ANNALES DE L'INSTITUT FOURIER

DAVID SOLOMON

On the classgroups of imaginary abelian fields

Annales de l'institut Fourier, tome 40, n° 3 (1990), p. 467-492
<http://www.numdam.org/item?id=AIF_1990__40_3_467_0>

Ann. Inst. Fourier, Grenoble
40, 3 (1990), 467-492

ON THE CLASSGROUPS OF IMAGINARY ABELIAN FIELDS

by David SOLOMON

I. INTRODUCTION

Let p be a prime number, K a finite, imaginary, abelian extension of $\mathbb{Q}$ and $\mathcal{C}\ell(K)$ the class group of K. This paper is concerned with the size of certain odd "eigenspaces" for the action of $G = \mathrm{Gal}(K/\mathbb{Q})$ on the p–primary part of $\mathcal{C}\ell(K)$ when $p \neq 2$. The situation of particular interest to us, and in which our results are new, is that in which p divides the order of G.

Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and let

$$\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \overline{\mathbb{Q}}_p^*$$

be an odd Dirichlet character. Let F denote $\mathbb{Q}_p(\chi)$, the field generated over $\mathbb{Q}_p$ by the values of χ and denote by $\mathcal{O} = \mathbb{Z}_p[\chi]$ its ring of integers. Suppose that $K \subset \overline{\mathbb{Q}}$ is as above, with $\ker \chi \supset \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. If we further assume that $p \nmid |G|$ (hence $p \nmid \mathrm{ord}\,\chi$) then the χ eigenspace $(\mathcal{C}\ell(K) \otimes \mathcal{O})^\chi$ of $\mathcal{C}\ell(K) \otimes \mathcal{O}$ is unambiguously defined (for example, as the image of $\mathcal{C}\ell(K) \otimes \mathcal{O}$ under the action of the idempotent for χ in $\mathcal{O}G$). Moreover, up to a natural isomorphism it is independent of K. Iwasawa and Leopoldt conjectured the following result, proven in [7] (Theorem 2, p. 216) as a consequence of the proof [*ibid.*] of the Main Conjecture of Iwasawa Theory over $\mathbb{Q}$:

Key-words : Class group – Abelian field – Dirichlet character – Generalized Bernoulli number – p–adic L–function – Iwasawa theory – Main conjecture.
A.M.S. Classification : 11R29.

"If $p \neq 2$ and $\chi \neq \omega$ (the Teichmüller character) then the length of $(\mathcal{C}\ell(K) \otimes \mathcal{O})^{\chi}$ as an $\mathcal{O}-$module is equal to the $F-$valuation of the generalized Bernoulli number $B_{1,\chi^{-1}}$."

Our main result (Theorem II.1) is a generalization of this statement, removing the assumption that $p \nmid \operatorname{ord}\chi$. I am grateful to the referee for pointing out that our result appears in an equivalent form as a conjecture of G. Gras in [4]. (Gras also conjectures a corresponding result for the case $p = 2$, which, however, we do not prove). The major tool in our proof is still the Main Conjecture over $\mathbb{Q}$ (whose proof in [7] is for *all* χ), however the possibility $p \mid |G|$ clearly engenders a number of complications. Firstly, although there is a natural generalization of $(\mathcal{C}\ell(K) \otimes \mathcal{O})^{\chi}$ for any K as above, without the restriction that $p \nmid [K : \mathbb{Q}]$ it is no longer independent of K. Therefore, in Theorem II.2 we shall specify K to be the field "cut out by χ" (that is, $\ker\chi = \operatorname{Gal}(\overline{\mathbb{Q}}/K)$). Moreover, when $p \mid |G|$ calculations are hampered by the fact that the "$\chi-$eigenspace" functor is no longer exact. We also remark that new cases will arise in the Iwasawa Theoretic context, when χ is no longer purely "of the first kind" (*i.e.* χ may be wildly ramified at p).

One should mention here the remarkable new methods which have recently been introduced by Kolyvagin and Rubin and which have led (among other things) to a new and essentially "elementary" proof of the Main Conjecture over $\mathbb{Q}$ in certain cases (see *e.g.* [9]). Furthermore, these methods also apply "at the finite level" (rather than as a limit in a $\mathbb{Z}_p-$tower), which holds out the hope of proving results like Theorem II.1 without any recourse to Iwasawa Theory. For example, by means of a system of Gauss sums Rubin proves in [8], Theorem 4.3, a result (attributed to Kolyvagin) which amounts to a classical case of Theorem II.1, namely that in which K is obtained by adjoining a primitive p^{th} root of unity to $\mathbb{Q}$ and χ is any odd character of $\operatorname{Gal}(K/\mathbb{Q})$, $\chi \neq \omega$. These methods undoubtedly extend to more general K and χ and may indeed be applicable to the cases of interest to us ($p \mid \operatorname{ord}\chi$). If this is so, it would seem nevertheless likely that such cases would introduce significant technical complications into the method, as they do in our own approach via the Main Conjecture.

In Section II of this paper we set up notation and state the main result. Some preliminary results are also established which will help to deal with the above-mentioned complications. Section III contains the deduction of the main result by methods analogous to those of [7].

Some notations used in this paper : μ_n is the group of all n^{th} roots of unity in $\overline{\mathbb{Q}}$ and we shall denote $\mathbb{Q}(\mu_n)$ by $\mathbb{Q}(n)$. Similarly, for a prime p, $\mu_{p^\infty} = \bigcup_1^\infty \mu_{p^n}$, $\mathbb{Q}(p^\infty) = \mathbb{Q}(\mu_{p^\infty})$. For any number field K, $\mu_n(K)$, $E(K)$, $I(K)$ and $P(K)$ will denote respectively the n^{th} roots of unity in K, the units, ideals and principal ideals of K. Also, if D is a discrete valuation ring, v_D will denote its valuation and $\ell_D(M)$ the length of a $D-$module M (possibly infinite).

II

1. $\chi-$parts.

Let p be a prime, G a group and $\chi : G \to \overline{\mathbb{Q}}_p^*$ a multiplicative character of finite order. Let $E \subset \overline{\mathbb{Q}}_p$ be a finite extension of $\mathbb{Q}_p$ with ring of integers D. Assume that D contains the values of χ and let $\underline{D}$ denote the $DG-$module structure on D induced by χ. (If G is finite then $\underline{D}$ is the $\chi-$component of a maximal order of EG.) For any $DG-$module M we define $D-$modules :

$$M^\chi =: \mathrm{Hom}_{DG}(\underline{D}, M)$$

and

$$M_\chi =: M \otimes_{DG} \underline{D}$$

by coextension and extension along $\chi : DG \to \underline{D}$. M^χ and M_χ are respectively the largest sub- and quotient-modules of M on which G acts by χ. Indeed, letting I_χ denote the ideal of DG generated by all elements of form $g - \chi(g)$, $g \in G$, one checks :

LEMMA II.1. — *There are natural isomorphisms of $D-$modules*

$$\{m \in M : gm = \chi(g)m \ \forall g \in G\} \cong M^\chi \cong (M \otimes_D \underline{D})^G$$

and

$$M/I_\chi M \cong M_\chi \cong (M \otimes_D \underline{D})_G$$

where $g \in G$ acts on $M \otimes_D \underline{D}$ by $g \otimes g^{-1}$, so that

$$M \otimes_D \underline{D} \underset{DG}{\cong} \mathrm{Hom}_D(\underline{D}, M). \qquad \square$$

These functors of M commute with extension and restriction of the ring D of scalars provided that it contains the values of χ. Temporarily

removing this restriction on D and writing $\tilde{D}$ for $D[\chi]$, we have isomorphisms

$$\mathrm{Hom}_D(\tilde{D}, M) \cong M \otimes_D \tilde{D}$$

and

$$(M \otimes_D \tilde{D})^\chi \cong \mathrm{Hom}_{DG}(\underline{\tilde{D}}, M)\ , \quad (M \otimes_D \tilde{D})_\chi \cong M \otimes_{DG} \underline{\tilde{D}}$$

as $\tilde{D}-$modules. For finite G, $\underline{\tilde{D}}$ is the component of a maximal order of EG corresponding to the $E-$conjugacy class of χ. This suggests a unified definition of the notations M^χ and M_χ for all D. However, we avoid such a definition, since it does not in general commute with restriction of scalars and so the notation could result in non-trivial ambiguities were D not specified. We note, however, that if U is a module for $\mathbb{Z}_pG$, the module "U_χ" defined on p. 192 of [7] coincides in our notation with the module $(U \otimes_{\mathbf{Z}} \mathbb{Z}_p[\chi])_\chi$.

If $G = G_1 \times G_2$ is a direct product and χ_i denotes $\chi|_{G_i}$, $i = 1, 2$, we shall write $\chi = \chi_1\chi_2$. Clearly M^{χ_1} is a DG_2-module and $M^\chi = (M^{\chi_1})^{\chi_2}$.

If G is finite and $p \nmid |G|$, then $\underline{D}$ is a direct factor of DG whence we may identify both M^χ and M_χ with the '$\chi-$part' $e_\chi M$, where e_χ is the idempotent of DG corresponding to χ. In this case we obtain an exact functor of M, commuting with most other operations.

Now suppose that χ is faithful. Then G is finite, cyclic of order $\mathrm{ord}\,\chi$. G is uniquely a product $G' \times G_p$ of cyclic subgroups with $p \nmid |G'|$ and $|G_p| = p^r$, $r \geq 0$. Correspondingly, $\chi = \chi'\chi_p$ and let $\mathcal{O}, \mathcal{O}'$ denote $\mathbb{Z}_p[\chi]$ and $\mathbb{Z}_p[\chi']$ respectively and F, F' their fraction fields. If $p \mid |G|$ (*i.e.* if $r \geq 1$), then C will denote the subgroup of order p in G_p and N_C its norm element in $\mathbb{Z}G_p$.

