ANNALES

DE

L'INSTITUT FOURIER

Cornelius GREITHER & Radan KUČERA

Annihilators of minus class groups of imaginary abelian fields

Tome 57, nº 5 (2007), p. 1623-1653.

<http://aif.cedram.org/item?id=AIF_2007__57_5_1623_0>

Ann. Inst. Fourier, Grenoble
57, 5 (2007) 1623-1653

ANNIHILATORS OF MINUS CLASS GROUPS OF IMAGINARY ABELIAN FIELDS

by Cornelius GREITHER & Radan KUČERA

Abstract. — For certain imaginary abelian fields we find annihilators of the minus part of the class group outside the Stickelberger ideal. Depending on the exact situation, we use different techniques to do this. Our theoretical results are complemented by numerical calculations concerning borderline cases.

Résumé. — Pour certains corps imaginaires abéliens, on trouve des annulateurs pour la partie moins du groupe des classes en dehors de l'idéal de Stickelberger. En fonction du cadre précis, on emploie des méthodes différentes. Les résultats théoriques sont accompagnés de calculs numériques, ayant trait à quelques cas extrêmes.

Introduction

This article deals with the question whether Stickelberger's theorem tells us the whole truth about the annihilators of the minus class group Cl_L^- of an absolutely abelian field L, and our main results say that in several more or less frequently occurring situations there are extra annihilators, that is, annihilators outside the Stickelberger ideal in the sense of Sinnott. To simplify the setup, we fix an odd prime ℓ and only look at ℓ-primary parts of class groups (a quite harmless restriction), and we also assume that L has a particular shape: It is the compositum of an imaginary quadratic field F and a (real) elementary ℓ-abelian extension $K/\mathbb{Q}$. This restriction is not so harmless, but it should be pointed out that the case "$[L\colon \mathbb{Q}]$ coprime to ℓ" is probably less interesting: This is the so-called semisimple case, and we do not expect in that case to find extra annihilators in any systematic way.

Keywords: Imaginary abelian number fields, minus part of the ideal class group, annihilators, Stickelberger ideal, Fitting ideals.
Math. classification: 11R20, 11R29.

Before we start, we would like to point out that there are large classes of cases even in our restricted setting where one should not expect extra annihilators in general. We are interested in results which hold in large families, and not in a search à la Cohen-Lenstra, where one conjectures that any Galois module one could possibly expect does occur for a positive density of cases. Thus for example we may not expect general results on extra annihilators if $L = F$ (the very simplest case), since $A_F^- := \mathrm{Cl}_F\{\ell\}^-$ is often cyclic as a Galois module (the Cohen-Lenstra heuristics even predict the precise frequency of this event), and one knows then that the annihilator is essentially the Stickelberger ideal. (Note that $\mathrm{Cl}_F = \mathrm{Cl}_F^-$.) From this one obtains many similar situations (*cf.* [4], Theorem 2.1): If no rational prime that ramifies in $K/\mathbb{Q}$ is split in F and $\zeta_\ell \notin F$, then $A_L^- := \mathrm{Cl}_L\{\ell\}^-$ is cohomologically trivial over $\mathrm{Gal}(L/F)$. This implies Galois codescent, that is: The $\mathrm{Gal}(L/F)$-coinvariants of A_L^- can be identified with A_F^-. Therefore, by Nakayama's Lemma, A_L^- will be a cyclic Galois module whenever A_F^- is cyclic. In this frequently occurring case the annihilator of A_L^- agrees with the (initial) Fitting ideal of A_L^-, and by a recent result of Kurihara this agrees with the Stickelberger ideal in the minus part.

In all cases considered in this paper there will be at least one prime that ramifies in $K/\mathbb{Q}$ and splits in F. Recall $L = FK$.

We consider three different situations:

(a) In §2-3, $K/\mathbb{Q}$ is its own genus field (§1 contains algebraic preparations).

(b) In §4, we assume $K/\mathbb{Q}$ to ramify in many primes and that K is not too far below its genus field.

(c) In §6 we consider the case that $K/\mathbb{Q}$ is cyclic (§5 is again devoted to preparations).

The assumptions we have to impose and the degree of explicitness we achieve vary strongly, depending on the situations just sketched. In more detail:

(a) We work with fairly indirect algebraic methods in §2. We do obtain, under a suitable hypothesis, explicit annihilators outside the Stickelberger ideal, but this arises from algebraic considerations and not from the discovery of new principal ideals. Our hypothesis can be loosely expressed by saying that A_L^- needs more generators as a Galois module than usual; we provide a simple arithmetic criterion just when this happens, see Theorem 2.2. If s is the number of ramified primes in $K/\mathbb{Q}$ which split in F, and we put $\Gamma = \mathrm{Gal}(L/F) = \mathrm{Gal}(K/\mathbb{Q})$, and $m(M) = m_{\mathbb{Z}[\Gamma]}(M)$ denotes the minimal number of generators of a $\mathbb{Z}[\Gamma]$-module M, then $m(A_L^-) \geqslant s$ is always true. If $m(A_L^-) \geqslant s+2$, then we can construct new annihilators. In the borderline cases $m(A_L^-) = s$ or $m(A_L^-) = s+1$ we did computer calculations which show that no general result is possible: In some examples one finds some extra annihilators, in some others (and they seem to be more frequent) there are none (see §3). We also ran one case with $m(A_L^-) = s+2$ on the machine, as a numerical test and as an illustration.

(b) In §4 we prove some results on non-genus fields, which are derived algebraically from the genus field case, making suitable assumptions. Here we assume that all primes ramifying in K are split in F, and we can only prove *the existence* of extra annihilators, because the methods of §4 are too indirect to write them down explicitly.

(c) In contrast with (a) and (b), we show in §6 that for cyclic L one may extract certain roots from Gauss sums, which gives new annihilators in a rather satisfactory way whenever $s \geqslant 2$. This is based on the distribution relation for Gauss sums, which is recalled in §5, and shown by methods used before by Darmon, Hayward, and the present authors in slightly different contexts.

A concluding comment: For finite $\mathbb{Z}$-modules M, it is quite easy to see that the annihilator of M is larger than its $\mathbb{Z}$-Fitting ideal if (and only if) M is not cyclic. One might expect a similar behaviour for Galois modules, and therefore our results which give extra annihilators in cases where many generators are needed are perhaps not totally unexpected. On the other hand, our calculations in §3.1-3.2 together with Kurihara's theorem show that A_L^- can be non-cyclic and still its annihilator can agree with the Fitting ideal, and this seems to be an interesting observation.

1. Preliminary lemmas

In this section, all rings are commutative, all modules finitely generated, and the minimal number of generators of the R-module M is denoted $m_R(M)$ or $m(M)$ if R is clear from the context. The i-th Fitting ideal of M over R is denoted $\mathrm{Fitt}_R^i(M)$ (the i is never an exponent here). If $i=0$, it may be omitted from the notation, and $\mathrm{Fitt}_R^0(M)$ is known as the initial Fitting ideal (sometimes, abusively, called first Fitting ideal).

Lemma 1.1. — *Let R be a discrete valuation ring (DVR) whose maximal ideal is generated by π, and M a torsion R-module with $m_R(M) = n$. Let f be a generator of* $\mathrm{Fitt}_R^0(M)$*. Then $f\pi^{1-n}$ is in R and*

$$\frac{f}{\pi^{n-1}} \mathrm{Fitt}_R^1(M) \subset \mathrm{Fitt}_R^0(M).$$

Proof. — We may calculate the Fitting ideals from any presentation $R^n \to R^n \to M \to 0$; in particular, since R is a DVR, we may assume that the map $R^n \to R^n$ is afforded by a diagonal matrix $D = \operatorname{diag}(\pi^{k_1}, \dots, \pi^{k_n})$. All k_i must be positive since M cannot be generated by fewer than n elements. Then $\mathrm{Fitt}^0_R(M)$ is generated by π^k where $k = k_1 + \dots + k_n$, and $\mathrm{Fitt}^1_R(M)$ is generated by $\pi^{k-k'}$ where k' is the maximum of the k_i. So f is exactly divisible by π^k, and since $k \geqslant n$ we of course have $f\pi^{1-n} \in R$. Since $k - k'$ is the sum of all k_i with just one of them omitted, we also have $k - k' \geqslant n-1$, so $\pi^{1-n}\,\mathrm{Fitt}^1_R(M) \subset R$. The inclusion stated above is equivalent to this. □

Lemma 1.2. — *If R is any commutative ring, M has a projective resolution of length one and $\mathrm{Fitt}_R(M)$ is generated by a nonzerodivisor f, then for every $b \in R$ we have the implication:*

$$b\,\mathrm{Fitt}^1_R(M) \subset \mathrm{Fitt}^0_R(M) \Rightarrow bM = 0.$$

Proof. — It is routine to reduce the lemma to the case where R is local. We write $M = R^n/U$, where U is R-free of rank n because f is a nonzerodivisor. Let $z_1, \dots, z_n \in R^n$ be fixed generators of U and let Z be the square matrix whose rows are the z_i. Then $f = \det(Z)$ generates $\mathrm{Fitt}^0_R(M)$. Let $e_i \in R^n$ be the i-th standard basis vector. Write be_i as a linear combination of the z_j with coefficients in $R[1/f]$. The coefficients are, by Cramer's rule, all of the form: b times a maximal minor of Z divided by f. By our hypothesis, b times every maximal minor is in $\mathrm{Fitt}^0_R(M)$, that is, divisible by f. Hence the coefficients are in R, be_i is in the R-span of the z_j, and $bR^n \subset U$. This says that $bM = 0$. □

From now on we assume that R is local and its full ring of quotients is a finite product of fields (main example: Group rings of abelian ℓ-groups over a DVR of residue characteristic ℓ). This will not be repeated. We also make the assumption that the integral closure $\widetilde{R}$ of R in its ring of quotients is a finite product of DVRs:

$$\widetilde{R} = \bigoplus_{i=1}^{t} R_i.$$

This holds true for group rings over DVRs.

The conductor $\mathfrak{c} = \mathfrak{c}(\widetilde{R}/R)$ is defined as the set of all $x \in \widetilde{R}$ with $x\widetilde{R} \subset R$. It is an ideal in $\widetilde{R}$, contained in R, and can be described as the largest $\widetilde{R}$-ideal contained in R, or alternatively, as the R-annihilator of $\widetilde{R}/R$. In general it can be hard to calculate the conductor exactly.

Lemma 1.3. — *Let R and $\widetilde{R}$ be as above and $c \in \mathfrak{c}$. Let M be an R-module satisfying the conditions imposed on M in the last lemma, and let $n = m_R(M)$. Then for every $a \in \widetilde{R}$ such that the valuations $v_{R_i}(a) = 1$ for $1 \leqslant i \leqslant t$ we have:*

$$fa^{1-n} \in \widetilde{R}, \text{ and } R \ni cfa^{1-n} \text{ annihilates } M.$$

Proof. — As in the last proof we write $M = R^n/U$ with U again free of rank n. Let f be a generator for $\mathrm{Fitt}_R^0(M)$. Since M needs n generators, all entries of vectors in U must lie in the Jacobson radical of R. We note that $\mathrm{rad}(R) \subset \mathrm{rad}(\widetilde{R})$ since $\widetilde{R}$ is integral over R. We consider the module $\widetilde{M} = \widetilde{R} \otimes_R M$. The well-known base change properties for the Fitting ideal give us that $\mathrm{Fitt}^i_{\widetilde{R}}(\widetilde{M}) = \widetilde{R} \cdot \mathrm{Fitt}^i_R(M)$ for $i = 0, 1$. (This is all we need to know about $\widetilde{M}$; we do not claim that M embeds into $\widetilde{M}$, which is actually false in general). The module $\widetilde{M}$ again requires n generators over $\widetilde{R}$, since $\widetilde{R}U$ is in the radical of $\widetilde{R}^n$. Lemma 1.1 now yields that $fa^{1-n} \in \widetilde{R}$ and

$$fa^{1-n}\,\mathrm{Fitt}^1_{\widetilde{R}}(\widetilde{M}) \subset \mathrm{Fitt}^0_{\widetilde{R}}(\widetilde{M}).$$

Therefore $fa^{1-n}\widetilde{R}\ \mathrm{Fitt}^1_R(M) \subset \widetilde{R}\ \mathrm{Fitt}^0_R(M)$, and this gives

$$fa^{1-n}\ \mathrm{Fitt}^1_R(M) \subset \widetilde{R}\ \mathrm{Fitt}^0_R(M).$$

Upon multiplying with c, we then find

$$cfa^{1-n}\,\mathrm{Fitt}^1_R(M) \subset c\widetilde{R}\ \mathrm{Fitt}^0_R(M) \subset \mathrm{Fitt}^0_R(M).$$

We can now finish the argument by using Lemma 1.2 on $b = cfa^{1-n}$. □

Now we apply this in a rather concrete situation: First we specify R, and later we establish the connection with abelian genus fields.

