Séminaire de Théorie des Nombres
Paris 1988–89

The structure of the minus class groups of abelian number fields

René SCHOOF*

Abstract. It is shown that sometimes one can read off the structure of the minus class groups of abelian number fields from certain Stickelberger elements; the question is raised whether one can always determine the structure of these class groups from Stickelberger elements. Some numerical and theoretical evidence for an affirmative answer is presented.

1. — Introduction

Ideal class groups of cyclotomic or abelian number fields have been a subject of study for a long time [5,14]. The problem naturally falls apart in two. The class groups of real abelian number field are still relatively poorly understood. But about the other parts, the minus parts of the class groups of imaginary abelian number fields, much more is known. For an imaginary abelian number field K the minus class group $C\ell_K^-$ of K is defined to be $C\ell_K/\mathrm{im}(C\ell_{K^+})$ where K^+ is the maximal real subfield of K. The analytic class number formula gives an expression for the cardinality of $C\ell_K^-$ in terms of certain generalized Bernoulli numbers which are defined in terms of the Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}^{\mathrm{ab}}/\mathbf{Q})$. This formula is quite practical and can be used to compute the cardinalities of minus class groups of abelian fields of small conductor, see [7,12,16]. More precise results were recently obtained by B. Mazur and A. Wiles [9]. They took the action of the Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ into account. They obtained formulas for the cardinalities of certain eigenspaces for this action. Apart from their results there does not appear to be a general way to describe the structure of the minus class groups as abelian groups in similar terms. For instance, in the case of a complex quadratic field K, there does not seem to be a way to tell, in terms of

generalized Bernoulli numbers or Stickelberger elements what the structure of $C\ell_K$ as an abelian group is.

In this paper we will discuss a way that might possibly lead to a procedure to describe the structure of minus class groups of abelian number fields in terms of Stickelberger elements. In the case of a complex quadratic field and an odd prime p this leads to a necessary and sufficient criterion for the p-part of the class group to be a cyclic group [8]. This criterion is elementary and solely in terms of $\mathrm{Gal}(\overline{\mathbb{Q}}^{\mathrm{ab}}/\mathbb{Q})$. While for quadratic fields there are definitely more practical ways to compute the structure of the class group, it seems that for abelian fields of high degree our method is quite practical.

Section 2 contains a preliminary discussion of Fitting ideals. In section 3 we introduce our "Stickelberger ideal" and we pose the question whether it is equal to a certain "Fitting ideal". An affirmative answer to this question would imply that one can completely describe the structure of the odd parts of the minus class groups of abelian number fields in terms of Stickelberger elements. One might even hope that this, in combination with an effective Čebotarev Density Theorem, leads to an efficient way to determine this structure. Finally, in section 4 we present some numerical examples indicating that the answer to our question is affirmative. Another indication in this direction is the result mentioned above, joint with Hendrik Lenstra, on quadratic fields. The details of the proof will be published elsewhere.

I would like to thank Serge Lang for stimulating discussions concerning this work and the Department of Mathematics of the University of California at Berkeley, where part of this research was done, for its hospitality.

After this paper was written I became aware of Kolyvagin's results [4,11] on p-class groups of $\mathbb{Q}(\zeta_p)$. He gives a new proof of the theorem of Mazur and Wiles and he gives in addition a description of the Galois module structure of these groups in terms of certain higher "Stickelberger elements". His results can easily be generalized to abelian fields F for which p does not divide $[F:\mathbb{Q}]$. His paper does, however, not seem to contain an explicit answer to questions (3.2) and (3.2)'.

2. — Fitting ideals

For the definition and the basic properties of the R-Fitting ideals of finitely generated R-modules A we refer to the books by Lang and Northcott [5,10] and the appendix to the paper by Mazur and Wiles [9].

We let R denote a discrete valuation ring with uniformizing element π. Any finitely generated R-module is a finite product of copies of R and modules of the form $R/(\pi^n)$. The R-Fitting ideal $\mathrm{Fit}_R(A)$ of an R-module A measures the "size" of A : if A admits R as a direct summand then $\mathrm{Fit}_R(A) = 0$ and when $A \cong \oplus_{i=1}^d R/(\pi^{n_i})$ then $\mathrm{Fit}_R(A) = (\pi^m)$ where $m = \sum_{i=1}^d n_i$. The R-Fitting ideal does, in general, not reveal the entire R-structure of the module. One has, for instance, that $\mathrm{Fit}_R(R/(\pi^2)) = \mathrm{Fit}_R(R/(\pi) \times R/(\pi)) = (\pi^2)$. We can, however, recover the R-isomorphism class of a finitely generated R-module A from the Fitting ideal of A with respect to a larger ring as follows. We let $\Lambda = R[[T]]$ denote the ring of power series with coefficients in R. We turn every R-module into a Λ-module by letting T act as zero on A.

PROPOSITION 2.1. — *Let λ and $n_1 \le n_2 \le n_3 \le \ldots$ denote non-negative integers. For the R-module*

$$A = R^\lambda \oplus \bigoplus_{i=1}^{d} R/(\pi^{n_i})$$

one has that

$$\mathrm{Fit}_\Lambda(A) = \{\sum_{i=0}^{\infty} a_i T^i \in \Lambda : a_i = 0 \text{ for } 0 \le i < \lambda$$

and

$$a_i \equiv 0 \pmod{\pi^{\sum_{j=i-\lambda}^{d} n_j}} \text{ for } \lambda \le i \le \lambda + d\}.$$

Proof : From [5, Ch. XIII,Cor.10.6] we see that $\mathrm{Fit}_\Lambda(R) = (T)$ and that $\mathrm{Fit}_\Lambda(R/(\pi^n)) = (T, \pi^n)$. Since moreover [5,Ch.XIII,Prop.10.8] one has that $\mathrm{Fit}_\Lambda(A \oplus B) = \mathrm{Fit}_\Lambda(A)\mathrm{Fit}_\Lambda(B)$ we conclude that

$$\mathrm{Fit}_\Lambda(A) = (T^\lambda) \prod_{i=1}^{d} (T, \pi^{n_i}).$$

It is easy to see that this ideal is actually equal to the ideal in the statement of the proposition. This proves Prop.(3.1).

