ANNALES DE L'INSTITUT FOURIER

CORNELIUS GREITHER

Class groups of abelian fields, and the main conjecture

Annales de l'institut Fourier, tome 42, nº 3 (1992), p. 449-499

<http://www.numdam.org/item?id=AIF_1992__42_3_449_0>

Ann. Inst. Fourier, Grenoble
42, 3 (1992), 449-499.

CLASS GROUPS OF ABELIAN FIELDS, AND THE MAIN CONJECTURE

by Cornelius GREITHER

Introduction.

The relative class number $h^{-}(F)$ of an abelian number field F is expressed by the analytic class number formula (roughly speaking) as a product of certain generalized Bernouilli number $\mathbf{B}_{1,\chi}$. It is customary here to fix a prime p and only consider the p-parts of the involved numbers. It is natural to ask for an algebraic version of that formula which connects the orders of χ-parts of p-class groups to p-parts of individual generalized Bernouilli number $\mathbf{B}_{1,\chi}$. A precise formulation of this idea has been proved by Greenberg, Mazur and Wiles (see Mazur, Wiles [17]) for odd p and $[F:\mathbb{Q}]$ not divisible by p, and by Solomon [22] for odd p and rather general abelian fields F. (The first-mentioned result is called Conjecture of Leopoldt and Iwasawa.) In this paper we prove a similar theorem for $p = 2$. This also gives an amelioration of Stickelberger's annihilation theorem « by a factor two », a result obtained previously by G. Gras in many cases. A simple nontrivial example for this is the class group of $F = \mathbb{Q}(\zeta_{29})$. It is $(\mathbb{Z}/2\mathbb{Z})^3$, equal to the minus class group, and the customary form of Stickelberger's theorem gives no information on its Galois module structure at all.

In a similar vein, the p-adic class number formula connects the class number of a real abelian field F with a product of certain values $L_p(1,\chi)$. Since this formula also contains the regulator of F (which is hard to evaluate), it is more convenient to deal with χ-parts of ray class groups modulor p^{∞} (one must assume χ nontrivial in order that these χ-parts be finite). One then gets a real analog of the Conjecture

Key words : Cyclotomic extensions - Iwasawa theory - Class groups - p-adic L-functions - Units.

A.M.S. Classification : 11R18 - 11R23 - 11R29 - 11R42 - 11R27.

of Iwasawa and Leopoldt, which we again prove for all p. As a consequence one obtains, building on work of Greenberg and Sinnott, a generalization of Gras' conjecture, which postulates a close connection between the class group of the real field F and the quotient group of the units of F by the circular units.

All these results are based on the Main Conjecture for F. This conjecture, which identifies the characteristic power series of certain projective limits of p-class groups with certain p-adic L-series, was proved for odd p and $F/\mathbb{Q}$ abelian by Mazur and Wiles (1984). Their methods have been developed further by Wiles (1990), so that now the Main Conjecture is established even for Galois extensions of a totally real ground field if $p \neq 2$, and (at least) for abelian extensions of $\mathbb{Q}$ if $p = 2$. Nevertheless, for abelian fields there is now a much more elementary approach which uses « Euler systems », is due to Kolyvagin and was developed by Rubin (see e.g. Rubin [19]). It seems that this has not yet been done for all p and all abelian F, so we offer in this paper (§ 3) a detailed proof of the « full » main conjecture, including in particular the case $p = 2$. (It is probably no surprise that the technique of Kolyvagin and Rubin is supple enough to do this.) We use Euler systems of circular units to prove a « real main conjecture » in § 3 and get back on the minus side using Kummer duality and the appropriate general form of Iwasawa's and Gillard's results on semilocal units modulo circular units which we prove in § 2. (Of course, one can go the other way and use this, and the main conjecture as proved by Wiles, to infer the « real main conjecture ».)

The final section § 4 is devoted to the aforementioned applications: χ-parts of class groups, imaginary and real. We draw on methods of Greenberg and Sinnott, and ideas of Solomon.

Notation is standard if not explained. Throughout, ζ_n is a primitive n-th root of unity and $\mathbb{Q}(n) = \mathbb{Q}(\zeta_n)$. Because of the technical character of § 2-4, we had to redefine notations at some points. Note in particular that X is an indeterminate in § 2 but X is an Iwasawa module in the other sections.

At the end of this introduction, we discuss what we call « χ-parts ». Let p be any prime, and let us agree that all characters are p-adic, i.e. take values in the algebraic closure of $\mathbb{Q}_p$. Each character χ of an abelian field is also considered as a primitive Dirichlet character whenever the need arises.

Definition. — *Let Δ be any finite abelian group, χ a character of Δ, and M any $\mathbb{Z}_p[\Delta]$-module. Let $\mathbb{Z}_p(\chi) = \mathbb{Z}_p(\chi(\delta) \mid \delta \in \Delta)$. Then $M_\chi = M \otimes_{\mathbb{Z}_p[\Delta]} \mathbb{Z}_p(\chi)$ is called the χ-part of M. We sometimes denote the canonical surjection $M \to M_\chi$ just by $y \mapsto y_\chi$, $y \in M$.*

We list some simple, mostly well-known properties:

(*a*) The functor $M \mapsto M_\chi$ is right exact; if $|\Delta|$ is prime to p, it is even exact.

(*b*) If χ is conjugate to ψ over $\mathbb{Q}_p$ (i.e. there is an automorphism τ of $\mathbb{Q}_p^{alg}$ over $\mathbb{Q}_p$ with $\psi = \tau\chi$), then $M_\chi \simeq M_\psi$ over $\mathbb{Z}_p[\Delta]$.

(*c*) Let $S = \mathbb{Z}_p[\Delta]$. The ideals $\ker(S \to S_\chi = \mathbb{Z}_p(\chi))$, χ character of Δ, are just the minimal prime ideals of S.

(*d*) If $|\Delta|$ is prime to p, then S is a product of (complete) discrete valuation rings, and for any S-module M, the canonical map $M \to \prod M_\chi$ (product over all characters χ of Δ, modulo $\mathbb{Q}_p$-conjugacy) is an isomorphism.

Now assume also that $\Delta = \mathrm{Gal}(F/\mathbb{Q})$, F an (abelian!) number field. Let j denote complex conjugation, considered as an element of Δ. Recall: a character χ is *odd* if $\chi(j) = -1$, *even* if $\chi(j) = 1$.

(*e*) If χ is odd, then $1 + j$ maps to 0 in S_χ (recall $S = \mathbb{Z}_p[\Delta]$), hence for any M, $(1+j)M$ goes to zero in M_χ.

(*f*) If $M = A_p(F)$, $M^+ = A_p(F^+)$, then the norm $M \to M^+$ is onto as is well-known. Consequently, the image $\mathrm{im}\, M^+$ of M^+ in M coincides with $(1+j)M$, and we obtain for odd χ from (*a*) and by right exactness: $M_\chi \simeq (M/\mathrm{im}\, M^+)_\chi$.

We need one last observation:

(*g*) If $p = 2$, and Δ is cyclic of order 2^r with generator δ_0, say, and $j \neq 1$ (i.e. F is imaginary), then for every odd χ and every module M on which j acts as multiplication by -1 (M is a « minus module »), we have $M_\chi = M$. (Proof: Since $\chi(j) = -1$, χ must be injective with $\mathrm{Im}(\chi) = \langle \zeta_{2^r} \rangle$, and hence $\mathbb{Z}_2(\chi) \simeq \mathbb{Z}_2[T]/(T^{2^{r-1}}+1) \simeq \mathbb{Z}_2[\delta_0]/(j+1)$. From this we obtain $M_\chi = M/(1+j)M = M$.) More generally, if $\Delta = \Delta_2 \times \Delta_0$, with $|\Delta_0|$ odd and Δ_2 cyclic of 2-power order, then for any odd character χ of Δ one has $M_\chi \simeq M_{\chi_0}$ with $\chi_0 = \chi | \Delta_0$.

Most of this paper was written during a one-year stay of the author at the University of Karlsruhe. It is a pleasure to thank this institution, and Mathematisches Institut II in particular, for their hospitality.

1. The Main Conjecture and its consequences.

We shall first state the Main Conjecture for all p. To this end, let F be an abelian number field, unramified in p, with Galois group Δ. Further, let $K_n = F(\zeta_{2p^{n+1}})(n \geqslant 0)$, $K_\infty = \bigcup K_n$, $G = \mathrm{Gal}(K_\infty/\mathbb{Q}) \simeq \Delta \times \mathbb{Z}_p^\times \simeq \Delta' \times \Gamma$ with $\Gamma = \mathrm{Gal}(K_\infty/K_0) \simeq \mathbb{Z}_p$ and $\Delta' = \mathrm{Gal}(K_0/\mathbb{Q})$. We may consider any character χ of Δ also as a character of Δ'. Moreover one has the Teichmüller character $\omega : G \to \mu_{2p} \subset \overline{\mathbb{Q}_p}$. Let us make the convention $\check{\chi} = \chi^{-1}\omega$.

By $G_p(T,\psi)$ (for ψ an even character of Δ', considered as primitive p-adic Dirichlet character), we denote the element in $\mathrm{Quot}(\mathbb{Z}_p(\psi)[[T]])$ which is written $f(T,\psi)$ in Washington [23], p. 122. In particular:

$$L_p(s,\psi) = G_p(u^s-1,\psi) \text{ for } s \in \mathbb{Z}_p, \ (s \neq 1 \text{ for } \psi \text{ trivial})$$

where $u = 1 + q_0$ is an integer fixed in the construction of G_p, see *loc. cit*. For ψ nontrivial, $\frac{1}{2} G_p(T,\psi)$ is in $\mathbb{Z}_p(\psi)[[T]]$. For ψ the trivial character, $\frac{1}{2} G_p(T,\psi)\cdot(T-q_0)$ is in $\mathbb{Z}_p(\psi)[[T]]$, and even a unit, see Washington [23], p. 125. For any number field K, denote the p-part of the class group of K by $A_p(K)$. The correct formulation for the main conjecture including $p = 2$ is now (cf. Federer [4]):

THEOREM (=Thm. 3.2). — *Let* $X = \varprojlim A_p(K_n)$, $X^+ = \varprojlim A_p(K_n^+)$. *Let* χ *be any odd character of* Δ'. *Then* $(X/\mathrm{im}\, X^+)_\chi \simeq X_\chi$ *canonically, and we have*

$$\mathrm{char}\,(X_\chi) = \left(\frac{1}{2}\cdot G_p(T,\check{\chi})\right) \textit{ if } \check{\chi} \textit{ is not trivial},$$

$$\mathrm{char}\,(X_\chi) = \left(\frac{1}{2}\cdot G_p(T,\check{\chi})\cdot(T-q_0)\right) = (1) \textit{ if } \check{\chi} \textit{ is trivial},$$

as ideals of the ring $\Lambda_\chi = \mathbb{Z}_p(\chi)[[T]]$. (*For the notation* «char» *see* Rubin [19].)

Remark. — The canonical isomorphism in the theorem is easy to see: Since the norm map $A_2(K_n) \to A_2(K_n^+)$ is surjective, the group $\mathrm{im}\, A_2(K_n^+)$ is contained in $(1+j)\cdot A_2(K_n)$. Whenever χ is odd, all multiples of $1 + j$ map to zero in $A_2(K_n)_\chi$, and the map $A_2(K_n)_\chi \to A_2(K_n^+)_\chi$ is already the zero map.

The theorem will be proved in § 3 (using the result of § 2). We now describe the arithmetical consequences, starting with the following analog of a conjecture of Iwasawa and Leopoldt for $p = 2$:

THEOREM A. – *If $F/\mathbb{Q}$ is abelian imaginary, unramified in 2, with Galois group Δ; such that the 2-Sylow subgroup Δ_2 is cyclic, then for every odd 2-adic character χ of Δ which is not of 2-power order :*

$$|A_2(F)^-_\chi| = \left|\frac{1}{2}\mathbf{B}_{1,\chi^{-1}}\right|_2^{d(\chi)} .$$

(*Notation.* – $|a|_2 = 2^e$ for $a = 2^e \cdot u \in \mathbb{Z}_2(\chi)$, u a unit; $d(\chi) = [\mathbb{Z}_2(\chi) : \mathbb{Z}_2]$. Further, $A_2(F)^-_\chi$ is the χ-part of the minus part $A_2(F)^- = \{x \in A_2(F) : x^j = -x\}$. The notion « χ-part » has been explained in the introduction.)

Remark. – *a*) Write $\Delta = \Delta_2 \times \Delta_0$, $|\Delta_0|$ odd. For any character χ of Δ, let $\chi_0 = \chi|\Delta_0$. Then χ has 2-power order iff χ_0 is the trivial character ε of Δ_0. The idempotent $e_\varepsilon = |\Delta_0|^{-1} \cdot \sum_{\delta \in \Delta_0} \delta$ lies in $\mathbb{Z}_2[\Delta]$. It is then a corollary of Thm. A that the $\mathbb{Z}_2\Delta_0$-module $(1-e_\varepsilon) . A_2(F)^-$ (i.e. we remove the trivial representation of Δ_0 from $A_2(F)^-$) is annihilated by 1/2 times the images in $(1-e_\varepsilon)\mathbb{Z}_2[\Delta]/(1+j)$ of all the usual Stickelberger elements belonging to F. This is a sharpening of Stickelbergers's Theorem for $p = 2$, and generalizes results of Gras [7]. Examples show that some condition on Δ_2 is necessary.

b) There is, up to $\mathbb{Q}_2$-conjugacy, just one odd character χ_2 for Δ of 2-power order. Let L be the fixed field of Δ_0. Then one obtains from the analytic class number formula $|A_2(F)^-_{\chi_2}| = |A_2(L)^-| = 2 \cdot |2^{-1}\mathbf{B}_{1,\chi_2^{-1}}|_2 \cdot k_L$, where $k_L = |\ker(A_2(L^+) \to A_2(L))|$. We used that $Q_L = 1$.

As is common in such situations, one can show that it is enough to prove a divisibility statement in Thm. A. Moreover, on can replace the left hand side by another term which is easier to treat. This leads to the following formulation :

THEOREM B (= Thm. 4.1). – *For all odd characters χ of Δ which are not of 2-power order :*

$$\left|\left(\frac{A_2(F)}{\operatorname{im} A_2(F^+)}\right)_\chi\right| \quad \textit{is divisible by} \quad \left|\frac{1}{2}\mathbf{B}_{1,\chi^{-1}}\right|^{d(\chi)} .$$

(Note that the expression inside $|\cdot|$ on the left is isomorphic to $A_2(F)_\chi/\mathrm{im}\,(A_2(F^+)_\chi)$, by our definition of χ-components and right exactness of $\otimes$, and also to $A_2(F)_\chi$, since χ is odd and the norm: $A_2(F) \to A_2(F^+)$ is onto.)

Thm. B will be derived from the main conjecture in § 4. Here we show how Thm. A follows from Thm. B: Let $L = F^{\Delta_0}$ as in the last Remark. Note that $A_2(L)^- \simeq e_\varepsilon A_2(F)^-$. Now $|A_2(F)^-| = h_2^-(F)\cdot k_F$ and similarly for L (see Remark *b*)). One sees that $k_F = k_L$, hence one gets from the analytic class number formula that $|(1-e_\varepsilon)A_2(F)^-|$ equals the product over all odd χ with $\chi|\Delta_0 \neq \varepsilon$, modulo $\mathbb{Q}_2$-conjugacy, of $|2^{-1}B_{1,\chi^{-1}}|_2^{d(\chi)}$. Moreover (for the same set of χ's) one has $|A_2(F)_\chi^-| = |(A_2(F)/\mathrm{im}\,A_2(F^+))_\chi|$, and the product of all these terms equals $|(1-e_\varepsilon)A_2(F)^-|$. From this one sees that Thm. B implies Thm. A.

Theorem A has a counterpart for real fields. Assume as above $F/\mathbb{Q}$ abelian, unramified in p (p is again arbitrary) with $\mathrm{Gal}\,(F/\mathbb{Q}) = \Delta = \Delta_0 \times \Delta_p, \Delta_p$ the p-part of Δ.

THEOREM C. — *If F is real and Δ_p is cyclic, then for all characters χ of Δ whose order is not a power of p (i.e. $\chi|\Delta_0 \neq \varepsilon$), and which are faithful on Δ_p, we have*

$$|A'_p(F)_\chi| = \left|\frac{1}{2}L_p(1,\chi)\right|_p^{d(\chi)},$$

where $A'_p(F)$ is the p-part of the projective limit of the ray class groups $C_{(p^\nu)}(F)$, $\nu \in \mathbb{N}$. (Note that $A'_p(F)$ is infinite, but we will see that $(1-e_\varepsilon)A'_p(F)$ is finite.)

We shall also obtain a generalization of Gras' conjecture. For the precise statement, see Thm. 4.14. We only mention the following corollary (see 4.15): If $p=2$ and $|\Delta|$ is odd, then E/C_1 and $A_2(F)$ have isomorphic composition series as $\mathbb{Z}_2[\Delta]$-modules, where $E = \mathcal{O}_F^\times$ and C_1 is the « large » group of circular units of F, as defined by Sinnott [20], p. 209. For odd p, a similar result has been proven (modulo the main conjecture) by Greenberg [9].

Finally let us mention that (as Wiles points out) the 2-adic main conjecture implies the 2-part of the Birch-Tate conjecture by a theorem of Kolster [14], so that now the full Birch-Tate conjecture is established for real abelian fields.

2. Semilocal units and circular units.

Let p be a prime number, and $F/\mathbb{Q}$ abelian such that p does not divide the conductor of F. Define:

$K_n = F(\zeta_{2p^{n+1}})$, $K_\infty = \bigcup K_n$;

$\mathcal{U}_n = (\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_{K_n})^\times$ (semilocal units of K_n over p);

U_n = pro-p-part of $\mathcal{U}_n$ (= principal semilocal units);

$\mathcal{C}_n$ = circular units of K_n in the sense of Sinnott;

$\bar{\mathcal{C}}_n$ = closure of $\mathcal{C}_n$ in $\mathcal{U}_n$; C_n = pro-p-part of $\bar{\mathcal{C}}_n$;

$\mathcal{C}_\infty = \varprojlim \bar{\mathcal{C}}_n \subset \mathcal{U}_\infty = \varprojlim \mathcal{U}_n$;

C_∞ = pro-p-part of $\mathcal{C}_\infty$; U_∞ = pro-p-part of $\mathcal{U}_\infty$.

Let χ be any nontrivial character of $\mathrm{Gal}(F/\mathbb{Q})$.

LEMMA 2.1. — *Suppose $F' \subset F$, and denote* $\mathrm{Gal}(F/F')$ *by H. Define $\mathcal{U}'_n$ for F' in the same way as $\mathcal{U}_n$ as F. Then the kernel and the cokernel of the map*

$$\alpha : (\mathcal{U}_n)_H \to \mathcal{U}'_n \text{ (the subscript } H \text{ means : take } H\text{-coinvariants)},$$

induced by the norm $F \to F'$, are annihilated by the number $|H| \doteq [F:F']$.

Proof. — The kernel in question is $H^1(H,\mathcal{U}_n)$, and the cokernel is $\check{H}^0(H,\mathcal{U}_n)$. □

COROLLARY. — *If χ is already a character of F', i.e. $\chi(H) = 1$, then the kernel and cokernel of the natural map*

$$\alpha_\chi : (\mathcal{U}_\infty)_\chi \to (\mathcal{U}'_\infty)_\chi$$

are annihilated by the number $[F:F']^2$.

Proof. — Let $A = \ker(\alpha)$, $B = \mathrm{coker}(\alpha)$. On taking χ-parts, we obtain:

$A_\chi \to \mathcal{U}_{\infty,\chi} \to \mathrm{Im}(\alpha)_\alpha \to 0$ (we may drop the suffix $-_H$);

$\mathrm{Tor}(\mathbb{Z}_p(\chi), B) \to \mathrm{Im}(\alpha)_\chi \to \mathcal{U}'_{\infty,\chi} \to B_\chi \to 0$.

(Tor is taken over $\mathbb{Z}_p[\mathrm{Gal}\,(F/\mathbb{Q})]$.) Then $[F:F']$ annihilates A_χ, B_χ and $\mathrm{Tor}\,(\mathbb{Z}_p(\chi), B)$. The two sequences, together with Lemma 2.1, give the corollary. □

Lemma 2.1 is an instance of the more general

LEMMA 2.2. – *Let $H \subset \Delta$ be finite abelian groups, X a $\mathbb{Z}_p\Delta$-module, X' a $\mathbb{Z}_p(\Delta/H)$-module. Assume there exist Δ-maps $N: X \to X'$ and $i: X' \to X$ such that Ni = multiplication by $|H|$, and iN = multiplication by $\sum_{\sigma\in H}\sigma$. Then kernel and cokernel of the induced map $\bar{N}: X_H \to X$ are annihilated by $|H|$. (Example : $X = A_p(F)$, $X' = A_p(F')$).*

The proof is easy. □

We need a better understanding of the projective limit of the circular units. One could do without the following lemma if one just took the right hand side in its statement instead of the left hand side in all what follows, but this would be somewhat unsatisfactory.