LEMMA II.2. — *Suppose $p \mid |G|$ and A is an $\mathcal{O}'G$ module then there are functorial isomorphisms of $\mathcal{O}'-$modules :*

$$(A \otimes_{\mathcal{O}'} \mathcal{O})^\chi \cong \ker N_C|A^{\chi'} \quad \textit{and} \quad (A \otimes_{\mathcal{O}'} \mathcal{O})_\chi \cong \mathrm{coker}\, N_C|A^{\chi'}.$$

Proof. — By the above remarks, the left hand sides are easily seen to be

$$(A^{\chi'} \otimes_{\mathcal{O}'} \mathcal{O})^{\chi_p} \cong \mathrm{Hom}_{\mathcal{O}'G_p}(\underline{\mathcal{O}}, A^{\chi'})$$

and

$$(A^{\chi'} \otimes_{\mathcal{O}'} \mathcal{O})_{\chi_p} \cong A^{\chi'} \otimes_{\mathcal{O}'G_p} \underline{\mathcal{O}}$$

respectively. Now a choice of generator g for G_p identifies $\mathcal{O}'G_p$ with $\mathcal{O}'[X]/(X^{p^r} - 1)$ and, since χ_p is faithful, a minimal polynomial for $\chi_p(g)$ over $\mathcal{O}'$ is $X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + 1$. If follows that the sequence

$$\mathcal{O}'G_p \xrightarrow{N_C} \mathcal{O}'G_p \xrightarrow{\chi_p} \underline{\mathcal{O}} \longrightarrow 0$$

is exact. Now apply the functors $\mathrm{Hom}_{\mathcal{O}'G_p}(\_, A^{\chi'})$ and $A^{\chi'} \otimes_{\mathcal{O}'G_p} \_$. □

We remark that the above exact sequence extends in an obvious way to a periodic, complete resolution of $\underline{\mathcal{O}}$ as $\mathcal{O}'G_p$–module, from which the derived functors of $\_^{\chi}$ and $\_\chi$ may be calculated. Notice also that the proof only requires G to be finite and χ to be faithful on the unique Sylow p–subgroup of G.

COROLLARY II.1. — *In the situation of Lemma II.2, suppose that B is an $\mathcal{O}'G'$–module with maps α and β :*

$$A \underset{\beta}{\overset{\alpha}{\rightleftarrows}} B$$

respectively surjective and injective on χ'–parts and such that $\beta \circ \alpha = N_C | A$. Then there are exact sequences of $\mathcal{O}'$–modules

$$0 \longrightarrow (A \otimes \mathcal{O})^{\chi} \longrightarrow A^{\chi'} \xrightarrow{\alpha} B^{\chi'} \longrightarrow 0$$

and

$$0 \longrightarrow B^{\chi'} \xrightarrow{\beta} A^{\chi'} \longrightarrow (A \otimes \mathcal{O})_{\chi} \longrightarrow 0.$$ □

2. The Main Result.

From now on, p is fixed and not equal to 2 and $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \overline{\mathbb{Q}}_p^*$ is an odd Dirichlet character. K will denote the field cut out by χ (*i.e.* the fixed field of $\ker \chi$), thus $\chi : G \to \overline{\mathbb{Q}}_p^*$ is faithful. Henceforth we shall adopt the notations of Lemma II.2 so $\mathcal{O} = \mathbb{Z}_p[\chi]$ *etc.* but in general we shall treat the cases $p | \operatorname{ord} \chi$, $p \nmid \operatorname{ord} \chi$ together. The conductor of χ will be denoted f and for $n \in \mathbb{Z}$, $(n, f) = 1$ we shall write σ_n for the image of $\overline{n}$ under the Artin map $(\mathbb{Z}/f\mathbb{Z})^* \to G$. We write $\chi(n)$ for $\chi(\sigma_n)$ and if $(n, f) > 1$ then $\chi(n) = 0$ by definition. $B_{1,\chi^{-1}}$ will denote the first generalized Bernoulli number :

$$B_{1,\chi^{-1}} = \frac{1}{f} \sum_{n=1}^{f} n\chi^{-1}(n) \in F^*.$$

We state our main result as :

THEOREM II.1.

$$v_{\mathcal{O}}(B_{1,\chi^{-1}}) = \ell_{\mathcal{O}}((\mathcal{C}\ell(K) \otimes_{\mathbf{Z}} \mathcal{O})^{\chi}) - \delta_{\chi} \tag{1}$$

where

$$\delta_{\chi} = \begin{cases} 1 \text{ if } K = \mathbf{Q}(p^{r+1}) \text{ and } \chi' = \omega, \text{ the Teichmüller character} \\ 0 \text{ otherwise.} \end{cases}$$

Remarks II.1. — (a) Suppose that $\delta_{\chi} = 1$ and let a be a primitive root modulo p^{r+2}. On the one hand it is not hard to show that in this case $(\chi(a) - a)B_{1,\chi^{-1}}$ is a unit of $\mathcal{O}$. On the other hand, Stickelberger's Theorem shows that it annihilates $(\mathcal{C}\ell(K) \otimes \mathcal{O})^{\chi}$ which allows us to deduce Theorem II.1 in this case. (Indeed, equation (1) becomes : $-1 = 0 - 1$).

(b) In general, let σ be a generator of G and P the minimal polynomial of $\chi(\sigma)$ over $\mathbf{Q}_p$. The remarks following Lemma II.1 show that $(\mathcal{C}\ell(K) \otimes \mathcal{O})^{\chi}$ identifies as $\mathcal{O}$–module with $\mathrm{Hom}_{\mathbf{Z}_p G}(\underline{\mathcal{O}}, \mathcal{C}\ell(K)_p)$ and a similar argument to that of Lemma II.2 identifies the latter with $\{a \in \mathcal{C}\ell(K)_p : P(\sigma)a = 0\}$, considered as a module for $\mathbf{Z}_p G/(P(\sigma)) \cong \mathcal{O}$. (Here $\mathcal{C}\ell(K)_p$ denotes the p–primary part of $\mathcal{C}\ell(K)$). In this form the Theorem becomes the case $p \neq 2$ of the conjecture of Gras mentioned in the introduction. (See [4], "Conclusion", p. 44, taking into account also Remark (a) above).

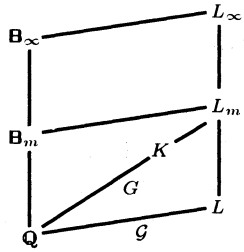
(c) If $L/\mathbf{Q}$ is any finite extension through which χ factors, one may form $(\mathcal{C}\ell(L) \otimes \mathcal{O})^{\chi} = (\mathcal{C}\ell(L)^H \otimes \mathcal{O})^{\chi}$ where $H = \mathrm{Gal}(L/K)$. However, except in special circumstances (*e.g.* $p \nmid [L : K]$, see also Proposition II.1) this is not isomorphic to $(\mathcal{C}\ell(K) \otimes \mathcal{O})^{\chi}$.

(d) If we replace $\mathcal{O}$ by the integers of a finite extension E of F, then the first terms on both sides of (1) are multiplied by $e(E/F)$.

3. Notation and Preliminaries.

Retaining the above notation we describe the Iwasawa Theoretic context of the proof of Theorem II.1. Let $\mathbf{B}_{\infty}$ denote the cyclotomic $\mathbf{Z}_p$–extension of $\mathbf{Q}$, thus $\mathbf{B}_{\infty} = \bigcup_{n=0}^{\infty} \mathbf{B}_n$ where $\mathbf{B}_n/\mathbf{Q}$ is cyclic of degree p^n. Let Γ denote $\mathrm{Gal}(\mathbf{B}_{\infty}/\mathbf{Q}) \cong \mathbf{Z}_p$ and $\Gamma_n = \mathrm{Gal}(\mathbf{B}_{\infty}/\mathbf{B}_n)$. Now $K\mathbf{B}_{\infty}$ can be uniquely written as $L\mathbf{B}_{\infty}$ where $L/\mathbf{Q}$ is finite and tamely ramified

at p, hence linearly disjoint from $\mathbf{B}_\infty/\mathbf{Q}$. Write L_n for $L\mathbf{B}_n$ and let $m = \min\{n : L_n \supset K\}$:



Then

$$L_m = L\mathbf{B}_m = KL = K\mathbf{B}_m\ , \quad \mathrm{Gal}(L_m/\mathbf{Q}) = \mathrm{Gal}(L_m/\mathbf{B}_m) \times \mathrm{Gal}(L_m/L)$$

and correspondingly, regarding χ as a character of $\mathrm{Gal}(L_m/\mathbf{Q})$ we have

$$\chi = \chi_t \rho.$$

χ_t is faithful on $\mathrm{Gal}(L_m/\mathbf{B}_m)$ which is identified with $\mathrm{Gal}(L/\mathbf{Q})$ and denoted $\mathcal{G}$. χ_t is an odd Dirichlet character of the *first kind* (with respect to p) in Iwasawa's terminology. ρ is faithful on $\mathrm{Gal}(L_m/L)$ (identified with Γ/Γ_m) and is of the *second kind*. $\mathcal{G}$ is further decomposed :

$$\mathcal{G} = \mathcal{G}' \times \mathcal{G}_p$$

and correspondingly

$$\chi_t = \chi' \chi_{t,p}.$$

Let $|\mathcal{G}_p| = p^s$. Then $\chi = \chi' \chi_{t,p} \rho$ has kernel $H = \mathrm{Gal}(L_m/K)$ on $\mathrm{Gal}(L_m/\mathbf{Q})$, and H is cyclic of order $\min(p^s, p^m)$, whilst $\chi_p = \chi_{t,p}\rho$ has order $p^r = \max(p^s, p^m)$. Thus χ, χ', χ_t and ρ all take values in $\mathcal{O}$. We shall also write $\mathcal{O}_t$ and $\mathcal{O}_\rho$ for $\mathbb{Z}_p[\chi_t]$ and $\mathbb{Z}_p[\rho]$ and F_t, F_ρ for their fraction fields. Since $p \neq 2$ and χ is odd, so are χ_t and χ', that is, $\chi_t(\tau) = \chi'(\tau) = -1$ where τ is the unique complex conjugation in $\mathcal{G}$. If M is any $\mathbb{Z}_p[\langle\tau\rangle]$−module, M^- will denote the 'minus part', *i.e.* $(1 - \tau)M$. Since $p \neq 2$, this is an exact functor of M. Using this notation we have :

PROPOSITION II.1.

$$(\mathcal{C}\ell(\dot{K}) \otimes \mathcal{O})^\chi \cong (\mathcal{C}\ell(L_m) \otimes \mathcal{O})^\chi.$$

