

## 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  $\| \cdot \|_w$  is normalized so that it is equal to  $\mathbf{N}w^{-1}$  on uniformizing elements.

Given a finite abelian extension  $M/K$ , we let

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

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

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

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.

© Canadian Mathematical Society, 1995.

We write  $\text{Div}(K)$  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  $\text{Div}(K)/P(K)$ . Given a set  $S$  of places of  $K$ , let  $\langle S \rangle$  be the  $\mathbf{Z}$ -span of the elements of  $S$  in  $\text{Div}(K)$ , and let

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

**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

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

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  $(O_S^*)_T$  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  $[(O_S^*)_T]_{\text{torsion}}$  which is cyclic of order  $w_{S,T}$ . (Typically we will choose  $T$  so that  $w_{S,T} = 1$ .)

3. The Picard group  $\text{Pic}(O_S)_T$  of invertible  $O_S$ -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  $X = \text{Div}^0(S)$  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  $\log_S: O_S^* \rightarrow \mathbf{R} \otimes X$  of the  $S$ -units is defined by

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

Both  $(O_S^*)_T$  and  $X$  are of rank  $r$ . Let

$$(6) \quad \Lambda^r \log_S: \Lambda^r O_S^* \longrightarrow \Lambda^r (\mathbf{R} \otimes X)$$

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

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

where  $\gamma_1, \dots, \gamma_r$  (resp.  $v_1, \dots, v_r$ ) 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  $G = \text{Gal}(L/K)$ . Define a complex-valued function  $\hat{\theta}_G$  on the dual group  $\hat{G} = \text{hom}(G, \mathbf{C}^*)$  by

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

where, for a complex character  $\chi: G \rightarrow \mathbf{C}^*$  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

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

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  $L_{S,T}(K, \chi, 0)$ ,

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

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 than the residue field characteristic minus 1.*

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

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

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

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

one has  $\mathbf{Z}[G]/I = \mathbf{Z}$ . The higher quotients in the filtration are torsion. For instance, there is a natural homomorphism  $G \rightarrow I/I^2$  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

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

which sends  $\sigma_1 \otimes \dots \otimes \sigma_r$  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  $\text{Sym}(G) \rightarrow \bigoplus_r I^r/I^{r+1}$ , the reader may consult [Pa], [H1], [H2].)

The element  $\theta_G$  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  $\theta_G$  belongs to  $I^r$ .*

The leading coefficient  $\tilde{\theta}_G$  in the refined class number formula is defined to be the projection of  $\theta_G$  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

$$(12) \quad \text{rec}_S: \mathcal{O}_S^* \longrightarrow (I/I^2) \otimes_{\mathbf{Z}} X$$

defined by

$$(13) \quad \text{rec}_S(u) = \sum_{v \in S} (\text{rec}_v(u_v) - 1) \otimes v,$$

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

$$\Lambda^r \text{rec}_S: \Lambda^r \mathcal{O}_S^* \longrightarrow \Lambda^r (I/I^2 \otimes X) \longrightarrow (I^r/I^{r+1}) \otimes \Lambda^r X,$$

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

$$(14) \quad \Lambda^r \text{rec}_S(\gamma_1 \wedge \dots \wedge \gamma_r) = R_{S,T} \otimes (v_1 \wedge \dots \wedge v_r),$$

where  $\gamma_1, \dots, \gamma_r$  and  $v_1, \dots, v_r$  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  $\Gamma$ -factors in the functional equation force a zero at  $s = 0$  in the twisted  $L$ -function  $L_{S,T}(K, \chi, s)$  for all  $\chi$ . Hence  $\theta_G = 0$ . But  $\text{rec}_v$  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  $F'/F^{+1}$ . (Also one can show that  $2\tilde{\theta}_G = 0$ .) 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  $\omega$  be an even primitive Dirichlet character of conductor  $N$ . In order to simplify the exposition, we assume that  $\omega$  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  $\chi$  in  $\hat{G}$ , the Dirichlet  $L$ -series

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

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  $\theta'_G$  on  $\hat{G}$  by  $\theta'_G(\chi) = L'_S(0, \omega\chi)$ , and letting  $\theta'_G \in \mathbf{C}[G]$  be its Fourier transform as in Section 3. However, the coefficients of  $\theta'_G$  are not integral, or even algebraic. This leads to the problem of finding an appropriate substitute for  $\theta'_G$ , 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

$$(16) \quad \zeta_{nm}^m = \zeta_n.$$

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

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

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

Let  $\Gamma_S = \text{Gal}(K_S/K)$ , 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