LEMMA 2.3. – *Let F be as above, and let $m = \mathrm{cond}\,(F)$ (hence m is not divisible by p). Let $G = \mathrm{Gal}\,(K_\infty/\mathbb{Q})$. Then we have up to a finite prime-to-p torsion group :*

$$C_\infty = \textit{closure of the } \mathbb{Z}_pG\textit{-span of } \{\pm\eta_{m',F} \,|\, 1 \neq m' | m\} \cup \mathscr{C}_\infty(\mathbb{Q}(\zeta_{p^\infty})),$$

with

$$\eta_{m',F} = (\mathrm{N}_{\mathbb{Q}(m')/\mathbb{Q}(m')\cap F}(1-\zeta_m^{p^{-\nu}}\cdot\zeta_{p^{\nu+t}}))_{\nu\in\mathbb{N}} \quad \begin{matrix}(t=2 \text{ for } p=2,\\ t=1 \text{ for } p\neq 2).\end{matrix}$$

Proof. – The relation « $\supset$ » is evident from the definition of circular units. (Note here that the η's are well-defined, i.e. we do have a norm-coherent sequence on the right.)

« $\subset$ » : We make three preliminary remarks.

1) If some relative norm of some circular number x is a (circular) unit, then x is itself a unit, hence a circular unit by definition (Sinnott [20], p. 202).

2) Fix an abelian extension $k/\mathbb{Q}$. We claim : In Sinnott's definition of circular numbers in k

$$D(k) = \mathbb{Z}[\mathrm{Gal}\,(k/\mathbb{Q})] - \mathrm{span}\,\{\pm N_{\mathbb{Q}(n)/\mathbb{Q}(n)\cap k}(1-\zeta_n^a) \,|\, n, a \in \mathbb{N}\}$$

we may just as well take $a = 1$: it is allright to restrict to all a dividing n; let $n' = n/a$. Since the map $\mathrm{Gal}\,(\mathbb{Q}(n)/\mathbb{Q}(n) \cap k) \to \mathrm{Gal}\,(\mathbb{Q}(n')/\mathbb{Q}(n') \cap k)$ is surjective, one easily sees that $N_{\mathbb{Q}(n)/\mathbb{Q}(n)\cap k}(1-\zeta_n^a)$ equals $N_{\mathbb{Q}(n')/\mathbb{Q}(n')\cap k}(1-\zeta_{\eta'})^{\beta}$, β a suitable element of $\mathbb{Z}[\mathrm{Gal}\,(k/\mathbb{Q})]$.

3) Let $k/\mathbb{Q}$ be abelian of conductor dividing m. Define $D_m(k) = D(k) \cap \mathcal{O}_k[m^{-1}]$. Then $D_m(k) = \langle \pm N_{\mathbb{Q}(n)/k\cap\mathbb{Q}(n)}(1-\zeta_n) | n \text{ divides } m \rangle$.

(Proof of 3): « $\supset$ » is clear since the right hand side consists of circular numbers, and also of m-units.

« $\subset$ »: We first claim that we may even omit in the definition of $D(k)$ all n which are not prime to m *and* do not divide m. For suppose n is not prime to m, i.e. $n' = \mathrm{gcm}(n,m) \neq 1$. One quickly checks that $N_{\mathbb{Q}(n)/\mathbb{Q}(n')}(1-\zeta_n)$ is in the Galois span of $1-\zeta_{n'}$, and $\mathbb{Q}(n) \cap k = \mathbb{Q}(n') \cap k$, hence the contribution of n is already covered by the contribution of n'.

Now we can show « $\subset$ » in 3): Consider an expression

$$\prod_{n|m} N_{\mathbb{Q}(n)/k\cap\mathbb{Q}(n)}(1-\zeta_n)^{\alpha_n} \cdot \prod_{(u,n)=1} N_{\mathbb{Q}(u)/k\cap\mathbb{Q}(u)}(1-\zeta_u)^{\alpha_u}$$

(second product also finite, of course), and assume it represents an m-unit. Since $k \cap \mathbb{Q}(u)$ is just $\mathbb{Q}$ for all u prime to m, the second $\prod$ is an integer, prime to m. The first $\prod$, however, is an m-unit. Hence the second $\prod$ is $\pm$ 1, and Remark 3) is proved).

After these remarks, we can now prove « $\subset$ » of Lemma 2.3. It suffices to show for all $\nu > 0$.

$$(*) \quad (\text{universal norms in } \mathscr{C}_\nu) \subset \langle \{\pm \eta_{m'F}^{(\nu)} | 1 \neq m' | m\} \cup \mathscr{C}_\nu(\mathbb{Q}) \rangle$$

with $\eta_{m'F}^{(\nu)} = N_{m'}(1-\zeta_{m'}\zeta_{p^{\nu+t}})$ and $N_{m'}$ short for $N_{\mathbb{Q}(m')/\mathbb{Q}(m')\cap F}$, and $\langle \cdots \rangle$ means « closure of Galois span of .. ».

It does not change anything if we also admit all $\eta_{m'F}^{(\nu')}$ with $0 \leqslant \nu' \leqslant \nu$ in the right side of (*). Denote the right side of (*) by A_ν; write A'_ν for the group that we get if we replace $\mathscr{C}_\nu(\mathbb{Q}) = \mathscr{C}(\mathbb{Q}(\zeta_{p^{\nu+t}}))$ by $D(\mathbb{Q}(\zeta_{p^{\nu+t}}))$. (This amounts to adjoining the circular number $1-\zeta_{p^{\nu+t}}$.) Write $N_{\nu+\mu/\nu}$ for the norm from $K_{\nu+\mu}$ to K_ν, and D_ν for the circular numbers $D(K_\nu)$.

Claim (**). – $N_{\nu+\mu/\nu}(D_\nu) \subset A'_\nu . (D_\nu)^{p^\mu}$ for all $\mu \geqslant 0$.

This claim implies the lemma as follows: Letting $\mu \to \infty$, we find that the universal norms in D_ν are contained in $A'_\nu \cdot$(non-p torsion of D_ν). We now intersect with the global units of K_ν, taking into account Remark 1). We find: The universal norms in $\mathscr{C}_\nu$ lie in $A_\nu \cdot$(a prime-to-p torsion group). Passing to the closure and to the projective limit, we get « $\subset$ » of Lemma 2.3.

We still have to show (**). From Remark 3) we know

$$D(F_{\nu+\mu}) = \text{Galois span } \{\pm x(n) | n = m' \cdot p^\alpha, m' | m, 0 \leqslant \alpha \leqslant \nu + t + \mu\}$$

with $x(n) = N_{\mathbb{Q}(n)/K_{\nu+\mu} \cap \mathbb{Q}(\nu)}(1-\zeta_n)$. Let $N = N_{\nu+\mu/\mu}$. What is $N(x(n))$? For $\alpha \leqslant \nu + t$, $x(n)$ is already in K_ν, hence N acts on it as p^μ-th power. For $\alpha > \nu + t$ and $m' \neq 1$, one easily checks that $x(n)$ is in the Galois span of $\eta_{m',F}^{(\nu+\mu)}$, and hence $N(x(n))$ is in A_ν. Finally, for $m' = 1$, we certainly have $N(\alpha(n)) \in D_\nu(\mathbb{Q}) \subset A'_\nu$. This finishes the proof of Lemma 2.3.

Remark. – We conjecture that a similar lemma concerning the projective limit of certain Stickelberger ideals is true.

It is now our objective to establish a sort of isomorphism of U_∞/C_∞ with a certain factor ring of $\mathbb{Z}_p[[X]][\Delta']$ (X an indeterminate), $\Delta' = \mathrm{Gal}(K_0/\mathbb{Q})$. We employ Coleman's technique, working over $\mathbb{Q}_p$ (i.e. with denominators) towards the end. (NB. The indeterminate is T, not X, in Coleman's paper. We shall reserve the letter T for the indeterminate in Iwasawa algebras.)

Recall p is an arbitrary prime. Let $\mathcal{O}$ be a finite unramified Galois extension of $\mathbb{Z}_p$ with Galois group Δ. (Later on, $\mathcal{O}$ will be $\mathcal{O}_F$, $F/\mathbb{Q}$ abelian, unramified over p.) If $e_1, \ldots, e_g$ are the primitive idempotents of $\mathcal{O}$, then $\mathbb{Z}_p^g = e_1\mathbb{Z}_p \times \cdots \times e_g\mathbb{Z}_p$ is a subring of $\mathcal{O}$, and all $e_i\mathcal{O}$ are discrete valuation rings. The stabilizer D in Δ of e_i is independent of i and may be called the decomposition group of $\mathcal{O}$.

Definition. – a) $\mathcal{O}[[X]]^0 = \{f \in \mathcal{O}[[X]] : f(0) \equiv 1 \bmod p\}$.

b) $\varphi : \mathcal{O}[[X]] \to \mathcal{O}[[X]]$ *is the unique* $\mathbb{Z}_p$-*algebra endomorphism given by* $\varphi | \mathcal{O} =$ Frob = Frobenius *of* p, *and* $\varphi(1-X) = (1-X)^p$. Frob *has a continuation to* $\mathcal{O}[[X]]$ *with* $X \mapsto X$, *which we also call* Frob.

Let $\Gamma' = \mathbb{Z}_p^\times$. Then Δ and Γ' operate on $\mathcal{O}[[X]]$, the latter via $[a](1-X) = (1-X)^a$, $a \in \mathbb{Z}_p^\times$. Recall $t = 1$ for p odd, $t = 2$ for $p = 2$.

THEOREM 2.4 (Coleman [2]). — *After choosing a generator $\zeta = (\zeta_{p^{\nu+t}})$ of $\mathbb{Z}_p(1) = \varprojlim \mu_{p^{\nu+t}}$, one has for odd p an exact sequence of $\Delta \times \Gamma'$-modules, where Γ' operates on $\mathbb{Z}_p(1)$ in the usual manner : $[a]\zeta = \zeta^a$.*

$$0 \to \mathbb{Z}_p(1)^g \to \mathcal{O}[[X]]^0 \xrightarrow{\left(1-\frac{\varphi}{p}\right)\log} \mathcal{O}[[X]] \to \mathbb{Z}_p(1)^g \to 0\,.$$

For $p = 2$, replace the terms $\mathbb{Z}_p(1)^g$ by $(\mathbb{Z}_p(1) \times \{1, -1\})^g$. The map from the i-th factor $\mathbb{Z}_p(1)[\times\{1, -1\}]$ is given by $\zeta \mapsto e_i(1-X)$ (and $-1 \mapsto -e_i$ for $p=2$); the map to the i-th factor $\mathbb{Z}_p(1)[\times\{1, -1\}]$ is given by

$$f \mapsto \zeta^{\mathrm{Tr}\,(e_i f'(0))} \quad (\mathrm{Tr} : \mathcal{O} \to \mathbb{Z}_p \textit{ the trace}) \textit{ for } p \neq 2\,,$$

$$f \mapsto (\zeta^{\mathrm{Tr}\,(e_i f'(0))}, (-1)^{\mathrm{Tr}\,(e_i f(0))}) \textit{ for } p = 2\,.$$

Proof. — One easily reduces to the case $g = 1$, i.e. $\mathcal{O}$ a domain. In this case, this is essentially Theorem 2.2 of Coleman [2]. We explain the differences in notation, and terminology : our $\mathcal{O}$ is $\mathcal{O}_H$ in *loc. cit*; our $\mathcal{O}[[X]]$ is I; the maximal ideal (p,X) is $\mathfrak{m}$ in *loc. cit*; Coleman's formal group $\mathcal{F}$ is just the multiplicative group G_m our context, and $\mathcal{F}(\mathfrak{m}) = \mathcal{O}[[X]]^0$. Coleman establishes the following sequence :

$$0 \to \mathcal{C}[+][\mathcal{A}_\infty]X \to \mathcal{F}(\mathfrak{m}) \xrightarrow{\Theta_{\mathcal{F}}} A \to 0\,.$$

The term $\mathcal{F}(\mathfrak{m}) = \mathcal{O}[[X]]^0$ is already one term of the sequence we want. We shall verify : the first nonzero term is $\mathbb{Z}_p(1)[\times\{1, -1\}]$; the term A is isomorphic to $\ker(\mathcal{O}[[X]] \to \mathbb{Z}_p(1)[\times\{1, -1\}])$, and the maps are correct.

We first look at $\Theta_{\mathcal{F}}$. By def. (*loc. cit.* p. 108), $\Theta_{\mathcal{F}} = \Theta \circ \lambda$ with λ = Lubin-Tate logarithm of $\mathbf{G}_m$ = the usual log function, and Θ the map $f \mapsto f - \frac{\varphi f \pi}{\pi}\cdot$ Here, just for the moment, φ is Coleman's notation, i.e. φ is Frobenius. Since we may take π (the parameter) $= p$, and f_p is $[p]f$ in our notation, we find (in our notation) that $\Theta_{\mathcal{F}} = \left(1 - \frac{\varphi}{p}\right)\log$.

Next, consider $\mathcal{C}$. This is defined in *loc. cit.* as the group of torsion points of $\mathcal{F} = \mathbf{G}_m$ in $\mathcal{O}$ which are $\equiv 1 \bmod \pi = p$, i.e. $\mathcal{C} = 1$ for p odd and $\mathcal{C} = \{1, -1\}$ for $p = 2$. The symbol $[+]$ is the group law in

$\mathscr{F}$, i.e. just multiplication. Moreover $\mathscr{A}_\infty$ is defined as the closure of $\mathcal{O}_K[G_\infty]$ in R_∞ (notations K, G_∞, R_∞ from Coleman p. 94); in our situation this simplifies to: $\mathscr{A}_\infty =$ profinite group ring $\mathbb{Z}_p[[\Gamma']]$, and $[\mathscr{A}_\infty]X =$ topological span of all $(1-X)^a$, $a \in \Gamma' \simeq \mathbb{Z}_p$. Hence the beginning of Coleman's sequence is $0 \to (1-X)^{\mathbb{Z}_p}[\times\{1,-1\}] \to \mathcal{O}[X]]^0$, and $(1-X)^{\mathbb{Z}_p}$ is Γ-isomorphic to $\mathbb{Z}_p(1)$.

Finally we calculate A: In *loc. cit.*, we find

$$A=\{g\in\mathcal{O}[[X]] \mid \frac{d}{dX}g(0)\in(1-\mathrm{Frob})\mathcal{O}\} \ (p \text{ odd})$$

$$=\{g\in\mathcal{O}[[X]] \mid \frac{d}{dX}g(0)\in(1-\mathrm{Frob})\mathcal{O}, g(0)\in 2\mathcal{O}+(1-\mathrm{Frob})\mathcal{O}\} \ (p=2).$$

Since $(1-\mathrm{Frob})\mathcal{O} = \ker(\mathrm{Tr}:\mathcal{O}\to\mathbb{Z}_p)$, we find that A is in fact the kernel of our map $\mathcal{O}[[X]] \to \mathbb{Z}_p(1)[\times\{1,-1\}]$; to conclude, one has to make sure the latter is surjective, but this is easy. □

Definition. – $R = \mathcal{O}[[\Gamma']]$, $F = \mathbb{Q}_p\mathcal{O}$. *(For $\mathcal{O}$ a domain, $F =$ Quot$(\mathcal{O})$.) Let R operate on $\mathcal{O}[[X]]$ as follows: it is clear how $\mathcal{O}$ operates, and for $a \in \Gamma'$, we let $[a](1-X) = (1-X)^a$ as earlier.*

Lemma 2.5. – $\mathcal{O}[[X]] = R\cdot(1-X) + \varphi(\mathcal{O}[[X]])$.

Proof. – As in Coleman [3], Lemma 2. (Note $\varphi(1-X) = (1-X)^p$.) □

Definition. – *Let $\mathscr{S} : \mathbb{Z}_p[[X]] \to \mathbb{Z}_p[[X]]$ be the trace operator in the sense of Coleman* [2], [3]. *$\mathscr{S}$ has an $\mathcal{O}$-linear prolongation to $\mathcal{O}[[X]]$. Define $\mathscr{V} = \ker(\mathscr{S} : \mathcal{O}[[X]] \to \mathcal{O}[[X]])$.*

Theorem 2.6. – $\mathscr{V} = R\cdot(1-X)$.

Proof. – We have $\mathscr{S}(1-X) = 0$ (easy, see Coleman [3] p. 1). The identity (6) in *loc. cit.* generalizes in our context to give

$$\mathscr{S}\varphi(g) = p\cdot\mathrm{Frob}(g) \quad (g \in \mathcal{O}[[X]])$$

(check it on $\mathcal{O}$ and $\mathbb{Z}_p[[X]]$). Hence $\mathscr{S}\varphi$ is injective. The rest of the proof goes as in Coleman [3], Thm. 3. □

COROLLARY 2.7. – *Let $D : \mathcal{O}[[X]] \to \mathcal{O}[[X]]$ be the $\mathcal{O}$-linear operator $(1-X)\cdot\frac{d}{dX}$. Then $D\mathcal{V} = \mathcal{V}$, and there is an R-isomorphism*

$$D : \mathcal{V} \to \mathcal{V}(1) = \mathcal{V} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1), \ z \mapsto Dz \otimes \zeta.$$

Proof. – First of all, $D(1-X) = (1-X)\cdot(1-X)' = -(1-X)$. Since $D([a]g) = a\cdot([a]D(g))$ for all $a \in \mathbb{Z}_p^\times$ (chain rule, see Coleman [3] p. 2), we obtain $DRg = RDg$, hence $D : \mathcal{V} \to \mathcal{V}$ is well-defined and surjective by Thm. 2.6 (put $g = 1-X$). From the same rule as in the last sentence, one sees that $D : \mathcal{V} \to \mathcal{V}(1)$ is R-linear. Finally, $D|\mathcal{V}$ is injective: $\ker(D) = \ker(d/dX) = \mathcal{O} \subset \mathcal{O}[[X]]$, and $\mathcal{O} \cap \mathcal{V} = 0$ ($\mathcal{S}$ is multiplication by p on $\mathcal{O}$). □

Now let $\mathcal{N} : \mathcal{O}((X))^\times \to \mathcal{O}((X))^\times$ be Coleman's norm operator (Coleman [2] Thm. 11).

DEFINITION. – $\mathfrak{M} = \{f \in \mathcal{O}((X))^\times \mid \mathcal{N}f = \text{Frob}(f)\}$; $\mathfrak{M}^0 = \mathfrak{M} \cap \mathcal{O}[[X]]^0$.

According to Coleman [2] Thm. 16, for every norm-coherent sequence $\alpha = (\alpha_i)_{i\in\mathbb{N}}$, $\alpha_i \in F(\zeta_{p^{i+t}})^\times$, there exists exactly one $f = f_\alpha \in \mathfrak{M}$ with

$$f_\alpha(1-\zeta_{p^{i+t}}) = \text{Frob}^i(\alpha_i), \qquad i \geqslant 0.$$

Note that in our situation $\mathcal{O}$ is allowed to be a *finite product* of maximal orders in p-adic fields (and F a product of p-adic fields), which does not present problems.

THEOREM 2.8 (Coleman [2]). – *There is an exact sequence*

$$0 \to \mathbb{Z}_p(1)^g \to \mathfrak{M}^0 \xrightarrow{\beta} \mathcal{V} \to \mathbb{Z}_p(1)^g \to 0.$$

Proof. – We use 2.4. Since $\mathcal{N}(1-X) = 1 - X = \text{Frob}(1-X)$, we have $1 - X \in \mathfrak{M}^0 \subset \mathcal{O}[[X]]^0$. Claim: The precise preimage under $\beta : = (1-p^{-1}\varphi)\log$ of $\mathcal{V} \subset \mathcal{O}[[X]]$ is $\mathfrak{M}^0[\times\{1,-1\}^g]$ (no $[\cdot\cdot]$ term for p odd), the map $\mathcal{O}[[X]] \to (\mathbb{Z}_p(1)[\times\{1,-1\}])^g$ has the same kernel as the restricted map $\mathcal{V} \to \mathbb{Z}_p(1)^g$, and this restricted map is surjective. From this claim, and Theorem 2.4, one deduces

$$0 \to (\mathbb{Z}_p(1)[\times\{1,-1\}])^g \to \mathfrak{M}^0[\times\{1,-1\}^g] \to \mathcal{V} \to \mathbb{Z}_p(1)^g \to 0,$$

which gives the theorem.

Proof of claim. – One may again assume $g = 1$. We use the identity $\varphi(f) = p \cdot \mathrm{Frob}\,(f)$ (cf. Coleman [3]), and the identity $\mathcal{S}\log(f) = \log(\mathcal{N}f)$, see Coleman [2], remark following Cor. 12. We calculate for $f \in \mathcal{O}[[X]]^0$:

$$\begin{aligned}\mathcal{S}\left(\left(1-\frac{\varphi}{p}\right)\log f\right) &= \mathcal{S}\log(f) - \mathrm{Frob}\,(\log(f))\\ &= \log \mathcal{N}f - \log(\mathrm{Frob}\,(f))\\ &= \log(\mathcal{N}(f)/\mathrm{Frob}\,(f)).\end{aligned}$$

Recall $\mathcal{V}$ was $\ker(\mathcal{S})$. Hence: $\beta(f) \in \mathcal{V} \Leftrightarrow \mathcal{S}\beta(f) = 0 \Leftrightarrow \log(\mathcal{N}(f)/\mathrm{Frob}\,(f)) = 0 \Leftrightarrow \mathcal{N}(f)/\mathrm{Frob}\,(f)$ a root of unity, and $\equiv 1 \bmod p\mathcal{O}$. For odd p, 1 is the only such root of unity, and for $p = 2$, there are two, $+1$ and -1. For odd p, we therefore may continue: $\cdots \Leftrightarrow \mathcal{N}(f) = \mathrm{Frob}\,(f) \Leftrightarrow f \in \mathfrak{M}^0$. For $p = 2$, we have $\mathcal{N}(-1)/\mathrm{Frob}\,(-1) = +1/-1 = -1$, and we obtain as correct condition: $\cdots \Leftrightarrow +f$ or $-f$ is in $\mathfrak{M}^0$, as claimed.

