SÉMINAIRE N. BOURBAKI

JOHN COATES

The work of Mazur and Wiles on cyclotomic fields

Séminaire N. Bourbaki, 1981, exp. n° 575, p. 220-242

<http://www.numdam.org/item?id=SB_1980-1981__23__220_0>

© Association des collaborateurs de Nicolas Bourbaki, 1981, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (http://www.bourbaki.ens.fr/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI
33e année, 1980/81, n° 575

575-01
Juin 1981

THE WORK OF MAZUR AND WILES ON CYCLOTOMIC FIELDS

by John COATES

Introduction

Let p be an odd prime number, $\mu_{p^{n+1}}$ the group of p^{n+1}-th roots of unity, and F_n the cyclotomic field $\mathbb{Q}(\mu_{p^{n+1}})$. Let $\zeta(s)$ denote the Riemann zeta function. The remarkable connexion, perceived by Kummer in special cases, between the arithmetic of the fields F_n and the rational numbers $\zeta(-k)$ (k odd and positive) has been one of the most tantalising and inaccessible problems in number theory for over a hundred years. We owe to Iwasawa [6], [7] several important contributions to this problem, including a precise formulation of the problem in terms of his Γ-modules attached to the tower of fields F_n ($n = 0,1,\ldots$), which has subsequently become known as the main conjecture on cyclotomic fields. In a discovery whose importance it is difficult to overestimate, Mazur and Wiles [13] have recently proven this main conjecture by a beautiful generalisation of earlier work of Ribet [15] and Wiles [22] on the construction of unramified extensions of the fields F_n via points of finite order on the Jacobians of modular curves. The aim of the present exposé is to give a not too technical account of the key ideas in Mazur and Wiles' proof. From lack of both space, and knowledge on my part, I shall say very little about the subtle and difficult geometry of modular curves and their reductions, even though this plays an essential role in Mazur and Wiles' work. Indeed this subject has considerable independent interest, and certainly merits a Bourbaki lecture devoted to it alone.

Notation

Throughout, p will be an odd prime number, and $\mathbb{Z}_p$ the p-adic integers. For each integer $N \geq 1$, μ_N will denote the group of N-th roots of unity. If L/K is a Galois extension of fields, $G(L/K)$ will denote the Galois group of L over K. Put

$$F_n = \mathbb{Q}(\mu_{p^{n+1}}) \quad , \quad F_\infty = \bigcup_{n \geq 0} F_n \ ,$$

and write A_n for the p-primary subgroup of the ideal class group of F_n. Let

$$G_\infty = G(F_\infty/\mathbb{Q}) \quad , \quad \Gamma = G(F_\infty/F_0) \quad , \quad \Delta = G(F_0/\mathbb{Q}) \ .$$

The restriction map induces an isomorphism from the torsion subgroup of G_∞ onto Δ , and we henceforth indentify these two groups. We then have

$$G_\infty = \Delta \times \Gamma \ .$$

The cyclotomic character $\psi : G_\infty \longrightarrow \mathbb{Z}_p^\times$ is defined by the action of G_∞ on μ_{p^∞} , i.e. $\sigma(\zeta) = \zeta^{\psi(\sigma)}$ for all $\sigma \in G_\infty$ and $\zeta \in \mu_{p^\infty}$. It is an isomorphism by the irreducibility of the cyclotomic equation. We write ϑ and K for the respective restrictions of ψ to Δ and Γ . These give isomorphisms

$$(1) \qquad \vartheta : \Delta \xrightarrow{\sim} \mu_{p-1} \quad , \quad K : \Gamma \xrightarrow{\sim} U \ ,$$

where U denotes the group of p-adic units $\equiv 1$ mod. p . In particular, ϑ generates the group of p-adic characters of Δ . Write j for the element of order 2 in Δ , given by complex conjugation for any embedding of F_∞ into $\mathbb{C}$. A character χ of Δ will be said to be *even* (respectively, *odd*) if $\chi(j) = 1$ (respectively, $\chi(j) = -1$).

1. The main theorem of Mazur-Wiles

It is simplest to begin by stating the result of Mazur and Wiles for the field F_∞ . The p-primary subgroup A_∞ of the ideal class group of F_∞ is defined as follows. If $n \leq m$, there is a natural map $A_n \longrightarrow A_m$, and we let $A_\infty = \varinjlim A_n$, relative to these homomorphisms. Thus A_∞ is a discrete p-primary G_∞-module. It is more convenient to work with the Pontrjagin dual

$$X_\infty = \mathrm{Hom}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$$

which is a compact G_∞-module ; in general, if A and B are G_∞-modules, we endow $\mathrm{Hom}(A,B)$ with the G_∞-structure given by $(\sigma f)(a) = \sigma f(\sigma^{-1}a)$. Let Y be any compact G_∞-module, which is also a $\mathbb{Z}_p$-module. Recalling that $G_\infty = \Delta \times \Gamma$, we first decompose

$$(2) \qquad Y = \bigoplus_\chi Y^{(\chi)} \ ,$$

where χ runs over the characters in $\hat{\Delta} = \mathrm{Hom}(\Delta, \mathbb{Z}_p^\times)$ (in other words, χ runs over the ϑ^i for i mod. $(p-1)$), and where $Y^{(\chi)}$ denotes the submodule of Y on which Δ acts via χ (i.e. $\sigma m = \chi(\sigma)m$ for all $\sigma \in \Delta$ and $m \in Y^{(\chi)}$). Secondly, let $\Lambda = \mathbb{Z}_p[[T]]$ denote the ring of formal power series in an indeterminate T with coefficients in $\mathbb{Z}_p$. For simplicity, take γ_0 to be the unique topological generator of Γ with $K(\gamma_0) = 1 + p$, in the second isomorphism of (1). Then, defining $(1 + T)m = \gamma_0 m$ for all $m \in Y^{(\chi)}$, it is not difficult to see ([16]) that we can extend this by linearity and continuity to a continuous action of Λ on $Y^{(\chi)}$. The proof of the following theorem of Iwasawa (see [8] for a convenient reference, but in fact he established it much earlier) is algebraic

in the sense that it depends only on global class field theory, and not on the p-adic analytic theory of the numbers $\zeta(-2k-1)$ $(k = 0,1,\ldots)$.

THEOREM 1 (Iwasawa).– *For each* $\chi \in \hat{\Delta} = \mathrm{Hom}(\Delta, \mathbb{Z}_p^{\times})$, $X_\infty^{(\chi)}$ *is a finitely generated* Λ*-torsion* Λ*-module, which has no non-zero finite* Λ*-submodule.*

Similar algebraic arguments show that $X_\infty^{(\chi)} = 0$ for $\chi = \vartheta^0, \vartheta, \vartheta^{-1}$, but give no further information on the other components $X_\infty^{(\chi)}$ for $\chi \neq \vartheta^0, \vartheta, \vartheta^{-1}$. However, Theorem 1 and the structure theory of finitely generated Λ-modules ([16]) immediately implies that, for each $\chi \in \hat{\Delta}$, we have an exact sequence of Λ-modules

$$0 \longrightarrow X_\infty^{(\chi)} \longrightarrow \mathfrak{G}_\chi \longrightarrow D_\chi \longrightarrow 0 ,$$

where D_χ is finite, and $\mathfrak{G}_\chi$ is of the form

$$\mathfrak{G}_\chi = \Lambda/(f_{\chi,1}) \oplus \ldots \oplus \Lambda/(f_{\chi,r_\chi})$$

with r_χ some integer ≥ 0 , and $f_{\chi,k}$ $(1 \leq k \leq r_\chi)$ non-zero elements of Λ . The ideal $\left(\prod_{k=1}^{r_\chi} f_{\chi,k}\right)$ in Λ is uniquely determined by $X_\infty^{(\chi)}$, and we call any generator of this ideal a characteristic power series of $X_\infty^{(\chi)}$. Thus a characteristic power series of $X_\infty^{(\chi)}$ is only determined up to multiplication by a unit in Λ . The simplest way to specify a power series in Λ uniquely is to give its values at any infinite subset of the points $T = (1+p)^s - 1 \in p\mathbb{Z}_p$, where s runs over $\mathbb{Z}_p$ (note that the elements of Λ converge at these points). Iwasawa [6], [7] had the remarkable insight to see that many of the open problems on the arithmetic of the fields F_n would be a consequence of a (conjectural) description of a characteristic power series of $X_\infty^{(\chi)}$, for each odd character χ in $\hat{\Delta}$ distinct from ϑ^{-1} , in terms of the p-adic interpolation properties of the numbers $\zeta(-k)$ $(k = 1,3,\ldots)$. Here $\zeta(s)$ denotes the Riemann zeta function, and we recall that Euler proved that

$$\zeta(-k) = -\frac{B_{k+1}}{k+1} \qquad (k \geq 1 \ , \ k \text{ odd}) ,$$

where B_r is the r-th Bernouilli number, defined by the expansion

$$\frac{t}{e^t - 1} = \sum_{r=0}^{\infty} \frac{B_r}{r!} t^r .$$

Although it is not at all obvious, it is known that, given an odd character χ in $\hat{\Delta}$ distinct from ϑ^{-1} , there exists a unique power series $L_\chi(T)$ in Λ satisfying

(3) $$L_\chi((1+p)^k - 1) = (1 - p^k)\zeta(-k) ,$$

for all positive integers $k \geq 1$ such that $\chi = \vartheta^k$ (i.e., writing $\chi = \vartheta^i$, for all integers $k \geq 1$ with $k \equiv i \bmod (p-1)$). The following is Mazur and Wiles' main result, which proves Iwasawa's conjecture in the affirmative.

THEOREM 2 (Mazur-Wiles).– *Let* $\chi \in \hat{\Delta}$ *be an odd character distinct from* ϑ^{-1} . *Define the odd residue class* $i \bmod (p-1)$ *by* $\chi = \vartheta^i$. *Then the power series*

$L_\chi(T)$ *satisfying* (3) *for all* $k \geq 1$ *with* $k \equiv i \bmod. (p-1)$ *is a characteristic power series of* $X_\infty^{(\chi)}$.