It follows at once that one can read off the invariants λ and $n_1, n_2, \ldots$ from the Λ-Fitting ideal of $A = R^\lambda \oplus \oplus_{i=1}^d R/(\pi^{n_i})$. We conclude that the R-isomorphism class of any finitely generated R-module A can be recovered from its Λ-Fitting ideal. For instance one has that A is cyclic over R if and only if $T \in \mathrm{Fit}_\Lambda(A)$. More generally the number of R-generators of A is at least d if and only if $\mathrm{Fit}_\Lambda(A) \subset (T, \pi)^d$. It is easy to see that the R-ideal generated by the coefficients of T^k of the $f(T) \in \mathrm{Fit}_\Lambda(A)$ is precisely the k-th Fitting ideal of A as defined in [10].

3. — Minus class groups

In this section we will discuss minus class groups of imaginary abelian number fields. We will study one p-part at the time. Let us therefore fix a prime p which we will suppose to be odd. Let F be a finite abelian extension of $\mathbf{Q}$ of degree prime to p. The Galois group $\mathrm{Gal}(F/\mathbf{Q})$ acts on the class group $C\ell_F$ and in this way its p-part $C\ell_{F,p}$ becomes a module over the ring $\mathbf{Z}_p[\Delta]$. Since p does not divide $\#\Delta$, the group ring $\mathbf{Z}_p[\Delta]$ decomposes as a product of discrete valuation rings. We have

$$\mathbf{Z}_p[\Delta] \cong \bigoplus_\chi R_\chi$$

where the product runs over the characters $\chi : \Delta \longrightarrow \overline{\mathbf{Q}}_p^*$ upto $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-conjugacy. By R_χ we denote the ring $\mathbf{Z}_p[\mathrm{im}\,\chi]$ which is a finite extension of $\mathbf{Z}_p$; it is a $\mathbf{Z}_p[\Delta]$-module via $\delta \cdot x = \chi(\delta)x$ for $\delta \in \Delta$ and $x \in R_\chi$. The above isomorphism of rings is given by $\delta \longmapsto (\chi(\delta))_\chi$. Accordingly the p-class group of F is decomposed as a direct sum

$$C\ell_{F,p} \cong \bigoplus_\chi C\ell_{F,p}(\chi)$$

where $C\ell_{F,p}(\chi)$ denotes $C\ell_{F,p} \otimes_{\mathbf{Z}_p[\Delta]} R_\chi$. When F is an imaginary field, the characters of Δ come in two types : they are even or odd according as χ assumes the value 1 or -1 on complex conjugation. The sum over the even characters χ of the groups $C\ell_{F,p}(\chi)$ is just $C\ell_{F^+,p}$ where F^+ denotes the maximal real subfield of F. The sum over the odd characters is the p-part of the minus class group of F.

A standard argument shows that the R_χ-module $C\ell_{F,p}(\chi)$ does not depend on F. We will therefore just write $C\ell(\chi)$ for $C\ell_{F,p}(\chi)$. When χ is even, very little can be said about $C\ell(\chi)$ in general. For odd χ there is a beautiful explicit formula for the cardinality of $C\ell(\chi)$:

THEOREM 3.1 (Mazur and Wiles). — *Let p be an odd prime and let $\chi : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \overline{\mathbf{Q}}_p^*$ be an odd character of conductor f not equal to the Teichmüller character ω. One has*

$$\#C\ell(\chi) = \#R_\chi/(B_{1,\chi^{-1}})$$

where $B_{1,\chi^{-1}}$ denotes a generalized Bernoulli number

$$B_{1,\chi^{-1}} = \sum_{x=1}^{f} \frac{x}{f}\chi^{-1}(x) \in R_\chi.$$

Proof : This is Theorem 2 of the introduction of [9].

We view χ as a function on $\mathbf{Z}/f\mathbf{Z}$ in the usual way : first we identify $\mathrm{Gal}(\mathbf{Q}(\zeta_f)/\mathbf{Q})$ with $(\mathbf{Z}/f\mathbf{Z})^*$ using the action on the f-th roots of unity; the character on $(\mathbf{Z}/f\mathbf{Z})^*$ is then extended by 0 to all of $\mathbf{Z}/f\mathbf{Z}$. The Teichmüller character $\omega : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{Z}_p^*$ is given by the action of the Galois group on the p-th roots of unity μ_p. It is determined by

$$\sigma(\zeta) = \zeta^{\omega(\sigma)} \qquad \text{for } \sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \text{ and } \zeta \in \mu_p.$$

It is well known that $C\ell(\omega) = 0$.

The result of Mazur and Wiles does not, however, give any information on the isomorphism class of $C\ell(\chi)$ as an R_χ-module. In the remainder of this section we will explain how one may get information on the R_χ-structure of $C\ell(\chi)$. We recall that we have fixed an odd prime p and from now on we also fix an odd character $\chi : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longmapsto \overline{\mathbf{Q}}_p^*$ not equal to ω. Its conductor will be denoted by f_χ.

Let F denote the fixed field of $\ker(\chi)$ and let Δ denote the Galois group $\mathrm{Gal}(F/\mathbf{Q})$. For every prime ℓ which does not divide f_χ we consider the extension $F(\zeta_\ell)$ of F. We write G for $\mathrm{Gal}(F(\zeta_\ell)/F)$. Clearly $G \cong \mathrm{Gal}(\mathbf{Q}(\zeta_\ell)/\mathbf{Q})$ is a cyclic group of order $\ell - 1$. The p-part M of the class group of $F(\zeta_\ell)$ is a module over

the group ring $\mathbf{Z}_p[\Delta \otimes G]$. Its χ-part $M(\chi) = M \times_{\mathbf{Z}_p[\Delta]} R_\chi$ is therefore a module over the ring $R_\chi[G]$. The ring $R_\chi[G]$ is isomorphic to $R_\chi[[T]]/((1+T)^{\ell-1}-1)$ by letting $T+1$ correspond to a generator of the cyclic group G. We see that $M(\chi)$ becomes in this way a Λ-module, the ring $\Lambda = R_\chi[[T]]$ acting via its quotient.