Proof. — On the right hand side, χ is of course regarded as a character of $\mathrm{Gal}(L_m/\mathbf{Q})$ with kernel H. Since χ is odd it will suffice to show that the natural map $\mathcal{C}\ell(K) \xrightarrow{\alpha} \mathcal{C}\ell(L_m)^H$ induces an isomorphism

$$(\mathcal{C}\ell(K) \otimes \mathbb{Z}_p)^- \xrightarrow{\alpha^-} (\mathcal{C}\ell(L_m) \otimes \mathbb{Z}_p)^{-,H} \tag{2}$$

on minus parts. Now we have an exact sequence

$$(3) \qquad 0 \longrightarrow \mu_{p^\infty}(L_m) \longrightarrow (L_m^* \otimes \mathbb{Z}_p)^- \longrightarrow (P(L_m) \otimes \mathbb{Z}_p)^- \longrightarrow 0.$$

CLAIM 1. — $\hat{H}^i(H, \mu_{p^\infty}(L_m)) = 0 \ \forall i$ *(Tate cohomology).*

Proof of Claim 1. — w.l.o.g. $\mu_{p^\infty}(L_m)$ is non-trivial so equal to $\mu_{p^{m+1}}$. Thus $L_m = K\mathbb{Q}(p^{m+1})$ and the restriction to $\mathbb{Q}(p^{m+1})$ takes H isomorphically onto $\overline{H} =: \mathrm{Gal}(\mathbb{Q}(p^{m+1})/\mathbb{Q}(p^{k+1}))$ for some $k \leq m$. It is well known that $\hat{H}^i(\overline{H}, \mu_{p^{m+1}}) = 0 \ \forall i$, (since $\mu_{p^{m+1}}$ is finite and $\overline{H}$ cyclic, one only needs to check that

$$\mathrm{Norm}_{\mathbb{Q}(p^{m+1})/\mathbb{Q}(p^{k+1})} : \mu_{p^{m+1}} \longrightarrow \mu_{p^{k+1}}$$

is onto). This proves Claim 1.

Now take $H-$invariants in (3). Dropping $\otimes\mathbb{Z}_p$ from the notation we have : $P(L_m)^{-,H} = P(K)^-$ and $H^1(H, P(L_m)^-) = 0$ (by Hilbert's Theorem 90). Taking $H-$invariants in the exact sequence

$$0 \longrightarrow P(L_m)^- \longrightarrow I(L_m)^- \longrightarrow \mathcal{C}\ell(L_m)^- \longrightarrow 0$$

we see that α^- is injective and $\mathrm{coker}\,\alpha^- \cong I(L_m)^{-,H}/I(K)^-$. Thus the result will follow from :

CLAIM 2. — L_m/K *is unramified at all finite places.*

Proof of Claim 2. — Let Q be a prime of K and T its inertia group in L_n/K. We need that $T = \{1\}$. There are two cases : if $p \nmid Q$ then the projection of T on $\mathrm{Gal}(\mathbb{B}_m/\mathbb{Q})$ is trivial, hence $T \subset H \cap \mathrm{Gal}(L_m/\mathbb{B}_m) = \{1\}$. If $p|Q$ then, since H is a $p-$group and $L/\mathbb{Q}$ is tame at p, the projection of T on $\mathrm{Gal}(L/\mathbb{Q})$ is trivial. Hence $T \subset H \cap \mathrm{Gal}(L_m/L) = \{1\}$. □

Now let $A_n(L)$ denote $\mathcal{C}\ell(L_n) \otimes_{\mathbf{Z}} \mathbb{Z}_p$ ($p-$primary part) for $n = 0, 1, 2\ldots$ and let $A_\infty = A_\infty(L)$ denote $\varinjlim_n A_n(L)$ where the limit is with respect to the natural maps $A_n(L) \to A_{n+1}(L)$. These are known to be injective on minus parts so we may write $A_\infty^- = \bigcup_n A_n(L)^-$. A_∞ is a discrete $\mathbb{Z}_p-$module and its Pontryagin dual $\mathrm{Hom}_{\mathbf{Z}_p}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ is compact. Both are topological modules for $\Gamma \times \mathcal{G}$ (where $g \in \Gamma \times \mathcal{G}$ sends $f \in \mathrm{Hom}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ to $f \circ g^{-1}$). Let $\mathbb{Z}_p[[\Gamma]]$ denote $\varprojlim_n \mathbb{Z}_p[\Gamma/\Gamma_n]$. Fixing for once and for all a topological generator c of Γ, we identify $\mathbb{Z}_p[[\Gamma]]$ with the ring of formal power series $\mathbb{Z}_p[[T]]$ by the usual topological

isomorphism taking c to $T+1$. Then $\mathrm{Hom}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ is a finitely generated, torsion $\mathbb{Z}_p[[T]]$−module with commuting $\mathcal{G}$−action. Starting instead with $A_n \otimes_{\mathbb{Z}_p} \mathcal{O}_t$ there are isomorphisms of $\mathcal{O}_t[[T]]$−modules :

$$\varinjlim (A_n \otimes \mathcal{O}_t) \cong A_\infty \otimes \mathcal{O}_t$$

and

$$\mathrm{Hom}_{\mathcal{O}}(A_\infty \otimes \mathcal{O}, F_t/\mathcal{O}_t) \cong \mathrm{Hom}_{\mathbb{Z}_p}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathcal{O}_t.$$

(Note that $\mathcal{O}_t$ is free of finite rank over $\mathbb{Z}_p$). Now form the module

$$\mathrm{Hom}_{\mathcal{O}_t}(A_\infty \otimes \mathcal{O}_t, F_t/\mathcal{O}_t)_{\chi_t^{-1}}.$$

It is not hard to show that this is isomorphic to

$$\mathrm{Hom}_{\mathcal{O}_t}((A_\infty \otimes \mathcal{O}_t)^{\chi_t}, F_t/\mathcal{O}_t).$$

Let $g(\chi_t, T)$ denote its *Iwasawa polynomial* as finitely generated, torsion $\mathcal{O}_t[[T]]$−module.

One can also form $H_\infty =: \varprojlim A_n(L)$ where the limit is now taken with respect to the maps induced by the norms. It follows from work of Iwasawa that $(\mathrm{Hom}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathcal{O}_t)_{\chi_t^{-1}}$ is *pseudo-isomorphic* to $((H_\infty \otimes \mathcal{O}_t)_{\chi_t})^*$, where the star indicates that the natural Γ−action has been composed with inversion in Γ. Thus if $h(X_t, T)$ denotes the Iwasawa polynomial of $(H_\infty \otimes \mathcal{O}_t)_{\chi_t}$ we find :

$$h(\chi_t, T) = g(\chi_t, (1+T)^{-1} - 1)$$

(up to a unit of $\mathcal{O}_t[[T]]$). We remark that by [3], Iwasawa's μ−invariant vanishes for $\mathrm{Hom}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$, hence also for all $\mathbb{Z}_p[[T]]-$ or $\mathcal{O}_t[[T]]$−modules appearing here. It follows, for example, that $g(\chi_t, T)$ may be interpreted as the characteristic polynomial of $T = c - 1$ acting on the finite dimensional F_t−vector space obtained by tensoring $\mathrm{Hom}((A_\infty \otimes \mathcal{O}_t)^{\chi_t}, F_t/\mathcal{O}_t)$ with F_t over $\mathcal{O}_t$. The Main Conjecture of Iwasawa Theory over $\mathbb{Q}$ can now be introduced as follows. For any even Dirichlet character ψ with values in $\overline{\mathbb{Q}}_p^*$, let $L_p(\psi, s)$ denote the Leopoldt-Kubota p−adic L−function attached to ψ. As with χ, ψ may be uniquely written $\psi = \theta\psi_t$ where θ is a character of Γ and the field cut out by ψ_t is at most tamely ramified at p over $\mathbb{Q}$. The action of $\mathrm{Gal}(\mathbb{Q}(p^\infty)/\mathbb{Q})$ on μ_{p^∞} identifies the former with $\mathbb{Z}_p^*$ in the usual way, inducing isomorphisms :

$$\omega : \mathrm{Gal}(\mathbb{Q}(p^\infty)/\mathbb{Q}) \xrightarrow[\sim]{} \mu_{p-1} \subset \mathbb{Z}_p^*$$

(the Teichmüller character), and

$$\Gamma \xrightarrow[\sim]{} 1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^*.$$

Let κ denote the image of c under the second isomorphism. Iwasawa showed that there is a unique power series $G_p(\psi_t, T)$ with coefficients in $\mathbb{Z}_p[\psi_t]$, depending only on ψ_t and c and such that, for $s \in \mathbb{Z}_p$

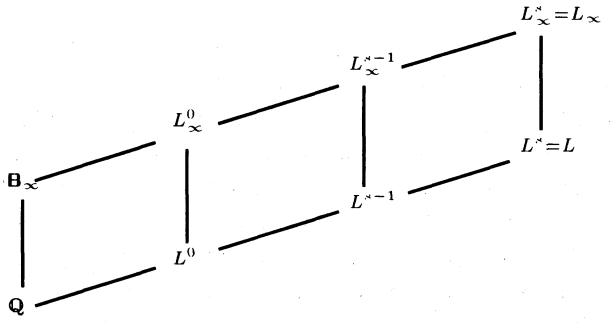
$$L_p(\psi, s) = \frac{G_p(\psi_t, \zeta\kappa^s - 1)}{(\zeta\kappa^s - \kappa)^\delta}$$

(here $\zeta = \theta(\gamma)^{-1}$ and $\delta = 1$ if ψ_t is trivial and 0 otherwise). The following is the Theorem on p. 214 of [7] (previously the Main Conjecture) :

THEOREM II.2.

$$h(\chi_t, T) = G_p(\omega\chi_t^{-1}, T) \quad \textit{up to a unit of } \mathcal{O}_t[[T]]. \qquad \square$$

In the case $p \mid \operatorname{ord} \chi_t$ (*i.e.* $s > 1$), the following notation will be useful. Since $L/\mathbb{Q}$ is cyclic of order divisible by p, there is a unique sequence of subfields $L = L^s \supset L^{s-1} \supset L^{s-2} \ldots \supset L^0$ with $[L^i : L^{i-1}] = p$ for $i = 1, \ldots, s$. (Thus $\operatorname{Gal}(L/L^0) = \mathcal{G}_p$ and $\operatorname{Gal}(L^0/\mathbb{Q}) \cong \mathcal{G}'$). We form $L_n^i =: L^i\mathbf{B}_n$, $L_\infty^i =: L^i\mathbf{B}_\infty$, $A_n(L^i) = \mathcal{C}\ell(L_n^i) \otimes \mathbb{Z}_p$, $A_\infty(L^i) = \bigcup_{n=0}^{\infty} A_n(L^i)$ *etc.* When $i = s$, however, we shall continue to abbreviate $A_\infty(L^s) = A_\infty(L)$ to A_∞ *etc.* :



PROPOSITION II.2. — *Let N_n and η_n denote the maps*

$$(\mathcal{C}\ell(L_n^i) \otimes \mathcal{O}')^{\chi'} \underset{\eta_n}{\overset{N_n}{\rightleftarrows}} (\mathcal{C}\ell(L_n^{i-1}) \otimes \mathcal{O}')^{\chi'}$$

induced by norm and extension of ideals respectively. Then N_n is surjective and η_n is injective for all i and n.

