ANNALES

DE

L'INSTITUT FOURIER

Cornelius GREITHER & Radan KUČERA

Eigenspaces of the ideal class group

Tome 64, n° 5 (2014), p. 2165-2203.

<http://aif.cedram.org/item?id=AIF_2014__64_5_2165_0>

Ann. Inst. Fourier, Grenoble
64, 5 (2014) 2165-2203

EIGENSPACES OF THE IDEAL CLASS GROUP

by Cornelius GREITHER & Radan KUČERA (*)

Abstract. — The aim of this paper is to prove an analog of Gras' conjecture for an abelian field F and an odd prime p dividing the degree $[F : \mathbb{Q}]$ assuming that the p-part of $\mathrm{Gal}(F/\mathbb{Q})$ group is cyclic.

Résumé. — Cet article se propose de démontrer une version analogue de la conjecture de Gras pour un corps abélien F et un nombre premier $p > 2$ qui divise le degré $[F : \mathbb{Q}]$. On fait l'hypothèse que la p-partie du groupe $\mathrm{Gal}(F/\mathbb{Q})$ est cyclique.

Introduction

Let p be a fixed odd prime number. Let $L \neq \mathbb{Q}$ be a real abelian field such that the exponent of $H = \mathrm{Gal}(L/\mathbb{Q})$ is a divisor of $p-1$. We fix a cyclic field K of absolute degree p^u, u being a positive integer, and we assume that there is not both tame and wild ramification in $K/\mathbb{Q}$, *i.e.*, either $K/\mathbb{Q}$ is only tamely ramified or K is the field of degree p^u and conductor p^{u+1}. Let K' be the subfield of K satisfying $[K : K'] = p$. Let C_F and $C_{F'}$ be the p-parts of the ideal class groups of $F = KL$ and of $F' = K'L$, respectively. By E_R and Cyc_R we shall denote the group of units and the Sinnott group of circular units of an abelian field R, respectively. Let χ be a nontrivial Dirichlet character of L and

$$e_\chi = \frac{1}{|H|} \sum_{\tau \in H} \chi(\tau)\tau^{-1} \in \mathbb{Z}_p[H]$$

be the idempotent corresponding to χ. In this paper we shall prove:

Keywords: Gras' conjecture, circular (cyclotomic) units, ideal class group, Euler system, annihilators of the class group.
Math. classification: 11R20, 11R29.
(*) The second author was supported under Project P201/11/0276 of the Czech Science Foundation.

THEOREM 8.1. — *We have*

$$|e_\chi C_F| = |e_\chi C_{F'}| \cdot \left|\left((E_F/\operatorname{Cyc}_F E_{F'}) \otimes \mathbb{Z}_p\right)^{e_\chi}\right| = \left|\left((E_F/\operatorname{Cyc}_F) \otimes \mathbb{Z}_p\right)^{e_\chi}\right|.$$

Finally, for $j = 0, 1, \dots, u$, let $F^{(j)}$ be the subfield of F determined by $[F : F^{(j)}] = p^j$, so $F^{(0)} = F$, $F^{(1)} = F'$, $\dots$, $F^{(u)} = L$. As corollaries of the previous theorem we shall obtain the following statements on annihilators:

COROLLARY 9.4. — *Let* $\Gamma = \operatorname{Gal}(F/L)$. *We have*

$$\operatorname{Ann}_{\mathbb{Z}_p[\Gamma]}\left((E_L/\operatorname{Cyc}_L)\otimes\mathbb{Z}_p\right)^{e_\chi} \cdot \prod_{j=0}^{u-1} \operatorname{Ann}_{\mathbb{Z}_p[\Gamma]}\left((E_{F^{(j)}}/\operatorname{Cyc}_{F^{(j)}} E_{F^{(j+1)}})\otimes\mathbb{Z}_p\right)^{e_\chi} \subseteq \operatorname{Ann}_{\mathbb{Z}_p[\Gamma]}(e_\chi C_F).$$

COROLLARY 9.6. — *Assume that* $u = 1$, *so* $F' = L$. *Then*

$$(1-\sigma) \cdot \operatorname{Ann}_{\mathbb{Z}_p[G]}\left((E_F/\operatorname{Cyc}_F E_L) \otimes \mathbb{Z}_p\right) \subseteq \operatorname{Ann}_{\mathbb{Z}_p[G]}(C_F),$$

where σ *is a generator of* $\Gamma = \operatorname{Gal}(F/L)$ *and* $G = \operatorname{Gal}(F/\mathbb{Q})$.

This paper is another attempt to make the Euler system machinery work in a "non-semi-simple" situation. We are concerned with $\mathbb{Z}_p[\Gamma]$-modules where the order of Γ is a p-power. Our results do not entail the class group of F and the quotient of units modulo circular units in F directly, instead they use relative versions: take the object for F modulo the image of the corresponding object attached to the subfield F' such that $[F : F'] = p$. (The relative group $E_F/\operatorname{Cyc}_F E_{F'}$ is already visible in Theorem 8.1; the relative class group $C_F/\operatorname{im}(C_{F'})$ is implicit in that theorem and will come up explicitly in the proofs. We should remark here that the term "relative class group" refers to a slightly different structure in the literature: the kernel of the norm map instead of the cokernel of the extension map.) But there is another complication. The relative group $E_F/\operatorname{Cyc}_F E_{F'}$ does not lead to bounds on the relative class group, but only on its quotient modulo the subgroup generated by the classes of ambiguous ideals in F/F'. That is, we bound a module which is smaller than it should be. To make the numbers come out right in the end, we therefore need sharper bounds, in other words: we need to enlarge the group of circular units. More concretely we extract certain roots from circular units, and show that these roots still can be fed into the Euler-Kolyvagin machinery.

We hope that the preceding remarks at least partly explain the technical complexities of this paper. One technical prerequisite, Theorem 3.1, which concerns the image of linear forms on the Sinnott module U, is proven in a separate paper [5] since we like to think that it is of independent interest.

Our Theorem 8.1 is closely related to one of the principal results of L. V. Kuzmin in [8], which was reproved in a more direct way by J.-R. Belliard and T. Nguyen Quang Do in [1]. If we fix a prime p (which is supposed to be odd in [1]), any real abelian field F can be written as the compositum $F = KL$, where the degree of $K/\mathbb{Q}$ is a power of p and the degree of $L/\mathbb{Q}$ is relatively prime to p. Taking any $\mathbb{Z}_p$-valued $\mathbb{Q}_p$-irreducible character χ of $\mathrm{Gal}(F/K)$, the mentioned result describes the fudge factor c_χ in the following formula

$$|e_\chi C_F| = c_\chi \cdot \left|\left((E_F/\operatorname{Cyc}_F) \otimes \mathbb{Z}_p\right)^{e_\chi}\right|$$

by means of the χ-part $(e_\chi R : e_\chi U)$ of the index of Sinnott's module U. Using results of Sinnott published in [11] one can show that $c_\chi = 1$ if χ is nontrivial, $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic and p is odd: in this case, [11, Theorem 5.3] states that $p \nmid (R : U)$, so the product on the right hand side of formula (5.23) for $e = 1$ on [11, page 219] equals 1. But to prove that $c_\chi = 1$ we need to show that each factor of this product equals 1. This follows from the fact that each factor is a positive integer since [11, Lemma 5.1] holds true for $\mathbb{Q}_p[G]$ even though it is formulated for $\mathbb{Q}[G]$ only. The authors of [1] probably had exactly this reasoning in mind in their remark a)(i) on page 921.

There also seems to be a connection to a recent paper [2] of Kâzim Büyükboduk. Howewer, the exact relation of the right hand side of Theorem (B) in loc.cit. to our circular unit index is not at all clear.

1. Euler system machinery

We shall slightly modify Karl Rubin's exposition of Euler systems given in [10] by lowering the degree of the auxiliary fields[(1)].

Let F be a real abelian number field, $F \neq \mathbb{Q}$. Let M be a fixed (large) odd integer (later on it will be a power of a prime). Let $\mathcal{S}_M$ be the set of all positive square-free integers divisible only by primes ℓ splitting completely in F and satisfying $\ell \equiv 1 \pmod{M}$. For any prime $\ell \in \mathcal{S}_M$ let $\mathbb{Q}_\ell$ be the unique subfield of the ℓth cyclotomic field of absolute degree M, $G_\ell = \mathrm{Gal}(\mathbb{Q}_\ell/\mathbb{Q})$ and σ_ℓ a fixed generator of G_ℓ. Confusion with the more usual

(1) The main difference with respect to [10] is that we consider only auxiliary primes $\ell \equiv 1 \pmod{M}$ and for each such prime ℓ we do not take the compositum with the ℓth cyclotomic field but only with its subfield of absolute degree M. The reason is that we want each ramified prime to have trivial Frobenius automorphism on these auxiliary fields, see (7.4).

meaning of $\mathbb{Q}_\ell$ is unlikely, since we never use completions of fields in this paper. Let us denote

$$\mathrm{N}_\ell = \sum_{j=0}^{M-1} \sigma_\ell^j, \quad \mathrm{D}_\ell = \sum_{j=1}^{M-1} j\sigma_\ell^j \in \mathbb{Z}[G_\ell],$$

so $(\sigma_\ell - 1)\mathrm{D}_\ell = M - \mathrm{N}_\ell$. For any $r \in \mathcal{S}_M$ let $\mathbb{Q}_r$ denote the compositum of $\mathbb{Q}_\ell$ for all primes $\ell \mid r$, so for example $\mathbb{Q}_1 = \mathbb{Q}$, and let F_r be the compositum of F and $\mathbb{Q}_r$. We have

$$G_r := \mathrm{Gal}(F_r/F) \cong \mathrm{Gal}(\mathbb{Q}_r/\mathbb{Q}) \cong \prod_{\substack{\ell \mid r \\ \ell \text{ is a prime}}} G_\ell,$$

and so we can identify G_r with the latter product. Using this identification, σ_ℓ is an automorphism of any F_r with trivial restriction to any subfield of F_r where ℓ is unramified. Let

$$\mathrm{D}_r = \prod_{\substack{\ell \mid r \\ \ell \text{ is a prime}}} \mathrm{D}_\ell, \qquad \mathrm{N}_r = \prod_{\substack{\ell \mid r \\ \ell \text{ is a prime}}} \mathrm{N}_\ell \in \mathbb{Z}[G_r].$$

For any prime $\ell \in \mathcal{S}_M$ and any $r \in \mathcal{S}_M$ such that $\ell \nmid r$ let Fr_ℓ be the Frobenius automorphism of ℓ in $F_r/\mathbb{Q}$; we have $\mathrm{Fr}_\ell \in G_r$.

Let m be the conductor of F, and for any positive integer n let ζ_n be a fixed primitive nth root of unity. For any $r \in \mathcal{S}_M$ we define

$$\xi_r = \mathrm{N}_{\mathbb{Q}(\zeta_{mr})/F_r}\left(1 - \zeta_m \cdot \prod_{\substack{\ell \mid r \\ \ell \text{ is a prime}}} \zeta_\ell\right).$$

The following four lemmas describe properties of the ξ_r which are in close analogy with ES1-ES4 and Lemmas 2.1, 2.2 and 2.3 in [10].

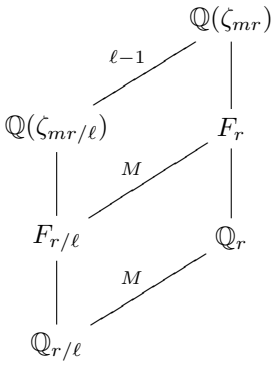
LEMMA 1.1. — *For any $r \in \mathcal{S}_M$ and any prime $\ell \mid r$ we have*

(1) $\xi_r \in F_r^\times$.
(2) *ξ_r is a circular number of F_r; it is a circular unit if and only if mr is not a prime power (which is always the case if $r > 1$).*
(3) $\xi_r^{\mathrm{N}_\ell} = \xi_{r/l}^{\mathrm{Fr}_\ell - 1}$.
(4) $\xi_r \equiv \xi_{r/l}^{(\ell-1)/M}$ *modulo each prime ideal of F_r dividing ℓ.*

Proof. — The first two properties are well-known. The third one follows from

$$\xi_r^{\mathrm{N}_\ell} = \mathrm{N}_{\mathbb{Q}(\zeta_{mr})/F_{r/\ell}}\Big(1-\zeta_m\cdot\prod_{\substack{t\mid r\\ t\text{ is a prime}}}\zeta_t\Big)$$
$$= \mathrm{N}_{\mathbb{Q}(\zeta_{mr/\ell})/F_{r/\ell}}\Big(1-\zeta_m\cdot\prod_{\substack{t\mid r,\,t\neq\ell\\ t\text{ is a prime}}}\zeta_t\Big)^{\mathrm{Fr}_\ell-1} = \xi_{r/l}^{\mathrm{Fr}_\ell-1}.$$

To prove the fourth property, consider the following diagram



As $\mathbb{Q}(\zeta_{mr/\ell})\cap F_r = F_{r/\ell}$, the restriction

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{mr})/F_r)\to\mathrm{Gal}(\mathbb{Q}(\zeta_{mr/\ell})/F_{r/\ell})$$

is surjective. Moreover $\zeta_\ell\equiv 1$ modulo each prime ideal of $\mathbb{Q}(\zeta_{mr})$ dividing ℓ and so

$$\xi_r\equiv\mathrm{N}_{\mathbb{Q}(\zeta_{mr})/F_r}\left(1-\zeta_m\cdot\prod_{\substack{t\mid r,\,t\neq\ell\\ t\text{ is a prime}}}\zeta_t\right)=\xi_{r/l}^{(\ell-1)/M}$$

modulo each prime ideal of F_r dividing ℓ. □

Lemma 1.2. — *For any $r\in\mathcal{S}_M$ the image of $\xi_r^{\mathrm{D}_r}$ in the quotient module $F_r^\times/(F_r^\times)^M$ is fixed by all elements of G_r, i.e.,*

$$\xi_r^{\mathrm{D}_r}\in\big(F_r^\times/(F_r^\times)^M\big)^{G_r}.$$

Proof. — Following the proof of Lemma 2.1 in [10], use induction on the number of primes dividing r; the statement is clear if $r=1$. Suppose that a prime $\ell\mid r$ and denote $s=\frac{r}{\ell}$. Then the third part of Lemma 1.1 implies

$$\xi_r^{\mathrm{D}_r(\sigma_\ell-1)}=\xi_r^{\mathrm{D}_s(M-\mathrm{N}_\ell)}=\big(\xi_r^{\mathrm{D}_s}\big)^M\cdot\xi_s^{(1-\mathrm{Fr}_\ell)\,\mathrm{D}_s}.$$

Since $\mathrm{Fr}_\ell \in G_s$, the induction hypothesis gives $\xi_s^{(1-\mathrm{Fr}_\ell)\,\mathrm{D}_s} \in (F_s^\times)^M$ and so $\xi_r^{\mathrm{D}_r(\sigma_\ell - 1)} \in (F_r^\times)^M$. The lemma follows as these σ_ℓ generate G_r. □

LEMMA 1.3. — *For any $r \in \mathcal{S}_M$ there is $\kappa_r \in F^\times$, uniquely defined modulo $(F^\times)^M$, such that $\kappa_r^{-1} \cdot \xi_r^{\mathrm{D}_r} \in (F_r^\times)^M$.*

Proof. — This can be proved in the same way as Lemma 2.2 in [10]. □

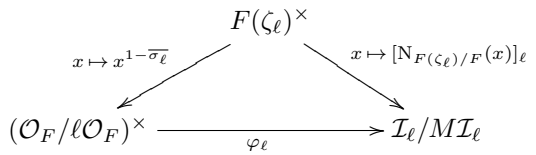
Let $\mathcal{O}_F$ denote the ring of integers of F, and write $\mathcal{I} = \oplus_\lambda \mathbb{Z}\lambda$ for the group of fractional ideals of F, written additively. For every rational prime p write $\mathcal{I}_p = \oplus_{\lambda|p}\mathbb{Z}\lambda$, so $\mathcal{I} = \oplus_p \mathcal{I}_p$. For any $y \in F^\times$ let $(y) \in \mathcal{I}$ be the principal ideal generated by y and $(y)_p \in \mathcal{I}_p$, $[y] \in \mathcal{I}/M\mathcal{I}$, $[y]_p \in \mathcal{I}_p/M\mathcal{I}_p$ the projections of (y). The projections $[y]$ and $[y]_p$ are well defined also for any $y \in F^\times/(F^\times)^M$. Denote $G = \mathrm{Gal}(F/\mathbb{Q})$.

For any prime $\ell \in \mathcal{S}_M$, each prime ideal λ of F above ℓ ramifies totally in $F(\zeta_\ell)/F$ and so there is a unique prime ideal λ' of $F(\zeta_\ell)$ above λ and we can identify $\mathcal{O}_{F(\zeta_\ell)}/\lambda'$ and $\mathcal{O}_F/\lambda$. This identification leads to a canonical isomorphism of G-modules

$$(\mathcal{O}_F/\ell\mathcal{O}_F)^\times \cong \oplus_{\lambda|\ell}(\mathcal{O}_{F(\zeta_\ell)}/\lambda')^\times$$

(G acts transitively on the summands on the right hand side). Let $\overline{\sigma_\ell}$ be a fixed generator of $\mathrm{Gal}(F(\zeta_\ell)/F)$ whose restriction to F_ℓ is σ_ℓ (it is easy to see that such a generator always exists). Since $\overline{\sigma_\ell}$ fixes each prime ideal of $F(\zeta_\ell)$ above ℓ, it is easy to see that $x^{1-\overline{\sigma_\ell}}$ is a unit modulo each of them for any $x \in F(\zeta_\ell)^\times$.

LEMMA 1.4. — *For any prime $\ell \in \mathcal{S}_M$ there is a unique surjective homomorphism of G-modules $\varphi_\ell\colon (\mathcal{O}_F/\ell\mathcal{O}_F)^\times \to \mathcal{I}_\ell/M\mathcal{I}_\ell$ such that the following diagram commutes*



Proof. — This is exactly Lemma 2.3 in [10]. □

The previous lemma gives the value $\varphi_\ell(\alpha)$ for each $\alpha \in \mathcal{O}_F$, $(\alpha)_\ell = 0$. This definition can be uniquely extended to a surjective homomorphism of G-modules $\varphi_\ell\colon \{\alpha \in F^\times;\, [\alpha]_\ell = 0\} \to \mathcal{I}_\ell/M\mathcal{I}_\ell$ satisfying $(F^\times)^M \subseteq \ker\varphi_\ell$.

PROPOSITION 1.5. — *Let $r \in \mathcal{S}_M$ and ℓ be any rational prime.*

(1) *If $\ell \nmid r$, and either $r > 1$ or m is not a power of ℓ, then $[\kappa_r]_\ell = 0$.*

(2) *If $\ell \mid r$ then*

$$\frac{\ell-1}{M}\cdot[\kappa_r]_\ell = \frac{\ell-1}{M}\cdot\varphi_\ell(\kappa_{r/\ell}).$$

Proof. — Due to the definition of κ_r in Lemma 1.3 there is $\beta_r \in F_r^\times$ satisfying $\xi_r^{\mathrm{D}_r} = \kappa_r\cdot\beta_r^M$. The second part of Lemma 1.1 states that ξ_r is a unit unless mr is a prime power, which can be the case only if m is a power of a prime q and $r=1$. But then ξ_r is a unit outside of prime ideals above q. In any case ξ_r is a unit at prime ideals above ℓ. If $\ell\nmid r$ then the prime ideals above ℓ are unramified in F_r/F, and so the valuation of κ_r at any prime ideal of F above ℓ is divisible by M.