We fix a positive integer s and an odd prime ℓ. The group Γ will always be abelian of order ℓ^s, generated by $\sigma_1, \ldots, \sigma_s$ where each σ_i has order ℓ. The notation N_σ will mean the norm element $1 + \sigma + \cdots + \sigma^{\ell-1}$. For ease of writing let $Z = \mathbb{Z}_\ell[\zeta_\ell]$. Let B denote the set of all multiindices $\underline{i} = (1\ i_2\ \ldots\ i_s)$ with $i_k \in \{1, \ldots, \ell{-}1\}$ for $2 \leqslant k \leqslant s$. We intend to examine the ring $R = \mathbb{Z}_\ell[\Gamma]/(\mathrm{N}_{\sigma_1}, \ldots, \mathrm{N}_{\sigma_s})$ more closely. We first remark that the $\mathbb{Z}_\ell$-algebra R can be decomposed as the following tensor product:

$$R = \Big(\mathbb{Z}_\ell[\sigma_1]/(\mathrm{N}_{\sigma_1})\Big) \otimes_{\mathbb{Z}_\ell} \cdots \otimes_{\mathbb{Z}_\ell} \Big(\mathbb{Z}_\ell[\sigma_s]/(\mathrm{N}_{\sigma_s})\Big).$$

Note that each tensor factor is a copy of the ring Z, and hence a DVR, but R itself is far from being a DVR if $s > 1$. Indeed, we have $\widetilde{R} = Z^B$ (cartesian product of copies of Z, indexed with the set B), and the inclusion (!) α from R to $\widetilde{R}$ is given by:

$$\alpha(x) = (\alpha_{\underline{i}}(x))_{\underline{i} \in B},$$

with

$$\alpha_{\underline{i}}(\sigma_k) = \zeta_\ell^{i_k}.$$

Thus, the map α is given by evaluating an element at all characters χ of Γ that map σ_1 to ζ_ℓ and that do not map any σ_k to 1.

We will identify $\mathbb{Z}_\ell[\sigma_1]/(\mathrm{N}_{\sigma_1})$ with Z by identifying (the image of) σ_1 with ζ_ℓ. Now we can describe the indecomposable idempotents of $\widetilde{R}$. For $\underline{i} \in B$ let

$$e_{\underline{i}} = |\Delta|^{-1} \sum_{\sigma\in\Delta} \alpha_{\underline{i}}(\sigma)\sigma^{-1} \in \mathbb{Q}R,$$

where Δ is the subgroup of Γ generated by $\sigma_2, \ldots, \sigma_s$. Then $e_{\underline{i}}$ maps to 1 under $\alpha_{\underline{i}}$ and to 0 under each $\alpha_{\underline{j}}$ with $\underline{i} \neq \underline{j}$, so we may identify it with the $\underline{i}$'th standard indecomposable idempotent of the product Z^B. In particular, the R-module $\widetilde{R}$ is generated by all these idempotents.

Probably it is difficult to calculate the conductor $\mathfrak{c} = \mathfrak{c}(\widetilde{R}/R)$ exactly, but we have a lower bound which will suffice for our applications. Let λ_i denote the image of $\sigma_i - 1$ in R. Since we factored out by N_{σ_i}, we know that $\lambda_i^{\ell-1}$ is associated to ℓ in R, and ℓ is a nonzerodivisor. Hence λ_i is also a nonzerodivisor and ℓ/λ_i is a well-defined element of R for all $i = 1, \ldots, s$.

Proposition 1.4. — *The conductor $\mathfrak{c}$ contains the ideal $\left\langle \ell/\lambda_1, \ldots, \ell/\lambda_s \right\rangle^{s-1}$.*

Proof. — We consider the idempotent $e = e_{(1\,1\,\ldots\,1)}$ and factor it as $e = e_2 \cdots e_s$ with $e_i = \ell^{-1} \sum_{t=0}^{\ell-1} \sigma_1^t \sigma_i^{-t}$. (Recall that we identify $\sigma_1 \in R$ with ζ_ℓ.) In R we have, using $\mathrm{N}_{\sigma_i} = 0$:

$$\begin{aligned} \ell e_i &= 1 + \sigma_1\sigma_i^{-1} + \ldots + \sigma_1^{\ell-2}\sigma_i^{2-\ell} + \sigma_1^{\ell-1}\sigma_i^{1-\ell} \\ &= (1 - \sigma_1^{\ell-1}) + (\sigma_1 - \sigma_1^{\ell-1})\sigma_i^{-1} + \ldots + (\sigma_1^{\ell-2} - \sigma_1^{\ell-1})\sigma_i^{2-\ell}, \end{aligned}$$

which is divisible by λ_1. Thus $(\ell/\lambda_1)e_i \in R$. Hence

$$(\ell/\lambda_1)^{s-1} e = \prod_{k=2}^{s} (\frac{\ell}{\lambda_1} e_k)$$

is likewise in R. On the other hand, $\sigma_i e = \sigma_j e$ for all $1 \leqslant i, j \leqslant s$, and this shows that

$$\left\langle \ell/\lambda_1, \ldots, \ell/\lambda_s \right\rangle^{s-1} e \in R.$$

If we replace each σ_k by its i_k-th power $(1 \leqslant i_k \leqslant \ell - 1)$, then we get the same statement with e replaced by $e_{\underline{i}}$, since the ideal $\left\langle \ell/\lambda_1, \ldots, \ell/\lambda_s \right\rangle$ stays the same (the element $\sigma_k^{i_k} - 1$ is associated to $\lambda_k = \sigma_k - 1$ in R). Since $\widetilde{R}$ is generated by the $e_{\underline{i}}$, we are done now. □

In the next result we prove an annihilation statement whose significance will only become clear in the next section, upon application to a certain minus class group. The statement below is sharper than just the statement $\mathrm{Fitt}_R(M) \subsetneq \mathrm{Ann}_R(M)$, and this extra sharpness will be needed in Section 2. Let $\lambda = \lambda_1 \cdots \lambda_s \in R$.

Corollary 1.5. — *Assume M is an R-module with $t = m_R(M) \geqslant s+2$ and which satisfies the hypotheses of Lemma 1.2, so in particular,* $\mathrm{Fitt}_R(M)$ *is principal and generated by a nonzerodivisor $f \in R$. Then for any positive integers k_i satisfying $\sum_{i=1}^s k_i = t-2$, the element*

$$\delta = \frac{f\ell^{s-1}}{\prod_{i=1}^s \lambda_i^{k_i+1}}$$

is in R, annihilates M, and $\lambda\delta$ is not divisible by f in R.

Proof. — Let β be any monomial in the λ_k of weight $t-1$. Let $\alpha \in R$ be such that in each $R_{\underline{i}}$, α has valuation 1. (For example any λ_k will do as α.) The quotient $\gamma = \beta/\alpha^{t-1}$ is a unit in $\widetilde{R}$. Then for any $c \in \mathfrak{c}$, we have

$$\delta = \frac{cf}{\beta} = \frac{cf}{\alpha^{t-1}}\gamma^{-1} = c\gamma^{-1}\frac{f}{\alpha^{t-1}},$$

and by Lemma 1.3 $\delta \in R$ is an annihilator for M since $c\gamma^{-1}$ is again in $\mathfrak{c}$. We now specify c and β: Let

$$c = \frac{\ell^{s-1}}{\lambda_1 \cdots \lambda_{s-1}}, \quad \beta = \lambda_1^{k_1} \cdots \lambda_{s-1}^{k_{s-1}} \lambda_s^{k_s+1},$$

where k_i are positive integers satisfying $\sum_{i=1}^s k_i = t-2$. Thus the element δ given by

$$\delta = \frac{cf}{\beta} = \frac{f\ell^{s-1}}{\prod_{i=1}^s \lambda_i^{k_i+1}}$$

annihilates M. We claim that $\lambda\delta$ is not divisible by f. Indeed $\lambda\delta = \eta f$ with

$$\eta = \frac{\ell^{s-1}}{\prod_{i=1}^s \lambda_i^{k_i}} \in \mathbb{Q}R,$$

and we must show that η is not in R. Since the exponents of λ_i in the denominator are positive, it suffices to show that λ_s does not divide the product $(\ell/\lambda_1)\cdots(\ell/\lambda_{s-1})$ in R. This is most easily done by passing to $R/\ell R$, which is isomorphic to $\bigotimes_{i=1}^s \mathbb{F}_\ell[\sigma_i]/(\mathrm{N}_{\sigma_i}) \cong \mathbb{F}_\ell[d_1,\ldots,d_s]/(d_1^{\ell-1},\ldots,d_s^{\ell-1})$ with λ_i mapping to d_i. Each element ℓ/λ_i is associated to $\lambda_i^{\ell-2}$ in R, hence $(\ell/\lambda_1)\cdots(\ell/\lambda_{s-1})$ maps to a unit times $d_1^{\ell-2}\cdots d_{s-1}^{\ell-2}$, and this is not divisible by d_s in $R/\ell R$. □

We finish this section by the following classical lemma on class groups. Recall that $A_L^- = \mathrm{Cl}_L\{\ell\}^-$.

Lemma 1.6. — *Let $N_0 \subset N$ be imaginary abelian fields. Then we have:*

(a) *The natural map (induced by the norm) from A_N^- to $A_{N_0}^-$ is surjective.*

(b) *If $\zeta_\ell \notin N$ then the natural map (induced by extension of ideals) $\iota\colon A_{N_0}^- \to A_N^-$ is injective.*

(c) *Let $\zeta_\ell \notin N$, $\alpha \in \mathbb{Z}_\ell[\mathrm{Gal}(N_0/\mathbb{Q})]$, and $\beta = \mathrm{cor}_{N/N_0}\,\alpha \in \mathbb{Z}_\ell[\mathrm{Gal}(N/\mathbb{Q})]$. Then β annihilates A_N^- if and only if α annihilates $A_{N_0}^-$.*

Proof.

(a) By class field theory, the cokernel of the norm map $\mathrm{Cl}_N \to \mathrm{Cl}_{N_0}$ can be identified with $\mathrm{Gal}(H_{N_0} \cap N/N_0)$, where H_{N_0} is the Hilbert class field of N_0. Complex conjugation acts naturally on this Galois group, and the two involved class groups. Moreover the action on $\mathrm{Gal}(H_{N_0} \cap N/N_0)$ is trivial, since N is absolutely abelian. Thus, on taking ℓ-parts and then minus parts, one sees that the cokernel of $A_N^- \to A_{N_0}^-$ vanishes.

(b) Let $\Delta = \mathrm{Gal}(N/N_0)$. The kernel of ι embeds into $\mathrm{H}^1(\Delta, \mathcal{O}_N^*)$. (Proof: $\ker(\iota)$ can be identified with a subgroup of P_N^Δ/P_{N_0}, where P_N denotes the group of principal fractional ideals of N. Since $P_N = N^*/\mathcal{O}_N^*$, one easily sees that P_N^Δ/P_{N_0} embeds into (actually is equal to) $\mathrm{H}^1(\Delta, \mathcal{O}_N^*)$.) On the ℓ-part of that cohomology group, complex conjugation acts trivially since the ℓ-part of the group μ_N of roots of unity in N is trivial. Since complex conjugation acts as inversion on the kernel in question, and the kernel is an ℓ-group, the kernel must be zero.

(c) Suppose $\beta\, A_N^- = 0$. Every $y \in A_{N_0}^-$ can be written in the form $y = \mathrm{N}_{N/N_0}\, x$, $x \in A_N^-$, by (a). We have $0 = \beta\, x = (\mathrm{cor}\ \alpha)x = \iota(\alpha\, y)$, where ι is the map from (b). Since ι is injective, we get $\alpha\, y = 0$. Suppose on the other hand $\alpha\, A_{N_0}^- = 0$. Take $x \in A_N^-$. Then $\beta\, x = \iota(\alpha\, \mathrm{N}_{N/N_0}\, x) = 0$. □

2. The case of K being a genus field

We are interested in imaginary abelian fields of the form $L = FK$ with F quadratic, and K a genus field. Before we come to that, we need a result on descent of so-called minus extensions. Let L always denote an imaginary abelian field over $\mathbb{Q}$, and consider abelian extensions H/L which have the extra property (tacitly assumed throughout this section) of being normal over $\mathbb{Q}$. In particular complex conjugation (denoted τ) acts canonically on $\mathrm{Gal}(H/L)$. We will also always assume that the degree of H over L

is odd. To simplify things we call H/L a "plus extension" (resp. "minus extension"), if τ acts on $\mathrm{Gal}(H/L)$ as identity (resp. as -1). Since H/L has odd degree, one can write H canonically as the disjoint compositum over L of a plus extension and a minus extension.

LEMMA 2.1. — *Let $L_0 \subset L$ be imaginary absolutely abelian fields and assume that $[L\colon L_0]$ is odd. Let H/L be an abelian minus extension of odd degree, which is normal over $\mathbb{Q}$, and assume that the resulting action of $\mathrm{Gal}(L/L_0)$ on $\mathrm{Gal}(H/L)$ is trivial. Then there exists a unique minus extension H'/L_0 with $H = LH'$.*

Proof. — Let us start by pointing out that $L \cap H'$ must equal L_0, since L/L_0 is a plus extension. This also proves uniqueness: H'/L_0 is the minus part of the abelian extension H/L_0. Note that the fact "H is abelian over L_0" is a byproduct of the whole proof, and not evident from the outset.