The surjectivity of $\mathcal{V} \to \mathbb{Z}_p(1)$ is seen by taking elements $y \cdot (1-X)$, $y \in \mathcal{O}$. For odd p, we are done. It remains to see that the maps $\mathcal{V} \to \mathbb{Z}_p(1) \times \{1, -1\}$ and $\mathcal{V} \to \mathbb{Z}_p(1)$ have the same kernel for $p = 2$. In elementary terms: if $g \in \mathcal{V}$, and if we know $g'(0)$, then we know $g(0) \bmod 2$. This is left as an exercise; use 2.6. □

LEMMA 2.9. – *Let* $U_i = \{x \in \mathcal{O}[\zeta_{p^{i+1}}] \mid x \equiv 1 \bmod (1-\zeta_{p^{i+1}})\}$. *Then the assignment* $\psi : \varprojlim U_i \to \mathfrak{M}$, $\alpha \mapsto f_\alpha$, *defines a* $\mathbb{Z}_p[[\Gamma']]$*-isomorphism* $U_\infty = \varprojlim U_i \to \mathfrak{M}^0$.

Proof. – This is Corollary 17 in Coleman [2]. □

From Thm. 2.8, Cor. 2.7, and Lemma 2.9 we now may deduce:

PROPOSITION 2.10. – *Let* $\delta = D\log : \mathcal{O}[[X]] \to F[[X]]$. *Recall* Δ *is the Galois group of* $\mathcal{O}$ *over* $\mathbb{Z}_p$. *Then we have an exact sequence of* $\mathbb{Z}_p[[\Gamma']][\Delta]$*-modules*

$$0 \to \mathbb{Z}_p(1)^g \to \mathfrak{M}^0 \xrightarrow{\alpha} \mathcal{V}(1) \to \mathbb{Z}_p(1)^g \to 0$$

with $\alpha = D\beta = D\left(1-\frac{\varphi}{p}\right)\log = (1-\varphi)D\log = (1-\varphi)\delta$, *and we have another sequence*

$$0 \to \mathbb{Z}_p(1)^g \to U_\infty \xrightarrow{\alpha\psi} \mathcal{V}(1) \to \mathbb{Z}_p(1)^g \to 0.$$

Proof. — We first remark that all maps in Cor. 2.7, Thm. 2.8 and Lemma 2.9 are also Δ-equivariant. The short exact sequence is obtained by combining 2.7 and 2.8. The second equality sign in the last line of the proposition is a consequence of the (easily checked) rule $D\varphi = p\varphi D$. The second sequence follows easily, using Lemma 2.9. □

So now we have « almost an isomorphism » of U_∞ with a certain very explicit module $\mathscr{V}(1)$. As usual, the next step is to determine the image of the circular units. This becomes easier if we work over $\mathbb{Q}_p$, and one character at a time. Hence, let $F/\mathbb{Q}$ be abelian, unramified over p, $K_n = F(\zeta_{p^{n+t}})$, $\Delta = \mathrm{Gal}(F/\mathbb{Q})$, $\mathcal{O} = \mathbb{Z}_p \otimes \mathcal{O}_{\mathrm{F}}$, $\Delta' = \mathrm{Gal}(K_0/\mathbb{Q})$. Note that $\Delta' \simeq \Delta \times \mathrm{Gal}(\mathbb{Q}\zeta_{p^t})/\mathbb{Q})$.

DEFINITION. — *If χ is any p-adic character of Δ, M any $\mathbb{Z}_p[\Delta]$-module, then*

$$V_\chi(M) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} M \otimes_{\mathbb{Z}_p[\chi]} \mathbb{Z}_p[\![\chi]$$

$$\simeq \mathbb{Q}_p \otimes_{\mathbb{Z}_p} M_\chi . \ (\chi\textit{-coinvariants, as in the introduction}).$$

The same construction is also defined with Δ' in the place of Δ and χ a character of Δ'. Sometimes we write $V_\chi^{(\Delta)}(M)$ or $V_\chi^{(\Delta')}(M)$, as the case may be, to make clear over which group ring we are working.

LEMMA 2.11. — *Assume χ is a character of Δ with conductor m (a divisor of* cond (F)), *and write $F' = F \cap \mathbb{Q}(M)$. Then :*

a) *The additive $\mathbb{Q}_p\Delta$-module $V_\chi(\mathbb{Q}_p \otimes_{\mathbb{Q}} F)$ is generated by $y_\chi = (\mathrm{Tr}_{\mathbb{Q}(m)/F'}(\zeta_m))_\chi$.*

b) *Assume $\chi \neq 1$. Recall $U_\infty = \varprojlim U_\nu$ is the projective limit of the local principal p-units of $K_\nu = F(\zeta_{p^{\nu+t}})$, $t = 1$ resp 2 according to whether p is odd or $p = 2$. (U_ν is also the pro-p-part of $\mathscr{U}_\nu$.) Also, $C_\infty =$ (pro-p-part of $\mathscr{C}_\infty$) is a subgroup of U_∞. Then*

$$V_\chi(C_\infty) = V_\chi(R[\Delta]) \cdot (\eta_m)_\chi, \ \textit{where}$$

$$\eta_m = (N_{\mathbb{Q}(m)/F'}(1 - \zeta_m \zeta_{p^{\nu+t}})^{\mathrm{Frob}^{-\nu}})_\nu .$$

(We suppress the projection $\mathscr{C}_\infty \to C_\infty$ in the notation.)

Proof. — *a)* The additive $\mathbb{Q}_p\Delta$-module $\mathbb{Q}_pF$ is generated by all elements $x_{m'} = \mathrm{Tr}_{\mathbb{Q}(m')/F \cap \mathbb{Q}(m')}(\zeta_{m'})$ where m' runs over all divisors of cond (F) (exercise, using the existence of additive normal bases). By definition, F' contains $F^{\ker(\chi)}$, the fixed field of the kernel of χ. Now $\ker(\chi)$ certainly operates trivially on $V_\chi(\mathbb{Q}_pF)$. Since the group ring $\mathbb{Q}[\ker\chi]$ is semisimple, we get a surjection $(\mathbb{Q}_pF)^{\ker\chi} \to V_\chi(\mathbb{Q}_pF)^{\ker(\chi)} = V_\chi(\mathbb{Q}_pF)$. Hence the natural map $\mathbb{Q}_pF' \to V_\chi(\mathbb{Q}_pF)$ is onto. Hence $V_\chi(\mathbb{Q}_pF)$ is already generated by the images of all $x_{m'}$ with m' a divisor of m. We show that the proper divisors m' contribute nothing: if $m'|m$, $m' \neq m$, then there exists $a \in \mathbb{Z}$, $a \equiv 1(m')$, $\chi(a) \neq 1$. If σ is the corresponding element of Δ, then we get for the image y of $x_{m'}$ in $F_\chi : \sigma(y) = \chi(a)\cdot y$; on the other hand, σ fixes $x_{m'}$, hence y, and we get $y = 0$.

b) We proved in Lemma 2.3: C_∞ is generated by -1, all $\eta_{m'}$, $1 \neq m'|\mathrm{cond}(F)$, and by $C_{\mathbb{Q}} = \text{pro-}p\text{-part}(\varprojlim \mathscr{C}(\mathbb{Q}(\zeta_{p^{\nu+t}})))$. Let $F'' = F^{\ker(\chi)}$. We then have (with self-explaining notation): $(\mathbb{Q}_p \otimes C_\infty(F))^{\ker(\chi)} = \mathbb{Q}_p \otimes C_\infty(F'')$. This is quite easy (idea: if u is a circular unit for F, fixed under $H = \mathrm{Ker}(\chi)$, then $u^{|H|} = N_{F/F''}(u)$ is circular for F'', and the power $|H|$ does not matter since we tensored with $\mathbb{Q}_p$).

(*Remark.* – It is a theorem that the above equality holds without tensoring with $\mathbb{Q}_p$, in the case that both F and F'' are cyclotomic fields (Gold, Kim [6]).)

Similarly as in *a*), we deduce that $\mathbb{Q}_p \otimes C_\infty(F') \to V_\chi(C_\infty(F))$ is surjective. From this one obtains: $V_\infty(C_\infty(F))$ is already generated by -1 and the images of all $\eta_{m'}$ with $1 \neq m'|m$, and the image of $C_{\mathbb{Q}}$. We may forget about $C_{\mathbb{Q}}$ since χ is nontrivial. Exactly as in *a*), one shows that one only needs the image of η_m. (What happened to -1? For p odd, -1 is projected away since we work in the pro-p-group C_∞. For $p = 2$, -1 drops out after tensoring with $\mathbb{Q}_2$.) □

Corollary 2.12. – *Let F, $\mathcal{O}$, χ be as above,* $\mathrm{cond}(\chi) = m$. *Then $V_\chi(\mathscr{V})$ is free on the generator $z_\chi = y_\chi\cdot(1-X)$ over $\mathbb{Q}_pR[\Delta]_\chi$, where $y_\chi = \mathrm{Tr}_{\mathbb{Q}(m)/\mathbb{Q}(m)\cap F}(\zeta_m)$ as in Lemma 2.11 a).*

Proof. – By 2.11 *a*), y_χ is a $\mathbb{Q}_p\Delta$-generator of $V_\chi(F)$, hence for some $N \in \mathbb{N} : p^N\mathcal{O}_\chi \subset (\mathbb{Z}_p\Delta)y_\chi$. From 2.6 one knows that $\mathscr{V}$ is the R-span of $\mathcal{O}\cdot(1-X)$, hence $p^N\mathscr{V}_\chi$ lies in the $R[\Delta]$-span of $y_\chi\cdot(1-X)$, hence $y_\chi\cdot(1-X)$ is a generator. $V_\chi(\mathscr{V})$ is free on it since it is not zero (easy) and $\mathbb{Q}_pR[\Delta]_\chi$ is a PID. □

For the next theorem we need some more notation. Let χ be any odd Dirichlet character of conductor d or pd ($4d$ if $p = 2$), d prime to p, $\rho = \omega\chi^{-1}$ the complementary even character. Let $\Lambda_\chi = \mathbb{Z}_p(\chi)[[T]]$ as usual. Then Λ_χ carries an involution $'$, which is identity on $\mathbb{Z}_p(\chi)$ and satisfies $T' = (1+T)^{-1} - 1$. (In the identification $\Lambda_\chi = \mathbb{Z}_p[[\Gamma]]$, $\Gamma \simeq \mathbb{Z}_p$, the involution corresponds to taking inverses in Γ.) For $\rho \neq 1$, we also have the Stickelberger series $G_p(T,\rho) \in \Lambda_\chi = \Lambda_\rho$. In the notation of Washington [23], $G_p(T,\rho) = f(T,\rho)$.

Recall $F/\mathbb{Q}$ is abelian, unramified over p; $K_0 = F(\zeta_{2p})$, $K_\infty = F(\zeta_{p\infty})$, $\Delta = \mathrm{Gal}\,(F/\mathbb{Q})$, $\Gamma' = \mathrm{Gal}\,(K_\infty/F) \simeq \mathbb{Z}_p^\times$. Let $\Delta' = \mathrm{Gal}\,(K_0/\mathbb{Q})$, $\Gamma = \mathrm{Gal}\,(K_\infty/K_0) \simeq 1 + 2p\mathbb{Z}_p$. We have a canonical decomposition $\Delta' = \Delta \times \Phi$ with $\Phi = \mathrm{Gal}\,(\mathbb{Q}(\zeta_{2p})/\mathbb{Q}) = \mathrm{Gal}\,(K_0/F)$. Then $\Gamma' = \Phi \times \Gamma$ and $R \simeq \mathbb{Z}_p[[\Gamma]][\Phi] \simeq \mathbb{Z}_p[[T]][\Phi]$. Finally $G = \mathrm{Gal}\,(K_\infty/\mathbb{Q}) = \Delta \times \Gamma' = \Delta' \times \Gamma$. The following is obvious for any $\mathbb{Z}_p[\Delta']$-module M and any character χ of Δ':

$$V_\chi^{\Delta'}(M)) = V_{\chi|\Phi}^{\Phi}(V_{\chi|\Delta}^{\Delta}(M)).$$

THEOREM 2.13. — *For any even nontrivial character* ρ *of* Δ', $\chi = \omega\rho^{-1}$:

$$\alpha\psi(V_\rho(C_\infty) = G_p(T',\rho)\cdot z_{\chi^{-1}} \subset V_\rho(\mathscr{V}(1)) = (V_{\chi^{-1}}(\mathscr{V}))(1).$$

COROLLARY 2.14. — *For any even nontrivial character* ρ *of* Δ', $\chi = \omega\rho^{-1}$, *consider the two* $\mathbb{Q}_p\Lambda_\rho$*-modules* $V_\rho(U_\infty/C_\infty)$ *and* $\mathbb{Q}_p(\chi)[[T]]/(G_p(T,\rho))^*\,(1)$. *These two modules have the same characteristic ideal over* $\mathbb{Q}_p\Lambda_\rho$. *If* $\chi(p) \neq 1$, *they are even isomorphic.* (*Cf. Thm.* 1 *of Gillard* [5]. *Recall :* * *means that* $\Delta' \times \Gamma$ *operates through the inverse map.*)

Proof of Corollary. — First note $\chi^{-1} = \rho\omega^{-1}\cdot V_{\chi^{-1}}(\mathscr{V})$ is free cyclic on $z_{\chi^{-1}}$ over $\mathbb{Q}_p(\chi^{-1})[[T]]$, since one already has an isomorphism $V_{\chi^{-1}|\Delta}(\mathscr{V}) \simeq V_{\chi^{-1}|\Delta}(R[\Delta]) \simeq \mathbb{Q}_p(\chi^{-1}|\Delta)[\Phi][[T]]$ by 2.12. One now checks easily that the map given by $T \mapsto T'$ and identity on $\mathbb{Q}_p(\chi) = \mathbb{Q}_p(\chi^{-1})$ induces an isomorphism over $\Delta' \times \Gamma$

$$\mathbb{Q}_p(\chi^{-1})[[T]]/(G_p(T',\rho)) \to (\mathbb{Q}_p(\chi)[[T]]G_p(T,\rho))^*.$$

From Prop. 2.10, one gets an exact sequence

$$0 \to V_\rho(\mathbb{Z}_p(1)^g) \to V_\rho(U_\infty/(C_\infty) \to V_\rho(\mathscr{V}(1))/\alpha\psi(V_\rho(C_\infty)) \to V_\rho(\mathbb{Z}_p(1)^g) \to 0.$$

(There is a small point here: $\mathbb{Z}_p(1)^g \cap C_\infty = \mathbb{Z}_p(1)$, and V_ρ of this is 0, since $\rho \neq \omega$.) Since $\mathbb{Z}_p(1)^g \simeq (\mathbb{Z}_p[\Delta/D]) \otimes \mathbb{Z}_p(1)$, $D =$ decomposition group for $\mathscr{O} =$ decomposition group of 2 in F, one has: $V_\rho(\mathbb{Z}_p(1)^g) = 0$ whenever $\chi(p) \neq 1$. At any rate, one obtains the corollary by using Thm. 2.13 and multiplicativity of characteristic ideals.

Remark. – One can show $V_\rho(U_\infty/C_\infty) = 0$ for ρ the trivial character.

Proof of Thm. 2.13. – Let m be the conductor of $\rho|\Delta$; let $\eta = \eta_m$ (notation of Lemma 2.11). Since $V_\rho(C_\infty)$ is generated by η_ρ by Lemma 2.11 *b*) (NB. the lemma is applied to $\rho|\Delta$), it will suffice to show $\alpha\psi(\eta_\rho) = G_p(T',\rho)\cdot z_{\chi^{-1}}$ in $V_{\chi^{-1}}(\mathscr{V})$.

Let $f_0 = \zeta_m X + (1-\zeta_m)$, $e = |(\mathcal{O}/p\mathcal{O})^\times|$. Then $f_0^e \equiv 1 \bmod p$ and $\mathcal{N}(f_0) = \mathrm{Frob}\,(f_0)$, hence $f_0^e \in \mathfrak{M}^0$. One easily sees that $\psi(\eta^e) = N_{\mathbb{Q}(m)/\mathbb{Q}(m)\cap F}(f_0^e)$ (if you substitute $1-\zeta_{p^{\nu+t}}$ for X in f_0, you get $1-\zeta_m\zeta_{p^{\nu+t}}$). Our task is therefore to evaluate $(1-\varphi)\delta(N_{\mathbb{Q}(m)/\mathbb{Q}(m)\cap F}(f_0))$. For this, it is enough to show that $1-\varphi)\delta(f_0)_{\chi^{-1}} = (G_p(T',\rho)\cdot\zeta_m\cdot(1-X))_{\chi^{-1}}$; then applying the norm gives the desired result by definition of $z_{\chi^{-1}}$.

Let $\nu' = \nu + t$ for brevity. There are evaluation maps $e_\nu (\nu \in \mathbb{N})$ from $\mathscr{V}$ to $\mathbb{Q}_p(\zeta_m, \zeta_{p^{\nu'}})$, and from $V_\rho(\mathscr{V})$ to $\mathbb{Q}_p(\zeta_m,\zeta_{p^{\nu'}})_\rho$, induced by $X \mapsto 1-\zeta_{p^{\nu'}}$, and one knows that the intersection of all kernels $\ker(e_\nu)$ is zero. It is suggestive to write $f|_{1-\zeta_{p^{\nu'}}}$ for $e_\nu(f)$. Thus, it is sufficient to show

$$((1-\varphi)\delta(f_0)|_{X=1-\zeta_{p^{\nu'}}})_\rho = G_p(T',\rho)(\zeta_m\zeta_{p^{\nu'}})_{\chi^{-1}}.$$

(It will become clear presently how $G_p(T',\rho)$ operates on $\mathbb{Q}(\zeta_m,\zeta_{p^{\nu'}})$ when we recall the definition of $G_p(T',\rho)$ as limit of certain Stickelberger elements.)

Calculation of left hand side:

We have $\delta(f_0) = Df_0/f_0 = (1-X)\zeta_m/(\zeta_m X + (1-\zeta_m))$. Therefore:

$$\delta(f_0)|_{1-\zeta_{p^{\nu'}}} = \frac{\zeta_{p^{\nu'}}\zeta_m}{1-\zeta_{p^{\nu'}}\zeta_m};$$

$$\varphi\delta(f_0) = \varphi\left(\frac{(1-X)\zeta_m}{\zeta_m X+(1-\zeta_m)}\right) = \frac{(1-X)^p.\zeta_m^p}{1-(1-X)^p\zeta_m^p},$$

hence for $\nu \geqslant 1$

$$(1-\varphi)\delta(f_0)|_{1-\zeta_{p^{\nu'}}} = (\delta-\varphi\delta)(f_0)|_{1-\zeta_{p^{\nu'}}}$$

$$= \frac{\zeta_{p^{\nu'}}\cdot\zeta_m}{1-\zeta_{p^{\nu'}}\cdot\zeta_m} - \frac{\zeta_{p^{\nu'-1}}\cdot\zeta_m^p}{1-\zeta_{p^{\nu'-1}}\cdot\zeta_m^p}.$$

For the calculation of the right hand side, we need some notation and a lemma. We use the notation of Washington [23] p. 118 (his d is our m): $q_\nu = m \cdot p^{\nu'}$, $\Gamma_\nu = \mathrm{Gal}(K_\nu/K_0)$; for a prime to q_ν, let $\sigma_a = \delta'(a)\gamma_\nu(a)$, $\delta'(a) \in \Delta'$, $\gamma_\nu(a) \in \Gamma$. Finally, let $\xi_\nu(\rho) = -q_\nu^{-1} \cdot \Sigma_a a \cdot \rho\omega^{-1}(a) \cdot \gamma_\nu^{-1}(a)$ (summation over $1 \leqslant a \leqslant a_\nu$, a prime to q_ν), and $\xi'_\nu(\rho) = -q_\nu^{-1} \cdot \Sigma_a a \cdot \rho\omega^{-1}(a) \cdot \gamma_\nu(a)$, so $G_p(T,\rho) = \lim \xi_\nu(\rho)$ and $G_p(T',\rho) = \lim \xi'_\nu(\rho)$ in $\mathbb{Z}_p(\rho)[[\Gamma]] = \Lambda_\rho$.