Remarks.— (i) The existence of the power series $L_\chi(T)$ (for χ odd in $\hat{\Delta}$, $\chi \neq \vartheta^{-1}$) is in fact equivalent to congruences on Bernoulli numbers which were known to Kummer (see [17], p. 243). The study of these congruences was revived and extended by Kubota and Leopoldt [11]. Indeed, it is plain that $L_\chi((1+p)^{-s} - 1)$, when viewed as a function of the variable s in $\mathbb{Z}_p$, is the p-adic L-function attached in [11] to the even character $\chi\vartheta$.

(ii) As will be explained in § 3, Iwasawa [7] gave a completely new construction of the $L_\chi(T)$ in terms of the classical Stickelberger elements for the tower F_∞ . His construction has the great merit that it immediately suggests a link between $L_\chi(T)$ and the Λ-module $X_\infty^{(\chi)}$. Specifically, Iwasawa's construction together with the classical theorem of Stickelberger on the factorisation of Gauss sums shows that $L_\chi(T)$ must annihilate $X_\infty^{(\chi)}$ (χ odd, $\chi \neq \vartheta^{-1}$).

(iii) Recall that r_χ denotes the number of direct summands occurring in the Λ-module $\mathcal{E}_\chi$. Let (H_p) denote the hypothesis that we can choose $r_\chi \leq 1$ for all odd characters χ in $\hat{\Delta}$. If (H_p) is valid, Theorem 2 is an easy consequence of Iwasawa's work referred to in (ii), and the analytic class number formula [1]. But this approach breaks down completely if hypothesis (H_p) does not hold. While the numerical evidence is in favour of hypothesis (H_p) , there is little theoretical evidence to support its validity, beyond the fact that it would greatly simplify the whole cyclotomic theory. It is striking that Mazur and Wiles' work gives no information at all about the values of r_χ .

(iv) Although the work of Mazur and Wiles throws no light on the mysterious question of determining the characteristic power series of the Λ-modules $X_\infty^{(\psi)}$ when ψ runs over the even characters of Δ , we briefly recall our fragmentary knowledge on this problem. Let (I_p) (resp. (K_p)) denote the hypothesis that $X_\infty^{(\psi)} = 0$ (resp. $A_o^{(\psi)} = 0$) for all even characters ψ of Δ . Note that (K_p) is none other than the classical hypothesis that p does not divide the class number of the maximal real subfield of $\mathbb{Q}(\mu_p)$.

Lemma 3.— *We have the implications* $(K_p) \Rightarrow (I_p) \Rightarrow (H_p)$.

We do not give the detailed proof of this well known lemma, but simply remark that the first implication holds because the theory of Γ-modules shows that, for any $\psi \in \hat{\Delta}$, $A_o^{(\psi)} = 0$ implies that $A_n^{(\psi)} = 0$ for all $n \geq 0$. To establish the second implication, one uses class field theory and Kummer theory to prove that if $X_\infty^{(\psi)} = 0$ for an even character $\psi \neq \vartheta^o$, then $r_\chi \leq 1$ for the odd character $\chi = \psi\vartheta^{-1}$. We also note that it is unknown whether (I_p) implies (K_p) . Since (K_p) has been verified numerically in [21] for all $p \leq 125{,}000$, we see that (I_p) is also valid in this range. But there is little theoretical

evidence in favour of (I_p), and the whole question seems inaccessible at present.

2. Consequences of the theorem of Mazur-Wiles

We begin by explaining how two long conjectured refinements of Kummer's analytic class number formulae for the field $F_o = \mathbb{Q}(\mu_p)$ are consequences of Theorem 2. If S is a finite set, write $\#(S)$ for the cardinality of S. We write $|\ |_p$ for the p-adic valuation of $\mathbb{Q}_p$, normalised by $|p|_p = p^{-1}$. Note that we can decompose A_o as a direct sum

$$A_o = A_o^+ \oplus A_o^- ,$$

where A_o^+ (resp. A_o^-) is the subgroup on which j acts by $+1$ (resp. -1). For $\chi \in \hat{\Delta}$, let the number $L(\chi,0) \in \mathbb{Q}_p$ be as defined in § 3 ; in fact, $L(\chi,0)$ belongs to the field obtained by adjoining the values of χ to $\mathbb{Q}$.

The first class number formula of Kummer asserts that

$$\#(A_o^-) = |p \prod_{\chi(j)=-1} L(\chi,0)|_p^{-1}, \tag{4}$$

the product being taken over all odd characters in $\hat{\Delta}$.

THEOREM 4 (Mazur-Wiles).— *For each odd character* $\chi \neq \vartheta^{-1}$ *in* $\hat{\Delta}$, *we have*

$$\#(A_o^{(\chi^{-1})}) = |L(\chi,0)|_p^{-1} .$$

This theorem is a refinement of (4) because it can easily be shown that $\#(A_o^{(\vartheta)}) = |pL(\vartheta^{-1},0)|_p = 1$. We stress that Theorem 4 seems inaccessible to classical methods on cyclotomic fields, althougher Stickelberger's theorem gives the partial result that $L(\chi,0)$ annihilates $A_o^{(\chi^{-1})}$ for all odd characters $\chi \neq \vartheta^{-1}$. The first person to obtain results in the other direction was Ribet [15], who introduced the key idea of constructing unramified extensions of F_o via the Jacobians of modular curves, and who proved that $A_o^{(\chi^{-1})} \neq 0$ when $L(\chi,0)$ is divisible by p, for any odd $\chi \neq \vartheta^{-1}$. We now outline the derivation of Theorem 4 from Theorem 2. Since $X_\infty^{(\chi)}$ has no finite non-zero Γ-submodule, we have

$$\#(X_\infty^{(\chi)}/TX_\infty^{(\chi)}) = |L_\chi(0)|_p^{-1}$$

by Theorem 2. The construction of $L_\chi(T)$ given in [7] shows that $L_\chi(0) = L(\chi,0)$. But $X_\infty^{(\chi)}/TX_\infty^{(\chi)}$ is dual to $(A_\infty^{(\chi^{-1})})^\Gamma$, and this latter group can be identified with $A_o^{(\chi^{-1})}$ by virtue of the following well known and elementary fact : for all $n \leq m$, the natural map $A_n^- \longrightarrow A_m^-$ is injective, and induces an isomorphism $A_n^- \xrightarrow{\sim} (A_m^-)^{G(F_n/F_m)}$. Although it plays no role in this argument, we recall that it is still unknown whether the map $A_n^+ \longrightarrow A_m^+$ is injective for all $n \leq m$.

Let E_o be the group of global units of the field F_o, and let C_o be the intersection with E_o of the subgroup of $F_o^\times$ generated by $1 - \zeta$, where ζ denotes a primitive p-th root of unity. We call C_o the group of cyclotomic units of F_o. The following facts were derived by Kummer from the theory of

complex L-functions attached to $F_o/\mathbb{Q}$. Firstly, the index of C_o in E_o is finite. Secondly, if we write B_o for the p-primary sybgroup of E_o/C_o , then

$$\#(B_o^+) = \#(A_o^+) \ , \tag{5}$$

where B_o^+ denotes the elements of B_o which are fixed by complex conjugation.

THEOREM 5 (Mazur-Wiles).— *For each even character* χ *in* $\hat{\Delta}$, *we have*

$$\#(A_o^{(\chi)}) = \#(B_o^{(\chi)}) \ .$$

See [5] for a proof that Theorem 5 is a consequence of Theorem 2.

We next briefly indicate one consequence of Theorem 2 for the higher K-theory of $\mathbb{Z}$. For each integer $m \geq 0$, let $K_m\mathbb{Z}$ denote Quillen's higher K-group of $\mathbb{Z}$. If m is even and positive, Borel has shown that $K_m\mathbb{Z}$ is finite. For $r \geq 1$, let $w_r(\mathbb{Q})$ denote the largest integer N such that the Galois group of $\mathbb{Q}(\mu_N)$ over $\mathbb{Q}$ is annihilated by r .

THEOREM 6.— *Let* n *be an odd positive integer. With the possible exception of its 2-primary subgroup, the order of* $K_{2n}\mathbb{Z}$ *is divisible by* $w_{n+1}(\mathbb{Q})\zeta(-n)$.

Lichtenbaum had earlier conjectured that the order of $K_{2n}\mathbb{Z}$ is precisely $\pm\, w_{n+1}(\mathbb{Q})\zeta(-n)$. The essential result in deriving Theorem 6 from Theorem 5 is the following theorem of Soulé [19], [14] (which remains valid if we replace $\mathbb{Q}$ by any totally real finite extension H of $\mathbb{Q}$, $\mathbb{Z}$ by the ring of integers of H , and $\mathbb{Q}(\mu_{p^\infty})$ by $H(\mu_{p^\infty})$). Let $\mathfrak{T} = \varprojlim \mu_{p^n}$ be the Tate module. Thus $\mathfrak{T}$ is a free $\mathbb{Z}_p$-module of rank 1 , on which G_∞ acts via the cyclotomic character ψ . If M is a G_∞-module which is also a $\mathbb{Z}_p$-module, we define, for each integer $k \geq 0$,

$$M(k) = M \otimes_{\mathbb{Z}_p} \mathfrak{T} \otimes_{\mathbb{Z}_p} \ldots \otimes_{\mathbb{Z}_p} \mathfrak{T} \qquad (k \text{ times}) \ , \tag{6}$$

endowed with the diagonal action of G_∞ . Soulé's theorem asserts that, for each odd prime p , and each odd positive integer n , there is a canonical surjection

$$K_{2n}\mathbb{Z}(p) \longrightarrow\!\!\!\!\!\rightarrow (A_\infty^-(n))^{G_\infty} \ ,$$

where the group on the left denotes the p-primary subgroup of $K_{2n}\mathbb{Z}$. Presumably this map is an isomorphism, but this is unknown at present for $n > 1$. In any case, a formal calculation using Theorem 2 shows that the order of the group on the right is $|w_{n+1}(\mathbb{Q})\zeta(-n)|_p^{-1}$, and so Theorem 6 follows.