We proceed by induction over $[L\colon L_0]$, beginning with the case that L/L_0 is cyclic. There we have a short exact sequence of groups

$$1 \to \mathrm{Gal}(H/L) \to \mathrm{Gal}(H/L_0) \to \mathrm{Gal}(L/L_0) \to 1,$$

and by assumption the cyclic group $\mathrm{Gal}(L/L_0)$ acts trivially on $\mathrm{Gal}(H/L)$. As is well-known, this implies that the group in the middle is also abelian. Since τ acts on $\mathrm{Gal}(H/L_0)$, we may write H uniquely as the composite $H = H_0H'$, where H_0/L_0 is a plus extension, H'/L_0 is a minus extension, and $H_0 \cap H' = L_0$. The extension H_0 must contain L since L is contained in H and L/L_0 is a plus extension. On the other hand, H_0 cannot be larger than L because this would produce a nontrivial plus part of the extension H/L. Thus $H_0 = L$ and we have decomposed $H = LH'$ as we wanted. From the uniqueness of H' we also get that H' must be again normal over $\mathbb{Q}$.

Induction step: Here we have three fields $L_0 \subset L_1 \subset L$ and assume both inclusions are proper. The action of $\mathrm{Gal}(L/L_1)$ on $\mathrm{Gal}(H/L)$ is trivial by hypothesis. Hence by induction, we obtain a decomposition $H = LH_1'$ with H_1'/L_1 an abelian minus extension which is normal over $\mathbb{Q}$. From the triviality of the $\mathrm{Gal}(L/L_0)$-action on $\mathrm{Gal}(H/L)$ we deduce the triviality of the $\mathrm{Gal}(L_1/L_0)$-action on $\mathrm{Gal}(H_1'/L_1)$, because the action respects the decomposition $H = LH_1'$, as at the end of the preceding paragraph. Hence we can repeat the argument, and finish the proof by a second application of the induction hypothesis. □

We now come to our arithmetic setup. We fix an odd prime number ℓ and a positive integer s. We consider different primes $p_1, \dots, p_s$ all congruent to 1 modulo ℓ and the cyclic fields K_i of degree ℓ and conductor p_i over $\mathbb{Q}$. Let $K = K_1 \cdots K_s$ be the compositum. Furthermore, we fix an imaginary quadratic field F, with the assumption that $\zeta_\ell \notin F$ and that each p_i splits in F. Let $L = FK$.

The Galois group $\Gamma = \mathrm{Gal}(L/F)$ is elementary abelian of order ℓ^s, and we fix generators $\sigma_1, \ldots, \sigma_s$ such that σ_i generates $\mathrm{Gal}(K_i/\mathbb{Q})$ and is identity on the other K_j. We are interested in the $\mathbb{Z}_\ell[\Gamma]$-annihilator of the module

$$A_L^- = \mathrm{Cl}_L\{\ell\}^-.$$

The first and rather important step is to understand the Γ-coinvariants of A_L^-; a main point is that $(A_L^-)_\Gamma$, which maps canonically to A_F^-, is larger than A_F^- in a systematic way. To make this precise, we require some more notation.

Let $\widetilde{N}/F$ be the maximal abelian ℓ-extension of F which is unramified outside $p_1, \ldots, p_s$ and whose inertia groups at each prime dividing some p_i are of exponent at most ℓ. Let N/F denote the minus part of the extension $\widetilde{N}/F$ (see above); clearly $\widetilde{N}$ is normal over $\mathbb{Q}$. Using the facts that $\mathcal{O}_F^*$ only consists of roots of unity, that $\zeta_\ell \notin F$, and that $\mathcal{O}_{F,\mathfrak{p}}^*/\ell \cong \mathbb{Z}/\ell\mathbb{Z}$ for every prime $\mathfrak{p}$ of F dividing some p_i, we get the following exact sequence from class field theory:

$$0 \to (\mathbb{Z}/\ell\mathbb{Z})^s \to \mathrm{Gal}(N/F) \to A_F^- \to 0. \qquad (*)$$

The exponent s (instead of $2s$) in the left hand term comes from taking minus parts. This sequence can be split or nonsplit. (Numerical examples: If we take $s = 1$, $\ell = 3$, $F = \mathbb{Q}(\sqrt{-23})$, we have A_F^- of order 3 and the sequence is split for $p_1 = 151$ and nonsplit for $p_1 = 73, 127, 139$.) But in any case, $\mathrm{Gal}(N/F)$ requires at least s generators as a $\mathbb{Z}$-module.

Theorem 2.2.

(a) $(A_L^-)_\Gamma$ *is canonically isomorphic to* $\mathrm{Gal}(N/F)$*.*

(b) *The* $\mathbb{Z}_\ell[\Gamma]$*-module* A_L^- *requires at least* s *generators.*

Proof.

(a) Let H/L be the largest abelian minus extension which is unramified, of ℓ-power degree, and such that Γ acts trivially on $\mathrm{Gal}(H/L)$. By class field theory, H exists and $\mathrm{Gal}(H/L)$ is isomorphic to $(A_L^-)_\Gamma$. By Lemma 2.1, we can write $H = LH'$ with a uniquely determined abelian minus extension H'/F. Since $H' \subset H$ and H/L is unramified, H'/F must be unramified outside $p_1, \ldots, p_s$, and at any prime dividing some p_i, the ramification group must be of exponent 1 or ℓ since this is so in L/F. (Indeed, the ramification degree can only be 1 or ℓ since all ramification is tame.) Hence H' is contained in N. To finish the proof, it suffices to show that H' is equal to N. Local class field theory gives that tame ramification groups in an abelian extension of number fields are always cyclic. In our situation each $\mathfrak{p} \mid p_i$ does ramify (tamely) in L/F with exponent ℓ, hence the extension LN/L is unramified everywhere, therefore $LN \subset H$. Since N/F is a minus extension, it must be contained in H' which is the minus part of H/F.

(b) This is a direct consequence of (a), the remark preceding the theorem, and Nakayama's lemma. □

The next step is to bring Stickelberger ideals (in the sense of Sinnott) into play. We know that they provide annihilators for class groups, and we are interested in finding cases where there are extra annihilators. To the extension $L/\mathbb{Q}$ one attaches the Stickelberger ideal $S_L \subset \mathbb{Z}_\ell[\mathrm{Gal}(L/\mathbb{Q})]$ as follows: For every subfield $L' \subset L$ which is the intersection of L and a cyclotomic field, one takes the standard Stickelberger element $\Theta_{L'} \in \mathbb{Z}_\ell[\mathrm{Gal}(L'/\mathbb{Q})]$ (*cf.* [11], beginning of §6.2), and lets S_L be the ideal generated by all $\mathrm{cor}_{L/L'}\,\Theta_{L'}$. (Note that we use the condition $\zeta_\ell \notin L$ to be sure that there are no denominators.) We identify the minus part of $\mathbb{Z}_\ell[\mathrm{Gal}(L/\mathbb{Q})]$ with the group ring $\mathbb{Z}_\ell[\Gamma]$. The image $\widetilde{S}_L$ of the minus part of S_L under this identification is then generated by all $\mathrm{cor}_{L/L'}\,\widetilde{\Theta}_{L'}$, where L' only runs over the imaginary intersections with cyclotomic fields, and $(1-\tau)\cdot\widetilde{\Theta}_{L'} = (1-\tau)\cdot\Theta_{L'}$. It follows from Sinnott's generalization of Stickelberger's classical theorem that $\widetilde{S}_L$ annihilates A_L^-. In fact we have a much stronger result due to Kurihara ([8], Theorem 0.6; note that this theorem also assumes $\zeta_\ell \notin L$):

Theorem 2.3. — *The $\mathbb{Z}_\ell[\Gamma]$-Fitting ideal of A_L^- is exactly $\widetilde{S}_L$.*

Proof. — Kurihara proved in loc. cit. that $\mathrm{Fitt}_{\mathbb{Z}_\ell[\Gamma]}(A_L^-) = \mathcal{S}_{\mathrm{Ku}}(L)$. Here $\mathcal{S}_{\mathrm{Ku}}(L)$ is obtained from Kurihara's Stickelberger ideal defined on page 48 (and written with capital Theta there) by tensoring with $\mathbb{Z}_\ell$ and taking the minus part. We must show that $\mathcal{S}_{\mathrm{Ku}}(L) = \widetilde{S}_L$ in our case.

Let $\bar{L}$ denote the genus field of L. As a genus field it satisfies condition (A) on page 47 of loc. cit., and therefore by Remark 2.4 of loc. cit., $\mathcal{S}_{\mathrm{Ku}}(\bar{L}) = \widetilde{S}_{\bar{L}}$. By definition

$$\mathcal{S}_{\mathrm{Ku}}(L) = \mathrm{res}_{\bar{L}/L}\,\mathcal{S}_{\mathrm{Ku}}(\bar{L}) = \mathrm{res}_{\bar{L}/L}\,\widetilde{S}_{\bar{L}} \subset \widetilde{S}_L.$$

For any $\alpha \in \widetilde{S}_L$ we have $\mathrm{cor}_{\bar{L}/L}\,\alpha \in \widetilde{S}_{\bar{L}} = \mathcal{S}_{\mathrm{Ku}}(\bar{L})$ and so

$$[\bar{L}\colon L]\alpha = \mathrm{res}_{\bar{L}/L}\,\mathrm{cor}_{\bar{L}/L}\,\alpha \in \mathrm{res}_{\bar{L}/L}\,\mathcal{S}_{\mathrm{Ku}}(\bar{L}) = \mathcal{S}_{\mathrm{Ku}}(L).$$

Therefore $[\widetilde{S}_{\bar{L}}\colon \mathcal{S}_{\mathrm{Ku}}(L)]$ can be nontrivial only if $\ell \mid [\bar{L}\colon L]$. This is not the case since $\bar{L}$ is the compositum of K and the genus field of F, and so the degree $[\bar{L}\colon L]$ is a power of 2. □

The trouble with Stickelberger ideals is that they need so many generators in general. This leads us to the following: We consider the ring R defined just after the proof of Lemma 1.3 and consider it as a factor ring of $\mathbb{Z}_\ell[\Gamma]$, factoring out by the ideal I generated by all norm elements N_{σ_i}, $i = 1, \dots, s$. Let overbar consistently denote base change from $\mathbb{Z}_\ell[\Gamma]$ to R, so in particular $\overline{A_L^-} = R \otimes_{\mathbb{Z}_\ell[\Gamma]} A_L^-$. From Kurihara's theorem and base change for Fitting ideals it follows that $\mathrm{Fitt}_R(\overline{A_L^-})$ is generated by the image of $\widetilde{S}_L$ in R. Taking this image drastically simplifies things: All generators of $\widetilde{S}_L$ go to zero except the generator $\vartheta := \widetilde{\Theta}_L$ associated to the top field. Let $f = \bar{\vartheta}$ be the image of ϑ in R. So $\mathrm{Fitt}_R(\overline{A_L^-}) = Rf$.

We can now combine this with a result of Cornacchia and the first author. Proposition 4 in [1] shows the equivalence of three properties; the basis ring used there is slightly more special, but the more general argument is exactly the same. Finiteness of $\overline{A_L^-}$ forces f to be a nonzerodivisor in R, so the R-Fitting ideal of $\overline{A_L^-}$ is principal and generated by a nonzerodivisor. This is exactly property 3 in the cited proposition. Hence property 2 in loc. cit. is also true, that is, $\overline{A_L^-}$ has a projective resolution of length one over R. This is just what we require for applying the results of §1. We can now show:

Theorem 2.4. — *With the above notations, as soon as A_L^- requires at least $s+2$ generators over $\mathbb{Z}_\ell[\Gamma]$, the $\mathbb{Z}_\ell[\Gamma]$-annihilator of A_L^- is strictly larger than the Stickelberger ideal $\widetilde{S}_L$ (and explicit annihilators outside the Stickelberger ideal will be given at the end of the proof).*

Proof. — In the sequel we let $\lambda' = (\sigma_1 - 1) \cdots (\sigma_s - 1)$ and we use the following abuse of notation: $\lambda'\delta$ denotes $\lambda'\delta'$ where δ' is any lift of $\delta \in R$ to $\mathbb{Q}_\ell[\Gamma]$. This makes sense since any two lifts δ' and δ'' differ by some element in $\mathbb{Q}_\ell I$, where $I \subset \mathbb{Z}_\ell[\Gamma]$ is generated by the norm elements N_{σ_i}, and $\lambda' I = 0$.

Let t be the number of generators of A_L^- over $\mathbb{Z}_\ell[\Gamma]$. Then by Nakayama's lemma the R-module $M := \overline{A_L^-}$ needs t generators as well. For any annihilator $\delta \in R$ of the R-module M, we claim that $\lambda'\delta$ (see above) annihilates A_L^-. Indeed, $\overline{A_L^-} = A_L^-/IA_L^-$ and so for any lift $\delta' \in \mathbb{Z}_\ell[\Gamma]$ of δ we have $\delta' A_L^- \subset IA_L^-$. From this it is immediate that $\lambda'\delta A_L^- = \lambda'\delta' A_L^- = 0$.

Recall that $f = \bar{\vartheta}$. By Corollary 1.5, for each choice of positive integers k_i satisfying $\sum_{i=1}^s k_i = t-2$, the corresponding elements

$$\delta = \frac{f \ell^{s-1}}{\prod_{i=1}^s \lambda_i^{k_i+1}}$$

are in $\mathrm{Ann}_R(M)$, where $\lambda_i \in R$ is the image of $\sigma_i - 1$. Hence $\lambda'\delta \in \mathrm{Ann}_{\mathbb{Z}_\ell[\Gamma]} A_L^-$. Corollary 1.5 says that $\lambda\delta$ (the image of $\lambda'\delta$ in R) is not in fR (the image of $\widetilde{S}_L$ in R), therefore $\lambda'\delta$ is never in $\widetilde{S}_L$.