Lemma 2.15.

a) $$\sum_{a=1}^{q_\nu} a \cdot (\zeta_m \cdot \zeta_{p^{\nu'}})^a = -q_\nu \cdot \frac{\zeta_m \zeta_{p^{\nu'}}}{1 - \zeta_m \zeta_{p^{\nu'}}} \qquad (\nu \geqslant 0)$$

b) $$\sum_{\substack{1 \leqslant a \leqslant q_\nu \\ (a,p)=1}} a \cdot (\zeta_m \cdot \zeta_{p^{\nu'}})^a = -q_\nu \cdot \frac{\zeta_m \zeta_{p^{\nu'}}}{1 - \zeta_m \zeta_{p^{\nu'}}} + q_\nu \cdot \frac{\zeta_m \zeta_{p^{\nu'-1}}}{1 - \zeta_m \zeta_{p^{\nu'-1}}} \qquad (\nu > 0).$$

Proof. — *a*) is quite easy, and *b*) follows from *a*). See Coleman [3], Prop. 5. □

We are ready to treat the right hand side, RHS for short. It is sufficient to show: q_ν times RHS, evaluated in $1 - \zeta_{p^{\nu'}}$, equals q_ν times LHS, evaluated in $1 - \zeta_{p^{\nu'}}$, for $\nu' > 0$ arbitrary. We calculate:

$$\begin{aligned} q_\nu \cdot G_p(T',\rho) \cdot z_{\chi^{-1}}|_{1-\zeta_{p^{\nu'}}} &= (q_\nu \cdot \xi'_\nu(\zeta_m \zeta_{p^{\nu'}}))_{\chi^{-1}} \quad \text{(construction of } G_p) \\ &= -\sum_{(a,q_\nu)=1} (a \cdot \chi^{-1}(a) \cdot \gamma_\nu(a))(\zeta_m \zeta_{p^{\nu'}})_{\chi^{-1}} \\ &= -\sum_{(a,q_\nu)=1} \chi \cdot (a\sigma(a) \cdot \gamma_\nu(a))(\zeta_m \zeta_{p^{\nu'}})_{\chi^{-1}} \\ &= -\left(\sum_{(a,q_\nu)=1} (a\sigma(a))(\zeta_m \zeta_{p^{\nu'}}) \right)_{\chi^{-1}} \\ &= -\left(\sum_{(a,q_\nu)=1} a(\zeta_m \zeta_{p^{\nu'}})^a \right)_{\chi^{-1}} \\ &= -\left(\sum_{\substack{1 \leqslant a \leqslant q_\nu \\ (a,p)=1}} a(\zeta_m \zeta_{p^{\nu'}})^a \right)_{\chi^{-1}} - \left(\sum_{\substack{1 \leqslant a \leqslant q_\nu \\ (a,p)=1 \\ (a,m)>1}} a(\zeta_m \zeta_{p^{\nu'}})^a \right)_{\chi^{-1}} . \end{aligned}$$

Now the first term is easily seen, by Lemma 2.15 b) and the calculation already done, to equal the left hand side in theorem 2.13, evaluated in $1 - \zeta_{p^{v'}}$. It remains to see that the second term is 0. This second term (without $(\ldots)_{\chi^{-1}}$), however, is a sum of algebraic numbers $y_d \in \mathbb{Q}(\zeta_d \zeta_{p^{v'}})$, where d runs over the proper divisors of m. Since $m = \operatorname{cond}(\rho|\Delta) = \operatorname{cond}(\chi^{-1}|\Delta)$ one sees, similarly as in 2.12, that already $V_{\chi^{-1}|\Delta}(\mathbb{Q}(\zeta_d \zeta_{p^{v'}})) = 0$, hence $V_{\chi^{-1}}(\mathbb{Q}(\zeta_d \zeta_{p^{v'}})) = 0$ for all proper divisors d of m, and the second term above is zero. □

Remark. – It appears likely that there is a version of Thm. 2.13 without denominators, building on the work of Sinnott [21].

3. The Main Conjecture for odd and even characters.

Let $F/\mathbb{Q}$ be abelian, unramified over p (p a fixed prime); let $X = \varprojlim A(K_n)$. (Recall : $K_n = F(\zeta_{2p^{n+1}})$, $A = A_p$ = « p-class group of ».) C_∞ was defined in the last section. Let $\mathscr{E}_n = \mathcal{O}(K_n)$, E_n the pro-p-part of the closure of $\mathscr{E}_n$ in $\mathscr{U}_n$, and $E_\infty = \varprojlim E_n$. Finally, let X^+, E_∞^+, C_∞^+ be defined by replacing K_n throughout by K_n^+. The following theorem is another main result of this paper.

THEOREM 3.1. – *For every even character $\rho \neq 1$ of K_0, the characteristic ideal of the Λ_ρ-module X_ρ divides the characteristic ideal of $(E_\infty/C_\infty)_\rho$.*

Remark. – *a*) If $\lambda < \infty$ and $\mu = 0$ for two Λ-modules Y and Y' ($\Lambda = \mathbb{Z}_p[[T]]$), then Y is quasi-isomorphic to Y' iff $\mathbb{Q}_p Y \simeq \mathbb{Q}_p Y'$. Moreover, it is an easy exercise to show that for even ρ, $\mathbb{Q}_p(X_\rho) \simeq \mathbb{Q}_p((X^+)_\rho)$. (Use e.g. Lemma 2.2.) Hence X_ρ is quasi-isomorphic to $(X^+)_\rho$, and the characteristic ideals of X_ρ and X_ρ^+ agree. We also have $\mathbb{Q}_p(E_\infty/C_\infty)_\rho \simeq \mathbb{Q}_p(E_\infty^+/C_\infty^+)_\rho$. Since we did not prove yet that E_∞/C_∞ has $\mu = 0$, we only may infer from this isomorphism that the characteristic ideals of $(E_\infty/C_\infty)_\rho$ and $(E_\infty^+/C_\infty^+)_\rho$ agree up to a factor power of p. Since char (X_ρ) is prime to p, we may replace X and E_∞/C_∞ by their plus counterparts in the proof of Theorem 3.1.

b) For $\rho = 1$, one can show that $\operatorname{char}(X_\rho) = \operatorname{char}((E_\infty/C_\infty)_\rho)) = (1)$.

c) It is a byproduct of the proof of Thm. 3.2 below that in Theorem 3.1, actually *equality* holds.

Thm. 3.1 implies the Main Conjecture:

THEOREM 3.2. – *For every odd character $\chi \neq \omega$ of K_0, one has with $\rho = \omega\chi^{-1}$:*

$$\text{char } (X_\chi) = \left(\frac{1}{2} G_p(T,\rho)\right) \subset \mathcal{O}_F(\chi)[[T]] = \Lambda_\chi, \quad \textit{if} \quad \rho \neq 1;$$

$$\text{char } (X_\chi) = \left(\frac{1}{2} G_p(T,\rho) \cdot (T-q_0)\right) = (1) \quad \textit{if} \quad \rho = 1.$$

Proof of the implication 3.1 ⇒ 3.2: This is a well-known argument (cf. Rubin [19], p. 415-416, and Greenberg [9] § 2), involving the injective limit $A_\infty = \varinjlim A(K_n)$, and the Galois group Y of the maximal abelian p-ramified p-extension of K_∞. One has

LEMMA 3.3. – *X is quasi-isomorphic to* $\mathrm{Hom}_{\mathbb{Z}}(A_\infty, \mathbb{Q}/\mathbb{Z})$ *over Λ_Δ. (Caution: the ring $\Lambda_{\Delta'} = \mathbb{Z}_p[\Delta'][[T]]$ operates via $\sigma f(a) = f(\sigma a)$, $\sigma \in \Lambda_{\Delta'}$, $a \in A_\infty$, not via the « inverse ».)*

Proof. – As stated in Solomon [22], p. 475, this follows from work of Iwasawa. Indeed, it is not hard to give a direct proof of the lemma, starting from Iwasawa's result that the two modules concerned are quasi-isomorphic over Λ.

Next, one uses the Kummer pairing, as in Greenberg [9], and obtains (Y^+ is defined for K_∞^+ just as Y for K_∞):

PROPOSITION 3.4. – *With V_ρ as in Section 2, we have for each even character ρ of K_0:*

$$\begin{aligned} V_\rho(Y^+) &\simeq V_\rho(X^*(1)^+) \\ &\simeq V_\rho(X^*(1)) \\ &\simeq V_\chi(X)^*(1) \quad \textit{with} \quad \chi = \omega\rho^{-1}. \end{aligned}$$

In different notation (χ odd): $V_\chi(X) \simeq V_\rho(Y^+)^*$ (1). □

Remark. – We preferred the simplest method here. Greenberg (see *op. cit.*) has done an analysis of the Kummer pairing for $p = 2$ without tensoring by $\mathbb{Q}_2$.

Theorem 3.2 will now follow from 3.4, 3.1, and Cor. 2.14: One starts from the two exact sequences (one from class field theory, the other tautological) :

$$0 \to U_\infty/E_\infty \to Y \to X \to 0,$$
$$0 \to E_\infty/C_\infty \to U_\infty/C_\infty \to U_\infty/E_\infty \to 0.$$

By 3.1, $h_\rho \cdot \mathrm{char}\,(X) = \mathrm{char}\,(E_\infty/C_\infty)_\rho$ for some $h_\rho \in \Lambda_\rho$. Moreover, the function « characteristic ideal » is multiplicative on short exact sequences. Hence one finds by comparison that for ρ nontrivial

$$\begin{aligned} h_\rho \cdot \mathrm{char}\,(Y_\rho) &= \mathrm{char}\,((U_\infty/C_\infty)_\rho) \\ &= \mathrm{char}\left(\Lambda_\chi \Big/ \left(\frac{1}{2} G_p(T,\rho)\right)^* (1)\right). \quad \text{(Corollary 2.14)} \end{aligned}$$

From Proposition 3.4 : $\mathrm{char}\,(Y_\rho) = \mathrm{char}\,(X_\chi^*(1))$. It finally follows that $\mathrm{char}\,(X_\chi)$ *divides* $\mathrm{char}\left(\Lambda_\chi \Big/ \left(\frac{1}{2} G(T,\rho)\right)\right) = \left(\frac{1}{2} G_p(T,\rho)\right)$ for *all* odd $\chi \neq \omega$. We claim that X_χ is finite for $\chi = \omega$. By Lemma 2.2, one can replace F by $F \cap \mathbb{Q}(\zeta_{2p})$ in showing this. For odd p, X_ω is then zero (see e.g. Mazur, Wiles [17], p. 183). For $p = 2$, $F = \mathbb{Q}$ or $\mathbb{Q}(i)$, X is itself zero. Hence we have $\mathrm{char}\,(X_\chi) = (1)$ for $\chi = \omega$. From the analytic class number formula for minus class groups, one deduces *equality*, as claimed in Thm. 3.2. (See e.g. Greenberg [8].) □

The rest of the section is devoted to the proof of Theorem 3.1. This is a very technical matter ; the principal ideas are already contained in the relevant papers of Kolyvagin and Rubin. As the proof wears on, factors p and $(\gamma - 1)$ $(\Gamma = \langle \gamma \rangle)$ accumulate in the formulas ; using $\mu = 0$ and Leopoldt's conjecture, one can fortunately throw them out at the end.

LEMMA 3.5 (Rubin [19] Lemma 2.3). — *Let $K/\mathbb{Q}$ be real and abelian, M some fixed power of p, ℓ a prime* $\equiv 1$ mod *M which splits totally in K. Let $G =$* Gal $(K/\mathbb{Q})$. *Then there is a unique G-equivariant epimorphism*

$$\begin{tikzcd} \varphi_\ell \colon (\mathcal{O}_K/\ell\mathcal{O}_K)^\times \arrow[rr] & & \mathcal{I}_\ell/M\mathcal{I}_\ell \\ & K(\mu_\ell)^\times \arrow[ul] \arrow[ur] & \end{tikzcd}$$

where :

$\mathcal{I}_\ell$ is the subgroup of the divisor group Div (K) *of K generated by all prime divisors of ℓ ; let $.._{[\ell]}$: $K^\times \to \mathcal{I}_\ell/M\mathcal{I}_\ell$ be the map which*

associates to $x \in K^\times$ *the «support over* ℓ*»-part of the principal ideal* (x)*;*

the map going right upward is $K(\mu_\ell)^\times \xrightarrow{\text{norm}} K^\times \xrightarrow{..[\ell]} \mathcal{J}_\ell/M\mathcal{J}_\ell$*;*

and the map going left upward is exponentiation with $1 - \sigma_\ell$*, where* σ_ℓ *is a generator of* $\mathrm{Gal}\,(K(\mu_\ell)/K)$*, fixed once and for all.*

Proof. – See Rubin *op. cit.* □

Remarks. – *a*) Since ℓ splits in K, we have a G-isomorphism $\mathcal{O}_K/\ell\mathcal{O}_K \to \mathbb{F}_\ell^G$. Since M divides $\ell - 1$, the unit group $(\mathbb{F}_\ell^\times)^G$ maps G-epimorphically onto $(\mathbb{Z}/M)[G] \simeq \mathcal{J}_\ell/M\mathcal{J}_\ell$. What the lemma above does, is to fix an epimorphism φ_ℓ in accordance with other data.

b) From φ_ℓ one obtains another map, abusively also written φ_ℓ:

$$\{\bar{y} \in K^\times/K^{\times M} | (y)_{[\ell]} \in M\mathcal{J}_\ell\} \to \mathcal{J}_\ell/M\mathcal{J}_\ell,$$

$y \mapsto \varphi_\ell(u)$ where $y = z^M u$, $z \in K^\times$, u a unit at all places over ℓ.

We need some notation from Kolyvagin's theory. Let K, M be as in the last lemma and define $\mathcal{S}_M = \mathcal{S}_{K,M} = \{r \in \mathbb{N} | r$ squarefree, all primes ℓ dividing r split in K and are $\equiv 1 \bmod M\}$. An *Euler system* (ES) over K is a family of algebraic integers (ξ_r), $r \in \mathcal{S}_M$, satisfying the properties ES 1 – 4 from Rubin [19], p. 398. (His F corresponds to our K.)

Given any Euler system (ξ_r) consisting of units, let $\varkappa_r \in K^\times/K^{\times M}$ be defined from (ξ_r) as in *loc. cit.* p. 399. (Rubin always works with a specific choice of (ξ_r).) We say : « x starts an ES » if there is an ES (ξ_r) with $\xi_1 = x$. We point out the probably well-known fact that every circular number x of K starts an ES. This is easy to check, using e.g. the description of circular units obtained in claim (3) in the proof of Lemma 2.3 : one reduces to $K = \mathbb{Q}(\zeta_m)$ and $x = 1 - \zeta_m$, and there one can take $\xi_r = 1 - (\Pi_{\ell|r}\zeta_\ell)\cdot\zeta_m$.

Lemma 3.6 (see 2.4 in *op. cit.*). – *Let* r *be an element of* $\mathcal{S}_M$*,* ℓ *a prime number,* (ξ_r) *an Euler system over* K*.*

a) *If* ℓ *does not divide* r*, then* $(\varkappa_r)_{[\ell]} = 0$ (*notation as in* 3.5).

b) *If* $r = \ell\cdot r'$*,* $r' \in \mathcal{S}_M$*, then* $(\varkappa_r)_{[\ell]} = \varphi_\ell(\varkappa_{r'})$.

Proof. – Exactly as in *loc. cit.* □

The next step (application of Čebotarev's Theorem) already necessitates some changes w.r.to Rubin's formulation, in order to cover the case $p = 2$.

THEOREM 3.7. – *Let K, M, G be as in* 3.5 ; *assume $M \geqslant 4$ for $p = 2$. Assume that we are given : $\mathfrak{c} \in A(K)$, a finite $\mathbb{Z}[G]$-submodule $W \subset K^\times / K^{\times M}$, and a G-homomorphim*

$$\psi : W \to \left(\frac{\mathbb{Z}}{M}\right)[G].$$

Let 2^c be the precise power of 2 *which divides* cond(K). *Then there exist infinitely many primes λ of K such that (quantities in $[\cdot\cdot]$ are to be omitted for odd p)* :

(1) $[\lambda] = [2^{c+2}] . \mathfrak{c}$ (*we use additive notation in $A(K)$ as always*) ;

(2) If ℓ *is the rational prime below λ, then $\ell \equiv 1 \bmod M$, and ℓ splits completely in K ;*

(3) *For all $w \in W$: $(w)_{[\ell]} = 0$ in $\mathcal{I}_\ell / M \mathcal{I}_\ell$; and there exists a unit u of $\mathbb{Z}/M$ such that*

$$\varphi_\ell(w) = [2^{c+2}] \cdot u \cdot \psi(w) \lambda \quad \textit{for all} \quad w \in W.$$

COMPLEMENT. – If $K = K_\nu^+$ (*notation from the beginning of the section*), $\nu \in \mathbb{N}$ *arbitrary, and $p = 2$, then we may replace the factor 2^{c+2} by* 4. (*This will be used later.*)

Proof. – For odd p, this is just Thm. 3.1 in Rubin [19]. Let therefore $p = 2$. Consider the following fields where H is the 2-class field of K in the wide sense, so Gal$(H/K) \simeq A(K)$:

$$\begin{tikzcd} & K'' = K(\mu_M, W^{1/M}) \arrow[d, dash] \\ & K' = K(\mu_M) \arrow[d, dash] \\ H \arrow[r, dash] & K \end{tikzcd}$$

The idea is (as in *loc. cit.*) to find a prime λ of K whose Frobenius on H is $\mathfrak{c}$ and whose Artin symbol on K'' is (the conjugacy class of) γ, where γ is an appropriate element of Gal(K''/K), constructed by Kummer theory. But there are slight obstructions.

Claim (a). – $[H \cap K' ; K] \leqslant 2^c$ (in case $K = K_\nu^+$, even $H \cap K' = K$).

Proof. – Let $c > 0$. Then 2 ramifies in $K/\mathbb{Q}$ with exponent at most 2^{c-1}, hence all divisors of 2 ramify in K'/K with exponent at least $M/2^c$; the degree of K'/K is at most $M/2$, hence the inertia field $H \cap K'$ has degree at most 2^{c-1} over K'. The case $c = 0$ is easy. (For $K = K_\nu^+ = F(\zeta_{2^{\nu+2}})^+$: Write $M = 2^m$. For $m \leqslant \nu + 2$, K' is quadratic over K. For $m > \nu + 2$, the field K_ν is quadratic over K and is the biggest subfield of K' which is unramified over K at all finite places. In both cases, the only subfield of K' unramified everywhere over K is K itself.)

Claim (b). – The abelian group $\mathrm{Gal}\,(H \cap K''/K)$ is annihilated by 2^{c+1} (by 2 in the case $K = K_\nu^+$).

Proof. – $\mathrm{Gal}\,(K'/K)$ operates on the abelian group $V = \mathrm{Gal}\,(K''/K')$; one easily sees that $j =$ (complex conjugation on K') operates as -1 on V. Since j operates as identity on $\mathrm{Gal}\,(HK'/K')$, the extension $K'' \cap HK'/K'$ must be 2-elementary, hence also $K'' \cap H/K' \cap H$. By claim (*a*) we may deduce that $\mathrm{Gal}\,(K'' \cap H/K)$ is killed by 2^{c+1} (resp. 2).

Claim (c). – The cokernel of the canonical injection from Kummer theory

$$\mathrm{Gal}\,(K''/K') \to \mathrm{Hom}\,(W, \mu_M)$$

is annihilated by 2.

Proof. – By Kummer theory it suffices to show: $U = \ker\,(K^\times/K^{\times M} \to K'^\times/K'^{\times M})$ is annihilated by 2. But U injects into $H^1(K'/K, \mu_M)$. Let $Z = K \cdot \mathbb{Q}(\zeta_M)^+$. Then $[K' : Z] = 2$ and Z/K is real cyclic. If $Z = K$, then $|H^1(K'/K, \mu_M)| \leqslant 2$ and we are done. If $Z \neq K$, then K'/K admits a subextension with Klein four group V_4 as Galois group, which implies that U contains a copy of V_4. But $|U| \leqslant |H^1(K'/Z, \mu_M)| \cdot |H^1(Z/K, \mu_M)|$, and both of these factors are at most two, as one checks easily, hence $|U| = 4$ and $U = V_4$, and we are done.

Now the core of the argument runs as follows: Consider the diagram

$$\begin{tikzcd}
\mathrm{Gal}\,(K''\mathrm{H}/K) \arrow[r, "\pi_1"] \arrow[d, "\pi_2"'] & \mathrm{Gal}\,(K''/K); \arrow[d, "\pi_4"'] \\
\mathrm{Gal}\,(H/K) \arrow[r, "\pi_3"] & \mathrm{Gal}\,(K'' \cap H/K);
\end{tikzcd}$$

It is cartesian (if $\pi_3(x) = \pi_4(y)$ then there is a unique z with $\pi_1(z) = y$, $\pi_2(z) = x$), and the lower right term is annihilated by 2^{c+1}(resp. 2).

Let ζ_M denote a primitive M-th root of 1, and define $\iota : (\mathbb{Z}/M)[G] \to \mu_M$ by $\iota(1) = \zeta_M$, $\iota(g) = 0$ for $1 \neq g \in G$. Then $\iota\psi \in \mathrm{Hom}\,(W,\mu_M)$. Therefore by (c), $2\iota\psi$ has a preimage $\gamma \in \mathrm{Gal}\,(K''/K')$. Let $\gamma_1 = 2\left(\frac{\mathfrak{c}}{H/K}\right) \in \mathrm{Gal}\,(H/K)$. With the help of the diagram we find $\delta \in \mathrm{Gal}\,(K''H/K)$ with $\delta | K'' = 2^{c+1}\gamma$, $\delta | H = 2^{c+1}\gamma_1$. By Čeboratev's theorem, there exists infinitely many primes λ of degree one, unramified in $K''H/K$ with $\left(\frac{\lambda}{K''H/K}\right)$ = conjugacy class of δ. Since δ is the identity on K' (because γ is), λ splits in K', i.e. ℓ (the rational prime under λ) is congruent 1 mod M. Moreover, $\left(\frac{\lambda}{H/K}\right) = \delta | H = 2^{c+2}\left(\frac{\mathfrak{c}}{H/K}\right)$, i.e. $[\lambda] = 2^{c+2}\mathfrak{c}$.