3. Iwasawa's construction of the p-adic L-functions

We first introduce the partial zeta functions for an arbitrary finite abelian extension K of $\mathbb{Q}$. By class field theory, $K \subset \mathbb{Q}(\mu_N)$ for some integer N , and we choose N to be minimal with this property. Let G denote the Galois group of K over $\mathbb{Q}$. If c is a rational integer prime to N , we write σ_c for the

restriction to K of the automorphism of $\mathbb{Q}(\mu_N)$ whose action on μ_N is given by $\zeta \mapsto \zeta^c$. For each $\sigma \in G$, we define the partial zeta function of σ by

$$\zeta_K(\sigma,s) = \sum_{\sigma_m=\sigma} m^{-s} \qquad (R(s) > 1) ,$$

where the sum is taken over all positive integers m with $\sigma_m = \sigma$. Now $\zeta_K(\sigma,s)$ has an analytic continuation over the whole complex plane, and it is known that $\zeta_K(\sigma,-n)$ is rational for all $n \geq 0$ in $\mathbb{Z}$. See [2] for a discussion of the integrality properties of these numbers. For $K = \mathbb{Q}(\mu_N)$ and $\sigma = \sigma_c$, we have the explicit formula

$$\zeta_K(\sigma_c,-n) = -\frac{N^n}{n+1} B_{n+1}(\{\frac{c}{N}\}) ;$$

here $B_{n+1}(x)$ denotes the $(n+1)$-th Bernoulli polynomial, and $\{y\}$ denotes the fractional part of a real number y.

Let $\mathbb{Z}[G]$ (respectively, $\mathbb{Q}[G]$) denote the integral (respectively, rational) group ring of G. We now define the analogue of the classical Stickelberger ideal which plays a central role in Mazur and Wiles' work. Let $\beta(K) \in \mathbb{Q}[G]$ be given by

$$\beta(K) = \sum_{\sigma \in G} \zeta_K(\sigma,-1)\sigma .$$

Take S to be an arbitrary finite set of prime numbers which contains all primes dividing both N and the integer $w_2(K)$ (= largest integer m such that $G(K(\mu_m)/K)$ has exponent 2). Then it is not difficult to show that, for each positive integer c prime to S,

$$(\sigma_c^{-1} - c^2)\beta(K) \tag{7}$$

belongs now to the integral group ring $\mathbb{Z}[G]$. For the proof of this and related facts, see [1] and [2]. We then define $\mathcal{S}(K)$ to be the ideal in $\mathbb{Z}[G]$ generated by all elements (7) for c ranging over all positive integers prime to S (in fact, $\mathcal{S}(K)$ does not depend on S). We call $\mathcal{S}(K)$ the Stickelberger ideal (but we stress that $\mathcal{S}(K)$ is only an analogue of the classical Stickelberger ideal), and its paramount importance will be explained later in the exposé.

We now briefly indicate Iwasawa's construction of the power series $L_\chi(T)$ in terms of the Stickelberger ideals. Take $K = F_n = \mathbb{Q}(\mu_{p^{n+1}})$, and write G_n for the Galois group of F_n over $\mathbb{Q}$. We define S_n to be the ideal of the p-adic group ring $\mathbb{Z}_p[G_n]$ generated by all elements (7) with the conditions on c given above. Now we have the canonical decomposition $G_n = \Delta \times \Sigma_n$, where Σ_n is cyclic of order p^n, which allows us to consider each G_n-module as a Δ-module, in particular. Moreover, if r_n denotes the projection of G_n on Σ_n, and $\phi \in \hat{\Delta}$, the map $\sigma \longrightarrow \phi(\sigma) r_n(\sigma)$ from G_n to the group ring

$$R_n = \mathbb{Z}_p[\Sigma_n]$$

induces an isomorphism

$$\mathbb{Z}_p[G_n]^{(\phi)} \xrightarrow{\sim} R_n \tag{8}$$

Lemma 7.— Let $\phi \in \hat{\Delta}$ *be distinct from* ϑ^{-2} *. Then the isomorphism* (8) *maps* $S_n^{(\phi)}$ *to the principal ideal of* R_n *generated by*

$$\beta_n^{(\phi)} = \sum_{\sigma \in G_n} \zeta_{F_n}(\sigma,-1)\phi(\sigma)r_n(\sigma) \ .$$

Indeed, $\beta_n^{(\phi)} \in R_n$ when $\phi \neq \vartheta^{-2}$, because we can choose a positive integer c prime to $w_2(F_n)$ such that $r_n(\sigma_c) = 1$ and σ_c generates Δ. The assertion of the lemma is then clear from the definition of the ideal S_n. Next, let $\omega_n = (1+T)^{p^n} - 1$. We have a unique isomorphism of $\mathbb{Z}_p$-algebras

$$R_n \xrightarrow{\sim} \Lambda/\omega_n\Lambda \tag{9}$$

such that the image of γ_0 in Σ_n is mapped to $1 + T$ mod. $\omega_n\Lambda$. Passing to the projective limit, we obtain an isomorphism $\varprojlim R_n \xrightarrow{\sim} \Lambda$ which maps γ_0 to $1 + T$. Now it follows easily from properties of the partial zeta functions that the $\beta_n^{(\phi)}$ $(n = 0,1,\ldots)$ define an element of $\varprojlim R_n$ when $\phi \neq \vartheta^{-2}$. Write $G_\phi(T)$ for the corresponding power series in Λ. One can evaluate these functions at the points $T = (1+p)^k - 1$ (where k is an integer ≥ 0) using the congruence given in Theorem 10 of [2]. We only state the result. For each $\chi \in \hat{\Delta}$, we define

$$L(\chi,-k) = \sum_{\sigma \in \Delta} \zeta_{F_0}(\sigma,-k)\chi(\sigma)$$

for all integers $k \geq 0$. If $\chi = \vartheta^0$ is the trivial character, we have $L(\vartheta^0,-k) = (1-p^k)\zeta(-k)$.

THEOREM 8 (Iwasawa).— *Let* ϕ *be a character in* $\hat{\Delta}$ *distinct from* ϑ^{-2}. *Then, for each integer* $k \geq 0$, *we have*

$$G_\phi((1+p)^k - 1) = L(\phi\vartheta^{-k}, -k-1) \ .$$

The number $L(\chi,-k)$ is zero if and only if χ and k have opposite parity (since the corresponding result holds for the complex L-functions because of the Γ-factors in their functional equation). In particular, $G_\phi(T)$ is identically zero when ϕ is odd.

COROLLARY 9.— *Let* χ *be an even character in* $\hat{\Delta}$ *distinct from* ϑ^{-1}. *Then the power series* $L_\chi(T)$ *is given by*

$$L_\chi(T) = G_{\chi\vartheta^{-1}}((1+p)^{-1}(1+T) - 1) \ .$$

4. Reduction of the problem

The first reduction of the problem is based on the generalisation of the analytic class number formula (4) to the fields F_n $(n = 0,1,\ldots)$.

PROPOSITION 10.— *In order to prove Theorem* 2, *it suffices to show that, for each odd* $\chi \in \hat{\Delta}$ *distinct from* ϑ^{-1}, $L_\chi(T)$ *divides a characteristic power series of* $X_\infty^{(\chi)}$.

By the Weierstrass preparation theorem, each non-zero f in Λ can be written uniquely in the form $f = p^{\mu}m(T)\upsilon(T)$, where $\mu \geq 0$, $m(T)$ is a distinguished polynomial, and $\upsilon(T)$ is a unit in Λ. Then the degree $\lambda = \lambda(f)$ of $m(T)$ and the integer $\mu = \mu(f)$ are invariants of f. Write $c_\chi(T)$ for a characteristic power series of $X_\infty^{(\chi)}$. As is explained in [9], the generalisation of the analytic class number formula (4) to the fields F_n implies that

$$\sum_\chi \lambda(c_\chi) = \sum_\chi \lambda(L_\chi) \quad , \quad \sum_\chi \mu(c_\chi) = \sum_\chi \mu(L_\chi) \ ,$$

where χ runs over all odd characters in $\hat{\Delta}$ distinct from ϑ^{-1}. Thus Proposition 10 is now clear.

Secondly, the construction of unramified extensions using the Jacobians of modular curves, makes it imperative to replace the G_∞-module A_∞ by its twisted version $A_\infty(1) = A_\infty \otimes_{\mathbb{Z}_p} \mathcal{T}$, endowed as before with the diagonal action of G_∞. Let

$$Z_\infty = \mathrm{Hom}(A_\infty(1), \mathbb{Q}_p/\mathbb{Z}_p) \ .$$

Thus $Z_\infty(1) = X_\infty$.

PROPOSITION 11.— *In order to prove Theorem 2, it suffices to show that, for each even $\phi \in \hat{\Delta}$ distinct from ϑ^{-2}, $G_\phi(T)$ divides a characteristic power series of $Z_\infty^{(\phi)}$.*

Since $Z_\infty(1) = X_\infty$, it is plain that if $d_\phi(T)$ is a characteristic power series for $Z_\infty^{(\phi)}$, then $d_\phi((1+p)^{-1}(1+T) - 1)$ is a characteristic power series for $X_\infty^{(\chi)}$, where $\chi = \phi\vartheta$. Hence Proposition 11 follows from Proposition 10 and corollary 9.

