_1 \cdots l_s$ is a product of split primes in $K/\mathbf{Q}$, and Q is a product of inert primes. When σ runs over Γ_S, write

$$\sigma = \sigma_1 \cdots \sigma_s \tau, \tag{51}$$

for its unique decomposition as a product with $\sigma_i \in \Gamma_{l_i}$, and $\tau \in \Gamma_Q$.

LEMMA 8.1.

$$\theta'(\omega, S) = \sum_{\sigma \in \Gamma_S} \sigma \alpha_S (\sigma_1 - 1) \cdots (\sigma_s - 1)\tau - \sum_{T|P, T \neq P} \Big(\mu(P/T) \cdot \theta'(\omega, TQ) \cdot \prod_{l|P/T} (1 - \sigma_{l,TQ}) \Big).$$

PROOF. By direct computation,

$$\sum_{\sigma \in \Gamma_S} \sigma \alpha_S (\sigma_1 - 1) \cdots (\sigma_s - 1)\tau = \theta'(\omega, S) + \sum_{T|, T \neq P} \mu(P/T) P_{S,TQ}\big(\theta'(\omega, S)\big). \tag{52}$$

The formula now follows from Lemma 7.2.

We are now ready to prove Theorem 4.2.

THEOREM 4.2 (ORDER OF VANISHING). *The element* $\theta'(\omega, S)$ *belongs to* $K_S^* \otimes I^s = K_S^* \otimes I^{r-1}$.

PROOF. By induction on s, using Lemma 8.1 for the induction step.

9. **The leading coefficient.** We now turn to the study of the element $\tilde{\theta}'(\omega, S)$ defined by projecting $\theta'(\omega, S)$ to the value group $K_S^* \otimes (I_2^{r-1}/I_2^r)$.

LEMMA 9.1. *The leading coefficient* $\tilde{\theta}'(\omega, S)_2$ *belongs to the subgroup of elements in* $\big(K_S^* \otimes (I_2^{r-1}/I_2^r)\big)^{\Gamma_S}$ *fixed by the left (Galois) action of* Γ_S.

PROOF. Given σ in Γ_S, by Lemma 7.1 we have

$$(\sigma - 1)\tilde{\theta}'(\omega, S)_2 = \tilde{\theta}'(\omega, S)_2(\sigma^{-1} - 1), \tag{53}$$

and Lemma 9.1 follows.

LEMMA 9.2. *Let* Γ *be a finite abelian group of odd order, and let* Γ_S *act on the module* $K_S^* \otimes \Gamma$ *by the Galois action. Then the natural map*

$$K^* \otimes \Gamma \longrightarrow (K_S^* \otimes \Gamma)^{\Gamma_S}$$

is an isomorphism.

PROOF. By decomposing Γ as a direct product of cyclic groups, one reduces the proof of Lemma 9.2 to the case where Γ is cyclic of odd order n. If K_S contains no n-th roots of unity, then we are in the situation of Lemma 6.3. In general, one uses the fact that the restriction map

$$H^1(K, \mu_n) \longrightarrow H^1(K_S, \mu_n)^{\Gamma_S} \tag{54}$$

is an isomorphism.

LEMMA 9.3. $n(S)(\gamma_{l_1} - 1) \cdots (\gamma_{l_s} - 1) = 0 \pmod{I_2^r}$.

PROOF. We can write $(\gamma_{l_1} - 1)\cdots(\gamma_{l_s} - 1)$ as a sum of terms of the form $(\gamma_{l_1}^{(p)} - 1)\cdots(\gamma_{l_s}^{(p)} - 1) \pmod{I_2^r}$, where the $\gamma_{l_i}^{(p)}$ are of order a power of p (p an odd prime) and at least one of the $\gamma_{l_j}^{(p)}$ is of order exactly $q = p^{\mathrm{ord}_p(n(S))}$. Hence it suffices to show the theorem when $n(S) = q$ is a power of a prime. In that case, one has

$$0 = \gamma_{l_j}^q - 1 = \sum_{i=1}^{q} \binom{q}{i} (\gamma_{l_j} - 1)^i,$$

so that $q(\gamma_{l_j} - 1) \in I_2^2$. The result follows.

The following proposition gives an inductive formula for the leading coefficient $\tilde{\theta}'(\omega, S)_2$.

PROPOSITION 9.4.

$$\begin{aligned}\tilde{\theta}'(\omega, S)_2 = {}& 2^{\#(l|Q)}\kappa(P) \otimes (\gamma_{l_1} - 1)\cdots(\gamma_{l_s} - 1) \\ & - \sum_{T|P, T\neq P} \mu(P/T) \cdot \tilde{\theta}'(\omega, T) \cdot \prod(1 - \sigma_{l,T}).\end{aligned}$$

PROOF. This follows from Lemma 8.1 together with the fact that

$$\sum_{\sigma\in\Gamma_S} \sigma\alpha_S \otimes (\sigma_1 - 1)\cdots(\sigma_s - 1)_T = 2^{\#(l|Q)}\beta(P) \otimes (\gamma_{l_1} - 1)\cdots(\gamma_{l_s} - 1) \tag{55}$$

in $K_S^* \otimes (I^{r-1}/I^r)$. Because $(\gamma_{l_1} - 1)\cdots(\gamma_{l_s} - 1)$ is killed by $n(P)$ in I_2^{r-1}/I_2^r (Lemma 9.3), one can replace $\beta(P)$ by $\kappa(P)$ in the formula.