Suppose that $\ell\mid r$ and put $s=\frac{r}{\ell}$. Since $[\kappa_s]_\ell=0$ and κ_s is well defined modulo $(F^\times)^M$, we can assume $(\kappa_s)_\ell=0$. There is $\beta_s\in F_s^\times$ satisfying $\xi_s^{\mathrm{D}_s}=\kappa_s\cdot\beta_s^M$, hence β_s is a unit at each prime ideal of F_s above ℓ. Any prime ideal λ of F_s above ℓ ramifies totally in F_r/F_s, and so there is a unique prime ideal λ' of F_r above λ and $\mathcal{O}_{F_r}/\lambda'$ and $\mathcal{O}_{F_s}/\lambda$ are canonically isomorphic. It is easy to see that σ_ℓ acts trivially on $\mathcal{O}_{F_r}/\lambda'$ and Fr_ℓ acts as ℓth power on $\mathcal{O}_{F_s}/\lambda$. Let Λ and Λ' be the prime ideals of F and F_ℓ below λ', respectively. The ramification index of Λ' above Λ is M, so the valuation $\nu_{\Lambda'}(\kappa_r)=M\cdot\nu_\Lambda(\kappa_r)$. There is $\gamma\in F_\ell^\times$ such that $\nu_{\Lambda'}(\gamma)=\nu_{\Lambda'}(\kappa_r)/M$ for each prime ideal Λ of F_ℓ above ℓ. Then $\nu_{\Lambda'}(\gamma^{-M}\kappa_r)=0$, which gives $\nu_{\lambda'}(\gamma^M\beta_r^M)=\nu_{\lambda'}(\gamma^M\kappa_r^{-1})=0$, and so $\nu_{\lambda'}(\gamma\beta_r)=0$. Therefore $\gamma\beta_r\in F_r^\times$ is a unit at each prime ideal of F_r above ℓ and $\gamma^{-M}\kappa_r\in F_\ell^\times$ is a unit at each prime ideal of F_ℓ above ℓ. The same can be said about $\gamma^{1-\sigma_\ell}$ and $\gamma^{\mathrm{N}_\ell-M}$ as σ_ℓ fixes these primes. Therefore $[\gamma^{\mathrm{N}_\ell}]_\ell=[\kappa_r]_\ell$. Both σ_ℓ and Fr_ℓ act trivially on F, so $\kappa_r^{\sigma_\ell-1}=\kappa_s^{\mathrm{Fr}_\ell-1}=1$. Hence the third part of Lemma 1.1 implies

$$\beta_r^{M(\sigma_\ell-1)}=\xi_r^{\mathrm{D}_r(\sigma_\ell-1)}=\xi_r^{\mathrm{D}_s(M-\mathrm{N}_\ell)}=\xi_r^{M\,\mathrm{D}_s}\cdot\xi_s^{\mathrm{D}_s(1-\mathrm{Fr}_\ell)}=\xi_r^{M\,\mathrm{D}_s}\cdot\beta_s^{M(1-\mathrm{Fr}_\ell)}.$$

Since F_r is real and M is odd, 1 is the only Mth root of unity in F_r, therefore

$$\beta_r^{\sigma_\ell-1}=\xi_r^{\mathrm{D}_s}\cdot\beta_s^{1-\mathrm{Fr}_\ell}.$$

As σ_ℓ acts trivially on $\mathcal{O}_{F_r}/\lambda'$, modulo λ' we have $(\gamma\beta_r)^{\sigma_\ell-1}\equiv 1$ and so

$$\gamma^{1-\sigma_\ell}\equiv\beta_r^{\sigma_\ell-1}=\xi_r^{\mathrm{D}_s}\cdot\beta_s^{1-\mathrm{Fr}_\ell}\equiv\xi_s^{\mathrm{D}_s(\ell-1)/M}\cdot\beta_s^{1-\ell}=\kappa_s^{(\ell-1)/M}$$

using the fourth part of Lemma 1.1. Finally, Lemma 1.4 gives

$$\begin{aligned}\frac{\ell-1}{M}\cdot\varphi_\ell(\kappa_s)&=\varphi_\ell(\kappa_s^{(\ell-1)/M})=\varphi_\ell(\gamma^{1-\sigma_\ell})=\varphi_\ell(\gamma^{1-\overline{\sigma_\ell}})=[\mathrm{N}_{F(\zeta_\ell)/F}(\gamma)]_\ell\\&=[\gamma^{\mathrm{N}_\ell(\ell-1)/M}]_\ell=\frac{\ell-1}{M}\cdot[\gamma^{\mathrm{N}_\ell}]_\ell=\frac{\ell-1}{M}\cdot[\kappa_r]_\ell.\end{aligned}$$

□

2. An application of the Čebotarev Theorem

Let us fix an odd prime number p and suppose that M is a large power of p. Let C be the p-part of the ideal class group of F, written additively. Let $\overline{F}$ denote the genus field of F in the narrow sense. Recall that $G = \mathrm{Gal}(F/\mathbb{Q})$.

ASSUMPTION 1. — *Assume that* $p \nmid \left[\left(\overline{F} \cap F(\zeta_{M^2})\right) : F\right]$.

Let us mention that Assumption 1 is satisfied for example if p ramifies in $F/\mathbb{Q}$ at most tamely or if $p \nmid [\mathbb{Q}(\zeta_m) : F]$.

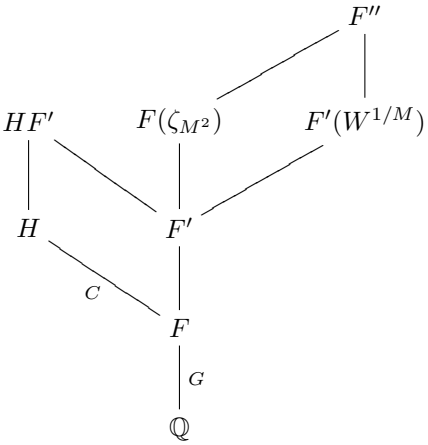
We shall prove the following modification of [10, Theorem 3.1]:

THEOREM 2.1. — *Suppose we are given a fixed* $\mathfrak{c} \in C$, *a finite* G*-submodule* W *of* $F^\times/(F^\times)^M$, *and a homomorphism of* G*-modules* $\psi\colon W \to (\mathbb{Z}/M\mathbb{Z})[G]$. *Then there are infinitely many prime ideals* λ *of* F *such that*

(1) $\lambda \in \mathfrak{c}$.
(2) $\ell \equiv 1 + M \pmod{M^2}$ *and* ℓ *splits completely in* $F/\mathbb{Q}$, *where* ℓ *is the rational prime below* λ.
(3) $[w]_\ell = 0$ *for all* $w \in W$, *and there is a unit* $u \in (\mathbb{Z}/M\mathbb{Z})^\times$ *such that* $\varphi_\ell(w) = u\psi(w)\lambda$ *for all* $w \in W$.

Proof. — Let H be the maximal unramified abelian p-extension of F, so that C is identified with $\mathrm{Gal}(H/F)$ by class field theory. Denote $F' = F(\zeta_M)$ and $F'' = F(\zeta_{M^2}, W^{1/M})$. Assumption 1 gives $H \cap F(\zeta_{M^2}) = F$. We want to show that the commutator subgroup of $\mathrm{Gal}(F''/F)$ is $\mathrm{Gal}(F''/F(\zeta_{M^2}))$. Let $\tau \in \mathrm{Gal}(F''/F)$ be the complex conjugation; then for any $\rho \in \mathrm{Gal}(F''/F(\zeta_{M^2}))$ we have $\rho\tau\rho^{-1}\tau = \rho^2$. But any element of the p-group $\mathrm{Gal}(F''/F(\zeta_{M^2}))$ is a square, so the commutator subgroup of $\mathrm{Gal}(F''/F)$ contains $\mathrm{Gal}(F''/F(\zeta_{M^2}))$. On the other hand $\mathrm{Gal}(F''/F)/\mathrm{Gal}(F''/F(\zeta_{M^2})) \cong \mathrm{Gal}(F(\zeta_{M^2})/F)$ is abelian. Therefore the largest subfield of F'' that is abelian over F is $F(\zeta_{M^2})$. Similarly, F' is the largest subfield of $F'(W^{1/M})$ that is abelian over F. Hence $F'(W^{1/M}) \cap F(\zeta_{M^2}) = F'$ and $F'' \cap H = F(\zeta_{M^2}) \cap H = F$.

We have the following diagram:



To continue let us follow Steps III and IV in [10, proof of Theorem 3.1]: the element $\gamma \in \mathrm{Gal}(F'(W^{1/M})/F')$ obtained in Step III is compatible with $\gamma' \in \mathrm{Gal}(F(\zeta_{M^2})/F)$ which sends ζ_{M^2} to $\zeta_{M^2}^{M+1}$. Hence there is $\delta \in \mathrm{Gal}(HF''/F)$ such that δ restricts to γ on $F'(W^{1/M})$, to γ' on $F(\zeta_{M^2})$, and to $\mathfrak{c}$ on H. The rest of the proof goes on the same lines as in [10], the chosen γ' guarantees furthermore $\ell \equiv 1 + M \pmod{M^2}$. □

3. The Sinnott module U

This section is devoted to a statement concerning a version of Sinnott's module U defined in [11], which is going to be used later in the present paper. We describe the statement now; for the proof we refer to [5]. We have to warn the reader that U is denoted U' in [5].

Let $T_1, \dots, T_v$ be finite abelian groups written multiplicatively, $v \geqslant 1$, and let

$$G = T_1 \times \cdots \times T_v$$

be their direct product. For any $N \subseteq I = \{1, \dots, v\}$ let $T_N = \prod_{i \in N} T_i \subseteq G$, so $T_I = G$ and $T_\emptyset = \{1\}$ by definition. For any $i \in I$ we fix any $\lambda_i \in T_{I-\{i\}}$, denote $t_i = |T_i|$, and define

$$I_i = \ker\bigl(\mathbb{Z}[G] \to \mathbb{Z}[G/\langle \lambda_i, T_i \rangle]\bigr),$$

the ideal of $\mathbb{Z}[G]$ generated by $1 - \lambda_i$ and $1 - g$ for all $g \in T_i$. For any $H \subseteq G$ let $s(H) = \sum_{h \in H} h \in \mathbb{Z}[G]$ and for any $N \subseteq I$ let

$$\rho_N = s(T_N) \cdot \prod_{i \in I - N} (1 - t_i^{-1} \lambda_i^{-1} s(T_i)) \in \mathbb{Q}[G].$$

Let U be the $\mathbb{Z}[G]$-submodule of $\mathbb{Q}[G]$ generated by all ρ_N, $N \subseteq I$. Then we have the following

THEOREM 3.1. — *Every* $\psi \in \mathrm{Hom}_{\mathbb{Z}[G]}\big(U, \mathbb{Z}[G]\big)$ *satisfies* $\psi(\rho_\emptyset) \in \prod_{i=1}^{v} I_i$.

Proof. — See [5, Theorem 1.1 (i)]. □

4. The choice of a specific field F

Let p be a fixed odd prime number. Let L be a real abelian field of conductor f such that the order of any $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ is a divisor of $p-1$. Hence each Dirichlet character of L can be viewed as $\mathbb{Z}_p$-valued. Let K be a cyclic field of absolute degree p^u, u being a positive integer, and let $p_1, \dots, p_s$ be all prime numbers that ramify in $K/\mathbb{Q}$. It is clear that $s \geqslant 1$.

ASSUMPTION 2. — *Assume that either $K/\mathbb{Q}$ is not wildly ramified (i.e., the ramified primes $p_1, \dots, p_s$ are different from p) or that K is the degree p^u subfield of the p^{u+1}th cyclotomic field.*[(2)]

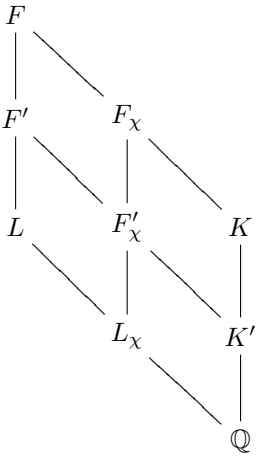
Thus the conductor of K is either the product $p_1 \dots p_s$ or p^{u+1}. Let $F = KL$ be the compositum of K and L. Again we denote $G = \mathrm{Gal}(F/\mathbb{Q})$. The conductor m of F equals the least common multiple of the conductors of L and K. It is easy to see that our F satisfies Assumption 1. Let σ be a fixed generator of $\mathrm{Gal}(F/L)$. Let K' be the subfield of K satisfying $[K : K'] = p$ and let $F' = K'L$. Let us fix a character χ of $H = \mathrm{Gal}(F/K)$, which we view as $\mathbb{Z}_p$-valued, and let

$$e_\chi = \frac{1}{|H|} \sum_{\tau \in H} \chi(\tau)\tau^{-1} \in \mathbb{Z}_p[H]$$

be the corresponding idempotent. Our choice of the character χ gives three more fields: let $L_\chi \subseteq L$ be the field corresponding to χ, *i.e.,* $\mathrm{Gal}(L/L_\chi) = \ker \chi$, and let $F_\chi = KL_\chi$ and $F'_\chi = K'L_\chi$ be its compositum with K

(2) We assume this because we want F to satisfy Assumption 1; the only wildly ramified cyclic field of degree p^u satisfying Assumption 1 is just the abelian field K of degree p^u and conductor p^{u+1}. We allow this K as even in this situation we can have nontrivial C_F: for example for $p = 3$, $u = 1$ and $L = \mathbb{Q}(\sqrt{43})$ we have $h_K = 1$, $h_L = 1$ and $h_F = 3$.

and K'.



For any abelian field R let C_R be the p-part of the ideal class group of R and let $C_{R,\chi} = e_\chi C_R$ be the corresponding eigenspace.

LEMMA 4.1. — *We have the following pairs of isomorphic G-modules:*

$$C_{F,\chi} \cong C_{F_\chi,\chi}, \quad C_{F',\chi} \cong C_{F'_\chi,\chi}.$$

Proof. — This can be easily proved as p does not divide the degree $[F : F_\chi] = [F' : F'_\chi]$. □

For any abelian field R let E_R and Cyc_R be the group of units and the Sinnott group of circular units, respectively. Let M be a power of the fixed prime p.

LEMMA 4.2. — *The following couples of G-modules are isomorphic:*

$$\begin{aligned}
\left(E_F/\,\mathrm{Cyc}_F\, E_F^M\right)^{e_\chi} &\cong \left(E_{F_\chi}/\,\mathrm{Cyc}_{F_\chi}\, E_{F_\chi}^M\right)^{e_\chi},\\
\left(E_F/\,\mathrm{Cyc}_F\, E_{F'} E_F^M\right)^{e_\chi} &\cong \left(E_{F_\chi}/\,\mathrm{Cyc}_{F_\chi}\, E_{F'_\chi} E_{F_\chi}^M\right)^{e_\chi},\\
\left(E_{F'}/\,\mathrm{Cyc}_{F'}\, E_{F'}^M\right)^{e_\chi} &\cong \left(E_{F'_\chi}/\,\mathrm{Cyc}_{F'_\chi}\, E_{F'_\chi}^M\right)^{e_\chi}.
\end{aligned}$$

Proof. — This is standard, just use the well-known fact that $\mathrm{Cyc}_{F_\chi} \subseteq \mathrm{Cyc}_F$ and $\mathrm{N}_{F/F_\chi}(\mathrm{Cyc}_F) \subseteq \mathrm{Cyc}_{F_\chi}$. □

For any abelian field R let $h_{R,p}$ be the p-part of the class number h_R of R, *i.e.*, $h_{R,p} = |C_R|$.

LEMMA 4.3. — *The p-parts of the indices of the groups of circular units are given by the following formulae*

$$[E_F : \mathrm{Cyc}_F]_p = h_{F,p} \cdot c_K, \qquad [E_K : \mathrm{Cyc}_K]_p = h_{K,p} \cdot c_K,$$

where $c_K = [K_1 : \mathbb{Q}] \cdot p^{-u}$ with K_1 being the maximal subfield of K such that at most one prime ramifies in $K_1/\mathbb{Q}$.

Proof. — This follows from Sinnott's results: [11, Theorem 5.3] says for both of these fields that the Sinnott index $(R : U)$ is not divisible by p as the p-part of the Galois group is cyclic. The lemma follows from [11, Theorem 4.1]. □

5. A simplification

For the field F chosen in Section 4 we want to prove Theorem 8.1, a relation between the cardinalities of the G-modules $C_{F,\chi}$, $C_{F',\chi}$, $\big(E_F/\operatorname{Cyc}_F E_{F'} E_F^M\big)^{e_\chi}$, and $\big(E_F/\operatorname{Cyc}_F E_F^M\big)^{e_\chi}$. Lemma 4.1 and Lemma 4.2 show that these cardinalities stay unchanged if we take L_χ instead of L. Therefore, fixing the character χ, which can be trivial, and without any loss of generality we can make the following simplifying

Assumption 3. — *Let us assume that $L = L_\chi$ and that the primes $p_1, \dots, p_s$ are indexed in such a way that $p_1, \dots, p_g$ split completely in $L/\mathbb{Q}$ while $p_{g+1}, \dots, p_s$ do not*[(3)] *(here $0 \leqslant g \leqslant s$). Moreover, assume that the conductor m of F is not a power of a prime (so $s > 1$ or χ is nontrivial).*

Recall that $\xi_1 = \kappa_1 = \mathrm{N}_{\mathbb{Q}(\zeta_m)/F}(1 - \zeta_m)$. Let $\rho = \sigma^{p^{u-1}}$ and $N' = \sum_{j=0}^{p-1} \rho^j$.

Lemma 5.1. — *Let M be a large power of p ($h_{F,p}|M$ suffices). Consider the tensor products $\overline{E_F} = E_F \otimes \mathbb{Z}_p$, $\overline{E_{F'}} = E_{F'} \otimes \mathbb{Z}_p$, $\overline{\operatorname{Cyc}_F} = \operatorname{Cyc}_F \otimes \mathbb{Z}_p$, and $\overline{\operatorname{Cyc}_{F'}} = \operatorname{Cyc}_{F'} \otimes \mathbb{Z}_p$.*

1. *The image of $\overline{\operatorname{Cyc}_F}$ in $\big(\overline{E_F}/\overline{E_{F'}}\big)^{e_\chi}$ is generated as a $\mathbb{Z}_p[\langle\sigma\rangle]$-module by the image $\xi_1^{e_\chi}$ of ξ_1.*
2. $\big|\big(\overline{E_F}/\overline{\operatorname{Cyc}_F}\big)^{e_\chi}\big| = \big|\big(\overline{E_F}/\overline{\operatorname{Cyc}_F}\,\overline{E_{F'}}\big)^{e_\chi}\big| \cdot \big|\big(\overline{E_{F'}}/\overline{\operatorname{Cyc}_{F'}}\big)^{e_\chi}\big|$.
3. $\big|\big(E_F/\operatorname{Cyc}_F E_F^M\big)^{e_\chi}\big| = \big|\big(E_F/\operatorname{Cyc}_F E_{F'} E_F^M\big)^{e_\chi}\big| \cdot \big|\big(E_{F'}/\operatorname{Cyc}_{F'} E_{F'}^M\big)^{e_\chi}\big|$.