The final reduction of Theorem 2 involves a technical ring-theoretic concept for replacing the characteristic power series of a Λ-module when one works at a finite layer F_n of the tower F_∞. In general, let R be a commutative ring, and M a finitely presented R-module. Take any finite presentation of M, say

$$R^m \xrightarrow{\varepsilon} R^q \longrightarrow M \longrightarrow 0 \ . \tag{10}$$

We define the Fitting ideal $\mathcal{F}_R(M)$ of M to be the ideal of R generated by all $q \times q$ minors of the matrix of ε (if $m < q$, we put $\mathcal{F}_R(M) = 0$). See [14] for the basic properties of $\mathcal{F}_R(M)$. In particular, $\mathcal{F}_R(M)$ does not depend on the choice of the presentation (10). We now use this notion with R given by the $\mathbb{Z}_p$-group ring $R_n = \mathbb{Z}_p[\Sigma_n] \xrightarrow{\sim} \Lambda/\omega_n\Lambda$ under the isomorphism (9); here $\omega_n = (1+T)^{p^n} - 1$. Recall that S_n denotes the ideal in $\mathbb{Z}_p[G_n]$ generated by the elements (7) with c ranging over all positive integers prime to $w_2(F_n)$. For each $\phi \in \hat{\Delta}$, we identify $S_n^{(\phi)}$ with its image in R_n under the isomorphism (8).

Assertion Φ_n.— *For each even character $\phi \neq \vartheta^{-2}$ in $\hat{\Delta}$, we have*

$$\mathfrak{F}_{R_n}(Z_\infty^{(\phi)}/\omega_n Z_\infty^{(\phi)}) \subset S_n^{(\phi)} \ .$$

It is precisely this statement which Mazur and Wiles use the theory of modular curves to prove for all $n \geq 0$. In view of the construction of $G_\phi(T)$ given in § 3, it is not difficult to show that the validity of (Φ_n) for all $n \geq 0$ implies the sufficient condition for Theorem 2 in Proposition 11.

5. The work of Kubert-Lang

We owe to Kubert and Lang [10] the important observation that the Stickelberger ideal defined in § 3 also arises naturally in the study of the cusps on the modular curve $X_1(N)$. In this section, we sketch that part of their work which is used by Mazur and Wiles. Throughout, $\mathcal{H}$ will denote the upper half plane, and $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. Also N will denote an integer ≥ 1 , and $G = (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$.

We recall that $\Gamma_1(N)$ denotes the group

$$\Gamma_1(N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : a \equiv d \equiv 1 \bmod. N \ , \ c \equiv 0 \bmod. N\right\} \ ,$$

which operates in the natural fashion on $\mathcal{H}^*$. Over the complex field $\mathbb{C}$ (see [18], and also the discussion in § 6), we define the modular curve $X_1(N)/\mathbb{C}$ by

$$X_1(N)/\mathbb{C} = \Gamma_1(N)\backslash\mathcal{H}^* \ .$$

We write π_N for the natural projection of $\mathcal{H}^*$ on $X_1(N)/\mathbb{C}$. By definition, the cusps of $X_1(N)/\mathbb{C}$ are the elements of $\pi_N(\mathbb{Q} \cup \{\infty\})$, and it is convenient to describe them by the following notation. On the set V of all pairs of integers (x,y) with $(x,y,N) = 1$, we impose the equivalence relation defined by the three conditions (i) $(x,y) \sim (x',y')$ if $x \equiv x' \bmod. N$, $y \equiv y' \bmod. N$, (ii) $(x,y) \sim (-x,-y)$, and (iii) $(x,y) \sim (x+y,y)$. Denote the equivalence class of (x,y) by $\begin{bmatrix} x \\ y \end{bmatrix}$. Let now x , y be relatively prime integers. Then the map $\pi_N\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{bmatrix} x \\ y \end{bmatrix}$ establishes a bijection between the set of cusps and the set of equivalence classes of elements of V . By definition, the set $\mathcal{Z}_0(N)$ of zero cusps of $X_1(N)/\mathbb{C}$ is the set of all cusps of the form $\begin{bmatrix} x \\ y \end{bmatrix}$, where $(y,N) = 1$ (in fact, each such cusp can plainly be written in the form $\begin{bmatrix} 0 \\ y \end{bmatrix}$, where $(y,N) = 1$).

The group $G = (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$ acts as a group of automorphisms of $X_1(N)/\mathbb{C}$. Given $\sigma \in G$, choose an integer m prime to N such that σ is the image of m in G , and choose m' such that $mm' \equiv 1 \bmod. N$. Let δ_m be an element of $SL_2(\mathbb{Z})$ such that

$$\delta_m \equiv \begin{pmatrix} m' & 0 \\ 0 & m \end{pmatrix} \bmod. N \ .$$

We then define the automorphism $\langle\sigma\rangle$ of $X_1(N)/\mathbb{C}$ by $\langle\sigma\rangle(\pi_N(z)) = \pi_N(\delta_m(z))$. An immediate calculation shows that $\langle\sigma\rangle$ operates on the cusps by

$$\langle\sigma\rangle\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} m' & x \\ m & y \end{bmatrix} \ .$$

In particular, the set of zero cusps $\mathcal{Y}_0(N)$ is given by

$$\mathcal{Y}_0(N) = \left\{ <\sigma> \begin{bmatrix} 0 \\ 1 \end{bmatrix} : \sigma \in G \right\} .$$

As a preliminary step to constructing functions on $X_1(N)/\mathbb{C}$, we recall some classical facts from the theory of elliptic functions. Let L be any lattice in $\mathbb{C}$, and let $\sigma(z,L)$ be the Weierstrass σ-function of L. Write $\zeta(z,L) = \sigma'(z,L)/\sigma(z,L)$, and for $\omega \in L$, define

$$\eta(\omega,L) = \zeta(z+\omega,L) - \zeta(z,L) .$$

We write $\eta(z,L)$ for the extension of $\eta(\omega,L)$ to $\mathbb{C}$ by $\mathbb{R}$-linearity. Let

$$\phi(z,L) = e^{-\frac{1}{2}z\eta(z,L)}\sigma(z,L) .$$

For L fixed, note that $\phi(z,L)$ is not a holomorphic function of z, because $\eta(z,L)$ is not holomorphic in z. We now vary both z and L simultaneously. Let $\alpha = (\alpha_1,\alpha_2)$ be a fixed element in $\mathbb{R}^2\backslash\mathbb{Z}^2$, let τ be a variable in the upper half plane $\mathcal{H}$, and let L_τ be the lattice $\mathbb{Z}\tau \oplus \mathbb{Z}$. The function $\eta^2(\tau)$ (which has nothing to do with $\eta(z,L)$) is defined by

$$\eta^2(\tau) = (2\pi i)q_\tau^{\frac{1}{12}} \prod_{m=1}^{\infty} (1 - q_\tau^m) \quad , \quad q_\tau = e^{2\pi i\tau} .$$

We recall that, if $\mathcal{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, then there is $\rho(\mathcal{M}) \in \mu_{12}$ such that

$$\eta^2(\mathcal{M}\tau) = \rho(\mathcal{M})(c\tau + d)\eta^2(\tau) .$$

We now introduce the function

$$\psi_\alpha(\tau) = \phi(\alpha_1\tau + \alpha_2, L_\tau)\eta^2(\tau) .$$

The following elementary proposition lists the properties of $\psi_\alpha(\tau)$ which will be used in the sequel. Recall that $B_2(x)$ denotes the secont Bernoulli polynomial.

PROPOSITION 12.— (i) *$\psi_\alpha(\tau)$ is a holomorphic non-vanishing function of τ in the upper half plane $\mathcal{H}$, given explicitly by*

$$(11)\ \psi_\alpha(\tau) = q_\tau^{\frac{1}{2}B_2(\alpha_1)} e^{\pi i(\alpha_1-1)\alpha_2}(e^{2\pi i\alpha_2}q_\tau^{\alpha_1} - 1) \prod_{m=1}^{\infty} \left\{ (1 - q_\tau^{m+\alpha_1}e^{2\pi i\alpha_2})(1 - q_\tau^{m-\alpha_1}e^{-2\pi i\alpha_2}) \right\} ;$$

(ii) *For each $\mathcal{M} \in SL_2(\mathbb{Z})$, we have*

$$\psi_\alpha(\mathcal{M}\tau) = \rho(\mathcal{M})\psi_{\alpha\mathcal{M}}(\tau) ;$$

(iii) *If $\beta = (\beta_1,\beta_2) \in \mathbb{Z}^2$, then*

$$\psi_{\alpha+\beta}(\tau) = \psi_\alpha(\tau)e^{\pi i(\alpha_1\beta_2 - \alpha_2\beta_1)}\varepsilon(\beta) ,$$

where $\varepsilon(\beta) = 1$ if $\beta \in 2\mathbb{Z}^2$, and $\varepsilon(\beta) = -1$ otherwise.

COROLLARY 13.— *Let N be an integer > 1, and suppose that $N\alpha \in \mathbb{Z}^2$. Then the order of $\psi_\alpha(\tau)$ as a power series in $q_\tau^{1/N}$ is given by*

$$\frac{N}{2} B_2(\{\alpha_1\}) .$$

We can now construct functions on $X_1(N)/\mathbb{C}$, whose divisors have support amongst the cusps. If $\sigma \in G$, one verifies immediately from (iii) of Proposition 12 that the function $\psi_\sigma(\tau) = \psi_{(0,m/N)}(\tau)\psi_{(0,-(m/N))}(\tau)$ depends only on σ; here m is any integer prime to N whose image in G is σ. In the following, $\mu : G \to \mathbb{Z}$ will denote a function, which will always be assumed to satisfy $\sum_{\sigma\in G} \mu(\sigma) = 0$. We define

$$\vartheta_\mu(\tau) = \prod_{\sigma\in G} \psi_\sigma(\tau)^{\mu(\sigma)} .$$

For $\sigma \in G$, put $\mathcal{N}_2\sigma$ for the residue class of m^2 modulo N, where m is any integer whose image in G is σ.

