SUB | NIEDERSÄCHSISCHE STAATS- UND UNIVERSITÄTSBIBLIOTHEK GÖTTINGEN

Werk

Titel: Inventiones Mathematicae
Verlag: Springer
Jahr: 1984
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN356556735_0076
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN356556735_0076

LOG Id: LOG_0020
LOG Titel: Class fields of abelian extensions of Q.
LOG Typ: article

Übergeordnetes Werk

Werk Id: PPN356556735
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN356556735
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=356556735

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.
Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.
Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Invent. math. 76, 179–330 (1984)

Inventiones mathematicae

© Springer-Verlag 1984

Class fields of abelian extensions of Q

To K. Iwasawa

B. Mazur and A. Wiles

Department of Mathematics, Harvard University, Cambridge, MA 02138, USA

Table of contents

Introduction

§ 1. General discussion

Let p be an odd prime number. The object of this paper is to show that the zeroes of the p-adic L-functions of Kubota-Leopoldt are equal to the eigenvalues of certain "arithmetically-defined" operators acting on finite-dimensional $\mathbf{Q}_p$-vector spaces. These $\mathbf{Q}_p$-vector spaces were defined by Iwasawa in terms of limits of certain components of the ideal class groups of towers of cyclotomic number fields. The connection between Iwasawa's vector spaces and the p-adic L-function was conjectured by him (the "main conjecture" for the prime p over the field $\mathbf{Q}$, cf. Chap. 1, § 1).

As the reader will see, if we take into account what is already known, – and much is known, thanks to the work of Kummer, Stickelberger, Iwasawa, Ferrero-Washington, – our problem can be reduced to the construction of enough classfields of abelian extensions of $\mathbf{Q}$, while keeping close tabs on the action of Galois on the classfields. Broadly speaking, the problem we face comes under the rubric of explicit classfield theory (for abelian extensions of $\mathbf{Q}$).

But a wrong impression might arise from the label "explicit classfield theory". First, we may ask in what sense is our construction explicit? We obtain our

classfields as splitting fields of certain finite subgroups of specific quotients of the jacobians of modular curves. By virtue of what we understand about these finite subgroups, we manage to show that our classfields are 'large enough', and that the Galois action is as predicted by the main conjecture. Beyond that, we have little explicit control. For example, our method sheds no light on whether Iwasawa's arithmetically-defined operators are semi-simple; a nontrivial question in the event of a multiple zero of some Kubota-Leopoldt p-adic L-function (of which no example is known).

Second, in what sense is it really classfield theory? We do not construct abelian extensions of a *given* abelian number field F, directly. Rather, we construct a "Tate-twisted" ideal class group of F^+, the maximal totally real subfield of F. This we could state less precisely by saying that we produce abelian everywhere unramified extensions of cyclotomic extensions of F, which are in the *minus part*, in the sense that the natural action of complex conjugation on their Galois group is by multiplication by -1.

To analyse $A(F)^-$, the p-primary component of the minus part of the ideal class group of F, we use Iwasawa theory. We pass to the field extension F_∞ of F generated by all p-power roots of unity; the "Tate-twisted" ideal class groups we construct at finite layers, when brought to this field, are untwisted. We then descend. In a simple case like $F = \mathbf{Q}(e^{2\pi i/p})$ we can recover $A(F)^-$ as the Galois invariants of $A(F_\infty)^-$. In general, the situation is more complicated. But if the degree of F over $\mathbf{Q}$ is prime to p, and if χ is an odd character of $\mathrm{Gal}(F/\mathbf{Q})$, we use the "main conjecture" and some key ideas of Greenberg to prove a formula for the order of the χ-part, $A(F)^\chi$. Specifically, this order is the maximal power of p dividing $\mathbf{B}_1(\chi^{-1})^g$, where $\mathbf{B}_k(\chi^{-1})$ denotes the k-th generalized Bernoulli number and g is the degree over $\mathbf{Q}_p$ of the field extension generated by the values of χ (cf. Chap. 1, §10). This formula was originally conjectured by Iwasawa and Leopoldt; it may be viewed as a refinement of the theorem of Kummer-Herbrand-Ribet [56].

Since the "Tate-twisted" ideal class group of F^+ is, by a theorem of Tate, isomorphic to $K_2(\mathcal{O}_{F^+})$, one might ask for some direct link between our construction and algebraic K_2; we haven't found any. Nevertheless, as was already known, the "main conjecture" implies the "Birch-Tate conjecture" which gives a formula for the odd part of the order of $K_2(\mathcal{O}_{F^+})$ in terms of the value of the Dedekind zeta-function of F^+ at -1. Specifically, this order is a power of 2 times $w_2(F) \cdot |\zeta_F(-1)|$, where $w_2(F)$ is defined as the largest positive integer N such that $\mathrm{Gal}(F(\zeta_N)/F)$ has exponent 2. Combining our results whith those of [5], [11], [63] one also obtains partial results (i.e., lower bounds) for the order of $K_{2n}(\mathcal{O}_{F^+})$ ($n \geqq 1$, odd).

Our method does not construct abelian extensions of F^+. As is known from the work of Kummer and Iwasawa, the p-part of the ideal class group of F^+ is majorized by the minus part of the p-part of the ideal class group of $F^+(e^{2\pi i/p})$. The class number of F^+ tends to be small, difficult to calculate, and as yet there is no systematic method known for constructing the corresponding extensions. Nevertheless, Greenberg has shown that the "main conjecture" implies the "Gras conjecture" which we now describe.

Let F^+ be of degree prime to p over $\mathbf{Q}$, with Galois group G, and let $B(F^+)$ denote the p-primary component of the quotient of the group of global units by

circular units of F^+. Then $A(F^+)$ and $B(F^+)$, viewed as $\mathbf{Z}_p[G]$-modules have isomorphic Jordan-Hölder series.

It is interesting to note that the three conjectures we have just discussed (the conjectures of Iwasawa-Leopoldt, of Birch-Tate and of Gras) are assertions about number fields of finite degree, and yet our proof, via the "main conjecture" of Iwasawa theory, involves passage to cyclotomic extensions of infinite degree.

In a beautiful paper [56] Ken Ribet established the converse to the Kummer-Herbrand theorem, using modular curves. This connection between modular curves and the arithmetic of cyclotomic fields was developed further in [67], and provides the starting point for the theory presented here. It may come as a surprise that modular curves can be brought to bear on Iwasawa theory with such effectiveness. Here is one way of viewing the intrinsic connection between the two subjects. Iwasawa theory is concerned with (everywhere unramified) abelian extensions of cyclotomic fields, i.e., metabelian extensions of **Q**. The Galois groups of such extensions tend to admit representations in (the upper triangular subgroup of) $GL_2(R)$ where R is a suitable finite commutative ring, of order a power of p. It is then natural to search for these representations in (finite pieces of) the p-adic cohomology of modular curves, which are canonical models for the group $GL_{2/\mathbf{Q}}$. This search would be more in accordance with the prevailing philosophy if the representations sought were over a field of characteristic 0 rather than over finite rings, and if they were irreducible. Of course, neither is the case, and moreover, the utility of the representations sought lies precisely in the fact that they are not completely reducible. The technique we refine in this paper to use to control these "triangular" representations is the theory of the Eisenstein ideal initiated in [47], and further developed in [67]. That our search has been successful promotes the hope that a similar theory exists for other reductive groups over **Q**.

§ 2. Iwasawa's conjecture

We review the basic construction of Iwasawa theory in the case where the base field F is $\mathbf{Q}(e^{2\pi i/p})$, the case of interest in a number of classical questions. For a more complete review, see Chap. 1, § 2.

Let $F_n = \mathbf{Q}(e^{2\pi i/p^{n+1}})$ and $F_\infty = \bigcup_n F_n$. Recall that $\mathrm{Gal}(F_\infty/\mathbf{Q}) = \mathbf{Z}_p^* = \mathbf{F}_p^* \times \Gamma$ where Γ is the subgroup in $\mathbf{Z}_p^*$ consisting of units congruent to 1 mod p. Choose a topological generator γ of Γ.

Let L_n be the p-Hilbert Class Field of F_n. Let $H_n = \mathrm{Gal}(L_n/F_n)$ viewed as $\mathrm{Gal}(F_n/\mathbf{Q})$-module via the natural action.

Let $H_\infty = \varprojlim H_n$ and $V = H_\infty \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. There is a natural action of the Galois group $\mathrm{Gal}(F_\infty/\mathbf{Q})$ on V. Equivalently, we have commuting actions of $\mathbf{F}_p^*$ and of Γ on V.

Let $\omega\colon \mathbf{F}_p^* \to \mathbf{Z}_p^*$ denote the Teichmüller character, i.e., the unique character such that $\omega(a) \equiv a \bmod p$.

If i is an odd integer modulo $p-1$, let $V^{[i]}$ denote the ω^i-eigensubspace of V. Define $H_\infty^{[i]}$ similarly. Since $\mathbf{F}_p^*$ and Γ commute, the operator γ preserves the

subspaces $V^{[i]}$. It is a theorem of Iwasawa that V and hence also $V^{[i]}$ is finite-dimensional. Let $h_p(\omega^i, T)$ denote the characteristic polynomial of the operator $\gamma - 1$ acting on $V^{[i]}$.

For each nonzero even integer j modulo $p-1$, Kubota and Leopoldt have defined power series $G_p(\omega^j, T)$ in $\mathbf{Z}_p[\![T]\!]$. If $u \in \mathbf{Z}_p$ denotes the chosen generator γ of Γ but viewed as p-adic unit, then the p-adic analytic function of s, $L_p(\omega^j, s)$ is $G_p(\omega^j, u^s - 1)$. The following interpolation property holds for $k = 1, 2, 3, \ldots$:

$$L_p(\omega^j, 1-k) = -\mathbf{B}_k(\omega^{j-k})/k \quad \text{if} \quad j \not\equiv k \mod p-1$$

where $\mathbf{B}_k(\chi)$ is the k-th generalized Bernoulli number.

The p-adic analytic functions $L_p(\omega^j, s)$ (*the Kubota-Leopoldt* p-*adic* L-*function* attached to the character ω^j), and the power series $G_p(\omega^j, T)$ are uniquely determined by the above interpolation property.

The "main conjecture" for powers of the Teichmüller character ("Iwasawa's conjecture") then asserts that the ideal in $\mathbf{Z}_p[\![T]\!]$ generated by $h_p(\omega^i, T)$ is equal to the ideal generated by $G_p(\omega^{1-i}, T)$, provided i is an odd number, not congruent to 1 mod $p-1$.

Equivalently, the zeroes of the Iwasawa characteristic polynomial $h_p(\omega^i, T)$ are equal to the zeroes of $G_p(\omega^{1-i}, T)$, counted with multiplicity, in the closed unit disc.

As for the excluded case $i = 1$, it is known that $V^{[1]}$ is trivial, and hence $h_p(\omega, T) = 1$.

§ 3. *An outline of the proof of "Iwasawa's conjecture"*

The proof of the "main conjecture" for powers of the Teichmüller character is significantly easier than the proof in general. It may be of help to outline the main steps of our proof, in this case.

Let, then, $\chi = \omega^i$ where i is an odd integer not congruent to 1 mod $p-1$. Call these characters *admissible characters.*

The first major simplification in proving the theorem is to observe that we need only prove that $h_p(\chi, T)$ is divisible by $G_p(\chi^{-1}\omega, T)$ *provided* that we prove this for every admissible χ. This follows from an easy application of the analytic class number formula (cf. Chap. 1, § 6). Roughly speaking the class number formula gives the asymptotic behaviour of the order of the minus part of H_n as $n \to \infty$ and if $\prod_\chi h_p(\chi, T)$ were strictly larger than $\prod_\chi G_p(\chi^{-1}\omega, T)$ (i.e., if the quotient were divisible by a nonunit power series) this would be contradicted.

The second simplification we make is the introduction of Fitting ideals (cf. appendix). If Λ is a commutative ring, and M a module of finite presentation over Λ, the Fitting ideal $F_\Lambda(M)$ is an ideal in Λ which is a delicate measure of the "size" of the Λ-module M. In the case where $\Lambda = \mathbf{Z}_p[\![T]\!]$ and $H_\infty^{[i]}$ is given a Λ-module structure by the rule $\gamma \cdot x = (1+T) \cdot x$, then Iwasawa's conjecture follows from the formula:

$$F_\Lambda(H_\infty^{[i]}) = (G_p(\omega^{1-i}, T)). \tag{1}$$

As indicated above, to prove this it will be sufficient to show that

$$F_\Lambda(H_\infty^{[i]}) \subset (G_p(\omega^{1-i}, T)) \tag{2}$$

for all odd $i \not\equiv 1 \bmod p-1$.

What we actually do, and this is also sufficient, is to construct a sequence of unramified p-abelian extensions $L_\chi^{(n)}$ of F_∞, for each admissible χ and for $n = 0, 1, \ldots$ with the property that

$$F_\Lambda(\mathrm{Gal}(L_\chi^{(n)}/F_\infty)) \subset (G_p(\chi^{-1}\omega, T), \quad u^{p^n} \cdot (1+T)^{p^n} - 1) \tag{3}$$

and such that $\mathrm{Gal}(L_\chi^{(n)}/F_\infty)$ is a quotient of $H_\infty^{[i]}$ if $\chi = \omega^i$. The extension $L_\chi^{(n)}$ will not, in general, be an abelian extension of F_n, only of F_∞.

By expressing the information in terms of Fitting ideals, we are not obliged to consider the connection between our construction of $L_\chi^{(n)}$ and $L_\chi^{(n+1)}$; still less are we obliged to pass to a limit as n goes to ∞. As the reader will see, this is a very useful simplification as it appears to be a non-trivial matter to determine what coherence there is in the constructions of $L_\chi^{(n)}$ for varying n.

The use of Fitting ideals has one other advantage, of crucial importance to the success of our method, about which we will comment later on.

In order to produce the unramified extensions $L_\chi^{(n)}/F_\infty$ and to demonstrate that they have the requisite properties there are five principal "structures" which need to be examined:

(a) "*Good*" *quotient abelian varieties* $B_{n/\mathbf{Q}}$ of the jacobian of $X_1(p^n)$.

(b) *The Hecke algebra* $\mathbf{T}^{(n)}$ in the Endomorphism ring of B_n.

(c) *The cuspidal subgroups* $C_\chi^{(n)} \subset B_n(\bar{\mathbf{Q}})$. These are finite abelian p-groups, stable under the action of $\mathbf{T}^{(n)}$ and of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$.

(d) *The Eisenstein ideal* $I_\chi^{(n)}$, defined to be the annihilator in $\mathbf{T}^{(n)}$ of $C_\chi^{(n)}$.

(e) *The kernel of the Eisenstein ideal* $E_\chi^{(n)} = B_n(\bar{\mathbf{Q}})[I_\chi^{(n)}]$ in $B_n(\bar{\mathbf{Q}})$. By construction we have

$$0 \to C_\chi^{(n)} \to B_n(\bar{\mathbf{Q}})[I_\chi^{(n)}] \to M_\chi^{(n)} \to 0 \tag{4}$$

where $M_\chi^{(n)}$ is defined to make the sequence exact.

The field $L_\chi^{(n)}$ is then defined to be the splitting field of $E_\chi^{(n)} = B_n(\bar{\mathbf{Q}})[I_\chi^{(n)}]$ over F_∞.

The "good" quotients B_n have the property that they achieve good reduction everywhere over the field $\mathbf{Q}(\zeta_{p^n})^+$ where ζ_{p^n} is a primitive p^n-th root of 1. This relies on a deep result, originally proved by Langlands [44] using representation theory, which has, more recently, been given an algebraic geometric proof by Katz [36]. There are no finite flat subgroup schemes isomorphic to μ_p in the Néron model $B_{n/\mathbf{Z}_p[\zeta_{p^n}]^+}$. The fibre of B_n in characteristic p is isogenous to the product of two copies of the jacobian of the Igusa curve (in characteristic p) of level p^n. The standard Hecke operators (T_l for $l \neq p$, U_p, $\langle a \rangle$ for integers a prime to p, modulo p^n) generate a subalgebra $\mathbf{T}^{(n)}$ of the endomorphism ring of B_n, which is a commutative separable algebra, and such that the Tate module tensored with $\mathbf{Q}$, $Ta(B_n) \otimes \mathbf{Q}$, is a free $\mathbf{T}^{(n)} \otimes \mathbf{Q}$ module of rank 2.

One can describe B_0 as follows. Let $A_0 = J_1(p)/J_0(p)$, the quotient of the jacobian of $X_1(p)$ by the jacobian of $X_0(p)$. Then $A_0(\bar{\mathbf{Q}})$ contains a maximal finite

subgroup N stable under the Hecke operators and under the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ having the further properties that it is annihilated by a power of $I_\chi^{(n)}$ and it possesses, as $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\zeta_p)^+)$-module, a Jordan-Holder decomposition whose successive quotients are isomorphic to $|\boldsymbol{\mu}_p$. Then B_0 is the quotient of A_0 by the subgroup N. The construction of B_0 in this case ($n=0$) was already given in [67], though the result (3) for $n=0$ was not obtained there.

There is a mapping of the group ring $\mathbf{Z}[\mathbf{Z}/p^n\mathbf{Z})^*/(\pm 1)]$ to $\mathbf{T}^{(n)}$ induced by $[a]\mapsto\langle a\rangle$. The ring $\mathbf{Z}_p[(\mathbf{Z}/p^n\mathbf{Z})^*/(\pm 1)]$ breaks canonically into a product of $(p-1)/2$ local rings corresponding to projection operaters e_ψ where ψ: $(\mathbf{Z}/p\mathbf{Z})^*\to\mathbf{Z}_p^*$ runs through the even powers of the Teichmüller character. Each of these local rings is canonically isomorphic to $\mathbf{Z}_p[\Gamma/\Gamma^{p^{n-1}}]\underset{\iota}{\cong}\mathbf{Z}_p[\![T]\!]/((1+T)^{p^{n-1}}-1)$ the isomorphism being determined by $\gamma\mapsto(1+T)$.

The p-primary component of the subgroup of $B_n(\mathbf{Q})$ generated by the image of the "zero-cusps" on $J_1(p^n)$ is a finite $\mathbf{Z}_p[(\mathbf{Z}/p^n\mathbf{Z})^*/(\pm 1)]$-module. Call $C^{(n)}$ the isomorphic image of this group under the operator $U_p^{n-1}\cdot(U_p-p)$. If χ is an odd power of the Teichmüller character, let $C_\chi^{(n)}$ denote the image of $C^{(n)}$ under the projection operator e_ψ where $\psi=\chi^{-1}\omega^{-1}$. We may view $C_\chi^{(n)}$ as a $\mathbf{Z}_p[\![T]\!]$-module, via the ring-isomorphism ι.

In Chap. 4, we study the structure of the cuspidal group $C_\chi^{(n)}$. Briefly, by reduction to characteristic p, and a re-examination of the theory of Kubert-Lang adapted to Igusa curves in characteristic p, we show that the annihilator of the $\mathbf{Z}_p[\![T]\!]$-module $C_\chi^{(n)}$ is the ideal generated by $G_p(\chi^{-1}\omega, u^{-1}(1+T)^{-1}-1)$ and $(1+T)^{p^n}-1$.

We show that the finite flat group schemes generated by the groups $C_\chi^{(n)}$ and $M_\chi^{(n)}$ of (4) over $\mathbf{Z}[\zeta_{p^n}]^+$ are étale and of multiplicative type, respectively. This is done by a careful study of the structure of the fibre in characteristic p of a good model of the modular curve. It then follows that the exact sequence (4), viewed as Galois modules over $\mathbf{Q}_p(\zeta_{p^n})^+$, or as finite flat group schemes over $\mathbf{Z}_p[\zeta_{p^n}]^+$, splits canonically; the connected component of the group scheme $E_{\chi/\mathbf{Z}_p[\zeta_{p^n}]^+}^{(n)}$ projects isomorphically to $M_\chi^{(n)}$ and the inverse of that isomorphism yields the splitting.

The isomorphism between $M_\chi^{(n)}$ and the connected component of $E_\chi^{(n)}$ is important: firstly, it shows by a standard argument that the splitting field of $E_\chi^{(n)}$ is unramified at p over some cyclotomic field.

Secondly, and crucially, it enables us to show that $M=M_\chi^{(n)}$ is not too small. Let $\mathscr{X}$ denote the contravariant Tate module of the connected component of the $I_\chi^{(n)}$-adic component of the p-divisible group associated to B_n over $\mathbf{Z}_p[\zeta_{p^n}]^+$. Then if $\mathbf{T}_\chi^{(n)}$ denotes the $I_\chi^{(n)}$-adic completion of the Hecke algebra, M is isomorphic to the Pontrjagin dual of $\mathscr{X}/I_\chi^{(n)}\cdot\mathscr{X}$; $M=\mathrm{Hom}(\mathscr{X}/I_\chi^{(n)}\mathscr{X}, \mathbf{Q}_p/\mathbf{Z}_p)$. We prove that $\mathscr{X}$ is a faithful $\mathbf{T}_\chi^{(n)}$-module. It is at this point that the Fitting ideal theory becomes indispensable. Since $\mathscr{X}$ is *faithful*, we have that:

$$F_{\mathbf{T}_\chi^{(n)}}(\mathrm{Hom}(M,\mathbf{Q}_p/\mathbf{Z}_p))\subset I_\chi^{(n)}\subset\mathbf{T}_\chi^{(n)} \tag{5}$$

which implies, by a fairly easy argument using the structure of $C_\chi^{(n)}$ as $\mathbf{Z}_p[\![T]\!]$-module that

$$F_{\mathbf{Z}_p[\![T]\!]}(Hom(M,\mathbf{Q}_p/\mathbf{Z}_p))\subset(G_p(\chi^{-1}\omega,u^{-1}(1+T)^{-1}-1))\subset\mathbf{Z}_p[\![T]\!].$$

Let us pause to consider this step. The $\mathbf{T}_\chi^{(n)}$-module $\mathscr{X}$ is the least accessible object in our theory. We know the important fact that it is faithful, by having proved that $\mathscr{X} \otimes \mathbf{Q}$ is a free $\mathbf{T}_\chi^{(n)} \otimes \mathbf{Q}$-module of rank 1. Beyond that the algebraic geometry of modular curves seems to put no further constraints on the isomorphy-type of $\mathscr{X}$ as $\mathbf{T}_\chi^{(n)}$-module. In fact, we do not expect any easy general description of its isomorphy-type. In the special case where $\mathscr{X}$ is free, (5) becomes an *equality*:

$$F_{\mathbf{T}_\chi^{(n)}}(\mathrm{Hom}(M, \mathbf{Q}_p/\mathbf{Z}_p)) = I_\chi^{(n)}.$$

The aid afforded us by Fitting ideal theory is that it shows us that, even if $\mathscr{X}$ is not free, the Fitting ideal of $\mathrm{Hom}(M, \mathbf{Q}_p/\mathbf{Z}_p)$ is contained in $I_\chi^{(n)}$, and consequently M is at least as large as we expect. But, as the reader will see, the larger M is, the larger $L_\chi^{(n)}$ is. To sum up, our ignorance of the isomorphy-type of $\mathscr{X}$ *doesn't matter.*

Early in our study of Iwasawa's conjecture, this obstacle (the fact that we knew very little about $\mathscr{X}$) seemed difficult to surmount. We were then concentrating on the first case of our construction ($n = 0$) where the difficulty still presents itself in full force. At the time, we did not see the relevance of the Fitting ideal theory; nevertheless we surmised that the isomorphy-type of $\mathscr{X}$ didn't matter, and we reduced our problem to a question concerning modules over commutative rings. This question was promptly answered by John Tate, who pointed us in the direction of the theory of Fitting ideals. It gives us pleasure to record our gratitude to him for this; and to David Eisenbud, and David Buchsbaum for their patient help in explaining to us that theory.

We continue with our outline of the proof. If $G_\chi^{(n)} = \mathrm{Gal}(L_\chi^{(n)}/F_\infty)$, then we have a pairing,

$$G_\chi^{(n)} \times M_\chi^{(n)} \to C_\chi^{(n)} \tag{6}$$

defined by $(g, x) \mapsto g\bar{x} - \bar{x}$ where $\bar{x}$ is any lifting of x to $E_\chi^{(n)}$.

And now we must deal with a confusing, but crucial, aspect of the structure of the pairing (6). The groups $M_\chi^{(n)}$ and $C_\chi^{(n)}$ admit *two* natural, and distinct, $\mathbf{Z}_p[\![T]\!]$-module structures. The first such structure comes from the natural action of Galois on these groups; the second comes from the induced action of the diamond operators on the jacobian of the modular curve $X_1(p^n)$. Call these structures the *arithmetic* and the *geometric* $Z_p[\![T]\!]$-module structure, respectively. Although these structures are distinct, they are related by simple laws (twists) and we refer to both structures, connected by such laws, as *yoked bimodule structures.*

The Galois group $G_\chi^{(n)}$ possesses in its own right a natural arithmetic $\mathbf{Z}_p[\![T]\!]$-module structure. The pairing (6) may be used to induce a geometric $\mathbf{Z}_p[\![T]\!]$-module structure on $G_\chi^{(n)}$ so as to make (6) a pairing of yoked bimodules.

We now use Fitting ideal theory again, together with the fact that, viewed with its geometric $\mathbf{Z}_p[\![T]\!]$-module structure $C_\chi^{(n)} = \mathbf{Z}_p[\![T]\!]/(G_p(\chi^{-1}\omega, T'), (1+T)^{p^n} - 1)$ where $(1+T') = u^{-1}(1+T)^{-1}$, to prove that The Fitting ideal of $G_\chi^{(n)}$, given its geometric $\mathbf{Z}_p[\![T_n]\!]$-module structure, is contained in $(G_p(\chi^{-1}\omega, T'), (1+T)^{p^n} - 1)$.

Using the law which yokes the geometric and arithmetic $\mathbf{Z}_p[\![T]\!]$-module structures of $G_\chi^{(n)}$ we get the sought-for assertion concerning the Fitting ideal of $G_\chi^{(n)}$, giving its arithmetic $\mathbf{Z}_p[\![T]\!]$-module structure, and hence Iwasawa's conjecture.

§ 4. Complications arising from the consideration of more general characters

The "main conjecture" requires us to deal with a general abelian field F, rather than just $F = \mathbf{Q}(\zeta_p)$. Instead of $X_1(\mathrm{p}^n)$, we must consider $X_1(ap^n)$ for a general integer a prime to p. For various reasons, we cannot work with a single tame character at a time. In place of a power of the Teichmüller character, we consider a local ring direct factor of the semi-local ring $\mathbf{Z}_p[\mathbf{Z}/ap^n\mathbf{Z})^*]$, which we call a *component* $\mathfrak{m}$. We can decompose the p-divisible groups associated to $J_1(ap^n)$, and to the "good" quotient abelian varieties we construct, into a product, where the factors are in 1 : 1 correspondence with the components.

As it turns out, we needn't consider all components: only pseudo-primitive ones (cf. Chap. 1, § 3). Although this general context necessitates significant modifications in the definitions, one can still define the cuspidal group $C_{\mathfrak{m}}^{(n)}$ attached to a pseudo-primitive component $\mathfrak{m}$, the Eisenstein ideal $I_{\mathfrak{m}}^{(n)}$, and the kernel of the Eisenstein ideal $E_{\mathfrak{m}}^{(n)}$.

Two major new problems do however arise in this more general context. For powers of the Teichmüller character (and, indeed, for any component possessing a tame character of the form $\chi' \cdot \omega^k$ where χ' is unramified at p, and the greatest common divisor of k and $p-1$ is >1) we may depend upon the fine structure theory of finite flat group schemes to enable us to pass from information about the Galois representation associated to our finite flat group schemes $C_{\mathfrak{m}}^{(n)}$, $M_{\mathfrak{m}}^{(n)}$, $E_{\mathfrak{m}}^{(n)}$ to information concerning their fibre in characteristic p, and conversely. However for certain troublesome components, the theory of finite flat group schemes is no aid.

Second, among these "troublesome components" there are some for which an even more serious problem is encountered: if the component $\mathfrak{m}$ possesses a tame character of the form $\chi' \cdot \omega^k$ where $k \equiv -1 \bmod p-1$ and $\chi'(p) = 1$, then one cannot distinguish $C_{\mathfrak{m}}^{(n)}$ and $M_{\mathfrak{m}}^{(n)}$ by their Galois actions. This leads to some rather subtle considerations discussed at length in Chap. 5.

We are not able to complete our construction for all these components but fortunately what we lack is compensated for by the theorem of Ferrero and Greenberg. In fact the zeroes of the p-adic L-functions which elude our methods are precisely the so-called trivial zeroes studied in the papers [22] and [18]. This together with the analytic class number formula, and for certain components also the theorem of Ferrero and Washington on the vanishing of the μ-invariant, are the only results we need from "classical" number theory. In particular we make no use of Stickelberger's theorem in this paper.

§ 5. An open question

Let $F/\mathbf{Q}$ be an imaginary abelian extension and let G denote its Galois group. Can one give a simple description of the Fitting ideal of the minus part of the ideal class group as a module over $\mathbf{Z}[G]$?

§ 6. The framework of the paper

In Chap. 1, we describe the conjectures and their applications. In § 9 of Chap. 1 we reduce the problem to that of constructing unramified extensions with specified properties.

In Chap. 2, we study the geometry of the modular curves, particularly in characteristic p. We would expect the reader to find it convenient to use Chap. 2 as a reference. The forthcoming book [36] might be consulted for a systematic treatment of the general theory of the reduction of good models for modular curves.

In Chap. 3, we study the "good" quotient abelian varieties of the jacobians of modular curves, and the Hecke algebra.

In Chap. 4, we study the cuspidal groups.

Our actual construction is given in Chap. 5.

The reader may profit by consulting [9] and [43] which are excellent expository accounts of the results and techniques used in this paper.

§ 7. Acknowledgements

It is a pleasure to thank all those who have in various ways helped us with this paper. We are indebted to John Coates, H. Gillard, R. Greenberg, N. Katz, M. Raynaud, K. Ribet, and W. Sinnott for conversations, suggestions, and their patient corrections. We thank O. Gabber for supplying us with proofs of some important propositions, and as we have already mentioned, we are very grateful to D. Buchsbaum, D. Eisenbud, and J. Tate for introducing us to the theory of Fitting ideals.

§ 8. Errata

Each of us would also like to take this opportunity to correct some errors in our earlier papers [47], [67].

I. Erata for [47]

1. Page 125, Corollary 16.3: The proof for this corollary is not given, and should have been. Briefly, one makes use of the fact that $J_{\mathbf{p}}$ is ordinary, and that the Weil pairing induces a self-duality between its multiplicative-type and its étale parts. These hints, together with what has been explicity proved in § 16 easily leads one to a proof.

2. Page 105, line 18: I am grateful to Gerd Faltings for pointing out to me that the middle equality on that line is not evident; indeed it just doesn't follow from lines 13 and 14. To show that $A+B=0$, one must proceed differently. I am thankful to Dan Kubert for helping me out with the correct argument, which I briefly sketch below.

Note that $2A=(f)$, the divisor of the function f defined at the top of page 108. If f^w denotes the composition of f with w, then $2B=(f^w)$. So: $2A+2B=(f\cdot f^w)$. We must show that $f\cdot f^w$ is a square in the rational function field of $X_0(N)^{\#}_{/\mathbf{C}}$. Or equivalently, and here we use that $N\equiv 9 \bmod 16$, in the rational function field of $X_1(N)_{/\mathbf{C}}$.

Now we have the defining expression for f in terms of Siegel functions:

$$f = \text{constant}) \cdot \prod_{a \in (\mathbf{Z}/p\mathbf{Z})^*} g_{0,a}^{\chi(a)},$$

where $\chi(a) = (a/p)$ is the Legendre symbol. Here I am using the obvious modification of Kubert-Lang's notation for Siegel functions, i.e., (a, b) in $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ rather than in $1/p\,\mathbf{Z}/\mathbf{Z} \times 1/p\,\mathbf{Z}/\mathbf{Z}$ [39].

To compute f^w we use a result of Kubert and Lang (§4 of [39]) which applied to our case gives:

$$f^w = (\text{constant}) \cdot \prod_{\substack{a \in (\mathbf{Z}/p\mathbf{Z})^* \\ b \in \mathbf{Z}/p\mathbf{Z}}} g_{a^{-1},b}^{\chi(a)}.$$

Now let $\equiv$ denote "mod squares":

$$f \cdot f^w = \prod_{a \in (\mathbf{Z}/p\mathbf{Z})^*} g_{0,a} \cdot \prod_{\substack{a \in (\mathbf{Z}/p\mathbf{Z})^* \\ b \in (\mathbf{Z}/p\mathbf{Z})}} g_{a^{-1},b} = \prod_{\substack{(a,b) \in \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z} \\ (a,b) \neq (0.0)}} g_{a,b}$$

and the latter product of Siegel functions is one.

3. Page 100, line 7 bot.. The formula for the action of T_l on $X_1(N)$ quoted here is incorrect. The correct formula is, of course, well known (cf., e.g., [67], §2), and the argument on the next page in which the formula is used is unaffected by the correction.

(B.M.)

II. Erata for [67]

Hida has pointed out that the formulas for U_p' in Theorem 5.3 are not correct as they stand. They should state:

On $\mathrm{Pic}^0(\mathscr{C}_\infty^{(N)})$, $U_p' = \langle n_p^{-1} \rangle (\mathrm{Frob}_p + \sum_{\zeta \neq 1} W_\zeta)$.

On $\mathrm{Pic}^0(\mathscr{C}_0^{(N)})$, $U_p' = \mathrm{Ver}_p$.

The proof is correct except for the formula giving the conjugation of Frob_p and Ver_p by W. They should read:

$$W^{-1}(\mathrm{Frob}_p) W = \mathrm{Frob}_p \cdot \langle n_p^{-1} \rangle, \; W^{-1}(\mathrm{Ver}_p) W = \mathrm{Ver}_p \cdot \langle n_p \rangle.$$

(A.W.)

Chapter 0. Notation and preliminaries

If K is a field, $\bar{K}$ denotes an algebraic closure. If K is a local or global field, $\mathcal{O}(K)$ is its ring of integers.

If Y is a scheme over a base S and $T \to S$ any base change, $Y_{/T}$ denotes the pullback of Y to T. If $T = \mathrm{Spec}\, A$, we may also denote this scheme by $Y_{/A}$. By $Y(T)$ we mean the T-rational points of the S-scheme Y, and again, if $T = \mathrm{Spec}\, A$, we may also denote this set by $Y(A)$.

If $A_{/T}$ is a group scheme and N an integer, $A[N]_{/T}$ is the kernel of multiplication by N in A, viewed as group scheme over T.

A finite flat group scheme G over S is said to be of *multiplicative-type* if its Cartier dual is étale; it is called *ordinary* for every geometric point s of S, the fibre G_s is a product of a multiplicative-type group scheme and an étale group scheme.

Proposition. *Let K be a finite extension of $\mathbf{Q}_p$ of ramification index not divisible by $p-1$. Let $\varphi\colon G_1 \to G_2$ be a morphism of ordinary finite flat group schemes over $\mathcal{O}(K)$ such that the induced map*

$$\varphi(\bar{K})\colon \quad G_1(\bar{K}) \to G_2(\bar{K})$$

is injective. Then if k is the residue field of $\mathcal{O}(K)$, the induced mapping

$$\varphi(\bar{k})\colon \quad G_1(\bar{k}) \to G_2(\bar{k})$$

is also injective.

Remark: Although this is all we shall use, much more is true: Under the same hypotheses on K, and G_1, G_2, any injection $\varphi_{/K}\colon G_{1/K} \hookrightarrow G_{2/K}$ extends to a closed immersion of G_1 to G_2.

If we *drop* the hypotheses that G_1 and G_2 are ordinary, but require that the ramification index of K be *less than* $p-1$, these results remain true by the work of Oort-Tate ([52]; for groups of order p); of Raynaud ([55]; for groups of type $(p, p, \ldots, p)$; and of Fontaine ([20]; for arbitrary groups).

Before we give the proof of this proposition, recall the following consequences of the theory of Oort-Tate [52]:

Any finite flat group scheme G of order p over $\mathcal{O}(k)$ is isomorphic to a group scheme of the form $G_{a,b}$ for a, b elements of $\mathcal{O}(K)$ such that $a \cdot b = w_p \cdot 1$ where w_p is equal to p times a unit. [52], § 2; especially Theorem 2). The pair (a, b) is uniquely determined by the isomorphism class of G up to multiplication by $(p-1)$-st powers of units in $\mathcal{O}(K)$, i.e. $G_{a,b} \underset{\mathcal{O}(k)}{\cong} G_{a',b'}$ if and only if $a' = u^{p-1} \cdot a$, $b = u^{p-1} \cdot b'$ for some $u \in \mathcal{O}(K)^*$.

The group schemes $G_{a,b}$ and $G_{a',b'}$ are isomorphic over K (i.e. they have isomorphic Galois representations) if and only if

$$a' = r^{p-1} \cdot a; \quad b = r^{p-1} \cdot b'$$

for some $r \in K^*$.

The group scheme $G_{a,b}$ is of multiplicative type if and only if b is a unit in $\mathcal{O}(K)$; it is étale if and only if a is a unit.

Lemma 1. *Let G, G' be finite flat group scheme of order p over $\mathcal{O}(K)$, where G is étale and G' is of multiplicative type. Suppose that the ramification index of K over $\mathbf{Q}_p$ is not divisible by $p-1$. Then there are no nontrivial homomorphisms over K from G to G'.*

Proof. Let $G = G_{a,b}$; $G' = G_{a',b'}$ where a and b' are units in $\mathcal{O}(K)$. Let v be the valuation of K, normalized so that if π is a uniformizer then $v(\pi) = 1$.

By our hypothesis, $v(p) \not\equiv 0 \bmod (p-1)$. But if there were a nontrivial homomorphism (hence isomorphism) from $G_{/K}$ to $G'_{/K}$ then $b = r^{p-1} \cdot b'$ for some $r \in K^*$ and $v(p) = v(b) = (p-1) \cdot v(r) + v(b') = (p-1) \cdot v(r)$ yields a contradiction.

We now return to the proposition.

Replacing K by a finite unramified extension, we may suppose that the étale quotients $G_1^{\text{ét}}$, $G_2^{\text{ét}}$ are constant group schemes, and the connected components G_1^0, G_2^0 are the Cartier duals of constant group schemes. By our hypotheses on K, there are no nontrivial mappings between constant group schemes over K and Cartier duals of constant group schemes (in either direction). It follows that the inverse image of $G_{2/K}^0$ under $\varphi_{/K}$ is $G_{1/K}^0$ and consequently induces an injection of étale quotients

$$\varphi^{\text{ét}}: \quad G_1^{\text{ét}} \hookrightarrow G_2^{\text{ét}},$$

proving the proposition.

In this paper we shall often be given p-divisible group schemes $\Gamma_{/\mathbf{Q}_p}$ such that for some finite field extension K of $\mathbf{Q}_p$, the "base change" $\Gamma_{/K}$ is isomorphic to the generic fibre of a p-division group scheme over $\mathcal{O}(K)$. By a theorem of Tate, this group scheme over $\mathcal{O}(K)$ is uniquely determined (up to a canonical isomorphism) by $\Gamma_{/K}$. We shall call it $\Gamma_{/\mathcal{O}(K)}$ and refer to it as the *prolongation* of $\Gamma_{/K}$ *over the base* $\mathcal{O}(K)$. By the uniqueness theorem, one has that prolongations "commute with base change".

Given a *finite flat* group scheme G over K it is not necessarily the case that it admits at most one *prolongation* to a finite flat group scheme over $\mathcal{O}(K)$.

Corollary to the Proposition. *Let K be as in the proposition and let $i_{/K}: \Gamma_{/K} \to \Gamma'_{/K}$ be an injection of p-divisible group schemes over K. Suppose that $\Gamma_{/K}$ and $\Gamma'_{/K}$ have ordinary prolongations over $\mathcal{O}(K)$. Then the unique homomorphism*

$$i: \Gamma_{/\mathcal{O}(K)} \to \Gamma'_{\mathcal{O}(K)}$$

which extends $i_{/K}$ ([64] Theorem 4) induces an injection on $\bar{k}$-valued points:

$$i(\bar{k}): \quad \Gamma(\bar{k}) \hookrightarrow \Gamma'(\bar{k}).$$

Remark. The morphism i is, in fact, a closed immersion.

For use in Chap. 4 we include the following result.

Lemma. *Let K be a finite extension field of $\mathbf{Q}_p$ and $\mathcal{O} = \mathcal{O}(K)$.*

Let $\mathcal{N}_{/\mathcal{O}}$ be the Néron model of an abelian scheme $A_{/K}$. Suppose $\mathcal{N}_{/\mathcal{O}}$ has semi-stable reduction.

Let $G_{/K} \subseteq A_{/K}$ be a finite subgroup scheme, and $G_{/\mathcal{O}}$ the Zariski-closure of $G_{/K}$ in $\mathcal{N}_{/\mathcal{O}}$. Suppose that the splitting field of the action of $\mathrm{Gal}(\bar{K}/K)$ *on $G(\bar{K})$ is an unramified extension of K.*

Then $G_{/\mathcal{O}}$ is a finite flate (étale) group scheme.

Proof. The Néron model commutes with unramified base change; schematic closure commutes with flat base change. Therefore we may suppose the Galois action on $G_{/K}$ trivial. Let $\mathcal{G}_{/\mathcal{O}}$ denote the constant group scheme $G(K)$ over $\mathcal{O}$. Since $\mathcal{N}(\mathcal{O}) \to \mathcal{N}(K)$ is a bijection, we have a morphism $u: \mathcal{G}_{/\mathcal{O}} \to \mathcal{N}_{/\mathcal{O}}$ such that $u_{/K}$ is an isomorphism of $\mathcal{G}_{/K}$ onto $G_{/K}$. Therefore u factors through the schematic closure $G_{/\mathcal{O}}$. Since $\mathcal{G}_{/\mathcal{O}}$ is finite, so is $G_{/\mathcal{O}}$.

Chapter 1. Iwasawa Theory, p-adic L-functions, and Fitting ideals

§ 1. Introduction

The object of this chapter is to recall the classical Iwasawa theory, to state the "Main Conjecture for $\mathbf{Q}$", and to show how all the arithmetic results obtained in this paper may be deduced from one result (the Theorem of §9) concerning the Fitting ideals of the Galois groups of a sequence of field extensions to be constructed in Chap. 5. For various technical reasons, it is important for us to work with components rather than with characters (this notion is explained in § 3) and so we devote some space to the translation.

§ 2. Iwasawa theory in terms of characters

Throughout the paper, p will be a fixed odd prime. A p-adic Dirichlet character will be understood to take values in $\overline{\mathbf{Q}}_p$. If χ denotes such a character, then "χ" will refer to the primitive character associated to χ. We sometimes also use the letter χ to denote the homomorphism from $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ to $\overline{\mathbf{Q}}_p^*$ associated to such a Dirichlet character by class field theory. We let $\mathcal{O}_\chi \subseteq \overline{\mathbf{Q}}_p$ denote the ring extension of $\mathbf{Z}_p$ generated by the values of χ, and K_χ the field of fractions of $\mathcal{O}_\chi$. In what follows, unless otherwise specified, χ will always refer to a p-adic character whose conductor is not divisible by p^2. Such a character is said to be of the first kind.

Let μ_{p^ν} be the group of p^ν-th roots of unity and set

$$\mathbf{Q}(\mu_{p^\infty}) = \bigcup_{\nu=1}^{\infty} \mathbf{Q}(\mu_{p^\nu}).$$

Let $\mathbf{Q}_\infty/\mathbf{Q}$ denote the cyclotomic $\mathbf{Z}_p$-extension, i.e., the unique $\mathbf{Z}_p$-extension of $\mathbf{Q}$. Thus $\mathbf{Q}_\infty$ is a subfield of $\mathbf{Q}(\mu_{p^\infty})$ of index $(p-1)$. Let $\mathbf{Q}_\nu \subseteq \mathbf{Q}_\infty$ be the subfield of degree p^ν over $\mathbf{Q}$.

Let F be a finite abelian extension of $\mathbf{Q}$, and let $F_\infty = F\mathbf{Q}_\infty$. We will assume throughout that $F \cap \mathbf{Q}_\infty = \mathbf{Q}$. (Note that any χ of the first kind is attached by class field theory to a field F for which $F \cap \mathbf{Q}_\infty = \mathbf{Q}$). Let $F_\nu = F\mathbf{Q}_\nu$ so that F_ν/F is cyclic of degree p^ν. Let A_ν denote the p-primary component of the ideal class group of F_ν and H_ν the Galois group of the p-Hilbert class field of F_ν (over F_ν). Then class field theory yields isomorphisms (via the mapping induced from ψ^{-1} as in [7], VII, §5);

$$A_v \xrightarrow{\sim} H_v, \tag{1}$$

compatible with the actions of $\mathrm{Gal}(F/\mathbf{Q})$ on domain and range. Here the action of $\mathrm{Gal}(F/\mathbf{Q})$ on H_v is given by conjugation; viz. if $h \in H_v$ and $\sigma \in \mathrm{Gal}(F/\mathbf{Q})$, let *$\tilde{\sigma}$ be any lift of σ* to an automorphism of the p-Hilbert class field of F_v, and then $h^\sigma = \tilde{\sigma} h \tilde{\sigma}^{-1}$.

The inclusion of the divisor group of F_v in the divisor group of F_{v+1} induces a map $i_v: A_v \to A_{v+1}$. This map i_v is not necessarily injective. However if A_v^- denotes the subgroup of A_v on which complex conjugation acts like -1 then the restriction of i_v to A_v^- is injective (c.f. [32]). The isomorphism of (1) is such that the diagrams

$$\begin{array}{ccc} A_{v+1} & \xrightarrow{\sim} & H_{v+1} \\ \downarrow{\scriptstyle \mathrm{Norm}} & & \downarrow{\scriptstyle \mathrm{Res}} \\ A_v & \xrightarrow{\sim} & H_v \end{array} \qquad \begin{array}{ccc} A_v & \xrightarrow{\sim} & H_v \\ \downarrow{\scriptstyle i_v} & & \downarrow{\scriptstyle \mathrm{transfer}} \\ A_{v+1} & \xrightarrow{\sim} & H_{v+1} \end{array}$$

are commutative. Set

$$A_\infty = \varinjlim A_v, \qquad H_\infty = \varprojlim H_v.$$

Both A_∞ and H_∞ are $\mathbf{Z}_p$-modules which admit a continuous action of $\mathrm{Gal}(F_\infty/\mathbf{Q})$. To mark their dependence on F we may write $A_v(F)$, $A_\infty(F)$, and $H_v(F)$, $H_\infty(F)$.

Because $F \cap \mathbf{Q}_\infty = \mathbf{Q}$ the group $\mathrm{Gal}(F_\infty/\mathbf{Q})$ has a natural product decomposition

$$\mathrm{Gal}(F_\infty/\mathbf{Q}) \xrightarrow{\sim} \mathrm{Gal}(F_0/\mathbf{Q}) \times \Gamma \tag{2}$$

where $\Gamma = \mathrm{Gal}(F_\infty/F_0)$. If U is any $\mathbf{Z}_p$-module with a continuous action of $\mathrm{Gal}(F_\infty/\mathbf{Q})$ on it we may view U as a module over the complete group ring,

$$\mathbf{Z}_p[\![\Gamma]\!] = \varprojlim \mathbf{Z}_p[\Gamma/\Gamma_v]$$

where $\Gamma_v = \mathrm{Gal}(F_\infty/F_v)$, and possessing a commuting action of $\mathrm{Gal}(F_0/\mathbf{Q})$. If $\chi: \mathrm{Gal}(F/\mathbf{Q}) \to \mathcal{O}_\chi^*$ is a p-adic character, we define the χ-part of U to be the $\mathcal{O}_\chi[\![\Gamma]\!]$-module obtained from U by change of scalars:

$$U_\chi = U \underset{\mathbf{Z}_p[\mathrm{Gal}(F/\mathbf{Q})]}{\otimes} \mathcal{O}_\chi.$$

For a given χ we let $\Lambda = \Lambda_\chi$ denote the topological ring $\mathcal{O}_\chi[\![\Gamma]\!]$. There is a non-canonical isomorphism $\mathcal{O}_\chi[\![\Gamma]\!] \xrightarrow{\sim} \mathcal{O}_\chi[\![T]\!]$, an isomorphism being given by picking a topological generator γ for Γ and mapping $\gamma \mapsto 1 + T$. We make an arbitrary choice of γ, which we fix from now on, and we denote this isomorphism by σ_γ. We use it to identify $\mathcal{O}_\chi[\![\Gamma]\!]$-modules with Λ-modules.

Let $\sim$ denote the relation on Λ-modules of finite type given by pseudo-isomorphism. Thus if A and B are Λ-modules we say $A \sim B$ if there exists a Λ-homomorphism from A to B with finite kernel and cokernel. For torsion

Λ-modules, $\sim$ is an equivalence relation. Iwasawa has proven that $\mathrm{Hom}(A_\infty, \mathbf{Q}_p/\mathbf{Z}_p)_{\chi^{-1}}$[1] and $H^*_{\infty,\chi}$ are finite-type torsion Λ-modules and are pseudo-isomorphic for each $\chi\colon \mathrm{Gal}(F/\mathbf{Q}) \to \mathcal{O}_\chi^*$ (cf. [32]). Here $H^*_{\infty,\chi}$ is the Λ-module with the same underlying group structure as $H_{\infty,\chi}$ but on which $\mathrm{Gal}(F_\infty/\mathbf{Q})$ acts by the rule $gh^* = g^{-1}h$.

By the structure theory of finite-type torsion Λ-modules (c.f. [62]), there is a pseudo-isomorphism

$$H_{\infty,\chi} \sim \Lambda/(h_1) \oplus \ldots \oplus \Lambda/(h_r)$$

for some integer r, where each $h_i \in \Lambda$. Moreover, the ideal $(h_1 \ldots h_r)$ is an invariant of $H_{\infty,\chi}$. We may pick a unique generator of this ideal of the form

$$h_p(\chi, T) = \pi^{\mu_\chi} \cdot h_\chi(T)$$

where $h_\chi(T)$ is a distinguished polynomial and π is a uniformizing parameter in $\mathcal{O}_\chi$. In the theory of Λ-modules, μ_χ is called the μ-invariant and $\lambda_\chi = \deg(h_\chi(T))$ the λ-invariant of the Λ-module $H_{\infty,\chi}$. We call $h_p(\chi, T)$ the *Iwasawa polynomial* of $H_{\infty,\chi}$. One checks easily that the Iwasawa polynomial for $\mathrm{Hom}(A_\infty, \mathbf{Q}_p/\mathbf{Z}_p)_\chi$ generates the same ideal in $\mathcal{O}_\chi[\![T]\!]$ as $h_p(\chi^{-1}, (1+T)^{-1} - 1)$.

Proposition 1. (i) *(Iwasawa) For each odd character χ, $H_{\infty,\chi}$ and $\mathrm{Hom}(A_\infty, \mathbf{Q}_p/\mathbf{Z}_p)_\chi$ have no finite Λ-submodule.*

(ii) *(Ferrero-Washington) For each character χ, $H_{\infty,\chi}$ and $\mathrm{Hom}(A_\infty, \mathbf{Q}_p/\mathbf{Z}_p)_\chi$ are both of finite type as $\mathbf{Z}_p$-modules. Equivalently, $\mu_\chi = 0$ for each χ.*

The proof of the first statement for $\mathrm{Hom}(A_\infty, \mathbf{Q}_p/\mathbf{Z}_p)_\chi$ may be found in [32] or [24] and of the second in [19]. A similar proof can be given for $H_{\infty,\chi}$. We make use of (ii) in the proof of our main theorem [in §9] only for a restricted class of characters (cf. Chap. 5, §4, Lemma 1).

Although the module $H_{\infty,\chi}$ depends upon the original field F we observe that the Iwasawa polynomial $h_p(\chi, T)$ depends only upon χ. For, suppose that F' is another abelian extension of $\mathbf{Q}$, containing F, and such that $F' \cap \mathbf{Q}_\infty = \mathbf{Q}$. By restriction, χ defines a character of $\mathrm{Gal}(F'/\mathbf{Q})$ and the natural restriction map from $H_{\infty,\chi}(F')$ to $H_{\infty,\chi}(F)$ is easily seen to be a pseudo-isomorphism. (Here we are also identifying $\mathrm{Gal}(F'_\infty/F'_0)$ and $\mathrm{Gal}(F_\infty/F_0)$ by restriction.) This follows from the fact that in a cyclotomic $\mathbf{Z}_p$-extension only finitely many primes lie above any prime of $\mathbf{Q}$.

If we make use of the result of Ferrero and Washington, then the Iwasawa polynomial has a simpler description. To each of the modules $H_{\infty,\chi}$ we consider the Γ-representation space

$$V_\chi(F) = H_{\infty,\chi}(F) \underset{\mathcal{O}_\chi}{\otimes} K_\chi.$$

Again, if F' is an abelian extension of $\mathbf{Q}$, containing F, and such that $F' \cap \mathbf{Q}_\infty = \mathbf{Q}$, then the natural map $V_\chi(F') \to V_\chi(F)$ is an isomorphism of Γ-modules. Hence we

[1] If $\gamma \in \Gamma$, $a \in A_\infty$, $f \in \mathrm{Hom}(A_\infty, \mathbf{Q}_p/\mathbf{Z}_p)$ then we define $(\gamma \cdot f)(a) = f(\gamma^{-1}a)$

write V_χ for $V_\chi(F)$. The dimension of the vector space V_χ is just the λ-invariant of $H_{\infty,\chi}$. Using the fixed topological generator γ of Γ, we find that the Iwasawa polynomial $h_p(\chi, T)$ is just the characteristic polynomial of the endomorphism γ-I acting on the K_χ-vector space V_χ:

$$h_p(\chi, t) = \det(t \cdot I - (\gamma - I)) \in \mathcal{O}_\chi[t].$$

(If we did not assume the result of Ferrero-Washington we would still have that $h_\chi(T)$ was the characteristic polynomial of $\gamma - I$.)

Although we will not use it in the rest of this paper there is another approach to Iwasawa theory which we present here. Let M_ν be the maximal abelian p-extension of F_ν which is unramified except possibly at the primes of F_ν lying above p. Let $M_\infty = \bigcup_{\nu=0}^{\infty} M_\nu$ and let $X_\infty = \mathrm{Gal}(M_\infty/F_\infty)$. To show its dependence on F we may write $X_\infty(F)$. Then X_∞ is a compact $\mathbf{Z}_p$-module with a continuous action of $\mathrm{Gal}(F_\infty/\mathbf{Q})$, this action being given by conjugation defined in a manner analogous to that for H_ν. If M is a Λ-module, let $\mathrm{tors}(M) \subset M$ denote the submodule of Λ-torsion elements.

Proposition 2. ([8], Theorem 1.8).

$$X_{\infty,\chi} \sim \Lambda^{\delta_\chi} \oplus \mathrm{tors}(X_{\infty,\chi})$$

where $\delta_\chi = 1$ *if* χ *is an odd character and* $\delta_\chi = 0$ *otherwise.*

If χ is an *even* character, we may consider the Iwasawa polynomial $f_p(\chi, T)$ for $X_{\infty,\chi}$. This polynomial is independent of F in the same sense that $h_p(\chi, T)$ was. As previously, if we assume the result of Ferrero and Washington, then this is the characteristic polynomial of γ-I acting on $W_\chi(F)$ where

$$W_\chi(F) = X_{\infty,\chi}(F) \underset{\mathcal{O}_\chi}{\otimes} K_\chi.$$

We will now show how this polynomial is related to $h_p(\chi, T)$.

Given a character χ of the first kind it is easy to check that there is an F such that $W_\chi = W_\chi(F)$ and F contains a primitive pth root of unity. We choose such an F and we note that then F_∞ contains $\mathbf{Q}(\mu_{p^\infty})$. Set

$$Ta(\mu_{p^\infty}) = \mathrm{Hom}(\mathbf{Q}_p/\mathbf{Z}_p, \mu_{p^\infty}).$$

Then $Ta(\mu_{p^\infty})$ is a free $\mathbf{Z}_p$-module of rank 1, the action of $\mathrm{Gal}(F_\infty/\mathbf{Q})$ on it being given by the *cyclotomic* character,

$$\varepsilon\colon \mathrm{Gal}(F_\infty/\mathbf{Q}) \to \mathbf{Z}_p^*$$

We write $\varepsilon = \omega \cdot \kappa$ where ω and κ are characters of $\mathrm{Gal}(F/\mathbf{Q})$ and Γ respectively, which induce characters on $\mathrm{Gal}(F_\infty/\mathbf{Q})$ via the natural product decomposition (2). Consider the μ-dual of A_∞,

$$\mathrm{Hom}(A_\infty, \mu_{p^\infty}) = \mathrm{Hom}(A_\infty, \mathbf{Q}_p/\mathbf{Z}_p) \otimes Ta(\mu_{p^\infty})$$

with its naturally induced $\mathrm{Gal}(F_\infty/\mathbf{Q})$-action: that is if $\varphi \in \mathrm{Hom}(A_\infty, \mu_{p^\infty})$, $\alpha \in A_\infty$ and $g \in \mathrm{Gal}(F_\infty/\mathbf{Q})$, then $(g\varphi)(\alpha) = g(\varphi(g^{-1}\alpha))$.

The following theorem is a result from Kummer theory proved by Iwasawa. As before χ is a p-adic character: $\mathrm{Gal}(F/\mathbf{Q}) \to \bar{\mathbf{Q}}_p^*$.

Proposition 3. *If χ is an even character, then there is an isomorphism of $\mathcal{O}_\chi[\![\Gamma]\!]$-modules*

$$X_{\infty,\chi} \xrightarrow{\sim} \mathrm{Hom}(A_\infty, \mu_{p^\infty})_\chi .$$

We note that we have assumed that $p > 2$. For $p = 2$ the proposition is not true as it stands, see [24], Proposition 2.

By computing the characteristic polynomial of $\mathrm{Hom}(A_\infty, \mu_{p^\infty})_\chi$ in terms of the polynomial for $\mathrm{Hom}(A_\infty, \mathbf{Q}_p/\mathbf{Z}_p)_{\omega^{-1}\chi}$ a simple calculation gives that the $\mathcal{O}_\chi[\![T]\!]$-ideals generated by $f_p(\chi, T)$ and by $h_p(\omega\chi^{-1}, u(1+T)^{-1} - 1)$ are the same. Here $u = \kappa(\gamma)$, where γ is our chosen topological generator of Γ.

§ 3. *Characters versus components*

Let $\mathbf{Z}[G]$ be the integral group ring of a finite abelian group G of order n. Fix p a prime number, and set $R = \mathbf{Z}_p[G] = \mathbf{Z}_p \otimes \mathbf{Z}[G]$. Then R is a complete semi-local ring, thus a product of local rings. If n is prime to p, R is an étale $\mathbf{Z}_p$-algebra, a finite product of discrete valuation rings. In general, if $\tilde{R}$ denotes the integral closure of R in its total quotient ring, then R is a subring of finite index in $\tilde{R}$. If n is a power of p, then R is a local ring. If G_p denotes the p-primary component of G, and $G_{p'}$ the product of all l-primary components for $l \neq p$, then $G = G_p \times G_{p'}$ and

$$R = \mathbf{Z}_p[G_p] \otimes \mathbf{Z}_p[G_{p'}] .$$

There is a natural bijective correspondence between any of the sets in the following list:

the connected components of Spec R

the maximal ideals of R

the irreducible idempotents of the ring R

the $\mathbf{Q}_p$-conjugacy classes of $\overline{\mathbf{Q}}_p^*$-valued characters of $G_{p'}$. (χ and ψ are in the same class if $\chi = \psi^\sigma$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$).