Proof. — The Sinnott group Cyc_F of circular units of F is the intersection of the group $\mathcal{D}_F$ defined just below and of the group E_F of all units of F. (Remark: $\mathcal{D}_F$ is somewhat smaller than Sinnott's group D of circular

(3) We allow any behaviour of p_i for $i > g$; it can be (partially) inert or even (partially) ramified in $L/\mathbb{Q}$. Let us mention that we can have nontrivial $C_{F,\chi}$ even if $g = 0$ and $h_L = 1$. [Example: let $K = \mathbb{Q}(\theta)$ where $\theta^3 + \theta^2 - 576\theta + 1665 = 0$. Then K is an abelian cubic field of conductor $1729 = 7 \cdot 13 \cdot 19$. Let $L = \mathbb{Q}(\sqrt{11})$, then 7, 13, and 19 are all inert in L, $h_L = 1$, $h_K = 9$, and $h_F = 27$ (the nontrivial class groups are 3-elementary).]

numbers attached to F, in particular it does not contain $\mathbb{Q}^\times$ whereas D does. But after intersection with E_F we get the same group Cyc_F.) One can get a list of $\mathbb{Z}[G]$-module generators of $\mathcal{D}_F$ as follows: for each subfield $R \subseteq F$ of conductor $n > 1$ take the norm $\mathrm{N}_{\mathbb{Q}(\zeta_n)/R}(1-\zeta_n)$ and take all roots of unity of F, too. But in our situation each of these norms is killed by e_χ up to the cases when $L \subseteq R$. Moreover ± 1 (there are no other roots of unity) as well as the above mentioned norms for R's with $L \subseteq R \subsetneq F$ belong to $\mathcal{D}_{F'}$. The norm term for $R = F$ equals ξ_1. For any $\tau \in H$ we have $\tau e_\chi = \chi(\tau) e_\chi$ and the first statement of the lemma follows. Let $\delta = 1$ if χ is trivial and $\delta = 0$ otherwise. The existence of a Minkowski unit of F implies that $\overline{E_{F'}}^{e_\chi}$ and $\big(\overline{E_F}/\overline{E_{F'}}\big)^{e_\chi}$ are $\mathbb{Z}_p$-free modules of $\mathbb{Z}_p$-ranks $p^{u-1} - \delta$ and $(p-1)p^{u-1}$, respectively. Let $\eta_1, \dots, \eta_{p^{u-1}-\delta}$ be a $\mathbb{Z}_p$-basis of $\overline{\mathrm{Cyc}_{F'}}^{e_\chi}$. Since $\xi_1^{N'} \in \mathrm{Cyc}_{F'}$,

$$\{\eta_1, \dots, \eta_{p^{u-1}-\delta}\} \cup \big\{\xi_1^{e_\chi \sigma^{j-1}};\ j = 1, \dots, (p-1)p^{u-1}\big\} \tag{5.1}$$

forms a system of $\mathbb{Z}_p$-generators of $\overline{\mathrm{Cyc}_F}^{e_\chi}$. Comparing the $\mathbb{Z}_p$-ranks gives that this is in fact a $\mathbb{Z}_p$-basis of $\overline{\mathrm{Cyc}_F}^{e_\chi}$. Let

$$\varepsilon_1, \dots, \varepsilon_{p^u-\delta} \tag{5.2}$$

be a $\mathbb{Z}_p$-basis of $\overline{E_F}^{e_\chi}$ such that $\varepsilon_1, \dots, \varepsilon_{p^{u-1}-\delta}$ is a $\mathbb{Z}_p$-basis of $\overline{E_{F'}}^{e_\chi}$. Then

$$\{\varepsilon_1, \dots, \varepsilon_{p^{u-1}-\delta}\} \cup \big\{\xi_1^{e_\chi \sigma^{j-1}};\ j = 1, \dots, (p-1)p^{u-1}\big\}$$

is a $\mathbb{Z}_p$-basis of $(\overline{\mathrm{Cyc}_F}\,\overline{E_{F'}})^{e_\chi}$. The transition matrix from (5.2) to (5.1) is block triangular and the indices in question are given by its determinant and by the determinants of its two blocks on the diagonal. This implies the second statement of the lemma, and the third statement follows easily. □

For brevity, let us write C and C_χ instead of C_F and $C_{F,\chi}$, respectively.

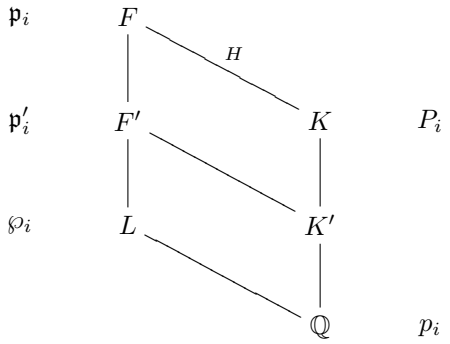
It is easy to see that C_χ is a $\mathbb{Z}_p[G]$-module whose number of elements is a power of p and where H acts via χ, *i.e.*, for any $\tau \in H$ and any $\mathfrak{c} \in C_\chi$ we have $\tau\mathfrak{c} = \chi(\tau)\mathfrak{c}$.

On one hand, each ideal I of F' generates an ideal $\mathcal{O}_F I$ of F, and this mapping gives the natural map $\iota : C_{F'} \to C$. Let $\iota_\chi : C_{F',\chi} \to C_\chi$ be its restriction to χ-components. We shall study the capitulation kernel $\ker \iota_\chi$.

On the other hand, the norm of ideals gives the map $\mathrm{N}_{F/F'} : C_\chi \to C_{F',\chi}$. Since F/F' is totally ramified at all primes above $p_1, \dots, p_s$ and $s \geqslant 1$, it is well-known (*e.g.* see [13, Theorem 10.1]) that $\mathrm{N}_{F/F'}$ is surjective. It is also well-known that $\iota_\chi \circ \mathrm{N}_{F/F'} : C_\chi \to C_\chi$ acts as N', so $\iota_\chi(C_{F',\chi}) = N'C_\chi$. Therefore we have

$$|C_{F',\chi}| = |N'C_\chi| \cdot |\ker \iota_\chi|.$$

For each $i = 1, \dots, s$ let n_i be the index of the decomposition group of p_i in $K/\mathbb{Q}$, so p_i is divisible by exactly n_i prime ideals of K. Let us fix one of them and call it P_i. Let $\wp_i$ be a fixed prime ideal of L above p_i. As the degrees $[K:\mathbb{Q}]$ and $[L:\mathbb{Q}]$ are relatively prime, this means that $\wp_i$ is divisible by exactly n_i prime ideals of F; let $\mathfrak{p}_i$ be the one of them which is divisible by P_i. Then $\mathfrak{p}_i$, $\sigma\mathfrak{p}_i$, $\dots$, $\sigma^{n_i-1}\mathfrak{p}_i$ is the complete list of prime ideals of F above $\wp_i$. Let $\mathfrak{p}'_i$ be the prime ideal of F' below $\mathfrak{p}_i$. Then $\mathfrak{p}'_i$ ramifies in F/F', so $\mathcal{O}_F\mathfrak{p}'_i = p \cdot \mathfrak{p}_i$ as ideals of F (recall that we write the group of fractional ideals additively).



Let $\mathcal{P}_i$ be the image of $\mathfrak{p}_i$ in C and $\overline{\mathcal{P}_i}$ its image in $C/N'C$. Since $p\mathcal{P}_i = N'\mathcal{P}_i \in N'C$, we have $p\overline{\mathcal{P}_i} = 0$. Let $\langle e_\chi \overline{\mathcal{P}_i}\rangle$ be the subgroup of $C_\chi/N'C_\chi$ generated by $e_\chi\overline{\mathcal{P}_i}$. For any $\tau \in H$ we have $\tau e_\chi \overline{\mathcal{P}_i} = \chi(\tau) e_\chi \overline{\mathcal{P}_i} \in \langle e_\chi \overline{\mathcal{P}_i}\rangle$, moreover $\sigma^{n_i}\overline{\mathcal{P}_i} = \overline{\mathcal{P}_i}$, and so

$$\langle e_\chi \overline{\mathcal{P}_i}\rangle_\sigma = \langle e_\chi \overline{\mathcal{P}_i}, \sigma e_\chi \overline{\mathcal{P}_i} \dots, \sigma^{n_i-1} e_\chi \overline{\mathcal{P}_i}\rangle \tag{5.3}$$

is the G-submodule of $C_\chi/N'C_\chi$ generated by $e_\chi\overline{\mathcal{P}_i}$. Hence the order of $\langle e_\chi \overline{\mathcal{P}_i}\rangle_\sigma$ divides p^{n_i}. If $i > g$ then the decomposition group of p_i in $\mathrm{Gal}(L/\mathbb{Q})$ is nontrivial; consider $\tau \neq 1$ in this decomposition group. We have $\tau\wp_i = \wp_i$ and so $\tau\mathfrak{p}_i = \mathfrak{p}_i$ and $\tau\mathcal{P}_i = \mathcal{P}_i$, which gives

$$(\chi(\tau) - 1) e_\chi \overline{\mathcal{P}_i} = \tau e_\chi \overline{\mathcal{P}_i} - e_\chi \overline{\mathcal{P}_i} = 0.$$

Assumption 3 implies that χ is injective on $\mathrm{Gal}(L/\mathbb{Q})$, hence $\chi(\tau) \not\equiv 1 \pmod{p\mathbb{Z}_p}$ and $e_\chi\overline{\mathcal{P}_i} = 0$. Thus

$$\langle e_\chi \overline{\mathcal{P}_1}, \dots, e_\chi \overline{\mathcal{P}_s}\rangle_\sigma = \langle e_\chi \overline{\mathcal{P}_1}, \dots, e_\chi \overline{\mathcal{P}_g}\rangle_\sigma$$

is a p-elementary G-submodule of $C_\chi/N'C_\chi$ whose order divides p^n, where $n = \sum_{i=1}^{g} n_i$ (see also Proposition 9.1 which says more about this order).

We shall work in the quotient of $C_\chi/N'C_\chi$ by this submodule, so we define

(5.4)
$$\overline{C}_\chi = (C_\chi/N'C_\chi)/\langle e_\chi\overline{\mathcal{P}_1},\dots,e_\chi\overline{\mathcal{P}_s}\rangle_\sigma = (C_\chi/N'C_\chi)/\langle e_\chi\overline{\mathcal{P}_1},\dots,e_\chi\overline{\mathcal{P}_g}\rangle_\sigma.$$

It is clear that its order $|\overline{C}_\chi| = p^k$ for a suitable non-negative integer k.

LEMMA 5.2. — *There are $\mathfrak{c}_1,\dots,\mathfrak{c}_k \in \overline{C}_\chi$ such that for each $i = 1,\dots,k$ the subgroup $\langle\overline{\mathfrak{c}_i}\rangle$ of $\overline{C}_\chi/\langle\mathfrak{c}_1,\dots,\mathfrak{c}_{i-1}\rangle$ generated by the image $\overline{\mathfrak{c}_i}$ of $\mathfrak{c}_i$ is a G-submodule of $\overline{C}_\chi/\langle\mathfrak{c}_1,\dots,\mathfrak{c}_{i-1}\rangle$ of order p.*

Proof. — As $\overline{C}_\chi$ is killed by N', it is a module over $\mathbb{Z}_p[\zeta_{p^u}]$, which is a discrete valuation ring. Hence $\overline{C}_\chi$, being a finite module over $\mathbb{Z}_p[\zeta_{p^u}]$, is a direct sum of submodules isomorphic to $\mathbb{Z}_p[\zeta_{p^u}]/\overline{\pi}^a\mathbb{Z}_p[\zeta_{p^u}]$, a being a positive integer and $\overline{\pi} = 1-\zeta_{p^u}$. Moreover H acts via χ, so only the action of σ is important. This representation as a direct sum directly implies the existence of a composition sequence with quotients all of order p, and we are done. □

6. Extracting roots

Retaining F and χ from the previous section, let us fix a large power M of p and assume

ASSUMPTION 4. — *Let r be a square-free positive integer such that each prime $\ell \mid r$ splits completely in $F/\mathbb{Q}$, satisfies $\ell \equiv 1 \pmod M$, and each prime $p_1,\dots,p_s$ is an M-th power modulo ℓ.*

Recall that F_r means the compositum of F and $\mathbb{Q}_r$ and that $F\cap\mathbb{Q}_r = \mathbb{Q}$. So there is an extension of σ to F_r whose restriction to $\mathbb{Q}_r$ is identity. By abuse of notation we denote this extension also by σ; still $\sigma^{p^u} = 1$. Let $\pi = 1-\sigma$, $N = \sum_{j=0}^{p^u-1}\sigma^j$ and $\Delta = \sum_{j=1}^{p^u-1} j\sigma^j$, so

$$\pi\cdot N = 0 \quad\text{and}\quad \pi\cdot\Delta = N - p^u.$$

Recall that $\rho = \sigma^{p^{u-1}}$ and $N' = \sum_{j=0}^{p-1}\rho^j$. Let $\pi_0 = 1-\rho$, then we have

$$\pi_0\cdot N' = 0 \quad\text{and}\quad \pi_0\cdot\Delta' = N' - p$$

for $\Delta' = \sum_{j=1}^{p-1} j\rho^j$. Moreover, recall that $\overline{\pi} = 1-\zeta_{p^u}$.

LEMMA 6.1. — *There is a unique ring homomorphism $\eta\colon \mathbb{Z}[\langle\sigma\rangle] \to \mathbb{Z}[\zeta_{p^u}]$ such that $\eta(\sigma) = \zeta_{p^u}$. This η is surjective, its kernel is $N'\mathbb{Z}[\langle\sigma\rangle]$, and η restricts to the following isomorphism of $\mathbb{Z}[\langle\sigma\rangle]$-modules*

$$\pi_0\mathbb{Z}[\langle\sigma\rangle] \cong \overline{\pi}^{p^{u-1}}\mathbb{Z}[\zeta_{p^u}].$$

For any nonzero $\delta \in \pi_0\mathbb{Z}[\langle\sigma\rangle]$ there is $y \in \{1,\dots,p-1\}$, an integer $x \geqslant 0$, and $z \in \mathbb{Z}[\langle\sigma\rangle]$ such that

$$\delta = \pi_0\pi^x(y + \pi z);$$

moreover x, y and $\pi_0 z$ are uniquely determined. If $\delta = \pi_0 p^t$ for a positive integer t then $x = t\varphi(p^u)$, where φ is the Euler totient function.

Proof. — Most of the lemma is easy to see. To prove the described decomposition of δ use the fact that there is a filtration of $\mathbb{Z}[\zeta_{p^u}]$ by powers of the ideal $\overline{\pi}\mathbb{Z}[\zeta_{p^u}]$ and that $p^t\mathbb{Z}[\zeta_{p^u}] = \overline{\pi}^{t\varphi(p^u)}\mathbb{Z}[\zeta_{p^u}]$. □

We shall need the following generalization of [4, Proposition 3.2]. In applications the polynomial $f(X)$ will be a monic divisor of $X^{p^u} - 1$.

Proposition 6.2. — *Let $f(X)$ be a polynomial in $\mathbb{Z}[X]$, $f(X) \notin \{0, \pm 1\}$, and let $R = \mathbb{Z}[X]/(f(X))$. Let $\mathcal{M}$ be a finitely generated R-module without $\mathbb{Z}$-torsion. Then*

1. $\mathrm{Ext}^1_R(\mathcal{M}, R) = 0$.
2. *Let y be a nonzerodivisor in R, and $x \in \mathcal{M}$. Then $x \in y\mathcal{M}$ if and only if for all $\varphi \in \mathrm{Hom}_R\big(\mathcal{M}, R\big)$ we have $\varphi(x) \in yR$.*

Proof. — Multiplication by a positive integer t on $\mathcal{M}$ gives the exact sequence

$$0 \longrightarrow \mathcal{M} \xrightarrow{\cdot t} \mathcal{M} \longrightarrow \mathcal{M}/t\mathcal{M} \longrightarrow 0,$$

and so

$$\mathrm{Ext}^1_R(\mathcal{M}, R) \xrightarrow{\cdot t} \mathrm{Ext}^1_R(\mathcal{M}, R) \longrightarrow \mathrm{Ext}^2_R(\mathcal{M}/t\mathcal{M}, R)$$

is also exact. The ring R is 1-dimensional and Gorenstein, since it was defined as $\mathbb{Z}[X]$ modulo $f(X)$, which is not a unit or zero. Hence the injective dimension of R is one (see [6, page 164, Exercise 17]) and $\mathrm{Ext}^2_R(\mathcal{M}/t\mathcal{M}, R) = 0$. But $\mathrm{Ext}^1_R(\mathcal{M}, R)$ is finitely generated over R, hence finitely generated over $\mathbb{Z}$, and multiplication by any positive integer is surjective. This implies the first part of the proposition.

In the second part, "only if" is obvious. For "if" let us argue indirectly: let $\overline{\mathcal{M}} = \mathcal{M}/y\mathcal{M}$, write $z \mapsto \overline{z}$ for the canonical map $\mathcal{M} \to \overline{\mathcal{M}}$, and assume that $\overline{x} \neq 0$. Then $\overline{\mathcal{M}}$ is a module over $\overline{R} = R/yR$, and $J = \mathrm{Ann}_{\overline{R}}\,\overline{x} \subsetneq \overline{R}$. There is a maximal ideal I of $\overline{R}$ containing J. Since $\overline{R}$ is commutative and Artinian, every simple module occurs as an ideal of $\overline{R}$. Fix a monomorphism $\overline{R}/I \to \overline{R}$. Composing with the obvious maps $R\overline{x} \to \overline{R}/J \to \overline{R}/I$, we obtain a map $\phi_0 : R\overline{x} \to \overline{R}$ with $\phi_0(\overline{x}) \neq 0$. Since the ring $\overline{R}$ is Gorenstein and zero-dimensional, it is self-injective, and so ϕ_0 is the restriction of some

$\phi_1 : \overline{\mathcal{M}} \to \overline{R}$. Let ϕ_2 be the composite of the canonical map $\mathcal{M} \to \overline{\mathcal{M}}$ and ϕ_1. The canonical exact sequence

$$0 \longrightarrow yR \longrightarrow R \xrightarrow{\pi} \overline{R} \longrightarrow 0$$

gives the exact sequence

$$\mathrm{Hom}_R(\mathcal{M}, R) \xrightarrow{\pi\circ} \mathrm{Hom}_R(\mathcal{M}, \overline{R}) \longrightarrow \mathrm{Ext}^1_R(\mathcal{M}, yR)\ .$$

Since y is a nonzerodivisor in R, we have $R \cong yR$ and the first part of the proposition gives $\mathrm{Ext}^1_R(\mathcal{M}, yR) = 0$. Therefore there is $\phi \in \mathrm{Hom}_R(\mathcal{M}, R)$ such that $\pi \circ \phi = \phi_2$. Then $\phi(x) \notin yR$ and we are done. □

The aim of the following section is to find an upper bound for $\frac{|C_X|}{|C_{F',\chi}|}$, which turns out to be the exact value later on. The following theorem plays a decisive role in this effort. Recall that n_j is the index of the decomposition group of p_j in $K/\mathbb{Q}$, that $H = \mathrm{Gal}(F/K)$, and define $\overline{K}$, $\overline{L}$, and $\overline{F}$ to be the genus field (in the narrow sense) of K, L, and F, respectively. So we have $\overline{F} = \overline{KL}$.