For the proof we shall use the following "well known" result.

LEMMA II.3. — *Let $\mathcal{L}/\mathcal{K}$ be any Galois extension of number fields with group $\mathcal{H}$. Let $U(\mathcal{L})$ denote the product of the local units in the completions of $\mathcal{L}$ at all finite places and let $\eta : Cl(\mathcal{K}) \to Cl(\mathcal{L})$ be the map induced by extension of ideals. Then*

$$\ker \eta \cong \ker(H^1(\mathcal{H}, E(\mathcal{L})) \longrightarrow H^1(\mathcal{H}, U(\mathcal{L}))).$$

Proof of Lemma. — Let $J_f(\mathcal{L})$ denote the finite idèles of $\mathcal{L}$. We have a commuting, exact diagram :

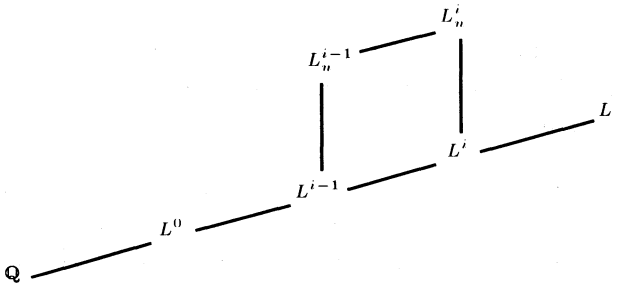
$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(\mathcal{L}) & \longrightarrow & \mathcal{L}^* & \longrightarrow & P(\mathcal{L}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & U(\mathcal{L}) & \longrightarrow & J_f(\mathcal{L}) & \longrightarrow & I(\mathcal{L}) & \longrightarrow & 0\,. \end{array}$$

Take $\mathcal{H}$–invariants to get :

$$\begin{array}{ccccccccc} & & 0 & & 0 & & & & \\ & & \downarrow & & \downarrow & & & & \\ 0 & \longrightarrow & P(\mathcal{K}) & \longrightarrow & P(\mathcal{L})^{\mathcal{H}} & \longrightarrow & H^1(\mathcal{H}, E(\mathcal{L})) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & I(\mathcal{K}) & \longrightarrow & I(\mathcal{L}) & \xrightarrow{\delta} & H^1(\mathcal{H}, U(\mathcal{L})) & & \end{array}$$

(in fact, the map δ is surjective). Now apply the Snake Lemma. □

Proof of Proposition II.2. — Since $h(\mathbb{Q}) = 1$, there is a prime of L totally ramified over L^0. (Otherwise there would be a p–subextension $N/\mathbb{Q}$ of $L/\mathbb{Q}$ unramified everywhere). This prime does not lie over p since $L/\mathbb{Q}$ is tame at p. Since L_n^i/L^i and L_n^{i-1}/L^{i-1} are unramified outside p, it follows that L_n^i/L_n^{i-1} is (totally) ramified at some place w, say, of L_n^i not dividing p. By class field theory this implies that N_n is surjective.



As for η_n, temporarily let C denote $\mathrm{Gal}(L_n^i/L_n^{i-1})$. The actions of $\mathcal{G}'$ and C commute and $\mathcal{O}'$ is flat over $\mathbb{Z}$ so Lemma II.3 gives :

$$\ker \eta_n \cong \ker((H^1(C, E(L_n^i)) \otimes \mathcal{O}')^{\chi'} \longrightarrow (H^1(C, U(L_n^i)) \otimes \mathcal{O}')^{\chi'}).$$

Since $p \nmid |\mathcal{G}'|$, the "χ'−parts" functor commutes with cohomology and since $p \neq 2$, χ' is odd which implies

$$(E(L_n^i) \otimes \mathcal{O}')^{\chi'} \cong (\mu_{p^\infty}(L_n^i) \otimes \mathcal{O}')^{\chi'}.$$

Thus it will suffice to show that

$$\alpha : H^1\big(C, \mu_{p^\infty}(L_n^i)\big) \longrightarrow H^1\big(C, U(L_n^i)\big)$$

is injective. Let k_w denote the residue field of L_n^i at w. Since $p \nmid w$ and w is totally ramified in L_n^i/L_n^{i-1} it follows that

$$\mu_{p^\infty}(L_n^i) \longrightarrow k_w^*$$

is an injective map of trivial C−modules. Thus the map

$$\beta : H^1\big(C, \mu_{p^\infty}(L_n^i)\big) \longrightarrow H^1(C, k_w^*)$$

is injective. But β factors through α, so the latter is also injective, as required. □

COROLLARY II.2. — *For each $i = 1, \ldots, s$ there are exact sequences of $\mathcal{O}'$−modules :*

$$(4)\quad 0 \longrightarrow (\mathcal{C}\ell(L^i) \otimes \mathcal{O}_t)^{\chi_t} \longrightarrow (\mathcal{C}\ell(L^i) \otimes \mathcal{O}')^{\chi'} \longrightarrow (\mathcal{C}\ell(L^{i-1}) \otimes \mathcal{O}')^{\chi'} \longrightarrow 0$$

$$(5)\quad 0 \longrightarrow (A_\infty(L^i) \otimes \mathcal{O}_t)^{\chi_t} \longrightarrow (A_\infty(L^i) \otimes \mathcal{O}')^{\chi'} \longrightarrow (A_\infty(L^{i-1}) \otimes \mathcal{O}')^{\chi'} \longrightarrow 0$$

and

$$(6)\quad 0 \to (\mathrm{Hom}(A_\infty(L^{i-1}), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathcal{O}')^{\chi'^{-1}} \to (\mathrm{Hom}(A_\infty(L^i), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathcal{O}')^{\chi'^{-1}} \to (\mathrm{Hom}(A_\infty(L^i), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathcal{O}_t)_{\chi_t^{-1}} \to 0$$

Proof. — Equation (4) follows from the Proposition (with $n = 0$) plus Corollary II.1. Similarly, passing to the limit over n, the Proposition gives maps N_∞ and η_∞ :

$$(A_\infty(L^i) \otimes \mathcal{O}')^{\chi'} \underset{\eta_\infty}{\overset{N_\infty}{\rightleftarrows}} (A_\infty(L^{i-1}) \otimes \mathcal{O}')^{\chi'},$$

respectively surjective and injective. Applying Corollary II.1 directly gives (5). Applying it to the dual maps

$$\widehat{N_\infty} = \mathrm{Hom}_{\mathcal{O}'}(N_\infty, \mathcal{O}'/F') \quad \text{and} \quad \widehat{\eta_\infty} = \mathrm{Hom}_{\mathcal{O}'}(\eta_\infty, \mathcal{O}'/F')$$

gives (6). □

The following Proposition is useful in extracting from $g(\chi_t, T)$ information about class groups at finite levels in the cyclotomic tower. It is a variation on a well-known result which must be considered afresh because of the possibility that p divides $[L : \mathbb{Q}] = \operatorname{ord} \chi_t$ in our situation.

PROPOSITION II.3. — $\operatorname{Hom}(A_\infty \otimes \mathcal{O}_t , F_t/\mathcal{O}_t)_{\chi_t^{-1}}$ *has no non-trivial finite* $\mathcal{O}_t[[T]]$*−submodules.*

Proof. — By duality it will suffice to show that $(A_\infty \otimes \mathcal{O}_t)^{\chi_t}$ has no non-trivial finite $\mathcal{O}_t[[T]]$−quotients. It is known (*cf.* [5]) that A_∞ has no non-trivial finite $\mathbb{Z}_p[[T]]$−quotients, thus $A_\infty \otimes \mathcal{O}'$ has none for $\mathcal{O}'[[T]]$ and its direct summand $(A_\infty \otimes \mathcal{O}')^{\chi'}$ has none either. When $\chi_t = \chi'$ we are done, so assume $p | \operatorname{ord} \chi_t$ and let C denote $\operatorname{Gal}(L^s/L^{s-1}) \subset \mathcal{G}$.

CLAIM. — $H^1(C, A_\infty^-) = 0$.

Before proving this, let us see that the result follows.

Lemma II.2 gives :

$$(A_\infty \otimes \mathcal{O}_t)^{\chi_t} \cong \ker N_C | (A_\infty \otimes \mathcal{O}')^{\chi'} \quad \textit{as } \mathcal{O}'[[T]] - \textit{modules},$$

where N_C is the norm element of the cyclic group C. On the other hand, since χ' is odd, the Claim shows that the right hand term is actually a quotient of $(A_\infty \otimes \mathcal{O}')^{\chi'}$ and hence has no non-trivial finite quotient modules for $\mathcal{O}'[[T]]$, by the above. *A fortiori* it has none for $\mathcal{O}_t[[T]]$, as required.

Proof of Claim. — Let $I(L_\infty^s)^-$ denote $\varinjlim_n (I(L_n^s) \otimes \mathbb{Z}_p)^-$ and let $P(L_\infty^s)^-$ denote $\varinjlim_n (P(L_n^s) \otimes \mathbb{Z}_p)^-$ *etc.* We have an exact sequence

$$0 \longrightarrow P(L_\infty^s)^- \longrightarrow I(L_\infty^s)^- \longrightarrow A_\infty^- \longrightarrow 0.$$

Hence

$$0 \longrightarrow H^1(C, A_\infty^-) \longrightarrow H^2(C, P(L_\infty^s)^-) \xrightarrow{\alpha} H^2(C, I(L_\infty^s)^-)$$

is exact and we require to prove that α is injective.