We shall call the set of connected components of Spec R: Π, and refer to the elements of that set as *components.*

For each $\mathfrak{m} \in \Pi$ we have $R_\mathfrak{m}$, the completion of R with respect to the corresponding maximal ideal, and $e_\mathfrak{m}$, the corresponding irreducible idempotent. We have

$$R = \prod_{\mathfrak{m} \in \Pi} R_\mathfrak{m}$$

where the idempotent $e_\mathfrak{m}$ is the projection operator of R onto the factor $R_\mathfrak{m}$, viewed as subring of R. The projection $R \to R_\mathfrak{m}$ is flat. The $\mathbf{Q}_p$-conjugacy class of characters associated to $\mathfrak{m}$ is represented by the restriction to G_p' of the composite map $R \to R_\mathfrak{m} \to \overline{\mathbf{Q}}_p$ for any homomorphism of $R_\mathfrak{m}$ to $\overline{\mathbf{Q}}_p$.

Call Σ the set of irreducible components of Spec R and refer to elements of Σ as the *sheets.* If σ is a sheet, let R_σ denote the quotient of R by the ideal of definition of σ. We have that the normalization of R is

$$\tilde{R} = \prod_{\sigma \in \Sigma} R_\sigma$$

but the projection $R \to R_\sigma$ is not necessarily flat. There is a natural bijective correspondence between the *irreducible* components of Spec R and $\mathbf{Q}_p$-conjugacy classes of $\bar{\mathbf{Q}}_p^*$-valued characters of G. Each $R_\sigma \otimes \mathbf{Q}_p$ is a field and the conjugacy class of $\bar{\mathbf{Q}}_p^*$-valued characters of G corresponding to σ is obtained by the restriction to G of the composite mappings $R \to R_\sigma \otimes \mathbf{Q}_p \to \bar{\mathbf{Q}}_p$, one for each embedding of $R_\sigma \otimes \mathbf{Q}_p$ in $\bar{\mathbf{Q}}_p$.

If χ is a $\bar{\mathbf{Q}}_p^*$-valued character of G, we say that χ *belongs* to the sheet σ if its $\mathbf{Q}_p$-conjugacy class corresponds σ. Every sheet is contained in a unique component, giving us a surjection $\Sigma \twoheadrightarrow \Pi$ and an isomorphism $R_\mathfrak{m} \otimes \mathbf{Q}_p \xrightarrow{\sim} \prod_{\sigma \in \mathfrak{m}} R_\sigma \otimes \mathbf{Q}_p$. In each component, we may single out a sheet, which we shall call the *basic sheet*, as follows: let χ' be a character of $G_{p'}$, in the $\mathbf{Q}_p$-conjugacy class of characters of $G_{p'}$ corresponding to the component $\mathfrak{m}$. The *basic sheet* of $\mathfrak{m}$ then corresponds to the $\mathbf{Q}_p$-conjugacy class of the character χ of G obtained from χ' by composition with the projection $G \to G_{p'}$. Thus the basic sheet of $\mathfrak{m}$ corresponds to the unique equivalence class of $\bar{\mathbf{Q}}_p^*$-valued characters of G belonging to $\mathfrak{m}$ which are of order prime to p. These will be called *basic* characters belonging to $\mathfrak{m}$.

Fix an integer a prime to p and, for $n \geqq 1$, set $G^{(n)} = (\mathbf{Z}/ap^n\mathbf{Z})^*$ and $R^{(n)} = \mathbf{Z}_p[G^{(n)}]$. We have the natural projections

$$\twoheadrightarrow R^{(n+1)} \twoheadrightarrow R^{(n)} \twoheadrightarrow \cdots \twoheadrightarrow R^{(1)}$$

and we let $R^{(\infty)}$ denote the projective limit. Since $(G^{(n)})_{p'} = (G^{(1)})_{p'}$ for any $n \geqq 1$, the components of $G^{(n)}$ are in one-one correspondence with the components of $G^{(1)}$. If $\mathfrak{m}$ is any such component, we have the projective system

$$\twoheadrightarrow R_\mathfrak{m}^{(n+1)} \twoheadrightarrow R_\mathfrak{m}^{(n)} \twoheadrightarrow \cdots \twoheadrightarrow R_\mathfrak{m}^{(1)}$$

whose limit we denote $R_\mathfrak{m}^{(\infty)}$. By definition, the *reduced conductor* of any component is the conductor of any character of order prime to p (i.e., any basic character) belonging to $\mathfrak{m}$. The reduced conductor of any component is a divisor of ap. A *primitive* component is one whose reduced conductor is exactly ap.

We shall say that a component $\mathfrak{m}$ is a-*primitive* if its reduced conductor is either a or ap. We say that it is *pseudo-primitive* if there is some character belonging to $\mathfrak{m}$ whose conductor is a or ap. Note that if $\mathfrak{m}$ is pseudo-primitive of reduced conductor ap/r then r is of necessity a square-free integer such that every prime q dividing r is either equal to p or congruent to $1 \bmod p$, and $(r, ap/r) = 1$.

Say that a component $\mathfrak{m}$ is *even* (resp. *odd*) if every character belonging to $\mathfrak{m}$ is even (resp. odd).

Let $\mathbf{Z}_{p,a} = \varprojlim_n \mathbf{Z}/ap^n\mathbf{Z}$ viewed as (compact) topological ring. Let $\Omega_{p,a}$ denote the kernel of the natural surjection

$$\mathbf{Z}_{p,a}^* \twoheadrightarrow (\mathbf{Z}/pa\mathbf{Z})^* . \tag{1}$$

Thus $\Omega_{p,a}$ is a compact topological group (the group of 1-units in $\mathbf{Z}_{p,a}^*$).

It is well known that $\Omega_{p,a}$ is free pro-p-group on one generator, and any 1-unit $u \in \mathbf{Z}_{p,a}^*$ such that $u \not\equiv 1 \bmod ap^2$ may be taken as topological generator. Explicitly, for such a choice u, we have an isomorphism of topological groups

$$\mathbf{Z}_p^+ \xrightarrow[\cong]{} \Omega_{p,a}$$

$$z \longrightarrow u^z$$

The natural projection $\mathbf{Z}_{p,a}^* \to \mathbf{Z}_{p,1}^* = \mathbf{Z}_p^*$ induces an isomorphism $\Omega_{p,a} \xrightarrow[\cong]{} \Omega_{p,1}$ and we identify $\Omega_{p,a}$ (all $a \geqq 1$) via these isomorphisms, denoting $\Omega_{p,1}$ by Ω.

One checks that (1) induces an isomorphism from the torsion subgroup of $\mathbf{Z}_{p,a}^*$ onto $(\mathbf{Z}/pa\mathbf{Z})^*$ and consequently there is a unique product decomposition

$$\mathbf{Z}_{p,a}^* \cong (\mathbf{Z}/pa\mathbf{Z})^* \times \Omega . \tag{2}$$

This induces an isomorphism of topological rings.

$$\mathbf{Z}_p[\![\mathbf{Z}_{p,a}^*]\!] \xrightarrow[\cong]{} \mathbf{Z}_p[(\mathbf{Z}/pa\mathbf{Z})^*]\,[\![\Omega]\!] \tag{3}$$

where we have used the convention that if A is a commutative topological ring then

$$A[\![\mathbf{Z}_{p,a}^*]\!] \cong \varprojlim_n A[\mathbf{Z}/p^n a\mathbf{Z})^*]$$

and

$$A[\![\Omega]\!] \cong \varprojlim_n A[\Omega/\Omega^{p^n}] .$$

In the notation of the previous discussion (3) becomes the isomorphism of topological rings.

$$R^{(\infty)} \xrightarrow[\cong]{} R^{(1)}[\![\Omega]\!] \tag{4}$$

and for each component $\mathfrak{m}$ there is an induced isomorphism

$$R_{\mathfrak{m}}^{(\infty)} \xrightarrow[\cong]{} R_{\mathfrak{m}}^{(1)}[\![\Omega]\!] \tag{5}$$

and also, for every $n \geqq 1$,

$$R_{\mathfrak{m}}^{(n)} \xrightarrow[\cong]{} R_{\mathfrak{m}}^{(1)}\,[\Omega/\Omega^{p^{n-1}}] . \tag{6}$$

Where no confusion can arise we identify the above rings by the above isomorphisms.

Examples. (1) $a = 1$: then $R^{(1)} = \mathbf{Z}_p[\mathbf{F}_p^*]$ and $R^{(\infty)} = \mathbf{Z}_p[\![\mathbf{Z}_p^*]\!]$. The components are in one-one correspondence with the integers j modulo p-1 where the j-th component $R^{(1)} \twoheadrightarrow R_{\mathfrak{m}_j}^{(1)}$ is the projection $\mathbf{Z}_p[\mathbf{F}_p^*] \to \mathbf{Z}_p$ induced by $x \to \omega^j(x)$ where $x \in \mathbf{F}_p^*$ and ω is the Teichmüller character ($\omega(x) \equiv x$ modulo p). We then have

$$R_{\mathfrak{m}_j}^{(\infty)} \xrightarrow{\sim} \mathbf{Z}_p[\![\Omega]\!] .$$

(2) To give a numerical example, consider $p=3$, $a=7$. The reader will easily check that in this case there are four components, and only one of them is a primitive component. Each component has two sheets. Belonging to the basic sheet, there is precisely one character of $G^{(1)}$; belonging to any non-basic sheet there are precisely two.

§ 4. Twisting and yokes

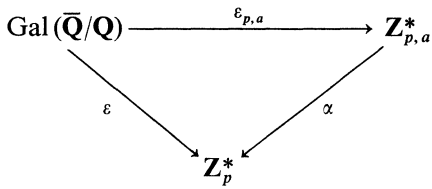
Consider the natural mapping

$$\varepsilon_{p,a}\colon \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{Z}_{p,a}^* = \varprojlim (\mathbf{Z}/ap^n\mathbf{Z})^*$$

characterized by the property that $\zeta^{\varepsilon_{p,a}(g)} = \zeta^g$ for every ap^n-th root ζ of 1 in $\bar{\mathbf{Q}}$, for each n. We refer to

$$\varepsilon = \varepsilon_{p,1}\colon \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{Z}_p^*$$

as the (p-) *cyclotomic character*. We let α denote the natural projection $\mathbf{Z}_{p,a}^* \to \mathbf{Z}_p^*$ so that we have a commutative diagram



Now consider the *twist* automorphism

$$\tau\colon \mathbf{Z}_p[\![\mathbf{Z}_{p,a}^*]\!] = R^{(\infty)} \to R^{(\infty)}$$

defined by sending the element $[g] \in \mathbf{Z}_p[\![\mathbf{Z}_{p,a}^*]\!]$ associated to $g \in \mathbf{Z}_{p,a}^*$ to $\alpha(g) \cdot [g]$. This twist automorphism τ takes even components to odd ones and vice versa.

The reason for the terminology 'twisting' is as follows. Suppose M is both an $R^{(\infty)}$-module and a $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-module such that its Galois action is obtained from its $R^{(\infty)}$ structure by composition with a homomorphism $h\colon \mathbf{Z}_p[\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})] \to R^{(\infty)}$. Then giving the Tate-twisted module $M(1) = M \underset{\mathbf{Z}_p}{\otimes} Ta^*(\mu_{p^\infty})$ an $R^{(\infty)}$ structure by its action on the first factor, we obtain its Galois-module structure from it via τh.

Definition. *If $k \in \mathbf{Z}$, the k-twisted yoke $\rho_k\colon \mathbf{Z}_p[\![\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})]\!] \to R^{(\infty)}$ is the unique continuous ring homomorphism such that*

$$\rho_k(g) = \varepsilon^k(g) \cdot [\varepsilon_{p,a}(g)].$$

Thus $\tau\rho_k = \rho_{k+1}$. Define the conjugate k-twisted yoke

$$\bar{\rho}_k\colon \mathbf{Z}_p[\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})] \to R^{(\infty)}$$

by the formula $\bar{\rho}_k(g) = \varepsilon^k(g) \cdot [\varepsilon_{p,a}(g)]^{-1}$. If $\mathfrak{m}$ is a component, we denote by $\eta_k = \eta_{k,\mathfrak{m}}$ and $\bar{\eta}_k = \bar{\eta}_{k,\mathfrak{m}}\colon \mathbf{Z}_p[\![\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})]\!] \to R_{\mathfrak{m}}^{(\infty)}$ the composition of ρ_k and $\bar{\rho}_k$ respectively with projection to the factor $R_{\mathfrak{m}}^{(\infty)}$.

We shall be concerned with $R_{\mathfrak{m}}^{(\infty)}$-modules (for some component $\mathfrak{m}$) which are also endowed with a commuting action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. We refer to these as *bimodules.*

Of the "twisted yokes" introduced above, the important ones for us will be η_1, $\bar{\eta}_{-1}$: $\mathbf{Z}_p[\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}] \to R_{\mathfrak{m}}^{(\infty)}$. For example, $\bar{\eta}_{-1}$ is a surjective homomorphism characterized by the formula

$$\bar{\eta}_{-1}(\varphi_l) = l^{-1} \cdot [l]_{\mathfrak{m}}^{-1}$$

where l is any rational prime number not dividing ap, φ_l is any Frobenius element in $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ associated to l, and $[l]_{\mathfrak{m}}$ refers to the image in $R_{\mathfrak{m}}^{(\infty)}$ of the element $[l]$ in $\mathbf{Z}_p[\![\mathbf{Z}_{p,a}^*]\!]$.

We shall say that a bimodule is $(\bar{\eta}_{-1})$-*yoked* if its $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ structure is obtained from its $R_{\mathfrak{m}}^{(\infty)}$ structure via the homomorphism $\bar{\eta}_{-1}$. Note that, since $\bar{\eta}_{-1}$ is a surjective ring homomorphism, a $\mathbf{Z}_p[\![\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})]\!]$ module admits a "yoked bimodule structure" if and only if $\ker \bar{\eta}_{-1}$ is contained in its annihilator ideal, and, in that case, the yoked bimodule structure is uniquely determined by the $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-structure.

§ 5. Stickelberger elements

Let $k \geqq 1$ be an integer and let $\mathbf{B}_k(x)$ be the k^{th} Bernoulli polynomial (cf. [41], Chap. 2). In particular, $\mathbf{B}_1(x) = x - \frac{1}{2}$ and $\mathbf{B}_2(x) = x^2 - x + \frac{1}{6}$. For $x \in \mathbf{R}$ let $\langle x \rangle$ denote the real number $\equiv x \bmod \mathbf{Z}$ with $0 \leqq \langle x \rangle < 1$. We now introduce the Stickelberger elements. For any positive integer N, consider

$$\vartheta_k(N) = (N^{k-1}/k) \sum_{\substack{t=1 \\ (t,N)=1}}^{N} \mathbf{B}_k\left(\left\langle \frac{t}{N} \right\rangle\right) [t]^{-1} \in \mathbf{Q}[(\mathbf{Z}/N\mathbf{Z})^*].$$

More generally, for any integer b, form the element

$$\vartheta_k(b; N) = (N^{k-1}/k) \sum_{\substack{t=1 \\ (t,N)=1}}^{N} \mathbf{B}_k\left(\left\langle \frac{bt}{N} \right\rangle\right) [t]^{-1} \in \mathbf{Q}[(\mathbf{Z}/N\mathbf{Z})^*].$$

Also, for use in Chap. 4, it is convenient to have notation for a minor modification of these elements. For any $\alpha = \Sigma a_i [x_i] \in \mathbf{Q}[\mathbf{Z}/N\mathbf{Z})^*]$ we write $\hat{\alpha}$ for $\Sigma a_i [x_i]^{-1}$. Similarly, for an ideal $\mathfrak{a}$ of the ring $\mathbf{Z}[(\mathbf{Z}/N\mathbf{Z})^*]$ we write $\hat{\mathfrak{a}}$ for the ideal of elements $\hat{\alpha}$ such that $\alpha \in \mathfrak{a}$. In particular, we have

$$\hat{\vartheta}_k(b; N) = (N^{k-1}/k) \cdot \sum_{\substack{t=1 \\ (t,N)=1}}^{N} \mathbf{B}_k\left(\left\langle \frac{bt}{N} \right\rangle\right) [t].$$

Note that $\vartheta_k(b; N)$ depends only on b mod N and that $[u]\,\vartheta_k(b; N) = \vartheta_k(u^{-1}b; N)$. Also of course $\vartheta_k(N) = \vartheta_k(1; N)$. The k^{th} *Stickelberger ideals* we define to be the ideals

$$S_k(N) = \mathbf{Z}[(\mathbf{Z}/N\mathbf{Z})^*] \cap \sum_{b \in \mathbf{Z}} \vartheta_k(b; N) \cdot \mathbf{Z}[(\mathbf{Z}/N\mathbf{Z})^*],$$

and

$$\hat{S}_k(N) = \mathbf{Z}[(\mathbf{Z}/N\mathbf{Z})^*] \cap \sum_{b \in \mathbf{Z}} \hat{\vartheta}_k(b; N) \cdot \mathbf{Z}[(\mathbf{Z}/N\mathbf{Z})^*].$$

If we restrict b to integers prime to p, we get ideals,

$$S'_k(N) = \mathbf{Z}[(\mathbf{Z}/N\mathbf{Z})^*] \cap \sum_{\substack{b \in \mathbf{Z} \\ (b,p)=1}} \vartheta_k(b; N) \cdot \mathbf{Z}[(\mathbf{Z}/N\mathbf{Z})^*],$$

and $\hat{S}'_k(N)$ defined similarly. The classical theorem of Stickelberger (cf. [61]) enables one to show that the elements of $2S_1(N)$ annihilate the ideal class group of $\mathbf{Q}(e^{2\pi i/N})$. We will not use this theorem in the present paper.

Let c be an integer prime to $2kN$ and to the denominators of the k^{th} Bernoulli polynomial. For such a choice of c the element

$$\vartheta_{k,c}(b; N) = (1 - c^k \cdot [c]^{-1}) \cdot \vartheta_k(b; N)$$

lies in $\mathbf{Z}[\mathbf{Z}/N\mathbf{Z})^*]$ (cf. [41] Theorem 2.1).

Now let $N = ap^n$ with $(a, p) = 1$ and $n \geqq 1$ and note that we have a compatibility $\vartheta_{k,c}(b; ap^{n+1}) \to \vartheta_{k,c}(b; ap^n)$ under the map $R^{(n+1)} \to R^{(n)}$. We may therefore pass to a limit to obtain an element

$$\vartheta_{k,c}(b; ap^\infty) = \varprojlim \vartheta_{k,c}(b; ap^n) \in R^{(\infty)}.$$

As usual, we set $\vartheta_{k,c}(ap) = \vartheta_{k,c}(1; ap^\infty)$.

Proposition 1. *If $\tau: R^{(\infty)} \to R^{(\infty)}$ is the twist automorphism of § 4, then*

$$\tau^{-1} \cdot \vartheta_{k,c}(ap^\infty) = \vartheta_{k+1,c}(ap^\infty).$$

This proposition is proved by showing that

$$\tau^{-1} \vartheta_{k,c}(ap^n) \equiv \vartheta_{k+1,c}(ap^n) \bmod p^n$$

for each n. For the details, see Theorem 2.1 (ii) of [41].

For the remainder of this section we specialize to the case $k = 2$. We will therefore write $\vartheta(b; N)$ for $\vartheta_2(b; N)$, $\vartheta_c(b; N)$ for $\vartheta_{2,c}(b; N)$, etc. We still assume that $N = ap^n$ with $(a, p) = 1$ and $n \geqq 1$.

If $\mathfrak{m}$ is any component of $R^{(n)}$ (cf. § 3), let $\hat{S}_\mathfrak{m}(N)$ and $\hat{S}'_\mathfrak{m}(N)$ denote the ideals in $R^{(n)}_\mathfrak{m}$ which are generated by the images of $\hat{S}(N)$ and $\hat{S}'(N)$ respectively. There is a surjection of ideals

$$\hat{S}'_\mathfrak{m}(ap^{n+1}) \to \hat{S}'_\mathfrak{m}(ap^n)$$

induced by the natural projection $R^{(n+1)}_\mathfrak{m} \to R^{(n)}_\mathfrak{m}$. We let $\hat{S}'_\mathfrak{m}(ap^\infty) \subseteq R^{(\infty)}_\mathfrak{m}$ be the ideal given by the projective limit as $n \to \infty$.

We let $\hat{\vartheta}_\mathfrak{m}(b; N)$ be the image of $\hat{\vartheta}(b; N)$ in $R^{(n)}_\mathfrak{m} \otimes \mathbf{Q}_p$. If $\mathfrak{m}$ is not associated to the basic character ω^2 then there is a smoothing number c for which $(1 - c^2[c])$ projects to a unit $u_c(n)$ in $R^{(n)}_\mathfrak{m}$. In this case we find that

$$\hat{\vartheta}_\mathfrak{m}(b; N) = u_c^{-1} \cdot (\text{image of } \hat{\vartheta}_c(b; N) \text{ in } R_\mathfrak{m})$$

and hence that $\hat{\vartheta}_\mathfrak{m}(b; N) \in R^{(n)}_\mathfrak{m}$. We refer to $\hat{\vartheta}_\mathfrak{m}(N) = \hat{\vartheta}_\mathfrak{m}(1; N)$ as the (principal) Stickelberger element at $\mathfrak{m}$ (of level N).

If $\mathfrak{m}$ is not associated to ω^{-2} we have then that $\hat{S}'_{\mathfrak{m}}(N)$ is generated by the Stickelberger elements $\hat{\vartheta}_{\mathfrak{m}}(b; N)$ where b runs through the divisors of N which are prime to p.

We define the "unhatted" versions, $\vartheta_{\mathfrak{m}}(b; N)$, $S_{\mathfrak{m}}(ap^n)$, $S'_{\mathfrak{m}}(ap^n)$ similarly.

Proposition 2. *Let $\mathfrak{m}$ be a pseudo-primitive component and not associated to ω^2 (resp. ω^{-2}) or the trivial character. Then $S'_{\mathfrak{m}}(N)$ (resp. $\hat{S}'_{\mathfrak{m}}(N)$) is generated by the $\vartheta_{\mathfrak{m}}(d; N)$ (resp. $\hat{\vartheta}_{\mathfrak{m}}(d; N)$) where d ranges through those divisors of r which are prime to p.*

For the definition of the integer r associated to a pseudo-primitive component $\mathfrak{m}$, see §3.

Corollary. *If $\mathfrak{m}$ is a-primitive and not associated to ω^2 or to the trivial character, then $S'_{\mathfrak{m}}(N)$ is the principal ideal in $R_{\mathfrak{m}}^{(n)}$ generated by the principal Stickelberger element $\vartheta_{\mathfrak{m}}(N)$.*

To prove this proposition we shall be translating results proved by Sinnott for the first Stickelberger ideal to the case of concern to us here (the second Stickelberger ideal). We refer to [61] for the details of the first two lemmas below.

Let Δ stand for the group $(\mathbf{Z}/N\mathbf{Z})^*/(\pm 1)$ and if b is an integer prime to N, let $[b]$ denote the element in the group ring $\mathbf{Z}[\Delta]$ determined by the image of b in Δ.

Lemma 1. (*cf. Lemma 2.1 of Sinnott [61]*). *Let ψ be any $\overline{\mathbf{Q}}_p$-valued character of Δ and f_ψ its conductor. Then if $\mathfrak{m}$ is any multiple of f_ψ,*

$$\sum_{\substack{t \bmod m \\ (t,m)=1}} \psi(t) \cdot \mathbf{B}_2\left(\left\langle \frac{t}{m} \right\rangle\right) = \frac{f_\psi}{m} \prod_{q|m} (1 - q\psi(q)) \cdot \mathbf{B}_2(\psi)$$

where q runs over the primes dividing m, and $\mathbf{B}_2(\psi)$ is the second generalized Bernoulli number associated to the character ψ.

Proof. This is an elementary calculation using the distribution relation satisfied by $\mathbf{B}_2$.

For any $\overline{\mathbf{Q}}_p$-valued character ψ of Δ define the projection operator

$$e_\psi = \frac{1}{|\Delta|} \sum_{\sigma \in \Delta} \psi^{-1}(\sigma) \cdot \sigma \in \overline{\mathbf{Q}}_p[\Delta].$$

For any prime number q, let

$$\gamma_q = \sum_{\chi: \Delta \to \overline{\mathbf{Q}}_p^*} \chi^{-1}(q) e_\chi \in \overline{\mathbf{Q}}_p[\Delta]$$

where the summation is taken over the even primitive Dirichlet characters of conductor N with values in $\overline{\mathbf{Q}}_p$. Note that γ_q lies in $\overline{\mathbf{Q}}_p[\Delta]$ and not just in $\overline{\mathbf{Q}}_p[\Delta]$.

For any positive divisor f of N let

$$s_f = \sum_t [t] \in \mathbf{Z}[\Delta]$$

where the summation is over those integers t modulo N which are relatively prime to N, and such that $t \equiv 1 \bmod f$. Let U denote the $\mathbf{Z}_p[\Delta]$-submodule of $\mathbf{Q}_p[\Delta]$

given by

$$U = \{\alpha_f : \alpha_f = (N/f) \cdot s_f \cdot \prod_{q|f} (1 - q\gamma_q) \text{ such that } 1 \leqq f \leqq N, p^n | f \text{ and } f | N\}.$$

In the above, the product is taken over the primes q which divide f.

Let w be the element

$$\sum_{\psi \neq 1} \mathbf{B}_2(\psi^{-1})/2 \cdot e_\psi \in \mathbf{Q}_p[\Delta]$$

where ψ runs through all nontrivial $\overline{\mathbf{Q}}_p$-valued characters of Δ.

Lemma 2. *One has*

$$(1 - e_1) \cdot \vartheta(d; N) = w \cdot \alpha_{N/d}$$

for $d < N$ and d a divisor of N. In particular,

$$(1 - e_1) \cdot S(N) = w \cdot U.$$

Proof. The second statement follows from the first because $w \cdot \alpha_1 = 0$. To prove the first statement, it is sufficient to check that

$$\rho_\psi((1 - e_1) \cdot \vartheta(d, N)) = \rho_\psi(w \cdot \alpha_{N/d})$$

for each character ψ of Δ where ρ_ψ is the homomorphism $\mathbf{Q}_p[\Delta] \to \overline{\mathbf{Q}}_p$ induced from ψ. For this, assume first that ψ is a nontrivial character and let $f = N/d$. Writing f_ψ for the conductor of ψ, consider the two cases:

$f_\psi \nmid f$:

In this case, $\rho_\psi(\vartheta(d; N)) = 0 = \rho_\psi(\alpha_{N/d})$ since on either side one can isolate a factor of the form

$$\rho_\psi\left(\sum_{t \equiv 1 \bmod f} [t]\right).$$

For details, see [61].

$f_\psi | f$:

In this case

$$\rho_\psi(\vartheta(d, N)) = N/2 \cdot \sum_{(t,N)=1} \psi^{-1}(t) \cdot \mathbf{B}_2(\langle t/f \rangle)$$

$$= N/2 \cdot (\varphi(N)/\varphi(f)) \cdot \sum_{(t,f)=1} \psi^{-1}(t) \cdot \mathbf{B}_2(\langle t/f \rangle)$$

where the second summation is over integers $t \bmod f$ which are, as indicated, relatively prime to f and φ is Euler's φ-function. Using Lemma 1, this becomes

$$\rho_\psi(\vartheta(d, N)) = N/2 \cdot (\varphi(N)/\varphi(f)) \cdot \mathbf{B}_2(\psi^{-1}) \cdot 1/f \cdot \prod_{q|f} (1 - q \cdot \psi^{-1}(q)). \qquad (1)$$

The term on the right is equal to $\rho_\psi(w \cdot \alpha_{N/d})$. For the trivial character one has also that $\rho_1(w \cdot \alpha_{N/d}) = 0$ since $\rho_1(w) = 0$. But $\rho_1(1 - e_1)$ is also zero. This completes the proof of Lemma 2.

We return now to the proof of Proposition 2. Let $\Theta_\mathfrak{m}$ denote the ideal in $R_\mathfrak{m}^{(n)}$ generated by all the elements $\vartheta_\mathfrak{m}(d, N)$ where d runs through the divisors of r, which are prime to p.

Let $\alpha_{N/d,\mathfrak{m}}$ denote the image of $\alpha_{N/d}$ in $R_\mathfrak{m}^{(n)} \otimes \mathbf{Q}_p$ under the projection $R^{(n)} \to R_\mathfrak{m}^{(n)}$ and let $\mathscr{A}_\mathfrak{m}$ denote the $R_\mathfrak{m}^{(n)}$-submodule in $R_\mathfrak{m}^{(n)} \otimes \mathbf{Q}_p$ generated by all the $\alpha_{N/d,\mathfrak{m}}$ where d runs through the divisors of r which are prime to p. The element w is a unit in $R_\mathfrak{m}^{(n)} \otimes \mathbf{Q}_p$ because $\mathfrak{m}$ is not associated to the trivial character. Hence multiplication by w induces an isomorphism

$$S_\mathfrak{m}/\Theta_\mathfrak{m} \cong U \otimes R_\mathfrak{m}^{(n)}/\mathscr{A}_\mathfrak{m}.$$

Our aim is to prove that the quotient modules above vanish.

Lemma 3. *For each prime number q dividing ap/r, the image $\gamma_{q,\mathfrak{m}}$ of γ_q in $R_\mathfrak{m}^{(n)} \otimes \mathbf{Q}_p$ vanishes.*

Proof. For each character ψ associated to the pseudo-primitive component $\mathfrak{m}$ we have $\rho_\psi(\gamma_q) = \psi(q) = 0$ since ψ has conductor divisible by ap/r and hence by q. Since γ_q is zero on each sheet of $\mathfrak{m}$, $\gamma_{q,\mathfrak{m}} = 0$.

Now suppose that α_f is one of the generators of U, i.e., that $p^n | f$. It will be enough to show that $\alpha_{f,\mathfrak{m}}$ is in $\mathscr{A}_\mathfrak{m}$. Let $r_0 = (r, p)$ and let $d_0 = (d, r_0)$. Then set $f_0 = N/d_0$. We claim that $\alpha_{f,\mathfrak{m}}$ is a multiple of $\alpha_{f_0,\mathfrak{m}}$ by an element of $R_\mathfrak{m}^{(n)}$. This will prove Proposition 2 since $\alpha_{f_0,\mathfrak{m}} \in \mathscr{A}_\mathfrak{m}$.

Now we have the formulae

$$\alpha_{f,\mathfrak{m}} = (N/f) \cdot s_{f,\mathfrak{m}} \cdot \prod_{q|f} (1 - q\gamma_{q,\mathfrak{m}}),$$

$$\alpha_{f_0,\mathfrak{m}} = (N/f_0) \cdot s_{f_0,\mathfrak{m}} \cdot \prod_{q|f_0} (1 - q\gamma_{q,\mathfrak{m}}).$$

Since $f/f_0 = d_0/d$ is prime to r (it is prime to p since by hypothesis d and d_0 are prime to p), hence the two products in the above expressions are the same by Lemma 3. For, as was noted earlier, by the assumption of pseudo-primitivity $(r, ap/r) = 1$. Also, it is clear that $s_{f,\mathfrak{m}}$ is a multiple of $s_{f_0,\mathfrak{m}}$ (indeed s_f is of s_{f_0}) and so Proposition 2 follows.

Finally, we consider the two special cases omitted from Proposition 2.

Proposition 2′. (i) *If $p > 3$ and $\mathfrak{m}$ is a pseudo-primitive component associated to ω^2, then $S'_\mathfrak{m}(N)$ is contained in the module generated by the set $\{\vartheta_\mathfrak{m}(d; N)\colon d | r, (d, p) = 1\}$. Furthermore, if q is a prime dividing r, then $q^2 \vartheta_\mathfrak{m}(1; N) - \vartheta_\mathfrak{m}(q; N) \in S'_\mathfrak{m}(N)$.*

(ii) *If $p > 3$ and $\mathfrak{m}$ is a pseudo-primitive component associated to χ_0 (the trivial character), then the module $(1 - e_1) S'_\mathfrak{m}(N)$ is generated by the set*

$$\{(1 - e_1)\vartheta_\mathfrak{m}(d; N)\colon d | r, (d, p) = 1\}.$$

(iii) *If $p = 3$ and $\mathfrak{m}$ is a pseudo-primitive component associated to χ_0, then the module $(1 - e_1) S'_\mathfrak{m}(N)$ is contained in the module generated by the set $\{(1 - e_1)\vartheta_\mathfrak{m}(d; N)\colon d | r, (d, p) = 1\}$. Furthermore, if q is a prime dividing r then*

$$(1-e_1)\,(q^2\,\vartheta_{\mathfrak{m}}(1;N)-\vartheta_{\mathfrak{m}}(q;N))\in(1-e_1)\,S'_{\mathfrak{m}}(N)\,.$$

Proof. Except for the statement that $q^2\,\vartheta_{\mathfrak{m}}(1;N)-\vartheta_{\mathfrak{m}}(q;N)$ is in $S'_{\mathfrak{m}}(N)$ in part (i) and the parallel statement in part (iii), the proof is, with some obvious modifications, the same as for Proposition 2. Note that the difficulty in part (i) is simply that the elements $\vartheta_{\mathfrak{m}}(c;N)$ are not necessarily in $R^{(n)}_{\mathfrak{m}}$, but only in $R^{(n)}_{\mathfrak{m}}\otimes\mathbf{Q}_p$.

To see that $q^2\,\vartheta_{\mathfrak{m}}(1;N)-\vartheta_{\mathfrak{m}}(q;N)$ is in $R^{(n)}$ and so also in $S'_{\mathfrak{m}}(N)$ one just observes that the usual proof for smoothing numbers (where the assumption is made that c is prime to N) works also in this case (cf. [41] Chap. 2, in particular, Theorem 2.1).

Remark. If in addition to the hypotheses of Proposition 2 we have that $N=ap$ (i.e., $n=1$), then $S'_{\mathfrak{m}}(N)=S_{\mathfrak{m}}(N)$. This follows easily from the fact that $\gamma_p\in R^{(n)}_{\mathfrak{m}}$ in this case.

In order to study the pseudo-primitive components we will need a further modification of the Stickelberger elements. Let $\mathfrak{m}$ be a primitive component with basic character χ of conductor ap/r where $r=q_1\cdots q_\nu$. The q_i are distinct primes and $(r, ap/r)=1$. For each $q_i\neq p$ let n_{q_i} be an integer such that $n_{q_i}\equiv q_i \bmod N/q_i$ and $n_{q_i}\equiv 1 \bmod q_i$. For any t dividing r, with $(t,p)=1$, set

$$\nu(t)=\prod_{q_i\mid t} q_i(n_{q_i})^{-1}\,,$$

$$\mu(t)=(-1)^{d(t)}$$

where $d(t)$ is the number of distinct prime divisors of t. Then for any integer s and any r' dividing r set

$$\vartheta^{(r')}(s;N)=\sum_{\substack{t\mid r'\\(t,p)=1}}\mu(t)\,\vartheta_2(\nu(t)s)\,.$$

Also, let $S^{(r')}_{\mathfrak{m}}(N)$ be the ideal of $R^{(n)}_{\mathfrak{m}}$, contained in $S'_{\mathfrak{m}}(N)$, given by the image in $R^{(n)}_{\mathfrak{m}}$ of

$$S^{(r')}_2(N)=\mathbf{Z}\,[(\mathbf{Z}/N\mathbf{Z})^*]\cap\sum_{\substack{b\in\mathbf{Z}\\(b,r'p)=1}}\vartheta^{(r')}_2(b;N)\,\mathbf{Z}\,[(\mathbf{Z}/N\mathbf{Z})^*]\,.$$

The following proposition is an analogue of Propositions 2 and 2′ and is proved in the same way. We omit the proof.

Proposition 3. (i) *If* $\mathfrak{m}$ *is pseudo-primitive and not associated to* χ_0, *nor to* ω^2 *if* $a=1$, *then*

$$S^{(r)}_{\mathfrak{m}}(N)=(\vartheta^{(r)}_{\mathfrak{m}}(1;N))\,.$$

(ii) *If* $\mathfrak{m}$ *is pseudo-primitive and associated to* χ_0, *then*

$$(1-e_1)\,S^{(r)}_{\mathfrak{m}}(N)=(1-e_1)\,(\vartheta^{(r)}_{\mathfrak{m}}(1;N))\,.$$

Proposition 4. *Let* $\mathfrak{m}$ *be a pseudo-primitive component of level* $N = ap^n$ *and let* ψ *be the basic character attached to* $\mathfrak{m}$. *Suppose that* ψ *is of conductor* ap/r *and that* $r_0 | r$. *Then for any divisor* d *of* N,

$$\rho_\psi(\vartheta_{\mathfrak{m}}^{(r_0)}(d; N)) = \tfrac{1}{2} c_d \cdot \mathbf{B}_2(\psi^{-1}) \cdot \prod_{q | r_0} (1 - q^2 \psi^{-1}(q))$$

for some integer c_d.

Proof. Recall that $r = q_1 \cdots q_v$ is a product of distinct primes, and that $(r, ap/r) = 1$. Suppose that $v = 1$ and let f_ψ be the conductor of ψ. If $q_1 = p$ the proposition is obvious in view of (1) since in this case the Euler factor is a unit. If $f_\psi \nmid f = N/d$ then the equation is satisfied with $c_d = 0$. If on the other hand $f_\psi | f$ and $q_1 \neq p$, we obtain from Eq. (1),

$$\begin{aligned}\rho_\psi(\vartheta_{\mathfrak{m}}^{(q_1)}(d; N)) &= \rho_\psi(\vartheta_{\mathfrak{m}}(d; N) - \vartheta_{\mathfrak{m}}(dqn_q^{-1}; N)) \\ &= \frac{N}{2f} \cdot \frac{\varphi(N)}{\varphi(f)} \cdot \mathbf{B}_2(\psi^{-1}) \cdot (1 - q^2 \psi^{-1}(q)).\end{aligned}$$

The general case is similar and we omit the calculation.

We have, also, analogous results for the "hatted" versions $\hat{\vartheta}^{(r')}(s; N)$, $\hat{S}_{\mathfrak{m}}^{(r')}(N)$ etc., defined in the evident manner.

§ 6. p-adic L*-functions*

Recall that the p-adic L-function $L_p(\chi, s)$ attached to *a* non-trivial, even, primitive p-adic Dirichlet character χ is the unique continuous function defined for $s \in \mathbf{Z}_p$ such that

$$L_p(\chi, 1 - k) = -(1 - \chi_k(p) p^{k-1}) \mathbf{B}_k(\chi_k)/k,$$

for $k = 1, 2, 3, \ldots$ Here $\chi_k =$ "$\chi\omega^{-k}$" is the primitive character associated to $\chi\omega^{-k}$ and

$$\mathbf{B}_k(\chi_k) = (1/f) \sum_{\substack{t=1 \\ (t,f)=1}}^{f} \mathbf{B}_k\left(\left\langle \frac{t}{N} \right\rangle\right) \cdot \chi_k(t),$$

where f is the conductor of χ_k.

Iwasawa has shown that if χ is of the first kind (i.e., with conductor not divisible by p^2) then there is a unique power series $G_p(\chi, T) \in \mathcal{O}_\chi[\![T]\!]$ such that

$$G_p(\chi, u^s - 1) = L_p(\chi, s) \text{ for all } s \in \mathbf{Z}_p.$$

Here $u = \kappa(\gamma)$ is chosen for later convenience (for the definitions of κ and γ see § 2); such a power series would exist for any p-adic unit $u \equiv 1 \bmod p$ and $u \not\equiv 1 \bmod p^2$. If χ is an arbitrary primitive even character then we may write χ uniquely in the form $\chi = \rho \cdot \chi_t$, where $\chi_t (= \chi_{\text{tame}})$ and ρ are of the first and second kinds respectively. (A p-adic Dirichlet character is said to be of the second kind if its conductor is a power of p and it has order a power of p). Iwasawa showed that if χ_t is non-trivial

$$G_p(\chi_t, \zeta u^s - 1) = L_p(\chi, s) \tag{1}$$

where $\zeta = \rho(u)^{-1}$. Similar statements hold even when χ_t is the principal character, although then there is a pole at $s=1$. For details, see [23] § 8 or [30].

Iwasawa gave an explicit construction of the power series $G_p(\chi, T)$ as follows. Suppose now that χ is a non-trivial primitive even character of conductor a or ap, with $(a,p)=1$. If $k \geqq 1$ and $\vartheta_{k,c}(ap^\infty) \in R^{(\infty)}$ is the k^{th} Stickelberger element smoothed by c (see § 5), denote by

$$G_{p,k,c}(\chi, T) \in \mathcal{O}_\chi[\![T]\!]$$

the image of $\vartheta_{k,c}(ap^\infty)$ under the following composition of homomorphisms:

$$\alpha_\chi\colon\ R^{(\infty)} = R^{(1)}[\![\Omega]\!] \xrightarrow[\chi]{} \mathcal{O}_\chi[\![\Omega]\!] \xrightarrow[\sigma_u]{\sim} \mathcal{O}_\chi[\![T]\!]. \tag{2}$$

Here we are considering χ as a homomorphism $(\mathbf{Z}/ap\mathbf{Z})^* \to \mathcal{O}_\chi^*$ even if the conductor of χ is a. The map σ_u is the unique continuous $\mathcal{O}_\chi$-linear isomorphism which maps $[u] \in \mathcal{O}_\chi[\![\Omega]\!]$ to $1+T$. If $\chi\omega^{-k}$ is not of p-power order, then the image of $1 - c^k[c]^{-1}$ under these homomorphisms is a unit power series $u_{p,k,c}(\chi, T)$ in $\mathcal{O}_\chi[\![T]\!]$. Under this hypothesis we define the k^{th} *Stickelberger power series attached to* χ

$$G_{p,k}(\chi, T) \in \mathcal{O}_\chi[\![T]\!]$$

to be the quotient power series $G_{p,k,c}/u_{p,k,c}$. It is easily seen to be independent of c.

Even if $\chi\omega^{-k}$ is p-power order the same construction still gives a power series $G_{p,k}(\chi, T) \in \mathcal{O}_\chi[\![T]\!]$ provided that $a > 1$. It is also the image of the element

$$\varprojlim (\vartheta(1; N) - (1/q^k)\vartheta(q; N)) \in \varprojlim R^{(n)} = R^{(\infty)}$$

under α_χ. Indeed, the equivalence of these two constructions shows that $G_p(\chi, T)$, a priori in the quotient field of $\mathcal{O}_\chi[\![T]\!]$, is actually in $\mathcal{O}_\chi[\![T]\!]$ itself.

Iwasawa's construction of $G_p(\chi, T)$ is in terms of the first Stickelberger power series. Specifically he proved that

$$G_p(\chi, T) = -G_{p,1}(\chi^{-1}\omega, T).$$

In view of Proposition 1 of § 5 we may also write this in terms of the k^{th} Stickelberger power series for any $k \geqq 1$,

$$G_p(\chi, T) = -G_{p,k}(\chi^{-1}\omega^k,\ u^{k-1}(1+T) - 1). \tag{3}$$

This follows easily from Proposition 1 of § 5 and the commutativity of the diagram

$$\begin{array}{ccc} R^{(\infty)} & \xrightarrow{\alpha_\chi} & \mathcal{O}_\chi[\![T]\!] \\ \Big\downarrow{\scriptstyle \tau^{-1}} & & \Big\downarrow \\ R^{(\infty)} & \xrightarrow[\alpha_{\chi\omega}]{} & \mathcal{O}_\chi[\![T]\!] \end{array} \qquad \begin{array}{c} T \\ \Big\downarrow \\ u^{-1}(1+T) - 1 \end{array}$$

where α_χ is the composite homomorphism in (2), and τ^{-1} is the inverse of the twist automorphism τ introduced in §4.

Let $\hat{\chi}$ denote the "dual" character, that is, $\hat{\chi} = "\omega\chi^{-1}"$, the primitive character attached to the product $\omega \cdot \chi^{-1}$. Recall from §2 that $h_p(\hat{\chi}, T)$ is the Iwasawa polynomial of $H_{\infty,\hat{\chi}}$. The *Main Conjecture* for **Q** ([23], §1; [8], §5) asserts:

Conjecture.[2] *Let χ be an even primitive Dirichlet character of conductor not divisible by p^2. Then as ideals of $\mathcal{O}_\chi[\![T]\!]$:*

$$(h_p(\hat{\chi}, T)) = (G_p(\chi, T)).$$

Remarks 1. If $\chi = \chi_0$ is the trivial character it will be convenient to define $G_p(\chi, T) = 1$ (though there is perhaps a more natural choice, cf. [23], §4). The conjecture then also makes sense for $\chi = \chi_0$. We note that for $\chi = \omega^2$, $p > 3$, $G_p(\chi, T)$ is a unit power series. This follows easily from the fact that $\mathbf{B}_2 = \frac{1}{6}$.

2. If χ is an odd character, then $G_p(\chi, T)$ is not defined, as the corresponding p-adic L-function is identically zero. There are no known examples for which $h_p(\hat{\chi}, T)$ is not equal to 1 in this case.

3. The main conjecture for **Q** as formulated above has been described by Greenberg [23]. In the article cited, Greenberg shows the equivalence between the main conjecture for **Q** and a broader conjecture involving p-adic L-functions attached to imprimitive Dirichlet characters over **Q**.

Coates has formulated a conjecture [8] (a main conjecture for any totally real field) which is more general than Greenberg's formulation in the sense that it concerns the p-adic L-functions attached to arbitrary totally real fields, but nevertheless it does not quite include Greenberg's since Coates considers only a restricted class of Dirichlet characters.

A crucial step in the direction of this conjecture is afforded by the analytic class number formula. One obtains from this classical formula two propositions, the first being essentially due to Iwasawa ([23], §5), the second using a theorem of Coates together with the p-adic residue formula of Leopoldt (cf. [24], Proposition 5).

If $f \in \mathcal{O}_\chi[\![T]\!]$ we write $\mu(f)$ for the largest integer such that $\pi^{-\mu(f)} f \in \mathcal{O}_\chi[\![T]\!]$ where π is a uniformizing parameter for $\mathcal{O}_\chi$. We may then write $\pi^{-\mu(f)} f$ in the form $f_0 \cdot u(T)$ where f_0 is a distinguished polynomial and $u(T)$ is a unit power series. We let $\lambda(f)$ be the degree of f_0.

Proposition 1. *Let F be a totally imaginary cyclic extension of* **Q**. *Then*

$$\sum_\chi \lambda(G_p(\chi, T)) = \sum_\chi \lambda(h_p(\hat{\chi}, T)), \quad \sum_\chi \mu(G_p(\chi, T)) = \sum_\chi \mu(h_p(\hat{\chi}, T)),$$

where the sums are taken over those even χ for which $F(\hat{\chi})$, the field attached to $\hat{\chi}$ by class field theory, is F, $\hat{\chi}$ being the corresponding dual characters.

Proposition 2. *Let F be a totally real cyclic extension of* **Q**. *Then*

$$\sum_\chi \lambda(G_p(\chi, T)) = \sum_\chi \lambda(h_p(\hat{\chi}, T)), \quad \sum_\chi \mu(G_p(\chi, T)) = \sum \mu(h_p(\hat{\chi}, T)),$$

where the sums are taken over those even χ for which $F(\chi) = F$, $\hat{\chi}$ being the corresponding dual character.

[2] See the theorem of §9

Using either of these we see that to prove the main conjecture it would be sufficient to show that the Iwasawa polynomial $h_p(\hat{\chi}, T)$ is *contained* in the ideal of $\mathcal{O}_\chi[\![T]\!]$ generated by $G_p(\chi, T)$ for each χ.

It remains to compare the Stickelberger *ideal* with Stickelberger power series. If $k=2$, and χ belongs to a pseudo-primitive component $\mathfrak{m}$ as in §3 and if

$$\alpha_{\mathfrak{m},\chi}\colon R_{\mathfrak{m}}^{(\infty)} \to \mathcal{O}_\chi[\![T]\!] \tag{4}$$

is the homomorphism such that composition with the natural projection $R^{(\infty)} \twoheadrightarrow R_{\mathfrak{m}}^{(\infty)}$ yields the homomorphism α_χ of (2), then we have

Proposition 3. *If χ is a non-trivial even character of conductor a or ap and $\chi \neq \omega^{-2}$ if $a=1$, then*

$$\alpha_{\mathfrak{m},\chi}(\hat{S}'_{\mathfrak{m}}(ap^\infty)) = G_{p,2}(\chi^{-1}, (1+T)^{-1}-1), \tag{5}$$

as ideals of $\mathcal{O}_\chi[\![T]\!]$.

Proof. In the case where $\mathfrak{m}$ is a-primitive, this follows immediately from the relation

$$\alpha_{\mathfrak{m},\chi}(\hat{\vartheta}_{\mathfrak{m}}(1; ap^\infty)) = G_{p,2}(\chi^{-1}, (1+T)^{-1}-1)$$

since it is clear from the corollary to Proposition 2 of §5 that $\hat{S}'_{\mathfrak{m}}(ap^\infty) = (\hat{\vartheta}_{\mathfrak{m}}(1; ap^\infty))$. More generally, if $\mathfrak{m}$ is pseudo-primitive and not associated to χ_0 or to ω^{-2} it follows from Proposition 2 of §5 that

$$\hat{S}'_{\mathfrak{m}}(ap^\infty) = \{\hat{\vartheta}_{\mathfrak{m}}(d; ap^\infty)\colon d \mid r,\ (d \not\mid p)\}.$$

To see this we just observe that

$$\{\hat{\vartheta}_{\mathfrak{m}}(d; ap^\infty)\colon d \mid r,\ d \not\mid p\}_{(1+T)^{p^s}-1} = \{\hat{\vartheta}_{\mathfrak{m}}(d; ap^s)\colon d \mid r,\ d \not\mid p\}$$

where $M_{(1+T)^{p^s}-1}$ denotes $M/((1+T)^{p^s}-1)M$. Now since χ is of conductor a or ap, $\alpha_{\mathfrak{m},\chi}(\hat{\vartheta}_{\mathfrak{m}}(d; ap^\infty)) = 0$ for $d \mid r$, $(d,p)=1$, and so again we have (5).

When $\mathfrak{m}$ is associated to ω^{-2} and $p>3$ the same argument shows that $\hat{S}'_{\mathfrak{m}}(ap^\infty) \subseteq (\hat{\vartheta}_{\mathfrak{m}}(1; ap^\infty))$ by Proposition 2′ of §5. However, as in this case $a \neq 1$, by the same proposition there is a $q \mid r$, $q \neq p$, such that

$$\varprojlim_{n\to\infty} \{q^2\,\hat{\vartheta}_{\mathfrak{m}}(1; ap^n) - \hat{\vartheta}_{\mathfrak{m}}(q; ap^n)\} \in \hat{S}'_{\mathfrak{m}}(ap^\infty).$$

Applying α_χ again gives the desired relation. The remaining cases where $\mathfrak{m}$ is associated to χ_0 also follow directly from Proposition 2′ using that $\rho_\chi(1-e_1)=1$.

§7. Iwasawa theory (in terms of components)

Let K be a number field, Galois over $\mathbf{Q}$, with abelian (but not necessarily finite) Galois group. Let L/K be an algebraic p-abelian extension (also not necessarily finite: a union of finite p-abelian extensions) with Galois group G. We suppose that $L/\mathbf{Q}$ is Galois, and we view G as a $\mathbf{Z}_p[\![\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})]\!]$ module via the usual conjugation operation.

Definition 1. *The extension L/K is said to be of type $\mathfrak{m}$ if the* $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ *module G can be given a $\bar{\eta}_{-1}$ "yoked module structure". It is equivalent to require that the kernel of $\bar{\eta}_{-1}: \mathbf{Z}_p[\![\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})]\!] \twoheadrightarrow R_{\mathfrak{m}}^{(\infty)}$ annihilate the module G.*

Remark. It is important to notice that our yoke $\bar{\eta}_{-1}$ has a twist inherent in it, and therefore an extension L/K of type $\mathfrak{m}$ where $\mathfrak{m}$ where $\mathfrak{m}$ is an *even* component will have the property that a complex conjugation of K acts as -1 on G.

Definition 2. *A finite extension L/K is said to be everywhere unramified if there is an algebraic number field of finite degree $K' \subset K$ and an $L' \subset L$ containing K' such that $L = L' \cdot K$ and L'/K' is everywhere unramified. In general an extension L/K will be said to be everywhere unramified if it is a union of finite everywhere unramified extensions.*

We shall be especially interested in everywhere unramified abelian extensions of type $\mathfrak{m}$ for some component $\mathfrak{m}$. More precisely, let $\mathfrak{m}$ be a component not necessarily primitive. Let $F_{\mathfrak{m}}^{+}$ denote the finite (real) abelian extension field of $\mathbf{Q}$ 'cut out' by the set of Dirichlet characters of conductor dividing ap belonging to $\mathfrak{m}$. That is, if S denotes this set of characters,

$$\mathrm{Gal}(\bar{\mathbf{Q}}/F_{\mathfrak{m}}^{+}) = \bigcap_{\chi \in S} \ker(\chi)$$

where the χ's are viewed as characters on $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Set $F_{\mathfrak{m}} = F_{\mathfrak{m}}^{+}(\zeta_p)$.

Recall that $\mathbf{Q}_\infty$ is the unique $\mathbf{Z}_p$-extension of $\mathbf{Q}$ and set $K_{\mathfrak{m}} = F_{\mathfrak{m}} \cdot \mathbf{Q}_\infty$. Let $L_{\mathfrak{m}}$ denote the *maximal* everywhere unramified abelian extension of $K_{\mathfrak{m}}$ of type $\mathfrak{m}$. Set $H_{\mathfrak{m}} = \mathrm{Gal}(L_{\mathfrak{m}}/K_{\mathfrak{m}})$.

The connection between $H_{\mathfrak{m}}$ and the $\mathcal{O}_\chi$-modules $H_{\infty,\chi}$ introduced in §2 is as follows. Let ψ be a character belonging to $\mathfrak{m}$ of conductor dividing ap. Let $H_{\mathfrak{m},\psi}$ denote the $\mathcal{O}_\psi[\![T]\!]$-module obtained from $H_{\mathfrak{m}}$ via the change of scalars

$$R_{\mathfrak{m}}^{(\infty)} = R_{\mathfrak{m}}^{(1)}[\![\Omega]\!] \longrightarrow \mathcal{O}_\psi[\![\Gamma]\!] \xrightarrow[\sigma_u]{\sim} \mathcal{O}_\psi[\![T]\!]. \tag{1}$$

Here σ_u is the same map as in (1) of §6. Then let $V_{\mathfrak{m},\psi}$ denote the K_ψ-vector space

$$V_{\mathfrak{m},\psi} = H_{\mathfrak{m},\psi} \otimes_{\mathcal{O}_\psi} K_\psi .$$

It inherits a continuous action of Γ.

Now let χ denote the character $(\psi\omega)^{-1}$ and let $H_{\infty,\chi} = H_{\infty,\chi}(F_{\mathfrak{m}})$ be the module studied in §2 with $F = F_{\mathfrak{m}}$. (Note that $F_{\mathfrak{m}} \cap \mathbf{Q}_\infty = \mathbf{Q}$ so this *is* defined). As previously we let V_χ be the corresponding K_χ-vector space. Then the following proposition is an immediate consequence of the definitions of H_∞ and $H_{\mathfrak{m}}$. Note that $\mathcal{O}_\psi = \mathcal{O}_\chi$.

Proposition. *The natural map $H_\infty \to H_{\mathfrak{m}}$ induces an isomorphism of $\mathcal{O}_\chi$-modules*

$$H_{\infty,\chi} \xrightarrow{\alpha} H_{\mathfrak{m},\psi}$$

and hence also of K_χ-vector spaces, $V_\chi \xrightarrow{\sim} V_{\mathfrak{m},\psi}$. The relation between the $\mathcal{O}_\chi[\![T]\!]$-module structures on domains and ranges is given by

$$u \cdot \alpha((1+T) \cdot x) = (1+T)^{-1} \cdot \alpha(x)$$

for $x \in H_{\infty,\chi}$ (or V_χ).

Remark. As Galois-modules the isomorphism α is of course compatible with the actions on range and domain. What we have done here is to introduce a 'twisted' action of $\mathcal{O}_\chi[\![T]\!]$ on $H_{\mathfrak{m},\chi}$ via its yoke whereas the action on $H_{\infty,\chi}$ has been left untouched. Our purpose in doing this is to lay the groundwork for Chap. 5 in which this twisted action will occur naturally on a certain quotient of $H_{\mathfrak{m},\chi}$.

§ 8. Virtually unramified extensions

Our main construction will not necessarily produce an everywhere unramified extension (Chap. 5, §6) if $\mathfrak{m}$ is not a-primitive. We shall therefore study a more general type of extension in this section.

Recall the standard terminology: $\mathfrak{m}$ is a component of $\mathbf{Z}_p[(\mathbf{Z}/ap^n\mathbf{Z})^*]$. We suppose that $\mathfrak{m}$ is pseudo-primitive with basic character of conductor ap/r. Let K denote a subfield of $\mathbf{Q}(\zeta_{ap^\infty})$.

Definition. *An abelian extension L/K is said to be virtually unramified of type $\mathfrak{m}$ if L/K is of type $\mathfrak{m}$ and if it is unramified except possibly at primes of residual characteristics dividing a.*

In the notation of the previous section, if $K_\mathfrak{m} = F_\mathfrak{m} \cdot \mathbf{Q}_\infty$, let $L^\#_\mathfrak{m}$ denote the *maximal* virtually unramified extension of $K_\mathfrak{m}$ so that we have the tower of fields

$$H^\#_\mathfrak{m} \left\{ \begin{array}{l} L^\#_\mathfrak{m} \\ | \\ \left.\begin{array}{l} L_\mathfrak{m} \\ | \end{array}\right\} I_\mathfrak{m} \\ K_\mathfrak{m} \end{array} \right\} H_\mathfrak{m} \tag{1}$$

with indicated Galois groups. If ψ is a character belonging to $\mathfrak{m}$, let $H^\#_{\mathfrak{m},\psi}$ denote the base change of $H^\#_\mathfrak{m}$ via the change of scalars (1) of §1.7.

Set

$$V^\#_{\mathfrak{m},\psi} = H^\#_{\mathfrak{m},\psi} \underset{\mathcal{O}_\psi}{\otimes} K_\psi .$$

We have natural mappings

$$H^\#_{\mathfrak{m},\psi} \to H_{m,\psi}; \quad V^\#_{\mathfrak{m},\psi} \to V_{\mathfrak{m},\psi} .$$

Proposition 1. *If $\mathfrak{m}$ is pseudo-primitive (notation as above) and if L/K is a virtually unramified extension of type $\mathfrak{m}$, then the primes of L which ramify over K have residual characteristics dividing r and different from p.*

Proof. Fix a prime q which divides a but not r. We may suppose that L is a finite extension of $\mathbf{Q}$. Let $L_0 \subset L$ be the maximal subextension which has the property that L_0/K is unramified at primes of residual characteristic q. By class field theory, the Galois group $\mathrm{Gal}(L/L_0)$ is isomorphic to a quotient of

$$\prod_{\lambda | q} \mathcal{O}(K_\lambda)^*$$

where K_λ is the completion of K at λ, λ runs through all primes of K of residual characteristic q, and $\mathcal{O}(K_\lambda)$ is the ring of integers of K_λ.

Since $q \neq p$ and L/L_0 is a p-extension, $\mathrm{Gal}(L/L_0)$ is, more precisely, a quotient of

$$\prod_{\lambda|q} k_\lambda^*$$

where k_λ is the residue field of K_λ.