Let us note that $M(\chi)$ is precisely the χ-component of the p-class group of F' where F' is the subextension of $F(\zeta_p)$ of maximal p-power degree over F. In the above discussion one could therefore replace $F(\zeta_p)$ by F' and the Galois group G by its p-part. As a result the ring $R_\chi[G]$ would be a local ring. We will choose this approach in section 4.

Since the extension $F(\zeta_\ell)$ is totally ramified over F, the norm map $M(\chi) \longrightarrow C\ell(\chi)$ is a surjective Λ-morphism. It follows, more or less from the definition of Fitting ideals, that

$$\mathrm{Fit}_\Lambda M(\chi) \subset \mathrm{Fit}_\Lambda C\ell(\chi).$$

Since χ is not the Teichmüller character ω the Stickelberger elements

$$\sum_{x \in (\mathbf{Z}/\ell f\mathbf{Z})^*} \langle \frac{x}{\ell f} \rangle \chi^{-1}(x)[\sigma_x]^{-1}$$

are integral i.e. they are in the ring $R_\chi[G]$. Here σ_x is determined by $\sigma_x(\zeta) = \zeta^x$ for $\zeta \in \mu_\ell$; by $[\sigma_x]$ we denote the corresponding element in the group ring $R_\chi[G]$. For $\alpha \in \mathbf{R}$ we denote by $\langle \alpha \rangle$ the fractional part of α; it is determined by $\alpha \equiv \langle \alpha \rangle \pmod{\mathbf{Z}}$ and $0 \leq \langle \alpha \rangle < 1$. In terms of the isomorphism of rings above we see that the Stickelberger elements are precisely

$$\phi_{\chi,\ell}(T) = \sum_{x \in (\mathbf{Z}/\ell f\mathbf{Z})^*} \langle \frac{x}{\ell f} \rangle \chi^{-1}(x)(1+T)^{-\mathrm{ind}_\ell(x)} \in \Lambda/((1+T)^{\ell-1}-1)$$

where $\mathrm{ind}_\ell(x)$ denotes the index of x with respect to a primitive root mod ℓ : one has $x = g^{\mathrm{ind}_\ell(x)}$ for $x \in (\mathbf{Z}/\ell\mathbf{Z})^*$.

It follows or should follow from the work of Mazur and Wiles that the Stickelberger elements are in the $\Lambda/((1+T)^{\ell-1}-1)$-Fitting ideal of $M(\chi)$. Therefore, by a standard property of Fitting ideals [10,appendix form.4]

$$\phi_{\chi,\ell}(T) \in \mathrm{Fit}_\Lambda M(\chi) \subset \mathrm{Fit}_\Lambda C\ell(\chi) \pmod{(1+T)^{\ell-1}-1}.$$

In this way one constructs for each prime ℓ and each isomorphism $R_\chi[G] \cong \Lambda/((1+T)^{\ell-1}-1)$ a power series in the ideal $\mathrm{Fit}_\Lambda C\ell(\chi) + ((1+T)^{\ell-1}-1)\Lambda$. For

each integer $n \geq 1$ we define $I_\chi^{(n)}$ to be the ideal generated in $\Lambda/((1+T)^{p^n}-1)$ by the images of the Stickelberger elements $\phi_{\chi,\ell}(T)$ for *all* primes $\ell \equiv 1 \pmod{p^n}$ and *all* possible identifications of the rings $R_\chi[G/G^{p^n}]$ and $\Lambda/((1+T)^{p^n}-1)$:

$$I^{(n)}(\chi) = \langle \phi_{\chi,\ell}(T) : \ell \equiv 1 \pmod{p^n} \rangle.$$

Finally we define the Λ-ideal $I(\chi)$:

$$I(\chi) = \bigcap_{n \geq 1} (I^{(n)}(\chi) + ((1+T)^{p^n}-1)\Lambda).$$

As we already remarked the "Stickelberger ideal" $I(\chi)$ is contained in the "Fitting ideal" $\mathrm{Fit}_\Lambda C\ell(\chi)$. Numerical experiments suggest that, given $C\ell(\chi)$, the only restriction on the $R_\chi[G]$-structure of the modules $M(\chi)$ is the fact that the norm map $M(\chi) \longrightarrow C\ell(\chi)$ is surjective and that the G-cohomology of $M(\chi)$ is as described in Lemma(4.1) below. One would therefore, apart from these restrictions, expect "random" behavior of the $R_\chi[G]$-isomorphism classes of $M(\chi)$ and of the Stickelberger elements. So one is tempted to ask the following question :

Question 3.2. — *Is $I(\chi) = \mathrm{Fit}_\Lambda C\ell(\chi)$ for characters χ which are not powers of the Teichmüller character?*

When χ is a power of ω the answer to the question would be negative because $I(\chi) \subset (T)$ while $\mathrm{Fit}_\Lambda(C\ell(\chi)) \not\subset (T)$. In this case we have a modified question :

Question 3.2. — *When $i \neq 1$ is $I(\omega^i) = \mathrm{Fit}_\Lambda C\ell(\omega^i) \cap (T)$?*

An affirmative answer to Questions(3.2) and (3.2)' would enable one to recover the structure of the class groups $C\ell(\chi)$ from certain Stickelberger elements. For χ not equal to a power of the Teichmüller character this is clear from Prop.(2.1). For powers of ω one can recover the isomorphism class of the p-group $C\ell(\omega^i)$ from the ideal $\mathrm{Fit}_\Lambda C\ell(\omega^i) \bigcap (T)$ and the class number $\#C\ell(\omega^i)$. We recall that $C\ell(\omega) = 0$.