Now

$$\ker \alpha = \frac{P(L_\infty^s)^{-, C} \cap N_C I(L_\infty^s)^-}{N_C P(L_\infty^s)^-} \subset \frac{P(L_\infty^s)^{-, C} \cap I(L_\infty^{s-1})^-}{N_C P(L_\infty^s)^-}.$$

The proof of Proposition II.2 shows that $(\mathcal{C}\ell(L_n^{s-1}) \otimes \mathbb{Z}_p)^- \to (\mathcal{C}\ell(L_n^s) \otimes \mathbb{Z}_p)^-$ is injective for all n, which implies $P(L_\infty^s)^{-, C} \cap I(L_\infty^{s-1})^- = P(L_\infty^{s-1})^-$. On

the other hand, we have $H^2(C, L_\infty^{s,*}) = 0$ (see for example [6] Lemma 5, p. 270). Thus Norm : $L_\infty^{s,*} \to L_\infty^{s-1,*}$ is surjective which implies $N_C P(L_\infty^s)^- = P(L_\infty^{s-1})^-$. Thus $\ker \alpha = \{0\}$, which proves the Claim. □

Remark II.2. — Let $\tilde{L}$ denote any abelian extension of $\mathbb{Q}$ containing L. Inflate χ_t to a character of $\mathrm{Gal}(\tilde{L}/\mathbb{Q})$ and consider

$$(\mathrm{Hom}(A_\infty(\tilde{L}), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathcal{O}_t)_{\chi_t^{-1}}.$$

In [7], Proposition 1, it is stated that this has no non-trivial, finite $\mathcal{O}_t[[T]]$–submodules (under the further condition that $\tilde{L} \cap \mathbb{B}_\infty = \mathbb{Q}$). Now, we have used the fact that χ_t is faithful, *i.e.* $\tilde{L} = L$, crucially in the proof of Proposition II.3 and in fact one can give examples to show that when p divides $[\tilde{L} : L]$, Mazur and Wiles' statement may not be valid, even in cases where $p \nmid \mathrm{ord}\, \chi_t$.

Before moving on to the proof of the main result we need a little more notation and a lemma. For a number field N, $I_p(N)$ will denote the subgroup of $I(N)$ generated by primes lying above the rational prime p. $D_n = D_n(L)$ will denote the subgroup of A_n generated by the classes of such primes of L_n, while $D_\infty =: \varinjlim_n D_n \subset A_\infty$ and $D_\infty^- =: \bigcup_{n=0} D_n^-$. Now similar arguments to the proof of Proposition II.1 (*cf.* [1] Proposition II) lead to :

$$(7) \qquad (P(L_k) \otimes \mathbb{Z}_p)^{-,\Gamma_n} = P(L_n)^- \qquad \text{for each } n, k, \quad k \geq n \geq 0$$

and to an exact sequence

$$(8) \qquad 0 \longrightarrow A_n(L)^- \longrightarrow A_k(L)^{-,\Gamma_n} \longrightarrow \left(\frac{I_p(L_k)}{I_p(L_n)} \otimes \mathbb{Z}_p\right)^- \longrightarrow 0$$

since L_k/L_n is ramified precisely at the primes over p. Moreover, these primes are totally ramified in L_k/L, so there is an isomorphism

$$(9) \qquad \left(\frac{I_p(L_k)}{I_p(L_n)} \otimes \mathbb{Z}_p\right) \cong \mathrm{Hom}_{\mathbb{Z}_p\mathcal{D}}(\mathbb{Z}_p\mathcal{G}, (p^{-(k-n)}\mathbb{Z}_p/\mathbb{Z}_p))$$

of $\mathbb{Z}_p\mathcal{G}$–modules, where $\mathcal{D}$ denotes the decomposition group of p in L. By total ramification, the Γ_n–action on $I_p(L_k)$ is trivial. Thus, by (7), principal "ideals" in $(I_p(L_k) \otimes \mathbb{Z}_p)^-$ come from L_n. Consequently :

$$(10) \qquad \text{the map } \left(\frac{I_p(L_k)}{I_p(L_n)} \otimes \mathbb{Z}_p\right)^- \longrightarrow \left(\frac{D_k(L)}{D_n(L)}\right)^- \text{ is an isomorphism.}$$

Putting together (8)–(10) and letting $k \to \infty$ we obtain :

LEMMA II.4. — *For each $n \geq 0$, there is an exact sequence*

$$0 \longrightarrow A_n^- \longrightarrow A_\infty^{-,\Gamma_n} \longrightarrow (D_\infty/D_n)^- \longrightarrow 0$$

so that $A_\infty^{-,\Gamma_n} = A_n^- D_\infty^-$.

Moreover

$$(D_\infty/D_n)^- \cong \left(\frac{I_p(L_\infty)}{I_p(L_n)} \otimes \mathbb{Z}_p\right)^- \cong \mathrm{Hom}_{\mathbb{Z}_p\mathcal{D}}(\mathbb{Z}_p\mathcal{G}, \mathbb{Q}_p/\mathbb{Z}_p)^-$$

as $\mathbb{Z}_p\mathcal{G}$*−modules with trivial* Γ_n*−action.* □

III. THE PROOF OF THEOREM II.1

As in [7], the proof falls into two cases according as $\chi(p)$ is or is not equal to 1, that is, whether or not p splits completely in K.

Case 1 : $\chi(p) \neq 1$.

This includes all the cases where $m \geq 1$, (that is $\rho \neq 1$), so that $\chi(p) = 0$. Recall that, for an even Dirichlet character ψ we have :

$$L_p(\psi, 1-n) = -\frac{1}{n}(1 - \psi_n(p)p^{n-1})B_{n,\psi_n} \qquad \text{for } n = 1, 2, 3 \ldots$$

where $\psi_n =: \omega^{-n}\psi$.

Thus

$$B_{1,\chi^{-1}} = -\frac{L_p(\omega\chi^{-1}, 0)}{(1 - \chi^{-1}(p))} = -\frac{G_p(\omega\chi_t^{-1}, \zeta - 1)}{(1 - \chi^{-1}(p))(\zeta - \kappa)^{\delta_\chi}}$$

where now $\zeta = \rho(c)$ so $v_\mathcal{O}(\zeta - 1) > 0$.

By the Main Conjecture (Theorem II.2) we have :

$$(11) \qquad v_\mathcal{O}(B_{1,\chi^{-1}}) = v_\mathcal{O}(h(\chi_t, \zeta - 1)) - v_\mathcal{O}(1 - \chi^{-1}(p)) - \delta_\chi v_\mathcal{O}(\zeta - \kappa)$$

and $\delta_\chi \neq 0$ implies $\mathcal{O} = \mathbb{Z}_p[\rho]$ so that $v_\mathcal{O}(\zeta - \kappa) = 1$. In view of Proposition II.1, the result will follow from

$$\ell_\mathcal{O}((A_m \otimes \mathcal{O})^\chi) = v_\mathcal{O}(h(\chi_t, \zeta - 1)) - v_\mathcal{O}(1 - \chi^{-1}(p))$$

which follows in turn from the two succeeding propositions, valid when $\chi(p) \neq 1$.

PROPOSITION III.1.

$$v_\mathcal{O}(h(\chi_t, \zeta - 1)) = \ell_\mathcal{O}\left((A_\infty \otimes \mathcal{O})^{\Gamma_m, \chi}\right)$$

and

PROPOSITION III.2.

$$\ell_{\mathcal{O}}((A_m \otimes \mathcal{O})^{\chi}) = \ell_{\mathcal{O}}\big((A_\infty \otimes \mathcal{O})^{\Gamma_m,\chi}\big) - v_{\mathcal{O}}(1-\chi^{-1}(p)).$$

(χ is here regarded as a character of $\mathrm{Gal}(L_m/\mathbb{Q})$*, by inflation).*

Proof of Proposition III.1. — For brevity, let M denote the $\mathcal{O}[[T]]$−module

$$\mathrm{Hom}(A_\infty \otimes \mathcal{O}_t, F_t/\mathcal{O}_t)_{\chi_t^{-1}} \otimes_{\mathcal{O}_t} \mathcal{O} = \mathrm{Hom}(A_\infty \otimes \mathcal{O}, F/\mathcal{O})_{\chi_t^{-1}}.$$

Its Iwasawa polynomial is $g(\chi_t, T)$ regarded as an element of $\mathcal{O}[[T]]$. By Proposition II.3 (applying $\otimes_{\mathcal{O}_t}\mathcal{O}$) and the Structure Theorem for finitely generated, torsion $\mathcal{O}[[T]]$−modules there is an exact sequence

$$0 \longrightarrow M \longrightarrow \bigoplus_{j=1}^{\ell} \mathcal{O}[[T]]/(g_j) \longrightarrow A \longrightarrow 0. \tag{12}$$

Here A is some finite $\mathcal{O}[[T]]$−module and the g_j are polynomials with $\prod_j g_j = g(\chi_t, T)$. Since $h(\chi_t, \zeta - 1) \neq 0$ by (11), $(T - (\zeta^{-1} - 1)) \nmid g_j$ for all j. Thus $(T - (\zeta^{-1} - 1))$ acts injectively on the middle term of (12) and an application of the Snake Lemma yields an exact sequence :

$$\begin{aligned} 0 \longrightarrow \ker(T-(\zeta^{-1}-1))|A \longrightarrow \mathrm{coker}(T-(\zeta^{-1}-1))|M \longrightarrow \\ \bigoplus_j \mathcal{O}[[T]]/(g_j, T-(\zeta^{-1}-1)) \longrightarrow \mathrm{coker}(T-(\zeta^{-1}-1))|A \longrightarrow 0. \end{aligned} \tag{13}$$

It is easy to see that

$$\mathrm{coker}(T-(\zeta^{-1}-1))|M = M_{\Gamma_m,\rho^{-1}}$$

and that

$$\mathcal{O}[[T]]/(g_j, T-(\zeta^{-1}-1)) \cong \mathcal{O}/g_j(\zeta^{-1}-1).$$

Since A is finite, applying $\ell_{\mathcal{O}}$ to (13) gives :

$$\ell_{\mathcal{O}}\big(M_{\Gamma_m,\rho^{-1}}\big) = \sum_j v_{\mathcal{O}}(g_j(\zeta^{-1}-1)) = v_{\mathcal{O}}(h(\chi_t, \zeta - 1)).$$

In particular $M_{\Gamma_m,\rho^{-1}}$ is finite and since

$$M_{\Gamma_m,\rho^{-1}} = \mathrm{Hom}((A_\infty \otimes \mathcal{O})^{\Gamma_m,\chi}, F/\mathcal{O}),$$

Proposition III.1 follows by duality. □

Proof of Proposition III.2. — We shall use the exact sequence

$$0 \longrightarrow A_m^- \otimes \mathcal{O} \longrightarrow (A_\infty^- \otimes \mathcal{O})^{\Gamma_m} \longrightarrow (D_\infty^-/D_m^-) \otimes \mathcal{O} \longrightarrow 0 \tag{14}$$

from Lemma II.4.