We have for $w \in W$: $\mathrm{ord}_\lambda\,(2^{c+2}\psi(w)\lambda)$ divisible by M $\Leftrightarrow 2^{c+2}\iota\psi(w) = 1 \Leftrightarrow (2^{c+1}\gamma)(w^{1/M})/w^{1/M} = 1 \Leftrightarrow w$ is an M-th power mod λ (the last equivalence holds because $2^{c+1}\gamma$ is the Artin symbol of λ on K''). On the other hand by definition of φ_ℓ and since $(w)_{[\ell]} \in M\mathcal{J}_\ell$ (because K''/K is unramified in λ): $\mathrm{ord}_\lambda\,(\varphi_\ell(w))$ divisible by $M \Leftrightarrow w$ an M-th power mod λ. Exactly as in *loc. cit.* p. 403 one infers that $\varphi_\ell(w) = 2^{c+2}u\psi(w)\lambda$ with suitable $u \in (\mathbb{Z}/M)^\times$ for all $w \in W$, as claimed. In the special case ($K = K_\nu^+$) one can replace 2^{c+1} by 2 in the construction of δ, and thus 2^{c+2} becomes replaced by 4. Q.E.D. □

For the rest of the section, let $F/\mathbb{Q}$ be abelian, unramified in p, and $K_\nu = F(\zeta_{2p^{\nu+1}})$ as always. It is convenient to restate 3.7 in the following form :

COROLLARY 3.8. – *Let* $K = K_\nu^+$. *Then Thm.* 3.7 *holds with the following modifications in the formulas of the conclusion, for all p :*

(1) $[\lambda] = p^2\mathfrak{c}$

(2) *as in* 3.7

(3) $\varphi_\ell(w) = p^2u\psi(w)\lambda$.

Proof. – It is easy to get in the factors p^2 for odd p, e.g. by just replacing $\mathfrak{c}$ by $p^2\mathfrak{c}$ and ψ by $p^2\psi$ in 3.7. □

We now introduce new notation for our Galois groups: Recall $F/\mathbb{Q}$ abelian unramified in p, $K_n = F(_{2p^{n+1}})$. From now on, $\Delta = \mathrm{Gal}\,(K_0^+/\mathbb{Q})$, $G_n = \mathrm{Gal}\,(K_n^+/\mathbb{Q})$, and $\Gamma_n = \mathrm{Gal}\,(K_n^+/K_0^+)$. (In earlier notation, Δ should be something like Δ'^+.) As always, $\Gamma = \varprojlim \Gamma_n \simeq \mathbb{Z}_p$. Fix a topological generator γ of Γ, and abbreviate the p^nth power of γ by γ_n. Let now χ range over characters of Δ; note χ is even (in contrast with earlier convention, where χ was odd). Another *important* change in notation: We already remarked (following Thm. 3.1) that in proving 3.1 we may replace X, E_∞/C_∞ by their plus counterparts. We shall do this now, even in notation. Thus: $X = \varprojlim A_n$ with $A_n = A(K_n^+)$; similarly for U_∞, E_∞ and C_∞. For any character χ of Δ, we have the ring $\Lambda_\chi = \mathbb{Z}_p(\chi)[[T]]$ and the Λ_χ-module $(E_\infty/C_\infty)_\chi$. This module is finitely generated (e.g. because U_∞/C_∞ is finitely generated over Λ), we therefore may choose a generator $H_\chi \in \Lambda_\chi$ of $\mathrm{char}\,(E_\infty/C_\infty)_\chi$. (It will be a byproduct that $H_\chi \neq 0$, i.e. $(E_\infty/C_\infty)_\chi$ is Λ_χ-torsion.) On the other hand, there is a quasi-isomorphism

$$\tau: \quad X_\chi \to \bigoplus_{i=1}^{k} \Lambda_\chi/(g_i),$$

and consequently $\mathrm{char}\,(X_\chi) = (g)$ with $g = g_1 \cdots g_k$.

We need two lemmas providing the link with the finite levels.

Lemma 3.9. – *Let $\chi \neq 1$ be a character of Δ. There exists a constant c_1 depending on F only, and G_n-homomorphisms $\vartheta_n : E_{n,\chi} \to \Lambda_{n,\chi} = \Lambda_\chi/(1-\gamma_n)$ for all n such that*

$$(\gamma-1)^2 p^{c_1}\cdot H_\chi \cdot \Lambda_\chi \subset \vartheta_n(\mathrm{im}\ C_{n,\chi}) \subset p^{-c_1}\cdot H_\chi \cdot \Lambda_\chi .$$

Lemma 3.10. – *Let χ be as in 3.9. There exists a constant c_2 depending on F only, and G_n-homomorphisms $\tau_n : A_{n\chi} \to \bigoplus_{i=1,\ldots,k} \Lambda_{n\chi}/(\bar{g}_i)$ for all n such that*

$$p^{c_2}\cdot \mathrm{coker}\,(\tau_n) = 0 .$$

Proof of 3.9. – Write $M_{(1-\gamma_n)}$ for the module of $(1-\gamma_n)$-coinvariants $M/(1-\gamma_n)M$ (M any Λ_χ-module), let $\Gamma_{mn} = \mathrm{Gal}\,(K_m^+/K_n^+)$ for $m \geqslant n$, and let $H^*(* \in \mathbb{Z})$ denote Tate cohomology. By Rubin [18], Lemma 1.2, there exists $\varkappa = \varkappa(F)$ such that $|(\gamma-1)H^i(\Gamma_{mn}, E_m)| \leqslant p^\varkappa$ for all $0 \leqslant n \leqslant m$ and $i \in \{-1,0\}$. NB. In *loc. cit.* there is a hypothesis

« $[K_0^+ : \mathbb{Q}]$ prime to p », but this is not used in full. One only needs that all divisors of p in K_0^+ are totally ramified in K_∞^+, and that K_0^+ is linearly disjoint with the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. As in *loc. cit.* p. 705 one obtains for any n a sequence

$$(*) \quad 0 \to \lim_{m \geqslant n} H^{-1}(\Gamma_{mn}, E_m) \to (E_\infty)_{1-\gamma_n} \to E_n \to \lim_{m \geqslant n} H^0(\Gamma_{mn}, E_m) \to 0.$$

(Our new notation omitting + is also applied to the symbols E_m here.)

We showed in the proof of Cor. 2.14 that $V_\chi(U_\infty)$ is free cyclic over $\mathbb{Q}_p \otimes \Lambda_\chi$. Hence the submodule $V_\chi(E_\infty)$ is also free cyclic, hence there exists a Λ_χ-homomorphism $\alpha : E_{\infty\chi} \to \Lambda_\chi$ with finite cokernel and kernel annihilated by some power of p. The first and last term in (*) are killed by $(\gamma-1)p^\kappa$. From this, one infers by an easy use of Tor the following sequence for arbitrary n:

$$(**) \qquad 0 \to A_n \to (E_{\infty\chi})_{1-\gamma_n} \to E_{n\chi} \to B_n \to 0$$

with $(\gamma-1)p^{c'}A_n = (\gamma-1)p^{c'}B_n = 0$ with c' a constant independent of n. Now it follows as in *loc. cit.* p. 705 that there exist G_n-maps ϑ_n making the following square commutative for all n:

$$\begin{tikzcd} E_{\infty\chi} \arrow[r, "(\gamma-1)^2p^{2c'}\alpha"] \arrow[d] & \Lambda_\chi \arrow[d] \\ E_{n\chi} \arrow[r, "\vartheta_n"] & \Lambda_{n\chi} = (\Lambda_\chi)_{1-\gamma_n}. \end{tikzcd}$$

On the other hand, $H_\chi(E_{\infty\chi}/\text{im } C_{\infty\chi})$ is finite, hence $H_\chi \cdot (\alpha(E_{\infty\chi})/\alpha(\text{im } C_{\infty\chi}))$ is also finite. From this and the finiteness of coker (α) one obtains $s = s(F) \in \mathbb{N}$ with $p^s H \in \alpha(\text{im } C_{\infty\chi})$. Using surjectivity of $\Lambda_\chi \to \Lambda_{n\chi}$ we deduce

$$(\gamma-1)^2 p^{s+2c'} \cdot H_\chi \cdot \Lambda_{n\chi} \subset \vartheta_n(\text{im } C_{n\chi}).$$

Similarly, there exists $s' \in \mathbb{N}$ with $p^{s'}(\text{im } C_{\infty\chi}) \subset H_\chi \cdot E_{\infty\chi}$ (this uses that $\mathbb{Q}_p E_{\infty\chi} = V_\chi(E_\infty)$ is Λ_χ-cyclic). One obtains

$$p^{s'} \vartheta_n(\text{im } C_{\infty\chi}) \subset H_\chi \cdot \Lambda_{n\chi}.$$

Setting $c_1 = \max(s', s+2c')$, we get the lemma. □

Proof of 3.10. – We need a sublemma which will be used again at the end of this section.

Lemma 3.11. – *The kernel and the cokernel of the multiplication of* $\gamma - 1$ *on* X *is finite.*

Proof (cf. Rubin [18] p. 705). – X is a finitely generated Λ-torsion module. By the structure theorem, it will be sufficient to show the statement concerning the cokernel. Let $Z = X/(\gamma-1)X$. Then $Z \simeq \mathrm{Gal}(N/K_\infty^+)$ where N is the maximal unramified p-extension of K_∞^+ which is abelian over K_0^+ (not only over K_∞^+). N is unramified outside p, and N is the composite of finitely many $\mathbb{Z}_p$-extensions with a finite extension. Since K_0^+ is real abelian, it has only one $\mathbb{Z}_p$-extension by Leopoldt's Conjecture, namely K_∞^+. Hence N is finite over K_∞^+, and $Z = \mathrm{coker}\,(\gamma-1 : X)$ is also finite.

Back to the proof of 3.10 : We intend to show that the surjections (!) $X_{(1-\gamma_n)} \to A_n$ have bounded kernels. The same then follows also for the surjections $X_{(1-\gamma_n),\chi} \to (A_n)_\chi$ for any χ (again an easy argument involving Tor). It is then a routine matter to deduce the requested morphisms τ_n from a quasi-isomorphism $\tau : X_\chi \to \bigoplus_{i=1,\dots,k} \Lambda_\chi/(g_i)$, which will finish the proof.

By Washington [23] p. 278 we have

$$A_n \simeq X/Y_n, \qquad Y_n = \frac{1-\gamma_n}{1-\gamma} Y_0 \text{ with } (\gamma-1)X \subset Y_0 \subset X.$$

Therefore the kernel of $X/(1-\gamma_n)X \to A_n$ is $Y_n/(1-\gamma_n)X$, which is an epimorphic image of $Y_0/(1-\gamma)X$. The latter group is finite, by 3.11, as was to be shown. This concludes the proof of 3.10. □

Before we can tackle the induction argument involved in proving 3.1, we first need an exceedingly technical lemma. It is modeled after Lemma 7.1 in Rubin [13].

Lemma 3.12. – *Let* $\mathbb{Q} \subset K$, *$K/\mathbb{Q}$ real abelian,* $G = \mathrm{Gal}(K/\mathbb{Q})$, Δ *a subgroup of* G. *Let* χ *be a character of* Δ, M *a power of* p, $r \in \mathcal{S}_{M,K}$, *and write* $r = \ell_1 \cdot \cdots \cdot \ell_i$, *with* ℓ_j *prime. Set* $\ell = \ell_i$. *Let* λ *be some fixed prime divisor of* ℓ *in* K, $\mathfrak{c} = [\lambda] \in A(K)$.

Write A *for* $A(K)$, *and let* $B \subset A$ *the subgroup generated by the classes of the primes above* $\ell_1, \cdots \ell_{i-1}$ *in* K. *Let* $x \in K^\times/K^{\times M}$ *such that* $(x)_{[q]} = 0$ *for all primes* q *not dividing* r (*notation from* 3.5), *and* $W \subset K^\times/K^{\times M}$ *the* $\mathbb{Z}_p[G]$-*module spanned by* x. *Assume that* E, g,

$\eta \in \mathbb{Z}_p[G]$ *satisfy the following properties :*

(i) $E \cdot$ *(annihilator of* $(\mathfrak{c})_\chi \in (A/B)_\chi) \subset g \cdot (\mathbb{Z}_p[G])_\chi$;

(ii) $\mathbb{Z}_p[G])_\chi/(g)$ *is finite ; and*

(iii) $M \geqslant |A_\chi| \cdot \left| \eta \cdot \left(\dfrac{\mathcal{J}_\ell / M \mathcal{J}_\ell}{(W)_{[\ell]}} \right)_\chi \right|$.

Then there is a G-homomorphism $\psi : W_\chi \to (\mathbb{Z}/M)[G]_\chi$ *such that*

$$(g \cdot \psi(x)\lambda)_\chi = E \cdot \eta \cdot (x_{[\ell]})_\chi .$$

Proof. – Choose some preimage β of x in $K^\times$. Notation : $\nu_\lambda(\beta)$ is defined as the element of $\mathbb{Z}_p[G]$ with $(\beta)_{[\ell]} = \nu_\lambda(\beta)\lambda$. (This works since ℓ is totally split in K.) By hypothesis, $(\beta)_{[q]} = 0$ for all primes q not dividing r, i.e. the support-q-part of (β) is an M-th power. Since $M \cdot A_\chi = 0$ (see iii)), we therefore obtain that the image of $(\beta)_{[\ell]}$ in $(A/B)_\chi$ is trivial (because it coincides with the image of the principal ideal (β), given the definition of B). Hence $\nu_\lambda(\beta)$ annihilates $(\mathfrak{c})_\chi$ in $(A/B)_\chi$, and by i) : $E \cdot \nu_\lambda(\beta)_\chi$ is divisible by g in $\mathbb{Z}_p[G]_\chi$. Abbreviate this ring by R.

Division by $(g)_\chi$ is unique (if possible) in R, since that ring has no $\mathbb{Z}_p$-torsion and its factor by $(g)_\chi$ is a finite ring by ii). Hence we may define $\delta = E \cdot \nu_\lambda(\beta)_\chi/(g)_\chi \in R$. We now define $\psi : W \to R/MR$ by setting $\psi(\rho \cdot x) = \eta\rho\delta \bmod MR$, for $\rho \in \mathbb{Z}_p[G]$. Once ψ is well-defined, it at once factors to $\psi : W_\chi \to R/MR$, and we also may check the conclusion : $g\psi(x)\lambda_\chi = (\eta|\Delta|g\delta)\lambda_\chi = \eta E \cdot \nu_\lambda(\beta)_\chi \lambda_\chi = (\eta E(x)_{[\ell]})_\chi$, as required. Thus all that matters is that ψ is well-defined. Just suppose $\rho x = 0$; we want $\eta\rho\delta \equiv 0 \bmod MR$. But $\rho x = 0$ means $\rho\beta = y^M$ for some $y \in K^\times$. Hence $\rho \cdot (x)_{[\ell]} = 0$. Let $h = |A_\chi|$. From iii) we get

$$M h^{-1} \eta \cdot (\mathcal{J}_\ell / M \mathcal{J}_\ell)_\chi \subset R \cdot (x)_{[\ell]\chi} ,$$

and ρ annihilates the right side. Hence $\eta\rho$ annihilates $Mh^{-1}(\mathcal{J}_\ell/M\mathcal{J}_\ell)_\chi$, which is R-isomorphic to R/hR (since already $\mathcal{J}_\ell/M\mathcal{J}_\ell$ is $(\mathbb{Z}/M)[G]$-free on λ) ; and therefore $\eta\rho$ is divisible by h in R/MR.

We claim that this implies : $\eta(y)_{[\ell]}$ goes to 0 in $(A/B)_\chi$. For this we write :

$$\begin{aligned}(y) &= \sum_{q \text{ prime}} (y)_{[q]} \\ &= (y)_{[\ell]} + \sum_{j=1}^{i-1} (y)_{[\ell_j]} + \sum_{q \nmid r} \rho M^{-1}(x)_{[q]}\end{aligned}$$

(note $(x)_{[q]}$ is a M-th power).

Multiply everything in this equation by η. Then the left side goes to 0 in $(A/B)_\chi$; the middle summand of the right hand side goes to 0 by definition, and the third summand goes to 0 since $\eta\rho$ is divisible by $h = |A_\chi|$. Hence $\eta(y)_{[\ell]}$ goes to 0 as claimed.

From the claim, we get: $\eta \cdot \nu_\lambda(y)$ annihilates $\mathfrak{c}_\chi$, hence by i) $E \cdot \eta \cdot \nu_\lambda(y)_\chi \in gR$, or, what is the same, $E \cdot \eta \cdot \nu_\lambda(\rho x)_\chi \in MgR$. But $E \cdot \eta \cdot \nu_\lambda(\rho x) = \eta \cdot \rho \cdot g \cdot \delta$, and (again since division by g is unique on R), $\eta\rho\delta \in Mr$, q.e.d. □

The map ψ produced by 3.12 goes to $(\mathbb{Z}/M)[G]_\chi$. We later would like to have a map which goes to $(\mathbb{Z}/M)[G]$ and whose composite with the natural map n: $(\mathbb{Z}/M)[G] \to (\mathbb{Z}/M)[G]_\chi$ is ψ. This can always be achieved at the cost of a factor $|\Delta|$, because of the following lemma:

LEMMA 3.13. – *Let N be any $\mathbb{Z}_p[\Delta]$-module, χ a character of Δ, n: $N \to N_\chi$ the natural epimorphism. Then there is a $\mathbb{Z}_p[\Delta]$-homormorphism ε_χ: $N_\chi \to N$ with $n\varepsilon_\chi = |\Delta| \cdot \mathrm{id}_N$.*

Proof (Maschke). – One may assume $N = \mathbb{Z}_p[\Delta]$, $N_\chi = \mathbb{Z}_p(\chi)$. Let f be a $\mathbb{Z}_p$-linear right inverse of n. Then ε_χ: $y \mapsto \Sigma_{\delta \in \Delta}\, \delta f(\delta^{-1}y)$ $(y \in N)$ does the trick. □

We now are ready for the main argument in the proof of Thm. 3.1. Recall that we have to prove: g (the characteristic series of X_χ) divides H_χ (the characteristic series of $(E_\infty/C_\infty)_\chi$). Let $c = \max(c_1, c_2)$ (see 3.9, 3.10). Let χ be a character of Δ. If χ is trivial, then it is not hard to see that X_χ is quasi-isomorphic to $\varprojlim A(\mathbb{Q}_\nu)$, with $\mathbb{Q}_\infty = \bigcup \mathbb{Q}_\nu$ the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, and it is quite well-known that here $A(\mathbb{Q}_\nu) = 0$, so there is nothing to prove, and we may assume $\chi \neq 1$. Fix $n \in \mathbb{N}$, let $K = K_n^+ (= F(\zeta_{2p^{n+1}})^+)$, choose h a power of p such that $h \geqslant \max(|\Lambda_{n\chi}/(H_\chi)|, \; |\Lambda_{n\chi}/(\mathrm{ord}(\Delta))|, \; |\Lambda_{n\chi}/(p)|)$ and let $M = |A_\chi| \cdot h^{3k+ck+1}$, where A is again short for $A(K)$. For $1 \leqslant i \leqslant k$, there is by 3.10 an element $\mathfrak{c}_i \in A_\chi$ with $\tau_n(\mathfrak{c}_i) = (0,\ldots,0,p^{c_2},0,\ldots,0) \in \oplus\, \Lambda_\chi/(g_i)$ with p^{c_2} in the i-th position; choose $\mathfrak{c}_{k+1} \in A_\chi$ at will. From 3.10 we obtain directly:

$$p^{c_2} \cdot (\text{Annihilator of } \mathfrak{c}_i \text{ in } A_\chi/(\mathfrak{c}_1, \ldots, \mathfrak{c}_{i-1})) \subset g_i \cdot \Lambda_{n\chi}.$$

By Lemma 3.9 there exists a circular unit $\xi \in K$ with $\vartheta_n(\xi) = (\gamma - 1)^2 p^{c_1} H_\chi$. Let (ξ_r), $r \in \mathscr{S}_{M,K}$, be an Euler system starting with ξ, and let $\varkappa_r$ be as earlier (cf. Rubin [19]).