We have some results that suggest that perhaps the answer to the questions is always "yes". In the next section we will present some numerical examples and some theoretical evidence.

4. — Examples

We recall that p denotes an odd prime, χ an odd p-adic character of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ and ℓ a prime which we suppose to be $1 \pmod p$. We let F denote the fixed field of $\ker(\chi)$ and K the maximal p-power degree extension of F inside $F(\zeta_\ell)$. The χ-part of the p-part of the class group of K is denoted by $M(\chi)$. It is isomorphic to the χ-part of the p-part of the class group of $F(\zeta_p)$ as we observed earlier. We let $G = \mathrm{Gal}(K/F)$ and $\Delta = \mathrm{Gal}(F/\mathbf{Q})$. Clearly the Galois group of K over $\mathbf{Q}$ is isomorphic to the direct product $G \times \Delta$. One can view χ as a character of Δ. The $\mathbf{Z}_p[\Delta]$-algebra $\mathbf{Z}_p[\mathrm{im}\,\chi]$ will be denoted by R_χ and the powerseries ring $R_\chi[[T]]$ will be denoted by Λ.

For the basic facts on cohomology of groups and of class field theory that we will use see [2]. We first prove a useful lemma.

LEMMA 4.1. — *When χ is not the Teichmüller character ω then the Tate cohomology groups of the G-module $M(\chi)$ are isomorphic to $R_\chi/(p^n)$ or 0 according as $\chi(\ell) = 1$ or not.*

(Here p^n denotes the order of G.)

Proof: Because Δ and G have coprime order the action of Δ commutes with G-cohomology. More precisely :

$$\widehat{H}^q(G,A)^\Delta \cong \widehat{H}^q(G,A^\Delta) \qquad \text{for every } \mathbf{Z}[G\times\Delta]-\text{module } A,$$
$$\widehat{H}^q(G,A)(\chi) \cong \widehat{H}^q(G,A(\chi)) \qquad \text{for every } \mathbf{Z}_p[G\times\Delta]-\text{module } A.$$

We compute the cohomology of $M(\chi)$ by taking χ-parts of the cohomology groups of the $G \times \Delta$-modules that occur in the exact sequence

$$0 \longrightarrow O_K^* \longrightarrow U_K \longrightarrow C_K \longrightarrow C\ell_K \longrightarrow 0.$$

Here O_K^* denotes the unit group of the ring of K-integers, C_K denotes the group of idèle classes of K and U_K denotes the subgroup of idèles that have trivial valuation at the finite primes of K.

By global class field theory we have that $\widehat{H}^q(G,C_K) \cong \widehat{H}^{q-2}(G,\mathbf{Z})$ for all $q \in \mathbf{Z}$ and therefore, since $\chi \neq 1$ that

$$\widehat{H}^q(G,C_K)(\chi) = 0 \qquad \text{for all } q \in \mathbf{Z}. \tag{1}$$

Since χ is odd and not equal to ω we have that

$$\widehat{H}^q(G,O_K^*)(\chi) = 0 \qquad \text{for all } q \in \mathbf{Z}. \tag{2}$$

We compute the cohomology of the idèle unit group U_K by means of local class field theory. It is known [2] that

$$\widehat{H}^q(G,U_K) = \bigoplus_{v|\ell} \widehat{H}^q(G_v,O_w^*)$$

where the sum runs over the primes v of F over ℓ and G_v denotes the decomposition group of any such v in G. We have, of course, that $G_v = G$ for every v. By w we denote a prime of K over v and by O_w^* the ring of integers of the completion K_w of K at w. The Galois group of the local field K_w over $\mathbf{Q}_p$ is just $G_v \times \Delta_\ell$ where Δ_ℓ denotes the decomposition group of a prime v in F over ℓ. The group $\Delta_\ell \subset \Delta$ acts trivially on the cohomology groups $\widehat{H}^q(G_v,\mathbf{Z})$ and therefore, by local class field theory, it acts trivially on the groups $\widehat{H}^q(G_v,K_w^*) \cong \widehat{H}^{q-2}(G_v,\mathbf{Z})$ as well. It follows from the long cohomology sequence of

$$0 \longrightarrow O_w^* \longrightarrow K_w^* \longrightarrow \mathbf{Z} \longrightarrow 0$$

and the fact that $\gcd(\#G_v,\#\Delta_\ell) = 1$ that Δ_ℓ acts trivially on the cohomology groups $\widehat{H}^q(G_v,O_w^*)$.

Each of the groups $\widehat{H}^q(G_v,O_w^*)$ is cyclic of order $\#G_v = p^n$ and Δ/Δ_ℓ permutes the sumands in the sum above. We conclude that for all $q \in \mathbf{Z}$

$$\widehat{H}^q(G,U_K) \cong \mathbf{Z}/p^n\mathbf{Z}[\Delta/\Delta_p] \qquad \text{as } \Delta\text{-modules.}$$

Since $\chi : \Delta \longrightarrow \overline{\mathbf{Q}}_p^*$ is injective we find

$$\widehat{H}^q(G,U_K)(\chi) = \begin{cases} R_\chi/(p^n), & \text{when } \chi(\ell) = 1; \\ 0 & \text{when } \chi(\ell) \neq 1. \end{cases} \tag{3}$$

The lemma now follows from (1), (2), (3) and the long cohomology sequences associated to the four term exact sequence above.

COROLLARY 4.2. — *If $\chi \neq \omega$ and $\chi(\ell) \neq 1$ then there exists an exact sequence*

$$0 \longrightarrow V \xrightarrow{\sigma} V \longrightarrow M(\chi) \longrightarrow 0$$

where V is $R_\chi[G]$-free of rank d = the minimal number of R_χ-generators of $C\ell(\chi)$.