It remains to write out explicitly the elements $\lambda'\delta$. They are in $\mathbb{Z}_\ell[\Gamma]$ since δ can be lifted to $\mathbb{Z}_\ell[\Gamma]$. We first transform δ: For each $i = 1, \dots, s$, let μ_i be determined by $\lambda_i\mu_i = \ell$ in R. Then μ_i is associated to $\lambda_i^{\ell-2}$, so we may choose its lift as follows: $\mu_i' = u_i'(\sigma_i - 1)^{\ell-2} \in \mathbb{Z}_\ell[\Gamma]$, where u_i' is a lift of a suitable unit u_i of R. Note that u_i' is automatically a unit since $\mathbb{Z}_\ell[\Gamma]$ and R are local. Then

$$\delta = f\ell^{s-1}\prod_{i=1}^{s}(\mu_i\ell^{-1})^{k_i+1} = f\ell^{1-t}\prod_{i=1}^{s}\mu_i^{k_i+1}.$$

Since $(\sigma_i - 1)\mu_i' = \ell - \mathrm{N}_{\sigma_i}$ and $k_i > 0$, we have

$$\lambda'\delta = \vartheta\ell^{1-t}\prod_{i=1}^{s}(\ell - \mathrm{N}_{\sigma_i})(u_i'(\sigma_i - 1)^{\ell-2})^{k_i} = \vartheta\ell^{s+1-t}\prod_{i=1}^{s}(u_i'(\sigma_i - 1)^{\ell-2})^{k_i}.$$

Therefore $\lambda'\delta$ is associated to

$$\vartheta\ell^{s+1-t}\prod_{i=1}^{s}(\sigma_i - 1)^{(\ell-2)k_i},$$

which is an explicit annihilator of A_L^- outside the Stickelberger ideal. □

The preceding theorem should be considered in conjunction with the following proposition, whose proof is clear from the short exact sequence $(*)$ (just before Theorem 2.2):

Proposition 2.5. — *The condition "A_L^- requires at least $s+2$ generators" and hence the conclusion of Theorem 2.4 hold in the following cases:*

(i) *The class group Cl_F has ℓ-rank at least $s+2$.*

(ii) *The class group Cl_F has ℓ-rank at least 2 and the exact sequence mentioned above is split.*

When looking for examples, we need ℓ-rank at least 3 in (i) (since we are assuming $s \geqslant 1$), which forces F to have a large conductor already for $\ell = 3$ (over 3 million). For an example where (ii) is applicable, see §3.3; we actually checked the validity of Theorem 2.4 numerically in this example.

Let us sum up: We know that A_L^- needs at least s generators. If the minimal number of generators is at least $s+2$, we are able to exhibit extra annihilators. The cases where $m_{\mathbb{Z}_\ell[\Gamma]}(A_L^-) = s$ or $s+1$ remain undecided. However, the case $s = 1$ and $m_{\mathbb{Z}_\ell[\Gamma]}(A_L^-) = s$ is clear: Here A_L^- is a cyclic Galois module, hence its annihilator and Fitting ideal coincide, and

Theorem 2.3 gives the answer: The Stickelberger ideal is indeed the exact annihilator.

Henceforward we shall relax our assumption that all primes p_i split in F. Let us assume that besides our primes $p_1, \dots, p_s$ we also have new primes $p_{s+1}, \dots, p_t$, all congruent to 1 modulo ℓ and all inert in F. Even though it would not be necessary, we exclude the case of primes ramifying in F to keep things simple. Again let K_i be the cyclic fields of degree ℓ and conductor p_i over $\mathbb{Q}$. Let $K' = K_1 \cdots K_t$ be the compositum and $L' = FK'$, so $K \subset K'$ and $L \subset L'$. We shall show that if η is a new annihilator of A_L^- then $\operatorname{cor}_{L'/L} \eta$ is a new annihilator of $A_{L'}^-$. Lemma 1.6(c) states that if η is an annihilator of A_L^- then $\operatorname{cor}_{L'/L} \eta$ is an annihilator of $A_{L'}^-$. So we need to show

Proposition 2.6. — *Let $\eta \in \mathbb{Z}_\ell[\mathrm{Gal}(L/F)]$. If $\eta \notin \widetilde{S}_L$ then $\operatorname{cor}_{L'/L} \eta \notin \widetilde{S}_{L'}$.*

Proof. — We begin by stating a lemma. For any subset $T \subset \{1, \dots, s\}$ and any subset $T' \subset \{s+1, \dots, t\}$ let $L_{T \cup T'} = F \prod_{i \in T \cup T'} K_i$. We shall also use the abbreviation $L'_T = L_{T \cup \{s+1, \dots, t\}}$ for any $T \subset \{1, \dots, s\}$. The Galois group $G = \mathrm{Gal}(L'/F)$ may be canonically identified with $\prod_{i=1}^t G_i$, where $G_i = \mathrm{Gal}(K_i/\mathbb{Q})$. Let us fix a generator σ_i of G_i; then $\sigma_1, \dots, \sigma_t$ form a basis of G (as a vector space over $\mathbb{Z}/\ell\mathbb{Z}$). So σ_i acts as identity on all K_j, $j \neq i$. Let $\Delta = \mathrm{Gal}(L'/L) = \langle \sigma_{s+1}, \dots, \sigma_t \rangle$.

Lemma 2.7. — *The set*

$$\left\{ \Big(\prod_{i \in T} \sigma_i^{a_i} \prod_{i=s+1}^{t} \sigma_i^{b_i} \Big) \operatorname{cor}_{L'/L'_T} \widetilde{\Theta}_{L'_T} \;\Big|\; T \subset \{1, \dots, s\}, \; 0 \leqslant a_i \leqslant \ell - 2, \; 0 \leqslant b_i \leqslant \ell - 1 \right\}$$

is a basis of $\widetilde{S}_{L'}$ as a $\mathbb{Z}_\ell$-module and in particular $\widetilde{S}_{L'}$ is free over $\mathbb{Z}_\ell[\Delta]$.

Proof. — It is easy to see that this set consists of exactly

$$\ell^{t-s} \sum_{j=0}^{s} \binom{s}{j} (\ell - 1)^j = \ell^t = [L' \colon F]$$

elements, which is the $\mathbb{Z}_\ell$-rank of $\widetilde{S}_{L'}$. Let M be the $\mathbb{Z}_\ell$-module generated by the mentioned set of generators. So we only need to show that $M = \widetilde{S}_{L'}$. For any $i \in T \subset \{1, \dots, s\}$ we have the following distribution relation

$$\Big(\sum_{a=0}^{\ell-1} \sigma_i^a \Big) \cdot \operatorname{cor}_{L'/L'_T} \widetilde{\Theta}_{L'_T} = (1 - \mathrm{Frob}(p_i)^{-1}) \cdot \operatorname{cor}_{L'/L'_{T \setminus \{i\}}} \widetilde{\Theta}_{L'_{T \setminus \{i\}}},$$

where $\mathrm{Frob}(p_i) \in G$ is any extension to L' of the Frobenius automorphism for p_i on $F \prod_{j=1,\dots,t,\, j\neq i} K_j$. Using induction with respect to the cardinality of T we can easily prove that the mentioned set generates

$$\Big(\prod_{i\in T} \sigma_i^{a_i} \prod_{i=s+1}^{t} \sigma_i^{a_i}\Big) \cdot \mathrm{cor}_{L'/L'_T} \widetilde{\Theta}_{L'_T}$$

for all $T \subset \{1,\dots,s\}$ and all $0 \leqslant a_i \leqslant \ell{-}1$. But this means that M is a $\mathbb{Z}_\ell[G]$-module. For any $i > s$ the prime p_i stays inert in F and so $\mathrm{Frob}(p_i)$ restricts on F to the nontrivial automorphism. Hence $\tau\,\mathrm{Frob}(p_i) \in G$ (recall that τ is complex conjugation). Therefore, in $\mathbb{Z}_\ell[\mathrm{Gal}(L'/\mathbb{Q})]$,

$$(1-\tau)(1-\mathrm{Frob}(p_i)^{-1}) = (1-\tau)(1+\tau\,\mathrm{Frob}(p_i)^{-1})$$

which gives for any $T' \subset \{s+1,\dots,t\}$ the following distribution relation (recall that we are identifying the minus part of $\mathbb{Z}_\ell[\mathrm{Gal}(L'/\mathbb{Q})]$ with the group ring $\mathbb{Z}_\ell[G]$)

$$\Big(\prod_{i\in\{s+1,\dots,t\}\setminus T'} \sum_{a_i=0}^{\ell-1} \sigma_i^{a_i}\Big) \cdot \mathrm{cor}_{L'/L'_T} \widetilde{\Theta}_{L'_T} = \Big(\prod_{i\in\{s+1,\dots,t\}\setminus T'} (1+\tau\,\mathrm{Frob}(p_i)^{-1})\Big) \cdot \mathrm{cor}_{L'/L_{T\cup T'}} \widetilde{\Theta}_{L_{T\cup T'}}.$$

Since $\ell \neq 2$, it is easy to see that $(1+\tau\,\mathrm{Frob}(p_i)^{-1})$ is a unit of $\mathbb{Z}_\ell[G]$, and so we have obtained that $\mathrm{cor}_{L'/L_{T\cup T'}} \widetilde{\Theta}_{L_{T\cup T'}} \in M$. The lemma follows. □

Let us finish the proof of Proposition 2.6. As $\widetilde{S}_{L'}$ is a free $\mathbb{Z}_\ell[\Delta]$-module, we have $\widetilde{S}_{L'}^{\Delta} = \mathrm{N}_\Delta \widetilde{S}_{L'}$ and so

$$\mathrm{cor}_{L'/L}^{-1}(\widetilde{S}_{L'}) = \mathrm{cor}_{L'/L}^{-1}(\widetilde{S}_{L'}^{\Delta}) = \mathrm{cor}_{L'/L}^{-1}(\mathrm{N}_\Delta \widetilde{S}_{L'}) = \mathrm{res}_{L'/L}(\widetilde{S}_{L'}) \subset \widetilde{S}_L,$$

and the proposition is proved. □

In the cases where we have proved the existence of extra annihilators, we did not prove explicitly that one can extract roots of Gauss sums. It is not clear how the fact that Cl_F has high ℓ-rank (which may be seen as a statement concerning Gauss sums attached to F) influences Gauss sums attached to L, since there is no direct arithmetic link between Gauss sums attached to L and Gauss sums attached to F: The norm from L to F annihilates the former ones, because of the presence of Euler factors and the condition that at least one ramified prime in L/F splits in F.

3. Numerical results for the borderline cases

We recall that $L = FK$, and K is the compositum of s distinct fields K_i, each abelian of the same odd prime degree ℓ, totally tamely ramified at p_i, unramified elsewhere. We also recall that the p_i are assumed to split in the quadratic field F. From Theorem 2.2 we know that $m(A_L^-)$ is always at least s, and we now distinguish three cases, two of which are not covered by Theorem 2.4.

3.1. The case $m(A_L^-) = s$

From Theorem 2.2 and the exact sequence $(*)$, we see that A_L^- needs exactly s generators over $\mathbb{Z}[\Gamma]$, whenever Cl_F^- has trivial ℓ-part.

We put $\ell = 3$ and $F = \mathbb{Q}(i)$, so that the latter condition is certainly satisfied. Hence $m(A_L^-) = s$, so the hypothesis of Theorem 2.4 is not satisfied, and it is not clear a priori whether the annihilator $\mathcal{J}_L$ of A_L^- is equal to, or larger than $\widetilde{S}_L$.

For our calculations we put $s = 2$. The smallest possible field K then has conductor $13{\cdot}37$. The minus class group of $L = K(i)$ is of type $18\times18\times9\times3$, so A_L^- has order 3^7, and $\widetilde{S}_L$ has index $|A_L^-|$ in $\mathbb{Z}_3[\Gamma]$. (The latter statement is correct for all odd ℓ, all s and K by Sinnott's formula – see Theorems 2.1, 5.2 and 5.4 of [10]). We then calculated the index of $\mathcal{J}_L$ as follows. PARI gives the class group as a product of cyclic groups, and also the action of Γ on the class group. The Galois group is given by PARI as an unstructured set of automorphisms, in which only the identity is clearly identifiable. We took the lazy approach of finding two generators of $\Gamma \cong \mathbb{Z}/3 \times \mathbb{Z}/3$ just by determining sufficiently many products of automorphisms, which is easy in PARI. (Of course one might be more systematic: Class field theory affords a natural epimorphism $(\mathbb{Z}/p_1p_2\mathbb{Z})^* \to \Gamma$. The natural thing to do would be to determine generators of Γ as images of generators of $(\mathbb{Z}/p_1p_2\mathbb{Z})^*$. However, PARI does not directly support this calculation, and we do not need the extra information.) We thus found, with little effort, generators σ_1 and σ_2 of Γ and 4×4-matrices M_1, M_2 that give the action of these two automorphisms on the module $A_L^- \cong \mathbb{Z}/9 \times \mathbb{Z}/9 \times \mathbb{Z}/9 \times \mathbb{Z}/3$.