THEOREM 14.— *$\vartheta_\mu(\tau)$ is a function on $X_1(N)/\mathbb{C}$ if and only if*

$$\sum_{\sigma\in G} \mu(\sigma)\mathcal{N}_2\sigma \equiv 0 \bmod. N . \tag{12}$$

Proof.— This follows immediately from Proposition 12. Indeed (i) shows that, for any μ, $\vartheta_\mu(\tau)$ is meromorphic at the cusps and (ii) and (iii) imply that, for all $\mathcal{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\Gamma_1(N)$, we have

$$\vartheta_\mu(\mathcal{M}\tau) = \vartheta_\mu(\tau)\exp\left(-\frac{2\pi i c}{N}\,\frac{\sum_{\sigma\in G}\mu(\sigma)\mathcal{N}_2(\sigma)}{N}\right) ,$$

whence the theorem is plain.

In view of Theorem 13, we define $\mathcal{P}$ to be the set of all functions $\mu : G \to \mathbb{Z}$ satisfying (12) and $\sum_{\sigma\in G}\mu(\sigma) = 0$. The next result is also an immediate consequence of (ii) and (iii) of Proposition 12.

PROPOSITION 15.— *Assume that $\mu \in \mathcal{P}$. Then, for each $\sigma \in G$,*

$$\vartheta_\mu(<\sigma>\tau) = \vartheta_{\mu_\sigma}(\tau) ,$$

where $\mu_\sigma \in \mathcal{P}$ is defined by $\mu_\sigma(\rho) = \mu(\rho\sigma^{-1})$.

It is easy to derive the expansions of $\vartheta_\mu(\rho)$ at the cusps from (i) of Proposition 12. We only state the result explicitly for the zero cusps. Since $\mathcal{G}_0(N) = \left\{<\sigma>\begin{bmatrix}0\\1\end{bmatrix}, \sigma \in G\right\}$, Proposition 15 shows that it suffices to work with $\begin{bmatrix}0\\1\end{bmatrix}$. Let K denote the maximal real subfield of $\mathbb{Q}(\mu_N)$, so that we can also identify G with the Galois group of K over $\mathbb{Q}$.

PROPOSITION 16.— *Assume that $\mu \in \mathcal{P}$. In terms of the local parameter at $\begin{bmatrix}0\\1\end{bmatrix}$ given by $t = e^{-2\pi i/N\tau}$, $\vartheta_\mu(\tau)$ has an expansion of the form*

$$t^{-\sum_{\sigma\in G}\mu(\sigma)\zeta_K(\sigma,-1)}(1 - 2\mu(1)t + t^2 w_\mu(t)) , \tag{13}$$

where $w_\mu(t)$ is a power series in $\mathbb{Z}[[t]]$.

As far as order of vanishing at the other cusps is concerned, we merely note the following two facts :

$$\operatorname{ord}_{\begin{bmatrix}x\\0\end{bmatrix}} \vartheta_\mu(\tau) = 0 , \tag{14}$$

(15) $$\operatorname{ord}_{\begin{bmatrix} x_1 \\ y \end{bmatrix}} \vartheta_\mu(\tau) = \operatorname{ord}_{\begin{bmatrix} x_2 \\ y \end{bmatrix}} \vartheta_\mu(\tau) \ .$$

However, if $y \not\equiv 0 \bmod N$, it is not in general true that the order in (15) is zero. In other words, the support of the divisor $(\vartheta_\mu(\tau))$ is not in general contained in $\mathcal{Y}_0(N)$.

Let $\Theta(N)$ denote the group of all principal divisors $(\vartheta_\mu(\tau))$ with μ running over $\mathcal{P}$. If D is a divisor on $X_1(N)/\mathbb{C}$, write $\mathrm{pr}_0(D)$ for the part of D whose support lies in $\mathcal{Y}_0(N)$. The following result shows how the Stickelberger ideal $\mathcal{S}(K)$ in $\mathbb{Z}[G]$ defined in § 3 arises in the context of the modular curve $X_1(N)/\mathbb{C}$. Let $\mathbb{Z}[G]^0$ be the ideal of $\mathbb{Z}[G]$ consisting of all elements of degree 0, and put

$$\mathcal{S}(K)^0 = \mathcal{S}(K) \cap \mathbb{Z}[G]^0 \ .$$

THEOREM 17 (Kubert-Lang).— $\mathrm{pr}_0(\Theta(N)) = \mathcal{S}(K)^0 \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

This is an immediate consequence of Proposition 16, and the following elementary lemma.

Lemma 18.— $$\mathcal{S}(K)^0 = \left\{ \beta(K) \sum_{\sigma \in G} \mu(\sigma)\sigma^{-1} \ : \ \mu \in \mathcal{P} \right\} \ .$$

Now let $P(N)$ denote the group of all principal divisors (f), where f is a function on $X_1(N)/\mathbb{C}$, whose zeros and poles lie amongst the cusps, and which satisfies (14) and (15) at the cusps. Since the $\mathbb{Z}$-rank of $\Theta(N)$ is $\#(G) - 1$, it is not in general true that $\Theta(N)$ has finite index in $P(N)$.

THEOREM 19 (Kubert-Lang).— *The torsion subgroup of* $P(N)/\Theta(N)$ *is annihilated by* 2.

The essential step in the proof is to deduce from the expansion (13) that a relation $f^m = \vartheta_\mu(\tau)$, where f is a function on $X_1(N)/\mathbb{C}$ implies that $m/2\mu(1)$. Proposition 15 then shows that $m/2\mu(\sigma)$ for all $\sigma \in G$, and the conclusion of the theorem follows from Theorem 14.

Let $\mathcal{C}_0(N)$ be the group of divisors of degree 0 on $X_1(N)/\mathbb{C}$ with support in $\mathcal{Y}_0(N)$, modulo the subgroup of principal divisors with the same property. The theory of Kubert and Lang described above does not in general give a simple description of $\mathcal{C}_0(N)$ as a $\mathbb{Z}[G]$-module in terms of $\mathcal{S}(K)^0$ alone, because of the fact that $\vartheta_\mu(\tau)$ may have zeros or poles at the intermediate cusps $\begin{bmatrix} x \\ y \end{bmatrix}$ where y and N have a common divisor d with $1 < d < N$. (Note that the finiteness of $\mathcal{C}_0(N)$ is already implied by earlier work of Manin and Drinfeld). At the end of the exposé, we shall say a few words about the beautiful manner in which Mazur and Wiles' work clarifies this problem, at least when $N = p^{n+1}$ with $n \geq 1$. Note that when $N = p \geq 5$, this difficulty does not occur since there are no intermediate cusps, and the following result is a simple consequence of Lemma 7, and Theorems 17 and 19.

THEOREM 20 (Kubert-Lang).— *Let* $p \geq 5$ *and let* $C_0(p)$ *be the* p*-primary subgroup*

of $\mathcal{C}_0(p)$. *Then, for each even* χ *in* $\hat{\Delta}$ *distinct from* ϑ^0 *and* ϑ^{-2} , *we have*

$$C_0(p)^{(\chi)} = \mathbb{Z}_p/L(-1,\chi)\mathbb{Z}_p \ .$$

6. Proof of Assertion Φ_n for $n = 0$.

All the techniques needed to prove Assertion Φ_0 are contained in [22], but the final argument is not given explicitly. We sketch the proof in this section.

Let $J_1(p)/\mathbb{C}$ denote the Jacobian variety of the curve $X_1(p)/\mathbb{C}$. Let ℓ be a prime number different from p , and let δ_ℓ be as defined in § 5. The following correspondences on $X_1(p)/\mathbb{C}$ induce endomorphisms of $J_1(p)/\mathbb{C}$, which we denote by the same symbols :

$$T_\ell(\pi_p(z)) = \sum_{k=0}^{\ell-1} \pi_p\left(\frac{z+k}{\ell}\right) + \pi_p(\delta_\ell(\ell z)) \qquad (\ell \neq p) \ ,$$

$$U_p(\pi_p(z)) = \sum_{k=0}^{p-1} \pi_p\left(\frac{z+k}{p}\right) \ ,$$

$$W(\pi_p(z)) = \pi_p\left(\frac{-1}{pz}\right) \ .$$

Also, for $\sigma \in G$, the automorphism $\langle\sigma\rangle$ of $X_1(p)/\mathbb{C}$ induces an automorphism of $J_1(p)/\mathbb{C}$, which we again denote by $\langle\sigma\rangle$. Put

$$U_p^* = W^{-1}U_pW \ ,$$

and define $\mathbb{T}$ to be the algebra of endomorphisms of $J_1(p)/\mathbb{C}$ generated by the T_ℓ for all primes $\ell \neq p$, U_p^* , and $\langle\sigma\rangle$ for all $\sigma \in G$. It is well known that $\mathbb{T}$ is commutative, and is a free finitely generated $\mathbb{Z}$-module.

In fact, the curve $X_1(p)/\mathbb{C}$ has a canonical model which is defined over $\mathbb{Q}$ (see [18], Chapter 6), and which we denote by $X_1(p)/\mathbb{Q}$. The elements of $\mathcal{H}_0(p)$ are $\mathbb{Q}$-rational points for this model. Moreover, writing $J_1(p)/\mathbb{Q}$ for the Jacobian variety of $X_1(p)/\mathbb{Q}$, the endomorphisms in $\mathbb{T}$ are all defined over $\mathbb{Q}$. The involution W is not defined over $\mathbb{Q}$, but only over the maximal real subfield F_0^+ of $F_0 = \mathbb{Q}(\mu_p)$. Write $\mathcal{H}_\infty(p)$ for the set of cusps of $X_1(p)/\mathbb{C}$ of the form $\begin{bmatrix} x \\ 0 \end{bmatrix}$, where x is an integer prime to p (we call these the ∞-cusps). Since $W(\mathcal{H}_0(p)) = \mathcal{H}_\infty(p)$, it follows that the ∞-cusps are defined over F_0^+ . Moreover, identifying G with the Galois group of F_0^+ over $\mathbb{Q}$, the Galois action of G on $\mathcal{H}_\infty(p)$ is easily seen to be the same as the diamond action. Let $\mathcal{C}_\infty(p)$ denote the group of divisors of degree zero on $X_1(p)/\mathbb{C}$ with support in $\mathcal{H}_\infty(p)$, modulo the subgroup of principal divisors with the same property. As $W \circ \langle\sigma\rangle = \langle\sigma\rangle^{-1} \circ W$ and $W(\mathcal{C}_0(p)) = \mathcal{C}_\infty(p)$ the theory of Kubert-Lang gives the structure of the finite group $\mathcal{C}_\infty(p) \subset J_1(p)(F_0^+)$ as a $\mathbb{Z}[G]$-module (neglecting the 2-primary part). Finally, the explicit formulae given above shows easily that

$$\mathbb{T}(\mathcal{C}_\infty(p)) \subset \mathcal{C}_\infty(p) \ .$$

Write $J_1(p)[p^\infty]$ for the group of p-power order in $J_1(p)(\overline{\mathbb{Q}})$. Let G_p denote the Galois group of the maximal extension of $\mathbb{Q}$ which is unramified outside p. As $J_1(p)/\mathbb{Q}$ is known to have good reduction at all primes different from p, the Galois module $J_1(p)[p^\infty]$ is unramified outside p, i.e. it is a G_p-module. For each prime $\ell \neq p$, let $\varphi_\ell \in G_p$ denote a Frobenius element for ℓ. Also we write σ_ℓ for the image of ℓ in $G = (\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$. The following is a reformulation of a classical result of Eichler and Shimura (see [18], Chapter 7).