Proof : Since χ is odd and not equal to ω, it follows from the proof of Lemma(4.1) that $\widehat{H}^1(G, O_K^*)(\chi) = 0$. This implies that the canonical map $C\ell(\chi) \longrightarrow M(\chi)$ is injective and it follows easily that the module $M(\chi)/(\tau - 1)M(\chi)$ is isomorphic to $\cong C\ell(\chi)$. (Here τ denotes a generator of the cyclic group G.) Therefore there is, by Nakayama's lemma, an exact sequence

$$0 \longrightarrow A \longrightarrow V \longrightarrow M(\chi) \longrightarrow 0$$

where V is $R_\chi[G]$-free of rank d. By Lemma(4.1) we have $\widehat{H}^q(G, M(\chi)) = 0$. Therefore since G is a p-group and $M(\chi)$ is finite we have that $M(\chi)$ is a cohomologically trivial G-module. Therefore $A \subset V$ is cohomologically trivial and one can show that A is a projective $R_\chi[G]$-module in a way similar to the proof of Théorème 8 of Chapitre IX of [13]. Since $R_\chi[G]$ is a local ring one concludes that A is free and since $M(\chi)$ is finite it is free of rank d. This proves (4.2).

The following theorem can often be used to prove that $C\ell(\chi)$ is cyclic over R_χ.

THEOREM 4.3. — *If there is a prime $\ell \equiv 1 \pmod{p^n}$ for which the Stickelberger element $\phi_{\chi,\ell}(T)$ has Weierstrass degree 1 then $C\ell(\chi)$ is cyclic over R_χ and*

$$I^{(n)}(\chi) = \mathrm{Fit}_\Lambda C\ell(\chi) \pmod{(1+T)^{p^n} - 1} \quad \text{when } \chi \neq \omega^i,$$
$$I^{(n)}(\omega^i) = \mathrm{Fit}_\Lambda C\ell(\omega^i) \bigcap (T) \pmod{(1+T)^{p^n} - 1} \quad \text{for } i \neq 1.$$

Proof: In the proof we will write h for p raised to the length of the R_χ-module $C\ell(\chi)$. In other words we have that $\#C\ell(\chi) = \#R_\chi/(h)$.

By Weierstrass' Preparation Theorem we have that

$$\phi \quad \mathrm{Stick}_{\chi,\ell}(T) = (T - \alpha) \cdot \text{unit} \qquad \text{in } \Lambda/((1+T)^{p^n} - 1).$$

We have that, upto a unit,

$$(4) \quad \alpha = \sum_{x \in (\mathbb{Z}/\ell f\mathbb{Z})^*} \langle \frac{x}{\ell f} \rangle \chi^{-1}(x) = (1 - \chi(\ell)) \sum_{x \in (\mathbb{Z}/f\mathbb{Z})^*} \langle \frac{x}{f} \rangle \chi^{-1}(x) = (\chi(\ell) - 1)h.$$

If $\chi(\ell) = 1$ this implies that $\alpha = 0$. By Stickelberger's Theorem [16] we see that T kills $M(\chi)$ i.e. the module $M(\chi)$ is G-invariant. Therefore the zero-th Tate cohomology group is $M(\chi)/p^n M(\chi)$. By Lemma(4.1) this group is cyclic over R_χ. This implies that the class group $C\ell(\chi)$ is also cyclic over R_χ and therefore its $\Lambda/((1+T)^{p^n} - 1)$-Fitting ideal is equal to (T, h). Since the constant terms of all Stickelberger elements are either 0 or a unit times h, we clearly have that $I^{(n)}(\chi) \subset \mathrm{Fit}_\Lambda C\ell(\chi) \pmod{(1+T)^{p^n} - 1}$. Since $T \in I^{(n)}(\chi)$ we are now done when χ is a power of ω. In all other cases there exists a prime $\ell' \equiv 1 \pmod{p^n}$ for which $\chi(\ell') \neq 1$. By (4) the Stickelberger element $\phi_{\chi,\ell'}(T)$ has constant term equal to a unit times h which shows that $h \in \mathrm{Stick}^{(n)}(\chi)$ as required.

If $\chi(\ell) \neq 1$ we have by Lemma(4.1) that $M(\chi)$ is a cohomologically trivial G-module. In the notation of Corollary(4.2) we let $f = \det(\sigma)$. The Fitting ideal $\mathrm{Fit}_{R_\chi[G]}(M(\chi))$ is generated by f. Since $M(\chi)/TM(\chi) \cong C\ell(\chi)$ we see that $f(0) = \text{unit} * h$. By Stickelberger's theorem $M(\chi)$ is annihilated by $\phi_{\chi,\ell}(T) = \text{unit} * (T - \alpha)$. Since $R_\chi[G]/(T-\alpha)$ is cyclic, the ideals between $(T-\alpha)$ and R_χ are linearly ordered. The smallest ideal strictly larger than $(T-\alpha)$ is $(T-\alpha, \alpha p^{n-1})$. The $R_\chi[G]$-annihilator is one of the ideals between $(T-\alpha)$ and R_χ. If it were not equal to $(T-\alpha)$ then $(T-\alpha, \alpha p^{n-1}) \subset \mathrm{Ann}_{R_\chi[G]}(M(\chi))$. It follows easily that $(1+T)^{p^{n-1}} - 1$ kills $M(\chi)$ and hence that the subgroup $H = G^{p^{n-1}}$ acts trivially on $M(\chi)$. This implies that the H-cohomology groups of $M(\chi)$ are non-trivial, contradicting the cohomological triviality of $M(\chi)$.