We shall use Thm. 3.7 to construct inductively prime ideals λ_i of K, $1 \leqslant i \leqslant k+1$, such that:

(*a*) $[\lambda_i]_\chi = p^2 \mathfrak{c}_i$

(*b*) ℓ_i, the rational prime below λ_i, is in $\mathcal{S}_{M,K}$

(*c*) In $\Lambda_{n\chi}/(M)$ we have:

$$\nu_{\lambda_1}(\varkappa_{\ell_1}) = \text{unit} \cdot |\Delta| \cdot (\gamma-1)^2 \cdot p^{2+c_1} \cdot H_\chi \,;$$

$$g_{i-1} \cdot \nu_{\lambda_i}(\varkappa_{\ell_1 \ldots \ell_i}) = \text{unit} \cdot |\Delta| \cdot p^{2+c_2} \cdot (\gamma-1)^{2^{i-1}} \cdot \nu_{\lambda_{i-1}}(\varkappa_{\ell_1 \ldots \ell_{i-1}})$$
$$(2 \leqslant i \leqslant k+1).$$

First we do the *case* $i = 1$: We apply Cor. 3.8 with $\mathfrak{c}$ = a preimage of $\mathfrak{c}_1$ in $A = A(K)$, $W = \mathscr{E}/\mathscr{E}^M$ ($\mathscr{E}$=units of K), and

$$\psi\colon\ W \to E_{n\chi}/E_{n\chi}^M \xrightarrow{\vartheta_n} \Lambda_{n\chi}/(M) \xrightarrow{\varepsilon_\chi} \Lambda_n/(M).$$

Cor 3.8 provides a λ which we call λ_1 and which satisfies $[\lambda_1]_\chi = p^2 \mathfrak{c}_\chi = p^2 \mathfrak{c}_1$, (*b*) above holds, and for (*c*) we calculate:

$$\nu_{\lambda_1}(\varkappa_{\ell_1})\lambda_1 = (\varkappa_{\ell_1})_{[\ell_1]} \overset{(3.6)}{=} \varphi_{\ell_1}(\xi) \overset{(3.7)}{=} p^2 \cdot \text{unit} \cdot \psi(\xi)\lambda_1$$
$$= p^2 \cdot \text{unit} \cdot \varepsilon_\chi \vartheta_n(\xi)\lambda_1$$
$$= p^2 \cdot \text{unit} \cdot \varepsilon_\chi (\gamma-1)^2 p^{c_1} H_\chi \lambda_1 \,;$$

if we apply $(..)_\chi$ to this equation, we get (the ε_χ gives a factor $|\Delta|$):

$$\nu_{\lambda_1}(\varkappa_{\ell_1})_\chi = p^{2+c_1} \cdot \text{unit} \cdot |\Delta| (\gamma-1)^2 \cdot H_\chi, \text{ as claimed.}$$

Induction step $i-1 \Rightarrow i$ $(2 < i \leqslant k+1)$: Let $r_{i-1} = \ell \cdots \ell_{i-1}$. Assume that $\lambda_1, \ldots, \lambda_{i-1}$ are already constructed. Putting together the formulas (*c*) for $1, \ldots, i-1$ gives that:

$$\nu_{\lambda_{i-1}}(\varkappa_{r_{i-1}}) \text{ divides } (\gamma-1)^{2^{i-1}} \cdot \underline{p^{2(i-1)} p^{c_2(i-2)} p^{c_1} \cdot |\Delta|^{i-1}} \cdot H_\chi \,;$$

abbreviate the underlined quantity by d. It follows that the $\Lambda_{n\chi}$-module

$$N = (\gamma-1)^{2^t} (\mathscr{J}_{\ell_{i-1}}/(M, (\varkappa_{r_{i-1}})_{[\ell_{i-1}]}))$$

is cyclic and annihilated by dH_χ. From the choice of h, it is then clear that $|N| \leqslant h^{2(i-1)+c_2(i-2)+c_1} \cdot h^{i-1} \cdot h$, and this is $\leqslant Mp^{-n}|C_\chi|^{-1}$. Let $W_i \subset K^\times/K^{\times M}$ be the Λ_n-module generated by $\varkappa_{r_{i-1}}$. We intend to apply Lemma 3.12 with:

$$r = r_{i-1}; \quad \ell = \ell_{i-1}; \quad \lambda = \lambda_{i-1}; \quad g = g_{i-1};$$
$$x = \varkappa_{r_{i-1}}; \quad E = p^{c_2}; \quad \text{and} \quad \eta = (\gamma-1)^{2^{i-1}}.$$

We have to check the hypotheses of 3.12. The condition on x is satisfied by 3.6; (i) is a consequence of 3.10 as has already been noticed, since B_χ is just the span of $[\lambda_1]_\chi, \ldots, [\lambda_{i-2}]_\chi$. Condition (ii) is a well-known fact about the characteristic ideal (g) of X_χ (it amounts to saying that g and $1-\gamma_n$ are coprime in Λ_χ). Condition (iii) is just what we have proved about the module N (with a superfluous factor p^n). Hence there exists a $\Lambda_{n\chi}$-homomorphism ψ_i: $W_{i\chi} \to \Lambda_{n\chi}/(M)$ with

$$(*) \qquad g_{i-1} \cdot \psi_i(\varkappa_{r_{i-1}}) = p^{c_2} \cdot (\gamma-1)^{2^{i-1}} \cdot \nu_{\lambda_{i-1}}(\varkappa_{r_{i-1}})_\chi .$$

Similarly as above we now apply Cor. 3.8 with $\mathfrak{c}$ a preimage of $\mathfrak{c}_i$, $W = W_i$, and $\psi = \varepsilon_\chi \psi_i$. Write λ_i for the resulting prime λ. Then (a) and (b) above are certainly satisfied. For (c), we calculate:

$$g_{i-1} \cdot \nu_{\ell_i}(\varkappa_{r_i})\lambda_i = g_{i-1} \cdot (\varkappa_{r_i})_{[\ell_i]} = g_{i-1}\varphi_{\ell_i}(\varkappa_{r_{i-1}})\lambda_i$$
$$= p^2 \cdot \text{unit} \cdot g_{i-1}\varepsilon_\chi \cdot \psi_i(\varkappa_{r_{i-1}}) \underset{(*)}{=} p^2 \cdot \text{unit} \cdot \varepsilon_\chi \cdot p^{c_2} \cdot (\gamma-1)^{2^{i-1}} \cdot \nu_{\lambda_{i-1}}(\varkappa_{r_{i-1}})\lambda_i .$$

Again, one applies $(..)_\chi$ to both sides and gets the correct statement.

Therewith the λ_i are constructed. The conditions $c)$ for $i = 1, \ldots, k+1$ give by inserting successively (suppress unit factor in $\Lambda_{n\chi}/(M)$):

$$\begin{aligned} g_1 \cdot \cdots \cdot g_k \cdot \nu_{\lambda_{k+1}}(\varkappa_{r_{k+1}}) &= g_1 \cdot \cdots \cdot g_{k-1} \cdot |\Delta| p^{2+c_2} \cdot (\gamma-1)^{2^k} \cdot \nu_{\ell_k}(\varkappa_{r_k}) \\ &= \ldots = \\ &= |\Delta|^k \cdot p^{k(2+c_2)}(\gamma-1)^{2^{k+1}-2} \nu_{\ell_1}(\varkappa_{r_1}) \\ &= \underline{|\Delta|^{k+1} \cdot p^{k(2+c_2)+(2+c_1)} \cdot (\gamma-1)^{2^{k+1}}} \cdot H_\chi . \end{aligned}$$

Call the underlined quantity η. We have now that $g = g_1 \cdot \cdots \cdot g_k$ divides ηH_χ in $\Lambda_{n\chi}/(M)$, hence in $\Lambda_{n\chi}/(p^n)$ (since certainly $p^n | M$). From this it follows as in Rubin [19] that g divides ηH_χ in Λ_χ. By Lemma 3.11 and since $\mu = 0$, see e.g. Washington [23] § 7.5, one finds that η acts on X_χ with finite kernel and cokernel, which means by the structure theorem that η and g are coprime in $\mathbb{Q}_p\Lambda_\chi$, i.e. we may write

$$p^N = \alpha\eta + \beta g \text{ (suitable } N \in \mathbb{N}, \alpha, \beta \in \Lambda_\chi).$$

From this one easily finds that g divides $p^N H_\chi$. Again since $\mu=0$, p does not divide g, and we finally get: $g = \operatorname{char}(X_\chi)$ divides $H_\chi = \operatorname{char}((E_\infty/C_\infty)_\chi)$, and this proves Theorem 3.1.

4. Theorems on class groups.

We begin with relative class groups. Theorem 3.2 states: If $F/\mathbb{Q}$ is abelian, p unramified in F, χ an odd character of $\Delta' = \operatorname{Gal}(K_0/\mathbb{Q})(K_0 = F(\zeta_{2p}))$, $\chi \neq \omega$, then

$$\operatorname{char}(X_\chi) = \left(\frac{1}{2} G_p(T,\check{\chi})\right) \subset \Lambda_\chi .$$

From this, we want to get information on $A(F)_\chi$. At present, we only succeed if χ is already a character of $\Delta = \operatorname{Gal}(F/\mathbb{Q})$. Assume χ is such, and let $F_\infty = \bigcup F_n$ be the cyclotomic $\mathbb{Z}_p$-extension of F. (Then $[K_\infty : F_\infty] = \varphi(2p)$.) Let $X' = \varprojlim A(F_n)$. Then it is well-known (and follows from 2.2) that $\operatorname{char}(X_\chi) = \operatorname{char}(X'_\chi)$. With this in mind, we shall henceforth only consider characters χ of Δ, and change notation as follows: $X = \varprojlim A(K_n)$. Note that now automatically $\chi \neq \omega$. For this whole section, we assume that Δ_p, the p-part of Δ, is cyclic and F is imaginary. Then for $p = 2$, every odd character χ is automatically faithful on Δ_2.

Our result is:

THEOREM 4.1. – *For all odd characters χ which are faithful on Δ_p, we have*

$$|A(F)_\chi| \geqslant \left|\frac{1}{2}\,\mathbf{B}_{1,\chi^{-1}}\right|_p^{d(\chi)} .$$

(Recall our notation: $|x|_p = p^{v(x)}$ for $x \in \mathbb{Q}_p^{alg}$. This theorem implies Thm. A from § 1. In particular, equality holds in Thm. 4.1., except the case $p = 2$ and χ of 2-power order; then $|A(F)_\chi| = 2 \cdot |2^{-1}\mathbf{B}_{1,\chi^{-1}}|_p^{d(\chi)}$ as we saw in § 1.)

For the proof, we first remark that the theorem is known for p odd, see Mazur and Wiles [17] (case $|\Delta|$ prime to p) and Solomon [22] (general case). For simplicity (although this is unnecessary), we suppose $p = 2$ for the rest of the proof. Recall our notation from § 1 : Δ_p = odd part of Δ and $\chi_0 =$ restriction of χ to Δ_0. There we also saw that $A(F)_\chi \simeq (A(F)/\mathrm{im}\, A(F^+))_\chi \simeq (A(F)/\mathrm{im}\, A(F^+))_{\chi_0}$.

The proof of 4.1 splits up in two cases: $\chi(2) \neq 1$ and $\chi(2) = 1$. The former is relatively easy, and the latter rather difficult.

Since $\chi(\text{complex conj.}) = -1$, χ is injective on Δ_2 (cf. end of introduction), hence $\ker(\chi)$ is contained in the odd part Δ_0 of Δ. Hence one may replace F throughout by the fixed field of $\ker(\chi)$, i.e. we may assume χ is injective on Δ.

The case $\chi(2) \neq 1$, i.e. 2 does not split completely in F. Let D be the decomposition group of 2 in Δ and let $\bar{\Delta} = \Delta/D$. Let γ be a topological generator of $\Gamma = \mathrm{Gal}(K_\infty/K_0)$, $\gamma_n = \gamma^{p^n}$. As in Washington [23] p. 278 we get:

$$0 \to \frac{1-\gamma_n}{1-\gamma} \cdot Y_0/(1-\gamma_n)X \to X/(1-\gamma_n)X \to A(K_n) \to 0,$$

and the first term is an epimorphic image of $Z = Y_0/(1-\gamma)X$. (The module Y_0 is defined in *loc. cit.* p. 278.)

Let L and $G = \mathrm{Gal}(L/F)$ be as in *loc. cit.* p. 277 and pick a divisor $\mathfrak{p}$ of p in F, $\mathfrak{P}$ a prime over $\mathfrak{p}$ in L, and σ a generator of the inertia group $I_{\mathfrak{P}}$ of $\mathfrak{P}$ in L/F. Let $G' = \mathrm{Gal}(L/\mathbb{Q})$ and Z' be the $\mathbb{Z}_p$-span of all $z_\tau = [\sigma^\tau \sigma^{-1}] \in X/(1-\gamma)X$ $(\tau \in G')$. Then G' operates naturally on Z'; for $\tau \in G$ we have $\sigma^\tau\sigma^{-1} \in [G,G] = (1-\gamma)X$ by *loc. cit.*, so $z_\tau = 0$. This implies that z_τ only depends on τ mod G, hence Z' is an epimorphic image of the augmentation ideal of $\mathbb{Z}_p\Delta$ via $\delta - 1 \mapsto z_\tau$ (τ any lift of δ), and also $Z' = Z$. Since the p-part of Δ is cyclic by hypothesis, $Z' = Z$ is cyclic over $\mathbb{Z}_p\Delta$. After a little calculation one finds that $D \subset \Delta$ acts trivially on Z', hence Z' is an epimorphic image of $\mathbb{Z}_p\bar{\Delta}$. By taking χ-parts, we find:

$$(\mathbb{Z}_p\bar{\Delta})_\chi \to X_\chi/(1-\gamma_n)X_\chi \to A(K_n)_\chi \to 0.$$

On the leftmost term, the Frobenius of $p = 2$ acts trivially (since D acts trivially), and also via $\chi(2)$, per definition. Hence the leftmost term is a cyclic $\mathbb{Z}_p(\chi)$-module annihilated by $1 - \chi(2)$, i.e. its 2-order is at most $|1-\chi(2)|_2^{d(\chi)}$. On the other hand,

$$\mathrm{char}\,(X_\chi) = (2^{-1}G_2(T,\check{\chi})),$$

and

$$2^{-1}G_2(T,\check{\chi})|_{T=0} = 2^{-1}L_2(0,\check{\chi}) = -2^{-1}(1-\chi^{-1}(2))\cdot \boldsymbol{B}_{1,\chi^{-1}} \neq 0.$$

Hence we get from a well-known lemma (see e.g. Coates [1] Lemma 9) :

$$|X_\chi/(1-\gamma)X_\chi| \geqslant \left|\mathbb{Z}_p(\chi)/(1-\chi^{-1}(2))\cdot\frac{1}{2}\mathbf{B}_{1,\chi^{-1}}\right|_2$$

$$= |1-\chi^{-1}(2)|_2^{d(\chi)}\cdot\left|\frac{1}{2}\mathbf{B}_{1,\chi^{-1}}\right|_2^{d(\chi)}.$$

From the exact sequence and the above dicussion, we then get the formula of 4.1.

The case $\chi(2)=1$. By our reduction to the case χ faithful on Δ, we have that 2 is totally split in F. The problem is that the error term linking $X_\chi/(1-\gamma_n)X_\chi$ and $A(F_n)$ is no longer a finite group, and correspondingly that the Iwasawa series $G_2(T,\chi)$ is divisible by T. So roughly speaking « we must divide 0 by 0 and end up with the correct result ».

We begin with a lemma for which we allow arbitrary p. Let B_n be the subgroup generated by the divisors of p in the divisor group of F_n, and D_n the image of B_n in $A_n = A(F_n)$. Let $D_\infty = \underset{\leftarrow}{\lim}\, D_n$, and define B_n^+, D_n^+ analogously with F_n^+ instead of F_n. (The following lemma only needs that p is totally split in $F_0(=F)$, all divisors of p in F_0 are totally ramified in the $\mathbb{Z}_p$-extension F_∞, and that $\mu_{p^\infty}(F_\infty)$ is finite.)

LEMMA 4.2. — *With the above notation and* j = *complex conjugation* $\in\Delta$, *one has an isomorphism of* $\mathbb{Z}_p\Delta[[\Gamma]]$-*modules, with trivial* Γ-*action on the right :*

$$D_\infty/\mathrm{im}\, D_\infty^+ \simeq \mathbb{Z}_p\Delta/((1+j)\mathbb{Z}_p\Delta).$$

Proof. — Fix a norm-coherent sequence of divisors $\mathfrak{p}_n$ of p in F_n. Let $h(h^+)$ be the p-class number of $F(F^+)$. Then the projective system $B_n/(hB_0+B_n^+)$ is isomorphic to the projective system $(\mathbb{Z}/hp^n\mathbb{Z})[\varDelta]/(1+j)$, via $1\mapsto\mathfrak{p}_n$. We now intend to show that the orders of the kernels of $\alpha_n : B_n/(hB_0+B_n^+)\to D_n/\mathrm{im}\, D_n^+$ are bounded. (NB. hB_0 maps to 0 in D_n.) This will imply that $\lim\alpha_n$ induces an isomorphism $\mathbb{Z}_p([\Delta]/(1+j)\to D_\infty/\mathrm{im}\, D_\infty^+$, for the $\ker(\alpha_n)$ disappear in the limit which is $\mathbb{Z}_p$-torsion free.

It suffices to show $|\mathrm{Im}(\alpha_n)| \geqslant p^{n.|\Delta|/2}\cdot\mathrm{const}$ for $n \to \infty$, or: $|D_n|/|D_n^+| \geqslant p^{n.|\Delta|/2}\cdot\mathrm{const}$. By Lang [16], chap. 13 § 4, formulas (2) and (3), we have for any cyclic extension K/F' with group G ($I =$ divisor group, $P =$ principal divisor group, $e(k/F') =$ product of all ramification indices of $K/F', N{=}N_{K/F'}$):

$$[I_K^G : P_K^G] = \frac{e(K/F')\cdot h_F}{[K : F']\cdot(E_{F'} : NE_k)}.$$

We apply this twice: for $(K,F') = (F_n, F)$ and $(K,F') = (F_n^+, F^+)$, and compare. Note that $B_n = I_K^G, (I_K^G/P_K^G)' \simeq D_n$ (for $K{=}F_n$), with $'$ short for « p-part ». One obtains

$$e(F_n/F) = p^{|\Delta|},\ e(F_n^+/F^+) = p^{|\Delta|/2},$$

$$|D_n| = p^{n\cdot(|\Delta|-1)}h\cdot(E_F : NE_{F_n})',$$

$$|D_n^+| = p^{n\cdot\left(\frac{|\Delta|}{2}-1\right)}h^+\cdot(E_{F^+} : NE_{F_n^+})'.$$

Since F contains only finitely many roots of 1 of p-power order, the quotient of the two norm indices in the last two equations stays bounded. Thus the quotient of the two right hand sides above can be minorated by $p^{n|\Delta|/2}$ times a constant, QED. □

Corollary 4.3. – *Let* $p = 2$ *again. Let* $X = \lim A(F_n)$, *and* $E = X/D_\infty \simeq \varprojlim (A_n/D_n)$, (*NB.* E *has no relation with units here*), *and similarly* X^+, E^+. *Let* $i : E^+ \to E$ *be the canonical map. Then* i *is injective.* (*We shall take the liberty of writing* E/E^+ *for* $E/\mathrm{im}\,E^+$.)

Proof. – Consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & D_\infty^+ \arrow[r] \arrow[d] & X^+ \arrow[r] \arrow[d] & E^+ \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & D_\infty \arrow[r] & X \arrow[r] & E \arrow[r] & 0.
\end{tikzcd}$$

We want $D_\infty \cap \mathrm{im}\,X^+ = \mathrm{im}\,D_\infty^+$ ($\supset$ is clear). Consider the operation of j on the quotient $Q = D_\infty \cap \mathrm{im}\,X^+/\mathrm{im}\,D_\infty^+$. It must be identity (because of the plus sign at X), but it must also be -identity, as it is so on the whole of $D_\infty/\mathrm{im}\,D_\infty^+$. Since $D_\infty/\mathrm{im}\,D_\infty^+$ has no 2-torsion by lemma 4.2, Q must be zero, q.e.d. □

Now let also $E_n = A_n/D_n$, $E_n^+ = A_n^+/D_n^+$. For brevity, we write M_x for M/xM throughout for $\mathbb{Z}_p[[\Gamma]]$-modules M and $x \in \mathbb{Z}_p[[\Gamma]]$. Look at the following diagram where Z and Z^+ are defined as kernels:

(*)
$$\begin{tikzcd} 0 \arrow[r] & Z^+ \arrow[r] \arrow[d, "\alpha"'] & (E^+)_{1-\gamma} \arrow[r] \arrow[d, "\beta"'] & E_0^+ \arrow[r] \arrow[d, "\varepsilon"'] & 0 \\ 0 \arrow[r] & Z \arrow[r] & E_{1-\gamma} \arrow[r] & E_0 \arrow[r] & 0. \end{tikzcd}$$

From the snake lemma we obtain, using $|E_0| \cdot |E_0^+|^{-1} = |\mathrm{coker}\,(\varepsilon)| \cdot |\ker\,(\varepsilon)|^{-1}$:

(**)
$$\begin{aligned} |(E/E^+)_{1-\gamma}| &= |\mathrm{coker}\,(\beta)| \\ &\leqslant |\ker\,(\beta)| \cdot |E_0| \cdot |E_0^+|^{-1} \cdot |\mathrm{coker}\,(\alpha)| \\ &= |\ker\,(\beta)| \cdot |E_0| \cdot |E_0^+|^{-1} \cdot |Z/\mathrm{im}\, Z^+|. \end{aligned}$$

(The $\leqslant$ sign comes from neglecting $|\ker\,(\alpha)|^{-1}$.)

Convention and Remark. – Denote $\chi_0 = \chi | \Delta_0$ by ξ for the rest of the proof. Since Δ_0 has odd order, the functor $(\cdot\cdot)_\xi$ is exact on $\mathbb{Z}_2[\Delta_0]$-modules. Hence the preceding formulas and the next lemma remain true on attaching $(\cdot\cdot)_\xi$ to all modules involved.