PROPOSITION 21.— *On* $J_1(p)[p^\infty]$, *we have*

$$T_\ell = \varphi_\ell + \ell \langle \sigma_\ell \rangle \varphi_\ell^{-1} .$$

For the rest of this section, fix an even character χ in $\hat{\Delta}$ with $\chi \neq 1$, $\mathfrak{S}^2$ such that p divides $L(-1,\chi^{-1})$. Write C_∞ for the χ-component of the p-primary subgroup of $\mathcal{C}_\infty(p)$. By Theorem 20, we have that as an abelian group

$$C_\infty = \mathbb{Z}_p/L(-1,\chi^{-1})\mathbb{Z}_p . \tag{16}$$

Also $\mathbb{T}(C_\infty) \subset C_\infty$.

CRUCIAL DEFINITION.— *We let* I *be the annihilator of* C_∞ *in* $\mathbb{T}$.

We also write $\mathfrak{m} = (\mathrm{I},p)$ for the associated maximal ideal in $\mathbb{T}$. For each integer r with $0 \leq r \leq \infty$, put $J_1(p)[\mathfrak{m}^r]$ for the set of points in $J_1(p)(\overline{\mathbb{Q}})$ which are annihilated by all endomorphisms α in the ideal $\mathfrak{m}^r$.

It is essential to work with a quotient of the abelian variety $J_1(p)/\mathbb{Q}$. Let $X_0(p)/\mathbb{C}$ be the modular curve $\Gamma_0(p)\backslash\mathfrak{H}^*$, where $\Gamma_0(p)$ is the subgroup of $SL_2(\mathbb{Z})$ consisting of all matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ad - bc = 1$ and $c \equiv 0 \bmod p$. Again this curve admits a canonical model $X_0(p)/\mathbb{Q}$ such that the natural map $X_1(p)/\mathbb{Q} \longrightarrow X_0(p)/\mathbb{Q}$ is also defined over $\mathbb{Q}$. Thus, writing $J_0(p)/\mathbb{Q}$ for the Jacobian of $X_0(p)/\mathbb{Q}$, we can define the abelian variety $A/\mathbb{Q}$ by the exactness of the sequence

$$0 \longrightarrow J_0(p)/\mathbb{Q} \longrightarrow J_1(p)/\mathbb{Q} \longrightarrow A/\mathbb{Q} \longrightarrow 0 . \tag{17}$$

The main reason for introducing $A/\mathbb{Q}$ is the following result [3].

THEOREM 22 (Deligne-Rapoport).— *The abelian variety* A/F_0^+ *has good reduction everywhere* (i.e. *including at the unique prime of* F_0^+ *above* p).

The Hecke algebra $\mathbb{T}$ also operates on $A/\mathbb{Q}$. Write $A[\mathfrak{m}^r]$ for the G_p-module of points in $A(\overline{\mathbb{Q}})$ which are annihilated by all elements of $\mathfrak{m}^r$. The exact sequence (17) induces a G_p-isomorphism $J_1(p)[\mathfrak{m}^r] \xrightarrow{\sim} A[\mathfrak{m}^r]$ because $\chi \neq 1$.

We say that a G_p-module N is of μ_p-type if every finite submodule of N has Jordan-Holder filtration whose successive quotients are all isomorphic to the G_p-module μ_p. We omit the proof of the following proposition (see [13], [22]).

PROPOSITION 23.— *Let* Ω *denote the maximal* μ_p*-type submodule of* $A[\mathfrak{M}^\circ]$. *Then* Ω *is finite.*

We now define $B/\mathbb{Q}$ to be the quotient of the abelian variety $A/\mathbb{Q}$ by Ω . Since B/F_0^+ is isogenous to A/F_0^+ , it follows that B/F_0^+ has good reduction everywhere. We can now construct the exact sequence of G_p-modules whose study leads to the proof of Assertion Φ_0 . The canonical surjection of $J_1(p)/\mathbb{Q}$ onto $B/\mathbb{Q}$ induces an isomorphism from C_∞ onto its image in $B(\overline{\mathbb{Q}})$ (which we again denote by C_∞), because $\chi \neq \mathfrak{I}^\circ$. Now $B/\mathbb{Q}$ inherits an action of $\mathbb{T}$, and we write $B[\Pi]$ for the points in $B(\overline{\mathbb{Q}})$ which are annihilated by all elements of Π . Clearly $C_\infty \subset B[\Pi]$, and we define the G_p-module M by the exactness of the sequence

$$0 \longrightarrow C_\infty \longrightarrow B[\Pi] \longrightarrow M \longrightarrow 0 \ . \tag{18}$$

Let W_χ denote the $\mathbb{F}_p$-vector space of dimension 1 on which G_p acts via χ .

PROPOSITION 24.— *Each simple sub-quotient of the* G_p*-module* M *is isomorphic either to* μ_p *or to* W_χ .

Proof.— An easy direct calculation shows that, for each α in $\mathcal{Y}_\infty(p)$ and each prime $\ell \neq p$, $T_\ell(\alpha) = (\ell + \langle \sigma_\ell \rangle)(\alpha)$, where σ_ℓ is the image of ℓ in G . Since Π annihilates M , we conclude from this fact and the Eichler-Shimura relation given in Proposition 21 that

$$(\varphi_\ell - \ell)(\varphi_\ell - \chi(\varphi_\ell))M = 0 \tag{19}$$

for all primes $\ell \neq p$. In particular, (19) must hold on each simple subquotient of M , and Proposition 24 is then a consequence of the Brauer-Nesbitt theorem and the Cebotarev density theorem (see [22]).

To study (18) further, we must use the detailed knowledge provided by algebraic geometry of the reduction of B/F_0^+ at the unique prime $\mathfrak{P}$ of F_0^+ above p . Write $\mathfrak{F}$ for the completion of F_0^+ at $\mathfrak{P}$, $\mathfrak{O}$ for the ring of integers of $\mathfrak{F}$, and $k_\mathfrak{P}$ for the residue field of $\mathfrak{P}$. We recall that the reduction of B at $\mathfrak{P}$ is an abelian variety $B_\mathfrak{P}/k_\mathfrak{P}$ which is defined as follows. Let $B/\mathfrak{O}$ denote the Néron minimal model of $B/\mathfrak{F}$. Then $B_\mathfrak{P}/k_\mathfrak{P}$ is the special fibre of $B/\mathfrak{O}$, i.e. $B_\mathfrak{P}/k_\mathfrak{P} = (B/\mathfrak{O}) \otimes_\mathfrak{O} k_\mathfrak{P}$. By the universal property of the Néron model, $\mathbb{T}$ operates on $B/\mathfrak{O}$ and so also on the special fibre $B_\mathfrak{P}/k_\mathfrak{P}$. We define $B_\mathfrak{P}[\Pi]$ to be the subgroup of $B_\mathfrak{P}(\overline{k_\mathfrak{P}})$ which is annihilated by all elements in Π . Recalling that C_∞ is defined over $\mathfrak{F}^{ur}$, we can identify C_∞ with a subgroup of the $\mathfrak{O}$-points of $B/\mathfrak{O}$ (as $B/\mathfrak{O}$ is the Néron model, the canonical map from the $\mathfrak{O}$-points of $B/\mathfrak{O}$ to the $\mathfrak{F}$-points of $B/\mathfrak{F}$ is an isomorphism), and we write $C_{\infty,\mathfrak{P}}$ for the image of C_∞ under the reduction map from the $\mathfrak{O}$-points of $B/\mathfrak{O}$ to the $k_\mathfrak{P}$-points of $B_\mathfrak{P}/k_\mathfrak{P}$. Plainly $C_{\infty,\mathfrak{P}} \subset B_\mathfrak{P}[\Pi]$. The following is a key result.

THEOREM 25.– (i) $C_{\infty,\mathfrak{P}} \xrightarrow{\sim} \mathbb{Z}_p/L(-1,\chi^{-1})\mathbb{Z}_p$; (ii) $C_{\infty,\mathfrak{P}} = B_{\mathfrak{P}}[\Pi]$.

Assertion (i) can be proven using analogues in characteristic p of the arguments of § 5 (alternatively, as the ramification index of $\mathfrak{F}'$ over $\mathbb{Q}_p$ is $< p-1$, one can invoke the specialisation lemma of Raynaud, namely Proposition 1.1 on [12], p. 135). For the proof of (ii), which depends on a detailed knowledge of the geometry of $B_{\mathfrak{P}}/k_{\mathfrak{P}}$, see [22].