Determining the $\mathbb{Z}_3[\Gamma]$-annihilator of this module is in principle easy linear algebra: Every element σ of Γ gives an automorphism M_σ of the $\mathbb{Z}_3$-module A_L^-, encoded as a square matrix with integer (or mod 9) entries, and the kernel of the map $\mathbb{Z}_3[\Gamma] \to \mathrm{End}_{\mathbb{Z}}(A_L^-)$, $\sigma \mapsto M_\sigma$, is $\mathcal{J}_L$. Hence the desired index $[\mathbb{Z}_3[\Gamma] \colon \mathcal{J}_L]$ is equal to the order of the additive group generated by all nine matrices M_σ. To find this order is not difficult: One unpacks the matrices M_σ into long row vectors (of length 16 in our example), and looks at the Hermite normal form of the resulting 9×16-matrix; from it one can read off the order of the row space. A little care is needed here and in all other examples, since A_L^- is a direct sum of modules $\mathbb{Z}/3^i$ with various i, and consequently the entries of the matrices live in different factor rings of $\mathbb{Z}$, but this is not a serious problem. The outcome in this example was: The index $[\mathbb{Z}_3[\Gamma]\colon \mathcal{J}_L]$ is 3^7 again, so $\mathcal{J}_L = \widetilde{S}_L$ (since one inclusion is clear from Stickelberger's classical theorem).

The main computational hurdle is to obtain the matrices for the action of σ_1 and σ_2 on the class group, since this invokes the function `bnfisprincipal`, one of the most time-consuming functions in this part of PARI. We computed 22 examples. In each example we had $\ell = 3$, $s = 2$, and p_1, p_2 were taken from the set $\{13, 37, 61, 73, 109, 157, 181, 337, 373, 421\}$. All ten combinations with both p_i at most 109 were done; the others were chosen by computational expedience (the calculations begin to get sluggish for greater values). The result is quick to state:

In one of these 22 cases, the annihilator ideal $\mathcal{J}_L$ is (by an index 3) larger than the Stickelberger ideal; in all other cases we have equality. The exceptional case is: $(p_1, p_2) = (109, 157)$.

There were various consistency checks in our calculations. First, no case was found where the index of the annihilator ideal was larger than that of the Stickelberger ideal. Second, we double-checked that the module A_L^- needs exactly two generators over $\mathbb{Z}_3[\Gamma]$, by calculating the coinvariants $(A_L^-)_\Gamma$ and noting that this is a $\mathbb{Z}_3$-module which needs exactly 2 generators.

We did not do any case with $s = 3$ since even the minimal choice $(p_1, p_2, p_3) = (13, 37, 61)$ probably leads to an intractable field.

3.2. The case $m(A_L^-) = s + 1$

This is another case where Theorem 2.4 gives no information. We again took $\ell = 3$, but now $s = 1$. We chose $F = \mathbb{Q}(\sqrt{-23})$ which has class number 3. Therefore, by Theorem 2.2 and the exact sequence $(*)$, the minimal number of generators of A_L^- is 2 or 1, depending on whether the exact sequence is split or not, and we will only consider cases where it splits. Via PARI we produced a list of primes p_1 such that for $L = FK$ with K the cubic field of conductor p_1, the sequence does split. This was easy by calculating a ray class group using `bnrclass`. The list begins with 151, 163, 307, ... It is relatively easy to calculate A_L^- (hence the index of $\widetilde{S}_L$) and also $\mathcal{J}_L$ for each case. For instance if $p_1 = 151$, A_L^- is $\mathbb{Z}/9 \times \mathbb{Z}/3$, with a generator σ of Γ acting via the matrix

$$\begin{pmatrix} 7 & 0 \\ 6 & 1 \end{pmatrix}$$

(multiplication by this matrix on the right). One can even check by hand that the annihilator is $(3, \sigma{-}1)^2$ (the square of the radical of $\mathbb{Z}_3[\Gamma]$) in this example, and this has index 3^3, hence one gets equality of indices.

We treated all relevant p_1 up to 5000. This comes to 43 values (the largest being 4957). Our findings can be summarized as follows:

In exactly 13 of these 43 cases, the annihilator ideal is larger than the Stickelberger ideal. The first such case is $p_1 = 307$, the third on the total list; it has $|A_L^-| = 3^3$ and annihilator index 3^2. In all of the 13 cases with a discrepancy, the discrepancy was exactly a factor 3. The largest value observed for $|A_L^-|$ was 3^9, for the single prime $p_1 = 4129$, and this happened to agree with the annihilator index.

3.3. The case $m(A_L^-) = s + 2$

In principle we do not need to calculate examples in this situation, since Theorem 2.4 applies! Nevertheless, we did one case numerically as a double-check. We take $s = 1$, $\ell = 3$ again; we need to change F however, since we need 3-rank 2 for Cl_F, plus splitting of $(*)$, to ensure that $m(A_L^-) = 3$. The minimal example for 3-rank 2 with prime conductor is $F = \mathbb{Q}(\sqrt{-4027})$; here $\mathrm{Cl}_F = A_F^- = \mathbb{Z}/3 \times \mathbb{Z}/3$. The prime 97 splits in F, and the exact sequence $(*)$ can be shown to split as well by PARI. One finds $A_L^- = \mathbb{Z}/9 \times \mathbb{Z}/9 \times \mathbb{Z}/3 \times \mathbb{Z}/3$. Hence the Stickelberger ideal has index 3^6, and the same kind of calculation as in earlier examples shows that the annihilator index is 3^4. (Note that the discrepancy 3^2 is larger than in the previous subsection. The first "3" comes from the fact that A_F^- is not cyclic, which yields the annihilator $3\,\mathrm{N}_\sigma$, while the Stickelberger ideal only contains $9\,\mathrm{N}_\sigma$. The second "3" comes from Theorem 2.4, which provides the annihilator $(\sigma{-}1)^3$, while the Stickelberger ideal only contains $(\sigma{-}1)^4$.) This numerically confirms Theorem 2.4.

4. The non-genus case

We now consider an imaginary field L_0 which is the compositum of the imaginary field F and an elementary ℓ-abelian field K_0 which is not a genus field. Let K be the genus field of K_0, and let $L = FK$. We retain the notations s, Γ attached to L in §2, and also the assumption that $\zeta_\ell \notin F$. As in §2, we think of K as being the compositum $K = K_1 \cdots K_s$ where $K_i/\mathbb{Q}$ is of degree ℓ and conductor p_i, and p_i splits in F, and we choose generators $\sigma_1, \dots, \sigma_s$ of Γ according to this decomposition. In particular s is the number of primes ramifying in $K_0/\mathbb{Q}$, and likewise in $K/\mathbb{Q}$. Let $\Delta = \mathrm{Gal}(K/K_0)$; this will always be identified with $\mathrm{Gal}(L/L_0)$. Let $\mathrm{cor} = \mathrm{cor}_{L/L_0}$ denote the usual corestriction $\mathbb{Q}_\ell[\Gamma/\Delta] \to \mathbb{Q}_\ell[\Gamma]$. We recall that the minus part of the Stickelberger ideals attached to L (resp. L_0) are identified (see §2) with ideals $\widetilde{S}_L \subset \mathbb{Z}_\ell[\Gamma]$ (respectively $\widetilde{S}_{L_0} \subset \mathbb{Z}_\ell[\Gamma/\Delta]$). If res denotes the canonical map $\mathbb{Q}_\ell[\Gamma] \to \mathbb{Q}_\ell[\Gamma/\Delta]$, then the maps $\mathrm{cor} : \widetilde{S}_{L_0} \to \widetilde{S}_L$ and $\mathrm{res} : \widetilde{S}_L \to \widetilde{S}_{L_0}$ are well-defined, and we remark that cor is injective.

The point of all this is that one sometimes can obtain annihilators for $A^-_{L_0}$ outside $\widetilde{S}_{L_0}$ by taking a detour via the genus field. Lemma 1.6(c) says: The full preimage $\mathrm{cor}^{-1}\widetilde{S}_L \subset \mathbb{Z}_\ell[\Gamma/\Delta]$ annihilates $A^-_{L_0}$. On the other hand it follows from the definition of cor that

$$\mathrm{cor}\ \mathrm{cor}^{-1}\widetilde{S}_L = \widetilde{S}_L^{\Delta}.$$

Thus cor induces an isomorphism

$$\mathrm{cor}^{-1}\widetilde{S}_L/\widetilde{S}_{L_0} \cong \widetilde{S}_L^{\Delta}/\,\mathrm{cor}\,\widetilde{S}_{L_0},$$

and we now see: As soon as these modules are nontrivial, the annihilator of $A^-_{L_0}$ is strictly larger than $\widetilde{S}_{L_0}$.

Our idea is now to relate the right hand quotient to $\widehat{\mathrm{H}}^0(\Delta, \widetilde{S}_L)$ in Tate's sense. Actually $\mathrm{cor}\,\widetilde{S}_{L_0}$ contains $\mathrm{N}_\Delta\,\widetilde{S}_L$, and we want to control both the discrepancy between $\mathrm{cor}\,\widetilde{S}_{L_0}$ and $\mathrm{N}_\Delta\,\widetilde{S}_L$, and the size of the module $\widehat{\mathrm{H}}^0(\Delta, \widetilde{S}_L)$. More to the point, we would like the discrepancy to be small, and $\widehat{\mathrm{H}}^0(\Delta, \widetilde{S}_L)$ to be large.

Let d denote the $\mathbb{Z}/\ell\mathbb{Z}$-dimension of Δ. Via the generators $\sigma_1, \dots, \sigma_s$ we identify Γ with $(\mathbb{Z}/\ell\mathbb{Z})^s$. We say that Δ is in general position, if any projection $(\mathbb{Z}/\ell\mathbb{Z})^s \to (\mathbb{Z}/\ell\mathbb{Z})^d$, arising from the choice of a d-element subset of $\{1, \dots, s\}$, becomes bijective when restricted to Δ. Note that in case $d = 1$, Δ is automatically in general position, since otherwise K_0 would have smaller conductor than K.

Lemma 4.1. — *If Δ is in general position, then* $\mathrm{cor}\,\widetilde{S}_{L_0}/\,\mathrm{N}_\Delta\,\widetilde{S}_L$ *can be generated by $a(d)$ elements over $\mathbb{Z}_\ell[\Gamma]$, where $a(d) = 1 + \binom{s}{1} + \cdots + \binom{s}{d-1}$. In case $d = 1$, this factor module is at most of order ℓ.*

Proof. — By the construction of Sinnott's Stickelberger ideal, $\widetilde{S}_{L_0}$ is generated by terms $\eta_{I,0} := \mathrm{cor}_{L_0/FK_I \cap L_0}\,\mathrm{res}_{FK_I/FK_I \cap L_0}\,\widetilde{\Theta}_{FK_I}$, where I runs through all subsets of $\{1,\dots,s\}$ and K_I is the compositum of the K_i with $i\in I$. One has the formula

$$[L\colon L_0K_I]\,\mathrm{cor}_{L/L_0}\,\eta_{I,0}=\mathrm{N}_\Delta\,\eta_I,$$

with $\eta_I=\mathrm{cor}_{L/FK_I}\,\widetilde{\Theta}_{FK_I}\in\widetilde{S}_L$. It suffices to show that the factor $[L\colon L_0K_I]$ is 1 for $|I|\geqslant d$: Then the quotient module in the lemma is generated by the $\eta_{I,0}$ with $|I|<d$, which gives exactly what we want. For $|I|\geqslant d$, the statement $[L\colon L_0K_I]=1$ is a consequence of the "general position" hypothesis: The degrees $[L\colon L_0]$ and $[FK_I\colon L_0\cap FK_I]$ are both equal to ℓ^d for $|I|\geqslant d$, and this translates into $[L\colon L_0K_I]=1$. For $d=1$, we only require the generator $\eta_{\emptyset,0}$, and this spans a trivial module; the quotient module in the lemma is a submodule of $\widehat{\mathrm{H}}^0(\Delta,\widetilde{S}_L)$, hence annihilated by $|\Delta|$ which is ℓ in case $d=1$. Hence this trivial submodule is of order at most ℓ. □

In general the cohomology of $\widetilde{S}_L$ does not seem to be manageable at all. We discuss one special case now.

Proposition 4.2. — *Suppose that each p_i is an ℓ-th power residue modulo every other p_j $(i,j\in\{1,\dots,s\})$. Then:*

(a) *The Γ/Δ-module $\widehat{\mathrm{H}}^0(\Delta,\widetilde{S}_L)$ has a direct summand which is a direct sum of $\binom{s}{d+1}$ cyclic factors.*

(b) *The module $\widetilde{S}_L^{\Delta}/\mathrm{cor}\,\widetilde{S}_{L_0}$ requires at least $\binom{s}{d+1}-a(d)$ generators; so if this number is positive, the annihilator of $A^-_{L_0}$ is strictly larger than $\widetilde{S}_{L_0}$.*

Proof.

(a) Under the hypothesis of the proposition, $\widetilde{S}_L$ is the direct sum of the Galois modules spanned by the generators η_I, and each of these is isomorphic to $R_I:=\mathbb{Z}_\ell[\langle\sigma_i\mid i{\in}I\rangle]/(\mathrm{N}_{\sigma_i}\mid i{\in}I)$ (*cf.* [3], Lemma 5.4). By the next lemma, for every I containing exactly $d+1$ elements, the group $\widehat{\mathrm{H}}^0(\Delta,R_I)$ is cyclic and nontrivial. The number of such sets I is exactly $\binom{s}{d+1}$.