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

Relation between  $\theta'(\omega, S)$  and  $L'_S(0, \omega\chi)$ : Let  $\log: K_S^* \rightarrow \mathbf{C}$  be a principal branch of the logarithm map induced by the complex embedding  $\Psi$  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  $\chi$  to give a linear map

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

We call a character  $\chi$  of  $\Gamma_S$  *primitive* if it does not factor through the natural homomorphism  $\Gamma_S \rightarrow \Gamma_T$  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  $\chi$  is primitive. Then*

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

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  $\infty$  on which the generator of  $\text{Gal}(K/\mathbf{Q})$  acts by  $-1$ . It is a free  $\mathbf{Z}$ -module of rank  $r$ , where

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

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  $\{v_\infty, v_1, \dots, v_{r-1}\}$  forms a basis for  $X^-$ . Let  $(O_S^*)^-$  be the group of  $S$ -units of  $K$  on which the generator of  $\text{Gal}(K/\mathbf{Q})$  acts by  $-1$ . This is also a free  $\mathbf{Z}$ -module of rank  $r$ . Choose a basis  $\omega_1, \dots, \omega_r$  for  $(O_S^*)^-$  in such a way that the regulator  $R_S$  for the logarithmic embedding

$$(20) \quad (O_S^*)^- \longrightarrow X^- \otimes \mathbf{R}$$

relative to the bases  $\{\omega_1, \dots, \omega_r\}$  and  $\{v_\infty, v_1, \dots, v_{r-1}\}$  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

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

and that

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

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  $O_S^* \otimes (I^{r-1}/I^r)$ .

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

$$(23) \quad \text{rec}_S: (O_S^*)^- \longrightarrow I_S \otimes Y^-$$

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

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

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

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

CONJECTURE 4.3.

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

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  $K_S^* \otimes (I_2^{-1}/I_2)$ , 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  $(I_2^{-1}/I_2) = (I^{-1}/I) \otimes \mathbf{Z}[\frac{1}{2}]$  is a finite abelian group of odd order, when  $r > 1$ .

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

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

Let  $n(S)$  be the greatest odd divisor of  $\text{gcd}_{l|S}(l-1)$ . 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  $K^* \otimes I_2^{-1}/I_2$ .

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

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  $\lambda$  be a prime of  $K$  above  $l$ , and let  $k_\lambda \simeq \mathbf{F}_l$  denote the residue field at  $\lambda$ . If the fundamental unit of  $K/\mathbf{Q}$  is a generator for  $k_\lambda^*$ , and  $\text{gcd}(h(K), n(l)) = 1$ , then

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

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  $S$  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

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

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

$$(27) \quad \Gamma_S = \Gamma_{l_1} \times \cdots \times \Gamma_{l_s}$$

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

$$(28) \quad \mathbf{N}_T = \sum_{\sigma \in \Gamma_T} \sigma.$$

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  $\sigma_{l,T} \in \text{Gal}(K_T/\mathbf{Q})$  be the automorphism sending the roots of unity to their  $l$ -th powers.

PROPOSITION 5.1.

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

PROOF. We can write

$$(29) \quad \zeta_{Tl} = \zeta_T^a \zeta_l^b,$$

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  $\lambda$  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  $\gamma_l$  for  $\Gamma_l$  and let

$$(30) \quad D_l = \sum_{i=1}^{l-2} i\gamma_l^i, \quad D_T = \prod_{l|T} D_l,$$

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

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



PROOF. A direct computation.

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

$$(31) \quad \beta(T) = D_T \alpha(T) \in K_T^*$$

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  $\Gamma_T$ , 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:

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

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

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

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

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

is exact. Taking  $\Gamma_T$ -invariants gives rise to the cohomology exact sequence

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

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  $\lambda$  of  $K$  above it. Write

$$(34) \quad v_\lambda: K^* \longrightarrow \mathbf{Z}$$

for the valuation map at  $\lambda$ , 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  $\gamma_l$  by the isomorphism  $\Gamma_l \rightarrow (\mathbf{Z}/l\mathbf{Z})^*$ . Given  $\kappa$  in  $K^*$ , let  $\text{red}_\lambda(\kappa) \in k_\lambda^*$  be the reduction of  $\kappa$  mod  $\lambda$ , in the residue field  $k_\lambda = \mathbf{Z}/l\mathbf{Z}$ . Finally, let

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

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  $\tilde{v}_\lambda(\kappa(T)) = 0$ .  
 2. If  $l$  is split in  $K_T/\mathbf{Q}$ , then

$$\tilde{v}_\lambda(\kappa(Tl)) = -\log_{u_l}(\text{red}_\lambda(\kappa(T))) \pmod{n(Tl)}.$$

PROOF. 1. If  $l$  does not divide  $T$ , then  $\lambda$  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  $\tilde{v}_\lambda(\beta(T)) = 0$ , since  $\beta(T)$  is a unit in  $K_T^*$ .