LEMMA 4.4. – *Let* $(\cdot\cdot)^{(1-\gamma)}$ *denote the annihilator of* $1-\gamma$ *in* $(\cdot\cdot)$. *If* $Z/\mathrm{im}\, Z^+$ *is finite, then*

$$|\ker\,(\beta)| \leqslant |(E/E^+)^{(1-\gamma)}| < \infty.$$

Proof. – There is a map β' with $\beta'\beta = 2 \cdot \mathrm{id}$ (use the norm $F_n \to F_n^+$). Hence $2 \cdot \ker\,(\beta) = 0$, and $\ker\,(\beta)$ is finite because E^+ (a quotient of X^+) is finitely generated over $\mathbb{Z}_2$. Since $|E_0|$ is finite, the hypothesis implies that $(E/E^+)_{(1-\gamma)}$ is finite, whence $T = 1-\gamma$ operates with finite kernel and cokernel on E/E^+. From $0 \to E^+ \to E \to E/E^+ \to 0$ we get (since $(\cdots)_{(1-\gamma)} = \Lambda/(T) \otimes_\Lambda \cdots$):

$$\mathrm{Tor}^\Lambda(\Lambda/(T), E/E^+) \to (E^+)_{1-\gamma} \xrightarrow{\beta} E_{1-\gamma} \to (E/E^+)_{1-\gamma} \to 0,$$

and the lemma follows because the Tor term is just $(E/E^+)^{(1-\gamma)}$. □

From this we get

PROPOSITION 4.5. – $\left|\frac{1}{2} G_2'(0, \check{\chi})\right|_2^{d(\chi)} \leqslant \frac{|E_0\xi|}{|E_0^+\xi|} \cdot |(Z/Z+)_\xi|$. (*′ is derivative w.r.to T*).

Proof. – There is a short exact sequence (from 4.3 and the snake lemma):

$$0 \to (D_\infty/D_\infty^+)_\xi \to (X/\mathrm{im}\, X^+)_\xi \to (E/E^+)_\xi \to 0\,.$$

In all three occurences, one may replace $(\cdot\cdot)_\xi$ by $(\cdot\cdot)_\chi$ without change. Thus we obtain for the characteristic ideals over $\Lambda_\chi = \mathbb{Z}_2(\chi)[[T]]$:

$$\mathrm{char}\,((D_\infty/D_\infty^+)_\chi) = (T) \text{ by Lemma 4.2};$$

$$\mathrm{char}\,((X/\mathrm{im}\, X^+)_\chi) = \left(\frac{1}{2}G_2(T,\check{\chi})\right) \text{ by Section 3}.$$

Hence $2^{-1}G_2(T,\check{\chi})$ is divisible by T (which one may also see directly form $\chi(2)=1$; so-called trivial zero), and

$$\mathrm{char}\,((E/E^+)_\chi) = \left(\frac{1}{2}G_2(T,\check{\chi})\cdot T^{-1}\right)\cdot$$

From a well-known lemma on Iwasawa modules (see e.g. Coates [1]), we obtain

$$|\mathrm{coker}\,(\beta_\xi)| = |(E/E^+)_{\xi,1-\gamma}| = |(E/E^+)_\xi^{(1-\gamma)}|\cdot\left|\frac{1}{2}G_2'(0,\check{\chi})\right|_2^{d(\chi)}\cdot$$

We now use (**) for the left hand side and obtain

$$|\ker(\beta_\xi)|\cdot|E_{0\xi}|\cdot|(E_0^+)_\xi|^{-1}\cdot|(Z/\mathrm{im}\, Z^+)_\xi| \geqslant |(E/E^+)_\xi^{(1-\gamma)}|\cdot\left|\frac{1}{2}\cdot G_2'(0,\check{\chi})\right|_2^{d(\chi)}\cdot$$

By (the ξ-version of) Lemma 4.4 we get the conclusion. (Note that the proposition is trivial if $(Z/Z^+)_\xi$ happens to be infinite.) □

We have $|E_0/E_0^+| = |E_0|/|E_0^+| = |A_0|\cdot|A_0^+|^{-1}\cdot|D_0|^{-1}\cdot|D_0^+|$, and the ξ-version of this is also true. Since ξ is nontrivial, the maps $(A_0^+)_\xi \to A_{0\xi}$ and $(D_0^+)_\xi \to D_{0\xi}$ are injective, whence $|A_{0\xi}|\cdot|A_{0\xi}^+|^{-1} = |A_{0\xi}/A_{0\xi}^+|^{-1}$, and similarly for D. Hence we may rewrite the statement of 4.5 as follows:

$$(***)\qquad \left|\frac{(A_0)_\xi}{(A_0^+)_\xi}\right| = \left|\frac{(E_0)_\xi}{(E_0^+)_\xi}\right|\cdot\left|\frac{(D_0)_\xi}{(D_0^+)_\xi}\right|$$

$$\geqslant \left|\frac{1}{2}\cdot G_2'(0,\check{\chi})\right|_2^{d(\chi)}\cdot\left|\left(\frac{Z}{\mathrm{im}\, Z^+}\right)_\xi\right|^{-1}\cdot\left|\frac{(D_0)_\xi}{(D_0^+)_\xi}\right|\cdot$$

Note that the left hand side of (***) is precisely $|A(F)_\chi|$. To prove Thm. 4.1, it therefore suffices to show the following

THEOREM 4.6. – $$\left|\frac{1}{2}\cdot G_2'(0,\check{\chi})\right|_2^{d(\chi)}\cdot\left|\left(\frac{Z}{\operatorname{im} Z^+}\right)_\xi\right|^{-1}\cdot\left|\frac{(D_0)_\xi}{(D_0^+)_\xi}\right|=\left|\frac{1}{2}B_{1,\chi^{-1}}\right|_2^{d(\chi)}.$$

We need some preparations. One main point is to get a better understanding of Z, Z^+ etc. Fix a prime divisor $\mathfrak{p}$ of p in F and a prime $\mathfrak{p}^+$ under $\mathfrak{p}$ in F^+. Then the prime divisors of p in F are precisely all $\mathfrak{p}_\delta=\mathfrak{p}^\delta$, $\delta\in\Delta$, and the prime divisors of p in F^+ are the $(\mathfrak{p}^+)^\delta$ where δ runs over a set of representatives of Δ mod $\{1,j\}$. Let $V\subset\mathbb{Q}_2^\times$ be the subgroup generated by -1 and 2, so $V=\{1,-1\}\times 2^{\mathbb{Z}}$. The group $(\mathbb{Q}_2\otimes F)^\times$ is canonically identified with $(\mathbb{Q}_2^\times)^\Delta$, the Δ-fold product of $\mathbb{Q}_2^\times$ with itself. We introduce the following group:

$$N(F)=(\mathbb{Q}_2\otimes F)^\times/\mathrm{closure}(\mathcal{O}_F[2^{-1}]^\times)\cdot V^\Delta$$

and similarly $N(F^+)$ (replace F by F^+, Δ by $\Delta^+=\Delta/\{1,j\}$). Note that $N(F)$ is an epimorphic image of $(\mathbb{Z}_2^\times)^\Delta$.

PROPOSITION 4.7. – *If* $\xi\neq 1$, *then :*

a) *There is a natural isomorphism* $Z_\xi\to N(F)_\xi$, *and ditto with* $+$.

b) $(Z/\operatorname{im} Z^+)_\chi\cong(N(F)/N(F^+))_\chi\cong N(F)_\chi$.

Proof. – *a*) (Cf. Sinnott [21].) We give the proof for F; the argument for F^+ is quite the same. Let L be the maximal unramified abelian 2-extension of F_∞ in which all divisors of 2 split completely. Then by class field theory, $\mathrm{Gal}(L/F_\infty)\cong E=X/D_\infty$. Similarly, $E_0=\mathrm{Gal}(L_0/F)$, L_0 the maximal abelian unramified 2-extension of F in which all divisors of 2 split completely. Let $M=L\cap F^{ab}$; $G=\mathrm{Gal}(L/F)$, $G/G'=\mathrm{Gal}(M/F)$. The fields involved form a diagram

$$\begin{tikzcd}
F_\infty \arrow[r, dash, "E_0"] \arrow[d, dash, "\Gamma"'] & F_\infty L_0 \arrow[r, dash] \arrow[d, dash, "\Gamma"'] & M \arrow[r, dash] & L \\
K_0 = F \arrow[r, dash, "E_0"] & L_0 & &
\end{tikzcd}$$

Claim. – $\mathrm{Gal}(M/L_0)$ is naturally isomorphic to $N(F)$. Proof of claim : M is the maximal abelian 2-ramified 2-extension of F satisfying simultaneously (i) M/F_∞ unramified and (ii) all divisors of 2 in F have inertial degree one in M. Let $C_2(F) = J(F)/F^\times \cdot \prod U_\mathfrak{q}(F)$ (product over all $\mathfrak{q}$ not dividing 2). Then M corresponds to some closed subgroup H of $C_2(F)$. We want to determine H. First of all:

$$M \supset F_\infty \Leftrightarrow H \subset N_{F/\mathbb{Q}}^{-1}(H_0) \subset C_2(F),$$

with $H_0 =$ (norm group belonging to $\mathbb{Q}_\infty/\mathbb{Q}$) $= \{1, -1\} \subset \mathbb{Q}_2^\times/2^\mathbb{Z} = C_2(\mathbb{Q})$. Recall we identified $(\mathbb{Q}_2 F)^\times$ with $(\mathbb{Q}_2^\times)^\Delta$; let $(...)^{(\delta)}$: $\mathbb{Q}_2^\times \to (\mathbb{Q}_2 F)^\times$ be the δ-th canonical injection. Of course there is the canonical map $(\mathbb{Q}_2 F)^\times \to C_2(\mathrm{F})$.

Since, for all $\mathfrak{p}_\delta$, the decomposition group and the inertia group of $\mathfrak{p}_\delta$ in M coincide, we know: $\mathrm{im}(\mathbb{Q}_2^{\times(\delta)}) = \mathrm{im}(\mathbb{Z}_2^{\times(\delta)})$ in $C_2(F)/H$. Hence one can find for all $\delta \in \Delta$ some $u_\delta \in \mathbb{Z}_2^\times$ with $2^{(\delta)} \equiv (u_\delta)^{(\delta)} \bmod H$, i.e. $(2 \cdot u_\delta^{-1})^{(\delta)} \in H$. Since $N_{F/\mathbb{Q}}((2 \cdot u_\delta^{-1})^{(\delta)}) = 2u_\delta^{-1} \in \mathbb{Q}_2^\times/2^\mathbb{Z}$, we must have $u_\delta \in \{1, -1\}$. On the other hand, we also have that M is unramified over K_∞, which translates to:

$$\mathrm{im}(\mathbb{Z}_2^{\times(\delta)}) \cap N_{F/\mathbb{Q}}^{-1}(H_0) \subset H,$$

and in particular $(-1)^{(\delta)} \in H$ for all δ. Taking all this together, we see that H is the image of V^Δ in $C_2(F)$. (Recall $V = \{1, -1\} \times 2^\mathbb{Z} \subset \mathbb{Q}_2^\times$.) Hence $\mathrm{Gal}(M/F) = C_2(F)/\mathrm{im}\mathrm{V}^\Delta$.

One now checks that one has a short exact sequence

$$0 \to \frac{\mathbb{Q}_2^\times F}{\mathcal{O}_F[2^{-1}]^\times \cdot V^\Delta} \to \frac{C_2(F)}{V^\delta} \to \frac{A_0}{D_0} \to 0,$$

where A_0/D_0 is the Galois group of L_0/F. Hence the first term, which is just $N(F)$, is canonically isomorphic to $\mathrm{Gal}(M/L_0)$, in other words:

$$0 \to N(F) \to G/G' \to E_0 \to 0$$

is exact. Now one has as usual (cf. Washington [23] Lemma 13.14):

$$0 \to E_{(1-\gamma)} \to G/G' \to \Gamma \to 0,$$

with Δ operating trivially on Γ, i.e. $\Gamma_\xi = 0$. Hence $E_{\xi(1-\gamma)} \cong (G/G')^\xi$, and since all the maps are canonical, we obtain $N(f)_\xi \cong \ker(E_{\xi(1-\gamma)} \to E_{0\xi}) = Z_\xi$, which proves part *a*).

Proof of b). — From *a)* for F and F^+ one obtains by naturality of the isomorphism an isomorphism $(Z/\operatorname{im} Z^+)_\xi \cong (N(F)/N(F^+))_\xi$. One sees directly that j operates as -1 on the right hand side, hence also on the left hand side, and we may replace the subscript ξ by χ on both sides. □

In order to process the quantity $(N(F)/N(F^+))_\chi$ further, we need the Gross-Koblitz formula, as used in Gross [10].

Definitions.

$$W = (\mathcal{O}_F[2^{-1}]^\times)/\mathcal{O}_{F^+}[2^{-1}]^\times \ \ (\textit{2-units of } F \text{ mod } \textit{2-units of } F^+)\,;$$

$$\begin{aligned} M &= (\textit{free } \mathbb{Z}_2\textit{-module on all } \mathfrak{p}_\delta,\ \delta\in\Delta)/(\textit{span of all } \mathfrak{p}_\delta\mathfrak{p}_\delta^j) \\ &\simeq \mathbb{Z}_2[\Delta]/(1+j)\,; \end{aligned}$$

$$\begin{aligned} \mu :\ & W \to M, \\ & u \mapsto \sum_{\delta\in\Delta} v_{\mathfrak{p}_\delta}(u)\cdot\mathfrak{p}_\delta\,; \\ \lambda :\ & W \to 4M \\ & u \mapsto \sum_{\delta\in\Delta} \log_2(\delta^{-1}u)\cdot\mathfrak{p}_\delta. \quad (\log_2 :\ F \to F_\mathfrak{p} = \mathbb{Q}_2 \xrightarrow{\log_2} 4\mathbb{Z}_2.) \end{aligned}$$

Then μ and λ are $\mathbb{Z}\Delta$-linear, with the evident Δ-action on M. Note that $M_\chi \cong \mathbb{Z}_2(\chi)$ via $\mathfrak{p} \mapsto 1$, and that we also have homomorphisms $\mu_\chi,\ \lambda_\chi :\ W_\chi \to M_\chi$.

The usefulness of μ and λ only becomes apparent when they are applied to a certain subgroup of W afforded by Gauss sums. In more detail: Let m be the conductor of F (hence m is odd), $\mathfrak{P}$ a prime of $\mathbb{Q}(m)$ over $\mathfrak{p}$, and $\eta :\ \mathcal{O}_{\mathbb{Q}(m)}/\mathfrak{P} \to \mu_m$ the m-th power residue symbol. Further, let $\psi :\ \mathbb{F}_2 \to \mu_2$ a (or rather: the) nontrivial additive character. Define a Gauss sum g by

$$g = -\sum \eta^{-1}(a)\cdot\psi(\operatorname{Tr}(a)) \quad (\operatorname{Tr} :\ \mathcal{O}_{\mathbb{Q}(m)}/\mathfrak{P} \to \mathbb{F}_2 \text{ the trace}).$$

Then $g \in F$. (This is an instance of the fact that for p arbitrary, g^{p-1} is in the decomposition field of p in $\mathbb{Q}(m)$.) Moreover, it certainly is a 2-unit. Denote the $\mathbb{Z}_2\Delta$-span of g in W by $\langle g\rangle$. From Stickelberger's theorem one obtains:

$$\text{(G1)}\quad g\mathcal{O}_{\mathbb{Q}(m)} = \mathfrak{p}^{\sum_b \sum_{t=1}^{f} m\langle p^t/m\rangle\cdot\sigma_b^{-1}}$$
$$(\text{outer sum over } b \in (\mathbb{Z}/m)^\times/\langle p\rangle,\ f = \operatorname{ord}(p \bmod m))$$

hence

$$\mu(g) = m\cdot\sum_{\delta\in\Delta}\ \sum_{\substack{b \bmod m\\ \sigma_b\mapsto\delta}} \langle b/m\rangle\cdot \mathfrak{p}_{\delta^{-1}},$$

$$\mu_\chi(g_\chi) = m\cdot(\Sigma_b\langle b/m\rangle\chi^{-1}(b))\,(\mathfrak{p})_\chi = m\cdot \mathbf{B}_{1,\chi^{-1}}\cdot(\mathfrak{p})_\chi .$$

On the other hand, we have from the Gross-Koblitz relation and the Ferrero-Greenberg relation, as used in Gross [10], p. 993 :

$$\lambda(g) = \sum_\delta \log_2(\delta^{-1}g)\cdot\mathfrak{p}_\delta \text{ by definition, hence}$$

$$\lambda_\chi(g_\chi) = (\sum_\delta \log_2(g^\delta)\cdot\chi^{-1}(\delta))\,(\mathfrak{p})_\chi$$

$$= (\sum_\delta \chi^{-1}(\delta)\cdot\log_2\prod_{i=1}^{f}\Gamma_p(\langle p^i a/m\rangle))\,(\mathfrak{p})_\chi \text{ (where } \sigma_a\mapsto\delta)$$

(Gross-Koblitz)

$$= \sum_{(b,m)=1} \chi^{-1}(b)\cdot\log_2\Gamma_2(\langle b/m\rangle))\,(\mathfrak{p})_\chi$$

$$= \sum_{(b,m)=1} \chi^{-1}(b)\cdot\zeta_2'(b,0)\,(\mathfrak{p})_\chi \text{ (Ferrero-Greenberg).}$$

For the definition of $\zeta_2(b,s)$, see Gross *op. cit.* By Lemma 4.8 below, the last expression equals $L_2'(0,\check{\chi})(\mathfrak{p})_\chi$. This in turn equals $\log_2(u)G_2'(0,\check{\chi})(\mathfrak{p}_\chi)$ by the formula $L_2'(s,\check{\chi}) = G_2(u^s - 1,\check{\chi})$, and $\log_2(u)$ is associated to 4. The end result is therefore :

$$\text{(G2)} \qquad \lambda_\chi(g_\chi) = 4G_2'(0,\check{\chi})\cdot\text{unit}\cdot(\mathfrak{p})_\chi .$$

LEMMA 4.8. — *With the above notation* $\sum_{(b,m)=1}\chi^{-1}(b)\cdot\zeta_2(b/s) = L_2(s,\check{\chi})$ *as meromorphic functions on* $\mathbb{Z}_2$.

Proof. — It suffices to check this for $s = 1 - n$, $n\in\mathbb{N}$ odd. This is easily done, using the definitions (see Washington [23] chap. 5 and Gross [10] p. 989). □

It remains to put everything together. From (G1) we see that $\mu_\chi \neq 0$; from Gross [10] we see $\lambda_\chi \neq 0$. (This follows from 1.15 in *op. cit.*, which in turn is a consequence of Conjecture 2.12. This conjecture is proved in the abelian case at the end of *op. cit.*). The range of λ_χ and μ_χ is M_χ ; let us identify M_χ with $\mathbb{Z}_2(\chi)$ with the help of the basis element $(\mathfrak{p})_\chi$ for the rest of the proof.

It is an easy exercise to show $\mathbb{Q}_2 \otimes W \simeq \mathbb{Q}_2\Delta/(1+j)$, whence also $\mathbb{Q}_2 \otimes W \simeq \mathbb{Q}_2(\chi)$. Let W'_χ be the 2-adic completion of W_χ, modulo 2-torsion. Then W'_χ is a rank one module over $\mathbb{Z}_2(\chi)$, hence λ_χ and μ_χ induce monomorphisms $W'_\chi \to M_\chi$.

Lemma 4.9. – $|\operatorname{coker}(\lambda_\chi)| = |(Z/\operatorname{im} Z^+)_\chi|$.

Proof. – We show $|\operatorname{coker}(\lambda_\chi)| = |(N(F)/N(F^+))_\chi|$ (this suffices by 4.7). Consider

$$\begin{tikzcd} & W'_\chi \arrow[r, "\lambda_\chi"] \arrow[d] & 4\mathbb{Z}_2(\chi) \arrow[d, equal] \\ V^\Delta \arrow[r] & ((\mathbb{Q}_2F)^\times/(\mathbb{Q}_2F^+)^\times)_\chi \arrow[r, "\lambda'_\chi"] & 4\mathbb{Z}_2(\chi) \end{tikzcd}$$

with $\lambda' : (\mathbb{Q}_2F)^\times \to 4\mathbb{Z}_2$ defined exactly as λ. Since $\ker(\log_2 : \mathbb{Q}_2^\times \to 4\mathbb{Z}_2) = V$, we easily see that the lower sequence is exact. Hence $\operatorname{coker}(\lambda_\chi) = \operatorname{domain}(\lambda'_\chi)/(\operatorname{im} W'_\chi \cdot \operatorname{im} V^\Delta) \simeq (N(F)/N(F^+))_\chi$, which proves the lemma. □

Lemma 4.10. – $|\operatorname{coker}(\mu_\chi)| = |(D_0/\operatorname{im} D_0^+)_\chi|$.

Proof. – From the definition of μ, one has a natural isomorphism $\operatorname{coker}(\mu) \simeq D_0/\operatorname{im} D_0^+)$.