(b) This follows from (a), the tautological short exact sequence

$$0\to\mathrm{cor}\,\widetilde{S}_{L_0}/\,\mathrm{N}_\Delta\,\widetilde{S}_L\to\widehat{\mathrm{H}}^0(\Delta,\widetilde{S}_L)\to\widetilde{S}_L^{\Delta}/\,\mathrm{cor}\,\widetilde{S}_{L_0}\to 0$$

and Lemma 4.1. □

Lemma 4.3. — *Under the above assumptions on Δ, let I be a subset of $\{1,\dots,s\}$, $|I|=d+1$, and $R_I:=\mathbb{Z}_\ell[\langle\sigma_i\mid i\in I\rangle]/(\mathrm{N}_{\sigma_i}\mid i\in I)$. Then $\widehat{\mathrm{H}}^0(\Delta,R_I)$ is a nontrivial cyclic $\mathbb{Z}_\ell[\Gamma]$-module.*

Proof. — We may suppose $I = \{1, \dots, d+1\}$ and consider everything as Γ'-modules, with $\Gamma' = \langle \sigma_1, \dots, \sigma_r \rangle$, where $r = d+1$. We also know that Δ has ℓ-rank d and is in general position. Without loss of generality we can assume that $\Delta = \langle \sigma_i \sigma_1^{-1} \mid i = 2, \dots, r \rangle$. Multiplication with $\lambda' := (\sigma_1 - 1) \cdots (\sigma_r - 1)$ induces an isomorphism $R_I \cong A \subset \mathbb{Z}_\ell[\Gamma']$, where A is the cyclic ideal generated by λ'. Then $\mathrm{N}_\Delta A$ is generated by $\mathrm{N}_\Delta \cdot \lambda'$, whereas $B := A^\Delta$ is the intersection of A with the cyclic ideal generated by N_Δ. By easy direct arguments one proves for any $\alpha \in \mathbb{Z}_\ell[\Gamma']$:

$$\alpha \in A \iff \mathrm{N}_{\sigma_i} \alpha = 0, \quad \forall i = 1, \dots, r.$$

On the other hand, since $\Delta = \langle \sigma_i \sigma_1^{-1} \mid i = 2, \dots, r \rangle$, the expressions $(\sigma_i - 1) \mathrm{N}_\Delta$ are all equal ($i = 1, \dots, r$). A direct argument shows: $\beta \in \langle \mathrm{N}_\Delta \rangle$ is annihilated by N_{σ_i} if and only if it has the form $(\sigma_i - 1) \mathrm{N}_\Delta \gamma$, where $\gamma \in \mathbb{Z}_\ell[\langle \sigma_i \rangle]$. Taking all this together yields:

$$A = \langle \mathrm{N}_\Delta \cdot (\sigma_1 - 1)^r \rangle; \quad B = \langle \mathrm{N}_\Delta \cdot (\sigma_1 - 1) \rangle.$$

Since B/A is the desired cohomology group, we are done. □

We have two applications of this, one for a whole range of values of d but assuming strong extra conditions, and another for $d = 1$.

Proposition 4.4. — *In the following two situations, the annihilator of $A^-_{L_0}$ is strictly larger than $\widetilde{S}_{L_0}$:*

(1) *For all $i, j \in \{1, \dots, s\}$, $i \neq j$, p_i is an ℓ-th power residue modulo p_j, and d is such that $\binom{s}{d+1} > a(d)$. (Recall that $a(d) = 1 + \binom{s}{1} + \cdots + \binom{s}{d-1}$.)*

(2) *$d = 1$ and $s > 1$.*

Proof.

(1) is already proved in Proposition 4.2 b).

(2) In this situation, the cohomology group $\widehat{\mathrm{H}}^0(\Delta, \widetilde{S}_L)$ was in principle already calculated by Sinnott (Proposition 5.3 in [10]): $\widetilde{S}_L$ is canonically isomorphic to the module U attached to K (the real subfield of L), $\tilde{\eta}_I$ mapping to α_{f, n_I}, where f is the conductor of K and n_I the conductor of K_I. The outcome is: $\widehat{\mathrm{H}}^0(\Delta, \widetilde{S}_L)$ is a direct sum of 2^{s-1} factors $\mathbb{Z}/\ell\mathbb{Z}$. We look again at the short exact sequence in the proof of Proposition 4.2 b). By Lemma 4.1 (last statement), the left hand term is of order at most ℓ. The middle term has 2^{s-1} factors $\mathbb{Z}/\ell\mathbb{Z}$, and therefore the right hand term cannot be trivial. As above this proves our assertion. □

5. Distribution relations for Gauss sums

Let m be a positive integer and p be an odd prime, $p \nmid m$. Let $\mathfrak{P} \mid p$ be a prime ideal of the m-th cyclotomic field $\mathbb{Q}(\zeta_m)$, where $\zeta_m = e^{2\pi i/m}$. Let f be the minimal positive integer satisfying $m \mid p^f - 1$, *i.e.* f is the absolute inertia degree of $\mathfrak{P}$. So $\mathbb{Z}[\zeta_m]/\mathfrak{P} \simeq \mathbb{F}_{p^f} \supset \mathbb{F}_p$. Let $\chi \colon \mathbb{F}_{p^f}^* \to \mu_m = \langle \zeta_m \rangle \subset \mathbb{Q}(\zeta_m)^*$ be the m-th power residue symbol, *i.e.* for any $a \in \mathbb{Z}[\zeta_m]$ such that $\mathfrak{P} \nmid a$ we have

$$\chi(a \mod \mathfrak{P}) \equiv a^{(p^f-1)/m} \pmod{\mathfrak{P}}.$$

Let $\psi \colon \mathbb{F}_{p^f} \to \mathbb{Q}(\zeta_p)$ be the usual additive character of $\mathbb{F}_{p^f}$, *i.e.* $\psi(t) = \zeta_p^{\mathrm{Tr}(t)}$. For any integer a, $0 < a < m$, let us consider the following Gauss sum x_a:

$$x_a = g(\chi^{m-a}, \psi) = -\sum_{t \in \mathbb{F}_{p^f}^*} \chi(t)^{m-a} \psi(t).$$

The following proposition states the well-known Davenport-Hasse distribution relations for Gauss sums.

Proposition 5.1. — *For any positive integer $r \mid m$ and any $a \in \mathbb{Z}$ we have*

$$\prod_{i=0}^{r-1} x_{a+i\frac{m}{r}} = \chi(r)^{ar} \cdot x_{ar} \cdot \prod_{i=1}^{r-1} x_{i\frac{m}{r}} \tag{5.1}$$

and

$$\prod_{i=1}^{r-1} x_{i\frac{m}{r}}^2 = \left((-1)^{(p-1)/2} \cdot p\right)^{f(r-1)}. \tag{5.2}$$

Proof. — The first formula (equation (5.1)) can for instance be found in Theorem 10.1 of Chapter 2 of [9]. The notations differ slightly, for example the m of loc. cit. corresponds to our r.

The second formula follows from Lemma 6.1(b) in [11] and the following easy observation concerning the case of even m: $\chi^{m/2}(-1) = -1$ if and only if the order of the multiplicative group of $\mathbb{F}_{p^f}$ is not divisible by 4, which is the case if and only if f is odd and $p \equiv 3 \pmod 4$. □

For any integer a we put $z_a = \left(x_a^2 \cdot \left((-1)^{(p-1)/2} p\right)^{-f}\right)^m$ if $m \nmid a$ and $z_a = 1$ if $m \mid a$. Well-known properties of Gauss sums show that z_a is a system of non-zero numbers of the m-th cyclotomic field. We can even say more, namely $z_a \in \mathbb{Q}(\zeta_{m/(a,m)})$. Moreover, if an automorphism σ of $\mathbb{Q}(\zeta_m)$ satisfies $\zeta_m^\sigma = \zeta_m^t$ for an integer t then we have $z_a^\sigma = z_{at}$. Finally, the numbers z_a satisfy distribution properties stated in the following corollary of Proposition 5.1:

Corollary 5.2. — *For any integer a and any positive $r \mid m$ we have*

$$\prod_{i=0}^{r-1} z_{a+i\frac{m}{r}} = z_{ar}. \tag{5.3}$$

Moreover, if $r > 1$ is a power of a prime s and $(r, \frac{m}{r}) = 1$, then we have

$$\prod_{\substack{b\equiv a \pmod{m/r} \\ s\nmid b,\ 0\leqslant b<m}} z_b = z_{ar}^{1-\mathrm{Frob}(s)^{-1}}, \tag{5.4}$$

where $\mathrm{Frob}(s)$ *is the Frobenius of s on the $\frac{m}{r}$-th cyclotomic field, i.e. the automorphism sending each root of unity to its s-th power.*

Proof. — It is easy to see that (5.3) follows directly from the definition of z_a and (5.1) and (5.2). To prove (5.4) let us notice that nothing is changed if we write $a + \frac{m}{r}$ instead of a. So we can assume that $s \mid a$ and so (5.3) gives

$$\begin{aligned}\prod_{\substack{b\equiv a \pmod{m/r} \\ s\nmid b,\ 0\leqslant b<m}} z_b &= \Big(\prod_{i=0}^{r-1} z_{a+i\frac{m}{r}}\Big)\cdot\Big(\prod_{i=0}^{r/s-1} z_{a+i\frac{ms}{r}}\Big)^{-1} \\ &= z_{ar}\cdot z_{ar/s}^{-1} = z_{ar}^{1-\mathrm{Frob}(s)^{-1}}\end{aligned}$$

and the corollary is proved. □

Formula (5.4) needs some final interpretation. Its left hand side is simply the norm of z_a from $\mathbb{Q}(\zeta_m)$ to $\mathbb{Q}(\zeta_{m/r})$. We will need to keep track of the conductor m in our notation, so we write $z_a^{(m)}$ for the quantity z_a when necessary. For $f = 1$ (which will always be assumed in the sequel) one easily checks that $z_{ar}^{(m)} = \big(z_a^{(m/r)}\big)^r$. Thus we may rewrite the last corollary in the following form, which does show that we have a kind of Euler system of Gauss sums.

Corollary 5.3. — *With notations as in Corollary 5.2 and assuming $f = 1$, we have*

$$\mathbb{N}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_{m/r})} z_a^{(m)} = \big(z_a^{(m/r)}\big)^{r\cdot(1-\mathrm{Frob}(s)^{-1})}.$$

This last corollary shows that we can perform just about the same tricks on the $z_a^{(m)}$ as on circular units. (It will suffice to work with $a = 1$.) The only major difference is the fact that the circular units form an even distribution while the $z_a^{(m)}$'s form an odd one, that is: $z_a^{(m)} \cdot z_{m-a}^{(m)} = 1$ for any integer a.

6. The cyclic case via roots of Gauss sums

We again consider an imaginary field L_0 which is the compositum of the imaginary field F of conductor f and an ℓ-abelian field K_0. But instead of assuming that K_0 is an elementary ℓ-abelian we assume that K_0 is cyclic of ℓ-power degree. Let $d = \ell^k = [K_0\colon \mathbb{Q}]$ denote this degree and let m be the conductor of K_0. We exclude the trivial case $K_0 = \mathbb{Q}$, so $k > 0$.

We suppose that ℓ does not ramify in $L_0 = FK_0$. This means that $m = p_1 \dots p_t$ with pairwise distinct primes p_i. Finally, we assume that all $p_1, \dots, p_s$ are split in F, while $p_{s+1}, \dots, p_t$ stay inert, where $1 \leqslant s \leqslant t$. (We repeat that the case of primes ramified in F is excluded for expository reasons.) So we are assuming that at least one prime ramifies in K_0 and splits in F. Then fm is the conductor of L_0 and $\ell \nmid fm$. The reader should note that f has an entirely different meaning compared to §5; the f occurring there will always have the value 1 (i.e., $\mathfrak{P}$ will be of absolute degree 1) in what follows, and therefore will never be needed again.

For each $i \in \{1, \dots, t\}$ let K_i be the unique subfield of the p_i-th cyclotomic field $\mathbb{Q}(\zeta_{p_i})$ such that the ramification index of p_i in K_0 equals $[K_i\colon \mathbb{Q}]$. For every subset $T \subset \{1, \dots, t\}$ let $m_T = \prod_{i \in T} p_i$ and $L_T = FK_T$, where $K_T = \prod_{i \in T} K_i$. Then $K_{\{1,\dots,t\}}$ is the genus field of K_0 and L_0 is a subfield of $L_{\{1,\dots,t\}}$. Let $G_T = \mathrm{Gal}(K_T/\mathbb{Q})$; as before, this will be identified with $\mathrm{Gal}(L_T/F)$. Each group G_T may be canonically identified with the product of the groups $G_{\{i\}} = \mathrm{Gal}(K_i/\mathbb{Q})$ with i running over T; at times it will also be convenient to consider $G_{\{i\}}$ as a subgroup of G_T in the obvious way. Let I_T denote the augmentation ideal of the group ring $\mathbb{Z}_\ell[G_T]$. Finally, the Galois group of L_0/F will be called Γ (not G!); we fix a generator γ of it, and the kernel of the natural epimorphism $G_{\{1,\dots,t\}} \to \Gamma$ will be denoted by Δ.