In the remainder of this section we will prove Theorem 4.5 which we first recall:

THEOREM 4.5. *1. Conjecture 4.3 is true when* $r = 1$. *2.* $\tilde{\theta}'(\omega, S)_2$ *belongs to* $K^* \otimes I_2^{r-1}/I_2^r$.

3. If $\gcd\big(h_S(K), n(T)\big) = 1$ *for all* $T|S$, *then* $\tilde{\theta}'(\omega, S)_2$ *belongs to* $O_S^* \otimes (I_2^{r-1}/I_2^r)$.

4. $h_S(K)$ *divides* $\tilde{\theta}'(\omega, S)_2$.

5. Suppose that $\Gamma_S = \Gamma_l$ *is cyclic, and that* l *is split in* $K/\mathbf{Q}$ *so that* $r = 2$. *Let* λ *be a prime of* K *above* l, *and let* $k_\lambda \simeq \mathbf{F}_l$ *denote the residue field at* λ. *If the fundamental unit of* $K/\mathbf{Q}$ *is a generator for* k_λ^*, *and* $\gcd\big(h(K), n(l)\big) = 1$, *then*

$$\tilde{\theta}'(\omega, l)_2 = \pm 2h_l R_l \pmod{I_2^2}.$$

PROOF. 1. When $r = 1$, we have $\tilde{\theta}'(\omega, S) = P_{S,1}\big(\theta'(\omega, S)\big)$, where $P_{S,1}\colon \mathbf{Z}[\Gamma_S] \longrightarrow \mathbf{Z}$ is the augmentation map. By lemma 7.2,

$$P_{S,1}\big(\theta'(\omega, S)\big) = \alpha(1)\prod_{l|S}\big(1 - \omega(l)\big) = 2^{\#(l|S)}\alpha(1), \tag{56}$$

since all the l dividing S are inert in $K/\mathbf{Q}$. We know from Dirichlet's analytic class number formula that $\alpha(1) = 2h_1R_1$, and hence the result follows.

2. Combine Lemmas 9.1 and 9.2.

3. By Proposition 6.4, we have $v_\lambda\big(\kappa(T)\big) = 0\big(\bmod n(T)\big)$ for all places λ which do not lie above S. Let $(K^*/K^{*n(T)})(S)$ denote the subgroup of elements in $K^*/K^{*n(T)}$ satisfying this property. There is a natural exact sequence

$$0 \longrightarrow O_S^*/O_S^{*n(T)} \longrightarrow (K^*/K^{*n(T)})(S) \longrightarrow C_S(K)\otimes \mathbf{Z}/n(T)\mathbf{Z}. \tag{57}$$

The assumption that $\big(h_S(K), n(T)\big) = 1$ for all $T|S$ implies that the natural map from $O_S^*/O_S^{*n(T)}$ to $(K^*/K^{*n(T)})(S)$ is an isomorphism, so that the $\kappa(T)$ are S-units modulo $n(T)$-th powers. The result follows from Proposition 9.4.

4. This is a direct consequence of Theorem 6.5 combined with Proposition 9.4.

5. The fact that $\gcd\big(h_l(K), n(l)\big) = 1$ implies, by the previous fact, that $\kappa(l)$ is an l-unit of K modulo $n(l)$-th powers, and hence $\tilde\theta'(\omega, l)$ belongs to $O_l^*\otimes(I_2/I_2^2)$. We want to prove the equality of two objects in $O_l^*\otimes(I/I^2)$. For this, we use two maps:

$$\phi_1\colon O_l^*\otimes(I_2/I_2^2)\longrightarrow I_2/I_2^2,\quad \phi_2\colon O_l^*\otimes(I_2/I_2^2)\longrightarrow I_2^2/I_2^3. \tag{58}$$

The first is induced from the map $v_\lambda\colon O_l^*\longrightarrow \mathbf{Z}$, and the second from the map $\mathrm{rec}_\lambda\colon O_l^*\longrightarrow \Gamma_l\longrightarrow I_2/I_2^2$ given by the reciprocity law of local class field theory. Because $\gcd\big(h(K), n(l)\big) = 1$, the kernel of the map ϕ_1 is just $O_K^*\otimes(I_2/I_2^2)$. The assumption that the fundamental unit for K is a generator of k_λ^* means that ϕ_2 is injective on $O_K^*\otimes(I_2/I_2^2)$. Hence, if two elements in $O_l^*\otimes(I_2/I_2^2)$ have the same image by ϕ_1 and ϕ_2, then they are equal.