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

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

Writing

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

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

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

By definition of  $u_l$ , one has

$$(39) \quad v_{\lambda''}(\rho) = \log_{u_l}(\text{red}_{\lambda''}((\gamma_l - 1)\rho)) \pmod{l-1}.$$

But

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

Hence by Proposition 5.2,

$$(40) \quad \text{red}_{\lambda''}((\gamma_l - 1)\rho) = \text{red}_{\lambda'}\left(\frac{l-1}{n(Tl)} D_T\alpha(T)\right),$$

and hence

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

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

$$(42) \quad \tilde{v}_\lambda(\kappa(Tl)) \equiv -\log_{u_l}(\text{red}_\lambda \kappa(T)) \pmod{n(Tl)}$$

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  $\text{ord}_p(m)$  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  $\text{ord}_p(m) = \infty$ .) 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 divisibility 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  $\text{ord}_p(\kappa(S)) = M_0 < \infty$ , and let  $M = M_0 + 1$ . We must show that  $p^M$  does not divide  $\text{gcd}(n(S), h_S(K))$ . 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  $S$  not dividing  $S$ , such that

1.  $l$  splits in  $K/\mathbf{Q}$ ; let  $\lambda$  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.  $\text{ord}_p(\text{red}_\lambda(\kappa(S))) = M_0$ .
4. The image of  $\lambda$  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  $\text{ord}_p(\lambda) = 0$ ).

Let  $F = K(\mu_{p^M}, \kappa(S)^{1/p^M})$ . Conditions 2 and 3 are equivalent to the condition that  $\text{Frob}_\lambda$  in  $\text{Gal}(F/K)$  belongs to the subgroup  $\text{Gal}(F/K(\mu_{p^M}))$  and is non-trivial. Condition 4 is equivalent to a condition on  $\text{Frob}_\lambda$  in  $\text{Gal}(H_S/K)$  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  $m = \text{ord}_p(\kappa(Sl))$ . By combining Proposition 6.4 with condition 3 satisfied by  $l$ , one has

$$(43) \quad \text{ord}_p(\tilde{v}_\lambda(\kappa(Sl))) = M_0,$$

and hence *a fortiori*  $m \leq M_0$ . Moreover, since  $p^M$  divides  $l - 1$ , it also divides  $n(Sl)$ . Let  $\rho$  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

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

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

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

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

$$(46) \quad \#C_S(K) \otimes \mathbf{Z}_p \leq p^m.$$

Combining the inequalities (45) and (46) gives

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

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

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

Given

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

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

The group  $\text{Gal}(K_S/\mathbf{Q})$  acts on the left of  $K_S^* \otimes \mathbf{Z}[\Gamma_S]$  by the Galois action, and  $\Gamma_S$  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  $P_{S,T}: K_S^* \otimes \mathbf{Z}[\Gamma_S] \rightarrow K_S^* \otimes \mathbf{Z}[\Gamma_S]$  be the map induced by the projection  $\Gamma_S \rightarrow \Gamma_T \subset \Gamma_S$ .

LEMMA 7.2.

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

PROOF. One has

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

Hence by Proposition 5.1

$$(50) \quad P_{S,T}(\theta'(\omega, S)) = \left( \prod_{l|S/T} (1 - \sigma_{l,T}^{-1}) \right) \theta'(\omega, T),$$

which is equal to  $\theta'(\omega, T) \cdot \prod (1 - \omega(l) \sigma_{l,T})$  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  $\sigma$  runs over  $\Gamma_S$ , write

$$(51) \quad \sigma = \sigma_1 \cdots \sigma_s \tau,$$

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

LEMMA 8.1.

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

PROOF. By direct computation,

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

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  $K_S^* \otimes F = K_S^* \otimes F^{-1}$ .*

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  $K_S^* \otimes (I_2^{-1}/I_2)$ .

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

PROOF. Given  $\sigma$  in  $\Gamma_S$ , by Lemma 7.1 we have

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

and Lemma 9.1 follows.

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

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

*is an isomorphism.*

PROOF. By decomposing  $\Gamma$  as a direct product of cyclic groups, one reduces the proof of Lemma 9.2 to the case where  $\Gamma$  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

$$(54) \quad H^1(K, \mu_n) \rightarrow H^1(K_S, \mu_n)^{\Gamma_S}$$

is an isomorphism.