THEOREM 6.3. — *Assuming $g \geqslant 1$, let $n = \sum_{j=1}^{g} n_j$ and $e \in \mathbb{Z}[\mathrm{Gal}(F_r/\mathbb{Q})]$ belong to the augmentation ideal, i.e., $e \cdot \sum_{\tau\in\mathrm{Gal}(F_r/\mathbb{Q})} \tau = 0$. Then there is $\mu_1 \in F_r^\times$ such that*

$$\mu_1^{\prod_{j=1}^{g}(1-\sigma^{n_j})} = \xi_r^{[\overline{L}:L]e} \quad \textit{and} \quad \mu_1^{1-\sigma^{n'}} \in \mathrm{Cyc}_{\overline{K}L_r}, \tag{6.1}$$

where $n' = \max_{1\leqslant j\leqslant g} n_j$. Moreover, there is $\mu \in F_r^\times$ such that

$$\mu^{\pi_0\pi^n} = \xi_r^{[\overline{L}:L]e\pi_0} \quad \textit{and} \quad \mu^{\pi_0} \in \mathrm{Cyc}_{\overline{K}L_r}\ .$$

Proof. — For each $j \leqslant g$ Assumptions 3 and 4 imply the Frobenius automorphism of p_j to be trivial on L_r, so $\xi_r^N = \mathrm{N}_{F_r/L_r}(\xi_r) = 1$. If $s = 1$ then $g = 1$ and p_1 is totally ramified in $K/\mathbb{Q}$, so $n = n_1 = 1$. Hilbert's Theorem 90 gives $v \in F_r^\times$ such that $v^\pi = \xi_r$ and the theorem follows with $\mu = \mu_1 = v^{[\overline{L}:L]e}$.

In the rest of the proof we shall assume $s > 1$. Let $\mathcal{R}$ be the set of rational primes ramifying in F_r and $\widetilde{G} = \mathrm{Gal}(\overline{F}_r/\mathbb{Q})$ be the Galois group of the genus field $\overline{F}_r$ (in the narrow sense) of F_r. For each $q \in \mathcal{R}$ let T_q be the inertia group of q in $\widetilde{G}$ and $t_q = |T_q|$ be the ramification index of q in both F_r and $\overline{F}_r$. Then $\widetilde{G}$ is the direct product of T_q for q running over $\mathcal{R}$. For any $J \subseteq \mathcal{R}$ let $T_J = \prod_{q\in J} T_q$. We now consider the module U from Section 3 for these T_q, so $v = |\mathcal{R}|$, where for each $q \in \mathcal{R}$ we define the corresponding λ_q of Section 3 to be the Frobenius automorphism of q in

$T_{\mathcal{R}-\{q\}}$. Hence U is the $\mathbb{Z}[\widetilde{G}]$-module generated by

$$\rho_J = s(T_J) \cdot \prod_{i \in \mathcal{R}-J} (1 - t_i^{-1}\lambda_i^{-1} s(T_i)) \in \mathbb{Q}[\widetilde{G}]$$

for all $J \subseteq \mathcal{R}$. Let $n_{\mathcal{R}}$ be the conductor of both F_r and $\overline{F}_r$. For each $J \subseteq \mathcal{R}$ let n_J be the J-part of $n_{\mathcal{R}}$, *i.e.*, the greatest divisor of $n_{\mathcal{R}}$ divisible only by primes in J, and let $\zeta_J = \exp(\frac{2\pi i}{n_J})$ be the corresponding primitive n_J-th root of unity. Let us fix any $\tilde{e} \in \mathbb{Z}[\widetilde{G}]$ such that $\mathrm{res}_{\overline{F}_r/F_r}\, \tilde{e} = e$. We shall construct a map $\vartheta\colon U \to \mathrm{Cyc}_{\overline{F}_r}$ putting $\vartheta(\rho_{\mathcal{R}}) = 1$ and

$$\vartheta(\rho_J) = \mathrm{N}_{\mathbb{Q}(\zeta_{\mathcal{R}-J})/\overline{F}_r \cap \mathbb{Q}(\zeta_{\mathcal{R}-J})}(1 - \zeta_{\mathcal{R}-J})^{\tilde{e}}$$

for each $J \subsetneq \mathcal{R}$. Using [5, Cor. 1.6(i)] we see that ϑ is well-defined: it is enough to check that the images satisfy the relations

$$s(T_i) \cdot \rho_N = (1 - \lambda_i^{-1}) \cdot \rho_{N \cup \{i\}} \qquad \text{for each } N \subsetneq I,\ i \in I - N.$$

But this follows from the norm relations for circular units; note that $\tilde{e}$ is here to take care of the norms to $\mathbb{Q}$. Theorem 3.1 then gives that

$$\Psi(\vartheta(\rho_\emptyset)) \in \prod_{q \in \mathcal{R}} I_q \qquad \text{for each } \Psi \in \mathrm{Hom}_{\mathbb{Z}[\widetilde{G}]}(\mathrm{Cyc}_{\overline{F}_r}, \mathbb{Z}[\widetilde{G}]), \tag{6.2}$$

where $I_q = \ker\big(\mathbb{Z}[\widetilde{G}] \to \mathbb{Z}[\widetilde{G}/\langle \lambda_q, T_q\rangle]\big)$.

Consider any $\Psi_1 \in \mathrm{Hom}_{\mathbb{Z}[\mathrm{Gal}(L\overline{K}_r/\mathbb{Q})]}\big(\mathrm{Cyc}_{L\overline{K}_r}, \mathbb{Z}[\mathrm{Gal}(L\overline{K}_r/\mathbb{Q})]\big)$ and use (6.2) for $\Psi = \mathrm{cor}_{\overline{F}_r/L\overline{K}_r} \circ \Psi_1 \circ \mathrm{N}_{\overline{F}_r/L\overline{K}_r}$ to obtain

$$\mathrm{cor}_{\overline{F}_r/L\overline{K}_r}\, \Psi_1\big(\mathrm{N}_{\mathbb{Q}(\zeta_{\mathcal{R}})/L\overline{K}_r}(1 - \zeta_{\mathcal{R}})^{\tilde{e}}\big) \in \prod_{q \in \mathcal{R}} I_q$$

which gives

$$\Psi_1\big(\mathrm{N}_{\mathbb{Q}(\zeta_{\mathcal{R}})/L\overline{K}_r}(1 - \zeta_{\mathcal{R}})^{[\overline{L}:L]\tilde{e}}\big) \in \prod_{q \in \mathcal{R}} \mathrm{res}_{\overline{F}_r/L\overline{K}_r}\, I_q \tag{6.3}$$

since $\mathrm{res}_{\overline{F}_r/L\overline{K}_r}\, \mathrm{cor}_{\overline{F}_r/L\overline{K}_r}\, x = [\overline{L} : L]x$ for any $x \in \mathbb{Z}[\mathrm{Gal}(L\overline{K}_r/\mathbb{Q})]$.

For brevity, let $e' = [\overline{L} : L]e$. Now we shall use the "lowering the top field" argument to show that

$$\Psi_2\big(\mathrm{N}_{\mathbb{Q}(\zeta_{\mathcal{R}})/F_r}(1 - \zeta_{\mathcal{R}})^{e'}\big) \in \prod_{q \in \mathcal{R}} \mathrm{res}_{\overline{F}_r/F_r}\, I_q \tag{6.4}$$

for each $\Psi_2 \in \mathrm{Hom}_{\mathbb{Z}[\mathrm{Gal}(F_r/\mathbb{Q})]}\big(\mathrm{Cyc}_{L\overline{K}_r} \cap F_r, \mathbb{Z}[\mathrm{Gal}(F_r/\mathbb{Q})]\big)$. Let us fix any such Ψ_2 and consider the corresponding $\Psi_2^1 \in \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Cyc}_{L\overline{K}_r} \cap F_r, \mathbb{Z})$, where $\Psi_2^1(u)$ means the coefficient of $1 \in \mathrm{Gal}(F_r/\mathbb{Q})$ in $\Psi_2(u)$. There is no $\mathbb{Z}$-torsion in $\mathrm{Cyc}_{L\overline{K}_r}/(\mathrm{Cyc}_{L\overline{K}_r} \cap F_r)$. Indeed, if $\varepsilon \in \mathrm{Cyc}_{L\overline{K}_r}$ satisfies $\varepsilon^n \in F_r$ for a positive integer n then $(\varepsilon^{1-\tau})^n = 1$ for each $\tau \in \mathrm{Gal}(L\overline{K}_r/F_r)$; but

$L\overline{K}_r$ is a real field, so this means $(\varepsilon^{1-\tau})^2 = 1$ and already $\varepsilon^2 \in F_r$. Then $\varepsilon \in F_r$, otherwise the degree $[L\overline{K}_r : F_r] = [\overline{K} : K]$, which is a power of p, would be even. Therefore there is $\psi \in \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Cyc}_{L\overline{K}_r}, \mathbb{Z})$ such that $\psi(\varepsilon) = \Psi_2^1(\varepsilon)$ for each $\varepsilon \in \mathrm{Cyc}_{L\overline{K}_r} \cap F_r$. Define

$$\Psi_1(\varepsilon) = \sum_{\tau \in \mathrm{Gal}(L\overline{K}_r/\mathbb{Q})} \psi(\varepsilon^\tau)\tau^{-1}$$

for each $\varepsilon \in \mathrm{Cyc}_{L\overline{K}_r}$. Then $\Psi_1 \in \mathrm{Hom}_{\mathbb{Z}[\mathrm{Gal}(L\overline{K}_r/\mathbb{Q})]}\big(\mathrm{Cyc}_{L\overline{K}_r}, \mathbb{Z}[\mathrm{Gal}(L\overline{K}_r/\mathbb{Q})]\big)$ and so it satisfies (6.3). But for any $\varepsilon \in \mathrm{Cyc}_{L\overline{K}_r}$ we have

$$\begin{aligned}
\mathrm{res}_{L\overline{K}_r/F_r}\,\Psi_1(\varepsilon) &= \sum_{\tau \in \mathrm{Gal}(L\overline{K}_r/\mathbb{Q})} \psi(\varepsilon^\tau)\,\mathrm{res}_{L\overline{K}_r/F_r}\,\tau^{-1} \\
&= \sum_{\tau \in \mathrm{Gal}(F_r/\mathbb{Q})} \psi\big(\mathrm{N}_{L\overline{K}_r/F_r}(\varepsilon)^\tau\big)\tau^{-1} \\
&= \sum_{\tau \in \mathrm{Gal}(F_r/\mathbb{Q})} \Psi_2^1\big(\mathrm{N}_{L\overline{K}_r/F_r}(\varepsilon)^\tau\big)\tau^{-1} = \Psi_2\big(\mathrm{N}_{L\overline{K}_r/F_r}(\varepsilon)\big).
\end{aligned}$$

This equality for $\varepsilon = \mathrm{N}_{\mathbb{Q}(\zeta_{\mathcal{R}})/L\overline{K}_r}(1-\zeta_{\mathcal{R}})^{[\overline{L}:L]\tilde{e}}$ gives that (6.4) follows from (6.3).

For each $j = 1, \dots, g$ the prime p_j splits completely in L_r due to Assumptions 3 and 4, hence $\mathrm{res}_{\overline{F}_r/F_r}\, I_{p_j} = (1-\sigma^{n_j})\mathbb{Z}[\mathrm{Gal}(F_r/\mathbb{Q})]$. Note that ξ_r is a conjugate of $\mathrm{N}_{\mathbb{Q}(\zeta_{\mathcal{R}})/F_r}(1-\zeta_{\mathcal{R}})$, hence (6.4) implies

$$\Psi_2\big(\xi_r^{e'}\big) \in \left(\prod_{j=1}^{g}(1-\sigma^{n_j})\right)\mathbb{Z}[\mathrm{Gal}(F_r/\mathbb{Q})] \tag{6.5}$$

for each $\Psi_2 \in \mathrm{Hom}_{\mathbb{Z}[\mathrm{Gal}(F_r/\mathbb{Q})]}\big(\mathrm{Cyc}_{L\overline{K}_r} \cap F_r, \mathbb{Z}[\mathrm{Gal}(F_r/\mathbb{Q})]\big)$.

Let $\Gamma = \mathrm{Gal}(F_r/L_r) = \langle\sigma\rangle$; then $\mathrm{Gal}(F_r/\mathbb{Q})$ is the direct product of Γ and $\mathrm{Gal}(F_r/K)$ and so $\mathbb{Z}[\mathrm{Gal}(F_r/\mathbb{Q})] = \mathbb{Z}[\Gamma][\mathrm{Gal}(F_r/K)]$. Let us consider any $\psi \in \mathrm{Hom}_{\mathbb{Z}[\Gamma]}\big(\mathrm{Cyc}_{L\overline{K}_r} \cap F_r, \mathbb{Z}[\Gamma]\big)$ and for each $\varepsilon \in \mathrm{Cyc}_{L\overline{K}_r} \cap F_r$ define

$$\Psi_2(\varepsilon) = \sum_{\tau \in \mathrm{Gal}(F_r/K)} \psi(\varepsilon^\tau)\tau^{-1}.$$

Then $\Psi_2 \in \mathrm{Hom}_{\mathbb{Z}[\mathrm{Gal}(F_r/\mathbb{Q})]}\big(\mathrm{Cyc}_{L\overline{K}_r} \cap F_r, \mathbb{Z}[\mathrm{Gal}(F_r/\mathbb{Q})]\big)$ and so it satisfies (6.5). This implies that

$$\psi(\xi_r^{e'}) \in \left(\prod_{j=1}^{g}(1-\sigma^{n_j})\right)\mathbb{Z}[\Gamma] \tag{6.6}$$

for any $\psi \in \mathrm{Hom}_{\mathbb{Z}[\Gamma]}\big(\mathrm{Cyc}_{L\overline{K}_r} \cap F_r, \mathbb{Z}[\Gamma]\big)$.

After all these algebraic preliminaries we now proceed to the extraction of roots. Recall that $n' = \max_{1\leqslant j\leqslant g} n_j$. Without any loss of generality we can suppose that $n_1 = n'$. Then $n_1 \mid p^u$ and $n_1 < p^u$. Let $f(X) = 1 + X^{n_1} + X^{2n_1} + \cdots + X^{p^u - n_1}$. Then

$$R = \mathbb{Z}[\Gamma]/(f(\sigma)) \cong \mathbb{Z}[X]/(f(X))$$

and $\mathcal{M} = \{\varepsilon \in \mathrm{Cyc}_{L\overline{K}_r} \cap F_r;\ \varepsilon^{f(\sigma)} = 1\}$ is an R-module without $\mathbb{Z}$-torsion. It is easy to see that $f(\sigma)$ acts as the norm from F_r to its subfield having degree n_1 over L_r. Since p_1 splits completely in this subfield and ramifies in F_r, we have $\xi_r \in \mathcal{M}$. Moreover, $(\mathrm{Cyc}_{L\overline{K}_r} \cap F_r)/(\pm\mathcal{M})$ has no $\mathbb{Z}$-torsion, too. Indeed, if $\varepsilon \in \mathrm{Cyc}_{L\overline{K}_r} \cap F_r$ satisfies $\pm\varepsilon^a \in \mathcal{M}$ for a positive integer a then $\varepsilon^{af(\sigma)} = \pm 1$ and so $\varepsilon^{f(\sigma)} = \pm 1$ since F_r is real, which means $\pm\varepsilon \in \mathcal{M}$ because $(-1)^{f(\sigma)} = -1$.