We conclude that $\mathrm{Ann}_{R_\chi[G]}(M(\chi)) = (T - \alpha)$ and hence that f is a multiple of $T - \alpha$. Since, upto units, we have that $f(0) = \phi_{\chi,\ell}(0) = h = \alpha$ we conclude that $f = (T - \alpha) * \text{unit}$. It follows that both $M(\chi)$ and $C\ell(\chi)$ are cyclic R_χ-modules. As in the previous case we have that $\mathrm{Fit}_{R_\chi[G]} C\ell(\chi) = (T, h)$ and the obvious inclusion $I^{(n)}(\chi) \subset \mathrm{Fit}_\Lambda C\ell(\chi) \pmod{(1+T)^{p^n} - 1}$. To prove the other inclusion we choose another isomorphism

$$R_\chi[G] \cong R_\chi[[T]]/((1+T)^{p^n} - 1)$$

by replacing $T+1$ by $(T+1)^2$. We see that $(T+1)^2 - 1 - \alpha = T^2 + 2T - \alpha \in I^{(n)}(\chi)$. It follows at once that T and $\alpha = \text{unit} * h$ are in $I^{(n)}(\chi)$ as required.

The following Corollary says that if the Stickelberger ideal $I(\chi)$ is very large, the answers to questions (3.2) and (3.2)' are affirmative.

COROLLARY 4.4. — *If there is a power series in $I(\chi)$ of Weierstrass degree 1 then*

$$I(\chi) = \mathrm{Fit}_\Lambda C\ell(\chi) \quad \text{when } \chi \neq \omega^i,$$
$$I(\omega^i) = \mathrm{Fit}_\Lambda C\ell(\omega^i) \bigcap (T) \quad \text{for } i \neq 1.$$

Proof : If there is a power series in $\phi_{\chi,\ell}$ of Weierstrass degree 1 then there must be a prime $\ell \equiv 1 \pmod p$ for which $\phi_{\chi,\ell}(T)$ has Weierstrass degree 1. It follows from the previous Theorem that $C\ell(\chi)$ is cyclic over R_χ and hence that $\mathrm{Fit}_\Lambda C\ell(\chi) = (T, h)$ in the notation of the proof of Theorem(4.3). It is obvious that $I(\chi) \subset \mathrm{Fit}_\Lambda C\ell(\chi)$ and the other inclucion follows by arguments similar to the ones employed in the proof of Theorem(4.3). This proves (4.4).

THEOREM 4.5. — *If χ is quadratic, not equal to the character of conductor 3, and $C\ell(\chi)$ is a non-trivial cyclic group then*

$$I(\chi) = \mathrm{Fit}_\Lambda C\ell(\chi).$$

Proof: It is easy to see that χ cannot be a power of the Teichmüller character. In [8] it is shown that for each $n \geq 1$ there exist primes $\ell \equiv 1 \pmod{p^n}$ for which $\phi_{\chi,\ell}(T)$ has its linear coefficient not divisible by p. As in the proof of Theorem (4.3) one concludes that $T \in I^{(n)}(\chi)$ for every $n \geq 1$. It follows that $I(\chi)$ contains T. The Theorem therefore follows from the previous Corollary.

In [8] it is shown that the set of primes $\ell \equiv 1 \pmod{p^n}$ for which the linear coefficient of $\phi_{\chi,\ell}(T)$ is not divisible by p has positive Čebotarev density. Moreover, the two subsets of primes for which in addition $\chi(\ell) = 1$ or $\chi(\ell) \neq 1$ respectively each have positive density.

Remark 4.6 : If χ is not a power of the Teichmüller character and $C\ell(\chi) = 0$ then the answer to questions (3.2) is affirmative. This follows easily from the fact that there is a prime ℓ congruent to $1 \pmod p$ for which $\chi(\ell) \neq 1$. By (1) the Stickelberger element $\phi_{\chi,\ell}(T)$ has constant term a unit. We conclude that both the Fitting and the Stickelberger ideal are the unit ideal. I do not have such a complete result in the case where χ is a power of the Teichmüller character. See example(4.6) for some numerical results.

We proceed by presenting some numerical evidence for a positive answer to Questions (3.2) and (3.2)'. The calculations involved are quite straightforward and not too lengthy.

EXAMPLE 4.7. — *p-parts of the class groups of $\mathbb{Q}(\zeta_p)$.*

It is known that all ω^i-eigenspaces of the p-parts of the class groups of $\mathbb{Q}(\zeta_p)$ are cyclic whenever $p < 150000$ cf [14,15]. It would follow from Vandiver's conjecture that these eigenspaces are in fact always cyclic [16,Cor.10.15]. An affirmative answer to Question(3.2)' combined with this conjecture would imply that for each prime p and each odd $i \not\equiv 1 \pmod{p-1}$ there exists a prime ℓ for which the linear coefficient of $\phi_{\omega^i,\ell}(T)$ is not zero mod p. A little calculation shows that this boils down to the following :

For an odd prime p and even i satisfying $2 \leq i \leq p-3$ does there exist a prime $\ell \equiv 1 \pmod p$ for which

$$\sum_{x=1}^{\ell-1} \mathrm{ind}_\ell(x) B_i(x) \not\equiv 0 \pmod p \ ?$$

(Here $B_k(t)$ denotes the k-th Bernoulli polynomial and ind_ℓ the index with respect to some primitive root mod ℓ.)

By Theorem(4.3) an affirmative answer to this question would imply that the first Stickelberger ideal $I^{(1)}(\omega^i)$ is equal to $\mathrm{Fit}_\Lambda C\ell(\omega^i) \bigcap (T)$ modulo $(1+T)^p - 1$ for $i \not\equiv 1 \pmod{p-1}$. It would, independently of the truth of Vandiver's conjecture, also imply that the ω^i-eigenspaces of the p-part of the class group of $\mathbb{Q}(\zeta_p)$ are cyclic groups. Our criterion is similar to Washington's [16,Prop 8.19] but it appears to be independent

For a few primes p and characters ω^i we checked the above. In all cases considered there appeared to exist a prime $\ell \equiv 1 \pmod p$ for which the linear coefficient of the Stickelberger element $\phi_{\omega^i,\ell}(T)$ is not zero mod p for all i simultaneously. We list the first few odd primes p and the corresponding smallest such ℓ. Often, but not always, ℓ is just the smallest prime congruent to $1 \pmod p$.