The case $\chi = \chi'$ (in which $m = 0$) is dealt with in [7] : since $p \nmid \operatorname{ord}\chi$ and $\chi(p) \neq 1$, Lemma II.4 implies $(D_\infty^-/D_0 \otimes \mathcal{O})^\chi = 0$. Since also $v_\mathcal{O}(1 - \chi^{-1}(p)) = 0$, the result follows from (14) on applying the functor $\_^\chi$.

From now on, assume $\chi \neq \chi'$. Then

$$((D_\infty^-/D_m^-) \otimes \mathcal{O})^\chi \quad \text{and} \quad v_\mathcal{O}(1 - \chi^{-1}(p))$$

are non-zero in general (respectively iff $\chi'(p) = 1$ and iff $\chi'(p) = 1$ and $\rho = 1$). On the other hand, the functor $\_^\chi$ is not exact, so some care is required. We consider the cases $m > 0$, $m = 0$ separately.

Case 1(i) : $m > 0$.

In this case $\rho \neq 1$ so $\chi^{-1}(p) = 0$ and the Proposition will follow from :

$$(A_m^- \otimes \mathcal{O})^\rho \longrightarrow (A_\infty^- \otimes \mathcal{O})^{\Gamma_m, \rho} \quad \textit{is an isomorphism}$$

on applying $\_^{\chi_t}$. Using Lemma II.2 with ρ for χ this in turn will follow from :

$$(\ker N_{\widetilde{C}} | A_m^-) \xrightarrow{\alpha} (\ker N_{\widetilde{C}} | A_\infty^{-,\Gamma_m}) \quad \textit{is an isomorphism}$$

where $\widetilde{C}$ denotes $\operatorname{Gal}(L_m/L_{m-1})$. Now α is clearly injective so take an element x of A_∞^{-,Γ_m} killed by $N_{\widetilde{C}}$ and, by Lemma II.4, write $x = [ad]$, $a \in (I(L_m) \otimes \mathbb{Z}_p)^-$, $d \in (I_p(L_k) \otimes \mathbb{Z}_p)^-$ some $k \geq m$. Clearly $(N_{\widetilde{C}} a) d^p = N_{\widetilde{C}}(ad)$ is in $(P(L_k) \otimes \mathbb{Z}_p)^{m-1}$ hence comes from L_{m-1}, by (7). Thus d^p comes from L_{m-1}. Since all primes above p are totally ramified in L_k/L_{m-1}, d comes from L_m. It follows that α is surjective as required.

Case 1(ii) : $m = 0$.

In this case $\Gamma_m = \Gamma$, $\chi = \chi_t$, $\mathcal{G} = G$, $L_m = L = K$, write K^i for L^i, $i = 0, 1, \ldots, s$ ($K^s = K$), and define $D_n(K^i)$ just as for $D_n = D_n(K)$, for each n and i. Consider the following commuting diagram, with exact rows from Lemma II.4 :

(15)

$$\begin{array}{ccccccccc}
0 & \to & (\mathcal{C}\ell(K) \otimes \mathcal{O}')^{\chi'} & \to & (A_\infty(K) \otimes \mathcal{O}')^{\Gamma, \chi'} & \to & ((D_\infty(K)/D_0(K)) \otimes \mathcal{O}')^{\chi'} & \to 0 \\
 & & \downarrow N' & & \downarrow N & & \downarrow N'' & & \\
0 & \to & (\mathcal{C}\ell(K^{s-1}) \otimes \mathcal{O}')^{\chi'} & \to & (A_\infty(K^{s-1}) \otimes \mathcal{O}')^{\Gamma, \chi'} & \to & ((D_\infty(K^{s-1})/D_0(K^{s-1})) \otimes \mathcal{O}')^{\chi'} & \to 0
\end{array}$$

Here the vertical maps are induced by the norms from K_n to K_n^{s-1}. By Corollary II.2, N' is *surjective* and

$$\ker N' \underset{\mathcal{O}'}{\cong} (\mathcal{C}\ell(K) \otimes \mathcal{O})^\chi \tag{16}$$

and

$$\ker N \underset{\mathcal{O}'}{\cong} (A_\infty(K) \otimes \mathcal{O})^{\Gamma,\chi}. \tag{17}$$

Now identify $((D_n(K)/D_0(K)) \otimes \mathcal{O}')^{\chi'}$ with $((I_p(K_n)/I_p(K)) \otimes \mathcal{O}')^{\chi'}$ by (10) and similarly with K replaced by K^{s-1}. Since K_n^{s-1}/K^{s-1} is totally ramified and K/K^{s-1} unramified at primes above p, we have $I_p(K_n^{s-1}) \cap I_p(K) = I_p(K^{s-1})$ in $I_p(K_n)$ for all n. Thus we may regard

$$((D_\infty(K^{s-1})/D_0(K^{s-1})) \otimes \mathcal{O}')^{\chi'}$$

as a submodule of

$$((D_\infty(K)/D_0(K)) \otimes \mathcal{O}')^{\chi'}$$

and replace N'' by the map induced by N_C on the latter. We then find :

(18)

$$\begin{aligned}\ker N'' &\underset{\mathcal{O}'}{\cong} ((D_\infty(K)/D_0(K)) \otimes \mathcal{O})^{\chi} \text{ by Lemma II.1} \\ &\underset{\mathcal{O}}{\cong} \mathrm{Hom}_{\mathcal{OG}}(\underline{\mathcal{O}}, \mathrm{Hom}_{\mathcal{OD}}(\mathcal{OG}, F/\mathcal{O})) \text{ by Lemma II.4, since } \chi \text{ is odd} \\ &\underset{\mathcal{O}}{\cong} \mathrm{Hom}_{\mathcal{OD}}(\underline{\mathcal{O}}, F/\mathcal{O}) \cong \ker(1-\chi(\sigma))|F/\mathcal{O}\end{aligned}$$

where $\mathcal{D}$ is generated by σ.

Equations (15)–(18), together with the surjectivity of N' give an exact sequence

$$0 \to (\mathcal{C}\ell(K) \otimes \mathcal{O})^{\chi} \to (A_\infty(K) \otimes \mathcal{O})^{\Gamma,\chi} \to \ker(1-\chi(\sigma))|F/\mathcal{O} \to 0 \tag{19}$$

Now suppose that p ramifies in K, then it ramifies tamely so that σ is not of $p-$power order. Since χ is faithful, this implies that

$$\ell_{\mathcal{O}}(\ker(1-\chi(\sigma))|(F/\mathcal{O})) = v_{\mathcal{O}}(1-\chi(\sigma)) = 0 = v_{\mathcal{O}}(1-\chi^{-1}(p))$$

and the Proposition follows from (19) in this case. If p is unramified, we may take $\sigma = \sigma_p$ so $\chi(\sigma) \neq 1$ and again the result follows from (19). □

This concludes the proof of Theorem II.1 in the case $\chi(p) \neq 1$.

Case 2 : $\chi(p) = 1$.

Since χ is faithful, $\mathcal{D} = \{1\}$ and p splits completely in K. Also, $m = 0$ so $\chi = \chi_t$, $\mathcal{G} = G$, $L = K$ and we write K^i for L^i as in Case 1(ii). The method of that case fails because $h(\chi_t, 0) = 1 - \chi(p)^{-1} = 0$ and indeed the last two non-zero modules in (19) are *infinite*. To harness the force of Theorem II.2 one must therefore factor out the "trivial" zero of $h(\chi_t, T)$ both algebraically and analytically. The method we shall use is an

adaptation of that explained in [7] (due to Greenberg) to suit our situation in which p may divide ord χ.

Algebraically, "removal of the zero" means replacing A_∞ by A_∞/D_∞ : for each i and n we denote $A_n(K^i)/D_n(K^i)$ by $E_n(K^i)$. Let

$$E_\infty(K^i) = \varinjlim_n E_n(K^i)$$

(in fact $E_\infty(K^i)^- = \bigcup_n E_n(K^i)^-$ by an easy argument). Also define $\Delta(K^i)$, a submodule of $H^1(\Gamma, D_\infty(K^i))$, by the exactness of the sequence

$$0 \longrightarrow D_\infty(K^i) \longrightarrow A_\infty(K^i)^\Gamma \longrightarrow E_\infty(K^i)^\Gamma \longrightarrow \Delta(K^i) \longrightarrow 0.$$

Since χ' is odd and $p \nmid |G'|$, Lemma II.4 gives :

$$(A_\infty(K^i)^\Gamma \otimes \mathcal{O}')^{\chi'} = (\mathcal{C}\ell(K^i) \otimes \mathcal{O}')^{\chi'} (D_\infty(K^i) \otimes \mathcal{O}')^{\chi'}.$$

Thus we have an exact sequence :

$$(20) \quad 0 \longrightarrow D_0(K^i)^{\chi'} \longrightarrow \mathcal{C}\ell(K^i)^{\chi'} \longrightarrow E_\infty(K^i)^{\chi',\Gamma} \longrightarrow \Delta(K^i)^{\chi'} \longrightarrow 0$$

where we have omitted $\otimes\mathcal{O}'$ from the notation.

Analytically, we need to work with $L_p'(\omega\chi^{-1}, 0)$. This was shown to be non-zero by Greenberg and Ferrero who evaluated it in terms of the p–adic logarithms of certain Gauss sums which we now define. Fix a prime $\mathfrak{p}$ above p in K and a prime $\mathfrak{P}$ above $\mathfrak{p}$ in $\mathbb{Q}(f)$. If k denotes the residue field at $\mathfrak{P}$ then for $x \in k^*$ the power residue symbol $\left(\frac{x}{\mathfrak{P}}\right)$ is defined by

$$\left(\frac{x}{\mathfrak{P}}\right) \in \mu_f \ , \quad \left(\frac{x}{\mathfrak{P}}\right) \equiv x^{|k^*|/f} \bmod \mathfrak{P}.$$

Choose a primitive p^{th} root of unity $\zeta \in \overline{\mathbb{Q}}$ and define the Gauss sum

$$\gamma = -\sum_{x \in k^*} \left(\frac{x}{\mathfrak{P}}\right) \zeta^{\mathrm{Tr}(x)}$$

where Tr denotes the trace from k to $\mathbb{Z}/p\mathbb{Z}$.