The following result produces a new annihilator for all $s \geqslant 2$. Let $\widetilde{\Theta}_{L_0} \in \mathbb{Z}_\ell[\Gamma]$ be obtained from the standard Stickelberger element $\Theta_{L_0} \in \mathbb{Z}_\ell[\mathrm{Gal}(L_0/\mathbb{Q})]$ (*cf.* [11], beginning of §6.2) by the condition $(1-\tau)\widetilde{\Theta}_{L_0} = (1-\tau)\Theta_{L_0}$ similarly as in the text preceding Theorem 2.3.

Theorem 6.1. — *There exists $\vartheta_0 \in \mathbb{Z}_\ell[\Gamma]$ with $(\gamma-1)^s\vartheta_0 = \widetilde{\Theta}_{L_0}$, and such that $\vartheta := (\gamma-1)\vartheta_0$ annihilates $A^-_{L_0}$.*
(Since the annihilators of $(\gamma-1)^s$ and $\gamma-1$ on $\mathbb{Z}_\ell[\Gamma]$ coincide, the element ϑ is independent of the choice of ϑ_0.)

Proof. — For now, we only give the proof modulo an intermediate result (Theorem 6.2). Lemma 1.6(a) gives that the natural map $A^-_{\mathbb{Q}(\zeta_{fm})} \to A^-_{L_0}$ is surjective. Therefore every element in $A^-_{L_0}$ is represented by some prime $\mathfrak{p}$ of

L_0 lying under a prime $\mathfrak{P}$ of $\mathbb{Q}(\zeta_{fm})$ *of absolute degree 1*, by Chebotarev's Theorem applied to $\mathbb{Q}(\zeta_{fm})$. Exactly as in §5 we have the element $z_1^{(fm)} \in \mathbb{Q}(\zeta_{fm})$ (obtained from a Gauss sum by a slight modification), where the dependency on $\mathfrak{P}$ is not expressed by the notation. We define more generally

$$x_{T,\mathfrak{P}_T} = \mathrm{N}_{\mathbb{Q}(\zeta_{fm_T})/L_T}(z_1^{(fm_T)}),$$

where $\mathfrak{P}_T$ is the prime of $\mathbb{Q}(\zeta_{fm_T})$ under $\mathfrak{P}$ and again the Gauss sum giving $z_1^{(fm_T)}$ is taken with respect to $\mathfrak{P}_T$. Let $z = \mathrm{N}_{L_{\{1,\dots,t\}}/L_0}(x_{\{1,\dots,t\},\mathfrak{P}})$. Then the classical Stickelberger factorization of Gauss sums gives

$$z\mathcal{O}_{L_0} = \mathfrak{p}^{2fm(1-\tau)\widetilde{\Theta}_{L_0}}.$$

We now state Theorem 6.2 and explain afterwards how it allows to finish the proof of Theorem 6.1:

Theorem 6.2. — *There is an element $y \in \mathbb{Z}_\ell \otimes L_0^*$ such that*

$$y^{(\gamma-1)^s} = z.$$

Let us assume this result and continue in the proof of Theorem 6.1. Theorem 6.2 together with the preceding formula implies directly that $2fm(1-\tau)\widetilde{\Theta}_{L_0}$, and hence also $\widetilde{\Theta}_{L_0}$, are divisible by $(\gamma-1)^s$ in $\mathbb{Z}_\ell[\Gamma]$. Pick $\vartheta_0 \in \mathbb{Z}_\ell[\Gamma]$ with $(\gamma-1)^s\vartheta_0 = \widetilde{\Theta}_{L_0}$. Let J denote the multiplicative group of fractional ideals of L_0, tensored with $\mathbb{Z}_\ell$. Then J is torsion-free, and again the annihilator of $\gamma-1$ is the same as the annihilator of $(\gamma-1)^s$ on J. Therefore the equality

$$y\mathcal{O}_{L_0} = \mathfrak{p}^{2fm(1-\tau)\vartheta_0}$$

holds in J up to a factor which is fixed by γ. If we let $\vartheta = (\gamma-1)\vartheta_0$ and $y_1 = y^{\gamma-1}$, we find that the following equality is valid in J:

$$y_1\mathcal{O}_{L_0} = \mathfrak{p}^{2fm(1-\tau)\vartheta}.$$

Passing to $A_{L_0}^-$, we see that the class represented by $\mathfrak{p}^\vartheta$ is trivial, as had to be shown. □

Theorem 6.2 in its turn follows from a more general result which we are going to formulate now. We will need Gauss sums in various fields. For any $T \subset \{1,\dots,t\}$ we defined the element $x_{T,\mathfrak{P}_T}$ in L_T^*. We recall that $\mathfrak{P}_T$ is the prime of L_T under a chosen degree one prime $\mathfrak{P}$ in the biggest occurring cyclotomic field $\mathbb{Q}(\zeta_{mf})$. Let p be the rational prime below $\mathfrak{P}$ and let E_T and E_0 be the groups of all p-units of L_T and L_0, respectively. So we have $x_{T,\mathfrak{P}_T} \in E_T$. From Corollary 5.3 we deduce, for every $i \in T$, the following formula which is an Euler system relation, up to the extra exponent p_i on the right:

$$\mathrm{N}_{G_i}(x_{T,\mathfrak{P}_T}) = x_{T\setminus i,\mathfrak{P}_{T\setminus i}}^{p_i\cdot(1-\mathrm{Frob}(p_i)^{-1})}.$$

Theorem 6.3. — *For all $T \subset \{1,\ldots,t\}$ the following statement holds:*

$$h(x_{T,\mathfrak{P}_T}) \in I_T^{|T\cap\{1,\ldots,s\}|} \quad \textit{for all } h \in \mathrm{Hom}_{\mathbb{Z}[G_T]}(E_T,\mathbb{Z}_\ell[G_T]).$$

(NB. The latter Hom can be identified with $\mathrm{Hom}_{\mathbb{Z}_\ell[G_T]}(\mathbb{Z}_\ell\otimes E_T,\mathbb{Z}_\ell[G_T])$.)

Proof. — This will be modeled on arguments of Darmon and Hayward. The main trick (the definition of u below) is due to Darmon (Lemma 8.1 in [2]), and Hayward introduced the systematic use of the "linear forms" h (*cf.* Proposition 5.5 in [6]).

We proceed by induction over $|T\cap\{1,\ldots,s\}|$. For empty $T\cap\{1,\ldots,s\}$ there is nothing to prove, so let us assume that we have $T\subset\{1,\ldots,t\}$ such that $T_1 = T\cap\{1,\ldots,s\}$ is not empty and that the theorem has been proved for all subsets $T'\subset T$ with $|T'\cap\{1,\ldots,s\}| < |T_1|$.

We need a little notation: For any $\sigma\in G_T$, denote by $\sigma_i\in G_i$ ($i\in T$) the elements which are uniquely determined by $\sigma=\prod_{i\in T}\sigma_i$. We express h via coefficients: $h(x)=\sum_{\sigma\in G_T}h_\sigma(x)\sigma$ with $h_\sigma\in\mathrm{Hom}_{\mathbb{Z}}(E_T,\mathbb{Z}_\ell)$. Notice that $h_\sigma(x^\rho)=h_{\rho^{-1}\sigma}(x)$ for any $\rho\in G_T$. We let

$$u=\sum_{\sigma\in G_T}h_\sigma(x_{T,\mathfrak{P}_T})\Big(\prod_{i\in T\setminus T_1}\sigma_i\Big)\prod_{i\in T_1}(\sigma_i-1).$$

Multiplying out the rightmost product into a sum of $2^{|T_1|}$ terms in the obvious way, we obtain

$$u=\sum_{\substack{T'\subset T\\ T\setminus T_1\subset T'}}(-1)^{|T|-|T'|}u_{T'},$$

with

$$u_{T'} := \sum_{\sigma\in G_T}h_\sigma(x_{T,\mathfrak{P}_T})\,\mathrm{pr}_{T'}(\sigma)=\mathrm{pr}_{T'}\big(h(x_{T,\mathfrak{P}_T})\big).$$

Here we have written $\mathrm{pr}_{T'}\colon\mathbb{Z}_\ell[G_T]\to\mathbb{Z}_\ell[G_T]$ for the linear mapping induced by the obvious projection $G_T\to G_{T'}$ followed by the obvious injection $G_{T'}\subset G_T$. We now define a new linear form

$$h'\in\mathrm{Hom}_{\mathbb{Z}[G_{T'}]}(E_{T'},\mathbb{Z}_\ell[G_{T'}]),\quad h'(x):=\sum_{\sigma'\in G_{T'}}h_{\sigma'}(x)\sigma'.$$

Then (letting $T'' = T \setminus T'$) we find

$$\begin{aligned}\mathrm{pr}_{T'}(h(x)) &= \sum_{\sigma' \in G_{T'}} \sum_{\sigma'' \in G_{T''}} h_{\sigma'\sigma''}(x)\sigma' \\ &= \sum_{\sigma' \in G_{T'}} \sum_{\sigma'' \in G_{T''}} h_{\sigma'}(x^{\sigma''^{-1}})\sigma' \\ &= h'\big(\mathrm{N}_{L_T/L_{T'}}(x)\big).\end{aligned}$$

Moreover the Euler condition implies that $\mathrm{N}_{L_T/L_{T'}}(x_{T,\mathfrak{P}_T}) = x^{\beta}_{T',\mathfrak{P}_{T'}}$ with some $\beta \in I_T^{|T|-|T'|}$, because p_i splits in F for each $i \in T \setminus T'$. For each proper subset T' of T, our induction hypothesis therefore implies that

$$u_{T'} = \mathrm{pr}_{T'}(h(x_{T,\mathfrak{P}_T})) = h'(\mathrm{N}_{L_T/L_{T'}}(x_{T,\mathfrak{P}_T})) = \beta h'(x_{T',\mathfrak{P}_{T'}})$$

lies in $I_T^{|T_1|}$. Since the term u visibly lies in $I_T^{|T_1|}$, we infer that $u_T \in I_T^{|T_1|}$, and u_T happens to coincide with the desired value $h(x_{T,\mathfrak{P}_T})$ itself. □

Comment. — Contrary to what Hayward is able to do in [6], it does not seem to be clear in our context how to prove a "leading term statement" – we just get a containment relation for now. However we hope to come back to "leading terms", that is, to a congruence modulo the next higher power of the augmentation ideal, in a future paper.

Lemma 6.4. — *Let G be an ℓ-group and let M be a finitely generated $\mathbb{Z}_\ell[G]$-module. If N is a submodule of M such that M/N is non-zero and without $\mathbb{Z}$-torsion, then any $\mathbb{Z}_\ell[G]$-homomorphism from N to $\mathbb{Z}_\ell[G]$ can be homomorphically extended to M.*

Proof. — Since both $\mathbb{Z}_\ell[G]$ and M/N are non-zero and without $\mathbb{Z}$-torsion they are of grade one, because one can take $\{\ell\}$ as a maximal $\mathbb{Z}_\ell[G]$-sequence on both $\mathbb{Z}_\ell[G]$ and M/N. As G is an ℓ-group, $\mathbb{Z}_\ell[G]$ is a local Gorenstein ring. Therefore Theorem 217 in [7] gives

$$\mathrm{Ext}^1_{\mathbb{Z}_\ell[G]}(M/N, \mathbb{Z}_\ell[G]) = 0,$$

and the lemma follows. □

It remains to prove Theorem 6.2 using Theorem 6.3. This is quite similar to the proof of Theorem 4.2 in [5], using the same kind of algebra, with one little twist.

First step: For all $\mathbb{Z}_\ell[\Gamma]$-homomorphisms $\phi\colon \mathbb{Z}_\ell \otimes E_0 \to \mathbb{Z}_\ell[\Gamma]$ we have $\phi(z) \in (\gamma-1)^s\mathbb{Z}_\ell[\Gamma]$. (Recall that $z \in E_0$ was a norm of a slightly modified particular Gauss sum.)

Let $T = \{1, \dots, t\}$. The corestriction map $\mathbb{Z}_\ell[\Gamma] \to \mathbb{Z}_\ell[G_T]$ gives an isomorphism $\nu\colon \mathbb{Z}_\ell[\Gamma] \to \mathrm{N}_\Delta\, \mathbb{Z}_\ell[G_T]$. Let ϕ be as in the statement of Step 1.

Lemma 6.4 for the submodule $\mathbb{Z}_\ell \otimes E_0$ of $\mathbb{Z}_\ell \otimes E_T$ gives that $\nu\phi$ extends to a $\mathbb{Z}_\ell[G_T]$-homomorphism $h\colon \mathbb{Z}_\ell \otimes E_T \to \mathbb{Z}_\ell[G_T]$. Then $\nu\phi(z) = h(\mathrm{N}_{L_T/L_0}\, x_{T,\mathfrak{P}}) = \mathrm{N}_\Delta \cdot h(x_{T,\mathfrak{P}})$ (the first equality by definition of z), and by Theorem 6.3, $h(x_{T,\mathfrak{P}}) \in I_T^s$. Thus $\nu\phi(z) \in \mathrm{N}_\Delta \cdot I_T^s = \nu((\gamma{-}1)^s\mathbb{Z}_\ell[\Gamma])$. Since ν is an isomorphism, we infer $\phi(z) \in (\gamma{-}1)^s\mathbb{Z}_\ell[\Gamma]$.