p	ℓ	p	ℓ	p	ℓ
5	11	41	83	83	167
7	29	43	947	89	1069
11	23	47	283	97	1553
13	79	53	107	101	809
17	137	59	709	103	1031
19	191	61	1709	107	857
23	139	67	269	109	2399
29	59	71	569	113	1583
31	311	73	439	127	509
37	149	79	317	131	263

EXAMPLE 4.8. — *Various fields of prime conductor.*

In [7] D.H. Lehmer and J. Masley computed the minus class numbers of the cyclotomic fields $\mathbf{Q}(\zeta_f)$ for the *primes* $f \leq 509$. In many cases one can determine the structure of these class groups as abelian groups by exploiting the action of $\mathrm{Gal}(\mathbf{Q}(\zeta_f)/\mathbf{Q})$. In some cases the action of this Galois group does not help very much. For instance, when χ is an odd character of degree d and p is a prime congruent to 1 (mod d) dividing $\#C\ell(\chi)$ more than once it is not immediately clear how to decide whether $C\ell(\chi)$ is cyclic over R_χ or not. In these cases we were always able to find an auxiliary prime ℓ for which the Weierstrass degree of $\phi_{\chi,\ell}(T)$ is equal to 1. We conclude from Theorem(4.3) that in all these cases the group $C\ell(\chi)$ is cyclic over R_χ.

Below we list the results in a small table. In the column "$g \mapsto \chi(g)$" we list a primitive root g mod f and the value of the character $\chi(g)$ mod p.

f	p^d	$\deg\chi$	$g \mapsto \chi(g)$	ℓ
139	47^2	46	$2 \mapsto -9$	283
281	41^2	40	$3 \mapsto 17$	83
443	27^2	26	$2 \mapsto \alpha$	7
461	5^2	4	$2 \mapsto 3$	11
491	11	10	$2 \mapsto 6$	–
491	11^2	10	$2 \mapsto 7$	23

Mutatis mutandis everything we said above also holds in the case $f = 443$. In this case, however, "cyclic" means cyclic over the ring $\mathbf{Z}_3[\zeta_{13}]$ which is of degree 3 over $\mathbf{Z}_3$. The character χ is given by $\alpha = \chi(g)$ which mod 3 is determined by $\alpha^3 + \alpha^2 - \alpha + 1 = 0$. The class group involved is cyclic over this ring, but as an abelian group it is isomorphic to $\mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z} \times \mathbf{Z}/9\mathbf{Z}$.

EXAMPLE 4.9. — *p-class groups of quadratic fields.*

Sofar we encountered only cyclic class groups in our examples. There are heuristics on the statistical behavior of the structure of class groups of number fields that suggest that non-cyclic groups $C\ell(\chi)$ are rare [3]. Probably any character χ for which the minimal number of R_χ-generators of $C\ell(\chi)$ is merely moderately large will have a large conductor.

The only examples we present are quadratic characters χ. In this case $C\ell(\chi)$ is for each odd prime p just the p-part of the class group of the quadratic field $\overline{\mathbf{Q}}^{\ker\chi}$. Thanks to the efforts of D. Shanks and others many examples of class groups of complex quadratic fields and small primes p are known for which the p-rank is somewhat large. We computed for some quadratic characters χ and some odd primes p several Stickelberger elements $\phi_{\chi,\ell}(T)$. In the table for a fixed prime ℓ a few Stickelberger elements are listed, each made with a different primitive root mod ℓ. For computational convenience we chose in all our examples the conductor f to be prime. We computed the Fitting ideals from the structure of the p-class groups which we took from Buell's tables [1]. We found that the Stickelberger elements generate the Λ-Fitting ideal modulo $((1+T)^{p^n} - 1)$ for certain small powers p^n. When the exact power of p dividing $\ell - 1$ is p^n, the Stickelberger element was computed modulo $((1+T)^{p^n} - 1, p^n T)$.

f	classgroup	ℓ	p^n	$\phi_{\chi,\ell}(T)$
3299	3×9	163	3^4	$27 + 15T + 49T^2 + \ldots$
				$27 + 48T + 61T^2 + \ldots$
				$27 + 24T + 70T^2 + \ldots$
		487	3^4	$45T + 201T^2 + 120T^3 + 47T^4 + \ldots$
				$144T + 75T^2 + 99T^3 + 167T^4 + \ldots$
				$72T + 183T^2 + 12T^3 + 71T^4 + \ldots$
		811	3^4	$27 + 42T + 58T^2 + \ldots$
				$27 + 21T + 70T^2 + \ldots$
				$27 + 51T + 25T^2 + \ldots$
		1297	3^4	$27 + 75T + 24T^2 + 62T^3 + \ldots$
				$27 + 78T + 27T^2 + 28T^3 + \ldots$
				$27 + 39T + 78T^2 + 59T^3 + \ldots$
		1459	3^5	$27 + 489T + 128T^2 + \ldots$
				$27 + 609T + 62T^2 + \ldots$
				$27 + 669T + 395T^2 + \ldots$
		1621	3^4	$12T + 21T^2 + 19T^3 + \ldots$
				$6T + 24T^2 + 41T^3 + \ldots$
				$3T + 66T^2 + 43T^3 + \ldots$
		1783	3^4	$39T + 37T^2 + \ldots$
				$60T + 55T^2 + \ldots$
				$30T + 67T^2 + \ldots$
134059	9×9	163	3^4	$36T + 43T^2 + 4T^3 + \ldots$
				$18T + 67T^2 + 21T^3 + \ldots$
				$9T + 55T^2 + \ldots$
		487	3^4	$81 + 45T + 94T^2 + \ldots$
				$81 + 144T + 109T^2 + \ldots$
				$81 + 72T + 70T^2 + \ldots$
		811	3^4	$54T + 35T^3 + \ldots$
				$27T + 54T^2 + 55T^3 + \ldots$
				$54T + 17T^3 + \ldots$