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

PROOF. We can write  $(\gamma_{l_1} - 1) \cdots (\gamma_{l_s} - 1)$  as a sum of terms of the form  $(\gamma_{l_1}^{(p)} - 1) \cdots (\gamma_{l_s}^{(p)} - 1) \pmod{I_2^2}$ , 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  $q = p^{\text{ord}_p(n(S))}$ . 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.

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

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

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

in  $K_S^* \otimes (I_2^{-1}/I_2)$ . Because  $(\gamma_{l_1} - 1) \cdots (\gamma_{l_s} - 1)$  is killed by  $n(P)$  in  $I_2^{-1}/I_2$  (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  $K^* \otimes I_2^{-1}/I_2$ .

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

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  $\lambda$  be a prime of  $K$  above  $l$ , and let  $k_\lambda \simeq \mathbf{F}_l$  denote the residue field at  $\lambda$ . If the fundamental unit of  $K/\mathbf{Q}$  is a generator for  $k_\lambda^*$ , and  $\text{gcd}(h(K), n(l)) = 1$ , then

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

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

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

since all the  $l$  dividing  $S$  are inert in  $K/\mathbf{Q}$ . We know from Dirichlet's analytic class number formula that  $\alpha(1) = 2h_1 R_1$ , and hence the result follows.

2. Combine Lemmas 9.1 and 9.2.

3. By Proposition 6.4, we have  $v_\lambda(\kappa(T)) = 0 \pmod{n(T)}$  for all places  $\lambda$  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

$$(57) \quad 0 \longrightarrow \mathcal{O}_S^*/\mathcal{O}_S^{*n(T)} \longrightarrow (K^*/K^{*n(T)})(S) \longrightarrow C_S(K) \otimes \mathbf{Z}/n(T)\mathbf{Z}.$$

The assumption that  $(h_S(K), n(T)) = 1$  for all  $T|S$  implies that the natural map from  $\mathcal{O}_S^*/\mathcal{O}_S^{*n(T)}$  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  $\gcd(h_l(K), n(l)) = 1$  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  $\mathcal{O}_l^* \otimes (I_2/I_2^2)$ . We want to prove the equality of two objects in  $\mathcal{O}_l^* \otimes (I/I^2)$ . For this, we use two maps:

$$(58) \quad \phi_1: \mathcal{O}_l^* \otimes (I_2/I_2^2) \longrightarrow I_2/I_2^2, \quad \phi_2: \mathcal{O}_l^* \otimes (I_2/I_2^2) \longrightarrow I_2^2/I_2^3.$$

The first is induced from the map  $v_\lambda: \mathcal{O}_l^* \rightarrow \mathbf{Z}$ , and the second from the map  $\text{rec}_\lambda: \mathcal{O}_l^* \rightarrow \Gamma_l \rightarrow I_2/I_2^2$  given by the reciprocity law of local class field theory. Because  $\gcd(h(K), n(l)) = 1$ , the kernel of the map  $\phi_1$  is just  $\mathcal{O}_K^* \otimes (I_2/I_2^2)$ . The assumption that the fundamental unit for  $K$  is a generator of  $k_\lambda^*$  means that  $\phi_2$  is injective on  $\mathcal{O}_K^* \otimes (I_2/I_2^2)$ . Hence, if two elements in  $\mathcal{O}_l^* \otimes (I_2/I_2^2)$  have the same image by  $\phi_1$  and  $\phi_2$ , then they are equal.

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

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

Hence, by Proposition 6.4,

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

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

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

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

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

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

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

by Proposition 5.1, we have by taking norms:

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

Hence  $\kappa(l)^{(l-1)/n(l)} = \pm \text{norm}_{K_l/K} x$ , 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

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

We choose a  $\mathbf{Z}$ -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

$$(65) \quad v_\lambda(u(l)) = h/h_l,$$

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

$$(66) \quad R_l = \pm \left( u \otimes (\text{rec}(u(l)) - 1) - u(l) \otimes (\text{rec}(u) - 1) \right).$$

Hence,

$$(67) \quad \phi_1(2h_l R_l) = \pm 2h_l v_\lambda(u(l)) \otimes (\text{rec}(u) - 1) = \pm 2h(\text{rec}(u) - 1).$$

It is immediate from the definition of  $R_l$  that

$$(68) \quad \phi_2(4h_l R_l) = 0.$$

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

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

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. Kolyagin, *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.*