Let us fix any $\varphi \in \mathrm{Hom}_R\big(\mathcal{M}, R\big)$. Since the linear map

$$\psi : R \to (1 - \sigma^{n_1})\mathbb{Z}[\Gamma]$$

determined by $\psi(1+(f(\sigma))) = 1-\sigma^{n_1}$ is an isomorphism of R-modules, $\psi\circ\varphi$ can be understood as an element of $\mathrm{Hom}_{\mathbb{Z}[\Gamma]}\big(\mathcal{M}, \mathbb{Z}[\Gamma]\big)$, so we can extend it to $\tilde{\varphi} \in \mathrm{Hom}_{\mathbb{Z}[\Gamma]}\big(\pm\mathcal{M}, \mathbb{Z}[\Gamma]\big)$ just setting $\tilde{\varphi}(-1) = 0$. The first part of Proposition 6.2 (for $f(X) = X^{p^u} - 1$) gives $\mathrm{Ext}^1_{\mathbb{Z}[\Gamma]}\big((\mathrm{Cyc}_{L\overline{K}_r} \cap F_r)/(\pm\mathcal{M}), \mathbb{Z}[\Gamma]\big) = 0$. Hence $\tilde{\varphi}$ can be enlarged to $\bar{\varphi} \in \mathrm{Hom}_{\mathbb{Z}[\Gamma]}\big(\mathrm{Cyc}_{L\overline{K}_r} \cap F_r, \mathbb{Z}[\Gamma]\big)$ and (6.6) implies that

$$\bar{\varphi}(\xi_r^{e'}) \in \left(\prod_{j=1}^{g}(1 - \sigma^{n_j})\right)\mathbb{Z}[\Gamma].$$

This means that $\varphi(\xi_r^{e'}) \in yR$, where $y = \prod_{j=2}^{g}(1 - \sigma^{n_j})$. We can apply the second part of Proposition 6.2 to get $\mu_0 \in \mathcal{M}$ satisfying $\mu_0^y = \xi_r^{e'}$. Since $\mu_0 \in \mathcal{M}$, we have $\mu_0^{f(\sigma)} = 1$ and Hilbert's Theorem 90 gives $\mu_1 \in F_r$ such that $\mu_1^{1-\sigma^{n_1}} = \mu_0$. Thus $\mu_1^{(1-\sigma^{n_1})y} = \mu_0^y = \xi_r^{e'}$ and (6.1) follows since $n' = n_1$. The isomorphism $\eta\colon \pi_0\mathbb{Z}[\langle\sigma\rangle] \to \overline{\pi}^{p^{u-1}}\mathbb{Z}[\zeta_{p^u}]$ (see Lemma 6.1) allows to see easily that $\pi_0(1-\sigma^{n_j})$ is associated to $\pi_0\pi^{n_j}$. As $n = \sum_{j=1}^{g} n_j$, we therefore obtain $v \in \mathbb{Z}[\Gamma]$ such that $v\pi_0\pi^n = \pi_0\prod_{j=1}^{g}(1 - \sigma^{n_j})$. Let $\mu = \mu_1^v$, then $\mu^{\pi_0\pi^n} = \mu_1^{v\pi_0\pi^n} = \xi_r^{e'\pi_0}$. But $n_1 \mid p^{u-1}$ and so

$$\pi_0 = 1 - \sigma^{p^{u-1}} = (1 - \sigma^{n_1})(1 + \sigma^{n_1} + \cdots + \sigma^{p^{u-1}-n_1}),$$

hence $\mu^{\pi_0} = \mu_1^{v\pi_0} = \mu_0^{v(1+\sigma^{n_1}+\cdots+\sigma^{p^{u-1}-n_1})} \in \mathcal{M}$. Theorem 6.3 is proved. □

Lemma 6.4. — *Let t be a non-negative integer and $b \in F^\times$. If there is $u \in F_r^\times$ such that $b = u^{\pi_0\pi^t}$ then there is $v \in F^\times$ satisfying $b = v^{\pi_0\pi^t}$.*

Proof. — We prove this by induction on t: if $t = 0$ then $b = u^{\pi_0}$, so $b^{N'} = 1$. Hilbert's Theorem 90 implies the existence of $v \in F^\times$ satisfying $b = v^{\pi_0}$. Assume that $t \geqslant 1$ and that the lemma has been proved for $t-1$. Again $b^N = u^{N\cdot\pi_0\pi^t} = 1$ and Hilbert's Theorem 90 gives $w \in F^\times$ satisfying $b = w^\pi$. Let $d = u^{\pi_0\pi^{t-1}} \cdot w^{-1}$. Then $d \in F_r^\times$ and

$$d^\pi = u^{\pi_0\pi^t} \cdot w^{-\pi} = b \cdot b^{-1} = 1,$$

and so

$$d^{p^u} = d^N = u^{N\cdot\pi_0\pi^{t-1}} \cdot w^{-N} = w^{-N} \in F^\times.$$

But $d \in F_r$, $\zeta_p \notin F_r$, and F_r/F is a Galois extension, hence $d \in F$. Then $b_1 = u^{\pi_0\pi^{t-1}} = dw \in F^\times$ and the induction hypothesis gives $v \in F^\times$ satisfying $b_1 = v^{\pi_0\pi^{t-1}}$. Therefore $b = u^{\pi_0\pi^t} = b_1^\pi = v^{\pi_0\pi^t}$. □

7. The inductive procedure

Let us fix a large power M of p (later on we shall see that the assumption $p^n \mid M$ and $p^3 \cdot h_{F,p}^2 \mid M$ suffices). Using Theorem 2.1 for the field F satisfying Assumption 3 for a *nontrivial* character χ, we shall successively construct prime ideals $\lambda_1, \ldots, \lambda_k$ of F and each prime ideal λ_i will give a prime number ℓ_i divisible by λ_i such that

(7.1) the ideal class containing λ_i maps to $\mathfrak{c}_i \in \overline{C}_\chi$ (see Lemma 5.2),

(7.2) ℓ_i splits completely in $F/\mathbb{Q}$,

(7.3) $\ell_i \equiv 1 + M \pmod{M^2}$,

(7.4) p_j is an M-th power modulo ℓ_i for each $j = 1, \ldots, s$.

For any $i = 0, 1, \ldots, k$ let $r_i = \prod_{j=1}^{i} \ell_j$. Let us fix such an i and suppose that prime ideals $\lambda_1, \ldots, \lambda_i$ have been already obtained, which is satisfied for $i = 0$ at the beginning, of course. As we know r_i, we can use ξ_{r_i} defined just prior to Lemma 1.1 and κ_{r_i} defined in Lemma 1.3. If $i < k$ we shall obtain λ_{i+1} during this step of the inductive procedure.

Let us choose and fix $e'_\chi \in \mathbb{Z}[H]$ such that

$$e'_\chi \equiv e_\chi \pmod{M\mathbb{Z}_p[H]} \quad \text{and} \quad e'_\chi \cdot \sum_{\tau\in H} \tau = 0. \tag{7.5}$$

This is always possible as χ is nontrivial. Let t_i be the largest non-negative integer such that there is $\alpha_i \in F^\times$ satisfying

$$\alpha_i^{\pi_0\pi^{t_i}} \cdot \kappa_{r_i}^{e'_\chi\pi_0} \in (F^\times)^M. \tag{7.6}$$

We must show that t_i is well-defined by this. It is clear that $\alpha_i = \kappa_{r_i}^{-e'_\chi}$ satisfies this condition for $t_i = 0$. But we need to know that this condition cannot be satisfied by all integers t_i if M is chosen large enough. (If M were too small, for example if $M = 1$, then for any positive integer t_i one could take $\alpha_i = 1$.) We prove it now for $i = 0$; later on we shall see that t_i is well-defined also for the other $0 < i \leqslant k$.

LEMMA 7.1. — *If M is a large power of p ($M > h_{F,p}$ suffices) then the integer t_0 is well defined by (7.6) and $t_0 < v\varphi(p^u)$, where $p^v = p \cdot h_{F,p}$.*

Proof. — Similarly as in Lemma 5.1 we shall work in the tensor products with $\mathbb{Z}_p$ to be able to apply the idempotent e_χ directly to units. Part 1 of Lemma 5.1 says that the image of $\overline{\mathrm{Cyc}_F}$ in $\big(\overline{E_F}/\overline{E_{F'}}\big)^{e_\chi}$ is generated as a $\mathbb{Z}_p[\langle\sigma\rangle]$-module by the image $\xi_1^{e_\chi}$ of $\xi_1 = \kappa_1$. Lemma 4.3 implies that this image of $\overline{\mathrm{Cyc}_F}$ is a $\mathbb{Z}_p[\langle\sigma\rangle]$-submodule of $\big(\overline{E_F}/\overline{E_{F'}}\big)^{e_\chi}$ of finite index and that this index divides $h_{F,p}$. Therefore for any integer $t \geqslant v-1$, the cardinality of $\big(E_F/\langle\xi_1\rangle_\sigma E_{F'} E_F^{p^t}\big)^{e_\chi}$ is independent of t, so

$$\big|\big(E_F/\langle\xi_1\rangle_\sigma E_{F'} E_F^{p^{v-1}}\big)^{e_\chi}\big| = \big|\big(E_F/\langle\xi_1\rangle_\sigma E_{F'} E_F^{p^{v}}\big)^{e_\chi}\big|. \tag{7.7}$$

We already mentioned in the proof of Lemma 5.1 that the $\mathbb{Z}_p$-rank of the $\mathbb{Z}_p$-free module $\big(\overline{E_F}/\overline{E_{F'}}\big)^{e_\chi}$ equals $\varphi(p^u)$. Hence

$$\big|\big(E_{F'} E_F^{p^{v-1}}/E_{F'} E_F^{p^{v}}\big)^{e_\chi}\big| = p^{\varphi(p^u)}. \tag{7.8}$$

Assume that (7.6) is satisfied for $t_0 \geqslant v\varphi(p^u)$, *i.e.*, there is $\alpha \in F^\times$ such that

$$\alpha^{\pi_0 \pi^{v\varphi(p^u)}} \cdot \xi_1^{e'_\chi \pi_0} \in (F^\times)^M.$$

Lemma 6.1 gives the existence of $z \in \mathbb{Z}[\langle\sigma\rangle]$ such that

$$\pi_0 \pi^{v\varphi(p^u)} = p^v \pi_0 z.$$

As $p^v \mid M$, we have $\xi_1^{e'_\chi \pi_0} \in (F^\times)^{p^v}$. Then $\xi_1^{e'_\chi \pi_0} \in E_F^{p^v}$ and so

$$\xi_1^{e'_\chi (N'-p)} = \xi_1^{e'_\chi \pi_0 \Delta'} \in E_F^{p^v}.$$

We have $\xi_1^{N'} \in E_{F'}$ which gives $\xi_1^{e'_\chi p} \in E_{F'} E_F^{p^v}$. This means that the image of $\xi_1^{e'_\chi}$ is of order 1 or p in $\big(E_F/E_{F'}E_F^{p^v}\big)^{e_\chi}$ and

$$\big|\big(E_F/E_{F'}E_F^{p^v}\big)^{e_\chi}\big| = \big|\big(E_F/\langle\xi_1\rangle_\sigma E_{F'}E_F^{p^v}\big)^{e_\chi}\big| \cdot d_v$$

for a suitable integer $d_v \mid p^{p^{u-1}}$, since $\xi_1^{e'_\chi \pi_0} \in E_F^{p^v}$. Similarly the image of $\xi_1^{e'_\chi}$ is of order 1 or p in $\big(E_F/E_{F'}E_F^{p^{v-1}}\big)^{e_\chi}$ and

$$\big|\big(E_F/E_{F'}E_F^{p^{v-1}}\big)^{e_\chi}\big| = \big|\big(E_F/\langle\xi_1\rangle_\sigma E_{F'}E_F^{p^{v-1}}\big)^{e_\chi}\big| \cdot d_{v-1}$$

for a suitable integer $d_{v-1} \mid p^{p^{u-1}}$. Then (7.7) gives

$$d_{v-1}^{-1} \cdot \left|\left(E_F/E_{F'}E_F^{p^{v-1}}\right)^{e_\chi}\right| = d_v^{-1} \cdot \left|\left(E_F/E_{F'}E_F^{p^v}\right)^{e_\chi}\right|,$$

which contradicts (7.8). The lemma is proved. □

Remark 7.2. — Recall that we are using an inductive procedure for $i = 0, 1, \ldots, k$. Thus now we can assume that $t_0 < v\varphi(p^u), \ldots, t_i < v\varphi(p^u)$ are all well defined, when we show that also $t_{i+1} < v\varphi(p^u)$ is well defined (see Lemma 7.5). Recall that $n = \sum_{j=1}^{g} n_j$.

LEMMA 7.3. — *If $p^n \mid M$ then we have $t_i \geqslant n$.*

Proof. — If $n = 0$ then there is nothing to prove, so assume $n \geqslant 1$. To simplify our notation write $r = r_i$. The definition of κ_r in Lemma 1.3 gives $\beta_r \in F_r^\times$ such that $\kappa_r = \xi_r^{\mathrm{D}_r} \cdot \beta_r^{-M}$. Lemma 6.1 gives the existence of $z \in \mathbb{Z}[\langle\sigma\rangle]$ such that

$$\pi_0 M = \pi_0 \pi^{n\varphi(p^u)} \cdot Mp^{-n} \cdot z.$$

Let $e = \sum_{\tau\in H}(1-\tau)$, Theorem 6.3 gives $\mu \in F_r^\times$ satisfying $\xi_r^{[\overline{L}:L]e\pi_0} = \mu^{\pi_0\pi^n}$, so

$$\kappa_r^{[\overline{L}:L]e\pi_0} = \xi_r^{[\overline{L}:L]e\pi_0\,\mathrm{D}_r} \cdot \beta_r^{-M[\overline{L}:L]e\pi_0} = (\mu^{\mathrm{D}_r} \cdot \beta_r^{-Mp^{-n}[\overline{L}:L]ez\pi^{n(\varphi(p^u)-1)}})^{\pi_0\pi^n}.$$

Since $\kappa_r \in F^\times$, Lemma 6.4 gives $v \in F^\times$ satisfying $v^{\pi_0\pi^n} = \kappa_r^{[\overline{L}:L]e\pi_0}$. We have

$$[\overline{L} : L]e = [\overline{L} : \mathbb{Q}] \cdot (1 - e_{\chi_0}),$$

where χ_0 means the trivial character on H. Since p does not divide $[\overline{L} : \mathbb{Q}]$, there is an integer c such that $c \cdot [\overline{L} : \mathbb{Q}] \equiv 1 \pmod{M}$. Then

$$e'_\chi \equiv e_\chi = (1 - e_{\chi_0})e_\chi \equiv c[\overline{L} : L]ee_\chi \equiv c[\overline{L} : L]ee'_\chi \pmod{M\mathbb{Z}[H]}.$$

Hence

$$(v^{-ce'_\chi})^{\pi_0\pi^n} \cdot \kappa_r^{e'_\chi\pi_0} = \kappa_r^{\pi_0(e'_\chi - c[\overline{L}:L]ee'_\chi)} \in (F^\times)^M.$$

This identity and the definition of t_i by (7.6) give $t_i \geqslant n$. □

LEMMA 7.4. — *Let W_i be the G-submodule of $F^\times/(F^\times)^M$, where $G = \mathrm{Gal}(F/\mathbb{Q})$, generated by the images of $\alpha_i^{e'_\chi\pi_0\pi^{t_i}}$ and of all primes $p_1, \ldots, p_s$. Then W_i is finite and there is a homomorphism of G-modules $\psi_i\colon W_i \to (\mathbb{Z}/M\mathbb{Z})[G]$ satisfying*

$$\psi_i(p_j) = 0 \qquad \text{for each } j = 1, \ldots, s, \text{ and}$$
$$\psi_i\left(\alpha_i^{e'_\chi\pi_0\pi^{t_i}}\right) = e_\chi\pi_0\pi^{t_i}.$$

Proof. — As an abelian group, W_i is finitely generated and annihilated by M, so W_i is finite. We must show that such a map ψ_i really exists. Assuming that $a \in \mathbb{Q}^\times$, $b \in F^\times$, and $\beta \in \mathbb{Z}[G]$ satisfy

$$\alpha_i^{e'_\chi \pi_0 \pi^{t_i} \beta} = a \cdot b^M$$

we need to prove that $e'_\chi \pi_0 \pi^{t_i} \beta$ is divisible by M in $\mathbb{Z}[G]$. As $(e'_\chi)^2 \equiv e_\chi^2 = e_\chi \equiv e'_\chi \pmod{M\mathbb{Z}_p[G]}$, we have $(e'_\chi)^2 \equiv e'_\chi \pmod{M\mathbb{Z}[G]}$, and so there is $b_1 \in F^\times$ such that

$$\alpha_i^{e'_\chi \pi_0 \pi^{t_i} \beta} = a^{e'_\chi} \cdot b_1^M.$$

Since $e'_\chi \cdot \sum_{\tau \in H} \tau = 0$, the augmentation map sends e'_χ to zero, and so $a^{e'_\chi} = 1$. For each $\beta \in \mathbb{Z}[G]$ there is $\beta' \in \mathbb{Z}_p[\langle\sigma\rangle]$ such that $\beta e_\chi = \beta' e_\chi$. Taking $\beta'' \in \mathbb{Z}[\langle\sigma\rangle]$ such that $\beta'' \equiv \beta' \pmod{M\mathbb{Z}_p[\langle\sigma\rangle]}$ we have $\beta e'_\chi \equiv \beta e_\chi = \beta' e_\chi \equiv \beta'' e'_\chi \pmod{M\mathbb{Z}_p[G]}$ and so $\beta e'_\chi \equiv \beta'' e'_\chi \pmod{M\mathbb{Z}[G]}$. Hence there is $b_2 \in F^\times$ such that

$$\alpha_i^{e'_\chi \pi_0 \pi^{t_i} \beta''} = b_2^M,$$

so we have

$$1 = \alpha_i^{e'_\chi \pi_0 \pi^{t_i} \beta'' N'} = b_2^{MN'}.$$

As $\zeta_p \notin F$, this implies $b_2^{N'} = 1$ and Hilbert's Theorem 90 guarantees the existence of $c \in F^\times$ such that $b_2 = c^{\pi_0}$. We have obtained

$$\alpha_i^{e'_\chi \pi_0 \pi^{t_i} \beta''} = c^{M\pi_0} \tag{7.9}$$

and we want to prove $\pi_0 \pi^{t_i} \beta'' \in M\mathbb{Z}[\langle\sigma\rangle]$. If $\pi_0 \beta'' = 0$ then there is nothing to prove, so assume $\pi_0 \beta'' \neq 0$.

Let us apply Lemma 6.1 to $M\pi_0$ and $\pi_0 \beta''$. If $M = p^t$ then

$$M\pi_0 = \pi_0 \pi^{t\varphi(p^u)}(y_1 + \pi z_1), \tag{7.10}$$

$$\pi_0 \beta'' = \pi_0 \pi^{x_2}(y_2 + \pi z_2), \tag{7.11}$$

where $x_2 \geqslant 0$ is an integer, $y_1, y_2 \in \{1, \dots, p-1\}$, and $z_1, z_2 \in \mathbb{Z}[\langle\sigma\rangle]$. It is easy to see that $(y_2 + \overline{\pi}\eta(z_2))$ and (M) are principal ideals of $\mathbb{Z}[\zeta_{p^u}]$ with relatively prime norms, and so there are $v_1, v_2 \in \mathbb{Z}[\zeta_{p^u}]$ such that

$$(y_2 + \overline{\pi}\eta(z_2))v_1 + Mv_2 = 1$$

and v_1 is not divisible by $\overline{\pi}$, so $v_1 = y_3 + \overline{\pi}w$ for $y_3 \in \{1, \dots, p-1\}$ and $w \in \mathbb{Z}[\zeta_{p^u}]$. Using the surjectivity of η we obtain that for suitable $z_3, z'_3 \in \mathbb{Z}[\langle\sigma\rangle]$ we have

$$(y_2 + \pi z_2)(y_3 + \pi z_3) \equiv 1 - Mz'_3 \pmod{N'\mathbb{Z}}.$$

Exactly in the same way we can prove the existence of $y_4 \in \{1, \dots, p-1\}$ and $z_4, z_4' \in \mathbb{Z}[\langle\sigma\rangle]$ satisfying

$$(y_1 + \pi z_1)(y_4 + \pi z_4) \equiv 1 - Mz_4' \pmod{N'\mathbb{Z}}. \tag{7.12}$$

Therefore

$$\pi_0 \pi^{t_i} \beta''(y_3 + \pi z_3) = \pi_0 \pi^{x_2 + t_i}(1 - Mz_3').$$

Acting on (7.9) by $y_3 + \pi z_3$ we get

$$c^{M\pi_0(y_3+\pi z_3)} = \alpha_i^{e_\chi' \pi_0 \pi^{t_i} \beta''(y_3+\pi z_3)} = \alpha_i^{e_\chi' \pi_0 \pi^{x_2+t_i}(1-Mz_3')},$$

and so

$$\alpha_i^{e_\chi' \pi_0 \pi^{x_2+t_i}} = \left(\alpha_i^{e_\chi' \pi^{x_2+t_i} z_3'} \cdot c^{y_3+\pi z_3}\right)^{M\pi_0}.$$

Define

$$c_1 = \left(\alpha_i^{e_\chi' \pi^{x_2+t_i} z_3'} \cdot c^{y_3+\pi z_3}\right)^{y_1+\pi z_1} \in F^\times$$

and (7.10) gives

$$\alpha_i^{e_\chi' \pi_0 \pi^{x_2+t_i}} = c_1^{\pi_0 \pi^{t\varphi(p^u)}}. \tag{7.13}$$