Let $v \geqq 0$ be such that $K \subseteq \mathbf{Q}(\zeta_{ap^v})$. The natural action of

$$\mathrm{Gal}(\mathbf{Q}(\zeta_{ap^v})/\mathbf{Q}) = (\mathbf{Z}/ap^v\mathbf{Z})^*$$

on $\prod_{\lambda|q} k_\lambda^*$ factors through the quotient

$$(\mathbf{Z}/ap^v\mathbf{Z})^* \to \left(\mathbf{Z}\Big/\frac{ap^v}{q}\cdot\mathbf{Z}\right)^*.$$

Consequently the same is true for the action of $(\mathbf{Z}/ap^v\mathbf{Z})^*$ on $\mathrm{Gal}(L/L_0)$. But $\mathrm{Gal}(L/L_0)$ is a yoked bimodule of type $\mathfrak{m}$ ([it is a bi-submodule of $\mathrm{Gal}(L/K)$]) and since every character belonging to $\mathfrak{m}$ has conductor divisible by q, it follows easily that $\mathrm{Gal}(L/L_0)$ vanishes.

Corollary. *If $\mathfrak{m}$ is a-primitive, then a virtually unramified extension of type $\mathfrak{m}$ is everywhere unramified.*

Proposition 2. *Let $\mathfrak{m}$ be pseudo-primitive and ψ a character belonging to $\mathfrak{m}$ such that a divides the conductor of ψ. Then the natural surjection $H^*_{\mathfrak{m},\psi} \to H_{\mathfrak{m},\psi}$ has finite kernel and so induces an isomorphism*

$$V^*_{\mathfrak{m},\psi} \simeq V_{\mathfrak{m},\psi}.$$

Proof. As in the proof of Proposition 1 above, using class field theory we may obtain $I_{\mathfrak{m}}$ as a quotient of some explicit $\mathbf{Z}_p$-module of finite type (there being only finitely many primes of $K_{\mathfrak{m}}$ lying above any rational prime). Moreover, $I_{\mathfrak{m}}$ is a product of $\mathbf{Z}_p$-modules on each of which the natural action of $\varprojlim \mathbf{Z}_p[(\mathbf{Z}/ap^n\mathbf{Z})^*]$ factors through the projection

$$\varprojlim \mathbf{Z}_p[(\mathbf{Z}/ap^n\mathbf{Z})^*] \to \varprojlim \mathbf{Z}_p\left[\left(\mathbf{Z}\Big/\frac{ap^n}{q}\mathbf{Z}\right)^*\right]$$

for some $q|r$, $q \neq p$.

For each such q we may find an integer $\alpha_q \bmod ap$ such that $\alpha_q \equiv 1 \bmod \left(\frac{ap}{q}\right)$ and $\psi(\alpha_q) \neq 1$. Then $\prod_{q|r} (\psi(\alpha_q) - 1)$ annihilates $I_{\mathfrak{m},\psi} = I_{\mathfrak{m}} \underset{R^{(1)}_{\mathfrak{m}}}{\otimes} \mathcal{O}_\psi$, which is therefore a finite group. The proposition follows.

§ 9. *Our Main theorem*

Let $\mathfrak{X}$ be the set of pseudo-primitive components of the following types.

(i) of level $N = p^n$ and with basic character ω^{-2}

(i) of level $N = p^n$ and with basic character χ_0 (the trivial character)

(iii) of level $N = ap^n$ and with $\hat{S}'_{\mathfrak{m}}(ap)$ the unit ideal in $R^{(1)}_{\mathfrak{m}}$.

It will be convenient to separate the pseudo-primitive components $\mathfrak{m} \notin \mathfrak{X}$ into two types. To distinguish these types let ψ be the basic character associated to $\mathfrak{m}$ and write

$$\psi = \psi_{p'} \cdot \omega^k$$

where $\psi_{p'}$ is a character of conductor prime to p, ω is the Teichmüller character and k is an integer, $0 \leqq k < p-1$. We will say that we are in case (1) if either of the following conditions hold

(a) $\psi_{p'}(p) \neq 1$

(b) $k \neq -1$.

Otherwise we say that we are in case (2).

In Chap. 4, § 3 we will define an ideal $\mathfrak{b}_{\mathfrak{m}}^{(n)}$ for any pseudo-primitive component. In case (2) we define a modification of this ideal, $\mathfrak{b}_{\mathfrak{m}}^{*(n)}$, in Chap. 5, § 5. This depends on the choice of integers κ and l (not to be confused with the k appearing above) which themselves depend on $\mathfrak{m}$. Rather than distinguish the two cases we will adopt the convention that for the rest of this section $\mathfrak{b}_{\mathfrak{m}}^{(n)}$ will refer to $\mathfrak{b}_{\mathfrak{m}}^{*(n)}$ in case (2). We hope that this will not lead to any confusion. Also we will define κ to be zero in case (1). Then for any pseudo-primitive component $\mathfrak{m} \notin \mathfrak{X}$ we shall produce two objects:

an ideal $\mathfrak{b}_{\mathfrak{m}}^{(n)} \subset R_{\mathfrak{m}}^{(n)}$

an extension of type $\mathfrak{m}$, $L_{\mathfrak{m}}^{(n)}/K_{\mathfrak{m}}$, which is virtually unramified in the sense of § 8. These constructions have the following properties.

(I) The ideal $\mathfrak{b}_{\mathfrak{m}}^{(n)}$ is closely related to the Stickelberger ideal. Explicitly, if n_{q_i} is an integer such that $n_{q_i} \equiv 1 \bmod q_i$ and $n_{q_i} \equiv q_i \bmod (N/q_i)$, then

$$(1 - l[l])^{\kappa} \prod_{\substack{q_i \neq p \\ q_i | r}} (q_i[n_{q_i}] - 1)\, \mathfrak{b}_{\mathfrak{m}}^{(n)} \subseteq \hat{S}'_{\mathfrak{m}}(N). \tag{1}$$

(II) The extension is 'large'. Explicitly, if $G_{\mathfrak{m}}^{(n)} = \mathrm{Gal}(L_{\mathfrak{m}}^{(n)}/K_{\mathfrak{m}})$ is the Galois group viewed as an $R_{\mathfrak{m}}^{(\infty)}$-module, and $\Phi_{\mathfrak{m}}^{(n)}$ is the $R_{\mathfrak{m}}^{(\infty)}$-fitting ideal of $G_{\mathfrak{m}}^{(n)}$, there is an ideal $\mathfrak{A}_{\mathfrak{m}} \subseteq R_{\mathfrak{m}}^{(\infty)}$ of finite index (and independent of n) such that $\mathfrak{A}_{\mathfrak{m}} \Phi_{\mathfrak{m}}^{(n)}$ is contained in the inverse image of $\mathfrak{b}_{\mathfrak{m}}^{(n)}$ in $R_{\mathfrak{m}}^{(\infty)}$, for all $n \geqq 1$. (The ideal $\mathfrak{A}_{\mathfrak{m}}$ can be taken to be the unit ideal in case (1)). Moreover, $L_{\mathfrak{m}}^{(n)}/K_{\mathfrak{m}}$ is 'virtually unramified', i.e., it is a p-extension unramified outside primes dividing a.

Remarks. (i) In each of types (i)–(iii) for the component $\mathfrak{m} \in \mathfrak{X}$ one checks that $G_p(\text{“}\psi\omega^2\text{”}, T)$ is a unit power series for any ψ attached to $\mathfrak{m}$. In the first two cases this is true by remark (I) of § 6. In the third case evaluating at $T = u^{-1} - 1$ and using the relations of § 6 (assuming that $\psi \neq \omega^2, \chi_0$),

$$G_p(\text{“}\psi\omega^2\text{”}, u^{-1} - 1) = -(1 - \psi(p)\, p)\, \mathbf{B}_2(\psi)/2 \in \mathcal{O}_{\psi}.$$

Now under the hypothesis that $\hat{S}'_{\mathfrak{m}}(ap)$ is the unit ideal we have that $\rho_{\psi^{-1}}(\hat{S}'_{\mathfrak{m}}(ap)) = \mathcal{O}_{\psi}$. But by the explicit formulas in the proof of Lemma 2 of § 5 every element of $\rho_{\psi^{-1}}(\hat{S}'_{\mathfrak{m}}(ap))$ is a multiple of $\mathbf{B}_2(\psi)$. Hence $\mathbf{B}_2(\psi)$ is a unit mod p and this shows that $G_p(\text{“}\psi\omega^2\text{”}, T)$ is a unit power series.

(ii) The ideal $\mathfrak{b}_{\mathfrak{m}}^{(n)}$ is defined to be the annihilator in $R_{\mathfrak{m}}^{(n)}$ of a certain finite subgroup, generated by divisors of degree zero with support on certain cusps, of the p-divisible group of a certain specific abelian variety quotient of $J_1(ap^n)$ (see Chap. 4 and 5). The action of $R_{\mathfrak{m}}^{(n)}$ on this p-divisible group is via the 'diamond operators'.

(iii) We show that if $\mathfrak{m}$ is a-primitive and we are in case (1) then the inclusion $\mathfrak{b}_{\mathfrak{m}}^{(n)} \subseteq \hat{S}'_{\mathfrak{m}}(N)$ of (1) is actually an equality. By the corollary to Proposition 2 of § 5 this ideal is principal, a generator being the principal Stickelberger element $\hat{\vartheta}_{\mathfrak{m}}(N)$. In general, we show that $\mathfrak{b}_{\mathfrak{m}}^{(n)}$ is a Gorenstein ideal in the sense that $R_{\mathfrak{m}}^{(n)}/\mathfrak{b}_{\mathfrak{m}}^{(n)}$ is a Gorenstein ring (Appendix, Proposition 4). We note that any principal ideal in $R_{\mathfrak{m}}^{(n)}$ is Gorenstein.

Let $\mathfrak{b}_{\mathfrak{m}}^{(\infty)} \subseteq R_{\mathfrak{m}}^{(\infty)}$ denote the intersection of the inverse images of the ideals $\mathfrak{b}_{\mathfrak{m}}^{(n)}$ under the natural projection $R_{\mathfrak{m}}^{(\infty)} \to R_{\mathfrak{m}}^{(n)}$ for $n = 1, 2, \cdots$. Recall that $H_{\mathfrak{m}}^{\#}$ is the Galois group of the maximal virtually unramified extension of $K_{\mathfrak{m}}$ of type $\mathfrak{m}$ (see § 7 and § 8 (1)). Let $\Phi_{\mathfrak{m}}^{\#}$ denote its Fitting ideal in $R_{\mathfrak{m}}^{(\infty)}$.

Proposition 1. *Assume that* $\mathfrak{m} \notin \mathfrak{X}$. *Then there is an ideal* $\mathfrak{A}_{\mathfrak{m}} \subseteq R_{\mathfrak{m}}^{(\infty)}$ *of finite index such that* $\mathfrak{A}_{\mathfrak{m}} \cdot \Phi_{\mathfrak{m}}^{\#}$ *is contained in* $\mathfrak{b}_{\mathfrak{m}}^{(\infty)}$.

Proof. The proposition follows from assertion II and the fact that the $R_{\mathfrak{m}}^{(\infty)}$-module $H_{\mathfrak{m}}^{\#}$ maps surjectively onto $G_{\mathfrak{m}}^{(n)}$ for every n, in view of Appendix (10).

Proposition 2. *Let* ψ *be an even character of conductor a or ap belonging to a pseudo-primitive component* $\mathfrak{m} \notin \mathfrak{X}$. *Then the Iwasawa polynomial* $h_{\mathfrak{m},\psi}(T)$ *of* $H_{\mathfrak{m},\psi}$ *satisfies the relation*

$$(1 - l\psi(l)[l](T))^{\kappa} \prod_{\substack{q_i | r \\ q_i \neq p}} (1 - q_i \psi(n_{q_i})[q_i](T)) h_{\mathfrak{m},\psi}(T) \subseteq (G_{p,2}(\psi^{-1}, (1+T)^{-1} - 1))$$

Proof. First, to interpret the proposition we note that we have written $[q_i](T)$ for the power series in T associated to it, namely if q_i is viewed as an element of $\mathbf{Z}_p$, $q_i = u^{a_i}$ for some $a_i \in \mathbf{Z}_p$, then $[q_i](T) = (1+T)^{a_i}$. (Note that $q_i \equiv 1 \bmod p$.)

By considering the relation (1) for each $n \geqq 1$ we obtain the inclusion of $R_{\mathfrak{m}}^{(\infty)}$-ideals,

$$y_{\mathfrak{m}} \cdot \mathfrak{b}_{\mathfrak{m}}^{(\infty)} \subseteq S'_{\mathfrak{m}}(ap^{\infty}) \tag{2}$$

where $y_{\mathfrak{m}}$ is given by the formula

$$y_{\mathfrak{m}} = \varprojlim_{n} (1 - l[l])^{\kappa} \prod_{\substack{qi | r \\ q_i \neq p}} (1 - q_i [n_{qi}^{(n)}]).$$

Here $n_{qi}^{(n)}$ is any integer $\bmod ap^n$ satisfying $n_{qi}^{(n)} \equiv q_i \bmod (ap^n/q_i)$, $n_{qi}^{(n)} \equiv 1 \bmod q_i$. We now apply the map $\alpha_{\mathfrak{m},\psi}$ to both sides of (2). From proposition 3 of § 6 we have that $\alpha_{\mathfrak{m},\psi}(S'_{\mathfrak{m}}(ap^{\infty})) = (G_{p,2}(\psi^{-1}, (1+T)^{-1} - 1)$. An easy calculation shows that

$$\alpha_{\mathfrak{m},\psi}(y_{\mathfrak{m}}) = (1 - l\psi(l)[l](T))^{\kappa} \prod (1 - q_i \psi(q_i)[q_i](T)).$$

By the proposition of § 7, $H_{\mathfrak{m},\psi}^{\#}$ and $H_{\mathfrak{m},\psi}$ have the same Iwasawa polynomial $h_{\mathfrak{m},\psi}(T)$. By the corollary to Proposition 2 of the appendix, there is an ideal of finite index $\mathfrak{A}'_{\mathfrak{m}} \subseteq R_{\mathfrak{m}}^{(\infty)}$ such that

$$\mathfrak{A}'_{\mathfrak{m}} \cdot h_{\mathfrak{m},\psi}(T) \subseteq \alpha_{\mathfrak{m},\psi}(\mathfrak{b}_{\mathfrak{m}}^{(\infty)}).$$

So, applying $\alpha_{\mathfrak{m},\psi}$ to both sides of (2) the proposition follows easily from Lemma 3 of the appendix.

Recall that for an even primitive non-trivial character χ of the first kind we have the power series $G_p(\chi, T)$ of §6 with the property that $G_p(\chi, u^s - 1) = L_p(\chi, s)$. We also have the Iwasawa polynomial $h_p(\hat{\chi}, T)$ of §2.

Theorem. *The main conjecture for* $\mathbf{Q}$ *and for odd primes* p *is true (cf. § 6), i.e., for each even primitive character* χ *of conductor not divisible by* p^2,

$$(h_p(\hat{\chi}, T)) = (G_p(\chi, T)).$$

Proof. We use the notation of §7. Let ψ denote the character $\chi\omega^{-2}$. Then ψ is a character of conductor a or ap (with $(a, p) = 1$), and we may view it in either case as giving a homomorphism $(\mathbf{Z}/ap\,\mathbf{Z})^* \to \mathcal{O}_\chi^*$. As such it is attached to some pseudo-primitive component $\mathfrak{m}$. By the proposition of §7 the Iwasawa polynomial of $H_{\infty,\hat{\chi}}$ is $h_{\mathfrak{m},\psi}(u^{-1}(1+T)^{-1} - 1)$. By Proposition 2, if $\mathfrak{m} \notin \mathfrak{X}$, then

$$(1 - \psi(l)[l])^\kappa \prod_{\substack{q_i | r \\ q_i \neq p}} (1 - \psi(n_{q_i})[q_i^{-1}]) h_{\mathfrak{m},\psi}(u^{-1}(1+T)^{-1} - 1)$$

$$\subseteq G_{p,2}(\psi^{-1}, u(1+T) - 1),$$

where here and subsequently in the proof we abbreviate $[q_i^{-1}](T)$ to $[q_i^{-1}]$. (We have used here that in the change of variable $T \mapsto u^{-1}(1+T)^{-1} - 1$, the element $[q_i]$ gets taken to $q_i^{-1}[q_i^{-1}]$.) We can rewrite this in terms of χ, using (3) of §6,

$$(1 - \psi(l)[l^{-1}])^\kappa \prod_{\substack{q_i | r \\ q_i \neq p}} (1 - \psi(n_{q_i}) \cdot [q_i^{-1}]) h_p(\hat{\chi}, T) \subseteq G_p(\chi, T).$$

Let us write $[q_1^{-1}] = (1+T)^{\alpha_i}$. Then the power series $1 - \psi(n_{q_i})(1+T)^{\alpha_i}$ has a zero if and only if $\psi(n_{q_i})$ is a p-power root of unity. This root is then a solution to the equation $(1+T)^{p^r} = 1$ for some r. If the root is non-zero, i.e., of the form $\zeta - 1$ for some non-trivial p-power root of unity ζ, then

$$G_p(\chi, \zeta - 1) = L_p(0, \chi\rho) = -(1 - \chi\rho\omega^{-1})(p))\,\mathbf{B}_1(\chi\rho\omega^{-1}) \neq 0$$

where ρ is the character of p-power conductor such that $\rho(\gamma) = \zeta^{-1}$, and the equation follows from (1) of §6, If, on the other hand, the root is at $T = 0$, then $G_p(\chi, 0)$ is again non-zero if $\chi\omega^{-1}(p) \neq 1$. But if $\chi\omega^{-1}(p) = 1$ then Ferrero and Greenberg have computed the multiplicity of the zero at $T = 0$ for both $h_p(\hat{\chi}, T)$ and $G_p(\chi, T)$ and they are both equal to 1 (cf. [22] and [18]). Here we only need the result for $G_p(\chi, T)$. Exactly the same analysis applies to the zeroes of $(1 - \psi(l)[l^{-1}])$. In all cases we can deduce the relation

$$G_p(\chi, T) \mid h_p(\hat{\chi}, T).$$

Finally, for those characters ψ associated to an $\mathfrak{m} \in \mathfrak{X}$, we have the same relation by remark (i) at the beginning of this section. This is sufficient to prove the theorem either by Proposition 1 or 2 of §6.

§ 10. Arithmetic applications

(i) Ralph Greenberg has shown how the main conjecture implies a conjecture of G. Gras concerning the structure of the ideal class group of real abelian fields.

Special cases of this conjecture were implicit in the work of Kummer and Iwasawa. We quote from Greenberg's paper [24].

Let $p > 2$ be a prime number and consider K a real abelian finite extension of $\mathbf{Q}$ whose degree over $\mathbf{Q}$ is prime to p.

For any cyclic subextension $F/\mathbf{Q}$ of $K/\mathbf{Q}$ suppose that f is the minimal integer such that $F \subseteq \mathbf{Q}(\zeta_f)$ for ζ_f a primitive f^{th} root of unity and let

$$\alpha_F = N_{\mathbf{Q}(\zeta_f)/F}(\zeta_f - 1).$$

Let H_K be the subgroup of K^* generated by α_F and its conjugates for all cyclic subfields F of K.

Let E_K denote the subgroup in K^* of units in the ring of integers of K. Define the *circular units* of K to be

$$C_K = H_K \cap E_K.$$

Define $A(K)$ to be the p-primary component of the ideal class group of K. Define $B(K)$ to be the p-primary component of E_K/C_K.

The finite groups $A(K)$ and $B(K)$ are known to have the same order.

Theorem 1 (conjecture of G. Gras [21]). *The* $\mathbf{Z}_p[\mathrm{Gal}(K/\mathbf{Q})]$*-modules* $A(K)$ *and* $B(K)$ *have isomorphic Jordan-Holder series.*

Proof. Greenberg (loc. cit.) has shown the above theorem to follow from the main conjecture.

(ii) This conjecture of Gras is an analogue of an earlier conjecture of Iwasawa and Leopoldt concerning the odd eigenspace of ideal class groups of cyclotomic fields. Just as the above theorem may be considered as a Galois-theoretic interpretation of the plus part of the class number formula, what follows may be considered as a Galois-theoretic interpretation of the minus part. We now show that this conjecture for the minus part is also a consequence of the main theorem of §9. The basic method for proving this, at least in the hard case where there is a trivial zero, is again due to R. Greenberg. An exposition of an equivalent form of it in the case where the ground field is $K(\zeta_p)$ with K imaginary quadratic may be found in [22]. We are indebted to him for explaining it to us. We note also that some of the main elements of it were generalized by Federer and Gross in [17], and we rely at certain points on their exposition.

(a) χ*-orders.* Let χ: $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathcal{O}_\chi^*$ be a p-adic Dirichlet character of order prime to p. Let $H \subset \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ be the kernel of χ. Let M be a $\mathbf{Z}_p$-module with an action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ which factors through a finite quotient group G.

Let M^χ be the $\mathcal{O}_\chi$-submodule of $M \underset{\mathbf{Z}_p}{\otimes} \mathcal{O}_\chi$ comprising all elements w such that $\sigma w = \chi(\sigma) \cdot w$ for all $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. If M^H denotes the submodule of invariants under H, then M^H is naturally a G/H-module, where G/H is a finite (cyclic) group of order prime to p. We have natural isomorphisms

$$M^\chi \cong (M^H)^\chi \cong M^H \underset{\mathbf{Z}_p[G/H]}{\otimes} \mathcal{O}_\chi$$

where $\mathcal{O}_\chi$ is viewed as $\mathbf{Z}_p[G/H]$-module via the ring-homomorphism induced by χ.

We refer to M^χ as the χ*-part* of M, and its order is denoted $\mathfrak{o}_\chi(M)$.

(b) *Statement of the theorem.* Let F be an abelian imaginary field extension of $\mathbf{Q}$ of degree prime to p. Let $G = \mathrm{Gal}(F/\mathbf{Q})$, and let $\chi: G \to \mathcal{O}_\chi^*$ be an odd character. We may view χ as a homomorphism from $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ to $\mathcal{O}_\chi^*$. Set $g = [\mathcal{O}_\chi : \mathbf{Z}_p]$. For χ not equal to ω, the Teichmüller character, we have the following theorem, where for two p-adic numbers a, b we write $a \sim b$ if they have the same p-adic valuation, and where $\mathbf{B}_1(\chi^{-1})$ denotes the Bernoulli number associated to the p-adic Dirichlet character corresponding to χ^{-1} (cf. § 6).

Theorem 2. *For any odd prime p not dividing $[F: \mathbf{Q}]$ and any odd character $\chi \neq \omega$,*

$$\mathfrak{o}_\chi(A(F)) \sim \mathbf{B}_1(\chi^{-1})^g.$$

Remarks. 1) If F is the cyclotomic field $\mathbf{Q}(\zeta_N)$ then we can reinterpret this in terms of the Stickelberger ideal. Letting $R = \mathbf{Z}_p[(\mathbf{Z}/N\mathbf{Z})^*]$ and identifying G with $(\mathbf{Z}/N\mathbf{Z})^*$, the theorem says that the minus-part $A^-(F) \otimes \mathbf{Z}_p$ and $R^-/S_1(N)^-$ have isomorphic Jordan-Holder series as R-modules.

2) If $\chi = \omega$, it is known that $A(F)^\chi = 0$. This follows easily from Stickelberger's theorem. It also follows from the main theorem of § 9 and the fact that $G_p(\omega^2, T)$ is a unit power series. For together these imply that $\mathrm{Hom}(A_\infty^\omega, \mathbf{Q}_p/\mathbf{Z}_p) = 0$.

3) We identify the character χ with a homomorphism $\mathrm{Gal}(\mathbf{Q}^{\mathrm{ab}}/\mathbf{Q}) \to \mathcal{O}_\chi^*$ using class field theory. Here $\mathbf{Q}^{\mathrm{ab}}$ is the maximal abelian extension of $\mathbf{Q}$. If $F \subset K$ is an inclusion of abelian field extensions of $\mathbf{Q}$, and χ a Dirichlet character of order prime to p, such that χ factors through $\mathrm{Gal}(F/\mathbf{Q})$, then the natural mapping

$$A(F)^\chi \to A(K)^\chi$$

is easily seen to be an isomorphism if the degree $[K: F]$ is prime to p. The following proposition, explained to us by Sinnott, shows that the above mapping is an isomorphism under other conditions, as well.

Proposition 1. *Let χ be odd. Let χ factor through $\mathrm{Gal}(F/\mathbf{Q})$ and suppose that we have equalities of conductors:*

$$\mathrm{cond}(\chi) = \mathrm{cond}(F) = \mathrm{cond}(K).$$

Then

$$A(F)^\chi \to A(K)^\chi$$

is an isomorphism.

In particular, we have that

$$\mathfrak{o}_\chi(A(F)) = \mathfrak{o}_\chi(A(K)).$$

Proof. We can assume that $F/\mathbf{Q}$ is the field extension cut out by χ so that $G = \mathrm{Gal}(F/\mathbf{Q})$ is of order prime to p. Let

$$H = \ker(\chi) \subseteq \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}).$$

Let $I(K)$ denote the group of ideals of K, tensored with $\mathbf{Z}_p$, and let $I(F)$ be defined similarly. Consider the diagram

$$\begin{array}{ccc} I(F) & \twoheadrightarrow & A(F) \\ \downarrow & & \downarrow \\ I(K)^H & \longrightarrow & A(K)^H \end{array}$$

and pass to χ-isotypic components, which we may write as follows:

$$\begin{array}{ccc} I(F)^\chi & \twoheadrightarrow & A(F)^\chi \\ \downarrow & & \downarrow \\ I(K)^\chi & \longrightarrow & A(K)^\chi. \end{array}$$

Since χ is odd, the right-hand vertical morphism is injective.

The lower horizontal morphism is surjective by the following argument. We have an exact sequence

$$0 \to (K^* \otimes \mathbf{Z}_p)^- \to I(K)^- \to A(K)^- \to 0$$

where the superscript $^-$ denotes the "minus part", i.e., the -1-eigenspace under complex conjugation. (Recall that K possesses no nontrivial p^{th} roots of 1). The above exact sequence remains exact when we pass to H-invariants, by Hilbert's theorem 90. Now pass to χ-parts.

Our proposition then follows if we prove that the inclusion $I(F)^\chi \hookrightarrow I(K)^\chi$ is an equality. But we can given an explicit description of $I(K)^H/I(F)$. For any rational prime q, let e_q be the maximal power of p dividing the ramification index for the extension K/F of any prime of F lying above q. Choose such a prime of F and let $D_q \subset G$ denote its decomposition group. Then there is an isomorphism of $\mathbf{Z}_p[G]$-modules

$$I(K)^H/I(F) \cong \bigoplus_q (\mathbf{Z}/e_q\mathbf{Z})[G/D_q]$$

where $(\mathbf{Z}/e_q\mathbf{Z})[G/D_q]$ is given the natural $\mathbf{Z}_p[G]$-module structure (G operating on the left). Of course, the direct sum on the right may be taken over only those primes q such that there is a prime of F, lying above q, which is ramified in K/F. But since $\operatorname{cond} K = \operatorname{cond} \chi$, any such prime is also ramified in $F/\mathbf{Q}$. In particular, D_q is nontrivial, and since χ is an injection of G into $\mathcal{O}_\chi^*$, $\chi|D_q$ is a nontrivial character of D_q. But then the tensor product of $(\mathbf{Z}/e_q\mathbf{Z})[G/D_q]$ with $\mathcal{O}_\chi$ over $\mathbf{Z}_p[G]$ vanishes.

(c) *Case* 1; *proof when* $\chi(p) \neq 1$. Let $A_n = A(F_n)$ where F_n is the extension of degree p^n inside F_∞, the cyclotomic $\mathbf{Z}_p$-extension of F. Note that $\operatorname{Gal}(F_n/\mathbf{Q})$ is canonically a product $G \times (\Gamma/\Gamma_n)$ where $G = \operatorname{Gal}(F/\mathbf{Q})$ and Γ_n is the subgroup of index p^n in Γ, the Galois group of the (cyclotomic) $\mathbf{Z}_p$-extension of $\mathbf{Q}$. Consequently, $A(F_n)$ (indeed, any $\operatorname{Gal}(F_n/\mathbf{Q})$-module) may be viewed as G-module. The natural map $A_n^\chi \to A_m^\chi (m > n)$ is injective for χ odd (see, for example, Corollary 2.6 of [17]). Furthermore, $A_n^\chi = (A_\infty^\chi)^{\Gamma_n}$, where $\Gamma_n = \operatorname{Gal}(F_\infty/F_n)$, so

$$\# A_n^\chi = \# (\operatorname{Hom}(A_\infty, \mathbf{Q}_p/\mathbf{Z}_p)^{\chi^{-1}})_{\Gamma_n}.$$

Now since $\operatorname{Hom}(A_\infty, \mathbf{Q}_p/\mathbf{Z}_p)^{\chi^{-1}}$ has no finite Λ-submodule (see Proposition 1(i) of § 2) this order is given by the power of p dividing the value of its characteristic

power series at $T=0$, [i.e., $h_p(\chi,0)$] raised to the g^{th} power. By the main theorem of § 9

$$h_p(\chi,0) \sim G_p(\chi^{-1}\omega,0) = L_p(\chi^{-1}\omega,0) = -(1-\chi^{-1}(p))\,\mathbf{B}_1(\chi^{-1}).$$

Since χ has order prime to p and $\chi(p) \neq 1$ the power of p dividing the term on the right is precisely the power of p dividing $\mathbf{B}_1(\chi^{-1})$ and so the theorem is proved in this case.

(d) *Preparation for the proof in case* 2.

$$(\chi(p)=1).$$

Now suppose that $\chi \neq \omega$ is an odd character of order prime to p, and $\chi(p)=1$.

Let $K/\mathbf{Q}$ be the field extension cut out by χ. If $a=\operatorname{cond}\chi$, then K may be imbedded in $\mathbf{Q}(\mu_a)$. Identifying $\operatorname{Gal}(\mathbf{Q}(\mu_a)/\mathbf{Q})$ with $(\mathbf{Z}/a\mathbf{Z})^*$, we let $F \subseteq \mathbf{Q}(\mu_a)$ be the fixed field of $D_p \subset (\mathbf{Z}/a\mathbf{Z})^*$, the subgroup generated by the image of p in $(\mathbf{Z}/a\mathbf{Z})^*$. Let $H \subseteq (\mathbf{Z}/a\mathbf{Z})^*$ denote the kernel of χ.

If $U \subseteq F^*$ is any subgroup, then passing to H-invariants we have

$$U^H \subseteq F^{*H} = K^*,$$

and consequently if U^χ is defined to be $(U \otimes \mathbf{Z}_p)^\chi$, we may view $U^\chi = (U^H)^\chi$ as a subgroup of $K^{*\chi}$. The functor $U \mapsto U^\chi$ preserves inclusions and intersections.

Let $W_F \subset F^*$, and $W_K \subset K^*$ denote the subgroups of p-units. For simplicity, set $W = W_K$. We have $W_F^H = W$, and $W_F^\chi = W^\chi$. Define a subgroup $V_F \subset W_F$ generated by Gauss sums, as follows: Fix a prime $\mathfrak{p} = \mathfrak{p}_1$ of $\mathbf{Q}(\mu_a)$ above $\mathbf{Q}$ and fix an isomorphism ψ: $\mathbf{Z}/p\mathbf{Z} \xrightarrow{\sim} \mu_p \subseteq \bar{\mathbf{Q}}$. Write $\mathcal{O}$ for the ring of integers of $\mathbf{Q}(\mu_a)$ and set

$$g\left(\frac{c}{a}\right) = -\sum_{x \in (\mathcal{O}/\mathfrak{p})^*} \left(\frac{x}{\mathfrak{p}}\right)^{-c} \psi \circ Tr(x) \in \mathbf{Z}[\mu_{ap}].$$

Here $(x/\mathfrak{p})$ is the power residue symbol, i.e., $(x/\mathfrak{p}) = \zeta$ where $\zeta \in \mu_a$ is such that $\zeta \equiv x^{\frac{N\mathfrak{p}-1}{a}} \bmod \mathfrak{p}$. The value of $g(c/a)$ is seen to lie in $\mathcal{O}_F[\mu_p]$. It is easy to show that $g(c/a)^a$ is in $\mathcal{O}_F$ and furthermore lies in W_F. We let V_F be the subgroup generated by these elements

$$V_F = \left\{ G\left(\frac{c}{a}\right) = g\left(\frac{c}{a}\right)^a : c \text{ such that } (c,a)=1 \right\}.$$

This group is independent of the choice of ψ and $\mathfrak{p}$. Note that for $\sigma_b \in \operatorname{Gal}(F/\mathbf{Q})$ (for $b \in (\mathbf{Z}/a\mathbf{Z})^*$), $G(c/a)^{\sigma_b} = G(bc/a)$.

Let V be the subgroup of V_F generated by the elements

$$\left\{ \prod_{h'} G\left(\frac{ch'}{a}\right);\ c \text{ such that } (c,a)=1 \right\}$$

where h' runs through representatives in $(\mathbf{Z}/a\mathbf{Z})^*$ for $H/\langle p\rangle \subseteq (\mathbf{Z}/a\mathbf{Z})^*/\langle p\rangle$. Thus $V \subseteq (V_F)^H$.

(e) *Sublattices in* M^χ. Let M be the free abelian group generated by the prime divisors of p in K. Let $M_p = M \otimes \mathbf{Z}_p$ and $M^\chi = (M_p)^\chi$. Define mappings

$$\mu\colon W \to M,$$

$$\lambda\colon W \to M_p$$

which induce $\mathcal{O}_\chi$-linear homomorphisms denoted by the same letter:

$$\mu\colon W^\chi \to M^\chi,$$
$$\lambda\colon W^\chi \to M^\chi$$

by the rules:

$$\mu(u) = \sum_{\substack{q\text{: prime} \\ \text{of } K \text{ over } p}} \operatorname{ord}_q(u)\cdot q,$$

$$\lambda(u) = \sum_{\substack{q\text{: prime} \\ \text{of } K \text{ over } p}} \log_p(\tau_q u)\cdot q$$

where $\tau_q\colon K \to \mathbf{Q}_p$ is the embedding corresponding to the prime q.

Proposition 2. *The module $V^\chi \subset W^\chi$ is nontrivial; it is an $\mathcal{O}_\chi$-lattice (of finite index) in W^χ.*

The mappings λ, μ are nontrivial; they map V^χ, W^χ isomorphically onto $\mathcal{O}_\chi$-lattices in M^χ (of finite index).

Proof. It suffices to show that μ is injective on W^χ, and that $\lambda(V^\chi)$ is nontrivial. The first assertion is elementary. As for the second, the main ingredient is the following result of Ferrero and Greenberg ([18] or [43]).

Let $\log_p$ denote the p-adic logarithm ($\log_p p = 0$), and note that if we view the element $G(c/a)$ as being in the completion of K at $q = q_1$, i.e., in $K_q \xrightarrow{\sim} \mathbf{Q}_p$, then as an element of $\mathbf{Q}_p$ it is independent of the original choice of $\mathfrak{p} = \mathfrak{p}_1$.

Theorem 3 (Ferrero – Greenberg).

$$L_p'(\chi\omega, 0) = \frac{1}{a} \sum_{c \in (\mathbf{Z}/a\mathbf{Z})^*/D_p} \chi(c)\log_p\left(G\left(\frac{c}{a}\right)\right) \neq 0.$$

To see that $\lambda(V^\chi)$ is nontrivial, note that $\lambda(V)$ contains the element

$$\lambda\left(\sum_{h'} G\left(\frac{h'}{a}\right)\right) = \sum_{h'}\sum_{q} \log_p\left(\tau_q G\left(\frac{h'}{a}\right)\right)\cdot q$$

where the summation over h' is of a complete set of representatives mod a of elements of $H \subset (\mathbf{Z}/a\mathbf{Z})^*$, and the q's run through all prime divisors of p in K. For the given odd character χ of Gal $(K/\mathbf{Q})$ we thus obtain an element of $(\lambda(V)\otimes \mathbf{Z}_p)^\chi$ given by

$$\begin{aligned} \mathfrak{x}_\chi &= e_\chi\left(\sum_{h'}\sum_{i=1}^{r} \log_p\left(\tau_i G\left(\frac{h'}{a}\right)\right) q_i\right) \\ &= [F\colon K] \sum_{c \in (\mathbf{Z}/a)^*/D_p} \chi^{-1}(c)\log_p\left(G\left(\frac{c}{a}\right)\right)\cdot e_\chi(q_1), \end{aligned} \tag{5}$$

where

$$e_\chi(q_1) = \frac{1}{[K\colon \mathbf{Q}]} \sum_{\sigma \in \mathrm{Gal}(K/\mathbf{Q})} \chi^{-1}(\sigma)\, q_1^\sigma.$$

But $e_\chi(q_1)$ is a generator of M^χ and according to Theorem 3, $\mathfrak{X}_\chi$ is non-zero.

(f) *Ideal classes supported at p.* Define $D_n \subset A_n$ as the subgroup comprising those ideal classes of p-power order which can be represented by ideals which are products of the primes of K_n above p. We have $D_n^\chi \subset A_n^\chi$, which we view as an $\mathcal{O}_\chi[\Gamma/\Gamma_n]$-module. Let E_n^χ be the quotient module, giving us an exact sequence

$$0 \to D_n^\chi \to A^{\chi n} \to E_n^\chi \to 0. \tag{1}$$

Since χ is odd, the mappings $A_n^\chi \to A_m^\chi$ are injective ($m \geqq n$) and therefore so are the mappings $D_n^\chi \to D_m^\chi$. It is also true that $E_n^\chi \to E_m^\chi$ is injective (cf. § 2 and the remark at the beginning of § 4 in [17]).

Passage to the direct limit (as n tends to ∞) gives an exact sequence of $\mathcal{O}_\chi[\![\Gamma]\!]$-modules

$$0 \to D_\infty^\chi \to A_\infty^\chi \to E_\infty^\chi \to 0. \tag{2}$$

The following statements are known about these $\mathcal{O}_\chi[\![\Gamma]\!]$-modules.

1. $D_\infty^\chi \cong \mathbf{Q} \otimes \mathcal{O}_\chi/\mathcal{O}_\chi$; the action of Γ on D_∞^χ is trivial.
2. The submodule of Γ-invariants in A_n^χ fits into an exact sequence:

$$0 \to D_n^\chi \to A_n^{\chi,\Gamma} \to E_0^\chi \to 0$$

which splits.

3. The submodule of Γ-invariants in E_∞^χ is finite and $E_\infty^{\chi,\Gamma} = E_m^{\chi,\Gamma}$ for m sufficiently large.

For 1. and 2. cf. [17] Proposition 3.4.

Part 3. is deeper, and due to Greenberg; we now review it.

From 1. above, the characteristic polynomial of

$$\mathrm{Hom}(D_\infty^\chi, \mathbf{Q}_p/\mathbf{Z}_p)$$

is seen to be $T \in \mathcal{O}_\chi[\![T]\!] \cong \mathcal{O}_\chi[\![\Gamma]\!]$. Therefore, a characteristic power series for $\mathrm{Hom}(E_\infty^\chi, \mathbf{Q}_p/\mathbf{Z}_p)$ is

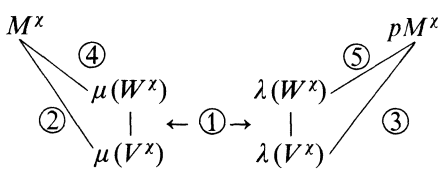
$$\mathscr{E}(T) \overset{\text{defn.}}{=\!=} h_p(\chi, (1+T)^{-1} - 1)/T.$$

Greenberg has proved in [22] that $\mathscr{E}(0)$, or equivalently $d/dT(h_p(\chi,(1+T)^{-1}-1))|_{T=0}$, does not vanish.

Since $\mathrm{Hom}(E_\infty^\chi, \mathbf{Q}_p/\mathbf{Z}_p)$ has no finite $\mathcal{O}_\chi[\![\Gamma]\!]$-submodules (as follows immediately from Prop. 1 (i) of § 2),

$$\mathscr{E}(0)^g \sim \#E_\infty^{\chi,\Gamma}, \tag{3}$$

(g) *Structure of the proof in case 2.* We have the following diagram of sublattices of M^χ and pM^χ.



about which we will prove these facts.

① $[\mu(W^\chi):\ \mu(V^\chi)] = [\lambda(W^\chi):\lambda(V^\chi)]$

② $[M^\chi:\ \mu(V^\chi)] \sim \mathbf{B}_1(\chi^{-1})^g[F:K]^g$

③ $[pM^\chi:\ \lambda(V^\chi)] \sim G_p'(\chi^{-1}\omega, 0)^g[F:K]^g$

④ $[M^\chi:\mu(W^\chi)] = \mathcal{O}_\chi(D_0) = \mathfrak{o}_\chi(A_0)/\mathfrak{o}_\chi(E_0)$

⑤ $[pM^\chi:\lambda(W^\chi)] \sim \mathscr{E}(0)^g/\mathfrak{o}_\chi(E_0)$.

Note that Theorem 2 follows from ①–⑤ together with the fact that $\mathscr{E}(0) \sim G_p'(\chi\omega^{-1}, 0)$. But this last assertion is a consequence of the main theorem of §9, which implies that

$$(G_p(\chi^{-1}\omega, T)) = (\mathscr{E}(T)\cdot T)$$

as ideals in $\mathcal{O}_\chi[\![T]\!]$.

Proofs.

① Both μ and λ are injective, by Proposition 1.

② According to Stickelberger's theorem ([41] Chap. 1)

$$\left(G\left(\frac{1}{a}\right)\right) = (q_1^{\theta(-1)})$$

as ideals of F, where $\theta(-1) = \sum_{c\in(\mathbf{Z}/a)^*/D_p} \langle -c/a\rangle \sigma_c^{-1}$ viewed as an element of $\mathbf{Z}[G]$. If we apply the map μ we see that $\mu(V)$ is generated as a $\mathbf{Z}[\mathrm{Gal}(K/\mathbf{Q})]$-module by

$$\mu\left(\prod_{h'} G\left(\frac{h'}{a}\right)\right) = \theta(-1)\sum_h \sigma_h \cdot q_1$$

where h runs through a system of representatives for $\mathrm{Gal}(F/K)$. Now taking χ-components we find that $\mu(V)^\chi$ is generated by

$$e_\chi \cdot \mu\left(\prod_{h'} G\left(\frac{h'}{a}\right)\right) = -a[F:K]\mathbf{B}_1(\chi^{-1})e_\chi(q_1).$$

③ We first observe that by the defining property of $G_p(\chi^{-1}\omega, T)$ in §6, we have that

$$pG_p'(\chi^{-1}\omega, 0) \sim L_p'(\chi^{-1}\omega, 0).$$

As a $\mathbf{Z}[\mathrm{Gal}(K/\mathbf{Q})]$-module, V is generated by $\prod_{h'} G\left(\frac{h'}{a}\right)$. Hence $\lambda(V)\otimes\mathbf{Z}_p$ is generated by $\lambda\left(\prod_{h'} G\left(\frac{h'}{a}\right)\right)$ as a $\mathbf{Z}_p[\mathrm{Gal}(K/\mathbf{Q})]$-module. In the notation of (5) $\{\lambda(V)\otimes\mathbf{Z}_p\}^\chi$ is generated by $\mathfrak{X}_\chi$, and since $e_\chi(q_1)$ is a generator of M_p^χ we see that the index $[M_p^\chi: \{\lambda(V)\otimes\mathbf{Z}_p\}^\chi]$ is given by the index of the ideal generated by

$$[F:K]\sum_{c\in(\mathbf{Z}/a)^*/D_p} \chi^{-1}(c)\log_p\left(G\left(\frac{c}{a}\right)\right) \sim [F:K]aG_p'(\chi^{-1}\omega, 0) \text{ in } \mathcal{O}_\chi$$

(cf. Theorem 3 and (5) following it).

④ This follows immediately from the definitions.

(h) *Proof of* ⑤. Consider the Γ-cohomology exact sequence coming from (2):

$$0 \longrightarrow D_\infty^\chi \longrightarrow A_\infty^{\chi,\Gamma} \longrightarrow E_\infty^{\chi,\Gamma} \xrightarrow[\delta]{} H^1(\Gamma, D_\infty^\chi).$$

Let Δ^χ denote the image of δ.
By fact 2 of (f), we have an exact sequence

$$0 \longrightarrow E_0^\chi \longrightarrow E_\infty^{\chi,\Gamma} \xrightarrow[\delta]{} \Delta^\chi \longrightarrow 0. \tag{4}$$

From (3) and (4), the proof of ⑤ follows from

Proposition 3. $$\Delta^\chi \cong pM^\chi/\lambda(W^\chi).$$

This proposition, in turn, follows from Lemmas 1 and 2 below. Let $m \geqq 0$ be an integer, and let $NK_m^* \subset K^*$ denote the image of K_m^* under the norm mapping $N_{K_m/K}$.

Lemma 1. *For m sufficiently large,*

$$\lambda(W^\chi \cap NK_m^{*\chi}) = p^{m+1}M^\chi.$$

Lemma 2. *For m sufficiently large, there is an isomorphism*

$$\rho^\chi\colon \Delta^\chi \xrightarrow[\cong]{} W^\chi \cap NK_m^{*\chi}/(W^\chi)^{p^m}.$$

Proof of Lemma 1. Recall that the superscript $^-$ means "minus part", i.e., the -1-eigenspace under the action of complex conjugations in $\mathrm{Gal}(K/\mathbf{Q})$.

We first show that the image does indeed lie in $p^{m+1}M^\chi$ (*a priori* it lies in pM^χ). Suppose that $\varepsilon \in W$. Then $\varepsilon \in \mathrm{Norm}(K_m^*)$ if and only if ε is a local norm everywhere. Since K_m/K is ramified only at p, this is so precisely when ε is a norm at each prime above p. But $K_{m,q_i} \xrightarrow{\sim} \mathbf{Q}_{m,p}$ (the completion of $\mathbf{Q}_m$ at the prime above p) and the norms for the extension $\mathbf{Q}_{m,p}/\mathbf{Q}_p$ are the group $p^{\mathbf{Z}} \times \mu_{p-1} \times (1+p^{m+1}\mathbf{Z}_p)$. Thus ε is a local norm at each i if and only if $\log_p(\tau_i \varepsilon) \equiv 0 \,(p^{m+1})$ for each i, that is, if and only if $\lambda(\varepsilon) \in p^{m+1}M_p^-$. This argument has the following consequence:

$$\lambda((W \cap NK_m^*)^-) \subset p^{m+1}M_p$$

and

$$\lambda(W^-) \cap p^{m+1}M_p \subseteq \lambda(NK_m^*)$$

for all m. Hence:

$$\lambda(W^\chi \cap NK_m^{*\chi}) \subset p^{m+1}M^\chi,$$

$$\lambda(W^\chi) \cap p^{m+1}M^\chi \subset \lambda(W^\chi \cap NK_m^{*\chi}).$$

But by Proposition 2, there is an m such that $p^{m+1}M^\chi \subset \lambda(W^\chi)$. Consequently, for such an m, $\lambda(W^\chi \cap NK_m^{*\chi}) = p^{m+1}M^\chi$, whence Lemma 1.

Proof of Lemma 2. The isomorphism ρ^χ was defined by Greenberg. It may be viewed as a "diagonal isomorphism" of the sort given in Lemma 3 below.

Lemma 3. Let

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & A_{11} & \longrightarrow & A_{12} & \longrightarrow & A_{13} & \longrightarrow & 0 \\
 & & i\downarrow & & \downarrow & & \downarrow & & \\
0 & \to & A_{21} & \longrightarrow & A_{22} & \longrightarrow & A_{23} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow j & & \\
0 & \to & A_{31} & \longrightarrow & A_{32} & \longrightarrow & A_{33} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

be a commutative diagram of C-modules, where every straight line is exact, and where C is a finite cyclic group. Suppose that $H^1(C, A_{i,2}) = 0$ *for* $i = 1, 2, 3$. *Then there is a canonical isomorphism* (*the "diagonal isomorphism"*)

$$A_{33}^C/jA_{23}^C \xrightarrow[\cong]{\delta} \mathrm{Hom}(C; i^{-1}NA_{21}/NA_{11})$$

where $N = \sum_{c \in C} c$ *is the "Norm element" in the group-ring* $\mathbf{Z}[C]$.

Proof of Lemma 3. Take $a_{33} \in A_{33}^\Gamma$, and we shall define $\delta(a_{33})$: $C \to i^{-1}NA_{21}/NA_{11}$. Let $c \in C$. Let $a_{22} \in A_{22}$ be an element which projects to a_{33} in A_{33}. Then $(c-1) \cdot a_{22}$ projects to zero in A_{33}, and consequently can be written as a sum $a_{21} + a_{22}$ where a_{21} is in the image of A_{21} and a_{12} is in the image of A_{12}. Since $Na_{21} = -Na_{12}$, there is an element $a_{11} \in A_{11}$ such that $i \cdot a_{11} = Na_{21}$.

Define $\delta(a_{33})(c) = a_{11} \bmod NA_{11}$. It is routine to check that $\delta(a_{33})$ is a well-defined homomorphism of C to $i^{-1}NA_{21}/NA_{11}$, and that δ is a homomorphism from A_{33}^C/jA_{23}^C to $\mathrm{Hom}(C; i^{-1}NA_{21}/NA_{11})$. To check injectivity one uses the hypothesis that $H^1(C, A_{12}) = 0$. To check surjectivity, we reverse the process. Fix $c \in C$ a generator, and $a_{11} \bmod NA_{11}$, where $a_{11} \in i^{-1}NA_{21}$. Write $ia_{11} = N\alpha_{21}$. Let α_{32} be the image of α_{21} in A_{32}. Since $N\alpha_{32} = 0$, and $H^1(C, A_{32}) = 0$, we may write $\alpha_{32} = (c-1)a_{32}$. Let a_{33} be the image of a_{32} in A_{33}. Then $a_{33} \in A_{33}^C$, and $\delta(a_{33})(c) = a_{11} \bmod NA_{11}$.

To conclude the proof of Lemma 2, apply Lemma 3 to the diagram:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & W_n^\chi & \longrightarrow & \mathrm{Div}_p(\mathcal{O}_{K_n})^\chi & \longrightarrow & D_n^\chi \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & K_n^{*\chi} & \longrightarrow & \mathrm{Div}(\mathcal{O}_{K_n})^\chi & \longrightarrow & A_n^\chi \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & K_n^{*\chi}/W_n^\chi & \longrightarrow & \mathrm{Div}(\mathcal{O}_{K_n}[1/p])^\chi & \longrightarrow & E_n^\chi \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
\end{array}$$

where $\mathrm{Div}(\mathcal{O}_{K_n})$ or $\mathrm{Div}(\mathcal{O}_{K_n}[1/p])$ denotes the group of divisors of the indicated rings, $\mathrm{Div}_p(\mathcal{O}_{K_n})$ means divisors supported at primes of residual characteristic p, W_n is the group of p-units in K_n^*, and the cyclic group C is $\Gamma/\Gamma_n = \mathrm{Gal}(K_n/K)$ acting on all groups involved, in the natural way. As usual, the superscript χ denotes the operation of first tensoring with $\mathbf{Z}_p$ and then taking χ-parts. Note that $W_n^\chi = W^\chi$ because the elements of W_n generate Γ/Γ_n-invariant ideals (each prime above p being totally ramified in K_n/K), and any Γ/Γ_n ideal generated by a minus-element is generated by an element of K^* (cf. [17] Cor. 2.6, § 2). Therefore $N_{K_n/K} W_n^\chi = (W^\chi)^{p^n}$.

(iii) As a final application of the main theorem we have certain results on $K_2\mathcal{O}_F$ where F is a real abelian field. In [10], using the theorem of Tate in [65], the following theorem is proved:

$$\text{For each odd prime } p,\ \#\, K_2\mathcal{O}_F \sim \#\, A_\infty(1)^\Gamma. \tag{6}$$

Recall that for a given prime p, $a \sim b$ if a and b have the same p-adic valuation. Here $A_\infty(1) = A_\infty \otimes Ta_{\mu_{p^\infty}}$ where $Ta_{\mu_{p^\infty}} = \varprojlim \mu_{p^n}$. From this result it is easy to deduce the following analogue of the class number formula for $K_2\mathcal{O}_F$ which was conjectured by Birch and Tate.

Theorem 5. *$\#\, K_2\mathcal{O}_F$ is equal to $w_2(F)\,|\zeta_F(-1)|$ multiplied by a power of 2. Recall that $w_2(F)$ is defined as the largest positive integer N such that $\mathrm{Gal}(F(\zeta_N)/F)$ has exponent 2.*

To deduce this from the main theorem of § 9 we note that

$$\#\, A_\infty(1)^\Gamma = \#\, \{\mathrm{Hom}(A_\infty, \mathbf{Q}_p/\mathbf{Z}_p)(-1)\}_\Gamma.$$

Now the characteristic polynomial of

$$\mathrm{Hom}(A_\infty, \mathbf{Q}_p/\mathbf{Z}_p)(-1) \quad \text{is} \quad \Pi h_p(\chi^{-1}, u^{-1}(1+T)^{-1} - 1)$$

where the product runs over all odd characters χ such that $\chi\omega^{-1}$ is a character of $\mathrm{Gal}(F/\mathbf{Q})$. Since this Λ-module has no finite Λ-submodule

$$\#\, A_\infty(1)^\Gamma \sim \prod_\chi h_p(\chi^{-1}, u^{-1} - 1)$$

where the product is taken over the same set of characters. By the main theorem of § 9 we can rewrite the right hand side in terms of the Stickelberger power series and then the p-adic L-function,

$$\prod_\chi h_p(\chi^{-1}, u-1) \sim \prod_{\chi\omega_{\mathrm{tame}} \neq \chi_0} G_p(\chi\omega, u-1) \sim \prod_{\chi\omega_{\mathrm{tame}} \neq \chi_0} L_p(\chi\omega, -1).$$

Thus we have that

$$\#\, A_\infty(1)^\Gamma \sim \prod_{\chi\omega_{\mathrm{tame}} \neq \chi_0} \mathbf{B}_2(\chi\omega)^{-1} = \prod_\psi \mathbf{B}_2(\psi) \tag{7}$$

where the product is taken over those even characters ψ of $\mathrm{Gal}(F/\mathbf{Q})$ for which $\psi\omega^2_{\mathrm{tame}} \neq \chi_0$. We claim now that

$$\prod_{\substack{\psi:\, \psi\omega^2_{\mathrm{tame}} = \chi_0 \\ \psi \neq \omega^{-2}}} \mathbf{B}_2(\psi) \sim (w_2(F))^{-1}. \tag{8}$$

To prove this assertion observe first that if ω^2 is not a character of $\mathrm{Gal}(F/\mathbf{Q})$, then $F(\zeta_p)$ is not quadratic over F and so $w_2(F)$ is prime to p. In this case there are no characters ψ such that $\psi\omega^2_{\mathrm{tame}} = \chi_0$. So now we assume that ω^2 is a character of $\mathrm{Gal}(F/\mathbf{Q})$ and hence that $F(\zeta_p)$ is quadratic over F. Then

$$\mathbf{B}_2(\psi) \sim 1/(\zeta_{p^r} - 1) \quad \text{if } \psi\omega^2 \text{ is of order } p^r \text{ and has conductor } p^{r+1}.$$

This follows immediately from ([31], § 3, Theorem 2, and § 6). The relation (8) now follows, and (6) and (7) give the theorem. Using the theorem referred to in (6) we can also give a description of $\# K_2\mathcal{O}_F$ analogous to that given for the minus part of the class group in Theorem 2.

Theorem 6. *Let F be a real abelian field and p an odd prime not dividing $[F:\mathbf{Q}]$. Then for any χ of order prime to p, $\chi \neq \omega^2$,*

$$\#\{K_2\mathcal{O}_F) \otimes \mathbf{Z}_p\}^{\chi} \sim \{\mathbf{B}_2(\chi^{-1})\}^g.$$

(For $\chi = \omega^2$ the left hand side is trivial).

Chapter 2.

Models and moduli

§ 1. Preliminaries concerning commutative group schemes. The relationship between the Picard functor and Néron models

If k is a perfect field, the category of commutative group schemes of finite type over k is an abelian category [51]. A member $G_{/k}$ of that category possesses a canonical filtration

$$0 \subset G^t \subset G^a \subset G^r \subset G^0 \subset G \qquad (*)$$

where G^0 is the connected component of G, G^r is the reduced group scheme associated to G^0, G^a is the maximal affine reduced, connected subgroup scheme of G^r, and G^t is the maximal subgroup scheme of multiplicative type contained in G^a. The successive quotients of the filtration (*) are of the following nature: G^a/G^t is a unipotent smooth connected group scheme, G^r/G^a is an abelian variety, G^0/G^r is a finite connected group scheme, and G/G^0 is a finite étale group scheme. The

filtration (*) is functorial in G. We shall refer to G^r/G^a as the *abelian variety part* of G, and we note that it, too, is functorial in G. References for the assertions made in this paragraph are to be found in add [51].

Example. Let X be a proper k-scheme such that every irreducible component of X is of dimension one. Let X_{red} denote the *reduced* k-scheme associated to X, and let $\tilde{X}_{\text{red}}$ denote the "normalization" of X_{red}; thus, $\tilde{X}_{\text{red}}$ is a disjoint union of smooth proper curves over k.

Lemma 1. *In the above example, the natural morphism*

$$\text{Pic}^0(X_{/k}) \to \text{Pic}^0(\tilde{X}_{\text{red}/k})$$

is a surjective homorphism of group schemes over k. Its kernel is a smooth connected affine groupscheme over k. The above morphism identifies $\text{Pic}^0(\tilde{X}_{\text{red}/k})$ *with the abelian variety part of the group scheme* $\text{Pic}^0(\tilde{X}_{\text{red}/k})$.

Proof. Compare the proof of Lemma 2.6 of [14]. Let $X^*_{\text{red}/k}$ be the scheme with morphisms

$$\tilde{X}_{\text{red}/k} \xrightarrow[\pi]{} X^*_{\text{red}/k} \xrightarrow[\varphi]{} X_{\text{red}/k} \longrightarrow X_{/k}$$

such that φ is an isomorphism of underlying topological spaces and

$$\Gamma(U, \mathfrak{O}_{X^*_{\text{red}/k}}) = \{f \in \Gamma(U, \pi_* \mathfrak{O}_{\tilde{X}_{\text{red}/k}}) \mid \text{if } x_1, x_2 \in \pi^{-1}U \text{ then } f(x_1) = f(x_2) \text{ when } \pi(x_1) = \pi(x_2)\}.$$

In the notation of the proof of Lemma 2.6 of [14], this is D^*. The arguments of ([14] 2.6) then show that $\text{Pic}^0(X^*_{\text{red}/k})$ is an extension of $\text{Pic}^0(\tilde{X}_{/k})$ by a smooth connected group scheme of multiplicative type, while $\text{Pic}^0(X_{\text{red}/k})$ is an extension of $\text{Pic}^0(\tilde{X}^*_{\text{red}/k})$ by a smooth connected unipotent group scheme.

Let K be a finite extension of $\mathbf{Q}_p$ whose ring of integers we denote $\mathcal{O}$, and whose residue field is k. If $V_{/k}$ is an abelian variety, let $V_{/\mathcal{O}}$ denote the Néron model of $V_{/K}$ over the base $\mathcal{O}$, and let $av(V)$ denote the abelian variety part of the fiber over k of $V_{/\mathcal{O}}$. We view $av(-)$ as a functor from the category of abelian varieties over K to the category of abelian varieties over k.