Second step: Let $U \subset \mathbb{Z}_\ell \otimes E_0$ be the kernel of multiplication with the norm element N_Γ. Then $z \in (\gamma{-}1)^{s-1}U$.

By Corollary 3.3 in [5] (the ring $\mathbb{Z}_\ell[\Gamma]/(\mathrm{N}_\Gamma)$ is written R there) it is enough to show that for all $\phi \in \mathrm{Hom}_{\mathbb{Z}_\ell[\Gamma]/(\mathrm{N}_\Gamma)}(U, \mathbb{Z}_\ell[\Gamma]/(\mathrm{N}_\Gamma))$ we have $\phi(z) \in (\gamma{-}1)^{s-1}\mathbb{Z}_\ell[\Gamma]/(\mathrm{N}_\Gamma)$. Multiplication by $\gamma{-}1$ defines an isomorphism $\iota\colon \mathbb{Z}_\ell[\Gamma]/(\mathrm{N}_\Gamma) \to (\gamma{-}1)\mathbb{Z}_\ell[\Gamma]$, and $\gamma{-}1$ is a nonzerodivisor on these two modules. So we need to show that for all $\phi \in \mathrm{Hom}_{\mathbb{Z}_\ell[\Gamma]}(U, (\gamma{-}1)\mathbb{Z}_\ell[\Gamma])$ we have $\phi(z) \in (\gamma{-}1)^s\mathbb{Z}_\ell[\Gamma]$. It is easy to see that $\mathrm{Hom}_{\mathbb{Z}_\ell[\Gamma]}(U, (\gamma{-}1)\mathbb{Z}_\ell[\Gamma]) = \mathrm{Hom}_{\mathbb{Z}_\ell[\Gamma]}(U, \mathbb{Z}_\ell[\Gamma])$, and Lemma 6.4 applied to the $\mathbb{Z}_\ell[\Gamma]$-modules $U \subset \mathbb{Z}_\ell \otimes E_0$ gives that each such ϕ can be extended to $\overline{\phi} \in \mathrm{Hom}_{\mathbb{Z}_\ell[\Gamma]}(\mathbb{Z}_\ell \otimes E_0, \mathbb{Z}_\ell[\Gamma])$. The first step gives $\phi(z) = \overline{\phi}(z) \in (\gamma{-}1)^s\mathbb{Z}_\ell[\Gamma]$ which we wanted to show.

Third and last step: From Hilbert 90 one easily obtains that $U \subset (\gamma{-}1)(\mathbb{Z}_\ell \otimes L_0^*)$. Putting this together with the result of the second step we obtain at once

$$z \in (\gamma{-}1)^s(\mathbb{Z}_\ell \otimes L_0^*),$$

and this proves Theorem 6.2.

We have two comments concerning Theorem 6.1.

(1) It is not difficult to show that there is some power ℓ^e such that $\ell^e\vartheta$ is in the $\mathbb{Z}[\Gamma]$-span of $\widetilde{\Theta}_{L_0}$. (Actually $\ell^e = d^{s-1}$ is enough.) This implies that $w_F\vartheta$ is in $\mathbb{Z}[\Gamma]$, and that $(1-\tau)w_F\vartheta$ annihilates the whole class group and not just the minus part of the ℓ-part of it (as usual, w_F denotes the number of roots of unity in F).

(2) If $s \geqslant 2$, then $(1-\tau)\vartheta$ is not in the ℓ-completion of the Stickelberger ideal S_{L_0} attached to L_0 in the sense of Sinnott. This can be seen as follows: S_{L_0} is generated by $(1{-}\tau)\widetilde{\Theta}_{L_0}$ and other terms coming from proper subfields; those other terms are all divisible by N_{Γ_0} where Γ_0 is the minimal nontrivial subgroup of Γ. The ring $R = \mathbb{Z}_\ell[\Gamma]/(\mathrm{N}_{\Gamma_0})$ is then a DVR; the image of ϑ in R cannot be a multiple of the image of $\widetilde{\Theta}_{L_0}$ because the image of $\gamma{-}1$ in R is not invertible, and the other generators of S_{L_0} go to zero in R.

To conclude the paper we show how to find still more annihilators. Let us consider all subfields

$$\mathbb{Q} = K_0^{(0)} \subset K_0^{(1)} \subset K_0^{(2)} \subset \cdots \subset K_0^{(k)} = K_0$$

with $[K_0^{(i)} \colon \mathbb{Q}] = \ell^i$. For each $0 \leqslant i \leqslant k$, let

$$L_0^{(i)} = FK_0^{(i)}, \qquad \varkappa_i = \operatorname{cor}_{L_0/L_0^{(i)}} \widetilde{\Theta}_{L_0^{(i)}} \in \mathbb{Z}_\ell[\Gamma],$$

and let s_i be the number of ramified primes in $K_0^{(i)}$ that split in F. If $s_i > 0$ then we define $\theta_i = \operatorname{cor}_{L_0/L_0^{(i)}} \vartheta_{L_0^{(i)}}$, where $\vartheta_{L_0^{(i)}}$ means the ϑ of Theorem 6.1 for the field $L_0^{(i)}$ instead of L_0. Theorem 6.1 gives $\widetilde{\Theta}_{L_0^{(i)}} = (\gamma{-}1)^{s_i-1}\vartheta_{L_0^{(i)}}$, so we have $\varkappa_i = (\gamma{-}1)^{s_i-1}\theta_i$. In the case $s_i = 0$ we put $\theta_i = \varkappa_i$. Let S be Sinnott's Stickelberger ideal of L_0. Then $(1-\tau)S \otimes \mathbb{Z}_\ell$ is equal to $(1-\tau)$ times the ideal $(\varkappa_0, \ldots, \varkappa_k) \subset \mathbb{Z}_\ell[\Gamma]$. But we can also consider the ideal $(\theta_0, \ldots, \theta_k)$, and Theorem 6.1 together with Lemma 1.6(c) gives that $(\theta_0, \ldots, \theta_k)$ annihilates $A_{L_0}^-$. We can even compute the relative index of these ideals:

Theorem 6.5. — *Let r be the smallest positive integer that $s_r > 0$. Then the relative index*

$$[(\theta_0, \ldots, \theta_k) \colon (\varkappa_0, \ldots, \varkappa_k)] = \prod_{i=r}^{k} \ell^{s_i-1},$$

which can be characterized as the product of the ramification degrees of all primes that ramify in K_0 and split in F divided by the largest of these ramification degrees. Moreover this index divides the relative class number $h_{L_0}^-$ of L_0.

Remark. — If there is no ramifying prime in K_0 that is inert in F then the product in Theorem 6.5 is equal to the degree $[\overline{K_0} \colon K_0]$, where $\overline{K_0}$ is the genus field of K_0.

Proof. — It is easy to see that s_i is the number of all primes that split in F and have ramification index in K_0 at least ℓ^{k-i+1}. So if such a prime has ramification index ℓ^a then it contributes the amount 1 to s_{k-a+1}, s_{k-a+2}, $\ldots$, s_k, and so $\prod_{i=r}^{k} \ell^{s_i}$ equals the product of the ramification degrees of all such primes, while ℓ^{k-r+1} is the largest of these ramification degrees. The divisibility relation for the relative class number follows from the Sinnott formula (see [10], Theorems 2.1 and 5.3) which implies that $[\mathbb{Z}_\ell[\Gamma] \colon (\varkappa_0, \ldots, \varkappa_k)]$ equals the ℓ-part of $h_{L_0}^-$. Therefore the theorem will be proved if we show by induction with respect to $j = 0, 1, \ldots, k$ that

$$[(\theta_0, \ldots, \theta_j) \colon (\varkappa_0, \ldots, \varkappa_j)] = \prod_{i=r}^{j} \ell^{s_i-1}.$$

If $j < r$ then $\theta_j = \varkappa_j$. So let us assume that $j \geqslant r$ and that the statement has been proved for $j-1$. The well-known distribution relations give that

$$(1-\tau)\,\mathrm{N}_j\,\varkappa_j = (1-\tau)\varkappa_{j-1}\prod_p (1-\mathrm{Frob}(p)^{-1}),$$

where $\mathrm{N}_j = \sum_{i=0}^{\ell-1}\gamma^{i\ell^{j-1}}$ is the norm operator from $L_0^{(j)}$ to $L_0^{(j-1)}$ and where the product is taken over all primes q that ramify in $L_0^{(j)}$ but do not ramify in $L_0^{(j-1)}$; here $\mathrm{Frob}(q)$ is an extension of the Frobenius automorphism for q on $L_0^{(j-1)}$ to L_0. If the prime q is inert in F then $\tau\,\mathrm{Frob}(q) \in \Gamma$ and so $1-\mathrm{Frob}(q)^{-1}$ acts on $(1-\tau)\varkappa_{j-1}$ as $1+\tau\,\mathrm{Frob}(q)^{-1}$ which is a unit in $\mathbb{Z}_\ell[\Gamma]$. But if the prime q splits in F (and we have exactly $s_j - s_{j-1}$ such primes) then $\mathrm{Frob}(q) \in \Gamma$ and so $1-\mathrm{Frob}(q)^{-1}$ is divisible by $1-\gamma$ in $\mathbb{Z}_\ell[\Gamma]$ (and belongs to the unique maximal ideal of $\mathbb{Z}_\ell[\Gamma]$). Therefore there is $\delta_j \in \mathbb{Z}_\ell[\Gamma]$ such that

$$\mathrm{N}_j\,\varkappa_j = (1-\gamma)^{s_j-s_{j-1}}\delta_j\varkappa_{j-1}.$$

We are assuming that $s_j > 0$ and so $\varkappa_j = (\gamma-1)^{s_j-1}\theta_j$. On one hand, if $s_{j-1} = 0$ then $\varkappa_{j-1} = \theta_{j-1}$ and so

$$\mathrm{N}_j(\gamma-1)^{s_j-1}\theta_j = (1-\gamma)^{s_j}\delta_j\theta_{j-1},$$

and since θ_j is in the augmentation kernel (see Theorem 6.1) we have

$$\mathrm{N}_j\,\theta_j = (1-\gamma)\delta_j\theta_{j-1}.$$

On the other hand if $s_{j-1} > 0$ then we have $\varkappa_{j-1} = (\gamma-1)^{s_{j-1}-1}\theta_{j-1}$ and so

$$\mathrm{N}_j(\gamma-1)^{s_j-1}\theta_j = (1-\gamma)^{s_j-1}\delta_j\theta_{j-1}$$

and since both θ_j and θ_{j-1} are in the augmentation kernel we have

$$\mathrm{N}_j\,\theta_j = \delta_j\theta_{j-1}.$$

The rest of the argument proceeds by induction over j quite similarly as in [5]. □

Acknowledgments. — We thank the referee for his thorough reading of the paper and his very apposite remarks. The first author was supported by a DFG grant (Sachbeihilfe). The second author was supported under Project Nr. 201/04/0381 of the Grant Agency of the Czech Republic and under the project MSM0021622409 of the Ministry of Education of the Czech Republic.

BIBLIOGRAPHY

[1] P. Cornacchia & C. Greither, "Fitting ideals of class groups of real fields with prime power conductor", *J. Number Theory* **73** (1998), no. 2, p. 459-471.

[2] H. Darmon, "Thaine's method for circular units and a conjecture of Gross", *Canad. J. Math.* **47** (1995), no. 2, p. 302-317.

[3] C. Greither, "Über relativ-invariante Kreiseinheiten und Stickelberger-Elemente", *Manuscripta Math.* **80** (1993), no. 1, p. 27-43.

[4] C. Greither, "Some cases of Brumer's conjecture for abelian CM extensions of totally real fields", *Math. Z.* **233** (2000), no. 3, p. 515-534.

[5] C. Greither & R. Kučera, "Annihilators for the class group of a cyclic field of prime power degree. II", *Canad. J. Math* **58** (2006), no. 3, p. 580-599.

[6] A. Hayward, "A class number formula for higher derivatives of abelian L-functions", *Compos. Math.* **140** (2004), no. 1, p. 99-129.

[7] I. Kaplansky, *Commutative rings*, Polygonal Publishing House, Washington, NJ, 1994.

[8] M. Kurihara, "Iwasawa theory and Fitting ideals", *J. Reine Angew. Math.* **561** (2003), p. 39-86.

[9] S. Lang, *Cyclotomic fields I and II*, second ed., Graduate Texts in Mathematics, vol. 121, Springer-Verlag, New York, 1990.

[10] W. Sinnott, "On the Stickelberger ideal and the circular units of an abelian field", *Invent. Math.* **62** (1980/81), no. 2, p. 181-234.

[11] L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1982.

Manuscrit reçu le 28 novembre 2005,
révisé le 30 mai 2006,
accepté le 6 juillet 2006.

Cornelius GREITHER
Universität der Bundeswehr München
Fakultät für Informatik
Institut für theoretische Informatik und Mathematik
85577 Neubiberg (Germany)
cornelius.greither@unibw.de

Radan KUČERA
Masarykova univerzita
Přírodovědecká fakulta
Janáčkovo nám. 2a
602 00 Brno (Czech Republic)
kucera@math.muni.cz