Finally, we can give the proof of Theorem 4.6:

$$\begin{aligned} |(Z/\operatorname{im} Z^+)_\chi|^{-1} \cdot |(D_0/\operatorname{im} D_0^+)_\chi| &\underset{4.9,\,4.10}{=} |\operatorname{coker}(\lambda_\chi)|^{-1} \cdot |\operatorname{coker}(\mu_\chi)| \\ &= |4\mathbb{Z}_2(\chi)/\lambda_\chi(\langle g_\chi \rangle)|^{-1} \cdot |\operatorname{Im}(\lambda_\chi)/\lambda_\chi(\langle g_\chi \rangle)| \cdot |\mathbb{Z}_2(\chi)/\mu_\chi(\langle g_\chi \rangle)| \\ &\qquad \cdot |\operatorname{Im}(\mu_\chi)/\mu_\chi(\langle g_\chi \rangle)|^{-1} \\ &= |4\mathbb{Z}_2(\chi)/\lambda_\chi(\langle g_\chi \rangle)|^{-1} \cdot |W'_\chi/\langle g_\chi \rangle \cdot |\mathbb{Z}_2(\chi)/\mu_\chi(\langle g_\chi \rangle)| \cdot |W'_\chi/(\langle g_\chi \rangle)|^{-1} \\ &= |G'_2(0,\chi)|_2^{-d(\chi)} \cdot |\mathbf{B}_{1,\chi^{-1}}|_2^{-d(\chi)} \quad \text{by (G1) and (G2) above.} \end{aligned}$$

This is, up to slight rearranging, precisely the formula of 4.6. Hence 4.6 and also 4.1 are proved.

We now turn to class groups of *real* abelian fields. Let for the rest of the section F be a real abelian number field, p a fixed prime, $\Delta = \Delta_p \times \Delta_0 = \operatorname{Gal}(F/\mathbb{Q})$, with Δ_p the p-part of Δ. First we consider a variant of the class group: let $A'(F) = \varprojlim C_{(p^\nu)}(F)$, with $C_{(p^\nu)}(F) = p$-part of $I_{(p^\nu)}(F)/P_{(p^\nu)}(F))$, the p-ray class group mod $p^\nu \mathcal{O}_F$. Then $Y = \varprojlim A'(F_n)$ (F_n as in § 3) is isomorphic to the Galois group of the maximal abelian p-ramified p-extension of F_∞. Recall $e = e_\varepsilon = |\Delta_0|^{-1} \cdot \sum_{\delta \in \Delta_0} \delta$.

THEOREM 4.11. – *The group* $(1-e)A'(F)$ *is finite, and for all characters* $\chi_0 \neq 1$ *of* Δ_0:

$$|A'(F)_{\chi_0}| = \prod_{\chi|\Delta_0=\chi_0} \left|\frac{1}{2}L_p(1,\chi)\right|_p^{d(\chi)}$$

(χ *character of* Δ).

Proof. – Y is a Λ_Δ-module, and one knows that $A'(F) \simeq Y/TY$. Let $\dot{T}$ be defined by $1+\dot{T} = u\cdot(1+T)^{-1}$; then by Theorem 3.2 and Prop. 3.4, for all characters χ of Δ:

$$\mathrm{char}_{\Lambda_\chi}(Y_\chi) = \frac{1}{2}G_p(\dot{T},\chi)\Lambda_\chi,$$

hence, as is easily verified,

$$\mathrm{char}_{\Lambda_{\chi_0}}(Y_{\chi_0}) = \left(\prod_\chi \frac{1}{2}G_p(\dot{T},\chi)\right)\Lambda_{\chi_0}. \quad \left(\prod \text{ over all } \chi \text{ with } \chi|\Delta_0=\chi_0\right).$$

From Iwasawa theory we get, letting $\delta(\chi_0)$ = order of module of T-coinvariants of $(Y_{\chi_0})^{tors}$: (A' is short for $A'(F)$)

$$|A'_{\chi_0}| = \prod_\chi \left|\frac{1}{2}G_p(\dot{T},\chi)|_{T=0}\right|_p^{d(\chi_0)} \cdot \delta(\chi_0)$$

$$= \prod_\chi \left|\frac{1}{2}L_p(1,\chi)\right|_p^{d(\chi_0)} \cdot \delta(\chi_0).$$

If we can show that, on the other hand, the product of $|A'_{\chi_0}|$ over all $\chi_0 \neq 1$ equals the product of $|2^{-1}L_p(1,\chi)|_p$ over all χ with $\chi|\Delta_0 \neq 1$, then all $\delta(\chi_0)$ must be 1, and we are done. The former product is equal to $|(1-e)A'| = |A'(F)|/|A'(L)|$, L the fixed field of Δ_0. Now consider the sequence

$$0 \to (1-e)(U_F/E_F) \to (1-e)A'(F) \to (1-e)A(F) \to 0.$$

We claim that $|(1-e)(U_F/E_F)| = p^{-[F:\mathbb{Q}]+[L:\mathbb{Q}]}\cdot R_p(F)\cdot R_p(L)^{-1}$.

(*Proof of claim* : Consider the homomorphism $\log_p : (1-e)\mathrm{U}_F \to (1-e)p(\mathbb{Z}_p\otimes\mathcal{O}_F)$. One has $|\ker(\log_p)| = |\mathrm{coker}(\log_p)|$ (for odd p, both are 1; for $p=2$, both are equal to $2^{g(F)-g(L)}$, g denoting the decomposition degree of 2 in an abelian field). Moreover, $(1-e)E_F \cap \ker(\log_p) = 0$. Hence we find $|(1-e)U_F/E_F)| = |(1-e)p\mathbb{Z}_p\mathcal{O}_F/(1-e)\log_p(E_F)|$. Using the definition of the regulators $R_p(F)$ and $R_p(L)$, one obtains the claimed formula.)

Hence we get:

$$|(1-e)A'(F)| = p^{-[F:\mathbb{Q}]+[L:\mathbb{Q}]}.\frac{R_p(F)}{R_p(L)}.\frac{|A(F)|}{|A(L)|}.$$

By the p-adic class number formula for F, *and* L (see e.g. Washington [23] Thm. 5.24), the last expression equals

$$(2p)^{-[F:\mathbb{Q}]+[L:\mathbb{Q}]}\left|\frac{d(F)}{d(L)}\right|_p^{1/2}\cdot\prod_{\chi|\Delta_0\neq 1}(1-p^{-1}\chi(p))^{-1}L_p(1,\chi).$$

Now L and F are unramified in p, and $\chi(p)$ is never zero. Hence this last expression has the same p-value as $\prod 2^{-1}L_p(1,\chi)$ (product over all χ with $\chi|\Delta_0\neq 1$), what was to be shown. □

This theorem has two consequences. First, we get a real analog for the Conjecture of Iwasawa and Leopoldt:

THEOREM 4.12 (= Thm. C in § 1). – *Let F be as in* 4.11, *and cyclic over* $\mathbb{Q}$. (*Actually Δ_p cyclic suffices.*) *Then for all characters χ of Δ such that $\chi|\Delta_p$ is faithful:*

$$|A'(F)_\chi| = \left|\frac{1}{2}L_p(1,\chi)\right|_p^{d(\chi)}.$$

Proof. – Let $\chi' = \chi|\Delta_0$, $\chi'' = \chi|\Delta_p$. If $\Delta_p = 1$, the theorem is immediate from Thm. 4.11. So suppose $\Delta_p \neq 1$ and let C be the unique subgroup of Δ_p with p elements. Denote the fixed field of C by F_1. By Lemma 4.13 below one has maps α: $A'(F)\to A'(F_1)$ and β: $A'(F_1)\to A'(F)$ such that α is surjective, β is injective, and $\beta\alpha$ is multiplication with $\sum_{\sigma\in C}\sigma\in\mathbb{Z}[\Delta]$. By Solomon [22] cor. II.1, we may infer:

$$|A'(F)_\chi| = |A'(F)_{\chi'}|/|A'(F_1)_{\chi'}|.$$

Now a character of F is also a character of F_1 iff it is not faithful on Δ_p. By 4.11, we hence obtain that the above quotient is equal to

$$\prod|2^{-1}L_p(1,\xi)|_p^{d(\chi')}$$

(product over all ξ with $\xi|\Delta_0 = \chi'$, ξ on Δ_p faithful).

It is easy to see that the latter product equals precisely $|2^{-1}L_p(1,\chi)|_p^{d(\chi)}$.

LEMMA 4.13. – *If F/K is a p-extension of cyclic number fields which are unramified over p, then there are Galois-equivariant homomorphisms $\alpha : A'(F) \to A'(K)$ and $\beta : A'(K) \to A'(F)$ such that α is onto, β is monic, and $\beta\alpha$ = multiplication by the norm element of $C = \mathrm{Gal}(F/K)$.*

Proof. – One naturally takes α to be the map induced by $N_{F/K}$, and β the map induced by the inclusion $K \subset F$. Since $\mathrm{Gal}(F/\mathbb{Q})$ is spanned by inertia groups, and is cyclic, one sees that some rational prime $(\neq p)$ ramifies totally in $F/\mathbb{Q}$. Hence F/K has no p-ramified subextensions, and therefore α is onto. The point is to show that β is injective. If $\mathfrak{m}$ is any divisor of K, then one verifies that $\ker(C_{\mathfrak{m}}(K) \to C_{\mathfrak{m}}(F))$ embeds into $H^1(C, E_{\mathfrak{m}}(F))$ where $E_{\mathfrak{m}}(F) = \ker(\mathcal{O}_F^\times \to (\mathcal{O}_F/\mathfrak{m}\mathcal{O}_F)^\times)$. It is therefore sufficient to show $\varprojlim H^1(C, E_{(p^\nu)}(F)) = 0$ (since $\varprojlim$ is left exact). The proof of this uses the validity of Leopoldt's conjecture for p and F: it is easily checked that there exists a constant $2 \leqslant N \in \mathbb{N}$ such that: if $x \in E_{(p^{N+1})}(F)$, then x is the p-th power of another unity y. Since p is unramified in F, y is necessarily already in $E_{(p^N)}(F)$. Now let $p^c = |C|$, $N \leqslant \nu \in \mathbb{N}$ and take any 1-cocycle $x = (x_\sigma)$ in $Z^1(C, E_{(p^{\nu+c})}(F))$. Then every x_σ can be written $y_\sigma^{p^c}$ with $y_\sigma \in E_{(p^\nu)}(F)$. Since there are no p-power roots of unity in F, (y_σ) is again a cocycle. Hence the image of x in $H^1(C, E_{(p^\nu)}(F))$ is divisible by p^c which means that it is zero. Since ν $(\geqslant N)$ was arbitrary, we get our conclusion.

Now we go back from ray class groups to class groups.

THEOREM 4.14. – *Let $F/\mathbb{Q}$ be real and cyclic with group Δ. (Again, it suffices that the p-part Δ_p is cyclic.) Let $\mathscr{C}_F$ be the group of circular units of F in the sense of Sinnott, $C_F = \mathscr{C}_F \cap E_F$. Then we have for all nontrivial characters χ' of Δ_0 (recall $\Delta = \Delta_p \times \Delta_0$):*

$$|(E_F/C_F)_{\chi'}| = |A(F)_{\chi'}| \cdot 2^{d(\chi')|\Delta_p|} \cdot |(R:U)_{\chi'}|,$$

where $R = \mathbb{Z}[\Delta]$ and U are as in Sinnott [20].

Remark. – The group C_F is usually a bit smaller than one would expect; e.g., if $F = \mathbb{Q}(\zeta_p)^+$, $p \geqslant 3$, then it does not contain $\zeta_p + \zeta_p^{-1}$ (only the square of this unit). This can be partly remedied by studying the group C_F (see *op. cit.* p. 209). Usually, this brings about indeterminacies in the formulas. However, one can prove the following :

COROLLARY 4.15. – *If $|\Delta|$ is prime to p, then the conjecture of G. Gras is true in the following form : $[E_F/C_{1F}] = [A(F)]$ in $K_0^{\mathrm{fin}}(\mathbb{Z}_p[\Delta])$, the Grothendieck group of the category of all finite $\mathbb{Z}_p[\Delta]$-modules.*

Assuming Thm. 4.14, we give the *proof* of the corollary :

It is not too hard to check that $\mathbb{Z}_pR = \mathbb{Z}_pU$ if $|\Delta|$ is prime to p. Using the description of $K_0^{\mathrm{fin}}(\mathbb{Z}_p[\varDelta])$ via χ'-parts, and Thm. 4.14, we obtain $[E_F/C_F] = [A(F)] + [(1-e)(\mathbb{Z}_p/2\mathbb{Z}_p)[\Delta]]$. For p odd, we are then done since C_{1F}/C_F is 2-elementary. For $p = 2$, one checks, using the arguments of Sinnott [20], p. 209 and $(p,|\Delta|) = 1$, that every totally positive element of C_F is a square in E_F, and hence $C_{1F}/C_F \simeq (1-e)(\mathbb{Z}/2\mathbb{Z})[\Delta]$, and we are again done. □

Proof of 4.14. – First note that U does not have to be a subset of R; the index notation is explained in Sinnott, *op. cit.* § 1. Let $e' = 1 - e$. The statement of 4.14 can be equivalently expressed in the form (suppress subscripts $(\,.\,.\,)_F$) :

$$[e'(E/C)] = [e'A(F)] + [e'\mathbb{Z}_p/2)[\Delta]] + [e'R/e'U]$$

in $K_0^{\mathrm{fin}}(\mathbb{Z}_p[\Delta])$. (To see the equivalence, note that $\mathrm{R}_{\chi'} = \mathbb{Z}_p(\chi')[\Delta_p]$ is local for any character χ' of Δ_0, and the class of an $\mathrm{R}_{\chi'}$ module in $K_0^{\mathrm{fin}}(\mathbb{Z}_p[\Delta])$ is determined by its length, i.e. by its order.) Let $\mathcal{O}$ be the ring obtained by adjoining all values of all characters χ of Δ to $\mathbb{Z}_p$. ($\mathcal{O}$ will play the role of $\mathbb{R}$ in Sinnott's proof.) Let $\mathcal{O}^{(\chi)}$ be the $\mathbb{Z}_p\Delta$-module $\mathcal{O}$ (Δ operating through χ).

Claim. — $[\mathcal{O}\otimes e'A(F)] = \sum_{\chi}[\mathcal{O}^{(\chi)}/(2^{-1}L_p(1,\chi))] - [e'U_F : e'E_F]$ in $K_0^{\mathrm{fin}}(\mathcal{O}\Delta)$.

(χ running over all characters of Δ which are nontrivial on Δ_0, $\otimes$ taken over $\mathbb{Z}_p$.)

To prove this claim, it suffices to see that for any $\chi' \neq 1$, $A'(F)$ has the cardinality p to the power $\sum v_p(2^{-1}L_p(1,\chi))$ (sum over χ with $\chi|\Delta_0 = \chi'$) ; but this follows directly from Theorem 4.11.

Since $[E_F/C_F] = [U_F/C_F] - [U_F/E_F]$ and since the natural map $K_0^{\mathrm{fin}}(\mathbb{Z}_p\Delta) \to K_0^{\mathrm{fin}}(\mathcal{O}\Delta)$ is injective, it remains to show :

$$(*)\quad [\mathcal{O}\otimes e'(U_F/C_F)] = \left[\prod_{\chi|\Delta_0\neq 1}\mathcal{O}^{(\chi)}\Big/\left(\frac{1}{2}L_p(1,\chi)\right)\right] + [e'(\mathcal{O}/2\mathcal{O})\Delta] + [e'\mathcal{O}R/e'\mathcal{O}U],$$

where the last summand means $[e'\mathcal{O}R/e'\mathcal{O}M] - [e'\mathcal{O}U/e'\mathcal{O}M]$, M arbitrary lattice contained in both R and U. This is proved by adapting the method of Sinnott [20] § 4. In particular, the L-functions used in *loc. cit.* are replaced by p-adic L-functions. We consider the p-adic logarithmic embedding

$$\ell_p : \mathcal{O} \otimes U_F \to p\mathcal{O}[\Delta], \qquad u \mapsto \sum_{\delta \in \Delta} \log_p(u^{\sigma}) . \sigma^{-1} .$$

One checks, using that $F/\mathbb{Q}$ is unramified in p, that

$$[\mathcal{O} \otimes e'(U_F/C_F)] = [\mathcal{O} \otimes e' p \mathcal{O}_F / \mathcal{O} \otimes \log_p(e'C_F)] = [e'p\mathcal{O}[\Delta]/\ell_p(e'C_F)] .$$

Following Sinnott, we define

$$\omega' = \sum_{\chi} e_{\chi^{-1}} \cdot L_p(1,\chi) \cdot (p^{-1}\chi(p) - 1)^{-1} \cdot f_\chi \cdot \tau_\chi^{-1} \in \operatorname{Quot}(\mathcal{O})[\Delta]$$

(sum over all characters χ of Δ). One rewrites prop. 4.2 and its corollary of *op. cit.* appropriately (using the formula for $L_p(1,\chi)$) and obtains:

$$\ell_p(e'C_F) = e'\omega' U .$$

On the other hand, since $R^{\sim} = \prod_{\chi} \mathcal{O}^{(\chi)}$ is the integral closure of $\mathcal{O}[\Delta]$, one obtains

$$[e'p\mathcal{O}[\Delta]/e'\omega'\mathcal{O}[\Delta]] = [e'pR^{\sim}/e'\omega R^{\sim}] = \left[\prod_{\chi|\Delta_0 \neq 1} \mathcal{O}^{(\chi)}/(L_p(1,\chi))\right]$$

(note $(p^{-1}\chi(p) - 1)^{-1} \sim p$). Putting the last three formulas together, we get

$$\begin{aligned} [\mathcal{O} \otimes e'(U_F/C_F)] &= [e'p\mathcal{O}[\Delta]/e'\omega' U] \\ &= [e'p\mathcal{O}[\Delta]/e'\omega'\mathcal{O}[\Delta]] \cdot [e'\mathcal{O}[\Delta]/e'U] \\ &= \left[\prod_{\chi|\Delta_0 \neq 1} \mathcal{O}^{(\chi)}/(L_p(1,\chi))\right] \cdot [e'R : e'U] , \end{aligned}$$

which implies the desired formula (*) immediately.

BIBLIOGRAPHY

[1] J. Coates, p-adic L-functions and Iwasawa theory, Proc. Symp. Alg. Number theory, Durham (1975), 269-353.

[2] R. Coleman, Division values in local fields, Invent. Math., 53 (1979), 91-116.

[3] R. Coleman, Local units modulo circular units, Proc. Amer. Math. Soc., 89, 1 (1983), 1-7.

[4] L. J. Federer, Regulators, Iwasawa modules, and the Main conjecture for $p = 2$, in: N. Koblitz (ed.): Number theory related to Fermat's Last Theorem, Birkhäuser Verlag (1982), 289-296.

[5] R. Gillard, Unités cyclotomiques, unités semi-locales et $\mathbb{Z}_\ell$-extensions, Ann. Inst. Fourier, Grenoble, 29-1 (1979), 49-79.

[6] R. Gold, J. Kim, Bases for cyclotomic units, Comp. Math., 71 (1989), 13-28.

[7] G. Gras, Sur l'annulation en 2 des classes relatives des corps abéliens, C.R. Math. Rep. Acad. Sci. Canada, 1 (1978), n° 2, 107-110.

[8] R. Greenberg, On p-adic L-functions and cyclotomic fields I, Nagoya Math. J., 56 (1975), 61-77.

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

[10] B. Gross, p-adic L-series at $s = 0$, J. Math. Soc. Japan, 28 (1981), 979-994.

[11] K. Iwasawa, On some modules in the theory of cyclotomic fields, J. Math. Soc. Japan, 16 (1964), 42-82.

[12] K. Iwasawa, Lectures on p-adic L-functions, Annals of Math. Studies n° 74, Princeton University Press, Princeton 1972.

[13] K. Iwasawa, On $\mathbb{Z}_\ell$-extensions of algebraic number fields, Ann. of Math., (2) (1979), 236-326.

[14] M. Kolster, A relation between the 2-primary parts of the main conjecture and the Birch-Tate conjecture, Canad. Math. Bull., 32 (1989), 248-251.

[15] V. A. Kolyvagin, Euler systems. In: The Grothendieck Festschrift, vol. 2, 435-483, Birkhäuser Verlag 1990.

[16] S. Lang, Cyclotomic fields II, Graduate Texts in Mathematics, Springer Verlag, 1980.

[17] B. Mazur, A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, Invent. Math., 76 (1984), 179-330.

[18] K. Rubin, On the main conjecture of Iwasawa theory for imaginary quadratic fields, Invent. Math., 93 (1988), 701-713.

[19] K. Rubin, The Main Conjecture, Appendix to the second edition of S. Lang: Cyclotomic fields, Springer Verlag, 1990.

[20] W. Sinnott, On the Stickelberger ideal and the circular units of an abelian field, Invent. Math., 62 (1980), 181-234.

[21] W. Sinnott, Appendix to L. Federer, B. Gross : Regulators and Iwasawa modules, Invent. Math., 62 (1981), 443-457.

[22] D. Solomon, On the class groups of imaginary abelian fields, Ann. Inst. Fourier, Grenoble, 40-3 (1990), 467-492.

[23] L. Washington, Introduction to cyclotomic fields, Graduate Texts in Mathematics n° 83, Springer Verlag, 1982.

[24] A. Wiles, The Iwasawa conjecture for totally real fields, Ann. Math., 131 (1990), 493-540.

Manuscrit reçu le 12 juillet 1991.

Cornelius Greither,
Mathematisches Institut
der Ludwig-Maximilians-Universität
Theresienstrasse 39
8000 München (Allemagne).