If $\gamma \in F^\times$ satisfies $\gamma^{\pi^2} = 1$ then $\gamma^{1-\sigma} = 1$. Indeed, $\gamma^{\pi^2} = 1$ implies that $g = \gamma^{1-\sigma} \in L^\times$, and so $\gamma^\sigma = \gamma \cdot g^{-1}$, which gives $\gamma = \gamma^{\sigma^{p^u}} = \gamma \cdot g^{-p^u}$ and $g^{p^u} = 1$ resulting in $g = 1$ as $\zeta_p \notin L$. Applying this fact to (7.13) we get that if $t\varphi(p^u) > x_2$ then

$$\alpha_i^{e_\chi' \pi_0 \pi^{t_i}} = c_1^{\pi_0 \pi^{t\varphi(p^u)-x_2}}.$$

The definition of t_i by (7.6) gives

$$c_1^{\pi_0 \pi^{t\varphi(p^u)-x_2}} \cdot \kappa_{r_i}^{e_\chi' \pi_0} \in (F^\times)^M,$$

hence $t_i \geqslant t\varphi(p^u) - x_2$. Notice that this inequality holds true in the other case $t\varphi(p^u) \leqslant x_2$ as well. Hence in both cases $x = t_i - t\varphi(p^u) + x_2 \geqslant 0$ and (7.11) gives

$$\begin{aligned} \pi_0 \pi^{t_i} \beta'' &= \pi_0 \pi^{x_2+t_i}(y_2 + \pi z_2) \\ &= \pi_0 \pi^{x+t\varphi(p^u)}(y_2 + \pi z_2). \end{aligned}$$

Using (7.12) and (7.10) we obtain

$$\begin{aligned} (1 - Mz_4')\pi_0 \pi^{t_i} \beta'' &= (1 - Mz_4')\pi_0 \pi^{x+t\varphi(p^u)}(y_2 + \pi z_2) \\ &= (y_1 + \pi z_1)(y_4 + \pi z_4)\pi_0 \pi^{x+t\varphi(p^u)}(y_2 + \pi z_2) \\ &= M\pi_0 \pi^x (y_2 + \pi z_2)(y_4 + \pi z_4), \end{aligned}$$

and so $\pi_0 \pi^{t_i} \beta''$ is divisible by M. □

If $i < k$ then we choose an ideal class $\mathfrak{c} \in C$ which maps to $\mathfrak{c}_{i+1} \in \overline{C}_\chi$. Theorem 2.1 for this $\mathfrak{c}$, the G-module W_i and the homomorphism ψ_i described in Lemma 7.4 gives a prime ideal λ_{i+1} of F such that the prime number ℓ_{i+1} divisible by λ_{i+1} satisfies (7.1), (7.2), and (7.3). Moreover $[w]_{\ell_{i+1}} = 0$ for all $w \in W_i$, and there is a unit $u_i \in (\mathbb{Z}/M\mathbb{Z})^\times$ such that

$$\varphi_{\ell_{i+1}}(w) = u_i \psi_i(w) \lambda_{i+1} \tag{7.14}$$

for all $w \in W_i$.

For each $j = 1, \dots, s$ we have $p_j \in W_i$ and $\psi_i(p_j) = 0$. Recall that $\overline{\sigma_{\ell_{i+1}}}$ is a fixed generator of $\mathrm{Gal}(F(\zeta_{\ell_{i+1}})/F)$. There is a positive integer y satisfying $\zeta_{\ell_{i+1}}^{y^{\overline{\sigma_{\ell_{i+1}}}}} = \zeta_{\ell_{i+1}}$, then y is a primitive root modulo ℓ_{i+1}. Take $1 - \zeta_{\ell_{i+1}}^y$ and consider its images in the diagram of Lemma 1.4. The left hand mapping sends $1 - \zeta_{\ell_{i+1}}^y$ to the class of

$$\left(1 - \zeta_{\ell_{i+1}}^y\right)^{1-\overline{\sigma_{\ell_{i+1}}}} = \frac{1 - \zeta_{\ell_{i+1}}^y}{1 - \zeta_{\ell_{i+1}}} \equiv y \pmod{1 - \zeta_{\ell_{i+1}}}$$

and the right hand mapping sends $1 - \zeta_{\ell_{i+1}}^y$ to $[\ell_{i+1}]_{\ell_{i+1}}$, hence

$$\varphi_{\ell_{i+1}}(y) = [\ell_{i+1}]_{\ell_{i+1}}.$$

Let us choose a positive integer a such that $p_j \equiv y^a \pmod{\ell_{i+1}}$, then

$$a[\ell_{i+1}]_{\ell_{i+1}} = a\varphi_{\ell_{i+1}}(y) = \varphi_{\ell_{i+1}}(y^a) = \varphi_{\ell_{i+1}}(p_j) = u_i \psi_i(p_j) \lambda_{i+1} = 0,$$

and so $M \mid a$, because ℓ_{i+1} splits completely in F. We have proved that ℓ_{i+1} satisfies (7.4).

Lemma 7.5. — *Let M be a large power of p ($M > h_{F,p}^2$ suffices) then the integer t_{i+1} is well defined by (7.6) and $t_{i+1} \leqslant t_i - 1$.*

Proof. — Let us assume that there is $\alpha \in F^\times$ such that

$$\alpha^{\pi_0 \pi^{t_i}} \cdot \kappa_{r_{i+1}}^{e'_\chi \pi_0} \in (F^\times)^M. \tag{7.15}$$

The lemma will be proved if we find a contradiction.

Since $(e'_\chi)^2 \equiv e'_\chi \pmod{M\mathbb{Z}[H]}$, (7.6) and (7.15) give

$$\varphi_{\ell_{i+1}}\left(\kappa_{r_i}^{e'_\chi \pi_0}\right) = -\varphi_{\ell_{i+1}}\left(\alpha_i^{e'_\chi \pi_0 \pi^{t_i}}\right),$$
$$\left[\kappa_{r_{i+1}}^{e'_\chi \pi_0}\right] = -\left[\alpha^{e'_\chi \pi_0 \pi^{t_i}}\right] = -e'_\chi \pi_0 \pi^{t_i}[\alpha].$$

The congruence (7.3) and Proposition 1.5 give

$$[\kappa_{r_{i+1}}] = \varphi_{\ell_{i+1}}(\kappa_{r_i}) + \sum_{j=1}^{i} [\kappa_{r_{i+1}}]_{\ell_j},$$

so (7.14) and Lemma 7.4 give

$$e'_\chi\pi_0\pi^{t_i}\Big([\alpha]-\sum_{j=1}^{i}[\alpha]_{\ell_j}\Big)=-\varphi_{\ell_{i+1}}\big(\kappa_{r_i}^{e'_\chi\pi_0}\big)=\varphi_{\ell_{i+1}}\big(\alpha_i^{e'_\chi\pi_0\pi^{t_i}}\big)$$
$$=u_i\psi_i\big(\alpha_i^{e'_\chi\pi_0\pi^{t_i}}\big)\lambda_{i+1}=u_ie'_\chi\pi_0\pi^{t_i}\lambda_{i+1}\in\mathcal{I}/M\mathcal{I}.$$

As u_i is a unit in $\mathbb{Z}/M\mathbb{Z}$, there is an integer v_i such that

$$v_ie'_\chi\pi_0\pi^{t_i}\Big([\alpha]-\sum_{j=1}^{i}[\alpha]_{\ell_j}\Big)=e'_\chi\pi_0\pi^{t_i}\lambda_{i+1}\in\mathcal{I}/M\mathcal{I}.$$

Denoting again $p^v=p\cdot h_{F,p}$, our assumption gives that M is divisible by p^{2v-1}. Hence there is $J\in\mathcal{I}$ such that we have the following identity in $\mathcal{I}$

$$p^{2v-1}J=e'_\chi\pi_0\pi^{t_i}\Big(v_i\Big((\alpha)-\sum_{j=1}^{i}(\alpha)_{\ell_j}\Big)-\lambda_{i+1}\Big).$$

Since multiplying by N' kills the right hand side, we have $N'J=0$, which means that there is $J'\in\mathcal{I}$ such that $J=\pi_0J'$. Lemma 6.1 gives that

$$p^{2v-1}J=p^{2v-1}\pi_0J'=h_{F,p}\pi_0\pi^{v\varphi(p^u)}J''$$

for a suitable $J''\in\mathcal{I}$ and Remark 7.2 says that $t_i<v\varphi(p^u)$. Having any $I\in\mathcal{I}$, it is easy to see that $\pi^2I=0$ implies $\pi I=0$. As $\pi\mid\pi_0$, we have $\pi_0I=0$ for

$$I=e'_\chi\lambda_{i+1}-v_ie'_\chi\Big((\alpha)-\sum_{j=1}^{i}(\alpha)_{\ell_j}\Big)+h_{F,p}\pi^{v\varphi(p^u)-t_i}J''.$$

The property $\pi_0I=0$ means that I can be written as a sum of an ideal supported on ramified prime ideals in F/F' and of the extension of a suitable ideal of F'. But such an extension belongs to $N'C$ and its image in $C/N'C$ is trivial. Similarly the image of any ramified prime ideal in $\overline{C}_\chi$ is trivial due to the construction in (5.4). The ideals $h_{F,p}J''$ and (α) have trivial image in C and we have obtained the following identity in $\overline{C}_\chi$

$$e'_\chi\lambda_{i+1}+v_ie'_\chi\sum_{j=1}^{i}(\alpha)_{\ell_j}=0.$$

The construction of $\mathfrak{c}_1,\dots,\mathfrak{c}_i$ accomplished in Lemma 5.2 and the property (7.1) imply that the image of $\sum_{j=1}^{i}(\alpha)_{\ell_j}$ belongs to $\langle\mathfrak{c}_1,\dots,\mathfrak{c}_i\rangle$, thus

$$e'_\chi\lambda_{i+1}=0$$

in $\overline{C}_\chi/\langle\mathfrak{c}_1,\dots,\mathfrak{c}_i\rangle$, which together with (7.1) contradicts Lemma 5.2. □

The following crucial inequality will be used in Proposition 7.10 to show that the size of $\left(E_F/\operatorname{Cyc}_F E_{F'}E_F^{M'}\right)^{e_\chi}$ dominates $\frac{|C_\chi|}{|C_{F',\chi}|}$.

COROLLARY 7.6. — *If $p^n \mid M$ and $M > h_{F,p}^2$ then we have $t_0 \geqslant k+n$.*

Proof. — This immediately follows from Lemma 7.3 using Lemma 7.5. □

LEMMA 7.7. — *Let M' be a large power of p ($M' > h_{F,p}$ suffices) and suppose that $e'_\chi \in \mathbb{Z}[H]$ satisfies $e'_\chi \equiv e_\chi \pmod{pM'\mathbb{Z}_p[H]}$. If there is $\varepsilon \in E_F$ such that*

$$\varepsilon^{\pi_0\pi^t} \cdot \xi_1^{e'_\chi \pi_0} \in E_F^{pM'} \tag{7.16}$$

for a positive integer t then p^t is a divisor of $\left|\left(E_F/\operatorname{Cyc}_F E_{F'}E_F^{M'}\right)^{e_\chi}\right|$.

Proof. — We have already mentioned in the proof of Lemma 7.1 that the $\mathbb{Z}_p$-rank of the $\mathbb{Z}_p$-free module $\left(\overline{E_F}/\overline{E_{F'}}\right)^{e_\chi}$ equals $\varphi(p^u)$. So we have

$$\left|\left(E_F/E_{F'}E_F^{M'}\right)^{e_\chi}\right| = (M')^{\varphi(p^u)} > h_{F,p} \geqslant \left|\left(E_F/\operatorname{Cyc}_F E_{F'}E_F^{M'}\right)^{e_\chi}\right| \tag{7.17}$$

due to Lemma 4.3. We have a $\mathbb{Z}[\langle\sigma\rangle]$-module homomorphism

$$\omega\colon \mathbb{Z}[\langle\sigma\rangle] \to \left(E_F/E_{F'}E_F^{M'}\right)^{e_\chi}$$

determined by $\omega(1) = \varepsilon^{e'_\chi} \cdot E_{F'}E_F^{M'}$. Then $\omega(N') = \varepsilon^{N'e'_\chi} \cdot E_{F'}E_F^{M'} = 1 \cdot E_{F'}E_F^{M'}$ as $\varepsilon^{N'} \in E_{F'}$. So the kernel of ω is a $\mathbb{Z}[\langle\sigma\rangle]$-submodule (so an ideal) of $\mathbb{Z}[\langle\sigma\rangle]$ containing $N'\mathbb{Z}[\langle\sigma\rangle]$ and its index is a power of p. Since $\mathbb{Z}[\langle\sigma\rangle]/N'\mathbb{Z}[\langle\sigma\rangle] \cong \mathbb{Z}[\zeta_{p^u}]$ with $\sigma \mapsto \zeta_{p^u}$, this ω gives a homomorphism

$$\omega'\colon \mathbb{Z}[\zeta_{p^u}] \to \left(E_F/E_{F'}E_F^{M'}\right)^{e_\chi}$$

and $\ker\omega'$ is an ideal of $\mathbb{Z}[\zeta_{p^u}]$ of p-power index, so $\ker\omega' = \overline{\pi}^r\mathbb{Z}[\zeta_{p^u}]$ for a suitable integer $r \geqslant 0$. Let us denote $x = \varepsilon^{e'_\chi\pi^t} \cdot \xi_1^{e'_\chi} \in E_F$, then (7.16) gives $x^{N'-p} = x^{\pi_0\Delta'} \in E_F^{pM'}$. Therefore there is $y \in E_F$ such that $x^{N'-p} = y^{pM'}$ and so $x^{N'} = z^p$ with $z = x \cdot y^{M'}$. Then $z^p \in F'$ which implies $z \in F'$, so $z \in E_{F'}$. Then $x = z \cdot y^{-M'} \in E_{F'}E_F^{M'}$. We have

$$\begin{aligned}\omega'(1) = \omega(1) &= \varepsilon^{e'_\chi} \cdot E_{F'}E_F^{M'},\\ \omega'(\overline{\pi}^t) = \omega(\pi^t) &= \varepsilon^{e'_\chi\pi^t} \cdot E_{F'}E_F^{M'} = \xi_1^{-e'_\chi} \cdot E_{F'}E_F^{M'}.\end{aligned}$$

Using Part 1 of Lemma 5.1 we see that the rows of the following diagram are exact.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \overline{\pi}^t\mathbb{Z}[\zeta_{p^u}]/\overline{\pi}^r\mathbb{Z}[\zeta_{p^u}] & \xrightarrow{\omega'} & (E_F/E_{F'}E_F^{M'})^{e_\chi} & \longrightarrow & (E_F/\mathrm{Cyc}_F\, E_{F'}E_F^{M'})^{e_\chi} & \longrightarrow & 0 \\
 & & \subseteq\downarrow & & =\downarrow & & \delta\downarrow & & \\
0 & \longrightarrow & \mathbb{Z}[\zeta_{p^u}]/\overline{\pi}^r\mathbb{Z}[\zeta_{p^u}] & \xrightarrow{\omega'} & (E_F/E_{F'}E_F^{M'})^{e_\chi} & \longrightarrow & (E_F/\langle\varepsilon^{e'_\chi}\rangle_\sigma E_{F'}E_F^{M'})^{e_\chi} & \longrightarrow & 0
\end{array}$$

The first row and the inequality (7.17) give $r > t$. The snake lemma implies

$$|\ker\delta| = |\mathbb{Z}[\zeta_{p^u}]/\overline{\pi}^t\mathbb{Z}[\zeta_{p^u}]| = p^t$$

and the lemma follows. □

For any $a \in F^\times$ we define the ambiguous part $\mathrm{amb}(a)$ to be the projection of the principal ideal $(a) \in \mathcal{I}$ to $\oplus_{j=1}^s(\mathcal{I}_{p_j}/p\mathcal{I}_{p_j})$, where $\mathcal{I}_{p_j}$ means the group of fractional ideals of F supported on the prime ideals of F dividing p_j, written additively.

LEMMA 7.8. — *If $a \in (F')^\times$ then $\mathrm{amb}(a) = 0$. For any positive integer t and any $b, c \in F^\times$ such that*

$$b^{\pi_0\pi^{(t-1)\varphi(p^u)}} = c^{p^t}$$

we have $\mathrm{amb}(b) = 0$.

Proof. — Each $\mathfrak{p}_j$ ramifies totally in F/F', and so $\mathrm{amb}(a) = 0$. If

$$b^{\pi_0\pi^{(t-1)\varphi(p^u)}} = c^{p^t}$$

then $c^{N'p^t} = 1$, so $c^{N'} = 1$ and Hilbert's Theorem 90 gives $d \in F^\times$ such that $c = d^{\pi_0}$. If $t = 1$ then $(bd^{-p})^{\pi_0} = 1$ and so $bd^{-p} \in (F')^\times$. Thus

$$\mathrm{amb}(b) = \mathrm{amb}(bd^{-p}) + p\,\mathrm{amb}(d) = 0.$$

Suppose $t > 1$. Lemma 6.1 gives

$$b^{\pi_0\pi^{(t-1)\varphi(p^u)}} = d^{\pi_0 p^t} = d^{p\pi_0\pi^{(t-1)\varphi(p^u)}(y+\pi z)}$$

for $y \in \{1, \dots, p-1\}$ and $z \in \mathbb{Z}[\langle\sigma\rangle]$. We know that if $\gamma \in F^\times$ satisfies $\gamma^{\pi^2} = 1$ then $\gamma^\pi = 1$ (see the reasoning below (7.13)) and $\pi \mid \pi_0$ implies

$$b^{\pi_0} = \left(d^{\pi_0(y+\pi z)}\right)^p.$$

The lemma follows from the proven case $t = 1$. □

Recall that $\iota_\chi : C_{F',\chi} \to C_\chi$ is given by extension of ideals and that (7.6) for $i = 0$ reads

$$\alpha_0^{\pi_0\pi^{t_0}} \cdot \xi_1^{e'_\chi\pi_0} \in (F^\times)^M. \tag{7.18}$$

Even though (7.18) only states that we can extract the $\pi_0\pi^{t_0}$-th root of $\xi_1^{-e'_\chi\pi_0}$ approximately (*i.e.*, modulo an M-th power in F), the following proposition says that this actually produces an exact $\pi_0\pi^{t_0}$-th root β of $\xi_1^{-e'_\chi\pi_0}$ in F.