Lemma 2. (a) *If* $\varphi\colon V_1 \to V_2$ *is an isogeny of abelian varieties over K, then the morphism* $av(\varphi)\colon av(V_1) \to av(V_2)$ *is an isogeny of abelian varieties over k.*

(b) *If*

$$0 \xrightarrow{d_0} V_1 \xrightarrow{d_1} V_2 \xrightarrow{d_2} V_3 \xrightarrow{d_3} 0$$

is a sequence of abelian varieties over K which is exact (or more generally, which is a cochain complex whose cohomology groups are finite group schemes), then

$$0 \to av(V_1) \to av(V_2) \to av(V_3) \to 0,$$

viewed as cochain complex, has finite cohomology groups.

Proof. Assertion (a) is immediate. For (b), find a morphism $i\colon V_3 \to V_2$ such that $d_2 \cdot i$ is multiplication by some nonzero integer. Then

$$d_1 \times i\colon V_1 \times V_3 \to V_2$$

is an isogeny of abelian varieties over K. Thus

$$av(d_1) \times av(i)\colon\ av(V_1) \times av(V_3) \to av(V_2)$$

is likewise an isogeny, and part (b) follows.

We keep to the notation that $\mathcal{O}$ is the ring of integers of a finite extension K of $\mathbf{Q}_p$ with residue field k. Then the following proposition is a special case of [26], Theorem 12.1.

Proposition 1. *(Raynaud [54^1). Let X be a regular scheme and $f\colon X \to S = \operatorname{Spec}\mathcal{O}$ a morphism satisfying these conditions*:

(a) *The morphism f is proper and flat with fibres of dimension 1*

(b) *$X_{/\bar{K}}$ is a smooth irreducible curve*

(c) *If $\bar{k}$ is an algebraic closure of k, then the greatest common divisor of the multiplicities of the irreducible components of $X_{/\bar{k}}$ is 1.*

Then the relative Picard functor of $X_{/S}$ is representable by a smooth group object in the category of algebraic spaces $\operatorname{Pic}(X_{/S})$ *and so is the functor* Pic^0 *(for definition, see* SGA 3 VI$_B$ 3.1). *The functor* Pic^0 *is actually representable by a smooth group scheme. Moreover, if $\mathcal{N}_S^0$ denotes the connected component of the Néron model of* $\operatorname{Pic}^0(X_{/K})$ *then the isomorphism* $\operatorname{Pic}^0(X_{/K}) \xrightarrow{\sim} \mathcal{N}_K^0$ *extends uniquely to an isomorphism*

$$\operatorname{Pic}^0(X_{/S}) \xrightarrow{\sim} \mathcal{N}_S^0 .$$

Remarks. (i) We note that the flatness and properness of f together with the fact that $X_{/K}$ is irreducible give the condition $f_*(\mathfrak{O}_X) = \mathfrak{O}_S$ in [26], Theorem 12.1.

(ii) Artin ([1], Theorem 7.3) has proved more generally that if $f\colon X \to S$ is a proper, flat map of schemes which is finitely presented and cohomologically flat in dimension zero then $\operatorname{Pic}(X_{/S})$ is representable by an algebraic space over S. Mumford and Mori showed us how an argument due to Artin and Winters can be used to check "cohomological flatness of f in dimension zero" directly (assuming the conditions of the proposition). We sketch this below.

Let $\bar{S}$ denote the maximal unramified extension of S and let $\bar{X}$ denote the base change of X to $\bar{S}$. We view $Z = X_{/\bar{k}}$ as a divisor on $\bar{X}$, and write $Z = \sum_{i=1}^{r} m_i Z_i$ where the Z_i are irreducible curves over $\bar{k}$, and where by hypothesis the greatest common divisor of the m_i is one. To check cohomological flatness of f in dimension zero, it suffices to check that every global function on $X_{/\bar{k}}$ is constant (E.G.A. III. 7.8.6).

Assume then that we are given a positive divisor $Z' \leqq Z$ such that $H^0(\mathfrak{O}_{Z'}) = \bar{k}$, and assume also that the degree of Z' is maximal with this property. If $Z' = Z$ we are done, so assume that $Z' < Z$. Then for any $Z_i \subset Z - Z'$ set $Z'' = Z + Z_i$ and consider the exact sequence of coherent sheaves over X:

$$0 \to \mathfrak{O}_{Z_i}(-Z' \cdot Z_i) \to \mathfrak{O}_{Z''} \to \mathfrak{O}_{Z'} \to 0 .$$

If there exists Z_i such that $-Z' \cdot Z_i > 0$ then there is no global section of $\mathfrak{O}_{Z_i}(-Z' \cdot Z_i)$ contradicting the maximality of Z'. If, on the other hand, for each $Z_i \leqq Z - Z'$ we have $Z' \cdot Z_i \leqq 0$, then

$$-(Z')^2 = Z' \cdot Z - (Z')^2 = Z' \cdot (Z - Z') \leqq 0 .$$

But then using the theorem ([59], Lecture 6) that the intersection matrix $(Z_i \cdot Z_j)$ is negative semi-definite of rank $(r-1)$ we get that Z' is a rational multiple of Z. Since the greatest common divisor of the m_i's is 1 we get that $Z' = Z$. This contradiction completes the proof.

Corollary. *Let f: $X \to S$ satisfy the hypotheses of Raynaud's proposition above. Let $Z_1, \ldots, Z_r$ denote the k-irreducible components of the "normalization" of the "reduction" of the k-fiber. That is,*

$$(\tilde{X}_{/k})_{\mathrm{red}} = Z_1 \amalg Z_2 \amalg \cdots\cdots \amalg Z_r .$$

There is a canonical isomorphism of group schemes over k making the following triangle commutative:

$$\begin{array}{ccc} & & \mathrm{Pic}^0(X_{/k}) \\ & \swarrow & \searrow \\ \mathrm{Pic}^0(\tilde{X}_k)_{\mathrm{red}} = \prod_{i=1}^{r} \mathrm{Pic}^0(Z_i) & \xrightarrow[\cong]{\iota} & av(\mathrm{Pic}^0(X_{/K})) \end{array}$$

Proof. This follows from Lemma 1 and Proposition 1.

For a specific application to Chap. 2, we state the following *criterion of compatibility* for a pair of correspondences in characteristics 0 and p. We keep to the notation of the preceding corollary, and suppose further that *any irreducible component of the special fibre $X_{/k}$ which has multiplicity greater than one is of genus* 0.

Let U: $\mathrm{Pic}^0(X_{/K}) \to \mathrm{Pic}^0(X_{/K})$ and

$$u\colon \prod_{i=1}^{r} \mathrm{Pic}^0(Z_{i/k}) \to \prod_{i=1}^{r} \mathrm{Pic}^0(Z_{i/k})$$

be endomorphisms. We shall state a criterion which will insure that the square

(**)
$$\begin{array}{ccc} \prod_{i=1}^{r} \mathrm{Pic}^0(Z_{i/k}) & \xrightarrow{u} & \prod_{i=1}^{r} \mathrm{Pic}^0(Z_{i/k}) \\ \downarrow \iota & & \downarrow \iota \\ av(\mathrm{Pic}^0(X_{/k})) & \xrightarrow{av(U)} & av(\mathrm{Pic}^0(X_{/K})) \end{array}$$

is commutative.

We prepare for it with some notation. If k'/k is a finite field extension, let $\mathcal{O}'/\mathcal{O}$ denote a finite discrete valuation ring extension of $\mathcal{O}$ which is unramified over $\mathcal{O}$ and such that the residue field of $\mathcal{O}'$ is k'. Let K' denote its field of fractions. If D is a relative Cartier divisor of $X_{/\mathcal{O}'}$, let $D_{/K'}$ and $D_{/k'}$ denote the restrictions of D to the indicated fields. Given a relative Cartier divisor D of degree zero on every irreducible component of each fiber, let $\{D\} \in \mathrm{Pic}^0(X_{/\mathcal{O}'})$ denote the class in Pic^0 represented by D.

Proposition 2. *Suppose that for every finite field extension k'/k and every pair of smooth k'-valued points of $X_{/k'}$ z_1, z_2 which lie on the same irreducible component of the special fiber $X_{/k}$ one is given the following:*

(a) *a pair of $\mathcal{O}'$-valued sections Z_1 and Z_2 of the smooth locus $X_{/\mathcal{O}'}^{\text{smooth}}$ whose specializations to k' are z_1 and z_2 respectively.*

(b) *a pair of effective relative Cartier divisors D_1, D_2 of $X_{\mathcal{O}'}^{\text{smooth}}$ of equal degree on every irreducible component of every fiber.*

Now suppose that, for all pairs z_1, z_2 as above.

(c) $$U \cdot \{Z_{1/K'} - Z_{2/K'}\} = \{D_{1/K'} - D_{2/K'}\}$$

and

(d) $$u \cdot \{z_1 - z_2\} = \{D_{1/k'} - D_{2/k'}\}$$

where, in the second equality (d) *we have identified z_1, z_2 with points, and $D_{1/k'}, D_{2/k'}$ with Cartier divisors, on $Z_1 \amalg \cdots \amalg Z_r$ by means of the lifting $X_{/k}^{\text{smooth}} \to (\tilde{X}_{/k})_{\text{red}}$.*

Then (**) *is a commutative diagram.*

§ 2. Passage to the quotient under the action of a finite group

Let B be a semi-local noetherian ring and Max Spec (B) its (finite) set of maximal ideals. Let us suppose that for every maximal ideal P of B, B_P, the completion of B at P, is a discrete valuation ring whose field of fractions, K_P, is of characteristic 0. Let k_P denote the corresponding residue field.

Let G be a finite group which acts faithfully as a group of automorphisms of the ring B. Then the ring of G-invariant elements of B, denoted $\overline{B}$, is again a semi-local ring such that the completions $\overline{B}_{\overline{P}}$ at maximal ideals $\overline{P} \in \text{Max Spec } (\overline{B})$ are discrete valuation rings with fields of fractions $\overline{K}_{\overline{P}}$ of characteristic 0.

The group G operates naturally on Max Spec (B) and we have a bijection

$$\text{Max Spec}\,(B)/G \xrightarrow{\sim} \text{Max Spec}\,(\overline{B})$$

such that the G-orbit of a maximal ideal P of B is sent to $\overline{P} = P \cap \overline{B}$.

If $G_P \subset G$ is the decomposition subgroup associated to P (i.e., the isotropy group of $P \in \text{Max Spec}\,(B)$) we have the identification

$$\overline{K}_{\overline{P}} = (K_P)^{G_P},$$

$$\overline{B}_{\overline{P}} = (B_P)^{G_P}$$

where the superscript G_P refers to G_P-invariant elements.

Moreover, if $I_P \subset G_P$ is the inertia subgroup associated to P, then G_P/I_P operates faithfully on k_P and the natural morphism $\bar{k}_{\overline{P}} \to (k_P)^{(G_P/I_P)}$ identifies $\bar{k}_{\overline{P}}$ with a subfield over which $(k_P)^{(G_P/I_P)}$ is purely inseparable.

Now suppose that the ring B contains a subring A which is a discrete valuation ring with uniformizer π such that B is a flat (but not necessarily finite) A-algebra.

Suppose that the finite group G which acts on B leaves A stable. Finally, we suppose the "multiplicity-one condition":

$$\pi \cdot B = \prod_{P \in \mathrm{Max\,Spec}(B)} P.$$

That is, every maximal ideal P occurs *to the first power* in the prime decomposition of $\pi \cdot B$.

Write:

$$\bar{\pi} \cdot \bar{B} = \prod_{\bar{P} \in \mathrm{Max\,Spec}(\bar{B})} \bar{P}^{e_{\bar{P}}}$$

where $\bar{\pi}$ is a uniformizer of $\bar{A} = A \cap \bar{B}$ and $e_{\bar{P}}$ is the multiplicity of $\bar{P}$ in the prime decomposition of $\bar{\pi} \cdot \bar{B}$.

The following "criterion for multiplicity-one" will serve:

Proposition 1. *In the above situation, $e_{\bar{P}} = 1$ under either of these two conditions:*

(a) *A is an unramified extension of $\bar{A} = A \cap \bar{B}$.*

(b) *B is an extension of $\bar{B}$ which is totally ramified at $\bar{P}$, i.e. $\bar{k}_{\bar{P}} \to k_P$ is an isomorphism.*

We apply the above discussion in the following context. Let Y be a regular connected projective scheme of dimension two, and f: $Y \to S$ a flat morphism of finite type where S is the spectrum of a Dedekind domain whose field of fractions is of characteristic 0.

We suppose that G is a finite group acting on S, and faithfully on Y in such a manner that f is a G-equivariant morphism. Let $s \in S$ be a closed point, fixed under the action of G. Let Y_s denote the fiber of f at s. Make the "multiplicity-one hypothesis": i.e., suppose that Y_s is a reduced scheme. Equivalently, if we view Y_s as a Cartier divisor on Y, and we let $\mathscr{I}(Y_s)$ denote the set of irreducible subvarieties of codimension one in Y contained in Y_s, then $Y_s = \sum_{Z \in \mathscr{I}(Y_s)} Z$.

Now let $X = Y/G$ and $T = S/G$ be the quotient schemes under the action of G ([53, 37]). We have a natural morphism which we also call f:

$$f\colon X \to T.$$

If $t \in T$ is the image of s, let X_t denote the fiber of f at the point t. We denote by $\mathscr{I}(X_t)$ the set of irreducible subvarieties of X of codimension one, contained in X_t. Again we write X_t, viewed as Weil divisor on X, as follows:

$$X_t = \sum_{\bar{Z} \in \mathscr{I}(X_t)} e_{\bar{Z}} \cdot \bar{Z}$$

where the $e_{\bar{Z}} \in \mathbf{N}$ are the multiplicities.

Definition. *A closed point x of X (or more generally of any two-dimensional normal scheme of finite type) is called an* inconsequential singularity *if the inverse image of x in a desingularization of X contains no curve whose normalization is of positive genus.*

Proposition 2. *The quotient scheme X of the discussion above is normal with at worst inconsequential singularities. The irreducible components $\mathscr{I}(X_t)$ of X_t are in natural one: one correspondence with G-orbits of irreducible components of Y_s, the G-orbit of $Z \in \mathscr{I}(Y_s)$ being sent to the image-component of Z in X_t:*

$$\mathscr{I}(Y_s)/G \to \mathscr{I}(X_t).$$

Let $Z \in \mathscr{I}(Y_s)$ and let $G_Z \subset G$ denote the subgroup of G stabilizing the component Z (the isotropy subgroup). If $\overline{Z} \in \mathscr{I}(X_t)$ is the image-component of Z, then the natural map

$$Z/G_Z \to \overline{Z}$$

induces a radicial morphism from the normalization of the domain to the normalization of the range.

Under the following further hypothesis, the multiplicity $e_{\overline{Z}}$ of an irreducible component $\overline{Z}$ in the Cartier divisor X_t is equal to one.

Hypothesis $H(\overline{Z})$. *There is a normal subgroup $G_0 \subset G$ such that*

(a) $S \to S/G_0$ *is unramified at s,*

and

(b) $Y/G_0 \to Y/G = X$ *is totally ramified over $\overline{Z} \in \mathscr{I}(X_t)$.*

Proof. The scheme X is normal since Y is normal. The following argument establishes that X has at worst inconsequential singularities. Let $\tilde{X} \to X$ be a regular resolution of X and Y' the normalization of the fibre-product of $\tilde{X}$ and Y over X. Let $\tilde{Y}$ be a regular resolution of Y'. We have a diagram

$$\begin{array}{ccc} \tilde{Y} & \longrightarrow & Y \\ {\scriptstyle h}\downarrow & & \downarrow \\ \tilde{X} & \xrightarrow{g} & X \end{array}$$

where all the morphisms are proper.

Let x be a closed point of X. Then any reduced curve in $\tilde{Y}$ lying in the inverse image $(gh)^{-1}(x)$ must collapse to a point in Y; since $\tilde{Y}$ is regular, any such curve is of genus zero. It follows from the properness of h and Luroth's theorem that the normalization of any reduced curve in $g^{-1}(x)$ is also of genus zero.

The remainder of the proposition follows directly from the discussion concerning semi-local rings which began this paragraph, and from Proposition 1 above, where $A = \mathcal{O}_{S,s}$, the local ring of the scheme S at s, and where B is the subring of rational functions on Y which are regular at (the generic point of) each irreducible component of Y_s.

§ 3. Models of modular curves

Consider the following list of well-known subgroups of $\Gamma = PSL_2(\mathbf{Z})$:

If N is a positive integer, write

$$\Gamma(N)=\left\{\pm\begin{pmatrix}a & b\\ c & d\end{pmatrix}\equiv\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\text{ modulo } N\right\}\Big/(\pm 1),$$

$$\Gamma_1(N)=\left\{\pm\begin{pmatrix}a & b\\ c & d\end{pmatrix}\equiv\begin{pmatrix}1 & *\\ 0 & 1\end{pmatrix}\text{ modulo } N\right\}\Big/(\pm 1),$$

$$\Gamma_0(N)=\left\{\pm\begin{pmatrix}a & b\\ c & d\end{pmatrix}\,\middle|\, c\equiv 0 \text{ modulo } N\right\}\Big/(\pm 1).$$

If M is a divisor of N, write

$$\Gamma_1(N,M)=\left\{\pm\begin{pmatrix}a & b\\ c & d\end{pmatrix}\,\middle|\, c\equiv 0 \text{ modulo } N,\ a\equiv 1 \text{ modulo } M\right\}\Big/(\pm 1).$$

If m is prime to N, write

$$\Gamma_1(N;m)=\Gamma_1(N)\cap\Gamma(m),$$

$$\Gamma_1(N,M;m)=\Gamma_1(N,M)\cap\Gamma(m).$$

If $Y_{\mathbf{C}}$ denotes the quotient of the upper half-plane by the action of any of the above groups, let $X_{\mathbf{C}}$ denote the corresponding complete Riemann surface obtained by "adding" the appropriate finite set of cusps to $Y_{\mathbf{C}}$. For the above set of groups, we denote the corresponding set of complete Riemann surface by $X(N)_{\mathbf{C}}$, $X_1(N)_{\mathbf{C}}$, $X_0(N)_{\mathbf{C}}$, $X_1(N,M)_{\mathbf{C}}$, $X_1(N;m)_{\mathbf{C}}$, and $X_1(N,M;m)_{\mathbf{C}}$, respectively. These Riemann surfaces are finite branched coverings of the "j-line":

$$X_{\mathbf{C}}\xrightarrow{j}\mathbf{P}^1_{\mathbf{C}}.$$

In general, we shall be considering canonical models over two types of fields:

(a) $\mathbf{Q}(\zeta_d)$ where d is an integer, and ζ_d a "specified" primitive d-th root of unity. We adopt the convention that $\mathbf{Q}(\zeta_d)$ be viewed as a subfield of $\mathbf{C}$ via the imbedding $\zeta_d\to\exp(2\pi i/d)$.

(b) $\mathbf{Q}(\zeta_d)^+$ the maximal totally real subfield of $\mathbf{Q}(\zeta_d)$, viewed again as subfield of $\mathbf{Q}$. If $\zeta_d^+=\zeta_d+\zeta_d^{-1}$, then $\mathbf{Q}(\zeta_d^+)=\mathbf{Q}(\zeta_d)^+$.

Much work has been done in the direction of providing adequate ("canonical") algebraic models for these Riemann surfaces. One can distinguish two aspects to this problem:

1. Canonical models over number fields. Let $K\subset\mathbf{C}$ be a number field. The problem is to describe an algebraic curve $X_{/K}$ whose associated Riemann surface is $X_{\mathbf{C}}$ and such that the function j is rational over K. Any such curve we will call *a* canonical model of $X_{\mathbf{C}}$.

For example, when $X_{\mathbf{C}}=X_0(N)_{\mathbf{C}}$ and K any number field, we may take $X_{/K}$ to be the smooth projective curve whose function field is $K(j,j_N)$, where $j=j(\tau)$ is the elliptic modular function, and $j_N(\tau)=j(N\tau)$. All the curves described above do possess canonical models over $\mathbf{Q}$.

2. Canonical models over rings of integers. Let $X_{/K}$ be a canonical model as described above, and let $\mathcal{O}$ denote the ring of integers of K. Let $\mathbf{P}^1_{/\mathcal{O}}$ denote the "j-line over $\mathcal{O}$". Define $X_{/\mathcal{O}}$ to be the normalization of $X_{/K}$ over the j-line $\mathbf{P}^1_{/\mathcal{O}}$. Then $X_{/\mathcal{O}}$ is a (proper

two-dimensional) scheme finite over $\mathbf{P}^1_{/\mathcal{O}}$. But our succinct construction of $X_{/\mathcal{O}}$ is not sufficient to determine the geometry: which fibers of $X \to \operatorname{Spec} \mathcal{O}$ are smooth, the irreducible components of the fibers, their multiplicities, and the nature of the singularities.

The sucessful line of attack on these problems has been to provide a modular interpretation for the scheme $X_{/\mathcal{O}}$ (or for some suitable family of coverings of $X_{/\mathcal{O}}$ obtained by imposing auxiliary level structures).

By this method, for example, if $X_{/K}$ denotes either the standard choice of canonical model $X_1(M, N)_{/\mathbf{Q}}$ or the standard choice of canonical model $X(N)_{/\mathbf{Q}(\zeta_N)}$ Igusa [29] has proven that $X_{/\mathcal{O}[1/N]}$ is smooth. For a prime p dividing N the characteristic p fibres for some of these curves has been studied extensively in [15]. The ideas of Drinfeld [15] give a simpler formulation of the moduli problems in question and we will use these to describe a model for $X(N)_{/\mathbf{Z}[\zeta_N]}$ for suitable N (with auxiliary level structure). This will be sufficient for our purposes though we note that we do not analyze the singularities in the models we consider.

The modular interpretation which we take for $X_1(N)_{/\mathbf{Q}}$ ($N \geqq 5$) is that its noncuspidal points 'represent' isomorphism classes of pairs (E, e_N) where E is an elliptic curve and e_N is a point of E of order N. More precisely, it is the coarse moduli scheme for the function which assigns to a scheme S the S-isomorphism classes of such pairs. We identify the Riemann surface $X_1(N)_{\mathbf{C}}$ with $X_1(N)_{/\mathbf{Q}} \otimes \mathbf{C}$ via the map

$$z \mapsto (\mathbf{C}/(z, 1),\ 1/N). \tag{*}$$

§ 4. "Incomplete" models and Igusa curves

Fix p a prime number, a an integer relatively prime to p, and let $N = ap^n$.

We choose an 'auxiliary level' $m \geqq 3$ such that m is relatively prime to ap.

Let $\varphi_m(X) \in \mathbf{Z}[X]$ denote the m-th cyclotomic polynomial.

Thus

$$X^m - 1 = \prod_{1 \leqq d \mid m} \varphi_d(X)\ .$$

We shall work over the base $\mathcal{O}' = \mathbf{Z}_p[X]/(\varphi_m(X))$. Let $\zeta_m \in \mathcal{O}'$ denote the image of X. Note that $\mathcal{O}' = \mathbf{Z}_p[\zeta_m]$ is a product of finitely many discrete valuation rings, which are extensions of $\mathbf{Z}_p$ generated by primitive m-th roots of unity.

Consider the following moduli problem: to each $\mathcal{O}'$-algebra R we associate the set of isomorphism classes of triples

$$(E, e_N,\ \alpha)_{/R}$$

where $E_{/R}$ is an elliptic curve (i.e., an abelian scheme of dimension 1); e_N is a section of E over R which is annihilated by N, and which specializes to a point of order N in every residue field of R (equivalently: the section e_N generates an *étale* constant subgroupscheme, finite flat of order N in $E_{/R}$); finally, α is a level m structure of E over R of *determinant* ζ_m: that is, α is an isomorphism of the constant group-scheme $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ onto $E[m]_{/R}$ such that the Weil pairing $\langle \alpha(0,1, \alpha(1,0) \rangle$ is equal to ζ_m.

It is known that the above moduli problem has a coarse moduli scheme which is a smooth irreducible (but nonproper) scheme of dimension one over $\mathcal{O}'$. Denote this scheme $\mathcal{Y}_1(N; m)_{/\mathcal{O}'}$ and compare the discussion in ([35], 4.3).

All geometric fibers of $\mathcal{Y}_1(N; m)_{/\mathcal{O}'}$ are irreducible affine curves. The characteristic 0 fibers have the property that their smooth projective models are *canonical* models for $X_1(N; m)$ in the sense of § 2. The fact that the characteristic p fibers are irreducible is a result due to Igusa ([28, 35], 4.3). If k' is a residue field of $\mathcal{O}' = \mathbf{Z}_p[\zeta_m]$ of characteristic p, we let $Igusa(N; m)_{/k'}$ denote the smooth projective model of the affine curve $\mathcal{Y}_1(N; m)_{/k'}$. We thus have the inclusion

$$\mathcal{Y}_1(N; m)_{/k'} \hookrightarrow Igusa(N; m)_{/k'}.$$

The action of $GL_2(\mathbf{Z}/m\mathbf{Z})$ on $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ induces an action on level m structures: $\alpha \mapsto \alpha \cdot {}^t g$ where $g \in GL_2(\mathbf{Z}/m\mathbf{Z})$. This action has the following effect on determinants:

$$\det(\alpha^g) = (\det \alpha)^{\det g}$$

and consequently it induces an action on the scheme $\mathcal{Y}_1(N; m)_{/\mathcal{O}'}$ which does *not* preserve its $\mathcal{O}'$-scheme structure.

We define $\mathcal{Y}_1(N)_{/\mathbf{Z}_p}$ to be the quotient scheme $\mathcal{Y}_1(N; m)/GL_2(\mathbf{Z}/m\mathbf{Z})$ which is easily seen to be independent of m in the sense that we have canonical isomorphisms:

$$\mathcal{Y}_1(N; m)/GL_2(\mathbf{Z}/m\mathbf{Z}) = \mathcal{Y}_1(N; m')/GL_2(\mathbf{Z}/m'\mathbf{Z})$$

for $m, m' \geqq 3$.

The general fibre $\mathcal{Y}_1(N)_{/\mathbf{Q}_p}$ we identify with the open subscheme of $X_1(N)_{/\mathbf{Q}_p}$ obtained by removing the cuspidal points. The mapping $\mathcal{Y}_1(N)_{/\mathbf{Q}_p} \to X_1(N)_{/\mathbf{Q}_p}$ is induced from the mapping

$$(E, e_N, \alpha)_{/R} \to (E, e_N)_{/R}$$

of $\mathcal{Y}_1(N; m)_{/\mathcal{F}} \to X_1(N)_{/\mathcal{F}}$. (Here $\mathcal{F} = \mathbf{Q}_p[X]/(\varphi_m(X))$, and we let $GL_2(\mathbf{Z}/m\mathbf{Z})$ act on $X_1(N)_{/\mathcal{F}}$ via the determinant on $\mathcal{F}$).

We let $Igusa(N)_{/\mathbf{F}_p}$ denote a smooth projective model of $\mathcal{Y}_1(N)_{/\mathbf{F}_p}$.

§ 5. *Standard automorphisms and the Hecke operators*

1. *The "diamond" operators.* If r is an integer prime to N, let $\langle r \rangle$ denote the automorphism of the $\mathcal{O}'$-scheme $\mathcal{Y}_1(N; m)$ induced by sending the isomorphism class of triples $(E, e_N, \alpha)_{/R}$ to $(E, r \cdot e_N, \alpha)_{/R}$. Clearly, $\langle r \rangle$ depends only on the congruence class of the integer r modulo N. We let $\langle r \rangle$ also denote the automorphisms induced on $Igusa(N; m)_{/k'}$, on $\mathcal{Y}_1(N)_{/\mathbf{Z}_p}$, and on $Igusa(N)_{/\mathbf{F}_p}$.

These are called the *diamond operators.* Since $\langle -1 \rangle$ is the identity on $\mathcal{Y}_1(N)_{/\mathbf{Z}_p}$ and on $Igusa(N)_{/\mathbf{F}_p}$, the diamond operators give us an action of the group $(\mathbf{Z}/N\mathbf{Z})^*/(\pm 1)$ on these two schemes.

. *The involutions.* Let $\zeta = \zeta_N$ be a primitive N-th root of unity in $\bar{\mathbf{Q}}$ and consider the canonical model $X_1(N)_{/\mathbf{Q}}$. For any integer i relatively prime to N, one has an

involution of $X_1(N)_{/\mathbf{Q}(\zeta)}$ usually denoted w_{ζ^i}, and defined in terms of the moduli problem as follows.

If (E, e_N) represents an R-valued point of $X_1(N)_{/\mathbf{Q}(\zeta)}$, where R is a $\mathbf{Q}(\zeta)$-algebra, let $C_N \subset E[N]$ denote the subgroup of E generated by e_N, and let

$$\gamma\colon\ E[N]/C_N \to \boldsymbol{\mu}_N$$

denote the isomorphism defined by $x \to \langle x, e_N\rangle$ (where $\langle\,,\rangle$ is a fixed choice of Weil pairing).

Set $\bar{E} = E/C_N$ and $\bar{e}_N = \gamma^{-1}(\zeta^i)$. Define:

$$w_{\zeta^i}(E, e_N) = (\bar{E}, \bar{e}_N)\,.$$

This induces an involution of the curve $X_1(N)$ rational over $\mathbf{Q}(\zeta)^+$ independent of the choice of sign in the Weil pairing. We have

$$w_{\zeta^i} = w_{\zeta^{-i}}$$

and the set of operators

$$\{\langle \pm r\rangle,\ \pm r \in (\mathbf{Z}/N\mathbf{Z})^*/(\pm 1) \text{ and } w_{\zeta^{+i}},\ \pm i \in (\mathbf{Z}/N\mathbf{Z})^*/(\pm 1)\}$$

form a group of operators on the curve $X_1(N)_{/\mathbf{Q}(\zeta)^+}$ called the twisted dihedral group, and described further in §2 of [48].

Note that the involutions described here do *not* extend to involutions on $\mathscr{Y}_1(N)_{/\mathbf{Z}_p}$. If M is relatively prime to N, then there are involutions $w_{\zeta_N^i}$ of $X_1(N\cdot M)$ rational over the field $Q(\zeta_N)$, which fit into a commutative diagram:

$$\begin{array}{ccc} X_1(NM) & \xrightarrow{w_{\zeta_N^i}} & X_1(NM) \\ \downarrow & & \downarrow \\ X_1(N) & \xrightarrow{w_{\zeta_N^i}} & X_1(N) \end{array}$$

where the vertical arrows are given by $(E, e_{N\cdot M}) \mapsto (E, M\cdot e_{N\cdot M})$.

3. The automorphism w_l. Let l be a prime number not dividing N. Let $B_l \subseteq GL_2(\mathbf{Z}/\mathbf{Z})$ denote the subgroup of matrices of the form $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$. Define

$$\mathscr{Y}_1(N\cdot l, N)_{/\mathbf{Z}_p}$$

to be the quotient of the scheme $\mathscr{Y}_1(N; l)$ by the action of the group B_l. Then the fibre $\mathscr{Y}_1(Nl, N)_{/\mathbf{Q}_p}$ is an affine curve whose smooth projective model is a canonical model for $\Gamma_1(N\cdot l, N) = \Gamma_1(N) \cap \Gamma_0(l)$.

The $\mathbf{F}_p$-fiber, $\mathscr{Y}_1(Nl, N)_{/\mathbf{F}_p}$ is an irreducible affine curve, whose smooth projective model we denote $Igusa\,(Nl, N)_{/\mathbf{F}_p}$.

If R is a $\mathbf{Z}_p$-algebra, an R-valued point of $\mathscr{Y}_1(Nl, N)_{/\mathbf{Z}_p}$ may be represented by an R-isomorphism class of triples (E, e_N, C_l) where (E, e_N) is a pair as in 2. above, and C_l is a subgroup of order l in E.

We define an automorphism of the scheme $\mathscr{Y}_1(Nl, N)_{/\mathbf{Z}_p}$ by the rule:

$$(E, e_N, C_l) \xrightarrow{w_l} (\bar{E}, \bar{e}_N, \bar{C}_l)$$

where:

$$\bar{E} = E/C_l, \quad \bar{e}_N = \text{image of } e_N \text{ in } \bar{E}, \text{ and } \bar{C}_l = E[l]/C_l.$$

Note that w_l is not an involution: $w_l^2(E, e_N, C_l) = (E, le_N, C_l)$. The automorphism w_l extends to an automorphism of $X_1(Nl, N)_{/\mathbf{Q}}$ and of $Igusa(Nl, N)_{/\mathbf{F}_p}$.

4. The Hecke operators $T_l (l \nmid N)$. If $f: U \to V$ is a finite morphism of smooth proper curves, let f_*: $\mathrm{jac}(U) \to \mathrm{jac}(V)$ and f^*: $\mathrm{jac}(V) \to \mathrm{jac}(U)$ denote the induced mappings on jacobians, where in the first instance we interpet the jacobian as "Albanese variety" and in the second as Pic^0. For simplicity we sometimes denote f_* by f.

Let

$$\begin{array}{ccc} X_1(Nl, N)_{/\mathbf{Q}} & \mathscr{Y}_1(Nl, N)_{/\mathbf{Z}_p} & Igusa(Nl, N)_{/\mathbf{F}_p} \\ \pi \downarrow & \pi \downarrow & \pi \downarrow \\ X_1(N)_{/\mathbf{Q}} & \mathscr{Y}_1(N)_{/\mathbf{Z}_p} & Igusa(N)_{/\mathbf{F}_p} \end{array}$$

be the natural projections.

Consider the endomorphisms of $J_1(N)_{/\mathbf{Q}} = \mathrm{jac}(X_1(N)_{/\mathbf{Q}})$ defined by the formulae:

$$\begin{aligned} T_{l*} &= \pi_* \cdot w_{l*} \cdot \pi^* \\ T_l^* &= \pi_* \cdot w_l^* \cdot \pi^*. \end{aligned} \tag{1}$$

We have

$$\begin{aligned} w_l^* &= \langle l^{-1} \rangle \cdot w_{l*} \\ T_l^* &= \langle l^{-1} \rangle \cdot T_{l*}. \end{aligned} \tag{2}$$

The endomorphism T_{l*} is the endomorphism of the Albanese variety $J_1(N)_{/\mathbf{Q}}$ induced by the correspondence

$$(E, e_N) \to \sum_{C_l} (E/C_l, \text{ image of } e_N \text{ in } E/C_l) \tag{3}$$

where the summation is taken over all subgroups of order l, $C_l \subset E[l](\bar{\mathbf{Q}})$.

We denote T_{l*} simply T_l and refer to it as the (l-th) *Hecke operator*. Consider the endomorphism of $j_1(N)_{/\mathbf{F}} = \mathrm{jac}(Igusa(N)_{/\mathbf{F}_p})$ defined by the analogous formulae:

$$\begin{aligned} t_{l*} &= \pi_* w_{l*} \pi^* \\ t_l^* &= \pi_* w_l^* \pi^*. \end{aligned} \tag{4}$$

Again,

$$t_l^* = \langle l^{-1} \rangle \cdot t_{l*}. \tag{5}$$

5. The Atkin operators $U_q (q \mid N)$. For prime numbers q dividing N there are endomorphisms U_q of $J_1(N)_{/\mathbf{Q}}$ (cf. [2, 40], Chap. VIII) whose description as self-correspondences of the curve $X_1(N)_{/\mathbf{Q}}$ is given as follows. If (E, e_N) is a $\bar{\mathbf{Q}}$-valued point of $Y_1(N)_{/\mathbf{Q}}$, then

$$U_q \cdot (E, e_N) = \sum_{C_q} (E/C_q, \text{ image of } e_N \text{ in } E/C_q) \tag{6}$$

where the summation is over those subgroups C_q of order q in $E[q](\bar{\mathbf{Q}})$ which are *not* contained in the subgroup of E generated by e_N. The operator U_q can be defined by a procedure analogous to the definition of T_l as follows. Let $\Gamma \subset SL_2(\mathbf{Z})$ denote the subgroup of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ such that $a \equiv 1 \bmod N$, $c \equiv 0 \bmod N$, and $b \equiv 0 \bmod q$. One gets a canonical model for Γ over **Q** by representing the moduli problem which associated to a **Q**-algebra R the set of R-isomorphism classes of triples $(E, e_N, C_q)_{/R}$ where e_N is a point of order N, and C_q is a subgroup of order q in E which is not contained in the subgroup generated by e_N. Call the projective smooth model of the schemes representing the above moduli problem $Z_{/\mathbf{Q}}$. There are two finite morphisms $\Phi, \Psi: Z_{/\mathbf{Q}} \to X_1(N)_{/\mathbf{Q}}$, defined on the moduli problems by the rules:

$$\Phi\colon\ (E, e_N, C_q) \to (E, e_N),$$
$$\Psi\colon\ (E, e_N, C_q) \to (E/C_q,\ \text{image of } e_N \text{ in } E/C_q).$$

we define:

$$U_q = U_{q*} = \Psi_* \cdot \Phi^* \quad \text{and} \quad U_q^* = \Phi_* \cdot \Psi^*. \tag{7}$$

An important distinction arises between the primes q dividing N which are different from p, and $q = p$, when we try to define operators u_{q*} and u_q^* on the Igusa curves, in analogy with the Atkin operators U_{q*} and U_q^*.

The case $q \mid N$, $q \neq p$:

Let $m \geqq 3$ denote an auxiliary level and k' as in §1, and define

$$u_q = u_{q*}\colon \operatorname{jac}(Igusa(N; m)_{/k'}) \to \operatorname{jac}(Igusa(N; m)_{/k'})$$

to be the endomorphism induced from the self-correspondence on $Igusa(N; m)_{/k'}$ which is characterized on $\bar{k}'$-valued points of $\mathscr{Y}_1(N; m)$ by the rule:

$$u_q(E, e_N, \alpha) = \sum_{C_q} (E/C_q,\ \text{image of } e_N \text{ in } E/C_q,\ \bar{\alpha}) \tag{8}$$

where C_q runs through all subgroups of order q in $E[q](\bar{k}')$ which are not contained in the subgroup generated by e_N, and $\bar{\alpha}$ is the level m structure induced from α. One can give a description of u_{q*} as a composition of morphisms in analogy with the definition of U_{q*} given in (7) and, in this way, we may define u_q^* as well.

Specifically, to define the analogue of $Z_{/\mathbf{Q}}$ in characteristic p one simply takes the incomplete model corresponding to the group $\Gamma_1(N) \cap \Gamma(q) \cap \Gamma(m)$. Then we define u_q^* and u_{q*} on $\operatorname{jac}(Igusa(N)_{/\mathbf{F}_p})$ by taking the induced action viewing it as a quotient of $\operatorname{jac}(Igusa(N; m)_{/k'})$ by the action of $GL_2(\mathbf{Z}/m\mathbf{Z})$.

The case $q = p$:

Here there is no obvious extension to $\mathscr{Y}_1(N)_{/\mathbf{Z}_p}$ of U_p^* and U_{p*}, but see (§10).

6. *Basic properties*

(a) (Recall) $T_{l*} = \langle l \rangle T_l^* \ \langle r \rangle_* = \langle r^{-1} \rangle^*$,

(b) The operators $T_l (l \nmid N)$, $U_q (q \mid N)$ and $\langle r \rangle$, $(r \in (\mathbf{Z}/N\mathbf{Z})^*)$ all commute. Call these operators the *standard operators*.

(c) If $\alpha = \langle r \rangle$, T_l or U_q (with the restrictions on r, l, and q as in (b) above), then

$$w_{\zeta_N^{-1}} \cdot \alpha^* \cdot w_{\zeta_N} = \alpha_* .$$

Remark. U_{q*} and U_q^* do not necessarily commute.

7. *Effect on cusps.* The action of the Hecke operators (as correspondences) on the cusps can be computed over $\mathbf{C}$. We obtain the following formulae for them acting on ∞: $(= [\begin{smallmatrix}1\\0\end{smallmatrix}]$ in the usual notation, cf. Chap. 4).

$$(T_{l*}) \cdot \infty = (l + \langle l \rangle) \cdot \infty \qquad \text{for } l \nmid N,$$

$$(U_{q*}) \cdot \infty = q \cdot \infty \qquad \text{for } q \mid N,$$

$$(U_q^*) \cdot \infty = \infty + \sum_{a=1}^{q-1} \begin{bmatrix} -1 \\ (N/q) \cdot a \end{bmatrix} \qquad \text{for } q \mid N.$$

Likewise the action on the cusp zero $(= [\begin{smallmatrix}0\\1\end{smallmatrix}]$ in the usual notation) is:

$$(T_{l*}) \cdot \mathbf{0} = (1 + l\langle l \rangle) \cdot \mathbf{0} \quad \text{for } l \nmid N,$$

$$(U_q^*) \cdot \mathbf{0} = q \cdot \mathbf{0} \qquad \text{for } q \mid N,$$

$$(U_{q*}) \cdot \mathbf{0} = \mathbf{0} + \sum_{a=1}^{q-1} \begin{bmatrix} a \\ q \end{bmatrix} \quad \text{for } q \mid N.$$

8. *Effect on differentials.* If $f: Y \to X$ is a finite morphism of smooth curves over a field K we denote by f^d: $H^0(X, \Omega^1_{X/K}) \to H^0(Y, \Omega^1_{Y/K})$ the induced morphism on regular differentials. When $X_{/K}$ and $Y_{/K}$ are proper there is also a trace mapping f_d: $H^0(Y, \Omega^1_{Y/K} \to H^0(X, \Omega^1_{X/K})$ obtained, for example, by applying duality to the induced morphism on global regular functions. Using the definitions of the Hecke correspondences in §5.4 and §5.5 we obtain endomorphisms of the spaces of regular differentials $H^0(X_1(N)_{/\mathbf{Q}}, \Omega^1)$ and $H^0(Igusa(N)_{/\mathbf{F}_p}, \Omega^1)$. If, for example, we write π_1 and π_2 for the two maps π and $\pi \circ w_l$ of $X_1(Nl, N)_{/\mathbf{Q}}$ to $X_1(N)_{/\mathbf{Q}}$ (cf. § 4) then we would naturally write $(T_l)^d = (\pi_1)_d \circ (\pi_2)^d$ and $(T_l)_d = (\pi_2)^d \circ (\pi_1)_d$. The classical action of the Hecke operators on differentials is that of $(T_l)^d$.

There is a second way of obtaining an action of the Hecke operators on the space of differentials and that is by viewing them as the cotangent spaces of the respective Jacobians. Thus if we use a superscript c to denote the action on cotangent spaces we may consider the actions of $(T_l^*)^c$ and $(T_{l*})^c$ on $H^0(X_1(N)_{/\mathbf{Q}}, \Omega^1)$. One checks that

$$(T_l^*)^c = (T_l)_d \quad \text{and} \quad (T_{l*})^c = (T_l)^d .$$

We will always use the action of $(T_l)^d$ on differentials and simply write T_l for it. We note that this action is induced by $(T_l)_*$ on $J_1(N)_{/\mathbf{Q}}$ which we have also sometimes abbreviated T_l.

§ 6. *Drinfeld bases*

Recall that $\varphi_N(X)$ denotes the cyclotomic equation of order N, so that $X^N - 1 = \prod_{1 \leq d \mid N} \varphi_d(X)$.

If R is a commutative ring, *a primitive N-th root of unity ζ_N of R* is an element of R satisfying the cyclotomic equation $\varphi_N(\zeta_N) = 0$.

For example, if R is a reduced ring of characteristic p, then the identity element 1 is the unique primitive p^n-th root of unity in R, for any n.

Let $\boldsymbol{\mu}_N^*$ be the functor which associates to a commutative ring R the set of primitive N^{th} roots of unity of R. The functor $\boldsymbol{\mu}_N^*$ is representable by an affine scheme $\boldsymbol{\mu}_N^*$ and *if we fix a primitive N^{th} root of unity ζ_N* of $\mathbf{Z}[X]/(\varphi_N(X))$ we obtain an isomorphism of $\boldsymbol{\mu}_N^*$ with $\operatorname{Spec}\mathbf{Z}[X]/(\varphi_N(X))$.

For later purposes, note that the group $GL_2(\mathbf{Z}/N\mathbf{Z})$ acts on $\boldsymbol{\mu}_N^*$ by the rule $g \circ \zeta = \zeta^{\det g}$.

Let N be a positive integer, and S a "base scheme". Let E^* be a generalized elliptic curve over S in the sense developed in ([15, II); we require that E^* be a proper flat S-scheme whose geometric fibers are either elliptic curves or "polygons with N sides" ([15], II, §1). The subscheme E of smooth points of $E^*_{/S}$ is open and dense in E^* and is endowed with the structure of smooth group scheme over S. The subgroup scheme $E[N]_{/S}$ is a finite flat group scheme over S of order N^2.

The "Weil pairing" on points of order N induces an isomorphism between $E[N]_{/S}$ and its Cartier dual. If t_1, t_2 are two sections of E over an S-scheme S' we denote the Weil pairing by

$$\langle t_1, t_2 \rangle \in \boldsymbol{\mu}_N(S').$$

The closed subscheme $E[N] \subset E$ (which is the inverse image of the 0-section under the faithfully flat morphism $[N] =$ multiplication-by-N) may be viewed as a *Cartier divisor* in $E_{/S}$. Also, if t is any S-valued section of $E[N]$ we may view $t(S) \subset E$ and $[a] \cdot t(S) \subset E$ for any $a \in \mathbf{Z}/N\mathbf{Z}$ as *Cartier divisors*. Given a pair t_1, t_2 of S-valued sections we may form the Cartier divisor

$$Z(t_1, t_2) = \sum_{(a_1, a_2) \in \mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}} [a_1] \cdot t_1(S) + [a_2] \cdot t_2(S).$$

We say that (t_1, t_2) form a *Drinfeld basis of level N for $E_{/S}$* if t_1 and t_2 are S-valued sections of $E[N]$ such that we have an equality between the Cartier divisors $Z(t_1, t_2) = E[N]$, and such that $\langle t_1, t_2 \rangle$ is a primitive N-th root of unity over S. Refer to $\langle t_1, t_2 \rangle$ as the *determinant* of the Drinfeld basis (t_1, t_2).

It $S = \operatorname{Spec} R$, and $\zeta_N \in R$ is a primitive N-th root of unity, we say that the pair (t_1, t_2) form a *Drinfeld ζ_N-basis of level N* if they form a Drinfeld basis of level N, and if we have the equality

$$\langle t_1, t_2 \rangle = \zeta_N \in R.$$

Examples. 1. Suppose that the residual characteristics of the points of S do not divide N.

Then a Drinfeld basis of level N is the same as a *level N structure* on $E_{/S}$. Explicitly, given a Drinfeld basis (t_1, t_2) we obtain an isomorphism of the constant group scheme $\mathbf{Z}/N\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}$ onto $E[N]_{/S}$ by sending (a_1, a_2) to $[a_1] \cdot t_1(R) + [a_2] \cdot t_2(R)$. A Drinfeld ζ_N-basis is the same as a level N structure of determinant ζ_N.

2. Suppose that S is the spectrum of a discrete valuation ring whose field of fractions K is of characteristic 0.

Then a Drinfeld basis of level N of $E_{/S}$ is the same as a level N structure on $E_{/K}$.

3. Suppose that $S = Spec\ k$ where k is a perfect field of characteristic p. Suppose further that $N = p^n$. Then we have two cases to consider:

(i) $E_{/k}$ is *supersingular*. In this case the Cartier divisor $E[N]$ is simply the origin of E taken with multiplicity p^{2n}. The only Drinfeld basis of level N is given by $t_1 = t_2 =$ the zero-section.

(ii) $E_{/k}$ is *ordinary*. In this case, $E_{/k}$ possesses a Drinfeld basis of level N (over k) if and only if the k-rational points of $E[N]$ form a cyclic group of order N. By choice of a generator we may identify this cyclic group with the group $\mathbf{Z}/N\mathbf{Z}$; under this identification, t_1 and t_2 are identified with integers modulo N, α_1 and α_2 respectively. One has that (t_1, t_2) form a Drinfeld basis of level N if and only if at least one of the two integers α_1, α_2 generate $\mathbf{Z}/N\mathbf{Z}$, i.e. is prime to p.

4. Suppose S is a smooth (irreducible) curve of characteristic p, and let $N = p^n$. Suppose further that E is ordinary at the generic point η of S, and consequently $E[N]_{/S}$ is generically ordinary. Let t be an S-valued section of $E[N]$ whose restriction to η is a generator of the étale (constant) group scheme $E[N]^{\text{ét}}_{/\eta}$. Thus $(E_{/S}, t)$ determines an S-valued point of the *Igusa curve of level N*. Let (α_1, α_2) be a pair of integers modulo N such that one of the two is prime to p.

Set $t_1 = [\alpha_1] \cdot t$, $t_2 = [\alpha_2] \cdot t$. Then (t_1, t_2) form a Drinfeld basis of level N for $E_{/S}$.

5. Let S be an irreducible scheme whose generic point is of characteristic 0 and let ζ_N be a primitive root of unity in the ring of global sections of S. Let $E_{/S}$ possess a Drinfeld basis of level N, (t_1, t_2). If $A \in GL_2(\mathbf{Z}/N\mathbf{Z})$ is a matrix:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

let (t_1', t_2') be given by the formula $(t_1, t_2) \cdot {}^tA = (t_1', t_2')$. Then (t_1', t_2') is again a Drinfeld basis. Clearly, $\langle t_1', t_2' \rangle = \langle t_1, t_2 \rangle^{\det A}$. The set of Drinfeld bases of level N on $E_{/S}$ is a principal homogeneous set under the action of $GL_2(\mathbf{Z}/N\mathbf{Z})$ and the set of Drinfeld ζ_N-bases of level N is a principal homogeneous set under the action of $SL_2(\mathbf{Z}/N\mathbf{Z})$.

6. Let us return to the case of Example 2, where S is the spectrum of a discrete valuation ring whose field of fractions K is of characteristic 0. Suppose, further that the residue field k is a perfect field of characteristic p, that $N = p^n$, and that the special fibre $E_{/k}$ is ordinary. Fix a primitive N-th root of unity ζ_N in K. We shall say that a Drinfeld basis (t_1, t_2) is *adapted* (in this situation) if t_1 specializes to the zero-section over k, and, consequently, t_2 specializes to a generator of $E(k)[N]$. It is useful, when we encounter such a situation, to *fix* an adapted Drinfeld basis (τ_1, τ_2), and to represent all the other ζ_N-bases as $(\tau_1, \tau_2)^t A$, where A varies through $SL_2(\mathbf{Z}/N\mathbf{Z})$.

The subgroup $B \subset GL_2(\mathbf{Z}/N\mathbf{Z})$ of upper triangular matrices, $B = \left(\begin{smallmatrix} a & r \\ 0 & d \end{smallmatrix}\right)$ operates transitively on the set of 'adapted' Drinfeld bases.

7. Let $N = m \cdot p^n$ where m is prime to p. Let ζ_N be a primitive N-th root of unity in R. Then $\zeta_m = (\zeta_N)^{p^n}$ and $\zeta_{p^n} = (\zeta_N)^m$ are primitive m-th and p^n-th roots of unity, respectively, in R. To give a Drinfeld ζ_N-basis of level N for $E^*_{/R}$ is equivalent to

giving a *pair* consisting in a Drinfeld ζ_{p^n}-basis of level p^n, and a Drinfeld ζ_m-basis of level m for $E^*_{/R}$.

$$\xi_N \longleftrightarrow (\xi_{p^n}, \xi_m). \qquad (*)$$

We have the natural product decomposition

$$GL_2(\mathbf{Z}/N\mathbf{Z}) = GL_2(\mathbf{Z}/p^n\mathbf{Z}) \times GL_2(\mathbf{Z}/m\mathbf{Z})$$
$$A \longleftrightarrow (A^{(p^n)}, \quad A^{(m)})$$

which is compatible with the correspondence $(*)$ in the sense that

$$\xi_N \cdot t_A = (\xi_{p^n} \cdot {}^tA^{(p^n)}, \ \xi_m \cdot {}^tA^{(m)}).$$

In what follows, the action of $GL_2(\mathbf{Z}/p^n\mathbf{Z})$ will play an especially important role.

Now fix a prime number p, an "auxiliary level" $m \geqq 3$ not divisible by p, and set $N = m \cdot p^n$ for some $n \geqq 1$. Consider

$$\mathscr{X}(N)\colon R \longrightarrow \left\{\begin{matrix}\text{isomorphism classes of pairs} \\ (E^*, (t_1, t_2))_{/R}\end{matrix}\right\}$$

where R runs through the members of the category of commutative rings, and $E^*_{/R}$ is a generalized elliptic curve over R, with (t_1, t_2) a Drinfeld basis of level N for R^* over R.

We have a morphism of functors

$$\mathscr{X}(N) \to \boldsymbol{\mu}^*_N,$$
$$(E^*, (t_1, t_2)) \to \langle t_1, t_2 \rangle$$

which we refer to as the *structural morphism*. It is equivariant with respect to the $GL_2(\mathbf{Z}/N\mathbf{Z})$-action defined on domain and range (cf. opening remarks and Example 5 above).

The following theorem is due to Drinfeld (unpublished). See pp. 152, 153 of [15] for a discussion of this theorem and its antecedents. See also [36] (First Main Theorem of Chap. IV, and Chap. XIII.)

Theorem. *The function $\mathscr{X}(N)$ is representable by a projective scheme over* **Z** *naturally endowed with "structural morphism" to $\boldsymbol{\mu}^*_N$. Denote this scheme $X(N)_{/\boldsymbol{\mu}^*_N}$.*

Choosing an isomorphism

$$\operatorname{Spec} \mathbf{Z}[\zeta_N] \underset{=}{\longrightarrow} \boldsymbol{\mu}^*_N$$

(i.e., choosing a "primitive N-th root of unity") we may identify $X(N)_{/\boldsymbol{\mu}^*_N}$ with the canonical model $X(N)_{/\mathbf{Z}[\zeta_N]}$ as described in § 3.

We have a natural action of $GL_2(\mathbf{Z}/N\mathbf{Z})$ on $X(N)$ and on the base $\boldsymbol{\mu}^*_N$ compatible with structural morphism.

The morphism $X(N) \to \operatorname{Spec} \mathbf{Z}[\zeta_N]$ is proper and flat with one-dimensional fibres described as follows.

The fibres in characteristic 0 are smooth irreducible curves. Indeed, if K is a field of characteristic 0, then a choice of primitive N-th root of unity in K is equivalent to

giving a homomorphism $\mathbf{Z}[\zeta_N] \to K$ *and the scheme* $X(N)_{/K}$ *obtained by base change via this homomorphism is isomorphic to the canonical model of the modular curve associated to* $\Gamma(N)$ *over* K *(§ 3).*

If k *is a characteristic* p *residue field of* $\mathbf{Z}_p[\zeta_N]$, *then the fibre* $X(N)_{/k}$ *is a union of irreducible components, each of which is a reduced smooth curve isomorphic to* $Igusa(p^n; m)_{/k}$. *The group* $GL_2(\mathbf{Z}/p^n\mathbf{Z})$, *which acts in the natural way (cf. Example 7) on* $X(N)$, *operates transitively on the set of irreducible components of* $X(N)_{/k}$[3]. *If* c *is such an irreducible component, and* $B_c \subset GL_2(\mathbf{Z}/p^n\mathbf{Z})$ *is the stabilizer (i.e., isotropy group) of the component* c, *then as* c *runs through the set of irreducible components of* $X(N)_{/k}$, *the subgroups* B_c *run through all subgroups of* $GL_2(\mathbf{Z}/p^n\mathbf{Z})$ *which are conjugate to the subgroup* $B \subset GL_2(\mathbf{Z}/p^n\mathbf{Z})$ *of upper triangular matrices. Making a choice of "base component"* c, *we may identify the set of irreducible components of* $X(N)_{/k}$, *viewed as a set with* $GL_2(\mathbf{Z}/p^n\mathbf{Z})$*-action, with:*

$$\mathbf{P}^1(\mathbf{Z}/p^n\mathbf{Z}) = GL_2(\mathbf{Z}/p^n\mathbf{Z})/B_c = SL_2(\mathbf{Z}/p^n\mathbf{Z})/SB_c$$

$$\text{where } SB_c = B_c \cap SL_2(\mathbf{Z}/p^n\mathbf{Z}).$$

All irreducible components of $X(N)_{/k}$ *meet at every supersingular point and, except for this, there are no further intersections between distinct irreducible components.*

Further discussion

Picture of a characteristic p *fibre.* Suppose that $N = m \cdot p$. Then there are $p+1 = \#(\mathbf{P}^1(\mathbf{F}_p))$ components, each isomorphic to $Igusa(p; m)$ all of which meet at every supersingular point, these intersections being *pairwise* transversal. For $p = 2$ we would have the following "schematic" diagram:

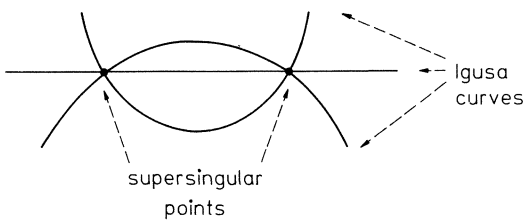


Fig. 1

Specialization of a given "ordinary elliptic curve" to characteristic p: Let S denote the spectrum of a discrete valuation ring which is a finite $\mathbf{Z}_p[\zeta_N]$-algebra. Let $E_{/S}$ be an elliptic curve over S, with ordinary reduction in characteristic p. Suppose a Drinfeld ζ_N-basis $\xi_N = (\xi_{p^n}, \xi_m)$ is given for $E_{/S}$, as in Example 7 above. Suppose, further, that ξ_{p^n} is *adapted* in the sense of Example 6 above.

---

[3] This is indeed an action *over* k, for the reader will recall that the subgroup $(\mathbf{Z}/p^n\mathbf{Z})^*$ of

$$(\mathbf{Z}/p^n\mathbf{Z})^* \times (\mathbf{Z}/m\mathbf{Z})^* = (\mathbf{Z}/N\mathbf{Z})^* = \mathrm{Gal}(\mathbf{Q}(\zeta_N)/\mathbf{Q})$$

is the inertia group for primes of residual characteristic p

Then as A runs through the elements of $SL_2(\mathbf{Z}/p^n\mathbf{Z})$, the specializations to a residue field k' of $\mathbf{Z}_p[\zeta_N]$ of characteristic p of the S-valued sections of $X(N)$ represented by the triples

$$e_A = (E_{/S},\ \xi_{p^n} \cdot {}^tA,\ \xi_m)$$

will lie on every irreducible component of $X(N)_{/k'}$. The specializations to k of the S-valued sections represented by e_A and $e_{A'}$ lie on the same irreducible component of $X(N)_{/k'}$ if and only if A and A' are in the same left-coset of $SL_2(\mathbf{Z}/p^n\mathbf{Z})$ relative to the subgroup B of upper triangular matrices.

Explicit relationship between Igusa curves and the characteristic p fibre. Let G be a finite group and $H \subset G$ a subgroup. Let Sch_G denote the category of schemes endowed with an action of G, as group of automorphisms. Let Ind_H^G denote the left adjoint to the "forgetful functor" $Sch_G \dashrightarrow Sch_H$. That is, if $X \in Sch_G$ and $Y \in Sch_H$ then we have 'natural isomorphisms'

$$\mathrm{Hom}_G(\mathrm{Ind}_H^G Y, X) = \mathrm{Hom}_H(Y, X).$$

Given a representative system $\{g_1, g_2, \ldots, g_r\}$ for left cosets of G relative to H, we may construct $\mathrm{Ind}_H^G Y$ explicitly as the disjoint union of r copies of Y, which may be conveniently labelled as follows:

$$\mathrm{Ind}_H^G Y = g_1 \cdot Y \amalg g_2 \cdot Y \amalg \cdots \amalg g_r \cdot Y.$$

To describe the group action of G on $\mathrm{Ind}_H^G Y$, it sufficies to say what the effect of an arbitrary element $g \in G$ is, on $g_i \cdot y$ for $1 \leqq i \leqq r$, and y a point in $Y(R)$ for R any ring. We have that $g \cdot g_i$ is equal to $g_j \cdot h$ for a unique j and $h \in H$. Then $g \cdot g_i \cdot y = g_j \cdot h \cdot y$.