PROPOSITION 26.– (i) *As modules for the local Galois group* $G(\overline{\mathfrak{F}}/\mathfrak{F})$, *we have* $B[\Pi] \xrightarrow{\sim} C_\infty \oplus M$; (ii) *As a module for the global Galois group* G_p , M *is of* μ_p*-type.*

Proof.– See [20], p. 160 for an explanation of the terminology and facts about commutative flat group schemes of finite order over $\mathfrak{O}$ used in this proof. The fact that $B/\mathfrak{O}$ has good reduction implies that the exact sequence (18) of $G(\overline{\mathfrak{F}}/\mathfrak{F})$-modules extends to an exact sequence of commutative flat group schemes of finite order

$$0 \longrightarrow C_\infty/\mathfrak{O} \longrightarrow B[\Pi]/\mathfrak{O} \longrightarrow M/\mathfrak{O} \longrightarrow 0 \tag{20}$$

(the exact sequence of general fibres of (20) is just (18) viewed as $G(\overline{\mathfrak{F}}/\mathfrak{F})$-modules). Moreover, we can identify the $\overline{k_{\mathfrak{P}}}$-points of the special fiber of $C_\infty/\mathfrak{O}$ with $C_{\infty,\mathfrak{P}}$, and the $\overline{k_{\mathfrak{P}}}$-points of the special fiber of $B[\Pi]/\mathfrak{O}$ with $B_{\mathfrak{P}}[\Pi]$. It follows from (i) of Theorem 25 that $C_\infty/\mathfrak{O}$ is étale, and from (ii) of Theorem 25 that $M/\mathfrak{O}$ is connected. If we now compare (20) with the standard exact sequence expressing $B[\Pi]/\mathfrak{O}$ as an extension of an étale group by a connected group, we conclude that (20) splits to give

$$(C_\infty/\mathfrak{O}) \oplus (M/\mathfrak{O}) \xrightarrow{\sim} B[\Pi]/\mathfrak{O}.$$

Assertion (i) of Proposition 26 is simply the statement that this decomposition is valid for the general fibres. As $M/\mathfrak{O}$ is connected, no non-zero subquotient of $M/\mathfrak{O}$ is étale. If M were not of μ_p-type, Proposition 24 and the specialisation lemma of Raynaud ([12], p. 135) imply that the constant group of order p over $\mathfrak{O}$ is a subquotient of $M/\mathfrak{O}$, and so (ii) also follows.

Lemma 27.– *The action of* G_p *on* M *is given by the cyclotomic character* ψ , i.e. $\sigma(m) = \psi(\sigma)m$ *for all* $m \in M$ *and* $\sigma \in G_p$.

Proof.– Let K be a finite extension of $\mathbb{Q}$ containing $\mathbb{Q}(\mu_p)$, and such that the action of G_p on M factors through $\mathcal{G} = G(K/\mathbb{Q})$. Let H be the kernel of the character $\chi\vartheta^{-1}$ of $\mathcal{G}$. Since χ is even, $H \neq \mathcal{G}$. Take a prime number $\ell \neq p$ such that the Frobenius element φ_ℓ of ℓ in $\mathcal{G}$ does not lie in H . We claim that the kernel of the endomorphism $\varphi_\ell - \chi(\varphi_\ell)$ must be zero on M . If this were not the case, the fact that M is of μ_p-type would imply that there exists a subquotient of this kernel which is isomorphic to μ_p , and this is impossible

because $\chi(\varphi_\ell) \not\equiv \vartheta(\varphi_\ell)$ by our choice of ℓ. Hence $\varphi_\ell - \chi(\varphi_\ell)$ is an automorphism of M and thus by (19) $(\varphi_\ell - \ell)M = 0$, for all such ℓ. The assertion of the lemma now follows from the Cebotarev density theorem and the fact that $\mathfrak{G}$ is plainly generated by $\mathfrak{G}\backslash H$.

If L is an abelian extension of $F_n = \mathbb{Q}(\mu_{p^{n+1}})$, which is Galois over $\mathbb{Q}$, we recall that there is a standard action of $G(F_n/\mathbb{Q})$ on $G(L/F_n)$ given by $\sigma \circ x = h_\sigma x h_\sigma^{-1}$; here $x \in G(L/F_n)$, $\sigma \in G(F_n/\mathbb{Q})$, and h_σ is any representative of σ in $G(L/\mathbb{Q})$. Define the integer $\rho \geq 0$ by

$$p^{\rho+1} = |L(-1,\chi^{-1})|_p^{-1} . \tag{21}$$

THEOREM 28.— *Let $\mathcal{L}$ be the splitting field over F_ρ of the module $B[\Pi]$ (i.e. the field obtained by adjoining to F_ρ the coordinates of all points in $B[\Pi]$). Then $\mathcal{L}/F_\rho$ is an unramified abelian p-extension, whose degree is the order of M. Moreover, $\mathcal{L}$ is Galois over $\mathbb{Q}$, and the action of $G(F_\rho/\mathbb{Q}) \xrightarrow{\sim} \Delta \times G(F_\rho/F_0)$ is given by (i) Δ acts via $\chi\vartheta^{-1}$, and (ii) $G(F_\rho/F_0)$ acts via the character K^{-1} modulo $p^{\rho+1}$.*

Proof.— The extension $\mathcal{L}/F_\rho$ is automatically unramified outside p, and (i) of Proposition 26 shows that it is also unramified at p. We construct a pairing $G(\mathcal{L}/F_\rho) \times M \longrightarrow C_\infty$ by $(\sigma,m) \longmapsto \sigma w - w$, where w is any representative of m in $B[\Pi]$. It is clear that this pairing is well defined and that the kernel on the left is zero. The kernel on the right is also zero because of the definition of the abelian variety $B/\mathbb{Q}$ as the quotient of $A/\mathbb{Q}$ by the maximal μ_p-type submodule of $A[\mathfrak{M}^\infty]$. Hence, as C_∞ is a cyclic abelian group, we obtain an isomorphism of $G(F_\rho/\mathbb{Q})$-modules

$$G(\mathcal{L}/F_\rho) \xrightarrow{\sim} \mathrm{Hom}(M,C_\infty) .$$

The final assertion of the theorem now follows from Lemma 27.

So far, we have proven nothing about the degree of $\mathcal{L}$ over F_ρ or equivalently the order of M. Indeed, up until now, we have not excluded the possibility that $M = 0$. The key to overcoming this difficulty was pointed out by Tate. Let R be an arbitrary commutative ring containing $\mathbb{Z}_p$ as a subring.

Lemma 29.— Let V be a faithful R-module, which is a free $\mathbb{Z}_p$-module of finite type. Let I be an ideal of R such that V/IV is finite of order p^m. Then $p^m \in I$.

Proof.— By the elementary divisor theorem, we can choose a basis $\{e_k : 1 \leq k \leq r\}$ of V as a $\mathbb{Z}_p$-module such that $IV = \bigoplus_{i=1}^{r} p^{h_i} e_i \mathbb{Z}_p$. Thus $h_1 + \ldots + h_r = m$. But $p^{h_i} e_i \in IV$, and so $p^{h_i} e_i = \sum_{k=1}^{r} x_{i,k} e_k$, with $x_{i,k} \in I$. It follows that $\det(x_{ik} - p^{h_i}\delta_{ik})V = 0$. Since V is faithful, we conclude that $\det(x_{ik} - p^{i}\delta_{ik}) = 0$, whence $p^m \in I$.

To apply this lemma, we take $R = \mathbb{T}_{\mathfrak{m}} = \varprojlim \mathbb{T}/\mathfrak{m}^n\mathbb{T}$, and $I = \mathbb{I}_{\mathfrak{m}} = \mathbb{I}\,\mathbb{T}_{\mathfrak{m}}$. Before defining V , we recall that, if D is a p-primary abelian group, then

$$T_p(D) = \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, D) \quad , \quad \hat{D} = \mathrm{Hom}(D, \mathbb{Q}_p/\mathbb{Z}_p) \ .$$

Moreover, there is a natural identification $T_p(D) = \mathrm{Hom}_{\mathbb{Z}_p}(\hat{D}, \mathbb{Z}_p)$. If $\hat{D}$ is a free $\mathbb{Z}_p$-module of finite rank, it follows that $\hat{D} = \mathrm{Hom}_{\mathbb{Z}_p}(T_p(D), \mathbb{Z}_p)$. Since $B/\mathcal{O}$ has good reduction, the $G(\bar{\mathcal{F}}/\mathcal{F})$-module $B[\mathfrak{m}^r]$ extends to a finite flat commutative group scheme $B[\mathfrak{m}^r]/\mathcal{O}$. Write B_r^0 for the $G(\bar{\mathcal{F}}/\mathcal{F})$-module of $\bar{\mathcal{F}}$-points of the general fibre of the connected subgroup scheme $B[\mathfrak{m}^r]^0/\mathcal{O}$ ([20], p. 160). Put $B_\infty^0 = \bigcup_{r \geq 1} B_r^0$, and take

$$V = \widehat{B_\infty^0} = \mathrm{Hom}(B_\infty^0, \mathbb{Q}_p/\mathbb{Z}_p) \ .$$

Thus V is a free $\mathbb{Z}_p$-module of finite rank, and we endow V with the $\mathbb{T}_{\mathfrak{m}}$-structure given by $(tf)(b) = f(tb)$ for $t \in \mathbb{T}_{\mathfrak{m}}$, $f \in V$, $b \in B_\infty^0$.

THEOREM 30.— *V is a faithful $\mathbb{T}_{\mathfrak{m}}$-module such that $V/\mathbb{I}_{\mathfrak{m}}V$ has the same order as M . Hence the order of M is at least $p^{\rho+1}$.*

The final assertion of Theorem 30 follows from the first assertion and Lemma 29, since it is clear that $p^{\rho+1}$ is the smallest power of p contained in $\mathbb{I}_{\mathfrak{m}}$. Also $V/\mathbb{I}_{\mathfrak{m}}V$ is dual to

$$B_\infty^0[\mathbb{I}_{\mathfrak{m}}] = B[\mathbb{I}]^0 = M \ .$$

Thus it only remains to show that V is a faithful $\mathbb{T}_{\mathfrak{m}}$-module. As V is a free $\mathbb{Z}_p$-module, it suffices to prove that

$$T_p(B_\infty^0) = \mathrm{Hom}_{\mathbb{Z}_p}(V, \mathbb{Z}_p)$$

is a faithful $\mathbb{T}_{\mathfrak{m}}$-module. Let A_∞^0 be the analogous local Galois module for the abelian variety $A/\mathbb{Q}$. Since $T_p(A_\infty^0) \subset T_p(B_\infty^0)$ and the canonical map $\mathbb{T}_{\mathfrak{m}} \longrightarrow \mathbb{T}_{\mathfrak{m}} \otimes_{\mathbb{Z}} \mathbb{Q}$ is injective, the proof of Theorem 30 will be complete once the following result has been established.