f	classgroup	ℓ	p^n	$\phi_{\chi,\ell}(T)$
351751	9×27	163	3^4	$243 + 45T + 57T^2 + 56T^3 + \ldots$
				$243 + 63T + 39T^2 + 28T^3 + \ldots$
				$243 + 72T + 12T^2 + 11T^3 + \ldots$
		487	3^4	$243 + 90T + 99T^2 + 57T^3 + 20T^4 + \ldots$
				$243 + 45T + 135T^2 + 132T^3 + 233T^4 + \ldots$
				$243 + 144T + 180T^2 + 48T^3 + 23T^4 + \ldots$
		811	3^4	$63T + 12T^2 + 80T^4 + \ldots$
				$72T + 66T^2 + 21T^3 + 56T^3 + \ldots$
				$36T + 48T^2 + 36T^3 + 14T^4 + \ldots$
		1297	3^4	$243 + 9T^2 + 28T^3 + \ldots$
				$243 + 63T^2 + 53T^3 + \ldots$
				$243 + 36T^2 + 46T^3 + \ldots$
		1458	3^5	$603T + 608T^2 + \ldots$
				$666T + 350T^2 + \ldots$
				$333T + 551T^2 + \ldots$
3321607	$3 \times 3 \times 9 \times 7$	163	3^4	$567 + 9T + 27T^2 + 51T^3 + 60T^4 + 3T^5 + 1$
				$567 + 18T + 36T^2 + 30T^3 + 60T^4 + 30T^6 +$
				$567 + 63T + 54T^2 + 42T^3 + 6T^4 + 12T^5 +$
		487	3^4	$51T^2 + 125T^3 + \ldots$
				$195T^2 + 232T^3 + \ldots$
				$231T^2 + 35T^3 + \ldots$
		811	3^4	$36T + 36T^2 + 38T^3 + \ldots$
				$18T + 45T^2 + 16T^3 + \ldots$
				$9T + 9T^2 + 11T^3 + \ldots$
		1297	3^4	$567 + 27T^2 + 9T^3 + 52T^4 + \ldots$
				$567 + 27T^2 + 72T^3 + 10T^4 + \ldots$
				$567 + 27T^2 + 63T^3 + 4T^4 + \ldots$
		1459	3^5	$567 + 171T + 252T^2 + 399T^3 + 866T^4 + \ldots$
				$567 + 450T + 315T^2 + 348T^3 + 317T^4 + \ldots$
				$567 + 225T + 387T^2 + 336T^3 + 17T^4 + \ldots$
		1621	3^4	$63T + 45T^2 + 66T^3 + 63T^4 + 52T^5 + \ldots$
				$72T + 54T^2 + 15T^3 + 72T^4 + 77T^5 + \ldots$
				$36T + 45T^2 + 57T^3 + 45T^4 + 10T^5 + \ldots$
		1783	3^4	$63T + 42T^2 + 70T^3 + \ldots$
				$72T + 33T^2 + 26T^3 + \ldots$
				$36T + 60T^2 + 7T^3 + \ldots$
12451	5×5	251	5^3	$25 + 90T + 121T^2 + \ldots$
				$25 + 45T + 19T^2 + \ldots$

f	classgroup	ℓ	p^n	$\phi_{\chi,\ell}(T)$
63499	7×7	197	7^2	$14T + 47T^2 + 32T^3 + \ldots$
				$7T + 10T^2 + 48T^3 + \ldots$
272231	11×33	727	11^2	$11T + 8T^2 + \ldots$
				$66T + 46T^2 + \ldots$
1016083	13×13	677	13^2	$13T + 151T^2 + \ldots$
				$91T + 15T^2 + \ldots$

Manuscrit reçu le 28 septembre 1989

* p. 185 *supported by the Netherlands Organization of Scientific Research.*

BIBLIOGRAPHY

[1] D.A. Buell. — Class groups of quadratic fields, *Math. Comp.* **30**, (1976), 610-623.

[2] J.W.S. Cassels and A. Fröhlich. — *Algebraic number theory*, Academic Press, London, 1967.

[3] H. Cohen and J. Martinet. — Class groups of number fields : Numerical heuristics, *Math. Comp.* **48**, (1987), 123-137.

[4] V.A. Kolyvagin. — Euler systems, To appear.

[5] S. Lang. — *Algebra*, 2nd edition, Addison-Wesley, Menlo Park, 1984.

[6] S. Lang. — *Cyclotomic fields*, Graduate Texts in Math. **59**, Springer-Verlag, New York 1978.

[7] D.H. Lehmer and J. Masley. — Table of the cyclotomic class numbers $h^*(p)$ and their factors for $200 < p < 521$, *Math. Comp.* **32**, (1978), 577-582, microfiche supplement.

[8] H.W. Lenstra and R.J. Schoof. — Class groups of imaginary quadratic number fields, in preparation.

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

[10] J. Northcott. — *Finite free resolutions*, Cambridge Tracts in Math. **71**, Cambridge University Press, Cambridge 1976.

[11] K. Rubin. — Kolyvagin's system of Gauss sums, To appear in *Arithmetic algebraic geometry Texel Birkaüser* 1990.

[12] G. Schrutka von Rechtenstamm. — Tabelle der (Relativ)-Klassenzahlen der Kreiskörper, deren ϕ-Funktion des Wurzelexponenten (Grad) nicht grösser als 256 ist, *Abh. Deutschen Akad. Wiss. Berlin, Kl. Math. Phys.* **2**, (1964), 1-64.

[13] J.-P. Serre. — *Corps Locaux*, Hermann, Paris, 1968.

[14] J.W. Tanner and S. Wagstaff. — New congruences for Bernoulli numbers, *Math. Comp.* **48**, (1987), 341-350.

[15] S. Wagstaff. — The irregular primes to 125,000, *Math. Comp.* **32**, (1978), 583-591.

[16] L.C. Washington. — *Introduction to cyclotomic fields*, Graduate texts in Math. **83**, Springer-Verlag, New York, 1982.

R. SCHOOF
Mathematisch Instituut
Rijksuniversiteit Utrecht
3508 TA Utrecht
The Netherlands