Now let $B_p \subset GL_2(\mathbf{Z}/p^n\mathbf{Z})$ denote the subgroup of upper triangular matrices. Thus $h \in B_p$ may be written $h = \left(\begin{smallmatrix} a & z \\ 0 & d \end{smallmatrix}\right)$. If the triple $(E, e_{p^n}, \xi_m)_{S'} = \mathbf{e}$ represents an S'-valued point of the Igusa curve $Igusa(p^n; m)_{/k'}$ where S' is a k'-scheme, $E_{/S'}$ is an elliptic curve, e_{p^n} is an S'-valued section of E which generates an étale subgroup of order p^n, and ξ_m is a level m structure, then define $h \cdot \mathbf{e} = \langle a \rangle \mathbf{e}$ where $\langle a \rangle$ is the diamond operator explained in §5.1. This induces an action of the group B_p on $Igusa(p^n; m)_{/k'}$. We may now define a morphism

$$\varphi\colon\ \mathrm{Ind}_{B_p}^{GL_2(\mathbf{Z}/p^n\mathbf{Z})}\ Igusa(p^n; m)_{/k'} \to X(N)_{/k'}$$

which is equivariant with respect to the $GL_2(\mathbf{Z}/p^n\mathbf{Z})$ action of domain and range. By the functorial property of Ind to define φ it suffices to define a B_p-equivariant mapping from $Igusa(p^n; m)_{/k'}$ to $X(N)_{/k'}$, and this we do by specifying such a mapping on points represented by triples $\mathbf{e}$ as above.

Explicitly, we send the triple $\mathbf{e}$ to the S'-valued point of $X(N)_{/k'}$ represented by (E, ξ_{p^n}, ξ_m) where ξ_{p^n} is the Drinfeld basis of level p^n: $(e_{p^n}, 0)$, and we call the component of $X(N)_{/k'}$ on which it lies the *base component*.

One sees easily that the mapping φ "is" the normalization of $X(N)_{/k'}$ in the sense that if $\widetilde{X(N)}_{/k'}$ denotes the normalization, there is an isomorphism

$$i\colon\ \mathrm{Ind}_{B_p}^{GL_2(\mathbf{Z}/p^n\mathbf{Z})} \{Igusa(p^n; m)_{/k'}\} \underset{\cong}{\longrightarrow} \widetilde{X(N)}_{/k'}$$

such that φ is the composition of i with the natural projection $\widetilde{X(N)} \to X(N)$.

§ 7. Actions of finite groups and quotient modular schemes

Let H denote a subgroup of $GL_2(\mathbf{Z}/N\mathbf{Z})$ containing the matrix $\left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right)$. For simplicity, we make the further hypothesis that

$$H = H_p \times H_m \subseteq GL_2(\mathbf{Z}/p^n\mathbf{Z}) \times GL_2(\mathbf{Z}/m\mathbf{Z}) = GL_2(\mathbf{Z}/N\mathbf{Z})$$

for subgroups $H_p \subset GL_2(\mathbf{Z}/p^n\mathbf{Z})$, and $H_m \subset GL_2(\mathbf{Z}/m\mathbf{Z})$.

Let $\det H \subset (\mathbf{Z}/N\mathbf{Z})^*$ denote the image of H under the determinant homomorphism. Let $SH = H \cap SL_2(\mathbf{Z}/N\mathbf{Z})$ and $SH_p = H_p \cap SL_2(\mathbf{Z}/p^n\mathbf{Z})$. Let $\Gamma \subset SL_2(\mathbf{Z})$ denote the full inverse image of SH under the homomorphism

$$SL_2(\mathbf{Z}) \longrightarrow\!\!\!\!\rightarrow SL_2(\mathbf{Z}/N\mathbf{Z}).$$

Let $R_H \subset \mathbf{Z}_p[\zeta_N]$ denote the subring of elements invariant under the action of $\det H$.

Define $X(N; H)$ to be the *quotient scheme* obtained from $X(N)$ by passage to the quotient under the action of the group H. Then $X(N; H)$ inherits the structure of R_H-scheme.

Proposition. *The scheme $X(N; H)$ is the quotient of a regular scheme by the action of a finite group of automorphisms. It is normal, and has only inconsequential singularities. The R_H-scheme $X(N; H)$ is a "canonical model" for X_Γ over the ring R_H.*

The characteristic 0 fibers of $X(N; H)$ are irreducible smooth projective curves. Let

$$\begin{array}{ccc} \mathbf{Z}_p[\zeta_N] & \longrightarrow\!\!\!\!\rightarrow & k' \\ \uparrow & & \uparrow \\ R_H & \longrightarrow\!\!\!\!\rightarrow & k \end{array}$$

be a commutative diagram, where k'/k is a (finite) extension of finite fields of characteristic p.

The set of irreducible components of $X(N; H)_{/k}$ is in canonical one: one correspondence with the set of H_p-orbits of irreducible components of $X(N)_{/k}$. This set may be identified with the set of double cosets:

$$H_p \backslash GL_2(\mathbf{Z}/p^n\mathbf{Z})/B_p.$$

The scheme $X(N; H)_{/k}$ is reduced if $\det H_p = 1$.

If $\widetilde{X(N; H)}_{/k}$ denotes the normalization of $(X(N; H)_{/k})_{\mathrm{red}}$, there is a natural radicial morphism

$$\frac{\mathrm{Ind}_{B_p}^{GL_2(\mathbf{Z}/p^n\mathbf{Z})} \{Igusa(p^n; m)_{/k'}\}}{H} \xrightarrow{\varphi} \widetilde{X(N; H)}_{/k}$$

where the domain is the quotient of $\mathrm{Ind}_{B_p}^{GL_2(\mathbf{Z}/p^n\mathbf{Z})} Igusa(p^n; m)_{/k'}$ by the (natural action of) H.

Proof. The above proposition is a straightforward deduction from Drinfeld's theorem and §2, Proposition 2. Note that if $\det H_p = 1$ and if $G = G_0 = H$, then the hypothesis of Proposition 2 of §2 is fulfilled and consequently $X(N; H)_{/k}$ is reduced.

It may be of use to "unwind" the definition of Ind, so as to make clearer the nature of the irreducible components of $X(N;H)_{/k}$ (up to radicial morphism). For this, recall that we are identifying $GL_2(\mathbf{Z}/N\mathbf{Z})$ with $GL_2(\mathbf{Z}/p^n\mathbf{Z}) \times GL_2(\mathbf{Z}/m\mathbf{Z})$. Fix $\{g_1, \ldots, g_r\}$, a representative system of left-cosets of $GL_2(\mathbf{Z}/p^n\mathbf{Z})$ relative to B_p; these may also be viewed as a representative system of left-cosets of $GL_2(\mathbf{Z}/N\mathbf{Z})$ relative to the subgroup of matrices $B = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbf{Z}/N\mathbf{Z})$ such that $c \equiv 0 \bmod p^n\}$.

We then have that $\mathrm{Ind}_{B_p}^{GL_2(\mathbf{Z}/p^n\mathbf{Z})} \{Igusa(p^n; m)_{/k'}\}$ has precisely r distinct irreducible components which may be labelled $g_i \cdot Igusa(p^n; m)_{/k'}$ for $i = 1, \ldots, r$. The stabilizer of the i-th component is the subgroup:

$$H_i = H \cap g_i B g_i^{-1} \subseteq GL_2(\mathbf{Z}/N\mathbf{Z}).$$

The quotient

$$\frac{Igusa(p^n; m)}{g_i^{-1} H g_i \cap B} \cong \frac{g_i \cdot Igusa(p^n; m)}{H_i}$$

maps radically (i.e., by a 'radicial morphism') onto its image in $\widetilde{X(N;H)}_{/k}$.

Consider the homomorphism α: $B \to (\mathbf{Z}/p^n\mathbf{Z})^*$ obtained by taking $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to a modulo p^n. Let n_i be the smallest positive integer such that $g_i^{-1} H g_i \cap B$ contains the kernel of the homomorphism $(\mathbf{Z}/p^n\mathbf{Z})^* \twoheadrightarrow (\mathbf{Z}/p^{n_i}\mathbf{Z})^*$. We shall refer to p^{n_i} as the *p-level* of the i-th component. The significance of the 'p-level' is that n_i is the smallest integer such that the natural map of $Igusa(p^n; m)$ onto the i-th component factors through the projection $Igusa(p^n; m) \twoheadrightarrow Igusa(p^{n_i}; m)$. In particular, the i-th component is a quotient of $Igusa(p^{n_i}; m)$.

Corollary 1. *Let N divide N'. Imbed $\mathbf{Z}_p[\zeta_N]$ in $\mathbf{Z}_p[\zeta_{N'}]$ by sending ζ_N to the N'/N-th power of ζ_N.*

Let H and H' be subgroups, as above, of $GL_2(\mathbf{Z}/N\mathbf{Z})$ and $GL_2(\mathbf{Z}/N'\mathbf{Z})$ respectively, such that H' is the full inverse image of H under the natural mapping $GL_2(\mathbf{Z}/N'\mathbf{Z}) \twoheadrightarrow GL_2(\mathbf{Z}/N\mathbf{Z})$.

Then $R_H = R_{H'}$ and the natural mapping

$$X(N')_{/\mathbf{Z}[\zeta_{N'}]} \to X(N)_{/\mathbf{Z}[\zeta_N]}$$

induces an isomorphism of R_H-schemes: $X(N';H') \xrightarrow[\cong]{} X(N;H)$.

Proof. These schemes are both normalizations of the same $\mathbf{Q} \otimes R_H$-scheme over the j-line over R_H (cf. §3.2).

In view of the above corollary, if $\mathscr{H} \subset GL_2(\hat{\mathbf{Z}})$ is the full inverse image of $H \subset GL_2(\mathbf{Z}/N\mathbf{Z})$, the ring R_H depends only on $\mathscr{H}$ (denote it $R_{\mathscr{H}}$) and the $R_{\mathscr{H}}$-scheme also depends only on $\mathscr{H}$ (denote it $X(\mathscr{H})$).

Return to the setting of the Proposition and form the following commutative diagram:

$$\begin{array}{ccc} \mathbf{Q}_p[\zeta_N] & \longrightarrow & K' \\ \uparrow & & \uparrow \\ \mathbf{Q} \otimes R_H & \longrightarrow & K \end{array}$$

where K' is the field of fractions of the discrete valuation ring quotient of $\mathbf{Z}_p[\zeta_N]$ obtained by completing with respect to the kernel of the homomorphism $\mathbf{Z}_p[\zeta_N] \twoheadrightarrow k'$.

We are now in a position to describe the abelian variety part of the special fiber (over k) of the Néron model of the Jacobian of $X(N;H)_{/K}$. The crucial point is that $X(N;H)$ has only inconsequential singularities and hence the proposition gives a good description of the characteristic p fibre of a regular resolution $X^*(N;H)$ of $X(N;H)$. Indeed, they differ only in the adjunction of projective lines. So using the results of §1 and the previous proposition we have:

Corollary 2. *There is a natural isogeny of abelian varieties over k:*

$$av\{\mathrm{Pic}^0(X(N;H)_{/K})\} \to \prod_{i=1}^{r} \mathrm{Pic}^0\left\{\frac{Igusa(p^n;m)}{g_i^{-1}Hg_i \cap B}\right\}.$$

§ 8. Examples

1. *The canonical model of $X_1(ap^n)_{/\mathbf{Z}_p[\zeta_{p^n}]}$.* Let a be an integer prime to p, and fix $m \geqq 3$ any integer prime to ap. Let $N = a \cdot m \cdot p^n$ and consider the subgroup $H = H_a \times H_m \times H_p$ of $GL_2(\mathbf{Z}/a\mathbf{Z}) \times GL_2(\mathbf{Z}/m\mathbf{Z}) \times GL_2(\mathbf{Z}/p^n\mathbf{Z}) = GL_2(\mathbf{Z}/N\mathbf{Z})$ defined as follows:

$$H_a = \left\{\pm\begin{pmatrix}1 & * \\ 0 & *\end{pmatrix} \in GL_2(\mathbf{Z}/a\mathbf{Z})\right\},$$

$$H_m = GL_2(\mathbf{Z}/m\mathbf{Z}),$$

$$H_p = \left\{\pm\begin{pmatrix}1 & * \\ 0 & 1\end{pmatrix} \in GL_2(\mathbf{Z}/p^n\mathbf{Z})\right\}.$$

Then $R_H = \mathbf{Z}_p[\zeta_{p^n}]$ and $X(N;H)$ is indeed a canonical model for $X_1(ap^n)$ over R_H. Call it $X_1(ap^n)_{/\mathbf{Z}_n[\zeta_{p^n}]}$. We shall refer to the residue field as k_n or as k, if n is understood. Of course, $k_n = k = \mathbf{F}_p$. The components of $X_1(ap^n)_{/k}$ are in natural one: one correspondence with the H_p-orbits of $\mathbf{P}^1(\mathbf{Z}/p^n\mathbf{Z})$ which we now proceed to describe.

A point of $\mathbf{P}^1(\mathbf{Z}/p^n\mathbf{Z})$ is given by an equivalence class of pairs of integers $\binom{d}{b}$ modulo p^n such that at least one of these integers is a unit modulo p^n, and where $\binom{d}{b} \sim \binom{d'}{b'}$ if and only if $d' = \lambda \cdot d$, $b' = \lambda \cdot b$ for λ a unit modulo p^n. For example, the "base component" of $X(N)_{/k'}$ (cf. discussion following Drinfeld's theorem) corresponds to the point $\binom{1}{p^n}$ in $\mathbf{P}^1(\mathbf{Z}/p^n\mathbf{Z})$. Any such equivalence class has a representative of the form $\binom{d}{p^j}$ for a unique integer j: $0 \leqq j \leqq n$ where d is determined up to multiplication by an arbitrary unit modulo p^n which is congruent to 1 modulo p^{n-j}.

Call the integer j the *exponent* of the equivalence class. The action of H_p preserves the exponent of an equivalence class, and two equivalence classes represented by $\binom{d}{p^j}$ and $\binom{d'}{p^j}$ are in the same H_p-orbit if and only if

$$d' \equiv d \cdot \lambda \bmod p^j \quad \text{where } \lambda \text{ is a unit } \equiv 1 \bmod p^{n-j}.$$

Distinguish two cases:

(i) $j=0$ and n: There is a *unique* orbit of exponent 0 and a *unique* orbit of exponent n; call these the *good* orbits.

(ii) $0<j<n$: In these cases an H_p-orbit is represented by $\binom{d}{p^j}$ where d is a unit, and is determined modulo $(p^j, p^{n-j}) = (p^{\min(j,n-j)})$. That is, the class of the integer d in the group

$$(\mathbf{Z}/p^{\min(j,n-j)}\mathbf{Z})^*$$

determines the H_p-orbit. Call this class the *invariant* of the H_p-orbit. The number of H_p-orbits of exponent j such that $0<j<n$ is:

$$\min(\varphi(p^j),\ \varphi(p^{n-j}))$$

where φ is Euler's φ-function.

Thus an irreducible component of $X_1(ap^n)_{/k}$ is determined by its *exponent* j and its *invariant* a (if $0<j<n$). The p-level of any irreducible component of exponent j is easily seen to be $p^{\max(j,n-j)}$ and, moreover, any component of exponent j has the property that its normalization is a radicial quotient of $Igusa(a\cdot p^{\max(j,n-j)})$.

Notation. Let $\mathscr{I}$ stand for the curve $\mathrm{Ind}_{B_p}^{GL_2(\mathbf{Z}/p^n\mathbf{Z})} Igusa(N)_{/k}$ so that $\mathscr{I}$ is a smooth projective (disconnected) curve over k. By the proposition of §7 we have a natural radicial surjection

$$H_p\backslash\mathscr{I} \xrightarrow{\varphi} \widetilde{X_1(N)}_{/k}$$

where $\sim$ denotes normalization of the reduced subscheme $\{X_1(N)_{/k}\}_{\mathrm{red}}$. The irreducible components of both domain and range of φ are in natural one: one correspondence with the H_p orbits of $\mathbf{P}^1(\mathbf{Z}/p^n\mathbf{Z})$. In particular, they admit natural decompositions into finite disjoint unions

$$H_p\backslash\mathscr{I} = \coprod_{j=0}^{n} (H_p\backslash\mathscr{I})_j,$$

$$\widetilde{X_1(N)}_{/k} = \coprod_{j=0}^{n} (X_1(N)_{/k})_j$$

where the subscript j denotes the union of all irreducible components of exponent j. The mapping φ respects this decomposition, and, restricted to the j-th piece, it gives rise to a radical surjection

$$(H_p\backslash\mathscr{I})_j \xrightarrow[\varphi_j]{} (\widetilde{X_1(N)}_{/k})_j.$$

There are finite morphisms

$$(H_p\backslash\mathscr{I})_j \xrightarrow[\Lambda_j]{} Igusa(N/p^j)_{/k}$$

whose definition is sketched below.

Let $\mathscr{S}$ be an irreducible component of the curve $\mathscr{I}$ which projects to an irreducible component of $(H_p\backslash\mathscr{I})_j$. Let $U\subset\mathscr{S}$ be an open dense subscheme contained in the complement of the supersingular locus, and which therefore we may view as a subscheme of $X(N)_{/k}$. Fix an "auxiliary level" $m\geqq 3$ prime to N and let $U'\twoheadrightarrow U$ denote the inverse image of U in $X(Nm)_{/k}$.

From the inclusion of U' in $X(Nm)_{/k'}$ we obtain an ordinary elliptic curve E over U' together with a Drinfeld basis (t_1, t_2) of level N and an "auxiliary" level m structure. Since U' is a smooth curve, it follows from our hypothesis ($\mathscr{S}$ projects to an irreducible component of $(H_p \backslash \mathscr{I})_j$) that t_2 is a U'-valued section generically of order N/p^j. Thus (E, t_2) determines a U'-valued section of $Igusa(N/p^j)_{/k}$. This U'-valued section "descends" to a U-valued section which determines the morphism Λ_j on $\mathscr{S}$.

The mappings β_0 *and* β_n: Define the mapping β_n: $Igusa(N)_{/k} \to (H_p \backslash \mathscr{I})_n \to (\widetilde{X_1(N)_k})_n$ of the Igusa curve of level N onto the good component of exponent 0 by composing the "identity mapping"

$$Igusa(N) \xrightarrow{=} g \cdot Igusa(N) \hookrightarrow \mathscr{I}$$

(g = the representative of the identity B_p-coset in $GL_2(\mathbf{Z}/p^n\mathbf{Z})$ with the projection mapping

$$\mathscr{I} \twoheadrightarrow H_p \backslash \mathscr{I}.$$

Then β_n is a radicial morphism of $Igusa(N)$ onto the normalization of the good component of exponent n.

In terms of moduli problems, β_n has the following simple description: To a triple consisting of $(E, e_{p^n}, e)_{/S'}$ ---- where S' is an $\mathbf{F}_p$-scheme, $E_{/S'}$ an elliptic curve, e_{p^n} an S'-valued point of E which generates an étale subgroup scheme, finite and flat over S', of order p^n, and e_a an S'-valued section of E of order a --- the mapping β_k associates the "triple" $(E, (t_1, t_2), e_a)_{/S'}$ where (t_1, t_2) is the Drinfeld "ζ_{p^n}"-basis of $E_{/S'}$ given by $t_1 = e_{p^n}$, and t_2 = the zero-section of E, where "ζ_{p^n}" is the constant unit section 1 over S'.

Define the mapping $\beta = \beta_0$: $Igusa(N) \to (H_p \backslash \mathscr{I})_0 \to (\widetilde{X_1(N)_{/k}})_0$ analogously. In terms of moduli problems it has the following description: To a triple $(E, e_{p^n}, e_a)_{/S'}$ as above, β_0 associates the triple $(E, (t_1', t_2'), e_a)_{/S'}$ where (t_1', t_2') is the Drinfeld "ζ_{p^n}" basis given by t_1' = zero-section of E, and $t_2' = e_{p^n}$.

It will be convenient for later purposes to use the notation $\Sigma^{\text{ét}}$ and Σ^{μ} for the curves $(X_1(N)_{/k})_0$ and $(X_1(N)_{/k})_n$ respectively. Though we have not actually even proved that these are non-singular, we do know that in the normalization of the reduced fibre, $(\widetilde{X_1(N)_{/k}})$ the natural maps

$$\beta_0\colon\ Igusa(N) \to \tilde{\Sigma}^{\text{ét}}, \quad \beta_n\colon\ Igusa(N) \to \tilde{\Sigma}^{\mu}$$

are radicial.

The mapping β_0 "extends" to an open immersion

$$b_0\colon\ \mathscr{Y}_1(ap^n)_{/\mathbf{Z}_p[\zeta_{p^n}]} \to X_1(ap^n)_{/\mathbf{Z}_p[\zeta_{p^n}]}$$

where $\mathscr{Y}_1(ap^n)$ is the "incomplete moduli space" studied in §4. The mapping b_0 is induced from the following rule expressed in terms of moduli data:

Let S be a $\mathbf{Z}_p[\zeta_{p^n}]$-scheme. Let $(E, e_{p^n}, e_a)_{/S}$ be a triple where $E_{/S}$ is an elliptic curve, e_a is an S-valued point of E of order a, and e_{p^n} is an *étale* S-valued point of E order p^n (étale in the sense that it generates a finite étale subgroup scheme of E over S, of order p^n). Let $y \in \mathscr{Y}_1(ap^n)(S)$ be the S-valued point represented by this triple. We may extend e_{p^n} to a Drinfeld ζ_{p^n}-basis of level p^n, $\xi_{p^n} = (e_{p^n}', e_{p^n})$ where e_{p^n}' is a

suitable point of order p^n. This determines a unique S-valued section of $X_1(ap^n)$ which we define to be $b_0(y)$. It is evident that b_0 induces an open immersion on generic fibres (the canonical open immersion).

Moreover, since $\mathscr{Y}_1(ap^n)_{/\mathbf{Z}_p[\zeta_{p^n}]}$ is a smooth scheme, quasi-finite over the j-line, and $X_1(ap^n)_{/\mathbf{Z}_n[\zeta_{p^n}]}$ is the normalization of its generic fibre over the j-line, it follows that b_0 is an open immersion on all of $\mathscr{Y}_1(ap^n)_{/\mathbf{Z}_n[\zeta_{p^n}]}$. If k_n is the residue field, it is immediate that the following triangle is commutative:

$$\begin{array}{ccc} \mathscr{Y}_1(ap^n)_{/k_n} & \hookrightarrow & Igusa(ap^n)_{/k_n} \\ & {\scriptstyle b_{0/k_n}} \searrow \quad \swarrow {\scriptstyle \beta_0} & \\ & X_1(ap^n)_{/k_n} & \end{array}$$

Consequently, we have

Proposition 1. *The mapping*

$$\beta_0\colon\ Igusa(ap^n)_{/k_n} \to \tilde{\Sigma}^{\text{ét}}_{/k_n}$$

is an isomorphism of curves.

2. The canonical model of $X_1(ap^n)_{/\mathbf{Z}_p[\zeta_{p^{n'}}]}$ $(n' \geqq n)$. Here we let $N' = a \cdot m \cdot p^{n'}$ and $H' = H_a \times H_m \times H'_p$ where H_a and H_m are as above, while $H'_p \subset GL_2(\mathbf{Z}/p^{n'}\mathbf{Z})$ is the subgroup:

$$H'_p = \left\{ g = \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{Z}/p^{n'}\mathbf{Z});\ c \equiv 0 \bmod p^n;\ \det g \equiv 1\ (p^n) \right\}.$$

Then $R_{H'} = \mathbf{Z}_p[\zeta_{p^{n'}}]$; Refer to $X(N'; H')_{/R_{H'}}$ as $X_1(ap^n)_{/\mathbf{Z}_p[\zeta_{p^{n'}}]}$.

If C denotes the subgroup of scalar matrices of $GL_2(\mathbf{Z}/p^{n'}\mathbf{Z})$ which are congruent to the identity matrix modulo p^n, then the full inverse image of H_p in $GL_2(\mathbf{Z}/p^{n'}\mathbf{Z})$ is $C \cdot H'_p$ and therefore the natural map induces a one:one correspondence

$$H'_p \backslash \mathbf{P}^1(\mathbf{Z}/p^{n'}\mathbf{Z}) \xrightarrow[\sim]{} H_p \backslash \mathbf{P}^1(\mathbf{Z}/p^n\mathbf{Z}).$$

Let $\{g'_1, \ldots, g'_r\}$ be a system of representatives in $GL_2(\mathbf{Z}/p^{n'}\mathbf{Z})$ for the double cosets $C \cdot H'_p \backslash GL_2(\mathbf{Z}/p^{n'}\mathbf{Z})/B'_p$ (where B'_p is the subgroup of upper triangular matrices in $GL_2(\mathbf{Z}/p^{n'}\mathbf{Z})$) and let $\{g_1, \ldots, g_r\}$ denote the system of images in $GL_2(\mathbf{Z}/p^n\mathbf{Z})$, viewed as representative system for the double cosets $H_p \backslash GL_2(\mathbf{Z}/p^n\mathbf{Z})/B_p$.

Then the full inverse image in B'_p of $g_i^{-1} H_p g_i \cap B_p$ is equal to $g_i'^{-1} C H'_p g'_i \cap B'_p = C \cdot g_i'^{-1} H'_p g'_i \cap B'_p$. This fact implies:

Proposition 1. *The natural map*

$$X_1(ap^n)_{/\mathbf{Z}_p[\zeta_{p^n}]} \to X_1(ap^n)_{/\mathbf{Z}_p[\zeta_{p^{n'}}]}$$

induces a one: *one correspondence of irreducible components of the fibers over the residue field* $k_n = k_{n'} = \mathbf{F}_p$. *The mapping induced on the normalizations of the reduction of the* $\mathbf{F}_p$*-fibers is a radicial morphism. The mapping induced on "abelian variety parts" on the* $\mathbf{F}_p$*-fibers of the Néron models of the jacobians of the fibers over the field of fractions is an isogeny*:

$$av(\mathrm{Pic}^0(X_1(ap^n)_{/\mathbf{Q}_p[\zeta_{p^{n'}}]}) \xrightarrow[\sim]{} av(\mathrm{Pic}^0(X_1(ap^n)_{/\mathbf{Q}_p[\zeta_{p^n}]}).$$

3. The canonical model of $X_1(ap^n, ap^{n-1})_{/\mathbf{Z}_p[\zeta_{p^n}]}$. Keeping the notation of example 1 above (e.g., $N = a \cdot m \cdot p^n$), let

$$\bar{H}_p = \left\{ g = \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{Z}/p^n\mathbf{Z}) \;\middle|\; \begin{array}{l} a \equiv 1 \bmod p^{n-1};\ c \equiv 0 \bmod p^n \\ \text{and } \det g \equiv 1 \bmod p^n \end{array} \right\}$$

and set $\bar{H} = H_a \times H_m \times \bar{H}_p$. One has that $\bar{H}_p$ contains H_p as a normal subgroup of index p; $\bar{H}$ contains H as normal subgroup of index p. The model $X(N; \bar{H})_{/R_{\bar{H}}}$ is a canonical model for $\Gamma_1(ap^n, ap^{n-1})$ over $\mathbf{Z}[\zeta_{p^n}]$ and we shall therefore refer to it as $X_1(ap^n, ap^{n-1})_{/\mathbf{Z}_p[\zeta_{p^n}]}$. The natural mapping

$$H_p \backslash \mathbf{P}^1(\mathbf{Z}/p^n\mathbf{Z}) \xrightarrow[\sim]{} \bar{H}_p \backslash \mathbf{P}^1(\mathbf{Z}/p^n\mathbf{Z})$$

is easily seen to be a bijection, and consequently the mapping

$$\Pi_n : X_1(ap^n)_{/\mathbf{Z}_p[\zeta_{p^n}]} \longrightarrow X_1(ap^n, ap^{n-1})_{/\mathbf{Z}_p[\zeta_{p^n}]}$$

induces a one: one correspondence on irreducible components of $\mathbf{F}_p$-fibers.

An irreducible component of the $\mathbf{F}_p$-fiber of $X_1(ap^n, ap^{n-1})_{/\mathbf{Z}_p[\zeta_{p^n}]}$ may be characterized, then, by its *exponent* and its *invariant*, as described in Example 1. One easily sees that the p-level of the two *good* components of the $\mathbf{F}_p$-fiber of $X_1(ap^n, ap^{n-1})_{/\mathbf{Z}_p[\zeta_{p^n}]}$ is p^{n-1}, and the mapping which Π_n induces on the normalizations of the reductions of the $\mathbf{F}_p$-fibers of domain and range has the following form:

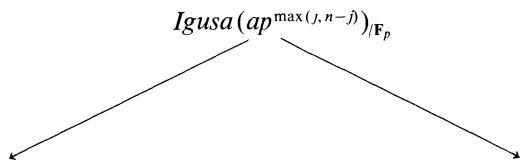
(i) the *good* components: We have a commutative diagram

$$\begin{array}{ccc} Igusa(ap^n)_{/\mathbf{F}_p} & \longrightarrow & Igusa(ap^{n-1})_{/\mathbf{F}_p} \\ \downarrow & & \downarrow \\ \text{the irreducible component of exponent 0 of the normalization of the reduction of the } \mathbf{F}_p\text{-fiber of } X_1(ap^n)_{/\mathbf{Z}_p[\zeta_{p^n}]} & \longrightarrow & \text{the irreducible component of exponent 0 of the normalization of the reduction of the } \mathbf{F}_p\text{-fiber of } X_1(ap^n, ap^{n-1})_{/\mathbf{Z}_p[\zeta_{p^n}]} \end{array}$$

where the horizontal mappings are the natural ones, and the vertical mappings are radicial morphisms.

We have a similar diagram for the irreducible components of exponent n.

ii) the *remaining* components: We have a commutative diagram



where the horizontal mapping is the natural one, and the oblique arrows refer to radicial morphisms.

It is also easy to analyze the natural mapping

$$\rho_n\colon X_1(ap^n, ap^{n-1})_{/\mathbf{Z}_p[\zeta_{p^n}]} \to X_1(ap^{n-1})_{/\mathbf{Z}_p[\zeta_{p^n}]}$$

which we may regard as being induced by the inclusion of the group $\bar{H} = H_a \times H_m \times \bar{H}_p$ of example 3 into the group $H'' = H_a \times H_m \times H_p''$ where

$$H_p'' = \left\{ g = \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \begin{matrix} a \equiv 1 \bmod p^{n-1} \\ c \equiv 0 \bmod p^{n-1} \end{matrix} \quad \det g \equiv 1 \bmod p^n \right\}$$

(i.e., H_p'' is the group H_p' of Example 2, where n' and n are n and $n-1$ respectively).

One finds that if $1 \leqq j \leqq n-1$, an irreducible component of exponent j and invariant $d \in (\mathbf{Z}/(p^j, p^{n-j}))^*$ of the $\mathbf{F}_p$-fiber of $X_1(ap^n, ap^{n-1})_{/\mathbf{Z}_p[\zeta_{p^n}]}$ maps to the irreducible component of exponent j and whose invariant is the image of d in $(\mathbf{Z}/(p^j, p^{n-i-j}))^*$, and that *good* components map by radicial morphisms onto good components.

4. The canonical model of $X_1(p^n, ap^{n-1})_{/\mathbf{Z}_p[\zeta_{p^{n'}}]}$. Keeping the notation of Example 2, let

$$\bar{H}_p' = \left\{ g = \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{Z}/p^{n'}\mathbf{Z}) \;\middle|\; \begin{matrix} a \equiv 1 \bmod p^{n-1} \\ c \equiv 0 \bmod p^n \end{matrix} \quad \det g \equiv 1 \bmod p^{n'} \right\}$$

and set $\bar{H}' = H_a \times H_m \times \bar{H}_p'$.

If C denotes the subgroup of scalar matrices of $GL_2(\mathbf{Z}/p^{n'}\mathbf{Z})$ which are congruent to the identity matrix modulo p^n, then, as in Example 2, we have that the full inverse image of $\bar{H}_p$ in $GL_2(\mathbf{Z}/p^{n'}\mathbf{Z})$ is $C \cdot \bar{H}_p'$ and one obtains by a process of reasoning analogous to that in Example 2 the following result:

Proposition 2. *The natural map*

$$X_1(ap^n, ap^{n-1})_{/\mathbf{Z}_p[\zeta_{p^{n'}}]} \to X_1(ap^n, ap^{n-1})_{/\mathbf{Z}_p[\zeta_{p^n}]}$$

induces a one: one correspondence of irreducible components of the fibers over the residue field $\mathbf{F}_p$. *The mapping induced on the normalizations of the reductions of the*

$\mathbf{F}_p$-fibers is a radicial morphism. The mapping induced on "abelian variety parts" of the $\mathbf{F}_p$-fibers of the Néron models of the jacobians of the fibers over the field of fractions is an isogeny:

$$av\ \mathrm{Pic}^0(X_1(ap^n, ap^{n-1})_{/\mathbf{Q}_p[\zeta_{p^{n'}}]}) \to av\ \mathrm{Pic}^0(X_1(ap^n, ap^{n-1})_{/\mathbf{Q}_p[\zeta_{p^n}]}).$$

Summary. Although the canonical models of $X_1(ap^n)$ and $X_1(ap^n, ap^{n-1})$ will not commute with a base extension of the type $\mathbf{Z}_p[\zeta_{p^{n'}}]/\mathbf{Z}_p[\zeta_{p^n}]$ there is *a* certain limited type of stability that obtains. That is, the normalization of the reductions of the $\mathbf{F}_p$-fibers will change by at most *radicial* morphisms. In consequence, if we are willing to consider the normalization of the $\mathbf{F}_p$-fiber *up to* the equivalence relation on the category of curves over $\mathbf{F}_p$ induced by radicial morphisms, we may talk of *the* $\mathbf{F}_p$-fiber without reference to n'. Up to this equivalence relation we have given a complete description of the morphisms

$$\begin{array}{lll} \text{normalization of the } \mathbf{F}_p\text{-fiber of } X_1(ap^n)_{/\mathbf{Z}_p[\zeta_{p^n}]} & \longrightarrow \text{normalization of the } \mathbf{F}_p\text{-fiber of } X_1(ap^n, ap^{n-1})_{/\mathbf{Z}_p[\zeta_{p^n}]} & \longrightarrow \text{normalization of the } \mathbf{F}_p\text{-fiber of } X_1(ap^{n-1})_{/\mathbf{Z}_p[\zeta_{p^n}]} \end{array} \quad (*)$$

(on good components)

$$\begin{array}{lll} Igusa(ap^n)_{/\mathbf{F}_p} & \longrightarrow Igusa(ap^{n-1})_{/\mathbf{F}_p} & \underset{=}{\longrightarrow} Igusa(ap^{n-1})_{/\mathbf{F}_p} \\ \text{exponent } 0 & \longrightarrow \text{exponent } 0 & \longrightarrow \text{exponent } 0 \\ \text{exponent } n & \longrightarrow \text{exponent } n & \longrightarrow \text{exponent } n-1 \end{array}$$

(on a component of exponent j: $n/2 < j < n$)

$$Igusa(ap^j)_{/\mathbf{F}_p} \longrightarrow Igusa(ap^j)_{/\mathbf{F}_p} \longrightarrow Igusa(ap^j)_{/\mathbf{F}_p}$$

$$\{\text{invariant } d \text{ in } (\mathbf{Z}/p^{n-j}\mathbf{Z})^*\} \longrightarrow \text{invariant } \bar{d} = \text{image of } d \text{ in } (\mathbf{Z}/p^{n-j-1}\mathbf{Z})^*\}$$

(on a component of exponent j: $n/2 \geqq j > 0$)

$$Igusa(ap^{n-j})_{/\mathbf{F}_p} \longrightarrow Igusa(ap^{n-j})_{/\mathbf{F}_p} \longrightarrow Igusa(ap^{n-j-1})_{/\mathbf{F}_p}$$

(all invariants d in $(\mathbf{Z}/p^j\mathbf{Z})^*$).

For example, when $n = 2$ we have the following description of $(*)$, up to radicial morphisms:

$$\begin{array}{ccccccc} Igusa(ap^2) & \amalg & \coprod_{(\mathbf{Z}/p\mathbf{Z})^*} & Igusa(ap) & \amalg & Igusa(ap^2) \\ \downarrow & & & \downarrow & & \downarrow \\ Igusa(ap) & \amalg & \coprod_{(\mathbf{Z}/p\mathbf{Z})^*} & Igusa(ap) & \amalg & Igusa(ap) \\ \downarrow & & & \searrow & & \swarrow \\ Igusa(ap) & \amalg & & & Igusa(ap) & \end{array}$$

where the mappings are the evident ones.

§ 9. *The correspondence U_p*

We have described the correspondence U_p on the modular curve $X_1(N)_{/\mathbf{Q}}$ in § 5.5. In this section we study the "effect" of U_p on the canonical model $X_1(N)_{/\mathbf{Z}_p[\zeta_{p^n}]}$, and, in particular, on the characteristic p fiber. (See Example 1 of § 8: we retain the notation from this example.)

To begin, consider two mappings

$$\mathscr{F}\colon Igusa(N)_{/\mathbf{F}_p} \longrightarrow Igusa(N)_{/\mathbf{F}_p}$$
$$\mathscr{V}\colon Igusa(N)_{/\mathbf{F}_p} \longrightarrow Igusa(N/p)_{/\mathbf{F}_p}$$

which are induced from mappings

$$\mathscr{F}\colon \mathscr{Y}_1(N;m)_{/k'} \longrightarrow \mathscr{Y}_1(N;m)_{/k'}$$
$$\mathscr{V}\colon \mathscr{Y}_1(N;m)_{/k'} \longrightarrow \mathscr{Y}_1(N/p;m)_{/k'}$$

characterized by the rules:

$$\mathscr{F}\colon (E, e_N, \alpha)_{/R} \longrightarrow (E/E[p]^0, \bar{e}_N, \bar{\alpha})_{/R}$$
$$\mathscr{V}\colon (E, e_N, \alpha)_{/R} \longrightarrow (E/C_p, \bar{e}_N, \bar{\alpha})_{/R}$$

where $E[p]^0$ is the connected component of the group scheme $F[p]_{/R}$ and where C_p is the finite flat étale subgroup scheme of $E_{/R}$ generated by $(N/p)\cdot e_N$. Here, $\bar{e}_N$ is the image of e_N in the appropriate quotient elliptic curve, and $\bar{\alpha}$ refers to the level m structure induced from α.

Note that $\mathscr{F}$ is the Frobenius morphism, associated to $Igusa(N)_{/\mathbf{F}_p}$. On the other hand, if R is a perfect field, then the elliptic curve E/C_p can be identified with $E^v_{/R'}$ where E^v is the image of E under Verschiebung.

We now make use of the notation of Example 1 of § 8. Consider the following correspondence

$$v\colon Igusa(N)_{/\mathbf{F}_p} \to H_p \backslash \mathscr{I}$$
$$v(x) = \beta_0 \cdot \mathscr{F}(x) + \Lambda_1^{-1} \cdot \mathscr{V}(x).$$

We consider the composite homomorphism v':

$$\mathrm{Pic}^0(Igusa(N)_{/k}) \xrightarrow{v} \mathrm{Pic}^0(H_p \backslash \mathscr{I}) \longrightarrow \mathrm{Pic}^0(\widetilde{X_1(N)}_{/k}) \Big\| \wr$$
$$av(\mathrm{Pic}^0(X_1(N)_{/\mathbf{Q}_p[\zeta_{p^n}]}))$$

Proposition 1. *We have a commutative diagram*

$$\begin{array}{ccc} Pic^0(Igusa(N)_{/k}) & \xrightarrow{\beta_0} & av(\mathrm{Pic}^0(X_1(N)_{/\mathbf{Q}_p[\zeta_{p^n}]})) \\ & {\scriptstyle v'} \searrow \quad \swarrow {\scriptstyle av(U_p)} & \\ & av(\mathrm{Pic}^0(X_1(N)_{/\mathbf{Q}_p[\zeta_{p^n}]})). & \end{array} \qquad (*)$$

Proof. To begin, let K be a field of characteristic 0 containing ζ_N a primitive N-th root of unity. Let x be a K-valued point of $X_1(N)$ which is represented by the elliptic curve E_K together with a Drinfeld basis (t_1, t_2) of level N.

If we modified the point t_1 by adding any multiple of t_2, we would still obtain a representative of the point x. Indeed, the point t_1 is a "redundant" piece of information in characteristic 0.

Let $C(r) \subset E[p](\bar{K})$ denote the cyclic subgroup of order p generated by the point $(N/p) \cdot (t_1 + rt_2)$ for $0 \leqq r < p$. Then $U_p(x)$ may be viewed as the divisor on $X_1(N)$ of degree p represented by $\sum_{r=0}^{p-1} (E/C(r), t_1(r), t_2(r))$ where $t_2(r)$ is simply the image of t_2 in $E/C(r)$ and the "redundant" point $t_1(r)$ is any other point of order N which renders $(t_1(r), t_2(r))$ a Drinfeld ζ_N-basis of $E/C(r)$. An elementary argument shows that we may take $t_1(r)$ to be the image of any point $t_1'(r)$ in E such that $p \cdot t_1'(r)$ is equal to $t_1 + rt_2$.

Now suppose that, as in Example 6 of §6, S is the spectrum of a discrete valuation ring whose field of fractions is K'. Let $E_{/S}$ be an elliptic curve whose reduction to the residue field k' is ordinary. Suppose, further, that (t_1, t_2) is a Drinfeld ζ_N-basis for $E_{/S}$, which is *adapted* in the sense that the specialization of t_1 to the residue field k' is of order a. Thus, $(a \cdot t_1, a \cdot t_2)$ is an adapted Drinfeld basis of level p^n. It follows that the specialization of $(E, t_1, t_2)_{/S}$ to k' represents a point lying in the irreducible component of $X_1(N)_{/k}$ of exponent 0.

Let us examine the specialization to $X_1(N)_{/k}$ of the sections of $X_1(N)_{/S}$ represented by the triples $(E/C(r), t_1(r), t_2(r))_{/S}$ for $r = 0, \ldots, p-1$.

$r = 0$: Since the Drinfeld basis (t_1, t_2) is adapted, and $C(0)$ is generated by $(N/p) \cdot t_1$ it follows that $(E/C(0), t_1(0), t_2(0))$ specializes to represent a point of $X_1(N)_{/k}$ lying in the irreducible component of exponent 0. This point is immediately seen to be $\beta_0 \cdot \mathscr{F}(e)$ where e is the point of $Igusa(N)$ represented by $(E_{/k'}, t_{2/k'})$.

$r \neq 0$: Here $E/C(r)_{/k'}$ may be identified with the image of $E_{/k'}$ under the Verschiebung morphism.

Clearly, $t_2(r)_{/k'}$ which is the image of $t_{2/k'}$ under the natural morphism is of order N/p and therefore $(E/C(r), t_1(r), t_2(r))_{/k'}$ represents a point of $X_1(N)_{/k}$ which lies in an irreducible component of exponent 1. One further checks that the "invariant" of the component containing the specialization $(E/C(r), t_1(r), t_2(r))_{/k'}$ is the image of r in $(\mathbf{Z}/p\mathbf{Z})^*$. In terms of the notation introduced in 8.1, if $e(r)$ is the point of $(H_p \setminus \mathscr{J})_1$ represented by $(E/C(r), t_1(r), t_2(r))_{/k'}$ then $\Lambda_1 \cdot e(r)$ is the point of $Igusa(N/p)$ represented by $\mathscr{V}(E, t_2)_{/k'}$ and therefore

$$\sum_{r=1}^{p-1} e(r) = \Lambda_1^{-1} \cdot \mathscr{V}(E, t_2)_{/k'}$$

the above equation being an equality between divisors of degree $p-1$ on $(H_p \setminus \mathscr{J})_1$.

The required formula then follows from the criterion of compatibility given in Proposition 2 of §1.

We also need a formula giving the effect of U_p on $\mathrm{Pic}^0(\tilde{\Sigma}^\mu)$. This time we do not use the map β_n but consider $\tilde{\Sigma}^\mu$ itself (rather than the Igusa curve).

Proposition 2. *We have a commutative diagram*

$$\begin{array}{ccc} \mathrm{Pic}^0(\tilde{\Sigma}^{\mu}) & \longrightarrow & av(\mathrm{Pic}^0(X_1(N)_{/\mathbf{Q}_p(\zeta_{p^n})})) \\ \Big\downarrow{\scriptstyle \mathrm{Ver}_p \cdot \langle n_p \rangle} & & \Big\downarrow{\scriptstyle av(U_p)} \\ \mathrm{Pic}^0(\tilde{\Sigma}^{\mu}) & \longrightarrow & av(\mathrm{Pic}^0(X_1(N)_{/\mathbf{Q}_p(\zeta_{p^n})})). \end{array}$$

where n_p is any integer satisfying $n_p \equiv 1 \bmod p^n$, $n_p \equiv p \bmod a$.

Proof. Let k_N be a residue field of $\mathbf{Z}_p[\zeta_N]$ and S the spectrum of a discrete valuation ring which is a finite extension of the completion of $\mathbf{Z}_p[\zeta_N]$ with respect to the maximal ideal corresponding to k_N. Let k' be the residue field of S. The field k' contains k_N. Let x be a point of $X_1(N)_{/\mathbf{Z}_p[\zeta_{p^n}]}$ which is represented by a triple $(E, t_1, t_2)_{/S}$ on $X(N)_{/\mathbf{Z}_p[\zeta_N]}$. Assume that the specialization of E is ordinary and that (t_1, t_2) is a Drinfeld ζ_N-basis with t_2 specializing to a point of order a. Thus the specialization of $(E, t_1, t_2)_{/S}$ represents a point of Σ^{μ} in $X_1(N)_{/k}$.

Applying U_p to x we find that $U_p \cdot x$ is represented by the divisor

$$\sum_{r=0}^{p-1} (E/C(r), t_1(r), t_2(r))$$

where $t_2(r)$ is the image of t_2 and $t_1(r)$ may be chosen to be the image of any point $t_1'(r)$ in E such that $p \cdot t_1'(r)$ is equal to $t_1 + rt_2$. The specialization of each point in the sum lies on Σ^{μ}. Now apply Frob_p to this sum. This, on $X(N)_{/k_N}$, amounts to division by the subgroup $\langle (N/p)t_2(r) \rangle$ over S and then specialization to characteristic p, and hence we have

$$(\mathrm{Frob}_p \circ U_p)(x) = \sum_{r=0}^{p-1} (E/E[p], \overline{t_1(r)}, t_2^*(r)) \qquad (**)$$

where $\overline{t_1(r)}$ is the image of $t_1(r)$ and $t_2^*(r)$ is any point which renders $(\overline{t_1(r)}, t_2(r))$ a $\zeta_N^{n_p}$-basis. Here $\zeta_N^{n_p}$ is the pull-back of $\zeta_N \in k_N$ under Frob_p. Using the natural isomorphism $E/E[p] \xrightarrow{\sim} E$ induced by multiplication by p we see that we may rewrite the right-hand side of (**) as

$$\sum_{r=0}^{p-1} (E, t_1 + rt_2, n_p t_2).$$

Thus we obtain the equation $\mathrm{Frob}_p \circ U_p = p \cdot \langle n_p \rangle$ on $\tilde{\Sigma}^{\mu}$ by invoking the criterion of compatibility in Proposition 2 of §1.

In order to give formulae for the action of U_p^* we recall that there is an involution w_{ζ_N} *of* $X_1(N)_{/\mathbf{Q}(\zeta_N)}$ for which $w_{\zeta_N}^{-1} \cdot U_p \cdot w_{\zeta_N} = U_p'$. Then w_{ζ_N} extends to an involution of $X_1(N)_{/\mathbf{Z}_p[\zeta_N]}$ and it is easily checked that it interchanges the components $\Sigma^{\text{ét}}$ and Σ^{μ}.

Suppose that we extend Ver_p to $\mathrm{Pic}^0(\tilde{\Sigma}^{\mu})_{/k_N}$ (where k_N is a residue field of $\mathbf{Z}_p[\zeta_N]$) by giving it the trivial action on k_N. Then w_{ζ_N} satisfies the relations

$$w_{\zeta_N}^{-1} \cdot \mathrm{Frob}_p \cdot w_{\zeta_N} = \langle n_p^{-1} \rangle \cdot \mathrm{Frob}_p$$
$$w_{\zeta_N}^{-1} \cdot \mathrm{Ver}_p \cdot w_{\zeta_N} = \langle n_p \rangle \cdot \mathrm{Ver}_p.$$

These follow from the fact that $w_{\zeta_N}^a = w_{\zeta_N} \cdot \langle a \rangle$. Hence we deduce the following formula for U_p^* over $\mathbf{Z}_p[\zeta_{p^n}]$ by first proving it over $\mathbf{Z}_p[\zeta_N]$.

Proposition 3. *We have a commutative diagram*

$$\begin{array}{ccc} \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}) & \longrightarrow & av(\mathrm{Pic}^0(X_1(N)_{/\mathbf{Q}_p[\zeta_{p^n}]})) \\ \downarrow{\scriptstyle \mathrm{Ver}_p} & & \downarrow{\scriptstyle av(U_p^*)} \\ \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}) & \longrightarrow & av(\mathrm{Pic}^0(X_1(N)_{/\mathbf{Q}_p[\zeta_{p^n}]})). \end{array}$$

Similarly we can prove a formula for $av(U_p^*)$ on $\mathrm{Pic}^0(\tilde{\Sigma}^{\mu})$ by applying w_{ζ_N} to diagram (*) of Proposition 9. Since w_{ζ_N} is only defined over $\mathbf{Z}[\zeta_N]$ we work over k_N and obtain a commutative diagram

$$\begin{array}{ccc} \mathrm{Pic}^0(Igusa(N)_{/k_N}) & \xrightarrow{w_{\zeta_N} \circ \beta_{0*}} & av(\mathrm{Pic}^0(X_1(N)_{/\mathbf{Q}_p[\zeta_N]})) \\ & {\scriptstyle w_{\zeta_N} \circ v} \searrow & \downarrow{\scriptstyle av(U_p^*)} \\ & & av(\mathrm{Pic}^0 X_1(N)_{/\mathbf{Q}_p[\zeta_N]})) \end{array}$$

§ 10. q-expansions

1. For the basic construction and facts about the Tate curves we refer the reader to [15] VII and [34]. The Tate curve $Tate(q)$ may be considered as an elliptic curve over $\mathbf{Z}((q^{1/N}))$. It is proved in [15] that it extends to a generalized elliptic curve over $\mathbf{Z}[\![q^{1/N}]\!]$.

Let a be an integer prime to p, and fix $m \geqq 3$ any integer prime to ap. Let $N = map^n$ and consider the scheme $X(N)$ over $\mathbf{Z}_p[\zeta_N]$ (cf. § 6). Let $Tate(q)$ over $\mathbf{Z}_p[\zeta_N][\![q^{1/N}]\!]$ be the Tate curve. Then associated to this curve we have a Drinfeld basis $(\zeta_N, q^{1/N})$ and thus also an associated point of $X(N)$,

$$\mathrm{Spec}\, \mathbf{Z}_p[\zeta_N][\![q^{1/N}]\!] \to X(N)_{/\mathbf{Z}[\zeta_N]}. \qquad (*)$$

The point corresponding to $q^{1/N} = 0$ is the point ∞, and it is shown in [15] that the map (*) may be identified with the formal completion of $X(N)_{/\mathbf{Z}[\zeta_N]}$ along the ∞-section.

Our objective now is to describe the formal completion of $X_1(ap^n)_{/\mathbf{Z}_p[\zeta_{ap^n}]}$ along the ∞-section. (Recall that as a point of $X_1(ap^n)_{/\mathbf{Q}}$, ∞ is only defined over $\mathbf{Q}(\zeta_{ap^n})$). To obtain this we observe that $X_1(ap^n)_{/\mathbf{Z}_p[\zeta_{ap^n}]}$ is obtained from $X(N)_{/\mathbf{Z}_p[\zeta_N]}$ by division by the subgroup H' generated by $H_a' \times H_m \times H_p'$. The groups H_a' and H_p' are defined by:

$$H_a' = \left\{ \pm \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbf{Z}/a\mathbf{Z}) \right\}, \quad H_p' = \left\{ \pm \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbf{Z}/p^n\mathbf{Z}) \right\}$$

and $H_m = GL_2(\mathbf{Z}/m\mathbf{Z})$. As in § 8, $H_a' \times H_m \times H_p'$ is viewed as a subgroup of $GL_2(\mathbf{Z}/N\mathbf{Z})$, and hence so is H'.

The stabilizer of the cusp ∞ in the group H' is the intersection of H' with the group $\left\{\begin{pmatrix}1 & * \\ 0 & *\end{pmatrix} \in GL_2(\mathbf{Z}/N\mathbf{Z})\right\}$. The action of this stabilizer on the parameter $q^{1/N}$ is readily computed and the invariants of the ring $\mathbf{Z}_p[\zeta_N][\![q^{1/N}]\!]$ is found to be $\mathbf{Z}_p[\zeta_{ap^n}][\![q]\!]$. Hence the formal completion τ_∞ of $X_1(ap^n)_{/\mathbf{Z}[\zeta_{ap^n}]}$ along the ∞-section fits into a commutative diagram

$$\begin{array}{ccc} \operatorname{Spec} \mathbf{Z}_p[\zeta_N][\![q^{1/N}]\!] & \longrightarrow & X(N)_{/\mathbf{Z}_p[\zeta_N]} \\ \downarrow & & \downarrow \\ \operatorname{Spec} \mathbf{Z}_p[\zeta_{ap^n}][\![q]\!] & \xrightarrow{\tau_\infty} & X_1(ap^n)_{/\mathbf{Z}_p[\zeta_{ap^n}]}. \end{array}$$

A similar computation at the cusp zero (corresponding to $(Tate(q))$ with Drinfeld basis $(q^{1/N}, \zeta_N)$) gives a commutative diagram

$$\begin{array}{ccc} \operatorname{Spec} \mathbf{Z}_p[\zeta_N][\![q^{1/N}]\!] & \longrightarrow & X(N)_{/\mathbf{Z}_p[\zeta_N]} \\ \downarrow & & \downarrow \\ \operatorname{Spec} \mathbf{Z}_p[\zeta_{p^n}][\![q^{1/N}]\!] & \xrightarrow{\tau_0} & X_1(ap^n)_{/\mathbf{Z}_p[\zeta_{p^n}]} \end{array}$$

where the top arrow is the formal completion along the zero-section of $X(N)_{/\mathbf{Z}_p[\zeta_N]}$.

2. Let R be a $\mathbf{Z}_p[\zeta_{ap^n}]$-algebra. The q-expansion at ∞ of a differential f defined on an open neighborhood of ∞/R is defined by means of the pull-back $\tilde{f}$ of f under τ_∞,

$$\tilde{f} = \sum_{i \geqq 0} a_i(f) q^i \cdot \frac{dq}{q}.$$

We will use this construction only in the special case where R is a field F. For a regular differential the q-expansion $\sum_{i \geqq 0} a_i(f) q^i$ has first term $a_0(f) = 0$. In the case $F = \mathbf{C}$ and $\zeta_N = e^{2\pi i/N}$ this is just the usual q-expansion. Now let f be a differential form and $\chi\colon (\mathbf{Z}/N\mathbf{Z})^* \to F^*$ such that

$$\langle r \rangle^d f = \chi(r) f \quad \text{for} \quad r \in (\mathbf{Z}/N\mathbf{Z})^*.$$

Suppose also that $F = \mathbf{C}$ and that $\tilde{f} = \sum a_i q^i \cdot dq/q$ is the q-expansion of f. Then the classical formulae give the action of the Hecke operators on f,

$$\widetilde{(T_l f)} = \sum_i a_{li} q^i + l\chi(l) \sum_i a_i q^{li} \qquad (**)$$

$$\widetilde{(U_q f)} = \sum a_q q^i.$$

Clearly these formulae hold for any field F of characteristic zero.

In the case where F is a field of characteristic p we now prove that similar formulae hold. First, recall that in the decomposition of the normalization $\tilde{X}_1(N)_{/k}$ of $X_1(N)_{/k}$ into irreducible components we have singled out two special ones $\tilde{\Sigma}^{\text{ét}}$ and $\tilde{\Sigma}^{\mu}$ of exponent zero and n respectively (cf. § 8). If we denote all the components $\tilde{\Sigma}_i^{(j)}$ where the i denotes the exponent then by (§ 7) there is an isomorphism

$$av(\operatorname{Pic}^0(X_1(N)_{/k})) \xrightarrow{\sim} \prod_{i,j} \operatorname{Pic}^0(\tilde{\Sigma}_i^{(j)}).$$

Here K denotes the field $\mathbf{Q}(\zeta_{pn})$. Each T_{l^*}, T_l^*, U_{q^*}, U_q^*, U_p, U_p^* and diamond operator induces an endomorphism of $av(\mathrm{Pic}^0(X_1(N)_{/K}))$ by the map $T \to av(T)$. Moreover, except for U_p, U_p^* they map $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})$ and $\mathrm{Pic}^0(\tilde{\Sigma}^{\mu})$ into themselves. Moreover, the map β_0 respects these actions in the sense that the diagram

$$\begin{array}{ccc} \mathrm{Pic}^0(Igusa(N)) & \xrightarrow{\beta_0} & \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}) \\ \Big\downarrow{\scriptstyle t} & & \Big\downarrow{\scriptstyle av(T)} \\ \mathrm{Pic}^0(Igusa(N)) & \xrightarrow{\beta_0} & \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}) \end{array}$$

commutes for each $T \in \{T_{l^*}, T_l^*, U_{q^*}, U_q^*(q \neq p), \langle a \rangle^*\}$ and t correspondingly chosen. We note that the map β_n does not commute in the same fashion. We now write t for $av(T)$ both as endomorphisms of $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})$ and of $\mathrm{Pic}^0(\tilde{\Sigma}^{\mu})$.

We now consider the induced actions of t for $t \in \{t_l, u_q(q \neq p), \langle a \rangle\}$ on the cotangent space $H^0(\tilde{\Sigma}^{\mu}, \Omega^1)$.[4] In a neighborhood of ∞, Σ^{μ} is isomorphic to $\tilde{\Sigma}^{\mu}$ and so we also have an action on the q-expansions at ∞. The formulae for t_l, for $\langle a \rangle$ and for u_q may be proved by a formal computation on Tate curves [34].

The formal justification for this is briefly as follows. On an open neighbourhood of the cusp ∞ the natural map $\tilde{\Sigma}^{\mu} \to \Sigma^{\mu}$ is an isomorphism. On such a neighbourhood we can define correspondences on Σ^{μ} by the standard formulae, by representing points of Σ^{μ} as images of points of $X(N)_{/k'}$ for suitable field extensions k'/k. For example, to each point of Σ^{μ} in such a neighbourhood there corresponds a triple $(E, t_1\ t_2)_{/k'}$ where (t_1, t_2) is a Drinfeld ζ_N-basis. We define t_l by the formula

$$t_l(E, t_1, t_2)_{/k'} = \sum (E/C_l, t_1', \bar{t}_2)_{/k'}$$

where C_l runs through the subgroups of order l, $\bar{t}_2$ is the image of t_2 and t_1' is a point chosen to make $(t_1', \bar{t}_2)$ a Drinfeld ζ_N-basis. This induces a correspondence t_l on an open neighbourhood of ∞ in Σ^{μ}, and so, too, of $\tilde{\Sigma}^{\mu}$, and using the criterion of compatibility (cf. §2) this t_l is compatible with the action of $t_l = av(T_l)$ on $\mathrm{Pic}^0(\tilde{\Sigma}^{\mu})$.