PROPOSITION 7.9. — *Let M be a large power of p ($M > p^{2v} = p^2 \cdot h_{F,p}^2$ suffices; recall that v was defined by this equality) and r be the greatest divisor of h_F which is relatively prime to p, i.e., $h_F = r \cdot h_{F,p}$. We can choose and fix $\delta \in F^\times$ satisfying*

$$\alpha_0^{\pi_0\pi^{t_0}} \cdot \xi_1^{e'_\chi\pi_0} = \delta^{p^{v+1}\pi_0\pi^{v\varphi(p^u)}} \tag{7.19}$$

and denote $\beta = \alpha_0 \cdot \delta^{-p^{v+1}\pi^{v\varphi(p^u)-t_0}}$; then $\beta^{\pi_0\pi^{t_0}} = \xi_1^{-e'_\chi\pi_0}$, so $\beta^{\pi^{t_0}} \cdot \xi_1^{e'_\chi} \in F'$ and the ideal $(\beta^{\pi^{t_0}}) \in \mathcal{I}$ is the extension of a principal ideal of F'. Let a and b be the smallest non-negative integers such that $(\beta^{e'_\chi r\pi^a}) \in \mathcal{I}$ is the extension of a principal ideal of F' and $\pi^b \cdot \mathrm{amb}(\alpha_0) = 0$. We have

(1) $0 \leqslant b \leqslant a \leqslant t_0$;
(2) p^{t_0-a} *is a divisor of* $\left|\left(E_F/\operatorname{Cyc}_F E_{F'}E_F^M\right)^{e_\chi}\right|$;
(3) $|\langle e_\chi\overline{\mathcal{P}_1},\dots,e_\chi\overline{\mathcal{P}_s}\rangle_\sigma| = |\langle e_\chi\overline{\mathcal{P}_1},\dots,e_\chi\overline{\mathcal{P}_g}\rangle_\sigma|$ *is a divisor of* p^{n-b};
(4) p^{a-b} *divides* $|\ker\iota_\chi|$.

Proof. — We have $p^{2v+1} \mid M$. To start with, let us mention that α_0 is not determined by (7.18). Nevertheless $\mathrm{amb}(\alpha_0)$ is well defined. Indeed, if both α_0 and $\tilde{\alpha}_0$ satisfy (7.18) then

$$\left(\frac{\tilde{\alpha}_0}{\alpha_0}\right)^{\pi_0\pi^{t_0}} \in (F^\times)^M.$$

Lemma 7.1 gives $t_0 < v\varphi(p^u)$, hence

$$\left(\frac{\tilde{\alpha}_0}{\alpha_0}\right)^{\pi_0\pi^{v\varphi(p^u)}} \in (F^\times)^{p^{v+1}}$$

and Lemma 7.8 gives $\mathrm{amb}(\alpha_0) = \mathrm{amb}(\tilde{\alpha}_0)$. Since $(e'_\chi)^2 \equiv e'_\chi \pmod{M\mathbb{Z}[H]}$, we obtain from (7.18)

$$\alpha_0^{e'_\chi\pi_0\pi^{t_0}} \cdot \xi_1^{e'_\chi\pi_0} \in (F^\times)^M. \tag{7.20}$$

Comparing with (7.18), we see that

$$\mathrm{amb}(\alpha_0) = \mathrm{amb}(\alpha_0^{e'_\chi}). \tag{7.21}$$

We know from (7.18) that there is $\gamma \in F^\times$ such that

$$\alpha_0^{\pi_0\pi^{t_0}} \cdot \xi_1^{e'_\chi\pi_0} = \gamma^{p^{2v+1}}.$$

Hence $\gamma^{p^{2v+1}N'}=1$, which implies $\gamma^{N'}=1$, and by Hilbert's Theorem 90 there is $\gamma_0\in F^\times$ such that $\gamma=\gamma_0^{\pi_0}$. Lemma 6.1 gives $y\in\{1,\dots,p-1\}$ and $z\in\mathbb{Z}[\langle\sigma\rangle]$ such that

$$p^v\pi_0=\pi_0\pi^{v\varphi(p^u)}(y+\pi z).$$

Therefore $\delta=\gamma_0^{y+\pi z}$ satisfies (7.19). Denoting $\beta=\alpha_0\cdot\delta^{-p^{v+1}\pi^{v\varphi(p^u)-t_0}}$ we have

$$\bigl(\beta^{\pi^{t_0}}\cdot\xi_1^{e'_\chi}\bigr)^{\pi_0}=1, \tag{7.22}$$

so $\beta^{\pi^{t_0}}\cdot\xi_1^{e'_\chi}\in F'$ and the ideal $(\beta^{\pi^{t_0}})=(\beta^{\pi^{t_0}}\cdot\xi_1^{e'_\chi})\in\mathcal{I}$ is the extension of a principal ideal of F'. Since $a\geqslant 0$ is the smallest integer such that there is $\mu\in F'$ satisfying $(\beta^{e'_\chi r\pi^a})=(\mu)\in\mathcal{I}$, clearly $a\leqslant t_0$ and $\varepsilon=\beta^{e'_\chi r\pi^a}\mu^{-1}\in E_F$. Recall that $p\nmid r$, so there is a positive integer r' such that $rr'\equiv 1 \pmod{p^{v+1}}$. Therefore

$$\pi^a\operatorname{amb}(\alpha_0)=\pi^a r're'_\chi\operatorname{amb}(\beta)=r'\operatorname{amb}(\beta^{\pi^a re'_\chi})=r'\operatorname{amb}(\varepsilon\mu)=0,$$

so $b\leqslant a$ and the first statement of the proposition follows. We have

$$\varepsilon^{\pi_0\pi^{t_0-a}}=\beta^{e'_\chi r\pi_0\pi^{t_0}}.$$

Computing modulo $(F^\times)^{p^{v+1}}$ we obtain

$$\varepsilon^{r'\pi_0\pi^{t_0-a}}\equiv\beta^{e'_\chi\pi_0\pi^{t_0}}\equiv\alpha_0^{e'_\chi\pi_0\pi^{t_0}}.$$

Therefore (7.20) implies

$$\varepsilon^{r'\pi_0\pi^{t_0-a}}\cdot\xi_1^{e'_\chi\pi_0}\in(F^\times)^{p^{v+1}}$$

and Lemma 7.7 gives that p^{t_0-a} divides $\bigl|\bigl(E_F/\operatorname{Cyc}_F E_{F'}E_F^{p^v}\bigr)^{e_\chi}\bigr|$, which is a divisor of $\bigl|\bigl(E_F/\operatorname{Cyc}_F E_{F'}E_F^{M}\bigr)^{e_\chi}\bigr|$. We have proved the second statement of the proposition.

If $i>g$ then the decomposition group of p_i in $\operatorname{Gal}(L/\mathbb{Q})$ is nontrivial, so we can take $\tau\neq 1$ in this decomposition group. Then $\tau\mathfrak{p}_i=\mathfrak{p}_i$ and

$$(\chi(\tau)-1)e_\chi\mathfrak{p}_i=\tau e_\chi\mathfrak{p}_i-e_\chi\mathfrak{p}_i=0$$

in $\oplus_{j=1}^s(\mathcal{I}_{p_j}/p\mathcal{I}_{p_j})$. Assumption 3 implies that χ is injective on $\operatorname{Gal}(L/\mathbb{Q})$, hence $\chi(\tau)\not\equiv 1 \pmod{p\mathbb{Z}_p}$ and $e_\chi\mathfrak{p}_i=0$ here, giving $e_\chi(\mathcal{I}_{p_i}/p\mathcal{I}_{p_i})=0$.

If $i\leqslant g$ then

$$\mathcal{I}_{p_i}\cong(\mathbb{Z}[x]/(x^{n_i}-1))[H]$$

as $\mathbb{Z}[G]$-modules (σ acts as x on the right-hand module). Hence

$$e_\chi(\mathcal{I}_{p_i}/p\mathcal{I}_{p_i})\cong(\mathbb{Z}/p\mathbb{Z})[x]/(x^{n_i}-1)=(\mathbb{Z}/p\mathbb{Z})[x]/((x-1)^{n_i}).$$

Therefore

$$\mathrm{amb}(\alpha_0) \in e_\chi \oplus_{j=1}^{g} (\mathcal{I}_{p_j}/p\mathcal{I}_{p_j}) \cong \oplus_{j=1}^{g} (\mathbb{Z}/p\mathbb{Z})[x]/(x^{n_i})$$

as $(\mathbb{Z}/p\mathbb{Z})[x]$-modules ($x$ acts as π on the left-hand module). Since $b \geqslant 0$ is the smallest integer such that $\pi^b \cdot \mathrm{amb}(\alpha_0) = 0$, the cyclic $(\mathbb{Z}/p\mathbb{Z})[x]$-submodule $\langle \mathrm{amb}(\alpha_0)\rangle_\sigma$ generated by $\mathrm{amb}(\alpha_0)$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})[x]/(x^b)$, hence $|\langle \mathrm{amb}(\alpha_0)\rangle_\sigma| = p^b$.

Computing in the group $\mathcal{I}$ of fractional ideals of F (written additively), the identity (7.22) gives $\pi_0 \pi^{t_0}(\beta) = (\xi_1^{-e'_\chi \pi_0}) = 0$ and so, since π is injective on $\mathbb{Z}[\langle\sigma\rangle]/N'$, we have $\pi_0(\beta) = 0$. Let us fix an ideal $J_0 \in \oplus_{j=1}^{g} \mathcal{I}_{p_j}$ such that the image of J_0 in $\oplus_{j=1}^{s}(\mathcal{I}_{p_j}/p\mathcal{I}_{p_j})$ equals $\mathrm{amb}(\alpha_0) = \mathrm{amb}(\beta)$. Then $(\beta) = J_0 + \widetilde{J_1}$ in $\mathcal{I}$ for the extension $\widetilde{J_1} \in \mathcal{I}$ of a suitable ideal J_1 of F'.

Consider the $\mathbb{Z}[G]$-module homomorphism

$$\Psi : \ e_\chi \oplus_{j=1}^{s} (\mathcal{I}_{p_j}/p\mathcal{I}_{p_j}) \ \to \ C_\chi/N'C_\chi \tag{7.23}$$

determined by $\Psi(e_\chi \mathfrak{p}_j) = e_\chi \overline{\mathcal{P}_j}$ (recall that $\overline{\mathcal{P}_j}$ was defined above (5.3)). Then

$$\mathrm{im}\,\Psi = \langle e_\chi \overline{\mathcal{P}_1}, \dots, e_\chi \overline{\mathcal{P}_s}\rangle_\sigma.$$

Since $e'_\chi \widetilde{J_1} \in N'C_\chi$, we have

$$\mathrm{amb}(\alpha_0) = e'_\chi \,\mathrm{amb}(\alpha_0) \in \ker \Psi.$$

So $\langle \mathrm{amb}(\alpha_0)\rangle_\sigma \subseteq \ker \Psi$ and p^b divides $|\ker \Psi|$. Since $|e_\chi \oplus_{j=1}^{s} (\mathcal{I}_{p_j}/p\mathcal{I}_{p_j})| = p^n$, we see that $|\mathrm{im}\,\Psi|$ divides p^{n-b} and the third statement of the proposition follows.

To prove the fourth statement we can assume $a > b$. Since $\pi^b \cdot \mathrm{amb}(\beta) = 0$, the ideal (β^{π^b}) is equal to the extension $\widetilde{J_2} \in \mathcal{I}$ of a suitable ideal J_2 of F'. We know that $h_{F'} \mid h_F$ (see [13, Theorem 10.1]) and so the class of J_2^r belongs to $C_{F'}$. Let $\mathfrak{c} \in C_{F',\chi}$ be the class of $J_2^{re'_\chi}$. Then $\iota_\chi(\mathfrak{c}) = 0$ and $\mathfrak{c} \in \ker \iota_\chi$.

Moreover $\widetilde{J_2}^{\,p} = \widetilde{J_2}^{\,N'} = (\mathrm{N}_{F/F'}(\beta^{\pi^b}))$ is a principal ideal of F' generated by $\beta^{\pi^b N'} \in F'$, so $\mathfrak{c}^p = 0$. Of course, $\mathfrak{c}^{\pi_0} = 0$. The definition of a gives $\mathfrak{c}^{\pi^{a-b}} = 0$ and $\mathfrak{c}^{\pi^{a-b-1}} \neq 0$. Similarly as above, the $\mathbb{Z}[\langle\sigma\rangle]$-submodule of $C_{F',\chi}$ generated by $\mathfrak{c}$ is a cyclic $(\mathbb{Z}/p\mathbb{Z})[x]/(x^{p^{u-1}})$-module whose annihilator is generated by x^{a-b}. Hence $|\langle\mathfrak{c}\rangle| = p^{a-b}$ divides $|\ker \iota_\chi|$. The proposition is proved. □

Proposition 7.10. — *If χ is a nontrivial Dirichlet character of $L = L_\chi$ and M is a large power of p ($p^n \mid M$ and $M > p^2 \cdot h_{F,p}^2$ suffice) then $|C_\chi|$ is a divisor of $|C_{F',\chi}| \cdot \left|\left(E_F/\,\mathrm{Cyc}_F\, E_{F'} E_F^M\right)^{e_\chi}\right|$.*

Proof. — Recall that $t_0 \geqslant k+n$ due to Corollary 7.6 and that (5.4) gives that

$$|C_\chi/N'C_\chi| = |\overline{C}_\chi| \cdot |\langle e_\chi \overline{\mathcal{P}_1}, \dots, e_\chi \overline{\mathcal{P}_g}\rangle_\sigma| = p^k \cdot |\langle e_\chi \overline{\mathcal{P}_1}, \dots, e_\chi \overline{\mathcal{P}_g}\rangle_\sigma|$$

and that $|\langle e_\chi \overline{\mathcal{P}_1}, \dots, e_\chi \overline{\mathcal{P}_g}\rangle_\sigma|$ divides p^{n-b} due to Proposition 7.9. Therefore $|C_\chi/N'C_\chi|$ is a divisor of p^{t_0-b} and so it divides

$$|\ker \iota_\chi| \cdot \left|\left(E_F/\operatorname{Cyc}_F E_{F'} E_F^M\right)^{e_\chi}\right|$$

again by Proposition 7.9. Recall that $\iota_\chi(C_{F',\chi}) = N'C_\chi$. Hence $|C_\chi|$ is a divisor of

$$|\iota_\chi(C_{F',\chi})| \cdot |\ker \iota_\chi| \cdot \left|\left(E_F/\operatorname{Cyc}_F E_{F'} E_F^M\right)^{e_\chi}\right| = |C_{F',\chi}| \cdot \left|\left(E_F/\operatorname{Cyc}_F E_{F'} E_F^M\right)^{e_\chi}\right|$$

and the proposition is proved. □

8. Removing the simplifying assumption

Let us remove Assumption 3 in this section, so F means again any field satisfying the conditions of Section 4. Lemmas 4.1 and 4.2 imply that Proposition 7.10 and Part 3 of Lemma 5.1 are still valid for our field F. We shall need the following corollary of Gras' conjecture

$$\left|\left(E_L/\operatorname{Cyc}_L E_L^M\right)^{e_\chi}\right| = |C_{L,\chi}| \qquad \text{if } \ h_{L,p} \mid M, \tag{8.1}$$

which R. Greenberg proved[(4)] in [3] to be a consequence of the Main Conjecture, which was proved by B. Mazur and A. Wiles in [9]. It is well-known that this can be proved by Kolyvagin's method (see [10, Theorem 4.2] for the case L being the maximal real subfield of the pth cyclotomic field).

THEOREM 8.1. — *Let M be a large power of p ($h_{F,p}|M$ suffices). If χ is a nontrivial Dirichlet character of L then*

$$|C_\chi| = |C_{F',\chi}| \cdot \left|\left(E_F/\operatorname{Cyc}_F E_{F'} E_F^M\right)^{e_\chi}\right| = \left|\left(E_F/\operatorname{Cyc}_F E_F^M\right)^{e_\chi}\right|. \tag{8.2}$$

Proof. — Notice that taking any higher power of p instead of M does not change the statement, so we can assume that M satisfies the assumption mentioned in Proposition 7.10.

Let χ_0 be the trivial character of L. Lemmas 4.1, 4.3, and 4.2 give

$$|C_{\chi_0}| = h_{K,p} = \frac{1}{c_K} \cdot [E_K : \operatorname{Cyc}_K]_p = \frac{1}{c_K} \cdot \left|\left(E_F/\operatorname{Cyc}_F E_F^M\right)^{e_{\chi_0}}\right|. \tag{8.3}$$

(4) R. Greenberg used there a different definition of circular units which gives only a subgroup of Cyc_L. Nevertheless their relative index is not divisible by p as $p \nmid [L:\mathbb{Q}]$, so the quotients $E_L/\operatorname{Cyc}_L E_L^M$ are isomorphic for these two definitions (see [7] for more details).

Lemma 4.3 implies (the products are taken over all Dirichlet characters χ of L *including the trivial one*)

$$\prod_{\chi}|C_\chi| = |C| = h_{F,p} = \frac{1}{c_K}\cdot[E_F : \mathrm{Cyc}_F]_p = \frac{1}{c_K}\cdot\left|E_F/\mathrm{Cyc}_F\, E_F^M\right|$$
$$= \frac{1}{c_K}\cdot\prod_{\chi}\left|\left(E_F/\mathrm{Cyc}_F\, E_F^M\right)^{e_\chi}\right|.$$

Using (8.3) and Part 3 of Lemma 5.1 we obtain

$$\prod_{\chi\neq\chi_0}|C_\chi| = \prod_{\chi\neq\chi_0}\left|\left(E_F/\mathrm{Cyc}_F\, E_F^M\right)^{e_\chi}\right| \tag{8.4}$$
$$= \prod_{\chi\neq\chi_0}\left|\left(E_F/\mathrm{Cyc}_F\, E_{F'}E_F^M\right)^{e_\chi}\right|\cdot\left|\left(E_{F'}/\mathrm{Cyc}_{F'}\, E_{F'}^M\right)^{e_\chi}\right|.$$

Now we shall prove the theorem by induction. If $u = 1$ then $F' = L$ and (8.1) reads

$$\left|\left(E_{F'}/\mathrm{Cyc}_{F'}\, E_{F'}^M\right)^{e_\chi}\right| = |C_{F',\chi}|. \tag{8.5}$$

The theorem for $u = 1$ follows from

$$\prod_{\chi\neq\chi_0}|C_\chi| = \prod_{\chi\neq\chi_0}|C_{F',\chi}|\cdot\left|\left(E_F/\mathrm{Cyc}_F\, E_{F'}E_F^M\right)^{e_\chi}\right| \tag{8.6}$$

using Proposition 7.10, (8.5) and Part 3 of Lemma 5.1.

Let us assume now that $u > 1$ and that the theorem holds true for $u-1$, *i.e.*, for F replaced by F'. Then (8.2) for $u-1$ implies (8.5) for the current u. By (8.4) we have (8.6) again and the theorem follows by exactly the same reasoning as above. □

9. Consequences

Let us assume Assumption 3 for a fixed nontrivial character χ again.