PROPOSITION 31.— *$T_p(A_\infty^0) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a free $\mathbb{T}_{\mathfrak{m}} \otimes_{\mathbb{Z}} \mathbb{Q}$ module of rank 1 .*

The four ingredients used in the proof of this result are : (i) $\mathbb{T}_{\mathfrak{m}} \otimes_{\mathbb{Z}} \mathbb{Q}$ is a product of fields ; (ii) $T_p(A_\infty) \otimes \mathbb{Q}$ is free of rank 2 over $\mathbb{T}_{\mathfrak{m}} \otimes_{\mathbb{Z}} \mathbb{Q}$; (iii) the p-divisible group over $\mathcal{O}$ attached to $A[\mathfrak{m}^\infty]$ is an extension of an étale group by one of multiplicative type ; (iv) a lemma of Serre asserting that neither non-trivial étale p-divisible groups nor their duals can occur as subquotients of the p-divisible group attached to an abelian variety defined over a number field K , which has good reduction at the primes of K above p .

To complete this section, we note that Assertion Φ_0 for the character $\phi = \chi^{-1}$ is equivalent to the existence of an extension $\mathcal{L}/F_\rho$ satisfying the conditions given in Theorem 28 with the degree of $\mathcal{L}/F_\rho$ at least $p^{\rho+1}$. This follows easily on recalling that the map $A_\rho^- \longrightarrow A_\infty^-$ is injective, and that the global Artin map gives a $G(F_\rho/\mathbb{Q})$-isomorphism from A_ρ to $G(L_\rho/F_\rho)$, where L_ρ

is the maximal unramified abelian p-extension of F_ρ .

7. Remarks on the proof of Assertion Φ_n for $n > 0$

This is essentially the content of [13], and the proof is long and diffucult. The definition of the correct analogue of the abelian variety $A = J_1(p)/J_0(p)$ for $n > 0$ is by induction on n . Put $\mathcal{A}_0 = A$, and suppose that the abelian variety $\mathcal{A}_{n-1}$ has already been defined as a quotient $\xi_{n-1} : J_1(p^n) \twoheadrightarrow \mathcal{A}_{n-1}$ of $J_1(p^n)$. Let $\Gamma(p^{n+1},p^n)$ be the group consisting of all matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL_2(\mathbb{Z})$, with $c \equiv 0$ mod. p^{n+1} and $a \equiv d \equiv 1$ mod. p^n . The modular curve $X(p^{n+1},p^n)$ associated to $\Gamma(p^{n+1},p^n)$ can also be defined over $\mathbb{Q}$, and we have the canonical maps

$$X_1(p^{n+1}) \xrightarrow{\lambda_n} X(p^{n+1},p^n) \xrightarrow{\eta_n} X_1(p^n) .$$

The inverse image and norm map on divisor classes of degree 0 give rise to respective homomorphisms

$$\lambda_n^* : J(p^{n+1},p^n) \longrightarrow J_1(p^{n+1}) , \quad \eta_{n*} : J(p^{n+1},p^n) \longrightarrow J_1(p^n) ,$$

where $J(p^{n+1},p^n)$ denotes the Jacobian of $X(p^{n+1},p^n)$. Let $\mathcal{B}_n$ be the subvariety of $J(p^{n+1},p^n)$ given by the kernel of $\xi_{n-1} \circ \eta_{n*}$. Mazur and Wiles then define the abelian variety $\mathcal{A}_n$ over $\mathbb{Q}$ by the exactness of

$$0 \longrightarrow \lambda_n^*(\mathcal{B}_n) \longrightarrow J_1(p^{n+1}) \xrightarrow{\xi_n} \mathcal{A}_n \longrightarrow 0 .$$

THEOREM 32 (Langlands [23]). *The abelian variety $\mathcal{A}_n$ has good reduction everywhere over the maximal real subfield of F_n .*

Let $\mathcal{C}_0(p^{n+1})$ be the image in $J_1(p^{n+1})$ of the group of divisors of degree 0 on $X_1(p^{n+1})$ with support in the set of zero cusps, and let $C_n = \xi_n(U_p^n \mathcal{C}_0(p^{n+1}))$ be the image of this group on the abelian variety $\mathcal{A}_n$. Write $C_n(p)$ for the p-primary subgroup of C_n . Via the diamond operators, we regard $C_n(p)$ as a module over the $\mathbb{Z}_p$-group ring of $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times/\{\pm 1\}$. By a remarkable combination of the geometry of the reduction of $\mathcal{A}_n$ at the unique prime above p in F_n^+ , and the ideas of Kubert and Lang, Mazur and Wiles [13] establish the following result.

THEOREM 33.– *Let ϕ be an even character in $\hat{\Delta}$ distinct from ϑ^0 and ϑ^{-2} . Then, in the notation of § 3, we have an isomorphism of R_n-modules*

$$C_n(p)^{(\phi)} \xrightarrow{\sim} R_n/S_n^{(\phi)} .$$

Roughly speaking, once these two deep theorems have been established, the proof of Φ_n for $n > 0$ follows fairly closely the proof of Φ_0 . Certain additional complications occur at the end of the proof because $C_n^{(p)}$ is no longer a cyclic group. Also it is of vital importance to prove the analogue of (ii) of Theorem 25 when $n > 0$.

8. Final remark

Let F be a totally real finite extension of $\mathbb{Q}$, and $\zeta(F,s)$ the complex zeta function of F. Siegel and Shintani have given proofs that the numbers $\zeta(F,-k)$ ($k > 0$ and odd) are rational, and Serre, Deligne-Ribet, and Pierrette Casson-Noguès have established the existence of analogues of the interpolation power series $L_\chi(T)$ for these numbers, where χ is now an odd character of $G(F(\mu_p)/F)$. It is natural to conjecture that Theorem 2 holds in this more general situation, where A_∞ is now the p-primary subgroup of the ideal class group of $F(\mu_{p^\infty})$. It seems that the methods of Mazur and Wiles generalize to prove this conjecture when F is a totally real *abelian* extension of $\mathbb{Q}$. However, the problem for arbitrary totally real F seems as inaccessible as ever. Nothing is known beyond some weak information given by the analytic class number formula (see [1]).

REFERENCES

[1] COATES, J., p-*adic* L-*functions and Iwasawa's theory*, in Algebraic Number Fields (ed. A. Fröhlich), Academic Press, (1977), 269-353.

[2] COATES, J., SINNOTT, W., *Integrality properties of the values of partial zeta functions*, Proc. London Math. Soc. 34(1977), 365-384.

[3] DELIGNE, P., RAPOPORT, M., *Schémas de modules de courbes elliptiques*, in Springer L. N., 349(1973).

[4] DWYER, W., FRIEDLANDER, E., *Etale K-theory and arithmetic*, (to appear).

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

[6] IWASAWA, K., *Some modules in the theory of cyclotomic fields*, J. Math. Soc. Japan 16(1964), 42-82.

[7] IWASAWA, K., *On* p-*adic* L-*functions*, Ann. of Math. 89(1969), 198-205.

[8] IWASAWA, K., *On* $\mathbb{Z}_\ell$-*extensions of algebraic number fields*, Ann. of Math. 98(1973), 246-326.

[9] IWASAWA, K., Lectures on p-adic L-functions, Ann. Math. Studies 74, Princeton (1972).

[10] KUBERT, D., LANG, S., *The index of Stickelberger ideals of order* 2 *and cuspidal class numbers*, Math. Ann. 237(1978), 213-232.

[11] KUBOTA, T., LEOPOLDT, H., *Eine* p-*adische Theorie der zetawerte*, Crelle 213(1964), 328-339.

[12] MAZUR, B., *Rational isogenies of prime degree*, Inventiones Math. 44(1978), 129-162.

[13] MAZUR, B., WILES, A., *Class fields of abelian extensions of* $\mathbb{Q}$, (to appear).

[14] NORTHCOTT, D., Finite Free Resolutions, Cambridge Tracts 71, Cambridge, 1976.

[15] RIBET, K., *A modular construction of unramified* p-*extensions of* $\mathbb{Q}(\mu_p)$, Inventiones Math. 34(1976), 151-162.

[16] SERRE, J.-P., *Classes des corps cyclotomiques*, Séminaire Bourbaki, exp. 174, (1958/59).

[17] SERRE, J.-P., *Formes modulaires et fonctions zêta* p-*adiques*, in Springer L. N. 350(1973).

[18] SHIMURA, G., Introduction to the arithmetic theory of automorphic functions, Publ. Math. Soc. Japan 11, Iwanami Shoten and Princeton (1971).

[19] SOULÉ, C., K-*théorie des anneaux d'entiers de corps de nombres et cohomologie étale*, Inventiones Math. 55(1979), 251-295.

[20] TATE, J., p-*divisible groups*, in Proceedings of a Conference on Local Fields, Springer (1967), 158-183.

[21] WAGSTAFF, S., *The irregular primes to* 125000 , Math. Comp. 32(1978), 583-591.

[22] WILES, A., *Modular curves and the class group of* $\mathbb{Q}(\zeta_p)$, Inventiones Math. 58(1980), 1-35.

[23] LANGLANDS, R., *Modular forms and* ℓ*-adic representations*, in Springer L. N. 349(1973).

John COATES

Université de Paris XI
Département de Mathématiques
Bâtiment 425
F-91405 ORSAY