The object of the rest of this section is to establish a "q-expansion principle" (the Proposition and Corollary below). An obstacle to this is that we lack an adequate "u_p-operator". We get around this by using the "operation of Cartier and Tate".

Let $\chi\colon (\mathbf{Z}/N\mathbf{Z})^*/(\pm 1) \to \bar{\mathbf{F}}_p^*$ be an even character, and c a function from the set of rational prime numbers to $\mathbf{F}_p(l \mapsto c_l)$. Let

$$\mathscr{C}\colon H^0(\tilde{\Sigma}^{\mu}, \Omega^1) \to H^0(\tilde{\Sigma}^{\mu}, \Omega^1)$$

be the operation of Cartier and Tate (in the terminology of [57]).

Now let f be a holomorphic differential form on $\tilde{\Sigma}^{\mu}$ such that

$$\begin{aligned} \langle r \rangle f &= \chi(r) \cdot f \quad && (r \in (\mathbf{Z}/N\mathbf{Z})^*) \\ t_l f &= c_l f && (l \nmid N) \\ u_{q^*} f &= c_q \cdot f && (q \mid a) \\ \mathscr{C} f &= c_p \cdot f \end{aligned} \tag{i}$$

[4] Recall the convention of §5.8 that $t = t^d$.

If $f = \sum a_n q^n$ is the q-expansion of f about the cusp ∞ ($a_n \in \overline{\mathbf{F}}_p$) we have the formula:

$$\begin{aligned} t_l f &= \sum a_{ln} q^n + l \cdot \langle l \rangle \sum a_n q^{ln} \\ u_{q^*} f &= \sum a_{qn} q^n \\ \mathscr{C} f &= \sum a_{pn}^{\sigma} q^n \end{aligned} \tag{ii}$$

where σ is the inverse of Frobenius.

Let k' be a finite field of characteristic p. In the scheme $\tilde{\Sigma}^{\mu}_{/k'}$, the locus of ∞-cusps is a closed k'-subscheme defined by a sheaf of ideals $\mathscr{J}$, and is isomorphic to $\operatorname{Spec} k'[\zeta_a]$, where $k'[\zeta_a]$ is the k'-algebra $k'[x]/(\Phi_a(x))$ with Φ_a the cyclotomic polynomial of level a. This can be seen using theorem 10.9.1 (3) of [36].

Set $G = \{r \in (\mathbf{Z}/N\mathbf{Z})^*,\ r \equiv 1 \bmod p^n\}$. Then $G \cong (\mathbf{Z}/a\mathbf{Z})^*$ acts on $\tilde{\Sigma}^{\mu}_{/k'}$ via the diamond operators, and leaves the ideal $\mathscr{J}$ stable.

Lemma 1. *Let $r \in G$. The action of the diamond operator $\langle r \rangle$ on the locus of ∞-cusps is given by the formula.*

$$\langle r \rangle : \operatorname{Spec} k'[\zeta_a] \to \operatorname{Spec} k'[\zeta_a].$$

$$\operatorname{Spec} k'$$

$$\langle r \rangle : \zeta_a = \zeta_a^r .$$

Proof. This may be deduced from the description of the cuspidal locus given in [36] Thm. 10.10.3 and the formulas of loc. cit. Lemma 10.3.2 (see also loc. cit. §10.5, §13.10). To make the translation from [36] to our setting let the N appearing in [36] be our a; let $\Gamma_2 \subseteq GL_2(\mathbf{Z}/a\mathbf{Z})$ be the subgroup $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$ and choose $\Lambda_2 \in \operatorname{Hom\,surj}((\mathbf{Z}/a\mathbf{Z})^2, \mathbf{Z}/a\mathbf{Z})$ to be such that $\operatorname{Fix} \Lambda_2 = \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$. The action of $\langle r \rangle$ is given by the matrix $g = \begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix} \in GL_2(\mathbf{Z}/a\mathbf{Z})$, or equivalently by $\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} \in \operatorname{Fix} \Lambda_2$ since $\begin{pmatrix} 1 & 0 \\ 0 & r^{-1} \end{pmatrix}$ lies in Γ_2. Now apply loc. cit. formula (10.3.3) noting that the locus of ∞-cusps on $\tilde{\Sigma}^{\mu}_{/k'}$ is obtained from the Λ-component of $[\Gamma(a)]_{G/S}$ (of 10.3.3), for a suitable choice of Λ_1, by the homomorphism $\mathbf{Z}[\zeta_a] \otimes_{\mathbf{Z}} G_1 \to k'[\zeta_a]$ where X is sent to 0 (terminology as in 10.3.3; see also Theorems 10.5.1 and 13.10.4(3)).

q.e.d.

Using loc. cit. Theorem 10.9.1, the $\mathscr{J}$-adic completion of $\tilde{\Sigma}^{\mu}_{/k'}$ is identified with $\operatorname{Spf} k'[\zeta_a][\![q]\!]$. A holomorphic differential form φ on $\tilde{\Sigma}^{\mu}_{/k'}$ has a q-expansion

$$\tilde{\varphi} = \sum_{n \geqq 1} a_n(\varphi) \cdot q^n$$

with coefficients $a_n(\varphi)$ in $k'[\zeta_a]$ where $\tilde{\varphi}\, dq/q$ is the restriction of φ to the completion of $\mathscr{J}$.

Consider the tangent space to the ∞-locus, $\mathscr{J}/\mathscr{J}^2$, which is isomorphic to the $k'[\zeta_a]$-module $k'[\zeta_a] \cdot q$. The $k'[\zeta_a]$-module $\mathscr{J}/\mathscr{J}^2$ is free of rank 1, and the group G

acts via diamond operators on $\mathcal{J}/\mathcal{J}^2$ in a manner compatible with its action on $k'[\zeta_a]$:

$$\langle r\rangle(\alpha \cdot m) = (\langle r\rangle \cdot \alpha) \cdot (\langle r\rangle \cdot m) \qquad (**)$$

Lemma 2. *We may choose a $k'[\zeta_a]$-generator of $\mathcal{J}/\mathcal{J}^2$ fixed under the action of G.*

Proof. Let $M = \mathcal{J}/\mathcal{J}^2$ and let $m \in M$ be any $k'[\zeta_a]$-generator. If the 1-cocycle $g \mapsto gm/m \in k'[\zeta_a]$ in $Z^1(G, k'[\zeta_a]^*)$ can be split, i.e. is a coboundary ($g \mapsto g^\alpha/\alpha$ for $\alpha \in k'[\zeta_a]^*$) then $\alpha^{-1} \cdot m$ is a G-fixed generator. It suffices to show that $H^1(G, k'[\zeta_a]^*) = 0$. But since a is prime to $p = \operatorname{char} k'$, the k'-algebra $k'[\zeta_a]$ is separable, hence decomposes into a product of fields, each one isomorphic to a field extension k'' of k' generated by a primitive a-th root of unity. Let $H = \mathrm{Gal}(k''/k')$ and let $H \hookrightarrow (\mathbf{Z}/a\mathbf{Z})^* = G$ be the natural imbedding. One sees that the G-module $k'[\zeta_a]^*$ is isomorphic to the G-module induced from H:

$$\mathrm{Ind}_H^G(k''^*).$$

Therefore $H^1(G, k'[\zeta_a]^*) = H^1(H, k''^*)$ and the second group vanishes by Hilbert's Theorem 90. q.e.d.

Now let us identify $\mathcal{J}/\mathcal{J}^2$ with $k'[\zeta_a]$ by choosing a G-fixed generator m and setting

$$i\colon k'[\zeta_a] \to \mathcal{J}/\mathcal{J}^2.$$

$$\alpha \mapsto \alpha \cdot m.$$

By Lemma 1, the natural action of G on $\mathcal{J}/\mathcal{J}^2$ is then given, after this identification, by the formula

$$\langle r\rangle \cdot \zeta_a = \zeta_a^r. \qquad (***)$$

At this point, let $k' \subseteq \overline{\mathbf{F}}_p$ be large enough to contain the values of c and of χ.

Let $V = \mathrm{Pic}^0(\tilde{\Sigma}^\mu_{/\mathbf{F}_p})[p](\mathbf{F}_p)$ and $V^{c,\chi,k'}$ the k' subspace of $V \otimes_{\mathbf{F}_p} k'$ consisting of those vectors v such that $t_l v = c_l v$, $u_q v = c_q v (q \mid a)$ and $\langle r\rangle v = \chi(r) \cdot v$. We say that a k'-valued character χ is *k'-pseudo-primitive* if there is a finite totally ramified discrete valuation ring extension D of the Witt vectors $W(k')$ and a pseudoprimitive D-valued character χ_D whose reduction to the residue field k' of D is equal to χ.

Proposition. *If χ is k'-pseudo-primitive, the k' vector space $V^{c,\chi,k'}$ is of dimension $\leqq 1$.*

Proof. The mapping

$$\theta\colon \mathrm{Pic}^0(\tilde{\Sigma}^\mu_{/\mathbf{F}_p})[p] \to H^0[\tilde{\Sigma}^\mu_{/\mathbf{F}_p}, \Omega^1)^{\mathscr{C}}$$

([57], §11, Prop. 10) identifies the k'-vector space $V^{c,\chi,k'}$ with the subspace of $H^0(\tilde{\Sigma}^\mu_{/\mathbf{F}_p}, \Omega^1)^{\mathscr{C}} \otimes_{\mathbf{F}_p} k'$ on which t_l acts like $c_l (l \nmid N)$, u_q acts like $c_q (q \mid a)$ and $\langle r\rangle$ acts like $\chi(r)$ ($r \in (\mathbf{Z}/N\mathbf{Z})^*$). If f is a differential form in this subspace, f is determined by its first Fourier coefficient $a_1(f)$ --- (note that $a_{pk}(f) = \langle n_p\rangle^{-1} a_k(f)$) --- and consequently $V^{c,\chi,k'}$ imbeds in the subspace of $k'[\zeta_a]$ consisting of elements v such that $\langle r\rangle v = \chi(r) \cdot v$. But this subspace is one-dimensional over k', as the reader can easily verify, using k'-pseudo-primitivity of χ, and the formula (***).

Corollary. *Let χ be k'-pseudo-primitive. Let $V_{\text{ét}}^{c,\chi,k'}$ be the subspace of*

$$\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})[p](\mathbf{F}_p)\otimes_{\mathbf{F}_p}k'$$

consisting of those elements such that t_l acts as (multiplication by) $c_l(l\nmid N)$, u_q acts as $c_q(q|a)$ and $\langle r\rangle$ acts as $\chi(r)(r\in(\mathbf{Z}/N\mathbf{Z})^*)$. Then the dimension of $V_{\text{ét}}^{c,\chi,k'}$ is less than or equal to 1.

Proof. The involution $w_{\zeta_{p^n}}$ on $X_1(N)$ induces isomorphisms from $\tilde{\Sigma}^{\mu}$ to $\tilde{\Sigma}^{\text{ét}}$ and from $\tilde{\Sigma}^{\text{ét}}$ to $\tilde{\Sigma}^{\mu}$, defined over $\mathbf{F}_p$. Let r_l denote the element in $(\mathbf{Z}/N\mathbf{Z})^*$ such that $r_l\equiv l \bmod p^n$ and $r_l\equiv 1 \bmod a$, for any prime $l\neq p$. Then we have the commutation rules

$$w_{\zeta_{p^n}} t_{l*}\, w_{\zeta_{p^n}}^{-1} = \langle r_l\rangle t_{l*} \quad \text{for} \quad l\nmid N$$

$$w_{\zeta_{p^n}} u_{q*}\, w_{\zeta_{p^n}}^{-1} = \langle r_q\rangle u_{q*} \quad \text{for} \quad q|a\,.$$

Moreover, conjugation by $w_{\zeta_{p^n}}$ preserves the group of diamond operators.

It follows that $w_{\zeta_{p^n}}$ will bring $V_{\text{ét}}^{c,\chi,k'}$ to a space of the form $V^{c',\chi,',k'}$ for suitable c' and χ'. The corollary then follows from the proposition.

Chapter 3. A study of abelian varieties which are "good" quotients of $J_1(N)$

§ 1. Construction of A_n

We fix an integer $n\geqq 1$ and set $N=ap^n$ with a a positive integer such that $(a,p)=1$. Recall that for any $i\geqq 1$ $X_1(ap^i;ap^{i-1})_{/\mathbf{Q}}$ is the modular curve associated to the group $\Gamma_0(ap^i)\cap\Gamma_1(ap^{i-1})$. Let π_i and ρ_i be the natural projections

$$\pi_i: X_1(ap^i)_{/\mathbf{Q}}\to X_1(ap^i;ap^{i-1})_{/\mathbf{Q}}, \qquad \rho_i: X_1(ap^i;ap^{i-1})_{/\mathbf{Q}}\to X_1(ap^{i-1})_{/\mathbf{Q}}$$

These induce maps of the associated Jacobians

$$\pi_i^*: J_1(ap^i;ap^{i-1})_{/\mathbf{Q}}\to J_1(ap^i)_{/\mathbf{Q}} \quad \text{and} \quad \rho_{i*}: J_1(ap^i;ap^{i-1})_{/\mathbf{Q}}\to J_1(ap^{i-1})_{/\mathbf{Q}}.$$

Also let w be the involution on $X_1(ap;a)$ given by

$$w: \quad (E,P_a,G_p)\to(E/G_p,\overline{P}_a,\overline{G}_p')$$

where the bar denotes image in E/G_p, and G_p' is a group of order p in E not equal to G_p, and P_a is a point of order a.

Consider the morphism:

$$\pi_1^*\times(w_*\circ\pi_1^*): \quad J_1(a)_{/\mathbf{Q}}\times J_1(a)_{/\mathbf{Q}}\to J_1(ap;a)_{/\mathbf{Q}}. \tag{1}$$

The kernel is shown to be finite by considering the induced map on differentials (viewed as the cotangent spaces of the abelian varieties). For on their associated q-expansions the two maps are respectively

$$\pi_1^*: \quad \sum a_n q^n \to \sum a_n q^n, \qquad w_* \circ \pi_1^*: \quad \sum a_n q^n \to \sum a_n q^{np}.$$

The theory of newforms implies that the dimension of the sum of the images of these maps is equal to $2 \dim J_1(a)_{/\mathbf{Q}}$ ([40], Chap. VIII, §3), and so the map (1) induces an injective map on differentials.

Let $\mathscr{K}_1$ be an abelian subvariety of $J_1(ap;a)_{/\mathbf{Q}}$ which is isogenous to $J_1(ap;a)/\text{image}\,(J_1(a) \times J_1(a))$. The quotient $J_1(ap;a)/\text{image}\,(J_1(a) \times J_1(a))$ has multiplicative reduction as follows easily from [15], VI, Theorem 6.9 and Raynaud's theorem (Prop. 1 of §1 of Chap. 2). Then since $J_1(a)_{/\mathbf{Q}} \times J_1(a)_{/\mathbf{Q}}$ has good reduction at p, it is clear that $\mathscr{K}_1$ is uniquely determined as the maximal abelian subvariety of $J_1(ap;a)_{/\mathbf{Q}}$ with multiplicative reduction at p. We define A_0 to be the quotient $J_1(ap;a)/\mathscr{K}_1$ and $\alpha_0: J_1(ap;a) \to A_0$ the natural map.

Now we will inductively define A_i and $\mathscr{K}_i$ for $1 \leqq i \leqq n$. Each $\mathscr{K}_i$ will be an algebraic subgroup of $J_1(ap^i, ap^{i-1})_{/\mathbf{Q}}$ and each A_i a natural quotient abelian variety of $J_1(ap^i)_{/\mathbf{Q}}$ via a map $\alpha_i: J_1(ap^i)_{/\mathbf{Q}} \to A_i$. Given $\mathscr{K}_i$ for some $1 \leqq i \leqq n$, define A_i and α_i by the exact sequence

$$\mathscr{K}_i \xrightarrow{\pi_i^* \mid \mathscr{K}_i} J_1(ap^i)_{/\mathbf{Q}} \xrightarrow{\alpha_i} A_i \longrightarrow 1.$$

Given A_i for some $1 \leqq i \leqq n-1$, define $\mathscr{K}_{i+1}$ by the exact sequence

$$0 \to \mathscr{K}_{i+1} \to J_1(ap^{i+1}, ap^i)_{/\mathbf{Q}} \xrightarrow{\alpha_i \circ \rho_{i+1*}} A_i.$$

It is clear from the definition of $\mathscr{K}_1$ that it is stable under all endomorphisms of $J_1(ap,a)_{/\mathbf{Q}}$. Hence any endomorphism of $J_1(ap,a)_{/\mathbf{Q}}$ also induces an endomorphism of $A_{0/\mathbf{Q}}$ which commutes with the projection α_0. In particular, we may view any operator in the set $\{\langle r\rangle, T_l, U_p^*, U_{q*}, U_p^*, U_{p*}\}$ as an endomorphism of $A_{0/\mathbf{Q}}$. One checks that the maps π_i^* and $\alpha_i \circ \rho_{i+1*}$ also commute with the naturally defined actions of the above Hecke operators on their respective domains and ranges (except for U_p^*). We thus get an action of the same operators (except for U_p^*) on each $A_{i/\mathbf{Q}}$ for $0 \leqq i \leqq n$.

Up to isogeny the $A_{i/\mathbf{Q}}$'s are given inductively by the formulae:

$$A_0 \sim J_1(a) \times J_1(a) \qquad \text{——I}$$

$$A_i \sim \{J_1(ap^i)/\pi_i^*(J_1(ap^i, ap^{i-1}))\} \times A_{i-1} \qquad \text{——II (for } i \geqq 1).$$

Furthermore, the isogenies given in II may be chosen so as to respect the natural actions of all the Hecke operators in the set $\{\langle r\rangle, T_l, U_q^*, U_{q*}$, for $q \mid a, U_{p*}\}$, whereas the isogeny I respects those in the set $\{\langle r\rangle, T_l, U_q^*, U_{q*}$, for $q \mid a\}$. We set

$$V_0 = A_0, \quad V_i = \{J_1(ap^i)/\pi_i^* J_1(ap^i; ap^{i-1})_{/\mathbf{Q}}\} \quad \text{for } i = 1, \ldots, n.$$

Then we may deduce from I and II that

$$A_n \sim \prod_{j=0}^{n} V_j, \tag{2}$$

and this isogeny respects the actions of $\{\langle r\rangle, T_l, U_q^*, U_{q*}\}$ on both sides.

If $A_{n,p/\mathbf{Q}}$ denotes the p-divisible group scheme over **Q** associated to the abelian variety $A_{n/\mathbf{Q}}$, we have a natural action of $\mathbf{Z}_p[(\mathbf{Z}/ap^n\mathbf{Z})^*/(\pm 1)]$ on $A_{n,p}$ where $r \in (\mathbf{Z}/ap^n\mathbf{Z})^*/(\pm 1)$ acts via the diamond operator $\langle r\rangle$. If $\mathfrak{m}$ is a component, let $A_{n,\mathfrak{m}/\mathbf{Q}}$ denote the p-divisible subgroup scheme of $A_{n,p/\mathbf{Q}}$ (the direct summand) which is the image of the irreducible idempotent $e_{\mathfrak{m}}$ (Chap. 1, §3). Thus $A_{n,\mathfrak{m}/\mathbf{Q}}$ is naturally endowed with the structure of $R_{\mathfrak{m}}$-module.

§ 2. *Reduction* mod p

Since n will be fixed throughout this chapter we will often write A for A_n. Our first goal is to prove the following theorem.

Proposition 1. *A acquires good reduction at p over $\mathbf{Q}(\zeta_{p^n})$.*

Since the property of having good reduction is invariant under isogeny (cf. [26], 2.2.9) it will be sufficient to prove the following lemma.

Lemma 1. *V_i acquires good reduction at p over $\mathbf{Q}(\zeta_{p^l})$ for $0 \leqq i \leqq n$.*

Proof. For $i = 0$ the lemma is well known. Suppose then that $i \geqq 1$. Let X_j be the abelian variety associated by Shimura to a newform f_j. Then it follows from the definition of V_i that there is an isogeny

$$V_i \sim \prod_{j_i \in J_i} X_{j_i} \tag{1}$$

where the newforms f_{j_i} attached to a $j_i \in J_i$ has level $a' p^i$ for some $a' | a$. Furthermore, the conductor of each such f_{j_i} must be divisible by p^i. We claim that the abelian variety X_{j_i} associated to such a form f_{j_i} acquires good reduction at p over $\mathbf{Q}(\zeta_{p^l})$. It will be sufficient to prove that X_{j_i} acquires good reduction at p over an extension of $\mathbf{Q}(\zeta_{p^l})$ which is unramified outside p. This result is an immediate consequence of the following Proposition which is a corollary of a very general theorem due to Langlands and whose relevance was pointed out to us by Ribet. Alternatively, we may use the Theorem of Chap. XIV of [36].

Proposition 2. Let *X_f be the abelian variety associated by Shimura to a newform f of level M with character ψ. Write $\psi = \psi_q \psi_{q'}$ where ψ_q is ramified only at the prime q, and $\psi_{q'}$ is unramified at q. Suppose that q is a prime divisor of M such that $(M/\mathrm{cond}\,\psi)$ is prime to q. Then X_f acquires good reduction at q over $\mathcal{O}_F$ where F is the splitting field of the character ψ_q over* **Q**.

Proof. 1) Langlands has shown how to attach to any newform f an irreducible admissible representation π of $GL_2(\mathbf{A}_f)$ where $\mathbf{A}_f$ denotes the adèles over **Q** with trivial ∞-component. The representation π decomposes as a restricted tensor product $\pi = \bigotimes_{l<\infty} \pi_l$ of infinite dimensional admissible representations π_l of

$GL_2(\mathbf{Q}_l)$. Furthermore, the L-series associated to f (via the Mellin transform) is the product of the local L-series attached to the representations π_l. A theorem of Ogg [45] shows that under the hypothesis that $q \nmid (M/\text{cond}\,\psi)$ there is a non-trivial Euler factor at q. In particular, the representation π_q is either a special representation or a principal series representation. It is proved in [3] that under the same hypothesis $q \nmid (M/\text{cond}\,\psi)$, π_q is in fact a principal series representation. (Actually they prove it under a weaker hypothesis). We give a simple alternative proof in this special case.

The representation π_q, if it were special, would have the form $\sigma(\mu, \mu|\ |^{-1})$ for some quasi-character μ of $\mathbf{Q}_q^*$. The existence of an Euler factor at q shows that μ must be unramified. But this contradicts the fact that ψ is ramified at q, and so π_q must be in the principal series.

To each π_l there is associated by the local Langlands correspondence a two-dimensional complex representation of $W_{\mathbf{Q}_l}$, the (absolute) Weil group. The representation of $W_{\mathbf{Q}_q}$ associated to π_q has the form

$$w \to \begin{bmatrix} \mu_1(\alpha(w)) & \\ & \mu_2(\alpha(w)) \end{bmatrix}$$

where α is the canonical surjection $W_{\mathbf{Q}_q} \to \mathbf{Q}_q^*$ and μ_1 and μ_2 are quasicharacters. Since there is an Euler factor at q, one of μ_1 and μ_2 is unramified. Thus we may assume that the representation has the form $\mu_1 = \psi_q \cdot \varepsilon$, $\mu_2 = \varepsilon^{-1}$ where ε is unramified and ψ_q is the restriction to $\mathbf{Q}_q^*$ of the idelic character associated to ψ.

Now let X_f be the abelian variety over $\mathbf{Q}$ which is associated to f. Then as is explained in [66] and in [6], especially § 3, for each prime s dividing N we may attach a representation π_s' of $W_{\mathbf{Q}_s}$ by its action on $H_l^1(X_f)$ where H_l^1 is l-adic cohomology. More precisely, if $K_f \subseteq \mathbf{C}$ is the field generated by the Fourier coefficients of f then we may view K_f as contained in $\text{End}(X_f) \otimes \mathbf{Q}$. Picking a prime λ above l in K_f and an embedding $K_{f,\lambda} \to \mathbf{C}$ compatible with the inclusion of K_f in $\mathbf{C}$, π_s' is the representation of $W_{\mathbf{Q}_s}$ on

$$H_\lambda^1(X_f) \underset{K_{f,\lambda}}{\otimes} \mathbf{C} = (H_l^1(X_f) \underset{K_f \otimes \mathbf{Q}_l}{\otimes} K_{f,\lambda}) \otimes \mathbf{C}.$$

The isomorphism class of this representation is independent of the choice of l and λ.

Langlands proved in [44] that when π_s is either a principal series or special representation, then $\pi_s = \pi_s'$. Hence the l-adic representation of $W_{\mathbf{Q}_q}$ associated to X_f when restricted to $\text{Gal}(\bar{\mathbf{Q}}/\ker \psi_q)$ is just the sum of two unramified quasicharacters. By the criterion of Néron-Ogg-Safarevich ([26], 2.2.9), $A_{/F}$ has good reduction at q where F is the splitting field of ψ_q over $\mathbf{Q}$.

2) *An alternate reference.* We may apply the good reduction theorem of Chapter XIII of [36] with $v = n$ in the terminology of that theorem. As in 1), the theorem of Néron-Ogg-Shafarevitch allows us to conclude the proof of proposition 2.

For ψ any $\bar{\mathbf{Q}}_p^*$-valued character recall the notation $\psi = \psi_p \cdot \psi_{p'}$ where $\psi_{p'}$ has conductor prime to p, and ψ_p has conductor a power of p.

Let $\mathfrak{m}$ be a component. If χ is a basic character belonging to $\mathfrak{m}$, then $\chi_p = \omega^k$ where ω is the Teichmüller character and $0 \leqq k < p-1$.

Definition. *The subring $\mathcal{O}_{n,\mathfrak{m}} \subseteq \bar{\mathbf{Q}}_p$ is defined to be the ring extension of $\mathbf{Z}_p$ generated by the splitting fields of ψ_p over $\mathbf{Q}_p$ where ψ runs through* all *characters of $(\mathbf{Z}/ap^n\mathbf{Z})^*$ belonging to $\mathfrak{m}$.*

The ring extension $\mathcal{O}_{n,\mathfrak{m}}/\mathbf{Z}_p$ is the (totally ramified) sub-discrete valuation ring in $\mathbf{Z}_p[\mu_{p^n}]$ of degree $\frac{p-1}{d}\cdot p^{n-1}$ where $d = \text{g.c.d.}(p-1, k)$.

Corollary (*to Proposition 2*). *The p-divisible group scheme $A_{n,\mathfrak{m}/\mathbf{Q}_p}$ admits a prolongation to a p-divisible group scheme over the base $\mathcal{O}_{n,\mathfrak{m}}$.*

Proof. This follows from the fact that Proposition 2 implies that for any new-form f with character

$$\psi: \quad (\mathbf{Z}/ap^n\mathbf{Z})^* \to \mathbf{C}$$

and any field isomorphism $\mathbf{C} \xrightarrow[i]{} \overline{\mathbf{Q}}_p$, such that $i\psi$ belongs to $\mathfrak{m}$, the abelian variety X_f achieves good reduction over $\mathcal{O}_{n,\mathfrak{m}}$.

We now obtain a more refined description of A by applying the results of §1. Let us write $K_\mathfrak{p}$ for the field $\mathbf{Q}_p(\zeta_{p^n})$. Then recall that there is an isomorphism

$$av(J_1(ap^n)_{/K_\mathfrak{p}}) \cong \mathrm{Pic}^0(\tilde{\Sigma}_n^{\text{ét}}) \times \mathscr{B}_n \times \mathrm{Pic}^0(\tilde{\Sigma}_n^{\mu}) \tag{1}$$

where we have used the notation $\tilde{\Sigma}_n^{\text{ét}}$ and $\tilde{\Sigma}_n^{\mu}$ to denote the normalizations of the "good" components of $X_1(ap^n)_{/k}$ of exponents 0 and n respectively, and where $\mathscr{B}_n$ denotes the "contribution" from all the middle components:

$$\mathscr{B}_n = \prod_{0<j<n} \mathrm{Pic}^0[(X_1(ap^n)_{/k})_j].$$

We also have an isogeny

$$av(J_1(ap^n, ap^{n-1})_{/K_\mathfrak{p}}) \approx \mathrm{Pic}^0(\tilde{\Sigma}_{n-1}^{\text{ét}}) \times \mathscr{B}_n \times \mathrm{Pic}^0(\tilde{\Sigma}_{n-1}^{\mu}). \tag{2}$$

To relate the "three-fold product decompositions" (1) and (2) to the natural mappings π^* and ρ_*, we have:

The natural mapping

$$\pi^*: \ av(J_1(ap^n, ap^{n-1})_{/K_\mathfrak{p}}) \to av(J_1(ap^n)_{/K_\mathfrak{p}}) \tag{3}$$

is compatible with a mapping of the right-hand side of (2) to the right-hand side of (1) which sends $(x, y, z) \in \mathrm{Pic}^0(\tilde{\Sigma}_{n-1}^{\text{ét}}) \times \mathscr{B}_n \times \mathrm{Pic}^0(\tilde{\Sigma}_{n-1}^{\mu})$ to the point (pr^*x, y, pr^*z) where pr denotes the natural projections

$$\tilde{\Sigma}_n^{\text{ét}} \xrightarrow[pr]{} \tilde{\Sigma}_{n-1}^{\text{ét}}, \quad \tilde{\Sigma}_n^{\mu} \xrightarrow[pr]{} \tilde{\Sigma}_{n-1}^{\mu}.$$

Recall that there is an isogeny (Prop. 1 of § 8)

$$av((J_1(ap^{n-1})_{\mathbf{Q}_p(\zeta_{p^{n-1}})}) \to av((J_1(ap^{n-1})_{/\mathbf{Q}_p(\zeta_{p^n})})$$

and hence an isogeny

$$\mathrm{Pic}^0(\tilde{\Sigma}_{n-1}^{\text{ét}}) \times \mathscr{B}_{n-1} \times \mathrm{Pic}^0(\tilde{\Sigma}_{n-1}^{\mu}) \to av(J_1(ap^{n-1})_{/K_\mathfrak{p}}) \tag{1}'$$

by (1). The mapping

$$\rho_*: \ av(J_1(ap^n, ap^{n-1})_{/K_\mathfrak{p}}) \to av(J_1(ap^{n-1})_{/K_\mathfrak{p}})$$

is *not* compatible with the three-fold product decompositions in (1) and (2); nevertheless there is a commutative diagram

$$\begin{array}{ccc} \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}_{n-1}) \times \mathrm{Pic}^0(\tilde{\Sigma}^{\mu}_{n-1}) & \longrightarrow & av(J_1(ap^n, ap^{n-1})_{/K_\mathfrak{p}}) \\ \downarrow = & & \downarrow \rho_* \\ \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}_{n-1}) \times \mathrm{Pic}^0(\tilde{\Sigma}^{\mu}_{n-1}) & \longrightarrow & av(J_1(ap^{n-1})_{/K_\mathfrak{p}}) \end{array} \tag{4}$$

where the horizontal mappings are given by the maps $(x, z) \to (x, o, z)$ composed with the isogenies in (1)′ and (2). The asserted commutativity follows from the explicit description of the relationship between the irreducible components of the fibre over k of $X_1(ap^n, ap^{n-1})$ and $X_1(ap^{n-1})$, as described in Chap. 2, § 7 (4). See also the *summary* following Proposition 2 there.

Since A_n has good reduction at p over $\mathbf{Q}(\zeta_{p^n})$, its Néron model $A_{n/\mathbf{Z}_p[\zeta_{p^n}]}$ is an abelian scheme. Thus $av(A_{n/K_\mathfrak{p}})$ is the fibre $A_{n/k}$ over k of the Néron model.

Let $\mathcal{O}'$ denote the ring of integers in any finite extension K' of $K_\mathfrak{p}$ with k' as residue field and $X_1(ap^n)^{\#}_{/\mathcal{O}'}$, $X_1(ap^n, ap^{n-1})^{\#}_{/\mathcal{O}'}$ regular schemes which are obtained by performing successive blow-ups on the appropriate canonical model. Let $J_1(ap^n)_{/\mathcal{O}'}$ and $J_1(ap^n, ap^{n-1})_{/\mathcal{O}'}$ denote the Néron models.

Proposition 2. *The natural mappings*

(i) $av(J_1(ap^n)_{/K'}) \to A_{n/k'}$

(ii) $av(J_1(ap^n, ap^{n-1})_{/K'}) \to A_{n-1/k'}$

are surjective.

The natural mappings

(iii)
$$J_1(ap^n)_{/\mathcal{O}'} \to A_{n/\mathcal{O}'}$$
$$\mathrm{Pic}^0(X_1(ap^n)^{\#}_{/\mathcal{O}'}) \to A_{n/\mathcal{O}'}$$

(iv)
$$J(ap^n, ap^{n-1})_{/\mathcal{O}'} \to A_{n-1/\mathcal{O}'}$$
$$\mathrm{Pic}^0(X_1(ap^n, ap^{n-1})_{/\mathcal{O}'}) \to A_{n-1/\mathcal{O}'}$$

are faithfully flat.

Proof. Since $A_{n/K'}$ is a quotient of $J_1(ap^n)_{/K'}$, there is an abelian subvariety of $J_1(ap^n)_{/K'}$ mapping isogenously to $A_{n/K'}$. One easily deduces (i) and similarly for (ii). By Raynaud's theorem (Proposition 1 of § 1 of Chap. 2) $\mathrm{Pic}^0(X_1(ap^n)^{\#}_{/\mathcal{O}'})$ is the connected component of $J_1(ap^n)_{/\mathcal{O}'}$ and therefore the morphisms of (iii) have constant fibre-dimension. Since the schemes involved are smooth, the morphisms are flat as can easily be seen using the "local criterion of flatness" (*Bourbaki*, Commutative Algebra III, § 5, Theorem 1; or [27], III, Lemma 10.3A). But the morphisms are also surjective, hence faithfully flat. A similar argument holds for the morphisms of (iv).

Consider the morphism $\sigma = \sigma_n$ given by the composition

$$\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}_n) \times \mathrm{Pic}^0(\tilde{\Sigma}^{\mu}_n) \to av(J_1(ap^n)_{/K_\mathfrak{p}}) \twoheadrightarrow A_{n/k_n}$$

where first map is $(x, z) \mapsto (x, o, z)$ in terms of the three-fold product given in (1) above, and $k_n = k$ is the residue field of $\mathbf{Q}_p(\zeta_{p^n})$.

Proposition. *The morphism*

$$\sigma\colon \mathrm{Pic}^0(\tilde{\Sigma}_n^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}_n^{\mu}) \to A_{n/k_n}$$

is an isogeny.

Proof. We proceed by induction on n. When $n=1$, we have that $\mathscr{B}_1 = 0$, and the subgroupscheme $\mathscr{K}_1$ in $J_1(ap^n)_{/K_\mathfrak{p}}$ is the largest abelian sub-variety which has multiplicative type reduction in characteristic p. The proposition then follows for $n=1$. See Proposition 4 below for a closer study of the case $n=1$.

Now let n be greater than 1. Consider the commutative diagrams

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathscr{K}_n & \longrightarrow & av(J_1(ap^n)_{/K_\mathfrak{p}}) & \longrightarrow & A_{n/k_n} & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ & & & & \pi^* = \pi_n^* & & & & \\ 0 & \longrightarrow & \mathscr{K}_n' & \longrightarrow & av(J_1(ap^n, ap^{n-1})_{/K_\mathfrak{p}}) & \longrightarrow & A_{n-1/k_n} & \longrightarrow & 0 \end{array} \tag{6}$$

where $\mathscr{K}_n$, $\mathscr{K}_n'$ are the subgroup schemes defined so that the horizontal rows are exact sequences. Note that each of the central terms comes from "*av*" applied to abelian varieties over the field $\mathbf{Q}_p(\zeta_{p^n}) = K_\mathfrak{p}$. There are isogenies (i.e., surjections of group schemes with finite kernel)

$$av(\pi_n^*(\mathscr{K}_{n/K_\mathfrak{p}})) \to \mathscr{K}_n, \quad av(\mathscr{K}_{n/K_\mathfrak{p}}) \to \mathscr{K}_n'$$

in the notation of § 1. This follows immediately from the definitions of $\mathscr{K}_n$ and A_n (in characteristic zero). Therefore, since π_n^* has finite kernel, the map it induces from $\mathscr{K}_n'$ to $\mathscr{K}_n$ is an isogeny (in the sense that it has finite kernel and cokernel).

Now assume that the proposition is true for $n-1$. Then by (4) we have a commutative (but not exact) diagram

$$\begin{array}{ccccc} \mathrm{Pic}^0(\tilde{\Sigma}_{n-1}^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}_{n-1}^{\mu}) & \longrightarrow & av(J_1(ap^n, ap^{n-1})_{/K_\mathfrak{p}}) & \longrightarrow & A_{n-1/k_n} \\ \downarrow = & & \downarrow \rho_* & & \downarrow = \\ \mathrm{Pic}^0(\tilde{\Sigma}_{n-1}^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}_{n-1}^{\mu}) & \longrightarrow & av(J_1(ap^{n-1})_{/K_\mathfrak{p}}) & \longrightarrow & A_{n-1/k_n}. \end{array}$$

By the inductive hypothesis the composition of the two morphisms in the lower row is an isogeny. (Note that although we are working with the base $K_\mathfrak{p} = \mathbf{Q}_p(\zeta_{p^n})$ the composite map of the lower row is still an isogeny). Hence the same is true for the top row. Thus the natural projection, $\lambda_n'\colon \mathscr{K}_n' \to \mathscr{B}_n$ formed from the commutative diagram (again not exact)

$$\begin{array}{ccccc} \mathscr{K}_n & \longrightarrow & av(J_1(ap^n)_{/K_\mathfrak{p}}) & \longrightarrow & \mathrm{Pic}^0(\tilde{\Sigma}_n^{\text{ét}}) \times \mathscr{B}_n \times \mathrm{Pic}^0(\tilde{\Sigma}_n^{\mu}) \\ \uparrow & & \uparrow \pi_n^* & & \uparrow \\ \mathscr{K}_n' & \longrightarrow & av(J_1(ap^n, ap^{n-1})_{/K_\mathfrak{p}}) & \longrightarrow & \mathrm{Pic}^0(\tilde{\Sigma}_{n-1}^{\text{ét}}) \times \mathscr{B}_n \times \mathrm{Pic}^0(\tilde{\Sigma}_{n-1}^{\mu}) \end{array}$$

is an isogeny (cf. (3) for the right hand square and (6) for the left hand one). Hence also the projection λ_n: $\mathscr{X}_n \to \mathscr{B}_n$ is an isogeny since the map $\mathscr{X}_n' \to \mathscr{X}_n$ is an isogeny. This is readily seen to be equivalent to the proposition for n.

The remainder of this section is devoted to the case $n=1$.

Let ρ_1 and ρ_1' denote the maps $X_1(ap;a) \to X_1(a)$ given by

$$\rho_1\colon (E, e_a, \mathscr{E}_p) \mapsto (E, e_a) \quad \text{and} \quad \rho_1'\colon (E, e_a, \mathscr{E}_p) \mapsto (E/\mathscr{E}_p, \bar{e}_a)$$

where e_a is a point of order a on E and $\mathscr{E}_p$ is a subgroup of order p. Recall that

$$\mathscr{K}_1 \subseteq \ker\{(\rho_1^* \times \rho_1'^*)\colon \ J_1(ap,a) \to J_1(a) \times J_1(a)\}.$$

(in fact, $\mathscr{K}_1$ is the connected component of the kernel of this map).

Since the composition

$$J_1(a) \times J_1(a) \xrightarrow{\rho_1^* \times \rho_1'^*} J_1(ap,a) \longrightarrow J_1(a) \times J_1(a)$$

is just multiplication by $(p+1)$, the mapping

$$\mathscr{K}_1 \times J_1(a) \times J_1(a) \xrightarrow[i \times \rho_1^* \times \rho_1'^*]{} J_1(ap,a)$$

is an isogeny with kernel of order prime to p. Here i is the natural injection.

Since the composition

$$J_1(ap,a) \xrightarrow{\pi_1^*} J_1(ap) \xrightarrow{\pi_{1*}} J_1(ap,a)$$

is multiplication by an integer prime to p, we get an isogeny with kernel of order prime to p,

$$\mathscr{K}_1 \times J_1(a) \times J_1(a) \times (\ker \pi_{1*})^0 \xrightarrow[\psi]{} J_1(ap)$$

where $(\ker \pi_{1*})^0$ is the connected component of the identity in $\ker \pi_{1*}$, where

$$\psi = \pi_1^* i \times \pi_1^* \rho_1^* \times \pi_1^* \rho_1'^* \times j$$

and where j is the natural inclusion.

Note that $\pi_1^* i$ is the natural mapping of $\mathscr{K}_1$ to $J_1(ap)$.

Let the subscript p denote associated p-divisible group. It follows from the above discussion that we have a canonical product decomposition of p-divisible groups over $\mathbf{Q}$:

$$J_1(ap)_p = \mathscr{K}_{1,p} \times A_{1,p}. \tag{7}$$

Let $\mathscr{O} = \mathbf{Z}_p[\zeta_p]$ with $k(=\mathbf{F}_p)$ as residue field. Let $J_1(ap)^0_{/\mathscr{O}}$ denote the connected component of the Néron model over $\mathscr{O}$, and $J_1(ap)^0_{p/\mathscr{O}}$ the ind-quasi-finite group scheme $\bigcup_{\nu=1}^{\infty} J_1(ap)^0[p^\nu]$.

We have

$$J_1(ap)^0_{p/\mathscr{O}} = \mathscr{K}^0_{1,p/\mathscr{O}} \times A_{1,p/\mathscr{O}}$$

where $A_{1,p/\mathcal{O}}$ is the p-divisible group scheme over $\mathcal{O}$ associated to the abelian scheme $A_{1/\mathcal{O}}$, $\mathcal{K}^0_{1/\mathcal{O}}$ is the connected component of the Néron model over $\mathcal{O}$, and consequently where $\mathcal{K}^0_{1,p/\mathcal{O}}$ is an ind-quasi finite group scheme whose special fibre is of multiplicative type. Projection onto the second factor is induced from the natural mapping

$$\alpha_1 : \ J_1(ap) \to A_1 .$$

Proposition 4. *The natural isogeny*

$$\sigma : \ \mathrm{Pic}^0(\tilde{\Sigma}_1^{\text{ét}})_p \times \mathrm{Pic}^0(\tilde{\Sigma}_1^{\mu})_p \to A_{1,p/k}$$

is an isomorphism.

Proof. Consider the commutative diagram

$$\begin{array}{ccc} J_1(ap)^0_{p/k} & \longrightarrow & A_{1,p/k} \\ \downarrow & & \downarrow \\ av(J_1(ap))_p & & av(A_1)_p \\ \| & & \| \\ \mathrm{Pic}^0(\Sigma_1^{\text{ét}})_p \times \mathrm{Pic}^0(\Sigma_1^{\mu})_p & \xrightarrow[\sigma]{} & A_{1,p/k} \end{array}$$

But $\mathcal{K}^0_{1/k}$ is a (connected) multiplicative type group scheme over k. It must therefore be in the kernel of the natural mapping

$$J_1(ap)^0_{/k} \to av(J_1(ap)) .$$

Consequently, $\mathcal{K}^0_{1,p/k}$ goes to zero under the left-hand vertical mapping of the above diagram. Since $\mathcal{K}^0_{1,p/k}$ is, in fact, the kernel of the unlabelled horizontal mapping, σ is an isomorphism.

§ 3. *Formulas for U_p*

Let $\mathcal{O} = \mathcal{O}_n = \mathbf{Z}_p[\zeta_{p^n}]$ and let $k = k_n$ be its residue field ($\cong \mathbf{F}_p$). Let $K_{\mathfrak{p}}$ be its field of fractions. We also let $\mathcal{O}'$ denote some finite unramified extension of $\mathcal{O}$; k' and $K'_{\mathfrak{p}}$ will be its residue field and field of fractions respectively.

Our standard diagram of maps

$$X_1(ap^n)_{/\mathcal{O}} \xrightarrow{\pi_n} X_1(ap^n, ap^{n-1})_{/\mathcal{O}} \xrightarrow{\rho_n} X_1(ap^{n-1})_{/\mathcal{O}}$$

gives a commutative diagram:

$$\begin{array}{ccc} \mathrm{Pic}^0(X_1(ap^n)_{/\mathcal{O}}) & \longrightarrow & A_{n/\mathcal{O}} \\ \uparrow{\scriptstyle \pi_n^*} & & \uparrow \\ \mathrm{Pic}^0(X_1(ap^n, ap^{n-1})_{/\mathcal{O}} & \longrightarrow & A_{n-1/\mathcal{O}} \\ \downarrow{\scriptstyle \rho_{n*}} & & \downarrow = \\ \mathrm{Pic}^0(X_1(ap^{n-1})_{/\mathcal{O}}) & \longrightarrow & A_{n-1/\mathcal{O}} \end{array} \qquad (*)$$

If D is a divisor on the smooth locus of $X_1(ap^n)_{/k'}$ such that the restriction of D to every irreducible component of $X_1(ap^n)_{/k'}$ has degree zero, then D determines a k'-valued point of $av(J_1(ap^n)/K'_*)$ and hence, by application of (*), a k'-valued point of A_n. We will say that D is *congruent* to 0 ($D \equiv 0$) if the k'-valued point of A_n which D determines is zero. More generally, let D_1, D_2 be two divisors on the smooth locus of $X_1(ap^n)_{/k'}$ such that $D_1 - D_2$ has degree zero on every irreducible component. Then if $D_1 - D_2 \equiv 0$, we will write $D_1 \equiv D_2$. Clearly if D_1 and D_2 lift to divisors $\tilde{D}_{1/\mathcal{O}'}, \tilde{D}_{2/\mathcal{O}'}$ which give rise to the same K'_*-valued section of $A_{n/k'}$, then they are congruent. By "lift" we mean as relative Cartier divisors (flat) over the base $\mathcal{O}'$.

Consider now the operator $\pi_n^* \circ \pi_{n*} = s$ on $\mathrm{Pic}^0(X_1(ap^n)_{/\mathcal{O}})$. Since π_n is simply passage to the quotient space of $X_1(ap^n)_{/\mathcal{O}}$ under the action of G_n (a cyclic group of order p), the endomorphism s is multiplication by the element $\sum_{t \in G_n} [t]$ of the group ring $\mathbf{Z}[G_n]$ which acts on $\mathrm{Pic}^0(X_1(ap^n)_{/\mathcal{O}})$ and so too on divisors.

Now restrict to characteristic p. We observe that on the intermediate components $\Sigma_j^{(i)}$, i.e., those of exponent j with $0 < j < n$, the map induced by π_n on $\Sigma_j^{(i)}$ is radicial. Thus the action of G_n on its k' valued points is trivial and the action of s on divisors supported on $\Sigma_j^{(i)}$ is just multiplication by p.

In the discussion below, we let $(E, e_a, (t_1, t_2))_{/k'}$ and $(E', e'_a, (t'_1, t'_2))_{/k'}$ be triples, where E and E' are ordinary elliptic curves over k', e_a and e'_a are points of order a on E and E' respectively, and (t_1, t_2) and (t'_1, t'_2) are Drinfeld bases of level p^n on E and E' respectively.

Let "square brackets" [...] denote the point on $X_1(ap^n)_{/k'}$ determined by such a triple.

Proposition 1. *Suppose that the points* $[E, e_a, (t_1, t_2)]$ *and* $[E', e'_a, (t'_1, t'_2)]$ *lie on the same irreducible component of* $X_1(ap^n)_{/k'}$ *of exponent* j *and invariant* d. *Suppose further that* $j > 0$. *Then the divisor*

$$D_1 = p^{n-j} \cdot [E, e_a, (t_1, t_2)] - p^{n-j} \cdot [E', e'_a, (t'_1, t'_2)]$$

is congruent to

$$D_2 = \sum_{r=0}^{p^{n-j}-1} ([E, e_a, (t_1 + rt_2, 0)] - [E', e'_a, (t'_1 + rt'_2, 0)]).$$

Proof. If $j = n$, then $t_2 = t'_2 = 0$ and there is nothing to prove. Thus we may assume that $n \geqq 2$. We proceed by induction, and suppose that $0 < j < n$. By the discussion above we see that $\pi^* \pi_* [E, e_a, (t_1, t_2)] = p \cdot [E, e_a, (t_1, t_2)]$ and consequently

$$D_1 = p^{n-j-1} \cdot \pi^* (\pi_* [E, e_a, (t_1, t_2)] - \pi_* [E', e'_a, (t'_1, t'_2)]).$$

Moreover,

$$D_2 = \pi^* \pi_* \sum_{r=0}^{p^{n-j-1}-1} ([E, e_a, (t_1 + rt_2, 0)] - [E', e'_a, (t'_1 + rt'_2, 0)]).$$

One easily sees, by considering diagram (*), and the two equalities above, that the proposition will follow if

$$p^{n-j-1} \rho_* \circ \pi_* ([E, e_a, (t_1, t_2)] - [E', e'_a, (t'_1, t'_2)])$$

is congruent to

$$\rho_* \circ \pi_* \sum_{r=0}^{p^{n-j-1}-1} ([E, e_a, (t_1 + rt_2, 0)] - [E', e'_a, (t'_1 + rt'_2, 0)]).$$

Since $\rho_* \circ \pi_*$ is just the mapping induced from the natural projection of $X_1(ap^n)_{/K'_\lambda}$ onto $X_1(ap^{n-1})_{/K'_\lambda}$ the desired congruence holds by our inductive hypothesis, and Proposition 1 of §8 of Chap. 2.

Consider the natural projection

$$\text{proj:} \quad X_1(ap^n)_{/k} \to X_1(a)_{/k}$$

and denote by p_j its restriction to the part of the domain which is of exponent j:

$$p_j: \quad (X_1(ap^n)_{/k})_j \to X_1(a)_{/k}.$$

In particular, setting $j=0$ and $j=n$, we obtain mappings

$$p_0: \quad \tilde{\Sigma}_n^{\text{ét}} \to X_1(a)_{/k}$$

$$p_n: \quad \tilde{\Sigma}_n^{\mu} \to X_1(a)_{/k}.$$

Define homomorphisms

$$c_1: \quad \text{Pic}^0 \tilde{\Sigma}_n^{\text{ét}} \to \text{Pic}^0 \tilde{\Sigma}_n^{\mu}, \qquad c_2: \quad \text{Pic}^0 \tilde{\Sigma}_n^{\mu} \to \text{Pic}^0 \tilde{\Sigma}_n^{\text{ét}}$$

by $c_1 = p_n^* \cdot p_{0*}$, $c_2 = p_0^* \cdot p_{n*}$.

Proposition 2. *The following diagrams with* u and U_{p*} or with u' and U_p^* are commutative:

$$\begin{array}{ccc} \text{Pic}^0 \tilde{\Sigma}_n^{\text{ét}} \times \text{Pic}^0 \tilde{\Sigma}_n^{\mu} & \xrightarrow{\sigma} & A_n \\ \Big\downarrow{\scriptstyle u'} \quad \Big\downarrow{\scriptstyle u} & & \Big\downarrow{\scriptstyle av(U_p^*)} \quad \Big\downarrow{\scriptstyle av(U_{p*})} \\ \text{Pic}^0 \tilde{\Sigma}_n^{\text{ét}} \times \text{Pic}^0 \tilde{\Sigma}_n^{\mu} & \xrightarrow{\sigma} & A_n \end{array}$$

where

$$u(x, y) = (Fx, c_1(x) + \langle n_p \rangle Vy)$$

$$u'(x, y) = (\langle n_p \rangle^{-1} c_2(y) + Vx, \langle n_p \rangle^{-1} Fy).$$

Here n_p is any integer $\equiv 1 \bmod p^n$ and $\equiv p \bmod a$, and F and V are the Frobenius and Verschiebung endomorphisms.

Proof. Set $U_p = U_{p*}$. We must check that $U_p \cdot (0, y) = (0, \langle n_p \rangle Vy)$ and that $U_p \cdot (x, 0) = (Fx, c_1(x))$. The first formula is immediate from Proposition 2 of Chap. 2, §9.

As for the second formula, it suffices to check that

$$p^{n-1} \cdot av(U_p) \cdot (x, 0) = p^{n-1}(Fx, c_1(x)). \qquad (*)$$

To prove this one uses the formula for U_p given in the proof of Proposition 1 of Chap 2, §9,

$$U_p x = \sum_{r=0}^{p-1} (E/C(r), t_1(r), t_2(r))$$

for x a divisor of $X_1(ap^n)_{/k'}$ corresponding to a triple (E, t_1, t_2) with (t_1, t_2) a Drinfeld basis of order ap^n. Let us separate the $r=0$ term from the rest. In the notation of the proof of Proposition 1 of Chap. 2, § 9,

$$U_p x = \beta_0 \mathscr{F}e + \sum_{r=1}^{p-1} (E/C(r), t_1(r), t_2(r))$$

where for $r=1, \cdots, p-1$, $E/C(r)$ may be identified with the image of $E_{/k'}$ under Verschiebung, and $(E/C(r), t_1(r), t_2(r))$ represents a point of $X_1(N)_{/k}$ which lies on an irreducible component of exponent 1. Applying p^{n-1} to both sides and using Proposition 1 for the terms where $r \neq 0$, one gets $(*)$ by virtue of the criterion of compatibility (Proposition 2 of Chap. 2, § 1).

The proof for U_p' is similar and we omit the details.

If Γ is a p-divisible group and ρ is an endomorphism of Γ, let Γ_ρ denote the p-divisible subgroup defined by:

$$\Gamma_\rho = \bigcup_{\nu=1}^{\infty} \Gamma[\rho^\nu]$$

(the *ρ-nilpotent part of Γ*).

We apply this to the p-divisible group

$$\Gamma = \mathrm{Pic}^0(\tilde{\Sigma}_n^{\text{ét}})_{p/k} \times \mathrm{Pic}^0(\tilde{\Sigma}_n^{\mu})_{p/k}$$

and to $\rho = u-1$.

Let $\Gamma' = \mathrm{Pic}^0(\tilde{\Sigma}_n^{\text{ét}})_{p/k}$, and $\Gamma'' = \mathrm{Pic}^0(\tilde{\Sigma}_n^{\mu})_{p/k}$ so that

$$\Gamma = \Gamma' \times \Gamma''. \tag{2}$$

Let $\tilde{V} = \langle n_p \rangle V$.

Proposition 3. *There is an isomorphism of p-divisible group schemes*

$$\Gamma_{u-1} \xrightarrow[\cong]{\eta} \Gamma'_{F-1} \times \Gamma''_{\tilde{V}-1}$$

(to be described below). The group scheme Γ_{u-1} is ordinary.

Proof. Since Γ'_{F-1} is étale, and $\Gamma''_{\tilde{V}-1}$ is of multiplicative type, the fact that Γ_{u-1} is ordinary follows from the existence of η. The isomorphism η is **not** compatible with the product decomposition (2). A precise description of η is given as follows.

If the *subscripts* ét and 0 refer to the étale and connected parts of a p-divisible group over k, we may consider the four-fold product decomposition

$$\Gamma = \Gamma'_{\text{ét}} \times \Gamma'_0 \times \Gamma''_{\text{ét}} \times \Gamma''_0. \tag{3}$$

Now if T is any k-scheme and $\xi = (x, y, z, w) \in \Gamma(T)$ is any T-valued point of Γ, described by the four coordinates obtained from (3), then $\xi = (x, y, z, w) \in \Gamma_{u-1}(T)$ if and only if ξ is annihilated by $(u-1)^a$ for some a, or equivalently (using the formula of Proposition 2) if and only if

(**1**) $(F-1)^a x = 0.$

(**2**) $y = 0.$

(**3**) $(\tilde{V}-1)^a z + \sum_0^{a-1} (\tilde{V}-1)^{a-k-1} \cdot (F-1)^k c_1(x) = 0.$

(**4**) $(\tilde{V}-1)^a w = 0.$

Here we have used that $(\Gamma_0')_{F-1} = 0$ to obtain (**2**), and (**2**) gives (**4**).

Now note that $\tilde{V}-1$ is an invertible endomorphism of $\Gamma_{\text{ét}}''$ so that we may deduce that

$$z = -\sum_0^{a-1} (\tilde{V}-1)^{-k-1}(F-1)^k c_1(x)$$

from formula (**3**).

The mapping

$$\eta^{-1}: \ \Gamma'_{F-1} \times \Gamma''_{\tilde{V}-1} \to \{\Gamma'_{\text{ét}} \times \Gamma'_0 \times \Gamma''_{\text{ét}} \times \Gamma''_0\}_{u-1}$$

is then defined by the rule that it take the T-valued point (x, w) to

$$(x, 0, -\sum_0^{\infty} (\tilde{V}-1)^{-k-1}(F-1)^k c_1(x), w).$$

Corollary 1. There is a commutative diagram

$$\begin{array}{ccc} \Gamma_{u-1} & \xrightarrow{\eta} & \Gamma'_{F-1} \times \Gamma''_{\tilde{V}-1} \\ \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle F \times \tilde{V}} \\ \Gamma_{u-1} & \xrightarrow{\eta} & \Gamma'_{F-1} \times \Gamma''_{\tilde{V}-1} \end{array}$$

A similar argument yields

Corollary 1′. *There is a commutative diagram*

$$\begin{array}{ccc} \Gamma_{u'-1} & \xrightarrow{\eta'} & \Gamma'_{V-1} \times \Gamma''_{\tilde{F}-1} \\ \downarrow{\scriptstyle u'} & & \downarrow{\scriptstyle V \times \tilde{F}} \\ \Gamma_{u'-1} & \xrightarrow{\eta'} & \Gamma'_{V-1} \times \Gamma''_{\tilde{F}-1} \end{array}$$

where $\tilde{F} = \langle n_p \rangle^{-1} F$.

Proposition 4. (“*q-expansion principle*” *for the étale part of* $\Gamma_{u'-1}$).

Let χ: $(\mathbf{Z}/N\mathbf{Z})^* \to \overline{\mathbf{F}}_p^*$ *be an even character and* c *a function from the set of rational primes, excluding* p, *to* $\overline{\mathbf{F}}_p$.

Let $V' = \Gamma_{u'-1}(\overline{\mathbf{F}}_p)[p]$ be the $\overline{\mathbf{F}}_p$*-valued points of order* p *in the* p*-divisible group* $\Gamma_{u'-1}$.

Let

$$(V' \otimes \overline{\mathbf{F}}_p)^{\chi, c} \subset V' \otimes \overline{\mathbf{F}}_p$$

denote the subspace of eigenvectors for the operators $\{t_l^*, u_q^* (q \neq p); \langle r\rangle^*\}$ *with eigenvalues given by* χ *and* c. *Explicitly*

$$\langle r\rangle^* x = \chi(r) \cdot x; \quad t_l^* x = c_l \cdot x; \quad u_q^* x = c_q \cdot x.$$

Then $(V' \otimes \overline{\mathbf{F}}_p)^{\chi, c}$ *is of dimension* $\leqq 1$ *over* $\overline{\mathbf{F}}_p$.

Proof. By Corollary 1′,

$$\Gamma_{u'-1}(\overline{\mathbf{F}}_p) = \Gamma^{\text{ét}}_{u'-1}(\overline{\mathbf{F}}_p) \cong \Gamma^{\mu}_{F-1}(\overline{\mathbf{F}}_p).$$

Now apply Proposition 2 of § 10 of Chap. 2.

We have the analogous:

Proposition 4′ (*q-expansion principle for the étale part of* Γ_{u-1}).
With notation as in Proposition 4, let V *denote* $\Gamma_{u-1}(\overline{\mathbf{F}}_p)[p]$ *and let*

$$(V \otimes \overline{\mathbf{F}}_p)^{\chi, c} \subset V \otimes \overline{\mathbf{F}}_p$$

denote the subspace of eigenvectors for the operators $\{t_{l^*}, u_{q^*}(q \neq p); \langle r\rangle_*\}$ *given by* χ *and* c.