Recall that $u_l\in k_\lambda^*$ denotes the element which corresponds to the chosen generator γ_l of Γ_l by the reciprocity law of local class field theory. By Proposition 9.4, we have

$$\tilde\theta'(\omega, l)_2 = \kappa(l)\otimes(\gamma_l - 1). \tag{59}$$

Hence, by Proposition 6.4,

$$\phi_1\big(\tilde\theta'(\omega, l)_2\big) = v_\lambda\big(\kappa(l)\big)\otimes(\gamma_l-1) = \log_{u_l}\big(\kappa(1)\big)(\gamma_l - 1). \tag{60}$$

Let u be a fundamental unit for K. By Dirichlet's class number formula, we can write

$$\kappa(1) = u^{\pm 2h}, \tag{61}$$

so that $\log_{u_l}\big(\kappa(1)\big) = \pm 2h\log_{u_l}(u)$. It follows that

$$\phi_1\big(\tilde\theta'(\omega, l)_2\big) = \pm 2h\log_{u_l}(u)(\gamma_l - 1) = \pm 2h\big(\mathrm{rec}(u) - 1\big). \tag{62}$$

Since $\kappa(l) = \beta(l)x^{n(l)}$, where x belongs to K_l^*, and since

$$\mathrm{norm}_{K_l/K}\big(\beta(l)\big) = 1$$

by Proposition 5.1, we have by taking norms:

$$\kappa(l)^{l-1} = \mathrm{norm}_{K_l/K}\, x^{n(l)}. \tag{63}$$

Hence $\kappa(l)^{(l-1)/n(l)} = \pm\,\mathrm{norm}_{K_l/K}\, x$, so that $\kappa(l)^{2^a}$ is a norm for some $a \geq 0$. Since norms lie in the kernel of the local reciprocity map, we find that

$$\phi_2\Big(\tilde{\theta}'(\omega, l)_2\Big) = 0. \tag{64}$$

We choose a **Z**-basis for O_l^*, given by a fundamental unit u and an l-unit $u(l)$. This can be done in such a way that

$$\nu_\lambda\big(u(l)\big) = h/h_l, \tag{65}$$

since this number is the order of the class of λ in the ideal class group of K. The regulator R_l can be written explicitly as

$$R_l = \pm\Big(u \otimes \Big(\mathrm{rec}\big(u(l)\big) - 1\Big) - u(l) \otimes \Big(\mathrm{rec}(u) - 1\Big)\Big). \tag{66}$$

Hence,

$$\phi_1(2h_lR_l) = \pm 2h_l\nu_\lambda\big(u(l)\big) \otimes \big(\mathrm{rec}(u) - 1\big) = \pm 2h\big(\mathrm{rec}(u) - 1\big). \tag{67}$$

It is immediate from the definition of R_l that

$$\phi_2(4h_lR_l) = 0. \tag{68}$$

Combining equations (62), (64), (67), and (68) we find that

$$\tilde{\theta}'(\omega, l)_2 = \pm 2h_lR_l \pmod{l_2^2},$$

as claimed.

References

[DR] P. Deligne and K. Ribet, *Values of abelian L-functions at negative integers over totally real fields*, Invent. Math. **59**(1980), 227–286.

[Gr] B. H. Gross, *On the values of abelian L-functions at s = 0*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. (1) **35**(1988), 177–197.

[H1] Alfred W. Hales, *Augmentation terminals of finite abelian groups*. In: SLN **1006**, 1983, 720–733.

[H2] ———, *Stable augmentation quotients of abelian groups*, Pacific J. Math. (2) **118**(1985), 401–410.

[Iw] K. Iwasawa, *On $\mathbf{Z}_l$-extensions of algebraic number fields*, Ann. of Math. (2) **98**(1973).

[Ko] V. A. Kolyvagin, *Euler Systems*, Birkhäuser volume in honor of Grothendieck, to appear.

[La] S. Lang, *Cyclotomic fields I and II, combined second edition*, Graduate Texts in Math. **121**, Springer-Verlag, 1990.

[MT] B. Mazur and J. Tate, *Refined conjectures of the "Birch and Swinnerton-Dyer type"*, Duke Math. J. (2) **54**(1987), p. 711.

[Pa] I. B. S. Passi, *Group rings and their augmentation ideals*, SLN **715**, Berlin, New York, 1979.

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

[Sch] R. Schoof, preprint.

[Th] F. Thaine, *On the ideal class groups of real abelian number fields*, Ann. of Math. **128**(1988), 1–18.

[Wa] L. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. **83**, Springer-Verlag, New York, 1982.

Department of Mathematics
Princeton University
Princeton, New Jersey 08540
U.S.A.