We find that γ^f, a priori an element of $\mathbb{Q}(pf)$, is actually in N, the decomposition field of p in $\mathbb{Q}(f)$ and is independent of the choice of ζ. Define $\overline{\gamma}$ to be $\mathrm{Norm}_{N/K}\, \gamma^f \in K$ and note :

(i) $\overline{\gamma}$ depends only on $\mathfrak{p}$. Furthermore, replacing $\mathfrak{p}$ by $\mathfrak{p}^\sigma$ for $\sigma \in G$ replaces $\overline{\gamma}$ by $\overline{\gamma}^\sigma$

(ii) $\overline{\gamma}$ is a p–unit. Indeed, by Stickelberger's Theorem :

$$(21) \qquad \overline{\gamma}\mathcal{O}_K = \mathfrak{p}^\theta \quad \text{where } \theta = \sum_{\substack{0<a<f \\ (a,f)=1}} a\sigma_a^{-1} \in \mathbb{Z}G$$

(iii) If we let $t_{\mathfrak{p}}$ denote the embedding of K in its completion at $\mathfrak{p}$ (isomorphic to $\mathbb{Q}_p$) and $\log_p$ the p–adic logarithm normalized by $\log_p(p)=0$, then

$$L_p'(\omega\chi^{-1},0) = -\frac{1}{f}\sum_{\sigma\in G}\chi^{-1}(\sigma)\log_p(t_{\mathfrak{p}}(\overline{\gamma}^{\sigma})) \neq 0 \tag{22}$$

(see [2]). This gives :

LEMMA III.1.

$$g(\chi,0) = 0$$

and

$$v_{\mathcal{O}}(g'(\chi,0)) = v_{\mathcal{O}}\Big(\frac{1}{p}\sum_{\sigma\in G}\chi^{-1}(\sigma)\log_p(t_{\mathfrak{p}}(\overline{\gamma}^{\sigma}))\Big) < \infty.$$

Proof. — Theorem II.2 implies

$$g(\chi,\kappa^{-s}-1) = u(\kappa^{-s}-1)L_p(\omega\chi^{-1},s) \quad \text{for any } s\in\mathbb{Z}_p$$

where $u(T)\in\mathcal{O}[[T]]^*$. Since $\chi(p)=1$, the right hand side is zero when $s=0$. Now differentiate both sides with respect to s and set $s=0$. □

Let $\mathfrak{p}^{(i)}$ denote the prime of K^i below $\mathfrak{p}$, $i=0,1,\ldots,s$. Starting with $\mathfrak{p}^{(i)}$ one defines $\mathfrak{P}^{(i)}$, $\gamma^{(i)}$ *etc.* by exact analogy with $\mathfrak{P}$, γ *etc.* In general, the notation for an object associated to K (*e.g.* f, G) will be augmented by a superscript 'i' to denote the version for K^i (*e.g.* $f^{(i)}, G^i$).

Let $W(K^i)$ denote the group of p–units of K^i regarded as a subgroup of $W(K^s)=W(K)$. The element $\overline{\gamma}^{(i)}\in W(K^i)$ is, in a sense, analogous to a cyclotomic unit of K^i. Its image in $(W(K^i)\otimes\mathbb{Z}_p)^-$ generates a $\mathbb{Z}_pG^i$–submodule which is not in general of finite index. This can be remedied by adding as further generators the p–units derived from Gauss-sums corresponding to all subfields of K^i of strictly smaller conductor (a similar phenomenon occurs with cyclotomic units). However, for our purposes, it will suffice to define submodules

$$V(K^i) =: \langle W(K^{i-1}), \mathbb{Z}G^i\overline{\gamma}^{(i)}\rangle \subset W(K^i)\ , \quad i=1,\ldots,s$$

and

$$V(K^0) =: \mathbb{Z}G^0\,\overline{\gamma}^{(0)} \subset W(K^0)$$

and work with

$$(V(K^i)\otimes\mathcal{O}')^{\chi'} \subset (W(K^i)\otimes\mathcal{O}')^{\chi'}.$$

Now define $\mathbb{Z}_pG$–linear maps

$$\mu,\lambda : W(K)\otimes\mathbb{Z}_p \longrightarrow I_p(K)\otimes\mathbb{Z}_p$$

by $\mu(x \otimes 1) = \sum_{\mathfrak{q}} \mathfrak{q} \otimes \mathrm{ord}_{\mathfrak{q}}(x)$

$$\lambda(x \otimes 1) = \sum_{\mathfrak{q}} \mathfrak{q} \otimes \log_{\mathfrak{q}}(t_{\mathfrak{q}}(x))$$

where $\mathfrak{q}$ runs over all primes dividing p in K, and $t_{\mathfrak{q}}$ denotes the embedding of K in its completion at $\mathfrak{q}$ (isomorphic to $\mathbb{Q}_p$). Clearly, λ and μ induce maps from $W(K^i)\otimes\mathcal{O}'$ to $I_p(K^i)\otimes\mathcal{O}'$, (denoted by the same letters) taking χ'−parts to χ'−parts. Since $\mu_p \notin K$ and χ' is odd, μ is an embedding on χ'−parts and λ will turn out to be one also. Also note that the image of λ is contained in $(pI_p(K) \otimes \mathcal{O}')^{\chi'}$. (We shall often omit $\otimes\mathcal{O}'$ for brevity).

Since $\left(\frac{I_p(K^i)}{\mu W(K^i)}\right)^{\chi'} \cong D_0(K^i)^{\chi'}$, we have, from (20) :

LEMMA III.2. — *For $i = 0, \ldots, s$, there are exact sequences of $\mathcal{O}'$−modules :*

$$(23)\quad 0 \longrightarrow \left(\frac{\mu W(K^i)}{\mu V(K^i)}\right)^{\chi'} \longrightarrow \left(\frac{I_p(K^i)}{\mu V(K^i)}\right)^{\chi'} \longrightarrow \mathcal{C}\ell(K^i)^{\chi'} \longrightarrow E_\infty(K^i)^{\Gamma,\chi'} \longrightarrow \Delta(K^i)^{\chi'} \longrightarrow 0$$

and

$$(24)\quad 0 \longrightarrow \left(\frac{\lambda W(K^i)}{\lambda V(K^i)}\right)^{\chi'} \longrightarrow \left(\frac{pI_p(K^i)}{\lambda V(K^i)}\right)^{\chi'} \longrightarrow \left(\frac{pI_p(K^i)}{\lambda W(K^i)}\right)^{\chi'} \longrightarrow 0.$$

The method of [7] for the case $\chi = \chi'$ consists essentially in showing that all the modules in (23) and (24) are finite and calculating and comparing their lengths. When $\chi \neq \chi'$ (*i.e.* $s > 0$) we shall recover the result by considering the sequences for $i = s$, $s - 1$ simultaneously. One could easily treat the case $s = 0$ in parallel. For simplicity, however, we shall assume $s > 0$ and refer to [7] for the case $s = 0$. In particular, this means we can assume that for $i = 0$, all modules in (23) and (24) are *finite*.

LEMMA III.3. — *$(E_\infty(K^s)\otimes\mathcal{O}')^{\Gamma,\chi'}$ and $(E_\infty(K^{s-1})\otimes\mathcal{O}')^{\Gamma,\chi'}$ are finite and*

$$\ell_{\mathcal{O}'}((E_\infty(K^s)\otimes\mathcal{O}')^{\Gamma,\chi'}) - \ell_{\mathcal{O}'}((E_\infty(K^{s-1})\otimes\mathcal{O}')^{\Gamma,\chi'}) = v_{\mathcal{O}}\left(\frac{1}{p}\sum_{\sigma\in G}\chi^{-1}(\sigma)\log_p(t_{\mathfrak{p}}(\bar{\gamma}^\sigma))\right).$$

Proof. — For $i = 1, \ldots, s$ let $a_i(\chi', T)$, $e_i(\chi', T) \in \mathcal{O}'[T]$ denote the Iwasawa polynomials of

$$(\mathrm{Hom}(A_\infty(K^i), \mathbb{Q}_p/\mathbb{Z}_p)\otimes\mathcal{O}')^{\chi'^{-1}}$$

and

$$(\mathrm{Hom}(E_\infty(K^i), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathcal{O}')^{\chi'^{-1}}$$

as $\mathcal{O}'[[T]]-$modules respectively. Since $\mathcal{D}^i = 1$, it follows from Lemma II.4 applied to K^i that

$$(\mathrm{Hom}(D_\infty(K^i), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathcal{O}')^{\chi'^{-1}}$$

has a submodule of finite index isomorphic to $\mathcal{O}'^{p^i}$ with trivial $\Gamma-$action. By the multiplicativity of Iwasawa polynomials, this gives

$$a_i(\chi', T) = e_i(\chi', T)T^{p^i}. \tag{25}$$

Also, by (6) of Corollary II.2 :

$$a_i(\chi', T) = a_{i-1}(\chi', T)f_i(T) \quad \text{for } i = 1, \ldots, s \tag{26}$$

where $f_i(T)$ is the Iwasawa polynomial of $(\mathrm{Hom}(A_\infty(K^i), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathcal{O})_\chi$ considered as an $\mathcal{O}'[[T]]-$*module*. By considering characteristic polynomials, it is not hard to see that

$$f_s(T) = \prod_\alpha g(\chi, T)^\alpha$$

where α runs through $\mathrm{Gal}(F/F')$. Thus, from (25) $(i = s, s-1)$ and (26) $(i = s)$ we get

$$e_s(\chi', T) = e_{s-1}(\chi', T) \prod_\alpha (g(\chi, T)/T)^\alpha$$

and so

$$v_{\mathcal{O}'}(e_s(\chi', 0)) = v_{\mathcal{O}'}(e_{s-1}(\chi', 0)) + v_{\mathcal{O}}(g'(\chi, 0)) \quad (\infty \textit{ allowed}). \tag{27}$$

On the other hand, $(\mathrm{Hom}(E_\infty(K^i), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathcal{O}')^{\chi'^{-1}}$, as a submodule of $(\mathrm{Hom}(A_\infty(K^i), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathcal{O}')^{\chi'^{-1}}$, has no nontrivial, finite $\mathcal{O}'[[T]]-$quotients, so arguing as in Proposition III.1, $v_{\mathcal{O}'}(e_i(\chi', 0)) = \ell_{\mathcal{O}'}((E_\infty(K^i) \otimes \mathcal{O}')^{\Gamma, \chi'})$ (both sides being simultaneously finite or infinite). Thus, the Lemma follows from (27) and Lemma III.1 provided that $(E_\infty(K^{s-1}) \otimes \mathcal{O}')^{\Gamma, \chi'}$ is finite. For $s = 1$ the latter is assumed (case $\chi = \chi'$) and so the result may be established by an induction on s. □