Explicitly,

$$\langle r\rangle_* \cdot x = \chi(r) \cdot x; \quad t_{l^*} x = c_l \cdot x; \quad u_{q^*} x = c_q \cdot x.$$

Then $(V \otimes \overline{\mathbf{F}}_p)^{\chi, c}$ *is of dimension* $\leqq 1$ *over* $\overline{\mathbf{F}}_p$.

Proof. This may be proved in a manner similar to Proposition 4.

§ 4. Properties of $\mathbf{T}_i$ *and* Y_i

We begin by defining the Hecke ring as a ring of endomorphisms of $A = A_n$. We assume that $N = ap^n$ with $n \geqq 1$ and $(a, p) = 1$.

Definition. *Let* $\mathbf{T}$ *be the subring of endomorphisms of* $A_{/\mathbf{Q}}$ *generated over* $\mathbf{Z}$ *by the set*

$$\{T_l \text{ for } l \nmid N,\ U_{q*} \text{ for } q \mid N, \langle r\rangle \text{ for } r \in (\mathbf{Z}/N\mathbf{Z})^*/(\pm 1)\}.$$

The ring $\mathbf{T}$ is free of finite rank as a module over $\mathbf{Z}$, and is commutative.

There is a natural map (not injective) of the group ring $\mathbf{Z}[(\mathbf{Z}/N\mathbf{Z})^*]$ to $\mathbf{T}$ given by $[\delta] \to \langle\delta\rangle$. Letting $\mathbf{T}_p = \mathbf{T} \otimes \mathbf{Z}_p$ we have an induced map from $R = \mathbf{Z}_p[(\mathbf{Z}/N\mathbf{Z})^*]$ to $\mathbf{T}_p$. The ring $\mathbf{T}_p$ is a complete semi-local ring so we may write

$$\mathbf{T}_p = \prod_{i \in I} \mathbf{T}_i$$

where each $\mathbf{T}_i$ is a complete local ring. The inverse image of each $\mathbf{T}_i$ under the map from R is one of the rings $R_{\mathfrak{m}}$ in the corresponding decomposition of R (see Chap. 1, § 3), and then we may view $\mathbf{T}_i$ as $R_{\mathfrak{m}}$-algebra. We say that $\mathbf{T}_i$ is primitive if the corresponding component of R is primitive. More generally, we associate to $\mathbf{T}_i$ any of the list of objects associated to a component of R (cf. Chap. 1, § 3), in particular, a $\mathbf{Q}_p$-conjugacy class of $\overline{\mathbf{Q}}_p$-valued characters.

Let $Ta_p(A)(\bar{\mathbf{Q}}) = \mathrm{Hom}(\mathbf{Q}_p/\mathbf{Z}_p, A_p(\bar{\mathbf{Q}}))$ be the p-adic Tate module of A. It is a module both for $\mathbf{T}_p$ and for $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. The aim of this section is to prove the following results about Y_i where

$$Y_i = Ta_p(A)(\bar{\mathbf{Q}}) \underset{\mathbf{T}_p}{\otimes} \mathbf{T}_i$$

is associated to a *primitive* $\mathbf{T}_i$.

Proposition 1. *If* $\mathbf{T}_i$ *is primitive, then* $\mathbf{T}_i \otimes \mathbf{Q}$ *is a product of fields.*

Proposition 2. *If* $\mathbf{T}_i$ *is primitive, then* $Y_i \otimes \mathbf{Q}$ *is free of rank* 2 *over* $\mathbf{T}_i \otimes \mathbf{Q}$.

Before proving these propositions we will prove a lemma which will be useful in understanding the $\mathfrak{m}$-divisible group of A. We introduce an abelian variety quotient A' of A which is defined as follows. Using the decomposition (cf. Chap. 1, § 3, formula 2)

$$(\mathbf{Z}/ap^n\mathbf{Z})^* \cong (\mathbf{Z}/ap\mathbf{Z})^* \times \Gamma/\Gamma_n$$

we consider the set S of subgroups H of $(\mathbf{Z}/ap^n\mathbf{Z})^*$ such that the intersection with $(\mathbf{Z}/ap\mathbf{Z})^*$ contains the kernel of the map $(\mathbf{Z}/ap\mathbf{Z})^* \to (\mathbf{Z}/r\mathbf{Z})^*$ for some $r \mid ap$, $r < ap$. Then let $J_1(ap^n)^*$ be the algebraic subgroup given by

$$J_1(ap^n)^* = \sum_{H \subseteq S} J_1(ap^n)^H,$$

where superscript H denotes the intersection of the fixed part under the action of $\langle h \rangle$ for all $h \in H$. Then define A' by the exact sequence

$$(\mathscr{K}_n + J_1(ap^n)^*) \to J_1(ap^n) \to A' \to 0.$$

Since A is the quotient of $J_1(ap^n)$ by the image of $\mathscr{K}_n$ there is a natural surjective map $A \to A'$. We note that the cotangent space of A', when identified with a space of cusp forms of level ap^n, contains only forms of *primitive nebentypus* (in the sense of Hijikata) of level ap^i, $1 \leqq i \leqq n$. Recall that a form has primitive nebentypus of level M if it is of level M and its nebentypus character has conductor M.

This will be made more precise in Lemma 4.

The Hecke operators $\{T_l$ for $l \nmid ap$, U_q for $q \mid ap$, $\langle r \rangle$ for $r \in (\mathbf{Z}/ap^n\mathbf{Z})^*/(\pm 1)\}$ all induce endomorphisms of $J_1(ap^n)$, and these all commute with the action of $(\mathbf{Z}/ap^n\mathbf{Z})^*$ on $J_1(ap^n)$. Hence $J_1(ap^n)^*$ is preserved by all these operators. The same being true for K_n (cf. § 1) we get an induced action on A' and we define $\mathbf{T}'$ to be the ring of endomorphisms which they generate, i.e.,

$$\mathbf{T}' = \{T_l \text{ for } l \nmid ap, U_{q*} \text{ for } q \mid ap, \langle r \rangle \text{ for } r \in (\mathbf{Z}/ap^n\mathbf{Z})^*/(\pm 1)\} \subseteq \mathrm{End}(A').$$

There is clearly a natural map $\mathbf{T} \to \mathbf{T}'$. We may consider both $\mathbf{T}$ and $\mathbf{T}'$ as $(\mathbf{Z}/ap^n\mathbf{Z})^*$-modules via the natural map $r \to \langle r \rangle$ and so also $\mathbf{T}_p$ and $\mathbf{T}'_p$ as R-modules. For a component $\mathfrak{m}$ of R (cf. Chap. 1, § 3) we set $\mathbf{T}_\mathfrak{m} = \mathbf{T}_p \otimes R_\mathfrak{m}$ and $\mathbf{T}'_\mathfrak{m} = \mathbf{T}'_p \otimes R_\mathfrak{m}$. Let $A_\mathfrak{m}$ and $A'_\mathfrak{m}$ be the $\mathfrak{m}$-divisible groups on A and A', i.e., $A_\mathfrak{m} = \varinjlim A[p^n](\bar{\mathbf{Q}}) \otimes R_\mathfrak{m}$ etc.

Lemma 3. *Let* $\mathfrak{m}$ *be a primitive component of* R. *Then the natural map* $A \to A'$ *induces an isomorphism* $A_{\mathfrak{m}} \xrightarrow{\sim} A'_{\mathfrak{m}}$. *Also the map* $\mathbf{T} \to \mathbf{T}'$ *induces an isomorphism* $\mathbf{T}_{\mathfrak{m}} \xrightarrow{\sim} \mathbf{T}'_{\mathfrak{m}}$.

Proof. Since $\mathfrak{m}$ is primitive $(J_1(ap^n)^*_{\mathfrak{m}} = 0$. This follows easily from the fact that all the characters associated to $\mathfrak{m}$ are of conductor divisible by ap. Hence from the sequence

$$J_1(ap^n)^*/J_1(ap^n)^* \cap K_n \to A \to A' \to 0$$

we deduce that $A_{\mathfrak{m}} \xrightarrow{\sim} A'_{\mathfrak{m}}$ (first taking ker p^∞ and then tensoring with $\mathfrak{m}$, both operations being exact).

To prove the second part note first that if X is an abelian variety, X_p its associated p-divisible group, and S a commutative subring of $\mathrm{End}(X)$, then $S \otimes \mathbf{Z}_p \hookrightarrow \mathrm{End}(X_p)$. Consider then the ring $\mathbf{T}_p$ acting on A_p. Since $\mathbf{T}_p$ commutes with the diamond operators it preserves each factor $A_{\mathfrak{m}}$ in the decomposition $A_p \otimes R = \prod A_{\mathfrak{m}}$. The map $\mathbf{T}_p \to \mathrm{End}(A_{\mathfrak{m}})$ induces an injection

$$\mathbf{T}_{\mathfrak{m}} = \mathbf{T}_p \otimes R_{\mathfrak{m}} \to \mathrm{End}(A_{\mathfrak{m}}).$$

Similarly there is an injection $\mathbf{T}'_{\mathfrak{m}} \to \mathrm{End}(A'_{\mathfrak{m}})$, and using that $A_{\mathfrak{m}} \xrightarrow{\sim} A'_{\mathfrak{m}}$ we have a diagram

$$\begin{array}{ccc} \mathbf{T}_{\mathfrak{m}} & \to & \mathrm{End}(A_{\mathfrak{m}}) \\ \downarrow & & \downarrow \cong \\ \mathbf{T}'_{\mathfrak{m}} & \to & \mathrm{End}(A'_{\mathfrak{m}}). \end{array}$$

This proves that the map $\mathbf{T}_{\mathfrak{m}} \to \mathbf{T}'_{\mathfrak{m}}$, which is obviously surjective, is also injective.

Now let $\mathbf{T}_i$ be a primitive factor of $\mathbf{T}_p$. Then $\mathbf{T}_i$ is a direct factor of $\mathbf{T}_{\mathfrak{m}}$ for some primitive component $\mathfrak{m}$. Similarly there is a factor A_i of $A_{\mathfrak{m}}$ corresponding to $\mathbf{T}_i$. We define A'_i and $\mathbf{T}'_i$ to be the images of A_i and $\mathbf{T}_i$ under the isomorphisms of Lemma 3. To prove the two propositions stated earlier in this section it will be sufficient to prove the analogous results for A'. That this is a simplification is due to the following lemma. Recall that X_f is the abelian variety associated by Shimura to a newform f, and that if it is of level M we may assume that X_f is given (uniquely) as an abelian subvariety of $J_1(M)$. Furthermore, Shimura has shown that the image of $\{T_l \text{ for } l \nmid M, \langle r \rangle \text{ for } r \in (\mathbf{Z}/M\mathbf{Z})^*\}$ generate over $\mathbf{Q}$ a field $K_f \subseteq \mathrm{End}(X_f) \otimes \mathbf{Q}$ such that $[K_f : \mathbf{Q}] = \dim X_f$. If $M \mid N$ we may consider the composite map with finite kernel

$$X_f \longrightarrow J_1(M) \xrightarrow{(\pi_{N/M})^*} J_1(N).$$

The image of X_f in $J_1(N)$ is again stable under $\{T_l \text{ for } l \nmid N, \langle r \rangle \text{ for } r \in (\mathbf{Z}/N\mathbf{Z})^*\}$. In particular, the group of diamond operators acts through its natural quotient by the subgroup $\{\langle a \rangle : a \equiv 1 \bmod M\}$.

Lemma 4. *There is an isogeny over* $\mathbf{Q}$

$$\prod X_f \sim A'$$

where the product is taken over those distinct X_f belonging to newforms f of level ap^i for $1 \leqq i \leqq n$ whose associated character is also primitive of conductor ap^i. The isogeny may be chosen to respect the action of all the operators in the set $\{T_l$ for $l \nmid N, \langle r\rangle$ for $r \in (\mathbf{Z}/N\mathbf{Z})^*\}$.

Passing to the quotient by $J_1(ap^n)^*$ has the effect of removing all forms from the cotangent space of $J_1(N)$ which are not both new of some level ap^i $(1 \leqq i \leqq n)$ and also having nebentypus character of conductor divisible by a. Dividing out by the image of $\mathscr{H}_n$ then ensures that, in the quotient, each such form is represented only once and its nebentypus character has conductor equal to its level ap^i. We note that the isogeny we have chosen is obtained by taking for each f the composition $X_f \to J_1(N) \to A'$.

We now turn to the proof of the two propositions. The mapping $\prod X_f \to A'$ induces a mapping of endomorphism rings,

$$\prod K_f \hookrightarrow \mathrm{End}(A') \otimes \mathbf{Q}.$$

Since each element of $\mathbf{T}'$ preserves the image of X_f for each f (as follows from the theorem of multiplicity one and the fact that $\mathbf{T}'$ is commutative), hence we have that $\prod K_f \xrightarrow{\sim} \mathbf{T}' \otimes \mathbf{Q}$. This proves Proposition 1.

To prove Proposition 2, note that there is a canonical decomposition of $\mathbf{Q}$-algebras

$$\mathbf{Q}[(\mathbf{Z}/N\mathbf{Z})^*] \cong \textit{Prim. Comps.} \times \textit{Imprim. Comps.}$$

having the property that any character χ on $(\mathbf{Z}/N\mathbf{Z})^*$ belongs to a primitive component $\mathfrak{m}$ if and only if the associated homomorphism is induced by a homomorphism on the first factor.

We have already established that the cotangent space of A' over $\mathbf{C}$, which is a $\mathbf{C}[(\mathbf{Z}/N\mathbf{Z})^*]$-module via the diamond operators, is a $\mathbf{C} \otimes$ *Prim. Comps.* module of rank 1. It then follows by an application of a standard duality theorem that $T_p(A') \otimes \mathbf{Q}_p$ is a $\mathbf{Q}_p \otimes$ *Prim. Comps.* module of rank 2.

§ 5. The pseudo-primitive case

Here we give the analogues of Proposition 1 and 2 of § 4 in the general pseudo-primitive case. Recall that in the proof of Proposition 1 we constructed an abelian variety A' for which the cotangent space contained only forms of primitive nebentypus of level ap^i for some i with $1 \leqq i \leqq n$. We adapt this construction to the present case as follows. Assume that we have fixed a pseudo-primitive component $\mathfrak{m}$ whose basic character χ has conductor $(ap/q_1 \ldots q_\nu)$ (cf. Chap. 1, § 3). Then consider the set S of subgroups H of $(\mathbf{Z}/ap^n\mathbf{Z})^*$ such that their intersection with $(\mathbf{Z}/ap\mathbf{Z})^*$ contains the kernel of $(\mathbf{Z}/ap\mathbf{Z})^* \to (\mathbf{Z}/r\mathbf{Z})^*$ for some $r \mid (ap/q_1 \ldots q_\nu)$, $r < (ap/q_1 \ldots q_\nu)$. Now define $J_1(ap^n)^*$ by

$$J_1(ap^n)^* = \sum_{H \in S} J_1(ap^n)^H$$

and let A' be given by the exact sequence

$$(\mathscr{K}_n + J_1(ap^n)^*) \to J_1(ap^n) \to A' \to 0\,.$$

As before, A' is naturally a quotient of A on which all the standard Hecke operators $(\{T_l, U_q, \langle r\rangle\})$ act.

The cotangent of A' may be identified with a subspace spanned by forms of level ap^n which come from forms of primitive nebentypus of level divisible by $(ap^i/q_1 \ldots q_v)$ for some $i \geqq 1$. The Hecke operators $\{T_l$ (for $l \nmid N$), U_q (for $q \mid N$), $\langle r\rangle\}$ generate a ring of endomorphisms $\mathbf{T}'$ of A'. As in § 4 it will be sufficient to prove a structure theorem for $\mathbf{T}' \otimes \mathbf{Q}$ and for the cotangent space of A' as a module over this ring. Actually we will show that the cotangent space of A' is free of rank one over $\mathbf{T}' \otimes \mathbf{Q}$. This will give the following versions of Propositions 1 and 2 of § 4.

Proposition 1. *Let* $\mathfrak{m}$ *be a pseudo-primitive component. Then* $\mathbf{T}_{\mathfrak{m}} \otimes \mathbf{Q}$ *is a product of fields and of* $\mathbf{Q}$*-algebras of the form* $K[x_1, \ldots, x_r]/(x_1^2, \ldots, x_r^2)$ *where* K *is a field.*

Proposition 2. $Y_{\mathfrak{m}} \otimes \mathbf{Q}$ *is free of rank 2 over* $\mathbf{T}_{\mathfrak{m}} \otimes \mathbf{Q}$ *where*

$$Y_{\mathfrak{m}} = Ta_p(A) \bigotimes_{\mathbf{T}} \mathbf{T}_{\mathfrak{m}}$$

is the $\mathfrak{m}$*-adic Tate-module.*

Proof. Let $S_2(\Gamma)$ denote the complex vector space of cusp forms of weight 2 for a subgroup $\Gamma \subseteq PSL_2(\mathbf{Z})$. We consider the two maps

$$\pi_1(d)\colon \quad S_2(\Gamma_1(ap^n/d)) \to S_2(\Gamma_1(ap^n))$$
$$\pi_2(d)\colon \quad S_2(\Gamma_1(ap^n)/d) \to S_2(\Gamma_1(ap^n))$$

given by

$$\pi_1(d)\,(\textstyle\sum a_n q^n) = \sum a_n q^n$$
$$\pi_2(d)\,(\textstyle\sum a_n q^n) = \sum a_n q^{nd}.$$

The maps commute with T_{l*} for $l \nmid N$ and with U_{q*} for $q \nmid d$. By the theory of Atkin and Lehner (but for $\Gamma_1(N)$ as in [40], Chap. VIII) there is a basis of cusp forms of $S_2(\Gamma_1(ap^n))$ of the form

$$\{\pi_1(d)\,\pi_2(d')\,f\colon \quad dd' = ap^n, \quad f \text{ a newform of level } ap^n/dd'\}\,. \tag{1}$$

Suppose that f is a newform of level ap^i/r. If $p \mid r$ then assume that $i = 1$. Then let $\Omega(f)$ denote the space generated by

$$\{\pi_1(d)\,\pi_2(d')\,f\colon \quad dd' = r\}\,.$$

We may identify the cotangent space of A' with $\sum_f \Omega(f)$ where f runs over the newforms f of level ap^i/r with $r \mid q_1 \ldots q_v$ and $1 \leqq i \leqq n$, with the restriction that $i = 1$ if $p \mid r$. Moreover, on each space $\Omega(f)$ the action of the operators $\{T_{l*}, \langle\ \rangle\}$ is via a field K_f.

All of the standard Hecke operators preserve $\Omega(f)$. For $q=q_i$, $q_i \nmid r$ and $q_i | N$, we find that $U_{q_i} | \Omega(f) \in \mathrm{K}_f$ since it commutes with each $\pi_i(d)$ for $d|r$. We now compute the minimal polynomial of U_{q_i} on $\Omega(f)$ when $q_i | r$. Let $f=\sum a_n q^n$. Then we have that f is an eigenform for T_{q_i} since $q_i \| ap^n$ and $q_i | r$, i.e., f has level prime to q_i. So $T_{q_i} f = \alpha_{q_i} f$ for some α_{q_i}. Thus

$$\alpha_{q_i} f = T_{q_i} f = U_{q_i}(\pi_1(q_i) f) + \varepsilon(q_i) q_i (\pi_2(q_i) f) \tag{2}$$

where ε is the nebentypus character of f. We also have the relation

$$U_{q_i}(\pi_2(q_i) f) = \pi_1(q_i) f. \tag{3}$$

Since U_{q_i} commutes with $\pi_\alpha(q_j)$ for $\alpha = 1,2$ and any $j \neq i$ we see that the decomposition

$$\Omega(f) = \bigoplus_{dd' | (r/q_i)} \{\pi_1(q_i) \cdot \pi_1(d) \pi_2(d') f + \pi_2(q_i) \cdot \pi_1(d) \pi_2(d') f\}$$

is respected by U_{q_i}. By formulas (2) and (3) we see that the minimal polynomial of U_{q_i} is $f_i(x) = (x^2 - \alpha_{q_i} \cdot x + \varepsilon(q_i) q_i)$. (It cannot strictly divide this since U_{q_i} would then be a scalar – but it does not preserve $\pi_2(r) f$, for example).

We now consider the linear map of K_f-vector spaces

$$\mathfrak{E}_f = K_f(x_1, \ldots, x_v)/(f_1(x_1), \ldots, f_v(x_v)) \to \Omega(f)$$

given by $p(x_1, \ldots, x_v) \mapsto p(U_{q_1}, \ldots, U_{q_v}) \cdot \pi_2(r) \cdot f$. This map is surjective and hence by counting dimensions, it is an isomorphism. Thus the subring of $\mathrm{End}(\Omega(f))$ generated by the Hecke operators $\{T_{l^*}, U_{q^*}$ (for $q|N$), $\langle r \rangle' s\}$ is a **Q**-algebra $K_f[U_{q_1}, \ldots, U_{q_v}]$ isomorphic to $\mathfrak{E}_f$. Furthermore, we see that $\Omega(f)$ is free of rank one, a generator being $\pi_2(r) f$.

The proof of Proposition 2 is parallel to that of Proposition 2 of § 4. Here we must note that there is a canonical direct product decomposition of the **Q**-algebra $\mathbf{Q}[(\mathbf{Z}/N\mathbf{Z})^*]$ into two factors, one corresponding to pseudo-primitive components, and the other to the remaining components.

Remark. We note that $\mathbf{T}_\mathfrak{m} \otimes \mathbf{Q}$ will actually be a product of fields unless $\alpha_{q_i} = 2\sqrt{\varepsilon(q_i) q_i}$ for some q_i.

§ 6. *A study of* $A^{\text{ét}}_{n|k}$

We are grateful to Ofer Gabber for explaining to us some results of his concerning the geometry of the mapping

$$\mathrm{Pic}^0(X_{/S}) \to \mathrm{Pic}^0(Y_{/S})$$

induced by finite morphisms of S-schemes $Y \to X$, which satisfy certain properties. We have attempted, in this section, to specialize some of Gabber's ideas to the specific context in which we work; the results whose proofs we present in this section are much weaker than those that he can establish.

Let $\mathfrak{m}$ be a component, and consider $A_{n,\mathfrak{m},U_p-1}$, the (U_p-1)-divisible subgroup scheme in $A_{n,\mathfrak{m}}$.

Proposition 1. *The natural mapping*

$$A_{n-1,\mathfrak{m},U_p-1}(\bar{k}) \to A_{n,\mathfrak{m},U_p-1}(\bar{k})$$

is injective for $n \geqq 2$.

Recall that $A_{n,\mathfrak{m},U_p-1}$ is an ordinary group scheme, as follows from the Proposition of § 3, and Proposition 3 of § 5. In fact, using the notation of § 5, we have an isogeny

$$\Gamma'_{\mathfrak{m},F-1} \times \Gamma''_{\mathfrak{m},\tilde{r}-1} \cong \Gamma_{\mathfrak{m},u-1} \xrightarrow{\sigma} A_{n,\mathfrak{m},U_p-1/k}$$

and since $\Gamma''_{\mathfrak{m},\tilde{r}-1}$ is a multiplicative-type group scheme, when we pass to $\bar{k}$-rational points, we have

Lemma 1. *The natural map induced by* σ *yields an isogeny*:

$$\sigma_1: \quad \mathrm{Pic}^0(\tilde{\Sigma}_n^{\text{ét}})_{\mathfrak{m},F-1}(\bar{k}) \to A_{n,\mathfrak{m},U_p-1}(\bar{k}),$$

and the zero-mapping:

$$\sigma_2: \quad \mathrm{Pic}^0(\tilde{\Sigma}_n^{\mu})_{\mathfrak{m}}(\bar{k}) \to A_{n,\mathfrak{m},U_p-1}(\bar{k}).$$

To prove Proposition 1, we let χ be a basic character attached to $\mathfrak{m}$ and write $\chi = \chi_{p'}\omega^k$ where $\chi_{p'}$ is a character of conductor prime to p, ω is the Teichmüller character, and $0 \leqq k < p-1$.

We have separate arguments for Proposition 1 in these two cases:

Case 1. *The greatest common divisor of* k *and* $p-1$ *is* >1.
Case 2. $k > 0$.

The reader should note that when χ is a power of the Teichmüller character, we are in case 1, and the proof of Proposition 1 (in this case) is quite easy.

Proof in Case 1. Using the notation of § 2 of Chap. 3, $A_{n,\mathfrak{m}}$ achieves good reduction over $\mathcal{O}_{n,\mathfrak{m}}$ whose field of fractions is the subfield of $\mathbf{Q}_p(\zeta_{p^n})$ which is of degree $\dfrac{p-1}{d}p^{n-1}$, where $d=(p-1,k)$.

The morphism

$$A_{n-1,\mathfrak{m},U_p-1/\mathbf{Z}_p[\zeta_{p^n}]} \to A_{n,\mathfrak{m},U_p-1/\mathbf{Z}_p[\zeta_{p^n}]}$$

comes by base change from a morphism of p-divisible groups

$$A_{n-1,\mathfrak{m},U_p-1/\mathcal{O}_{n,\mathfrak{m}}} \to A_{n,\mathfrak{m},U_p-1/\mathcal{O}_{n,\mathfrak{m}}}$$

which are ordinary, since their "base changes" to $\mathbf{Z}_p[\zeta_{p^n}]$ are.

The proposition of chapter zero then applies (since $d>1$) to give injectivity of

$$A_{n-1,\mathfrak{m},U_p-1/k} \to A_{n,\mathfrak{m},U_p-1/k}$$

and case 1 is proved.

Proof in Case 2. Set $\overline{K}=\overline{\mathbf{Q}}_p$, an algebraic closure of $\mathbf{Q}_p$, $\overline{\mathcal{O}}\subseteq\overline{K}$ the ring of integers with $\bar{k}$ its residue field.

Let $\zeta_{p^n}\in\overline{K}$ be a primitive p^n-th root of 1, and set $S_n=\operatorname{Spec}\mathbf{Z}_p[\zeta_{p^n}]$.

We "simplify" our standard notation of Chap. 2 by setting

$$X_n=X_1(ap^n)_{/S_n},$$
$$Y_{n-1}=X_1(ap^n,ap^{n-1})_{/S_n},$$

so that the standard diagram (§3) is:

$$X_n\xrightarrow[\pi]{}Y_{n-1}\xrightarrow[\rho]{}X_{n-1}\times_{S_{n-1}}S_n \tag{1}$$

where π identifies Y_{n-1} with the quotient of X_n by the cyclic group of order p, G_n.

Let $\sigma\in(\mathbf{Z}/p^n\mathbf{Z})^*/(\pm 1)$ be an element of order $(p-1)/2$. We view σ as acting on X_n via the diamond operator $\langle\sigma\rangle$.

Let the superscript # denote "minimal regular resolution"; thus $X_n^{\#}$ and $Y_{n-1}^{\#}$ are obtained from X_n and Y_{n-1} by successive blow-ups. Moreover, since the singularities of these schemes are *inconsequential* the exceptional curves are all of genus 0.

Consider the diagram ((*) of §3)

$$\begin{array}{ccc}\operatorname{Pic}^0(X_n^{\#}) & \to & A_{n/S_n}\\ \uparrow & & \uparrow\\ \operatorname{Pic}^0(Y_{n-1}^{\#}) & \to & A_{n-1/S_n}.\end{array} \tag{2}$$

By Proposition 2 of §1 the horizontal morphisms are faithfully flat. Let $X_{n/k}^{\#}$ and $Y_{n-1/k}^{\#}$ denote the special fibres and $\tilde{X}_{n/k}^{\#}$, $\tilde{Y}_{n-1/k}^{\#}$ their normalizations.

Let $\tilde{\Sigma}_{X_n}$, $\tilde{\Sigma}_{Y_{n-1}}$ refer to the irreducible components of $\tilde{X}_{n/k}^{\#}$ and $\tilde{Y}_{n-1/k}^{\#}$, respectively, which map surjectively to the *good* component of exponent 0 of $X_{n/k}$, $Y_{n-1/k}$. Write

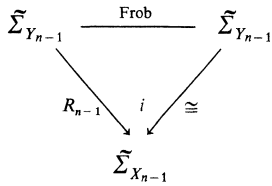
$$\tilde{X}_{n/k}^{\#}=\tilde{\Sigma}_{X_n}\amalg\tilde{\Sigma}'_{X_n}$$
$$\tilde{Y}_{n/k}^{\#}=\tilde{\Sigma}_{Y_{n-1}}\amalg\tilde{\Sigma}'_{Y_{n-1}}.$$

We have the maps induced by π, ρ of (1):

$$\begin{array}{ccccc}\tilde{X}_{n/k}^{\#} & = & \tilde{\Sigma}_{X_n} & \amalg & \tilde{\Sigma}'_{X_n}\\ \downarrow\tilde{\pi}_n & & \downarrow\Pi_n & & \downarrow\Pi'_n\\ \tilde{Y}_{n-1/k}^{\#} & = & \tilde{\Sigma}_{Y_{n-1}} & \amalg & \tilde{\Sigma}'_{Y_{n-1}}\\ \downarrow\tilde{\rho}_{n-1} & & \downarrow R_{n-1} & & \downarrow R'_{n-1}\\ (X_{n-1}^{\#}\times_{S_{n-1}}S_n)_{/k} & = & \tilde{\Sigma}_{X_{n-1}} & \amalg & \tilde{\Sigma}'_{X_{n-1}}\times_{S_{n-1}}S_n\end{array} \tag{3}$$

Moreover. Π_n is a separable morphism and R_{n-1} is purely inseparable of degree p.

Lemma 2. *There is an isomorphism* $\tilde{\Sigma}_{Y_{n-1}}\xrightarrow[i]{\cong}\tilde{\Sigma}_{X_{n-1}}$ *such that*



is commutative, where Frob *is the Frobenius endomorphism.*

Proof. Here we merely use that R_{n-1} is an inseparable morphism of a curve to a curve of degree p.

We also may "reduce" diagram (2) to characteristic p to get

$$\begin{array}{ccccc} \mathrm{Pic}^0(X^{\#}_{n/k}) & \longrightarrow & \mathrm{Pic}^0(\tilde{\Sigma}_{X_n}) \times \mathrm{Pic}^0(\tilde{\Sigma}'_{X_n}) & \longrightarrow & A_{n/k} \\ \uparrow & & \uparrow & & \uparrow \\ \mathrm{Pic}^0(Y^{\#}_{n-1/k}) & \longrightarrow & \mathrm{Pic}^0(\tilde{\Sigma}_{Y_{n-1}}) \times \mathrm{Pic}^0(\tilde{\Sigma}'_{Y_{n-1}}) & \longrightarrow & A_{n-1/k} \end{array} \tag{4}$$

where we have identified $\mathrm{Pic}^0(\tilde{\Sigma}_{X_n}) \times \mathrm{Pic}^0(\tilde{\Sigma}'_{X_n})$ with the abelian variety part of $\mathrm{Pic}^0(X^{\#}_{n/\mathbf{Q}_p[\zeta_{p^n}]})$ and similarly for $\mathrm{Pic}^0(\tilde{\Sigma}_{Y_{n-1}}) \times \mathrm{Pic}^0(\tilde{\Sigma}'_{Y_{n-1}})$.

In $A_{n-1}(\bar{k})$, let $A'_{n-1}(\bar{k})$ denote the image of

$$\{0\} \times \mathrm{Pic}^0(\tilde{\Sigma}'_{Y_{n-1}})(\bar{k})$$

under the natural mapping. Let

$$h\colon\ \mathrm{Pic}^0(\tilde{\Sigma}_{Y_{n-1}})(\bar{k}) \longrightarrow A_{n-1}(\bar{k})/A'_{n-1}(\bar{k})$$

denote the mapping induced from (4) to the indicated quotient.

A description of the kernel of $\mathrm{Pic}^0(Y^{\#}_{n-1})(\bar{K}) \to A_{n-1}(\bar{K})$:

Note that $\mathrm{Pic}^0(Y^{\#}_n)(\bar{K}) = \mathrm{Pic}^0(Y_n)(\bar{K})$. Let $k \geqq 1$ and let $N_{k,\underline{k}} \subset \mathrm{Pic}^0(Y_k)(\bar{K})$ be the kernel of the "norm mapping" $\mathrm{Pic}^0(Y_k)(\bar{K}) \to \mathrm{Pic}^0(X_{k-1})(\bar{K})$.

Define $N_{0,0} \subseteq \mathrm{Pic}^0(Y_0)(\bar{K})$ to be the kernel of $\mathrm{Pic}^0(Y_0)(\bar{K}) \to A_0(\bar{K})$.

Define $N_{k,n} \subset \mathrm{Pic}^0(Y_n)(\bar{K})$ for $n \geqq k \geqq 0$ by the inductive law: $N_{k,n} = (\rho_{n-1}\pi_n)^* N_{k,n-1}$.

Lemma 3. *The kernel of* $\mathrm{Pic}^0(Y^{\#}_{n-1})(\bar{K}) \to A_{n-1}(\bar{K})$ *is generated by the subgroups* $N_{n-1,k}$ *for* $k = 0, \ldots, n-1$.

Proof. This comes directly from the inductive definition of A_n.

A basic commutative diagram: The following compatibility was proved by Ofer Gabber.

Let L be a line bundle of degree 0 representing an isomorphism class of line bundles [44] in $\mathrm{Pic}^0(Y^{\#}_{n-1})(\bar{K})$.

Let $U^{\#}_{n-1} \subset Y^{\#}_{n-1/\bar{\mathcal{O}}}$ denote the open subscheme consisting of the generic fibre together with the open subscheme $\Sigma^0_{Y_{n-1}}$ of smooth points (over the base) in $\Sigma_{Y_{n-1}}$. Let $\mathscr{L}$ denote an extension of L to $U^{\#}_{n-1}$.

Let $\mathscr{L} \mid \Sigma^0_{Y_{n-1}}$ denote the restriction of $\mathscr{L}$ to the special fibre of $U^{\#}_{n-1}$ and let $\mathscr{L}' \mid \tilde{\Sigma}_{Y_{n-1}}$ denote *any* extension of $\mathscr{L} \mid \Sigma^0_{Y_{n-1}}$ to a line bundle on $\tilde{\Sigma}_{Y_{n-1}}$. Form the line bundle $\mathscr{L}'^{-1} \otimes \mathscr{L}'^{\sigma} = \mathscr{L}'^{\sigma-1}$ where σ is the element of order $(p-1)/2$ in $(\mathbf{Z}/p^{n-1}\mathbf{Z})^*/\pm 1$ chosen in the previous discussion.

Note that σ fixes pointwise the complement $\tilde{\Sigma}_{Y_{n-1}} - \tilde{\Sigma}^0_{Y_{n-1}}$. One sees that $\mathscr{L}'^{\sigma-1}$ is of degree zero, and that its isomorphism class in $\mathrm{Pic}^0(\tilde{\Sigma}_{Y_{n-1}})(\bar{k})$ depends only on $[L]$ and not on the choice $\mathscr{L}' \mid \tilde{\Sigma}_{Y_{n-1}}$. Denote this isomorphism class $c([L])$.

Consider the diagram

$$\begin{array}{ccccc}
\mathrm{Pic}^0(Y^{\#}_{n-1})(\bar{K}) & \xrightarrow{\alpha} & A_{n-1}(\bar{K}) & \cong & A_{n-1}(\bar{\mathcal{O}}) \\
\downarrow{\scriptstyle c} & & & & \downarrow \\
\mathrm{Pic}^0(\tilde{\Sigma}_{Y_{n-1}})(\bar{k}) & & & & A_{n-1}(\bar{k}) \\
\downarrow{\scriptstyle \sigma-1} & & & & \downarrow{\scriptstyle (\sigma-1)^2} \\
\mathrm{Pic}^0(\tilde{\Sigma}_{Y_{n-1}})(\bar{k}) & & & & A_{n-1}(\bar{k}) \\
{\scriptstyle h}\searrow & & & \swarrow & \\
 & & A_{n-1}(\bar{k})/A'_{n-1}(\bar{k}) & &
\end{array} \tag{5}$$

where the unlabeled maps are the natural ones.

Proposition 2. *Diagram* (5) *is commutative. Equivalently,* $h \circ (\sigma - 1) \circ c([L]) = f[L]$ *where* f: $\mathrm{Pic}^0(Y^{\#}_{n-1})(\bar{K}) \to A_{n-1}(\bar{k})/A'_{n-1}(\bar{k})$ *is obtained by proceeding clockwise in* (5).

Proof. Since $\mathrm{Pic}^0(Y^{\#}_{n-1})(\bar{\mathcal{O}}) \to A_{n-1}(\bar{\mathcal{O}})$ is surjective it suffices to show

(a) $h \circ (\sigma - 1) \circ c([L]) = f[L]$ where L represents an isomorphism class of line bundles in $\mathrm{Pic}^0(Y^{\#}_{n-1})(\bar{\mathcal{O}}) \subseteq \mathrm{Pic}^0(Y^{\#}_{n-1})(\bar{K})$.

(b) $h \circ (\sigma - 1) \circ c(N_{k,n-1}) = 0$ for $k = 1, \ldots, n-1$.

But assertion (a) is evident, for, by hypothesis, L extends to a line bundle $\mathscr{L}$ over $Y^{\#}_{n-1/\mathcal{O}}$ and we may take $\mathscr{L} \mid \tilde{\Sigma}_{Y_{n-1}}$ to be the restriction of this line bundle to $\tilde{\Sigma}_{Y_{n-1}}$.

As for (b) it sufficies to show that $cN_k = 0$ for all k. Here we use diagram (3) and Lemma 2. If $[L] \in N_k \subseteq \mathrm{Pic}^0(Y^{\#}_k)(\bar{K})$ for $k \geqq 1$ we have that

$$R_{n-1*}(\mathscr{L} \mid \Sigma^0_{Y_{n-1}})$$

is trivial, as line bundle on the curve $\Sigma^0_{X_{n-1}}$ of smooth points of $\Sigma_{X_{n-1}}$. But by Lemma 2, R_{n-1} is isomorphic to Frobenius, and an elementary local calculation then shows that $\mathscr{L} \mid \Sigma^0_{Y_{n-1}}$ is itself trivial, giving what we wish. If $[L] \in N_1$, one has only to note that $L^{\sigma-1}$ is trivial.

A "Snake Lemma". Using diagram (2), consider the mapping

$$\mathrm{Pic}^0(Y^{\#}_{n-1/\mathbf{Q}_p[\zeta_{p^n}]}) \xrightarrow[\varphi]{} \mathrm{Pic}^0(X^{\#}_{n/\mathbf{Q}_p[\zeta_{p^n}]}) \times A_{n-1/\mathbf{Q}_p[\zeta_{p^n}]}$$

and form $\tilde{P}_{/S_n}$ the scheme-theoretic closure in $\mathrm{Pic}^0(X^{\#}_n) \times A_{n-1/S_n}$ of the image of φ.

The natural mapping

$$\tilde{P} \longrightarrow \mathrm{Pic}^0(X^{\#}_{n/S_n})$$

is proper since A_{n-1} is proper over S_n, and by construction $\tilde{P}$ is a flat group scheme over S_n. We have a commutative diagram of group schemes over S_n:

$$\begin{array}{ccccccccc} 0 & \to & K_n & \longrightarrow & \mathrm{Pic}^0(X^{\#}_{n/S_n}) & \longrightarrow & A_{n/S_n} & \longrightarrow & 0 \\ & & \uparrow & & \uparrow \tilde{\pi}^* & & \uparrow & & \\ 0 & \to & \tilde{K}_n & \longrightarrow & \tilde{P} & \longrightarrow & A_{n-1/S_n} & \longrightarrow & 0 \end{array} \tag{6}$$

where $\tilde{P} \to A_{n-1}$ is faithfully flat by proposition 2 of §2.

Over $\mathbf{Q}_p[\zeta_{pn}]$ we have that $\tilde{\mathscr{K}}_n \to \mathscr{K}_n$ is surjective, and $A_{n-1} \to A_n$ is injective. Since $\mathscr{K}_n$ is $\mathrm{flat}_{/S_n}$ and $\tilde{\mathscr{K}}_{n/S_n} \to \mathscr{K}_{n/S_n}$ is proper it follows that $\tilde{\mathscr{K}}_n(\bar{k}) \to \mathscr{K}_n(\bar{k})$ is surjective. By the snake-lemma applied to $\bar{k}$-valued points of (6), we then have that the mapping of kernels

$$\begin{array}{ccc} \ker\{\tilde{P}(\bar{k}) & \longrightarrow & \mathrm{Pic}^0(X^{\#}_n)(\bar{k})\} \\ \downarrow & & \\ \ker\{A_{n-1}(\bar{k}) & \longrightarrow & A_n(\bar{k})\} \end{array}$$

is surjective.

Recall that an element of $\tilde{P}(\bar{k})$ can be lifted to $\tilde{P}(\bar{\mathcal{O}})$ and an element of $\tilde{P}(\bar{\mathcal{O}})$ is an element $y \in \mathrm{Pic}^0(Y_{n-1})(\bar{K})$ such that $\pi^* y$ lies in $\mathrm{Pic}^0(X^{\#}_{n-1})(\bar{\mathcal{O}})$.

It follows from this discussion that any $x_{/k} \in \ker\{A_{n-1}(\bar{k}) \to A_n(\bar{k})\}$ is the specialization of an element $x_{/\bar{K}} \in A_{n-1}(\bar{K})$ which is the image of some $y \in \mathrm{Pic}^0(Y_{n-1})(\bar{K})$ such that $\pi^* y$ lies in $\mathrm{Pic}^0(X^{\#}_n)(\bar{\mathcal{O}})$ and such that its specialization to $\bar{k}$, $\pi^* y_{/\bar{k}}$ is zero. Call such a y an *admissible lifting* for $x_{/\bar{k}}$.

Proposition 3. $(\sigma - 1)^2 \ker\{A_{n-1}(\bar{k}) \to A_n(\bar{k})\} \subseteq A'_{n-1}(\bar{k})$.

Proof. Let $x_{/\bar{k}}$ be in $\ker\{A_{n-1}(\bar{k}) \to A_n(\bar{k})\}$ and y an admissible lifting for $x_{/\bar{k}}$. By proposition 1, it suffices to show that $h \circ (\sigma - 1) \circ c(y) = 0$. We shall show, in fact, that $(\sigma - 1) \circ c(y) = 0$. Note first that there is a commutative diagram

$$\begin{array}{ccc} \mathrm{Pic}^0(Y^{\#}_{n-1})(\bar{K}) & \xrightarrow[\pi^*]{} & \mathrm{Pic}^0(X^{\#}_n)(\bar{K}) \\ \downarrow{\scriptstyle c} & & \downarrow{\scriptstyle c'} \\ \mathrm{Pic}^0(\tilde{\Sigma}_{Y_{n-1}})(\bar{k}) & & \mathrm{Pic}^0(\tilde{\Sigma}_{X_n})(\bar{k}) \\ \downarrow{\scriptstyle \sigma - 1} & & \downarrow{\scriptstyle \sigma - 1} \\ \mathrm{Pic}^0(\tilde{\Sigma}_{Y_{n-1}})(\bar{k}) & \xrightarrow[\pi^*]{} & \mathrm{Pic}^0(\tilde{\Sigma}_{X_n})(\bar{k}) \end{array}$$

where c' is defined in analogy with c. Consequently, since y is *admissible* we have that $(\sigma - 1) \circ c' \circ \pi^*(y) = 0$. To conclude what we wish, we note that

$$\pi^*\colon \mathrm{Pic}^0(\tilde{\Sigma}_{Y_{n-1}})(\bar{k}) \longrightarrow \mathrm{Pic}^0(\tilde{\Sigma}_{X_n})(\bar{k})$$

is injective.

To apply these two propositions we observe:

Proposition 4. *The subgroup*

$$A'_{n-1}(\bar{k}) \subseteq A_{n-1}(\bar{k})$$

is the image of $\{0\} \times \mathrm{Pic}^0(\tilde{\Sigma}^{\mu}_{n-1})(\bar{k})$ *under the isogeny* σ_{n-1} *and is stable under the operator* $U_p - 1$.

Proof. This follows from Propositions 1, 2 of §4.

Proposition 5 ("Case 2"). *Let* $\mathfrak{m}$ *be a component of reduced conductor divisible by p. (Equivalently: every basic character associated to* $\mathfrak{m}$ *has conductor divisible by p.) Then*

$$A_{n-1,\mathfrak{m},U_p-1}(\bar{k}) \longrightarrow A_{n,\mathfrak{m},U_p-1}(\bar{k})$$

is injective for $n \geqq 2$.

Proof. By Propositions 1, 2

$$(\sigma - 1)^2 \cdot \ker\{A_{n-1,\mathfrak{m},U_p-1}(\bar{k}) \longrightarrow A_{n,\mathfrak{m},U_p-1}(\bar{k})\}$$

is contained in $A'_{n-1,\mathfrak{m},U_p-1}(\bar{k})$ which vanishes by Lemma 1. But by hypothesis, $\sigma - 1$ is an automorphism on $\mathfrak{m}$-components.

§ 7. μ-deprived quotients

Let p be a prime and a an integer prime to p, $F/\mathbf{Q}$ a number field of finite degree, $\mathcal{O}(F)$ the ring of integers in F and $S = \mathrm{Spec}\,\mathcal{O}(F)\ [1/a]$.

Lemma (Serre). *Let* Γ *be a nontrivial p-divisible group scheme over S* ([16, 64]). *Suppose that* Γ *is either étale or that its dual group is étale over S. Then* $\Gamma_{/F}$ *does not occur as a subquotient of the p-divisible group associated to any abelian variety over F which has potentially good reduction at every prime above p.*

Proof. Replacing Γ by its dual if necessary, we may suppose that it is étale. Let $h = \mathrm{height}(\Gamma)$ and $H = Ta^*(\Gamma_{/F})$ which is, by definition, $\mathrm{Hom}(\Gamma(\bar{F}), \mathbf{Q}_p/\mathbf{Z}_p)$. Let E denote the h-th exterior product of H, $E = \Lambda^h H$. Thus E is free of rank 1 over $\mathbf{Z}_p$ and the action of $\mathrm{Gal}(\bar{F}/F)$ is therefore *abelian* in the sense that it factors through an abelian quotient of $\mathrm{Gal}(\bar{F}/F)$. Let G be the quotient of $\mathrm{Gal}(\bar{F}/F)$ which acts faithfully on E. Since $\Gamma_{/S}$ is étale, G is (a finite group times a pro-p group which is) the Galois group of an extension of F unramified at primes of F which do not lie over rational primes dividing a. Such an extension is then an abelian extension field of F such that every inertia group is finite. It follows that G is a *finite* group.

Suppose that $\Gamma_{/F}$ occurs as the subquotient of an abelian variety $A_{/F}$, with potentially good reduction at every prime above p. Extending F, if necessary, suppose that A has good reduction at every prime above p. If λ is a prime of S at which the abelian variety A has good reduction and Φ_λ is the associated Frobenius element, then the eigenvalues of Φ_λ acting on H are roots of unity. But, since $\Gamma_{/F}$ is a subquotient of the p-divisible group associated to $A_{/F}$, the eigenvalues of Φ_λ would have to be of absolute value $N_{F/\mathbf{Q}}(\lambda)^{h/2}$, yielding a contradiction.

Recall that a finite flat group scheme is said to be of *multiplicative type* if its dual is étale.

Let $\Gamma_{/S}$ be a p-divisible group, where S is as above. Let $E_1, E_2 \subseteq \Gamma$ be two finite flat subgroup schemes of Γ (over S) such that both are of multiplicative type. Then the subgroup scheme $E \subset \Gamma$ generated by E_1 and E_2 (which may be taken to be the Zariski closure in $\Gamma_{/S}$ of the group scheme over F generated by the generic fibres $E_{1/F}$ and $E_{2/F}$) is again of multiplicative type. One sees this easily, by considering the Cartier dual of the natural morphism $E_1 \oplus E_2 \to E$.

Let $\mu(\Gamma_{/S})$ denote the ind-finite subgroup scheme of $\Gamma_{/S}$ generated by all multiplicative-type subgroup schemes in $\Gamma_{/S}$.

Proposition 1. *If $\Gamma_{/S}$ is a p-divisible group scheme such that $\Gamma_{/F}$ occurs as a subquotient of the p-divisible group associated to an abelian variety over F with potentially good reduction at all primes above p, then $\mu(\Gamma_{/S})$ is a finite (flat) multiplicative-type group scheme; it contains all multiplicative-type subgroup schemes of $\Gamma_{/S}$.*

Proof. Consider the ind-finite subgroup scheme $\Gamma_{0/S}$ of $\mu(\Gamma_{/S})$ defined by the prescription that its $\overline{F}$-rational points are given by the subgroup of p-divisible elements in the $\overline{F}$-rational points of $\mu(\Gamma_{/S})$. Thus $\Gamma_{0/S}$ is the canonical p-divisible subgroup scheme of $\mu(\Gamma_{/S})$. Since the dual of $\Gamma_{0/S}$ is étale, and $\Gamma_{0/F}$ occurs as a subquotient of the p-divisible group associated to an abelian variety over F, we have that $\Gamma_0 = 0$ by Serre's lemma, from which it follows that $\mu(\Gamma_{/S})$ is finite.

Remark. If $\Gamma_{/S}$ is a p-divisible group scheme such that $\Gamma_{/F}$ occurs as a subquotient of the p-divisible group associated to an abelian variety over Γ with potentially good reduction at all primes above p, let $\Gamma'_{/S}$ denote the p-divisible group scheme obtained from Γ by dividing by the finite flat subgroup scheme $\mu(\Gamma_{/S})$. Since an extension of a multiplicative-type group scheme by a multiplicative-type group scheme is again of multiplicative type, it follows that $\mu(\Gamma'_{/S}) = 0$. We refer to $\Gamma'_{/S}$ as the canonical *μ-deprived quotient* of $\Gamma_{/S}$. If $\Gamma = \Gamma'$, we say that Γ is *μ-deprived.*

Proposition 2. . *Let $\Gamma_{/S}$ be as in Proposition* 1, *and suppose that $\Gamma_{/S}$ is μ-deprived. Let F'/F be a finite field extension and $S' = \operatorname{Spec} \mathcal{O}(F')[1/a]$. Then the base change $\Gamma_{/S'}$ is again μ-deprived.*

Proof. Without loss of generality we may suppose F'/F Galois. Let $\overline{F}$ be an algebraic closure of F'. Suppose that $M \subset \Gamma(\overline{F})$ is a finite $\operatorname{Gal}(\overline{F}/F')$-module that prolongs to a multiplicative-type subgroup scheme $\mathcal{M}$ in $\Gamma_{/S'}$. If $g \in \operatorname{Gal}(\overline{F}/F)$, then $g \cdot M \subset \Gamma(\overline{F})$ is again a finite $\operatorname{Gal}(\overline{F}/F')$-module, which prolongs to a finite flat subgroup scheme in $\Gamma_{/S'}$ which we call $g\mathcal{M}$.

Claim. *$g\mathcal{M}_{/S'}$ is of multiplicative-type.*

Proof. Consider an integer m large enough so that $\mathcal{M} \subseteq \Gamma[p^m]_{/S'}$ and let $\Gamma_m = \Gamma[p^m]_{/S}$. The restriction of g to F', $\bar{g}$: $F' \to F'$ induces compatible automorphisms of schemes

$$\begin{array}{ccc} \Gamma_m \underset{S}{\times} S' & \xrightarrow[\cong]{1 \times \bar{g}} & \Gamma_m \underset{S}{\times} S' \\ \downarrow & & \downarrow \\ S' & \xrightarrow[\cong]{\bar{g}} & S' \end{array}$$

and the restriction of $1 \times \bar{g}$ to $\mathscr{M}$, viewed as subscheme of $\Gamma_m \underset{S}{\times} S'$, is an isomorphism of the scheme $\mathscr{M}$ onto the scheme $g\mathscr{M}$. Of course, this isomorphism is *not* compatible with S'-scheme structures. Rather, we have a commutative diagram

$$\begin{array}{ccccc} \mathscr{M} & \longrightarrow & S' \underset{S'}{\times} g\mathscr{M} & \longrightarrow & g\mathscr{M} \\ & \searrow \quad \swarrow & & \searrow & \\ & S' & \xrightarrow[\bar{g}]{} & S' & \end{array}$$

where the parallelogram is cartesian, and the horizontal morphism in the triangle is an isomorphism of S'-group schemes. It is then immediate that $g\mathscr{M}$ is of multiplicative type and depends only on $\bar{g}$, and not on g.

Now form $W \subset \Gamma(\overline{F})$, the subgroup generated by $\{gM\}$ where g ranges through a (finite) system of elements of $\mathrm{Gal}(\overline{F}/F)$ such that $\bar{g}$ runs through every element of $\mathrm{Gal}(F'/F)$. By the discussion before proposition 2 and what we have just proved, one sees that the prolongation $\mathscr{W}'$ of W in $\Gamma_{/S'}$ is of multiplicative type. But W is $\mathrm{Gal}(\overline{F}/F)$-stable by construction. Thus W prolongs to $\mathscr{W}$, a finite flat group scheme in $\Gamma_{/S}$. Since $\Gamma_{/S'}$ is the base change of $\Gamma_{/S}$ to S', $\mathscr{W}'$ is the base change of $\mathscr{W}$ to S', and since $\mathscr{W}'$ is of multiplicative type, $\mathscr{W}$ also is. It follows from μ-deprivedness of $\Gamma_{/S}$ that $\mathscr{W} = 0$; hence $M = 0$ as was to be proved.

Now let $R_{\mathfrak{m}}^{(n)}$ be a factor of $\mathbf{Z}_p[(\mathbf{Z}/ap^n\mathbf{Z})^*]$ corresponding to an even pseudo-primitive component $\mathfrak{m}$. Let $F = \mathbf{Q}(\zeta_{p^n})$, $S = \mathscr{O}(F)[1/a]$, and let $A_{/S} = A_{n/S}$ be the Néron model of A_n which is defined in §1. Let P be a maximal ideal in $\mathbf{T}_{\mathfrak{m}}^{(n)} = \mathbf{T}_{\mathfrak{m}}$, containing the element $U_p - 1$. (Later we will let P be the Eisenstein prime of Chap. 5, §1). As usual, we let $\mathbf{T}_{\mathrm{P}}$ denote the P-adic completion of $\mathbf{T}$ and A_{P} the "P-divisible group" associated to A.

By Proposition 3 of Chap. 3, § 3, $A_{P/S}$ is an ordinary p-divisible group scheme (at the closed point $s \in S$ of characteristic p). Consider the exact sequence of Tate modules over $\mathscr{O}$, the completion of $\mathbf{Z}[\zeta_{p^n}]$ at the prime above p.

$$0 \to Ta^*(A^{\text{ét}}_{P/\mathscr{O}}) \to Ta^*(A_{P/\mathscr{O}}) \to Ta^*(A^{\text{m.t.}}_{P/\mathscr{O}}) \to 0 \tag{1}$$

where the superscripts ét and m.t. refer to étale and multiplicative-type parts. The above exact sequence may be viewed as an exact sequence of $\mathbf{T}_p$-modules.

Proposition 3.

$$Ta^*(A^{\text{ét}}_{P/F_s}) \otimes \mathbf{Q} \quad \text{and} \quad Ta^*(A^{\text{m.t.}}_{P/F_s}) \otimes \mathbf{Q}$$

are both free of rank 1 *over* $\mathbf{T}_P \otimes \mathbf{Q}$.

Proof. In the exact sequence (1) above we know by Proposition 2 of Chap. 3, §4 and §5 that $Ta^*(A_{P/F_s}) \otimes \mathbf{Q}$ is free of rank 2 over $\mathbf{T}_P \otimes \mathbf{Q}$. Moreover $\mathbf{T}_P \otimes \mathbf{Q}$ is a product of fields and of $\mathbf{Q}$-algebras of the form $K[x_1, \ldots, x_r]/(x_1^2, \ldots, x_r^2)$ where K is a field (cf. Proposition 1 of Chap. 3, §4 and §5).

A theorem of Tate asserts that the functor from p-divisible groups over $\mathscr{O}$ to their associated Galois modules is fully faithful. Hence there can be no non-trivial Galois-equivariant map from a $\mathrm{Gal}(\mathbf{Q}/\mathbf{Q})$-stable subquotient of $Ta^*(A^{\text{m.t.}}_{P/F_s}) \otimes \mathbf{Q}$

into a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-stable subquotient of $Ta^*(A^{\text{ét}}_{P/F_s}) \otimes \mathbf{Q}$ or vice versa. We now are in the situation of the following algebraic lemma.

Lemma 2. *Let K be a field and $\mathscr{K} = K[\varepsilon_1, \ldots, \varepsilon_n]$ the commutative K-algebra defined by the relations*

$$\varepsilon_1^2 = \cdots = \varepsilon_n^2 = 0.$$

Let

$$0 \to U \to V \to W \to 0 \tag{2}$$

be an exact sequence of nontrivial $\mathscr{K}$-modules with a commuting action of a group $\mathscr{G}$, such that

$$V \text{ is a free } \mathscr{K}\text{-module of rank } 2.$$

Suppose that there is no nontrivial $\mathscr{G}$-equivariant homomorphism from a $\mathscr{G}$-stable subquotient of W to a $\mathscr{G}$-stable subquotient of U. Then U and V are free $\mathscr{K}$-modules of rank 1.

Proof. Let d be the dimension of $\mathscr{K}$ as a vector space over K. Then V is of dimension $2d$ over K.

After passing to the K-dual, if necessary, we may suppose that $\dim_K U \leqq d$. Note that $\mathscr{K}$ is a Gorenstein ring, so that $\mathrm{Hom}(V, K)$ is also free of rank 2 over $\mathscr{K}$.

Let $\varepsilon = \varepsilon_1 \cdots \varepsilon_n$. To show that U is free of rank 1 over $\mathscr{K}$, it suffices to show that ε doesn't annihilate U. For then, taking $u \in U$ any element such that $\varepsilon \cdot u \neq 0$, one easily sees that u is a free generator for the $\mathscr{K}$-module U. Consider the map

$$\varepsilon\colon\ V \to \varepsilon V = V[\mathfrak{a}] \tag{3}$$

where $\mathfrak{a}$ is the maximal ideal $(\varepsilon_1, \ldots, \varepsilon_n) \subset \mathscr{K}$, and where $V[\mathfrak{a}]$ denotes the kernel of $\mathfrak{a}$ in V. If ε annihilates U, then (3) factors through the quotient V/U to give a surjective mapping

$$e\colon\ W \twoheadrightarrow V[\mathfrak{a}].$$

But since $V[\mathfrak{a}]$ contains $U[\mathfrak{a}]$ we may restrict e to

$W_0 = e^{-1}U[\mathfrak{a}]$, yielding a nontrivial $\mathscr{G}$-equivariant map, contradicting our hypothesis.

Passing again to the K-dual and noting that $\dim_K \mathrm{Hom}(W, K) = d$, we get that W is also free of rank 1.

Now to prove Proposition 3, apply the above lemma, taking (1) for (2) and $\mathrm{Gal}(\overline{F}_s/F_s)$ for $\mathscr{G}$.