In the previous sections we have studied the $\mathbb{Z}_p[\langle\sigma\rangle]$-modules appearing in the following exact sequence

$$0 \longrightarrow \ker\iota_\chi \longrightarrow C_{F',\chi} \xrightarrow{\iota_\chi} C_\chi \longrightarrow C_\chi/N'C_\chi \longrightarrow 0. \tag{9.1}$$

Both the kernel $\ker\iota_\chi$ and the cokernel $C_\chi/N'C_\chi$ of ι_χ are killed by N', hence these two modules are finite modules over

$$\mathbb{Z}_p[\langle\sigma\rangle]/N'\mathbb{Z}_p[\langle\sigma\rangle] \cong \mathbb{Z}_p[\zeta_{p^u}].$$

As $\mathbb{Z}_p[\zeta_{p^u}]$ is a discrete valuation ring with maximal ideal $\overline{\pi}\mathbb{Z}_p[\zeta_{p^u}]$, any finitely generated $\mathbb{Z}_p[\zeta_{p^u}]$-module is isomorphic to

$$\mathbb{Z}_p[\zeta_{p^u}]^r \oplus \big(\mathbb{Z}_p[\zeta_{p^u}]/\overline{\pi}^{a_1}\mathbb{Z}_p[\zeta_{p^u}]\big) \oplus \cdots \oplus \big(\mathbb{Z}_p[\zeta_{p^u}]/\overline{\pi}^{a_n}\mathbb{Z}_p[\zeta_{p^u}]\big)$$

for unique integers $r \geqslant 0$, $n \geqslant 0$, and $a_1 \geqslant \cdots \geqslant a_n > 0$. Hence any two finite $\mathbb{Z}_p[\zeta_{p^u}]$-modules have the same Fitting ideal if and only if they have the same cardinality. In the proofs of Lemmas 5.1 and 7.1 we have already mentioned that $\big((E_F/E_{F'}) \otimes \mathbb{Z}_p\big)^{e_\chi}$ is a $\mathbb{Z}_p$-free module of $\mathbb{Z}_p$-rank $\varphi(p^u)$ and so

$$\big((E_F/E_{F'}) \otimes \mathbb{Z}_p\big)^{e_\chi} \cong \mathbb{Z}_p[\zeta_{p^u}]$$

are isomorphic $\mathbb{Z}_p[\zeta_{p^u}]$-modules. Let an integer c be defined by

$$p^c = \big|\big((E_F/\operatorname{Cyc}_F E_{F'}) \otimes \mathbb{Z}_p\big)^{e_\chi}\big|.$$

Both the annihilator ideal and the Fitting ideal of $\big((E_F/\operatorname{Cyc}_F E_{F'}) \otimes \mathbb{Z}_p\big)^{e_\chi}$ are determined by c as follows

$$\begin{aligned} &\operatorname{Ann}_{\mathbb{Z}_p[\zeta_{p^u}]}\big((E_F/\operatorname{Cyc}_F E_{F'}) \otimes \mathbb{Z}_p\big)^{e_\chi} \\ &\qquad = \operatorname{Fitt}_{\mathbb{Z}_p[\zeta_{p^u}]}\big((E_F/\operatorname{Cyc}_F E_{F'}) \otimes \mathbb{Z}_p\big)^{e_\chi} \\ &\qquad = \overline{\pi}^c\mathbb{Z}_p[\zeta_{p^u}] \end{aligned} \tag{9.2}$$

and

$$\begin{aligned} \operatorname{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}\big((E_F/\operatorname{Cyc}_F E_{F'}) \otimes \mathbb{Z}_p\big)^{e_\chi} &= \operatorname{Fitt}_{\mathbb{Z}_p[\langle\sigma\rangle]}\big((E_F/\operatorname{Cyc}_F E_{F'}) \otimes \mathbb{Z}_p\big)^{e_\chi} \\ &= \pi^c\mathbb{Z}_p[\langle\sigma\rangle] + N'\mathbb{Z}_p[\langle\sigma\rangle]. \end{aligned} \tag{9.3}$$

Theorem 8.1 implies that

$$p^c = \big|\big((E_F/\operatorname{Cyc}_F E_{F'}) \otimes \mathbb{Z}_p\big)^{e_\chi}\big| = \frac{|C_\chi|}{|C_{F',\chi}|}. \tag{9.4}$$

Let us summarize what we know about the kernel and cokernel of ι_χ in (9.1). We shall obtain a complete description of capitulation in the extension F/F'.

PROPOSITION 9.1. — *Consider r, β, a and b defined in Proposition 7.9. Then*

$$\langle e_\chi\overline{\mathcal{P}_1}, \ldots, e_\chi\overline{\mathcal{P}_s}\rangle_\sigma \cong \big(e_\chi \oplus_{j=1}^g (\mathcal{I}_{p_j}/p\mathcal{I}_{p_j})\big)/\langle \operatorname{amb}(\alpha_0)\rangle_\sigma$$

is a submodule of the $\mathbb{Z}_p[\zeta_{p^u}]$-module $C_\chi/N'C_\chi$ of cardinality p^{n-b} and the minimal number of generators of $C_\chi/N'C_\chi$ is[5] *at least $g-1$. The kernel*

[5] We do not have equality here in general. [Example: let us take again $K = \mathbb{Q}(\theta)$ where $\theta^3 + \theta^2 - 576\theta + 1665 = 0$, so K is an abelian cubic field of conductor $1729 = 7 \cdot 13 \cdot 19$. Let $L = \mathbb{Q}(\sqrt{11})$, then 7, 13, and 19 are all inert in L and $g = 0$. Since $h_L = 1$, $h_K = 9$, and $h_F = 27$, we have $|C_{F',\chi}| = 1$ and $|C_\chi| = 3$, so $|C_\chi/N'C_\chi| = 3$.]

$\ker \iota_\chi$ *is a cyclic* $(\mathbb{Z}/p\mathbb{Z})[\langle\sigma\rangle]/(N')$*-module of cardinality*

$$|\ker \iota_\chi| = p^{a-b} \leqslant p^{p^{u-1}} \tag{9.5}$$

generated by the class $\mathfrak{c}$ *of an ideal* J*, whose extension* $\tilde{J} = (\beta^{e'_\chi r \pi^b}) \in \mathcal{I}$*.*

Proof. — Theorem 8.1 and the proof of Proposition 7.10 implies that all divisibilities of Propositions 7.9 and 7.10 are in fact equalities. The mentioned isomorphism is given by (7.23). In order to prove Proposition 7.10 we constructed a cyclic submodule of $\ker \iota_\chi$ generated by $\mathfrak{c}$. But now we know that this submodule is of the same cardinality as $\ker \iota_\chi$, so $\ker \iota_\chi$ is cyclic. The inequality in (9.5) follows from $\ker \iota_\chi \subseteq C_{F',\chi}$, which is killed by π_0. □

THEOREM 9.2. — *For any nontrivial character* χ *we have*

$$\mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}(C_{F',\chi}) \cdot \mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}\big((E_F/\operatorname{Cyc}_F E_{F'}) \otimes \mathbb{Z}_p\big)^{e_\chi} \subseteq \mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}(C_\chi).$$

Proof. — Let us consider the exact sequence

$$0 \longrightarrow C^0_\chi \xrightarrow{\subseteq} C_\chi \xrightarrow{\mathrm{N}_{F/F'}} C_{F',\chi} \longrightarrow 0,$$

defining a $\mathbb{Z}_p[\langle\sigma\rangle]$-module $C^0_\chi \subseteq C_\chi$. Then (9.4) gives

$$|C^0_\chi| = p^c. \tag{9.6}$$

Since C^0_χ is clearly killed by N', it is a $\mathbb{Z}_p[\zeta_{p^u}]$-module and

$$\overline{\pi}^c \mathbb{Z}_p[\zeta_{p^u}] = \mathrm{Fitt}_{\mathbb{Z}_p[\zeta_{p^u}]}(C^0_\chi) \subseteq \mathrm{Ann}_{\mathbb{Z}_p[\zeta_{p^u}]}(C^0_\chi)$$

and (9.3) implies

$$\mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}\big((E_F/\operatorname{Cyc}_F E_{F'}) \otimes \mathbb{Z}_p\big)^{e_\chi} \subseteq \mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}(C^0_\chi).$$

Let $\psi \in \mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}(C_{F',\chi})$ and $\nu \in \mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}(C^0_\chi)$, then for any $\mathfrak{c} \in C_\chi$ we have $\mathrm{N}_{F/F'}(\psi\mathfrak{c}) = \psi\,\mathrm{N}_{F/F'}(\mathfrak{c}) = 0$ because $\mathrm{N}_{F/F'}(\mathfrak{c}) \in C_{F',\chi}$, hence $\psi\mathfrak{c} \in C^0_\chi$ and $\nu\psi\mathfrak{c} = 0$. Therefore $\nu\psi \in \mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}(C_\chi)$ and the theorem is proved. □

For most values of g, the previous theorem may be made stronger. More precisely: Part (i) of the next result is an improvement on Theorem 9.2 (taking into account (9.2)) if $g > 3$; part (ii) is an improvement if $g > 2$.

THEOREM 9.3.

(i) *Let* $c' = c + 2 - g$*, then* $c' \geqslant 0$ *and for any nontrivial character* χ *we have*

$$\pi^{c'+1} \cdot \mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}(C_{F',\chi}) \subseteq \mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}(C_\chi).$$

(ii) *If* $\mathrm{amb}(\alpha_0) = 0$ *then we even have*

$$\pi^{c'} \cdot \mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}(C_{F',\chi}) \subseteq \mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}(C_\chi).$$

Proof. — Let $\mathcal{D} = \langle e_\chi \mathcal{P}_1, \ldots, e_\chi \mathcal{P}_g \rangle_\sigma \subseteq C_\chi$. Let $\tilde{g}$ be the minimal number of generators of $\mathcal{D}$; Proposition 9.1 states that $\tilde{g} \geqslant g - 1$ and that $\mathrm{amb}(\alpha_0) = 0$ implies $\tilde{g} = g$. Let $\mathcal{D}[p]$ mean the submodule of $\mathcal{D}$ killed by p, then $\mathcal{D}[p]$ is the kernel of $\iota_\chi \circ \mathrm{N}_{F/F'}$ on $\mathcal{D}$ and $\mathcal{D} \cap C_\chi^0$ is the kernel of $\mathrm{N}_{F/F'}$ on $\mathcal{D}$, so we have the following exact sequence

$$0 \longrightarrow \mathcal{D} \cap C_\chi^0 \xrightarrow{\subseteq} \mathcal{D}[p] \xrightarrow{\mathrm{N}_{F/F'}} \ker \iota_\chi$$

of $\mathbb{Z}_p[\zeta_{p^u}]$-modules. Since $\ker \iota_\chi$ is a cyclic $\mathbb{Z}_p[\zeta_{p^u}]$-module, C_χ^0 requires at least $\tilde{g} - 1$ generators and

$$p^{\tilde{g}-1} \cdot |\pi C_\chi^0| \leqslant |C_\chi^0| = p^c$$

due to (9.6). Therefore

$$\overline{\pi}^{c+1-\tilde{g}} \in \mathrm{Fitt}_{\mathbb{Z}_p[\zeta_{p^u}]}(\pi C_\chi^0) \subseteq \mathrm{Ann}_{\mathbb{Z}_p[\zeta_{p^u}]}(\pi C_\chi^0),$$

and so

$$\pi^{c+2-\tilde{g}} \in \mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}(C_\chi^0),$$

and the theorem follows from the properties of $\tilde{g}$ mentioned above, by the same reasoning as at the end of the proof of Theorem 9.2. □

Again, as in the beginning of Section 8 we can remove Assumption 3; Theorem 9.2 still holds true. Finally, for $j = 0, 1, \ldots, u$, let $F^{(j)}$ be the subfield of F determined by $[F : F^{(j)}] = p^j$, so $F^{(0)} = F$, $F^{(1)} = F'$, …, $F^{(u)} = L$.

Corollary 9.4. — *For any nontrivial character* χ *we have*

$$\mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}\big((E_L/\mathrm{Cyc}_L) \otimes \mathbb{Z}_p\big)^{e_\chi} \cdot \prod_{j=0}^{u-1} \mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}\big((E_{F^{(j)}}/\mathrm{Cyc}_{F^{(j)}} E_{F^{(j+1)}}) \otimes \mathbb{Z}_p\big)^{e_\chi} \subseteq \mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}(C_\chi).$$

Proof. — Thaine's theorem states (see [12])

$$\mathrm{Ann}_{\mathbb{Z}_p}\big((E_L/\mathrm{Cyc}_L) \otimes \mathbb{Z}_p\big)^{e_\chi} \subseteq \mathrm{Ann}_{\mathbb{Z}_p}(C_{L,\chi})$$

which implies

$$\mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}\big((E_L/\mathrm{Cyc}_L) \otimes \mathbb{Z}_p\big)^{e_\chi} \subseteq \mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}(C_{L,\chi}).$$

We can use induction with respect to u. If $u = 1$ then the theorem follows from the previous inclusion and Theorem 9.2. So suppose that $u > 1$ and

that this corollary has been already proved for F'. This hypothesis and Theorem 9.2 gives the result. □

Remark 9.5. — Let χ_0 be the trivial character. To keep the situation simple, just assume $u = 1$. Then the statement analogous to Theorem 9.2 can be proved[(6)] only if $s \neq 2$. Indeed, C_{F',χ_0} is trivial, and we need to show

$$\mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}\big((E_K/\operatorname{Cyc}_K)\otimes\mathbb{Z}_p\big) \subseteq \mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}(C_K)$$

if $s = 1$ or $s > 2$. For $s = 1$ we have $c_K = 1$ and $h_{K,p} = 1$, so both modules are trivial. Assuming $s > 2$ we shall prove the formula above in the course of the proof of the following result.

Corollary 9.6. — *Assume that $u = 1$, so $F' = L$. Then*

$$\pi \cdot \mathrm{Ann}_{\mathbb{Z}_p[G]}\big((E_F/\operatorname{Cyc}_F E_L)\otimes\mathbb{Z}_p\big) \subseteq \mathrm{Ann}_{\mathbb{Z}_p[G]}(C).$$

Proof. — Let χ_0 be the trivial character. Lemma 4.3 states

$$\big|\big((E_F/\operatorname{Cyc}_F E_L)\otimes\mathbb{Z}_p\big)^{e_{\chi_0}}\big| = \big|\big((E_K/\operatorname{Cyc}_K)\otimes\mathbb{Z}_p\big)\big| = |C_{\chi_0}|\cdot c_K,$$

where $c_K = 1$ if $s = 1$ and $c_K = p^{-1}$ if $s > 1$. Moreover

$$\big((E_F/E_L)\otimes\mathbb{Z}_p\big)^{e_{\chi_0}} \cong \mathbb{Z}_p[\zeta_p]$$

is a cyclic $\mathbb{Z}_p[\zeta_p]$-module and C_{χ_0} is a $\mathbb{Z}_p[\zeta_p]$-module. Hence

$$\mathrm{Fitt}_{\mathbb{Z}_p[\zeta_p]}\big((E_F/\operatorname{Cyc}_F E_{F'})\otimes\mathbb{Z}_p\big)^{e_{\chi_0}} = \mathrm{Ann}_{\mathbb{Z}_p[\zeta_p]}\big((E_F/\operatorname{Cyc}_F E_{F'})\otimes\mathbb{Z}_p\big)^{e_{\chi_0}}$$

and we have the following inclusion (which is an equality if $s > 1$)

$$(1-\zeta_p)\cdot\mathrm{Fitt}_{\mathbb{Z}_p[\zeta_p]}\big((E_F/\operatorname{Cyc}_F E_{F'})\otimes\mathbb{Z}_p\big)^{e_{\chi_0}} \subseteq \mathrm{Fitt}_{\mathbb{Z}_p[\zeta_p]}(C_{\chi_0}).$$

Therefore

$$(1-\zeta_p)\cdot\mathrm{Ann}_{\mathbb{Z}_p[\zeta_p]}\big((E_F/\operatorname{Cyc}_F E_{F'})\otimes\mathbb{Z}_p\big)^{e_{\chi_0}} \subseteq \mathrm{Ann}_{\mathbb{Z}_p[\zeta_p]}(C_{\chi_0}). \tag{9.7}$$

Notice that if $s \geqslant 3$ then C_{χ_0} is not cyclic due to genus theory and we obtain

$$\mathrm{Fitt}_{\mathbb{Z}_p[\zeta_p]}(C_{\chi_0}) \subseteq (1-\zeta_p)\,\mathrm{Ann}_{\mathbb{Z}_p[\zeta_p]}(C_{\chi_0}),$$

hence

$$\mathrm{Ann}_{\mathbb{Z}_p[\zeta_p]}\big((E_F/\operatorname{Cyc}_F E_{F'})\otimes\mathbb{Z}_p\big)^{e_{\chi_0}} \subseteq \mathrm{Ann}_{\mathbb{Z}_p[\zeta_p]}(C_{\chi_0})$$

which proves the statement of Remark 9.5. Inclusion (9.7) means

$$\pi\cdot\mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}\big((E_F/\operatorname{Cyc}_F E_{F'})\otimes\mathbb{Z}_p\big)^{e_{\chi_0}} \subseteq \mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}(C_{\chi_0}).$$

(6) Each of the two cubic fields K of conductor $7\cdot 13$ has class number $h_K = 3$ and $c_K = p^{-1}$ implies that $(E_K/\operatorname{Cyc}_K)\otimes\mathbb{Z}_p$ is trivial.

For any nontrivial character χ Theorem 9.2 states that

$$\pi \cdot \mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}\big((E_F/\operatorname{Cyc}_F E_{F'}) \otimes \mathbb{Z}_p\big)^{e_\chi} \subseteq \mathrm{Ann}_{\mathbb{Z}_p[\langle\sigma\rangle]}(C_\chi)$$

and the corollary follows. □

BIBLIOGRAPHY

[1] J.-R. Belliard & T. Nguyen Quang Do, "Formules de classes pour les corps abéliens réels", *Ann. Inst. Fourier (Grenoble)* **51** (2001), no. 4, p. 903-937.

[2] K. Büyükboduk, "Kolyvagin systems of Stark units", *J. Reine Angew. Math.* **631** (2009), p. 85-107.

[3] R. Greenberg, "On p-adic L-functions and cyclotomic fields. II", *Nagoya Math. J.* **67** (1977), p. 139-158.

[4] 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.

[5] ———, "Linear forms on Sinnott's module", *J. Number Theory* **141** (2014), p. 324-342.

[6] I. Kaplansky, "Commutative Rings", Polygonal Publishing House, 1994, Washington, NJ.

[7] R. Kučera, "Circular units and class groups of abelian fields", *Ann. Sci. Math. Québec* **28** (2004), no. 1-2, p. 121-136 (2005).

[8] L. V. Kuzmin, "On formulas for the class number of real abelian fields", *Izv. Ross. Akad. Nauk Ser. Mat.* **60** (1996), no. 4, p. 43-110.

[9] B. Mazur & A. Wiles, "Class fields of abelian extensions of $\mathbf{Q}$", *Invent. Math.* **76** (1984), no. 2, p. 179-330.

[10] K. Rubin, "The Main Conjecture", in *Appendix in S. Lang, Cyclotomic Fields I and II*, second ed, Graduate Texts in Mathematics, vol. 121, Springer, New York, 1990.

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

[12] F. Thaine, "On the ideal class groups of real abelian number fields", *Ann. of Math. (2)* **128** (1988), no. 1, p. 1-18.

[13] L. C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997, xiv+487 pages.

Manuscrit reçu le 26 novembre 2012,
accepté le 27 novembre 2013.

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

Radan KUČERA
Masaryk University
Faculty of Science
611 37 Brno (Czech Republic)
kucera@math.muni.cz