LEMMA III.4. — *The injection* $I_p(K^{s-1}) \otimes \mathcal{O}' \to I_p(K^s) \otimes \mathcal{O}'$ *induces injective maps of* $\mathcal{O}'-$*modules :*

$$\left(\frac{pI_p(K^{s-1})}{\lambda W(K^{s-1})}\right)^{\chi'} \xrightarrow{\alpha} \left(\frac{pI_p(K^s)}{\lambda V(K^s)}\right)^{\chi'}$$

and

$$\left(\frac{I_p(K^{s-1})}{\mu W(K^{s-1})}\right)^{\chi'} \xrightarrow{\beta} \left(\frac{I_p(K^s)}{\mu V(K^s)}\right)^{\chi'}$$

where $\otimes\mathcal{O}'$ has been omitted from the notation. Moreover

$$\ell_{\mathcal{O}'}(\operatorname{coker}\alpha) = v_{\mathcal{O}}\Big(\frac{1}{p}\sum_{\sigma\in G}\chi^{-1}(\sigma)\log_p(t_{\mathfrak{p}}(\overline{\gamma}^{\sigma}))\Big) \tag{28}$$

and

$$\ell_{\mathcal{O}'}(\operatorname{coker}\beta) = v_{\mathcal{O}}(B_{1,\chi^{-1}}). \tag{29}$$

Proof. — Consider α. First identify $pI_p(K^s)\otimes\mathcal{O}'$ with $\mathcal{O}'G$ via the $\mathcal{O}'G$–isomorphism taking $\mathfrak{p}\otimes p$ to 1. Thus $\lambda(\overline{\gamma}\otimes 1)$ corresponds to $\frac{1}{p}\sum_{\sigma\in G}\log_p(t_{\mathfrak{p}}(\overline{\gamma}^{\sigma}))\sigma^{-1}$. For brevity, denote the latter by ε, and the image of $\lambda(W(K^{s-1})\otimes\mathcal{O}')$ under this identification by $A\subset N_C\mathcal{O}'G$. Thus α becomes the map

$$\Big(\frac{N_C\mathcal{O}'G}{A}\Big)^{\chi'} \xrightarrow{\ \alpha\ } \Big(\frac{\mathcal{O}'G}{\varepsilon\mathcal{O}'G+A}\Big)^{\chi'}$$

(χ'–parts are just the images under the action of the idempotent attached to χ'). Now, it is easy to see that χ induces an isomorphism of $\mathcal{O}'$–algebras

$$(\mathcal{O}'G)^{\chi'}/N_C(\mathcal{O}'G)^{\chi'} \xrightarrow[\sim]{} \mathcal{O}$$

(*cf.* the proof of Lemma II.2), so consider the following commuting square

$$\begin{array}{ccc} (\mathcal{O}'G)^{\chi'}/N_C(\mathcal{O}'G)^{\chi'} & \xrightarrow[\sim]{x} & \mathcal{O} \\ \downarrow \times\varepsilon & & \downarrow \times\chi(\varepsilon) \\ (\mathcal{O}'G)^{\chi'}/N_C(\mathcal{O}'G)^{\chi'} & \xrightarrow[\sim]{x} & \mathcal{O} \end{array}$$

Now $\chi(\varepsilon) = \frac{1}{p}\sum_{\sigma\in G}\chi^{-1}(\sigma)\log_p(t_{\mathfrak{p}}(\overline{\gamma}^{\sigma})) \neq 0$. Thus the left hand vertical map is injective from which one deduces that α is injective, using the fact that $N_C\varepsilon = \lambda(\operatorname{Norm}_{K^s/K^{s-1}}\overline{\gamma}\otimes 1)$ is in A, by definition of $W(K^{s-1})$. Since the left-hand vertical map has the same cokernel as α, (28) also follows. (Note that $\mathcal{O}/\mathcal{O}'$ is totally ramified). The proof of the statements about β is similar : this time, identify $I_p(K^s)\otimes\mathcal{O}'$ with $\mathcal{O}'G$ by taking $\mathfrak{p}\otimes 1$ to 1. Then $\mu(\overline{\gamma}\otimes 1)$ corresponds to $\theta\in\mathcal{O}'G$ by (21) and the proof proceeds as before. □

COROLLARY III.1. — *The modules* $\Big(\frac{pI_p(K^i)}{\lambda V(K^i)}\Big)^{\chi'}$ *and* $\Big(\frac{I_p(K^i)}{\mu V(K^i)}\Big)^{\chi'}$ *are finite, for* $i = 0, 1, \ldots, s$.

Proof. — The statement for $i = 0$ is from the case $\chi = \chi'$. Inductively we may assume the statement holds for $i = 0, \ldots, s-1$. *A fortiori*, $\left(\frac{pI_p(K^{s-1})}{\lambda W(K^{s-1})}\right)^{\chi'}$ and $\left(\frac{I_p(K^{s-1})}{\mu W(K^{s-1})}\right)^{\chi'}$ are finite. Since the right hand sides of (28), (29) are finite, the statement holds for $i = s$. □

Together with Lemma III.3 this implies

COROLLARY III.2. — *For $i = s$, $s-1$, each of the modules in (23) and (24) is finite.* □

Next, the extreme terms of (23) "cancel" with those of (24). More precisely :

LEMMA III.5. — *There are isomorphisms*

(i) $\left(\frac{pI_p(K^i)}{\lambda W(K^i)}\right)^{\chi'} \cong (\Delta(K^i))^{\chi'}$ *and*

(ii) $\left(\frac{\mu W(K^i)}{\mu V(K^i)}\right)^{\chi'} \cong \left(\frac{\lambda W(K^i)}{\lambda V(K^i)}\right)^{\chi'} \cong \left(\frac{W(K^i)}{V(K^i)}\right)^{\chi'}$ *for $i = s$, $s-1$.*

Proof. — The isomorphism (i) is essentially Proposition 3 p. 222 of [7]. The proof goes through because we now know that both $E_\infty(K^i)^{\chi',\Gamma}$ and $\left(\frac{pI_p(K^i)}{\lambda W(K^i)}\right)^{\chi'}$ are finite. The finiteness of the latter also implies that λ is injective on $W(K^i)^{\chi'}$ (which is torsionfree). Since μ is also injective, (ii) follows. □

COROLLARY III.3.

$$(30)\quad \ell_{\mathcal{O}'}(C\ell(K^s)^{\chi'}) = \ell_{\mathcal{O}'}\left(\left(\frac{I_p(K^s)}{\mu V(K^s)}\right)^{\chi'}\right) + \ell_{\mathcal{O}'}(E_\infty(K^s)^{\Gamma,\chi'}) - \ell_{\mathcal{O}'}\left(\left(\frac{pI_p(K^s)}{\lambda V(K^s)}\right)^{\chi'}\right)$$

and

$$(31)\quad \ell_{\mathcal{O}'}(C\ell(K^{s-1})^{\chi'}) = \ell_{\mathcal{O}'}\left(\left(\frac{I_p(K^{s-1})}{\mu W(K^{s-1})}\right)^{\chi'}\right) + \ell_{\mathcal{O}'}(E_\infty(K^{s-1})^{\Gamma,\chi'}) - \ell_{\mathcal{O}'}\left(\left(\frac{pI_p(K^{s-1})}{\lambda W(K^{s-1})}\right)^{\chi'}\right)$$

(All terms being *finite*.)

Proof. — (23) and (24) together with Corollary III.2 and Lemma III.5 give (30) and also a similar equation with K^s replaced by K^{s-1}.

Adding and subtracting $\ell_{\mathcal{O}'}\left(\left(\frac{W(K^{s-1})}{V(K^{s-1})}\right)^{\chi'}\right)$ from the right hand side of the latter gives (31). □

To conclude the proof of Theorem II.1 in the case $\chi(p) = 1$, we need $\ell_{\mathcal{O}'}(\mathcal{C}\ell(K^s) \otimes \mathcal{O})^{\chi}) = v_{\mathcal{O}}(B_{1,\chi^{-1}})$. This follows on subtracting (31) from (30) and applying Corollary II.2, equation (4) to evaluate the left hand side and Lemmas III.3 and III.4 to evaluate the right hand side of the resulting equation.

The material described here appeared largely in the author's PhD thesis [10] in relation to a conjecture of Lichtenbaum on Artin L–functions at $s = 0$. I would like to thank my advisor, T. Chinburg and also R. Greenberg, K. Rubin, R. Schoof and M. Taylor for helpful and interesting conversations.

This work was partially supported by a grant from the S.E.R.C.

BIBLIOGRAPHY

[1] L. FEDERER, B. GROSS, Regulators and Iwasawa Modules, Inventiones Mathematicae, 62 (1981), 443–457.

[2] B. FERRERO & R. GREENBERG, On the Behavior of the p–Adic L–function at $s = 0$, Inventiones Mathematicae, 50 (1978), 91–102.

[3] B. FERRERO & L. WASHINGTON, The Iwasawa invariant μ_p vanishes for abelian number fields, Annals of Math., 109 (1979), 377–396.

[4] G. GRAS, Etude d'invariants relatifs aux groupes des classes des corps abéliens, Astérisque, 41–42 (1977), 35–53.

[5] R. GREENBERG, On p–Adic L–functions and Cyclotomic Fields II, Nagoya Math. J., 67 (1977), 139–158.

[6] K. IWASAWA, Riemann-Hurwitz Formula and p–Adic Galois Representations for Number Fields, Tôhoku Math. J., 33 (1981), 263–288.

[7] B. MAZUR & A. WILES, Class Fields of Abelian Extensions of $\mathbb{Q}$, Inventiones Mathematicae, 76 (1984), 179–330.

[8] K. RUBIN, Kolyvagin's System of Gauss Sums. Preprint.

[9] K. RUBIN, The Main Conjecture. Appendix to : Cyclotomic Fields I and II, combined 2nd edition, by S. Lang. Grad. Texts in Math., 121, Springer-Verlag, New York (1990), 397–419.

[10] D. SOLOMON, On Lichtenbaum's Conjecture in the Case of Number Fields, PhD. Thesis, Brown University, 1988.

Manuscrit reçu le 16 novembre 1989,
révisé le 25 juin 1990.

David SOLOMON,
Department of Mathematics
U.M.I.S.T.
Sackville Street
Manchester M60 1QD (U.K.).