We see then that if the proposition is false, then there is a $\mathbf{Q}$-algebra $\mathscr{K}$ of the type in the lemma occurring as a direct factor of $\mathbf{T}_P \otimes \mathbf{Q}$ such that one of the following two $\mathscr{K}$-modules vanishes:

$$Ta^*(A^{\text{ét}}_{P/F_s}) \otimes_{\mathbf{T}_P} \mathscr{K} \quad \text{or} \quad Ta^*(A^{\text{m.t.}}_{P/F_s}) \otimes_{\mathbf{T}_P} \mathscr{K}.$$

Suppose, for example, that it is the latter $\mathscr{K}$-module that vanishes. Then

$$Ta^*(A_{P/F_s}) \otimes_{\mathbf{T}_P} \mathscr{K} = Ta^*(A^{\text{ét}}_{P/F_s}) \otimes_{\mathbf{T}_P} \mathscr{K}.$$

Let $\mathscr{J} \subset \mathbf{T}_P$ denote the kernel of $\mathbf{T}_P \to \mathscr{K}$ and let $\Gamma_{/S}$ denote the quotient p-divisible group scheme $A_P/\mathscr{J} \cdot A_P$ over the base S. The p-divisible group scheme Γ inherits a $\mathbf{T}_P/\mathscr{J}\,\mathbf{T}_P$-module structure, and we have the natural isomorphism of $\mathscr{K}$-modules and $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-modules:

$$Ta^*(A_{P/F_s}) \otimes_{\mathbf{T}_P} \mathscr{K} = Ta^*(\Gamma_{/F_s}) \otimes_{\mathbf{T}_P/\mathscr{J}\mathbf{T}_P} \mathscr{K}.$$

From the discussion above, it then follows that $\Gamma_{/S}$ is an étale p-divisible group scheme such that $\Gamma_{/F}$ occurs as a subquotient of the p-divisible group associated to some abelian variety over F, of potentially good reduction at p, contradicting Serre's lemma.

Corollary 1.

$$Ta^*(A^{\text{ét}}_{P/F_s}) \quad \textit{and} \quad Ta^*(A^{\text{m.t.}}_{P/F_s})$$

are faithful $\mathbf{T}_P$*-modules.*

Proof. The natural mapping $\mathbf{T}_P \to \mathbf{T}_P \otimes \mathbf{Q}$ is injective, and by the proposition if U is either of the two modules above, $U \otimes \mathbf{Q}$ is free of rank 1, and hence faithful over $\mathbf{T}_P \otimes \mathbf{Q}$.

From Proposition 1, we conclude that $\mu(A_{P/S})$ is a finite flat subgroup scheme in the p-divisible group scheme $A_{P/S}$. If $B_{/S}$ denotes the quotient abelian scheme obtained from $A_{/S}$ by division by $\mu(A_{P/S})$ one easily sees that $B_{P/S}$ inherits a natural $\mathbf{T}_P$-module structure, and has the property that it contains no multiplicative type subgroup schemes over S. We refer to $B_{/S}$ as the canonical quotient of $A_{/S}$ which is *μ-deprived at P.*

From the arguments of proposition 2, $\mu(A_{P/S})(\bar{\mathbf{Q}}) \subset A(\bar{\mathbf{Q}})$ is easily seen to be stable under the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ and therefore we have that B is "defined over $\mathbf{Q}$" in the sense that we may take $B_{/\mathbf{Q}}$ to be the abelian variety defined as the quotient of $A_{/\mathbf{Q}}$ by the finite $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-module $\mu(A_{P/S})(\bar{\mathbf{Q}})$.

Corollary 2.

$$Ta^*(B^{\text{ét}}_{P/F_s}) \quad \textit{and} \quad Ta^*(B^{\text{m.t.}}_{P/F_s})$$

are faithful $\mathbf{T}_P$-modules.

Chapter 4. The cuspidal group

The main result of this chapter (the theorem of §3) shows that a certain cuspidal group on A_n is a cyclic $R^{(n)}_{\mathfrak{m}}$-module whose annihilator ideal (denoted $\mathfrak{b}^{(n)}_{\mathfrak{m}}$: the "basic ideal") is *closely related* to the Stickelberger ideal $\hat{S}'_{\mathfrak{m}}(N)$. If $\mathfrak{m}$ is a-primitive, this ideal is generated by the Stickelberger element $\vartheta^{(n)}_{\mathfrak{m}}$.

§ 1. The zero-cusps

Recall that the "zero-cusps" of $X_1(N)$ refer to the cusps of type $\begin{bmatrix} 0 \\ \pm b \end{bmatrix}$ in Shimura's notation, where b ranges through integers mod N which are relatively prime to N. That is, $\begin{bmatrix} 0 \\ \pm b \end{bmatrix}$ is the $\Gamma_1(N)$-orbit in $\mathbf{P}^1(\mathbf{Q})$ consisting of elements $\pm(\alpha, \beta)$ where α is an arbitrary integer and $\beta \equiv b \bmod N$.

We may view the set $\mathscr{Z}_n$ of zero-cusps in $X_1(ap^n)$ as a principal homogeneous set under the action of $(\mathbf{Z}/N\mathbf{Z})^*/(\pm 1)$ via the diamond operators. The zero-cusps are rational over $\mathbf{Q}$.

If $\mathbf{Z}[\mathscr{Z}_n]$ is the free abelian group generated by $\mathscr{Z}_n$ and $\mathbf{Z}[\mathscr{Z}_n]^0$ is the kernel of the degree-homomorphism

$$\mathbf{Z}[\mathscr{Z}_n] \xrightarrow{\deg} \mathbf{Z}$$

we view $\mathbf{Z}[\mathscr{Z}_n]^0$ as a group of divisors of degree zero on $X_1(ap^n)$; it is naturally a module over the ring $\mathbf{Z}[(\mathbf{Z}/N\mathbf{Z})^*/(\pm 1)]$ via the diamond operators, the action being given by:

$$\langle r \rangle \cdot \begin{bmatrix} 0 \\ b \end{bmatrix} = \begin{bmatrix} 0 \\ rb \end{bmatrix}.$$

The Hecke operators $T_l (l \nmid N)$ operate on $\mathbf{Z}[\mathscr{Z}_n]$ by the formula:

$$T_l \begin{bmatrix} 0 \\ b \end{bmatrix} = (l\langle l \rangle + l) \begin{bmatrix} 0 \\ b \end{bmatrix}.$$

The operator $U_q (q | N)$ acting on the cusp $z = r/s$ is given by the formula

$$U_q z = \sum \left(\frac{z + a}{q} \right).$$

In particular, in Shimura's notation, for the zero-cusp $\begin{bmatrix} 0 \\ b \end{bmatrix}$ (with $(b, N) = 1$) we obtain

$$U_q \begin{bmatrix} 0 \\ b \end{bmatrix} = \begin{bmatrix} 0 \\ b \end{bmatrix} + \sum_{i=1}^{q-1} \begin{bmatrix} i \\ qb \end{bmatrix} \tag{1}$$

and

$$(U_q^r - U_q^{r-1}) \begin{bmatrix} 0 \\ b \end{bmatrix} = \sum_{i \in (\mathbf{Z}/q^r\mathbf{Z})^*} \begin{bmatrix} i \\ q^r b \end{bmatrix} \tag{2}$$

The Zariski-closure of the subscheme $\mathscr{Z}_n$ in $\mathscr{X}_1(N)_{/\mathbf{Z}}$ (the "incomplete moduli space") is an étale ("constant") finite flat extension of Spec $\mathbf{Z}$ which we denote $\mathscr{Z}_{n/\mathbf{Z}}$. Its reduction to characteristic p may be regarded as a finite subscheme of $\tilde{\Sigma}_{\text{ét}/\mathbf{F}_p}$:

$$\mathscr{Z}_{n/\mathbf{F}_p} \subseteq \tilde{\Sigma}_{\text{ét}/\mathbf{F}_p}.$$

From the basic diagram of Chap. 3 we have the following connection between zero-cusps at level n and at level $n-1$:

$$\begin{array}{c}\text{zero-cusps of } X_1(ap^n) = \mathscr{Z}_n \\ \Big\downarrow \pi_n \\ \text{zero-cusps of } X_1(ap^n, ap^{n-1}) \\ \Big\downarrow \rho_n \quad (1:1 \text{ correspondence}) \\ \text{zero-cusps of } X_1(ap^{n-1})\end{array}$$

where $n > 1$. We identify $\mathscr{Z}_{n-1}$ with the set of zero-cusps of $X_1(ap^n, ap^{n-1})$ via ρ_n. We obtain the following commutative diagram of $\mathbf{Z}[(\mathbf{Z}/N\mathbf{Z})^*/(\pm 1)]$-modules and of group schemes over **Q**:

$$\begin{array}{ccccc}
\mathbf{Z}[\mathscr{Z}_n]^0 & \xrightarrow{\xi^{(n)}} & J_1(ap^n) & \longrightarrow & A_n \\
\uparrow \text{Tr} & & \uparrow \pi_n^* & & \uparrow i_{/\mathbf{Q}} \\
\mathbf{Z}[\mathscr{Z}_{n-1}]^0 & \longrightarrow & J_1(ap^n, ap^{n-1}) & \longrightarrow & A_{n-1} \\
\downarrow \text{identity} & & \downarrow \rho_{n*} & & \downarrow \text{identity} \\
\mathbf{Z}[\mathscr{Z}_{n-1}]^0 & \xrightarrow{\xi^{(n-1)}} & J_1(ap^{n-1}) & \longrightarrow & A_{n-1}
\end{array} \tag{3}$$

We have considered the left-hand groups as "constant" group-schemes over **Q**. Thus, since $\mathscr{Z}_{n/\mathbf{Z}}$ is a finite étale scheme over Spec **Z** isomorphic to the disjoint union of a finite number r of copies of Spec **Z**, $\mathbf{Z}[\mathscr{Z}_n]^0_{/\mathbf{Z}}$ is an étale "constant" free abelian group over Spec **Z** of rank $r-1$. The mapping Tr is the natural "trace" map which sends z to $\sum_{z'}[z']$ for $z \in \mathscr{Z}_{n-1}$ where the summation runs over $z' \in \mathscr{Z}_n$ which project to z. By the Manin-Drinfeld theorem, the image of $\mathbf{Z}[\mathscr{Z}_n]^0$ in $J_1(ap^n)$ is a finite subgroup. The mapping $i_{/\mathbf{Q}}$ is injective by construction. Let

$$\lambda^{(n)}\colon \mathbf{Z}[\mathscr{Z}_n]^0 \to A_n$$

denote the composition of the two homomorphisms in the top line of diagram (3).

If $\mathcal{O} = \mathbf{Z}_p[\zeta_{p^n}]$, since $\mathbf{Z}[\mathscr{Z}_n]^0_{/\mathcal{O}}$ is étale, diagram (3) induces a homomorphism

$$\xi^{(n)}_{/\mathcal{O}}\colon \mathbf{Z}[\mathscr{Z}_n]^0_{/\mathcal{O}} \to J_1(ap^n)_{/\mathcal{O}}$$

(where $J_1(ap^n)_{/\mathcal{O}}$ is the Néron model over $\mathcal{O}$ of $J_1(ap^n)$) and a commutative diagram of group-schemes over $\mathcal{O}$:

$$\begin{array}{ccc}
\mathbf{Z}[\mathscr{Z}_n]^0_{/\mathcal{O}} & \xrightarrow{\lambda^{(n)}_{/\mathcal{O}}} & A_{n/\mathcal{O}} \\
\uparrow \text{Tr} & & \uparrow i_{/\mathcal{O}} \\
\mathbf{Z}[\mathscr{Z}_{n-1}]^0_{/\mathcal{O}} & \xrightarrow{\lambda^{(n-1)}_{/\mathcal{O}}} & A_{n-1/\mathcal{O}}.
\end{array} \tag{4}$$

Here again the left-hand group schemes are constant group schemes over $\mathcal{O}$. The Néron model $A_{n/\mathcal{O}}$ is an abelian scheme. We do *not* know whether $i_{/\mathcal{O}}$ identifies $A_{n-1/\mathcal{O}}$ with an abelian subscheme of $A_{n/\mathcal{O}}$.

Note that since $\mathscr{Z}_n$ specializes to smooth points of the irreducible component $\tilde{\Sigma}_n^{\text{ét}}$ in $X_1(ap^n)_{/k}$ it follows (by considering a regular resolution of $X_1(ap^n)_{/\mathcal{O}}$ and applying Raynaud's Proposition 1 of §1 of Chap. 2) that $\xi_{/\mathcal{O}}^{(n)}$ maps $\mathbf{Z}[\mathscr{Z}_n]_{/\mathcal{O}}^0$ into the *connected component* $J_1(ap^n)_{/\mathcal{O}}^0$ of the Néron model.

We have the following commutative diagram which describes what happens when one specializes to characteristic p. Let $k \cong \mathbf{F}_p$ denote the residue field of $\mathcal{O}$.

$$\begin{array}{ccccc} & & & & J_1(N)_{/k}^0 \\ & \overset{\xi_{/k}^{(n)}}{\nearrow} & & \overset{u}{\searrow} & \\ \mathbf{Z}[\mathscr{Z}_n]^0 & \xrightarrow{s^{(n)}} & \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}) & \longrightarrow & \mathrm{Pic}^0(\widetilde{X_1(N)}_{/k}) \\ & & \downarrow & & \downarrow \\ & & \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}^{\mu}) & \xrightarrow[\sigma]{} & A_{n/k} \end{array} \tag{5}$$

where the mappings are as follows:

(a) $\mathrm{Pic}^0(\widetilde{X_1(N)}_{/k})$ breaks up canonically as the product of Pic^0 of the normalization of each irreducible component of $X_1(N)_{/k}$ and the injection of $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})$ in $\mathrm{Pic}^0(X_1(N)_{/k})$ is as a factor.

(b) The injection of $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})$ in the product $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}^{\mu})$ is as the first factor.

(c) The mapping σ is the *isogeny* of Chap. 3, §2.

(d) The mapping $\mathbf{Z}[\mathscr{Z}_n]^0 \to \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})$ is the natural one obtained by viewing an element of $\mathbf{Z}[\mathscr{Z}_n]^0$ as a divisor of degree zero in $\tilde{\Sigma}^{\text{ét}}$.

(e) The mapping $\xi_{/k}^{(n)}\colon \mathbf{Z}[\mathscr{Z}_n]^0 \to J_1(N)_{/k}^0$ is the reduction to k of the mapping

$$\xi_{/\mathcal{O}}^{(n)}\colon \mathbf{Z}[\mathscr{Z}_n]_{/\mathcal{O}}^0 \to J_1(N)_{/\mathcal{O}}^0 .$$

(f) The mapping $u\colon J_1(N)_{/k}^0 \to \mathrm{Pic}^0(X_1(N)_{/k})$ is the projection to the abelian variety part (cf. Cor. 2 of §7 of Chap. 2).

We have the commutative triangle:

$$\begin{array}{ccc} \mathbf{Z}[\mathscr{Z}_n]^0 & \xrightarrow{s^{(n)}} & \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}) \\ & \underset{\lambda_{/k}^{(n)}}{\searrow} \quad \swarrow & \\ & A_{n/k} & \end{array} \tag{6}$$

Since the image of $\mathbf{Z}[\mathscr{Z}_n]^0$ under $\lambda_{/\mathcal{O}}^{(n)}$ (and under $s^{(n)}$) is a finite group, we may pass to "p-primary components" [5] (of the images) replacing the abelian varieties by the associated p-divisible group schemes. This gives us commutative diagrams

---

[5] Note that for any prime q dividing N, we may extend the definition of $(U_q - q\langle n_q\rangle)\xi_{/k}^{(n)}$, and of $(U_q - q\langle n_q\rangle)s^{(n)}$ from $\mathbf{Z}[\mathscr{Z}_n]^0$ to all of $\mathbf{Z}[\mathscr{Z}_n]$ by setting $(U_q - q\langle n_q\rangle)\xi_{/k}^{(n)}\begin{bmatrix}0\\b\end{bmatrix}$ equal to the divisor class of

$$\begin{bmatrix}0\\b\end{bmatrix} + \sum_{i=1}^{q-1}\begin{bmatrix}i\\b\end{bmatrix} - q\begin{bmatrix}0\\qb\end{bmatrix}$$

in $J_1(ap^n)$, and similarly for $(U_q - q\langle n_q\rangle)s^{(n)}$

$$\begin{array}{ccc} Z_p[\mathscr{Z}_n]^0_{/\mathscr{O}} & \xrightarrow{\lambda^{(n)}_{p/\mathscr{O}}} & A_{n,\,p/\mathscr{O}} \\ \uparrow \mathrm{Tr} & & \uparrow \\ \mathbf{Z}_p[\mathscr{Z}_{n-1}]^0_{/\mathscr{O}} & \xrightarrow{\lambda^{(n-1)}_{p/\mathscr{O}}} & A_{n-1,\,p/\mathscr{O}} \end{array} \tag{7}$$

and

$$\begin{array}{ccc} \mathbf{Z}_p[\mathscr{Z}_n]^0 & \xrightarrow{s^{(n)}_p} & \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})_p \\ & {\scriptstyle\lambda^{(n)}_p}\searrow \quad \swarrow & \\ & A_{n,\,p/k} & \end{array} \tag{8}$$

where the subscript p attached to an abelian scheme means: associated p-divisible group scheme.

Now choose an *even* component $\mathfrak{m}$, whose associated factor of $R^{(n)} = \mathbf{Z}_p[(\mathbf{Z}/N\mathbf{Z})^*/(\pm 1)]$ we denote, as usual, $R^{(n)}_{\mathfrak{m}}$. Tensoring diagrams (7) and (8) with the projection

$$R(n) = \mathbf{Z}_p[(\mathbf{Z}/N\mathbf{Z})^*/(\pm 1)] \twoheadrightarrow R^{(n)}_{\mathfrak{m}}$$

allows us to pass to the component $\mathfrak{m}$.

Let the subscript $\mathfrak{m}$ denote the "$\mathfrak{m}$-part" of the p-divisible group scheme associated to an abelian scheme. Thus,

$$A_{n,\,\mathfrak{m}/\mathscr{O}} = R^{(n)}_{\mathfrak{m}} \otimes_{\mathbf{Z}_p[(\mathbf{Z}/N\mathbf{Z})^*/(\pm 1)]} A_{n,\,p/\mathscr{O}}$$

and similarly for $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})_{\mathfrak{m}}$.

With the above understandings, then, diagrams (7) and (8) yield the following:

$$\begin{array}{ccc} \mathbf{Z}_p[\mathscr{Z}_n]^0 \underset{R^{(n)}}{\otimes} R^{(n)}_{\mathfrak{m}} & \xrightarrow{\lambda^{(n)}_{\mathfrak{m}}} & A_{n,\,\mathfrak{m}}(\mathscr{O}) \\ \uparrow \mathrm{Tr} & & \uparrow i(\mathscr{O}) \\ \mathbf{Z}_p[\mathscr{Z}_{n-1}]^0 \underset{R^{(n-1)}}{\otimes} R^{(n-1)}_{\mathfrak{m}} & \xrightarrow{\lambda^{(n-1)}_{\mathfrak{m}}} & A_{n-1,\,\mathfrak{m}}(\mathscr{O}) \end{array} \tag{9}$$

$$\begin{array}{ccc} \mathbf{Z}_p[\mathscr{Z}_n]^0 \underset{R^{(n)}}{\otimes} R^{(n)}_{\mathfrak{m}} & \xrightarrow{s^{(n)}_{\mathfrak{m}}} & \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})_{\mathfrak{m}}(k) \\ \downarrow {\scriptstyle\lambda^{(n)}_{\mathfrak{m}}} & \searrow {\scriptstyle\lambda^{(n)}_{\mathfrak{m}}(k)} & \downarrow \\ A_{n,\,\mathfrak{m}}(\mathscr{O}) & \longrightarrow & A_{n,\,\mathfrak{m}}(k). \end{array} \tag{10}$$

In (10), the bottom horizontal line refers to the natural specialization homomorphism.

For any q dividing N, we have an extension of $(U_q - q\langle n_q\rangle)s^{(n)}_{\mathfrak{m}}$ from $\mathbf{Z}_p[\mathscr{Z}_n]^0 \underset{R^{(n)}}{\otimes} R^{(n)}_{\mathfrak{m}}$ to all of $\mathbf{Z}_p[\mathscr{Z}_n] \underset{R^{(n)}}{\otimes} R^{(n)}_{\mathfrak{m}}$, and similarly for $(U_q - q\langle n_q\rangle)\lambda^{(n)}_{\mathfrak{m}}$.

In the case where $\mathfrak{m}$ is a nonprincipal component (i.e., its basic character is of conductor greater than 1), the natural mapping

$$\mathbf{Z}_p[\mathscr{Z}_n]^0 \underset{R^{(n)}}{\otimes} R_{\mathfrak{m}}^{(n)} \to \mathbf{Z}_p[\mathscr{Z}_n] \underset{R^{(n)}}{\otimes} R_{\mathfrak{m}}^{(n)}$$

is an isomorphism of $R_{\mathfrak{m}}^{(n)}$-modules, the latter being *free* of rank one over $R_{\mathfrak{m}}^{(n)}$.

It will simplify notation considerably (and not add much confusion) if we *choose* an $R_{\mathfrak{m}}^{(n)}$-generator of this module. Indeed, we do this by choosing a "base cusp": if ζ_N is identified with $e^{2\pi i/N}$ in $\mathbf{C}$, then we take our "base cusp" to be $[{}^0_1]$ in $X_1(N)_{/\mathbf{C}}$.

§ 2. *The theory of Kubert-Lang in characteristic p*

It is a great convenience to us that the modular units of Kubert-Lang behave in many ways much better in characteristic p than in characteristic zero. In particular, we shall see that the so-called special group of [39] is, at least in the primitive components, precisely the kernel of specialization in a suitable sense.

Let g_{a_1, a_2} for $(a_1, a_2) \in (\mathbf{Z} \times \mathbf{Z}) - (N\mathbf{Z} \times N\mathbf{Z})$ be the Siegel functions as in [38] and [39]. The q-expansion at the cusp $[{}^0_1]$ of g_{a_1, a_2} is

$$-q^{\frac{1}{2}\mathbf{B}_2\left(\left\langle \frac{a}{N} \right\rangle\right)} \cdot e^{2\pi i \frac{a_1}{N}\left(\frac{a_2}{N} - 1\right)} \cdot \left(1 - \zeta_N^{a_1} q^{\frac{a_2}{N}}\right) \prod_{\nu=1}^{\infty} \left(1 - \zeta_N^{a_1} q^{\nu + \frac{a_2}{N}}\right)\left(1 - \zeta_N^{-a_1} q^{\nu - \frac{a_2}{N}}\right) \tag{1}$$

where $q = e^{2\pi i(-1/z)}$ and $\zeta_N = e^{\frac{2\pi i}{N}}$. Changing (a_1, a_2) by adding an element of $N\mathbf{Z} \times N\mathbf{Z}$ has the effect of multiplying $g_{(a_1, a_2)}$ by a root of unity. Hence the divisor of $g_{(a_1, a_2)}$ is determined by (a_1, a_2) modulo N.

Now consider the function $g_{0,s}$ for $s \in \mathbf{Z} - N\mathbf{Z}$. We observe first that $g_{0,s} = (\text{constant})\, g_{0,-s}$. For convenience of notation we shall write $g_{0,0} = 1$. If $m: \mathbf{Z}/N\mathbf{Z} \to \frac{1}{2}\mathbf{Z}$ is a function such that $m(0) = 0$ and $m(-s) = m(s)$ we write $g = g^m$ for the Siegel function

$$g^m = \prod g_{0,s}^{m(s)}$$

where s runs through a system of representative of $\mathbf{Z}/N\mathbf{Z} - 0$ in $\mathbf{Z} - N\mathbf{Z}$. The divisor of g^m is independent of the system of representatives chosen.

Kubert has determined necessary and sufficient conditions for a Siegel function to be of level N (i.e., to be "on $\Gamma(N)$"). We quote his basic result (§4, and Theorem 1 of §5 [38]) adapting it to our Siegel functions. Let $\nu = 12/(N, 12)$.

Proposition 1 (Kubert). *Let $m: \mathbf{Z}/N\mathbf{Z} \to \mathbf{Z}$ have the property that $m(0) = 0$. The Siegel function g^m is a modular function on $\Gamma_1(N)$ if and only if $\sum_{s \bmod N} m(s)\, s^2 \equiv 0 \bmod N$ and any of the following three conditions hold:*

(a) *N is* odd *and $\sum m(s) \equiv 0 \bmod \nu$.*

(b) *N is even, $\sum m(s) \equiv 0 \bmod \nu$, and $\sum m(s)\, s^2 \equiv 0 \bmod 2N$.*

(c) *$N \equiv 2 \bmod 4$, $(\sum m(s), \nu) = \frac{1}{2}\nu$ and $\sum m(s)\, s^2 \not\equiv 0 \bmod 2N$.*

Proof. Let $\eta_{0,s}=\eta^{-2}g_{0,s}$ be the Klein form (loc. cit.). Then the explicit transformation laws given in §1 of [Ku] show that a product $\prod \eta_{0,s}^{m(s)}$ is invariant under $\Gamma(N)$ if and only if it is invariant under $\Gamma_1(N)$. We have then only to copy the conditions given in Theorem 1 of [Ku].

In the subsequent discussion we suppose that m satisfies the conditions of the preceding proposition. Also if N is even we will always assume that $N\equiv 0 \bmod 4$.

Note that g^m, *when viewed as a modular function for* $\Gamma(N)$, has the property that all of its "translates" $g^m\circ\alpha\,(\alpha\in SL_2(\mathbf{Z}/N\mathbf{Z})$ have q-expansions with coefficients lying in $\mathbf{Z}[\zeta_N][1/N]$ and therefore g^m itself lies in the integral closure of $\mathbf{Z}[\zeta_N][1/N][j]$ in the rational function field of $X_1(N)_{/\mathbf{Q}[\zeta_N]}$. (Compare [39], Chap. 2, §5). But the integral closure alluded to is just the ring of regular functions on the affine scheme $Y_1(N)_{/\mathbf{Z}[\zeta_N][1/N]}$ and therefore we may view the Siegel functions as regular functions on $Y_1(N)_{/\mathbf{Z}[\zeta_N][1/N]}$.

One can easily determine the divisor of g^m on $X_1(N)_{/\mathbf{Q}[\zeta_N]}$ from the q-expansion (1) and the formula

$$\operatorname{ord}_{\sigma^{-1}\infty}(g_{0,s})=\operatorname{ord}_{\infty}(g_{(0,s)\sigma}) \quad \text{for} \quad \sigma\in SL_2(\mathbf{Z}/N\mathbf{Z}) \tag{2}$$

where the order on the left is with respect to $e^{2\pi i\sigma^{-1}(z)}$ (with the obvious meaning) and on the right with respect to $e^{2\pi iz}$. Using that the ramification index of $\begin{bmatrix}x\\y\end{bmatrix}$ on $X_1(N)$ over $X(1)$ is $N/(N,y)$ we obtain that at the cusp $\begin{bmatrix}x\\yd\end{bmatrix}$ with $d\mid N$, $(y,N)=1$,

$$\operatorname{ord}_{\left[\begin{smallmatrix}x\\yd\end{smallmatrix}\right]} g^m=\sum_{s\in\mathbf{Z}/N\mathbf{Z}} m(s)\cdot\frac{N}{2d}\cdot\mathbf{B}_2\left(\left\langle\frac{syd}{N}\right\rangle\right) \tag{3}$$

where here ord is taken with respect to a local parameter.

Consider the divisor (on the scheme $X_1(N)_{/\mathbf{Z}[\zeta_N]}$) of the rational function g^m. Let k' be a residue field of $\mathbf{Z}[\zeta_N]$ of characteristic p and note that $X_1(N)_{/k'}$ is the base change of $X_1(N)_{/k}$ to k'. Then one sees immediately from the q-expansion that the irreducible component $\Sigma^{\text{ét}}_{/k'}$ of $X_1(N)_{/k'}$ is not contained in the support of $\operatorname{div}(g^m)$.

It is possible, however, for other irreducible components of $X_1(N)_{/k'}$ to occur in the support of the divisor of g^m. The condition given in the proposition below insures that this does not happen:

Proposition 2. *Let m satisfy the hypotheses of Kubert's proposition 1. Suppose, further, that*

(i) $m(s)=0$ *if* $p\mid s$.

(ii) $\sum_{s\equiv 0 \bmod a} m(s)=0$.

Then the divisor (g^m) has support concentrated on the cuspidal sections of $X_1(N)_{/\mathbf{Z}[\zeta_N]}$.

Equivalently: *g^m is a unit in the ring of regular functions of the affine scheme $Y_1(N)_{/\mathbf{Z}[\zeta_N]}$.*

Proof. We shall work on the scheme $X(N)_{/\mathbf{Q}(\zeta_N)}$ where $\mathbf{Q}(\zeta_N)$ is viewed as a subfield of $\mathbf{C}$ by identifying ζ_N with $e^{2\pi i/N}$. Choose a residue field k_N of $\mathbf{Z}[\zeta_N]$ of characteristic p, and consider the fibre $X(N)_{/k_N}$. If $\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right]$ is a cusp of $X(N)$, let $\sum\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right]$ denote the irreducible component of $X(N)_{/k_N}$ containing the specialization of the cusp $\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right]$.

If h is a rational function on $X(N)_{/\mathbf{Q}(\zeta_N)}$ let *mult* $(h; \left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right])$ denote the multiplicity of the irreducible component $\sum\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right]$ in the divisor $\mathrm{div}(h)$.

If h is a general Siegel function (i.e., $h = \prod g_{(s_1,s_2)}^{m(s_1,s_2)}$ where $(s_1, s_2) \in \mathbf{Z} \times \mathbf{Z} - N\mathbf{Z} \times N\mathbf{Z}$ and m is zero for all but a finite number of pairs (s_1, s_2)) then

$$mult\left(\prod g_{(s_1,s_2)}^{m(s_1,s_2)}; \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right]\right) = \sum_{\substack{(s_1 s_2)\\ s_2 \equiv 0 \bmod N\\ s_1 \equiv 0 \bmod a}} \mathrm{ord}_\pi(1 - \zeta_N^{s_1}) \cdot m(s_1, s_2)$$

where $\pi = 1 - \zeta_N^a = 1 - \zeta_{p^n}$, as is easily seen from the formula (1) from which one can read off the constant terms of the q-expansions of $g_{(s_1,s_2)}$ at $\left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right]$.

One also easily obtains the formula

$$mult\ (g_{(0,s)}; \left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right]) = mult\ (g_{\alpha s, \beta s}; \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right])$$

from formula (2), [where we have allowed ourselves a mild abuse of notation since $g_{(0,s)}$ is not necessarily a function on $\Gamma(N)$].

Putting the above together, we have:

$$mult\left(\prod g_{(0,s)}^{m(s)}; \left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right]\right) = \sum_{\substack{s\\ \alpha s \equiv 0 (a)\\ \beta s \equiv 0 (N)}} \mathrm{ord}_\pi(1 - \zeta_N^{\alpha s})\, m(s).$$

But now, since (α, β, N) is the unit ideal, if $\alpha s \equiv 0 \bmod a$ and $\beta s \equiv 0 \bmod N$, it follows that $s \equiv 0 \bmod a$ so, writing $s = at$, we obtain:

$$mult\left(\prod g_{(0,s)}^{m(s)}; \left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right]\right) = \sum_{\beta t \equiv 0 \bmod p^n} \mathrm{ord}_\pi(1 - \zeta_{p^n}^{\alpha t})\, m(at) \tag{4}$$

which clearly vanishes for any $\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right]$ under the hypothesis of our proposition, and this completes the proof.

Note that the cusps of $\Sigma^{\text{ét}}$ have the form $\left[\begin{smallmatrix}x\\ yd\end{smallmatrix}\right]$ with $(d, p) = 1$, $d \mid N$ and $(y, N) = 1$. By formula (3) we have

$$\mathrm{ord}_{\left[\begin{smallmatrix}x\\ yd\end{smallmatrix}\right]} g^m = \mathrm{ord}_{\left[\begin{smallmatrix}x'\\ y'd\end{smallmatrix}\right]} g^m \tag{5}$$

if $y \equiv y' \bmod N/d$.

Let $\mathrm{div}_0(g^m)$ denote the restriction of the divisor of g^m to $\mathscr{Z}_n$, the zero-cusps in $\Sigma^{\text{ét}}$.

The divisor $\mathrm{div}_0 g^m$ is also given by (3),

$$\begin{aligned}\mathrm{div}_0 g^m &= \frac{N}{2} \sum_{(b,N)=1} \sum_{s \in \mathbf{Z}/N\mathbf{Z}} m(s)\, \mathbf{B}_2\left(\left\langle \frac{sb}{N} \right\rangle\right) \cdot \begin{bmatrix}0\\ b\end{bmatrix} \\ &= \sum_s m(s)\, \vartheta_2(s; N) \cdot \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right]\end{aligned} \tag{6}$$

where $\vartheta_2(s; N)$ is the second Stickelberger element (I, §1.5).

Recall that a cusp $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$ lies on $\tilde{\Sigma}^{\text{ét}}$ if and only if $(y, p) = 1$. Let D be the subgroup of the free abelian group $\{\sum a_i c_i \colon a_i \in \mathbf{Z}\}$ on the set $\{c_i\}$ of cusps on $\tilde{\Sigma}^{\text{ét}}$ satisfying

(i) $\Sigma a_i = 0$

(ii) $a_i = a_j$ if $c_i = \begin{bmatrix} x_i \\ y \end{bmatrix}$ and $c_j = \begin{bmatrix} x_j \\ y \end{bmatrix}$.

Then the **Z**-rank of D is seen to be 1 less than the cardinality of the set $\{y \in \mathbf{Z} \colon 0 < y \leqq (N/2), (y, p) = 1\}$. Note that D contains $\mathbf{Z}[\mathscr{Z}_n]^0$.

Let $\mathscr{F}$ be the group of *functions on* $\tilde{\Sigma}^{\text{ét}}$ of the form $\{c \cdot \prod g_{0,s}^{m(s)}\}$ with c a nontrivial constant, $m(s) = 0$ if $(s, p) \not\equiv 1$, $m(-s) = m(s)$, and $\sum_{s \equiv 0 \bmod a} m(s) = 0$. Let PD be the subgroup of D consisting of principal divisors.

Proposition 3. *The divisors of functions in $\mathscr{F}$ form a subgroup of PD of finite index prime to p.*

Proof. By (4) any function in $\mathscr{F}$ has its divisor in PD. We claim that to prove the proposition it is sufficient to show that if f is a function on $\tilde{\Sigma}^{\text{ét}}$ such that

$$f^p = c \cdot \prod g_{0,s}^{m(s)} \in \mathscr{F}, \tag{7}$$

then $f = c' \cdot \prod g_{0,s}^{m'(s)} \in \mathscr{F}$ with $pm' = m$. For applying this with $f = 1$ shows that the **Z**-rank of the group of functions $\mathscr{F}$ mod nontrivial constants is equal to the rank of D. Then applying it a second time shows that the quotient group of PD by the subgroup of divisors of functions in $\mathscr{F}$ has order prime to p.

Suppose then that $g^m = c \cdot \prod g_{0,s}^{m(s)} \in \mathscr{F}$ is a p^{th} power of a function on $\tilde{\Sigma}^{\text{ét}}$. Then the q-expansion of g^m, which we write in the form

$$q^{\frac{r}{N}}(1 + \alpha_1 \cdot q^{\frac{1}{N}} + \alpha_2 q^{\frac{2}{N}} + \cdots) \in \mathbf{F}_p[\![q]\!],$$

is also a p^{th} power. Recall that the q-expansion of $g_{0,s}$ has the form

$$g_{0,s} = -q^{\frac{t}{N}}(1 - q^{\frac{s}{N}}) \prod_{v=1}^{\infty} (1 - q^{v + \frac{s}{N}})(1 - q^{v - \frac{s}{N}})$$

for some integer t. Now using that g^m is a p^{th} power we must have that $\alpha_1 \equiv 0 (p)$. But $\alpha_1 = m(1) - m(N-1) = -2m(1)$, so also $m(1) \equiv 0 (p)$. Applying a diamond operator $\langle s \rangle$ to both sides of the equation in (6) shows that $m(s) \equiv 0 (p)$ for each s with $(s, N) = 1$. Now repeat the argument for α_d where d is the least prime divisor of N which is prime to p. This shows that $m(s) \equiv 0 (p)$ for each s such that $(s, N) = d$. Repeating the argument for each divisor of N which is prime to p in increasing order proves that $m(s) \equiv 0 (p)$ for each s. This establishes the proposition.

In order to study the pseudo-primitive components we now consider a modified version of Proposition 3. Let $D^{(r')}$ be the subgroup of the free abelian group $\{\sum a_i c_i \colon a_i \in \mathbf{Z}\}$ on the set $\{c_i\}$ of cusps of $\tilde{\Sigma}^{\text{ét}}$ satisfying

(i) $\sum a_i = 0$

(ii) $a_i = a_j$ if $c_i = \begin{bmatrix} x_i \\ y \end{bmatrix}$ and $c_j = \begin{bmatrix} x_j \\ y \end{bmatrix}$

(iii) $a_i = 0$ if $c_i = \begin{bmatrix} x_i \\ y \end{bmatrix}$ with $(y, r') > 1$.

Here r' may be taken to be any integer dividing N such that $r' = q_1 \cdots q_v$ for distinct primes q_i and $(r', N/r') = 1$. (Later we will choose r' to be a divisor of r, the integer associated to a pseudo-primitive component $\mathfrak{m}$, i.e., such that the basic character χ associated to $\mathfrak{m}$ has conductor ap/r).

The group $D^{(r')}$ is a subgroup of D. Its $\mathbf{Z}$-rank is one less than the cardinality of the set $\{y \in \mathbf{Z}: 0 < y \leqq N/2, (y, r'p) = 1\}$. Again $D^{(r')}$ contains $\mathbf{Z}[\mathscr{Z}_n]^0$. We let $PD^{(r')}$ be the subgroup of $D^{(r')}$ consisting of principal divisors.

Using the notation from the end of Chap. 1, §5,

$$\nu(t) = \prod_{q_i | t} q_i (n_{q_i})^{-1}$$
$$\mu(t) = (-1)^{d(t)}$$

where $d(t)$ is the number of distinct prime divisors of t, we let

$$f_{0,s} = f_{0,s}^{(r')} = \prod_{\substack{t | r' \\ (t,p)=1}} (g_{0,\nu(t)s})^{\mu(t)}$$

the product being taken over all the positive integers t which divide r' and are prime to p. We then let $\mathscr{F}^{(r')}$ be the subgroup of $\mathscr{F}$ consisting of functions which may be written in the form $c \cdot \prod f_{0,s}^{l(s)}$ with c a constant and $l(s) \in \mathbf{Z}$ and $l(s) = 0$ if $(s, rp) > 1$. We note that the divisor of $f^l = c \cdot \prod f_{0,s}^{l(s)}$ is given by (3), and in particular the restriction of this divisor to the zero cusps is given by

$$\mathrm{div}_0(f^l) = \sum l(s)\, \hat{\mathfrak{I}}^{(r')}(s; N) \cdot [{}^0_1] \tag{8}$$

Proposition 3$^{(r')}$. *The divisors of functions in $\mathscr{F}^{(r')}$ form a subgroup of $PD^{(r')}$ of finite index prime to p.*

Proof. Using (3) one verifies that any function in $\mathscr{F}^{(r')}$ has its divisor in $D^{(r')}$. As in the proof of Proposition 3, one checks that $\mathscr{F}^{(r')}$ has free rank equal to that of $D^{(r')}$, and so the divisors of these functions generate a subgroup of $PD^{(r')}$ of finite index. An application of (7) shows that the index is prime to p.

Let $\mathfrak{C}^{(n)}$ be the p-primary part of the subgroup of $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})(k)$ which is generated by the zero-cusps (the image of $s_p^{(n)}$ in the notation of §1). Then using the natural action of $R^{(n)} = \mathbf{Z}_p[(\mathbf{Z}/N\mathbf{Z})^*/(\pm 1)]$ (acting via the diamond operators) we may write $\mathfrak{C}^{(n)} = \bigoplus \mathfrak{C}_{\mathfrak{m}}^{(n)}$, the sum being taken over the components $\mathfrak{m}$ of $R^{(n)}$.

The action of $R^{(n)}$ on $\mathfrak{C}^{(n)}$ induces an action of $R_{\mathfrak{m}}^{(n)}$ on $\mathfrak{C}_{\mathfrak{m}}^{(n)}$. If $\mathfrak{m}$ is not associated to the trivial character then the elements of $R_{\mathfrak{m}}^{(n)}$, viewed as a subring of $R^{(n)}$, have degree zero. In this case, $\mathfrak{C}_{\mathfrak{m}}^{(n)} = R_{\mathfrak{m}}^{(n)} \cdot [{}^0_1]$ is a cyclic module. (Here we write $h_{\mathfrak{m}} \cdot [{}^0_1]$ where $h_{\mathfrak{m}} \in R_{\mathfrak{m}}^{(n)}$ for the element $\lim_{i \to \infty} (h_i \cdot [{}^0_1])_{\mathfrak{m}} \in \mathfrak{C}_{\mathfrak{m}}$ where $\{h_i\}$ is a sequence in $R^{(n)}$ such that $\lim_{i \to \infty} h_i = h_{\mathfrak{m}}$. More generally, if $\mathfrak{m}$ is not the trivial component, Δ is any divisor in $\mathbf{Z}[\mathscr{Z}_n]$, and $c \in \mathfrak{C}_{\mathfrak{m}}^{(n)}$ we write $\Delta_{\mathfrak{m}} \sim c$ if $s_{\mathfrak{m}}(\Delta) = c$.)

Proposition 4. *Suppose that $\mathfrak{m}$ is a pseudo-primitive component with basic character of conductor ap/r.*

(i) *If $\mathfrak{m}$ is not associated to the trivial character χ_0, nor to ω^{-2} if $a = 1$, then*

$$h_{\mathfrak{m}} \cdot [{}^0_1] = 0 \quad \textit{if and only if} \quad h_{\mathfrak{m}} \in (\hat{\mathfrak{I}}_{\mathfrak{m}}^{(r)}(1)).$$

(ii) *If* $\mathfrak{m}$ *is associated to the trivial character* χ_0 *and* $a>1$, *then*

$$h_{\mathfrak{m}} \cdot [{}^{0}_{1}] = 0 \quad \textit{if and only if} \quad h_{\mathfrak{m}} \in \{(1-\langle b\rangle)\,\hat{\vartheta}^{(r)}_{\mathfrak{m}}(1)\colon (b,N)=1\}\,.$$

In either case if $h_{\mathfrak{m}} \cdot [{}^{0}_{1}] = 0$ *then* $h_{\mathfrak{m}} \in \hat{S}'_{\mathfrak{m}}(ap^n)$.

Remark. The final assertion is true even without the hypothesis that $\mathfrak{m}$ is pseudo-primitive.

Proof. Suppose first that $\mathfrak{m}$ is not the trivial component. Then if $\mathfrak{m}$ is pseudo-primitive but not a-primitive one checks easily that $f_{0,1} = f^{(r)}_{0,1}$ satisfies the conditions of Proposition 2 and so is a function on $\hat{\Sigma}^{\text{ét}}$, provided that the conductor of the basic character χ associated to $\mathfrak{m}$ is not p. Here r is the integer for which the basic character associated to $\mathfrak{m}$ has conductor ap/r. Hence $\operatorname{div}(f_{0,1})_{\mathfrak{m}} \sim 0$. But since $\mathfrak{m}$ is pseudo-primitive

$$\operatorname{div}(f_{0,1})_{\mathfrak{m}} \sim \hat{\vartheta}^{(r)}_{\mathfrak{m}}(1) \cdot [{}^{0}_{1}]\,.$$

If the conductor of χ is p, we may choose a function $(f_{0,1}/f_{0,b})$ for some b prime to N and as $\mathfrak{m}$ is not trivial $(\langle b\rangle - 1)_{\mathfrak{m}}$ is a unit for a suitable choice of b.

If, on the other hand, $\mathfrak{m}$ is a-primitive, then suppose that $\mu\colon (\mathbf{Z}/N\mathbf{Z})^*/(\pm 1) \to \mathbf{Z}$ is any function such that

(i) $\sum_s \mu(\pm s)\, s^2 \equiv 0 (N)$ if N is odd and modulo $2N$ if N is even

(ii) $\sum_s \mu(\pm s) = 0$ if $a=1$

(iii) $\sum_s \mu(\pm s) \equiv 0$ modulo $v = 12/(N,12)$

the sum in each case being taken over all elements of $(\mathbf{Z}/N\mathbf{Z})^*/(\mp 1)$. Then by Proposition 2 if $m(s) = \mu(\pm s)$ for $(s,N)=1$, $m(s)=0$ otherwise, g^m is a function on $\tilde{\Sigma}^{\text{ét}}$ and has support on the cusps. For such a g^m

$$\operatorname{div}(g^m) \sim 0 \;\Rightarrow\; \left(\textstyle\sum \mu(s)[s]^{-1}_{\mathfrak{m}}\right) \hat{\vartheta}_{\mathfrak{m}}(1) \cdot [{}^{0}_{1}] = 0\,.$$

Assuming now that $\mathfrak{m}$ is not associated to ω^{-2} it is easy to show that the ideal of elements $\{\sum \mu(s)[s]^{-1}_{\mathfrak{m}}\}$ in $R_{\mathfrak{m}}$ obtained by taking all functions μ as above, is the unit ideal. Note that if $\mathfrak{m}$ is a-primitive, then $\hat{\vartheta}_{\mathfrak{m}}(1) = \hat{\vartheta}^{(r)}_{\mathfrak{m}}(1)$.

Finally, if $\mathfrak{m}$ is associated to the trivial character and $a>1$, then $f_{0,1}/f_{0,b}$ is a function on $\tilde{\Sigma}^{\text{ét}}$ for any b prime to N.

Conversely, if $\mathfrak{m}$ is any component and $h_{\mathfrak{m}}[{}^{0}_{1}] \sim 0$, then we can find $\delta \in R^{(n)}$ with $\delta \equiv h_{\mathfrak{m}} (\operatorname{mod} p^M)$ for M arbitrarily large, and satisfying $\delta \cdot [{}^{0}_{1}] \sim 0$. According to proposition $3^{(r)}$, $e\delta \cdot [{}^{0}_{1}] = \operatorname{div} f^l$ for some $f^l \in \mathscr{F}^{(r)}$, with e an integer prime to p. Then

$$\operatorname{div}(f^l) = \operatorname{div}_0(f^l) \in \hat{S}^{(r)}(N) \cdot [{}^{0}_{1}]\,.$$

If $\mathfrak{m}$ is pseudo-primitive and not associated to χ_0, nor to ω^{-2} if $a=1$, then by proposition 3(i) of chapter 1, §5, $\hat{S}^{(r)}_{\mathfrak{m}}(N) = (\hat{\vartheta}^{(r)}_{\mathfrak{m}}(1))$. If, on the other hand, $\mathfrak{m}$ is pseudo-primitive and associated to χ_0 then since f^l is a function one sees that in (8) we must have $\sum l(s) = 0$. (This is condition (ii) of proposition 2). It follows easily that $\operatorname{div}(f^l) \in \{(1-\langle b\rangle)\,\hat{\vartheta}^{(r)}(1)\colon (b,N)=1\}$.

Corollary . *If* $\mathfrak{m}$ *is a pseudo-primitive component not associated to the trivial character, nor to* ω^{-2} *if* $a=1$, *then*

$$\mathfrak{C}_{\mathfrak{m}}^{(n)} \xrightarrow{\sim} R_{\mathfrak{m}}^{(n)}/(\hat{\vartheta}_{\mathfrak{m}}^{(r)}(1))$$

as an $R_{\mathfrak{m}}^{(n)}$ *module.*

§ 3. A study of cuspidal groups

Let B_n be the canonical μ-deprived quotient abelian variety over $\mathbf{Q}$ derived from A_n, as in Chap. 3, §7, so that we have a natural isogeny

$$A_n \longrightarrow B_n$$

whose kernel is a finite group admitting a prolongation over the base $\mathcal{O}_{n,\mathfrak{m}}$ to a μ_p-type group scheme (see Chap. 3, §2).

Let $B_{n,\mathfrak{m}}$ denote the $\mathfrak{m}$-component of the p-divisible group associated to B_n, over $\mathcal{O}_{n,\mathfrak{m}}$.

(a) *Stabilized groups in characteristic* 0. For the remainder of this chapter we will suppose that $\mathfrak{m}$ is a pseudo-primitive component (cf. Chap. 1, §3). Thus a basic character χ of $\mathfrak{m}$ has conductor ap/r where $r=q_1\cdots q_\nu$ and each q_i divides ap "exactly once" (i.e., $q_i \| ap$) and that either $q_i \equiv 1 \bmod p$ or else $q_i = p$. We assume, moreover, that $\mathfrak{m} \notin \mathfrak{X}$ (cf. Chap. 1 §9). In particular, the second Stickelberger ideal $\hat{S}'_{\mathfrak{m}}(ap)$ is not the unit ideal.

The component $\mathfrak{m}$ may be principal or associated to the character ω^{-2}. In either of these cases the condition that $\hat{S}'_{\mathfrak{m}}(ap)$ be non-trivial implies that $a>1$.

If q divides r and $q \neq p$, let n_q be any integer such that $n_q \equiv q \bmod N/q$ and $n_q \equiv 1 \bmod q$. Note that if $q \neq p$ and Div (resp. Div^0) denotes the group of divisors (resp. of degree 0), then

$$(U_q - q[n_q])\,\mathrm{Div}(X) \subseteq \mathrm{Div}^0(X)$$

for $X = X_1(ap^n)$ or $X = \tilde{\Sigma}_n^{\text{ét}}$.

Formula (2) of §1 gives:

$$(U_q^2 - U_q)[^0_b] = q\langle n_q\rangle (U_q - 1)[^0_b] \tag{1}$$

$$(U_p^{n+1} - U_p^n)[^0_b] = p\langle n_p\rangle (U_p^n - U_p^{n-1})[^0_b]. \tag{2}$$

Lemma 0. (i) *The operator* U_p *fixes the image of*

$$U_p^{n-1}(U_p - p\langle n_p\rangle)\circ s^{(n)}\colon \mathbf{Z}[\mathscr{Z}_n] \to \{\mathrm{Pic}^0(\Sigma_n^{\text{ét}}) \times \mathrm{Pic}^0(\Sigma_n^{\mu})\}(k)$$

and of

$$U_p^{n-1}(U_p - p\langle n_p\rangle)\circ \xi^{(n)}\colon \mathbf{Z}[\mathscr{Z}_n] \to J_1(ap^n).$$

(ii) *If* $q \neq p$, $q \mid r$, *the operator* U_q *fixes the image of*

$$(U_q - q\langle n_q\rangle)\circ s^{(n)}\colon \mathbf{Z}[\mathscr{Z}_n] \to \mathrm{Pic}^0(\Sigma_n^{\text{ét}})(k)$$

and of

$$(U_q - q\langle n_q\rangle) \circ \xi^{(n)} \colon \mathbf{Z}[\mathscr{Z}_n] \to J_1(ap^n).$$

(iii) *If $q \mid a$, $q \nmid r$, the operator U_q fixes the image of*

$$s_{\mathfrak{m}}^{(n)} \colon \mathbf{Z}_p[\mathscr{Z}_n]^0 \to \mathrm{Pic}^0(\Sigma_n^{\text{ét}})_{\mathfrak{m}}(k)$$

and of

$$\xi_{\mathfrak{m}}^{(n)} \colon \mathbf{Z}_p[\mathscr{Z}_n]^0 \to J_1(ap^n).$$

Proof. Assertions (i), (ii) follows directly from formulas (1) and (2). To prove (iii), fix a prime $q \nmid pr$ such that q divides N. If d is an integer prime to N such that $d \equiv 1 \bmod N/q$, then $\langle d\rangle$ fixes any element x in the image of $(U_q - 1) \cdot s_{\mathfrak{m}}^{(n)}$ (by formula (1) of §1). Thus $[d]_{\mathfrak{m}} - 1$ annihilates x for all such d. But since the basic character χ belonging to $\mathfrak{m}$, which is of order prime to p, has the property that $\chi(d) \neq 1$ for some $d \not\equiv 1$, we have that $\{[d]_{\mathfrak{m}} - 1 \mid (d, N) = 1,\ d \equiv 1\ (N/q)\}$ generates the unit ideal in $R_{\mathfrak{m}}^{(n)}$, giving that $x = 0$.

If r' *is an integer dividing* r, let $\varepsilon_{r'}$ denote the operator.

$$\varepsilon_{r'} = U_p^{n-1} \prod_{q \mid pr'} (U_q - q\langle n_q\rangle).$$

Define the *r'-stabilized zero-cuspidal group* $C_{\mathfrak{m},r'}^{(n)}$ to be the finite subgroup of $B_{n,\mathfrak{m}}$ given by the image of the long arrow in the following diagram:

$$\begin{array}{ccccccccc}
\mathbf{Z}_p[\mathscr{Z}_n] & & \longrightarrow\!\!\!\!\!\!\rightarrow & & & & & & C_{\mathfrak{m},r'}^{(n)} \\
\downarrow & \subseteq & & & & & & & \downarrow \subseteq \\
\mathrm{Div}(X_1(ap^n)) \otimes \mathbf{Z}_p & \xrightarrow[\varepsilon_{r'}]{} & \mathrm{Div}^0(X_1(ap^n)) \otimes \mathbf{Z}_p & \longrightarrow & J_1(ap^n)_{\mathfrak{m}} & \longrightarrow & A_{n,\mathfrak{m}} & \longrightarrow & B_{n,\mathfrak{m}}
\end{array} \tag{3}$$

We view $C_{\mathfrak{m},r'}^{(n)}$ as a $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-module with trivial action, and $C_{\mathfrak{m},r'/\mathscr{O}_{m,n}}^{(n)}$ refers to the finite flat group scheme prolongation of $C_{\mathfrak{m},r'}^{(n)}$ in the abelian scheme $B_{n/\mathscr{O}_{m,n}}$.

Proposition 1. *The r'-stabilized zero-cuspidal group*

$$C_{\mathfrak{m},r'}^{(n)} \subseteq B_{n,\mathfrak{m}}(\mathbf{Q})$$

is preserved by the action of the following Hecke operators, the action being given by the formulae:

$$\begin{aligned}
&\langle l\rangle \cdot c = [l]_{\mathfrak{m}} \cdot c, \\
&T_l \cdot c = (l\,[l]_{\mathfrak{m}} + 1) \cdot c \quad \textit{for prime numbers } l \textit{ prime to } N, \\
&U_q \cdot c = c \quad \textit{for} \quad q \left| \frac{apr'}{r} \right..
\end{aligned}$$

The group schemes $C_{m,r'/\mathscr{O}_{m,n}}^{(n)}$ are étale. They are cyclic $R_{\mathfrak{m}}^{(n)}$-modules.

To show that $C^{(n)}_{\mathfrak{m},r'/\mathcal{O}_{\mathfrak{m},n}}$ is étale, we note that U_p acts as the identity on $C^{(n)}_{\mathfrak{m},r'}$ and therefore $C^{(n)}_{\mathfrak{m},r'}$ lies in $B_{n,\mathfrak{m},U_p-1}$ which is ordinary, since $A_{n,\mathfrak{m},U_p-1}$ is. (See Chap. 3: the proposition of §3 and Proposition 3 of §5.) But suppose $C^{(n)}_{\mathfrak{m},r'}$ were not étale. Since the $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ action on $C^{(n)}_{\mathfrak{m},r'}$ is trivial, there would then be a nontrivial μ_p-type subgroup scheme in $C^{(n)}_{\mathfrak{m},r'/\mathcal{O}}$ and consequently in $B_{n,\mathfrak{m}/\mathcal{O}}$, contradicting the fact that B_n is μ-deprived.

The $C^{(n)}_{\mathfrak{m},r'}$ are cyclic $R^{(n)}_{\mathfrak{m}}$-modules as can be seen from diagram (3).

Set $C^{(n)}_{\mathfrak{m}} = C^{(n)}_{\mathfrak{m},r}$.

Definition. *The basic ideal* $\mathfrak{b}^{(n)}_{\mathfrak{m}} \subseteq R^{(n)}_{\mathfrak{m}}$ *is the annihilator ideal of* $C^{(n)}_{\mathfrak{m}}$.

Theorem.

(i) $\prod_{\substack{q \mid r \\ q \neq p}} (q \cdot [n_q]_{\mathfrak{m}} - 1) \cdot \mathfrak{b}^{(n)}_{\mathfrak{m}} \subset \hat{S}'_{\mathfrak{m}}(ap^n)$.

(ii) *If* $\mathfrak{m}^{(n)}_{\mathfrak{m}}$ *is the maximal ideal of* $R^{(n)}_{\mathfrak{m}}$, *then*

$$(R^{(n)}_{\mathfrak{m}}/\mathfrak{b}^{(n)}_{\mathfrak{m}})[\mathfrak{m}^{(n)}_{\mathfrak{m}}]$$

is of dimension $\leqq 1$ *over* $R^{(n)}_{\mathfrak{m}}/\mathfrak{m}^{(n)}_{\mathfrak{m}}$.

The ring $R^{(n)}_{\mathfrak{m}}/\mathfrak{b}^{(n)}_{\mathfrak{m}}$ *is Gorenstein.*

The remainder of this chapter is devoted to the proof of this theorem.

Corollary. *Suppose that* $\hat{S}'_{\mathfrak{m}}(ap)$ *is not the unit ideal. Then the cuspidal group* $C^{(n)}_{\mathfrak{m}}$ *is nontrivial for n sufficiently large.*

Proof. This is the argument of the main theorem of Chap. 1 §9. Roughly speaking one checks that if $\mathfrak{m} \notin \mathfrak{X}$ then there are zeroes of the power series attached to $\hat{S}'_{\mathfrak{m}}(ap^{\infty})$ which are not attached to $y_{\mathfrak{m}}$ (cf. Proposition 2 and (2) of Chap. 1 §9).

Remark. We omit the details because we do not make essential use of this corollary. Our ultimate objective is to make the construction in (I) and (II) of Chap. 1 §9, and the required construction is trivial unless $C^{(n)}_{\mathfrak{m}}$ is non-zero as follows from the above theorem.

It is conceivable that even when $C^{(n)}_{\mathfrak{m}}$ is non-zero for large values of n, nevertheless it may be zero for small values of n. However it will be important for us that, under the hypothesis $\hat{S}'_{\mathfrak{m}}(ap)$ is not the unit ideal, the semi-stabilized group $C^{(n)}_{\mathfrak{m},r'}$ is always non-zero for $n \geqq 1$, (cf. Lemma 7 (ii) following).

(b) *Partially stabilized cuspidal groups in characteristic p.* Let $\mathfrak{C}^{(n)}_{\mathfrak{m}} \subset \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}_n)_{\mathfrak{m}}(k)$ denote the $\mathfrak{m}$-part of the subgroup of $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}_n)(k)$ generated by linear equivalence classes of divisors of degree zero which are supported on the zero-cusps. We view $\mathfrak{C}^{(n)}_{\mathfrak{m}}$ as a subgroup of

$$\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}_n)(k) \times \mathrm{Pic}^0(\tilde{\Sigma}^{\mu}_n)(k)$$

in the natural way.

For each divisor $r' \mid r$ we consider the *partially stabilized* cuspidal group $\mathscr{C}^{(n)}_{\mathfrak{m},r'}$ defined by the diagram:

$$\begin{array}{ccc} \mathbf{Z}_p[\mathscr{Z}_n] & \longrightarrow & \mathscr{C}^{(n)}_{\mathfrak{m},r'} \\ \downarrow \subseteq & & \downarrow \subseteq \\ \mathrm{Div}(\tilde{\Sigma}^{\text{ét}}_n) \otimes \mathbf{Z}_p & \xrightarrow[u_p^{n-1} \prod_{q \mid pr'} (U_q - q\langle n_q \rangle)]{} & \mathrm{Div}^0(\tilde{\Sigma}^{\text{ét}}_n \amalg \tilde{\Sigma}^{\mu}_n) \otimes \mathbf{Z}_p \to \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}_n)_{\mathfrak{m}} \times \mathrm{Pic}^0(\tilde{\Sigma}^{\mu}_n)_{\mathfrak{m}} \end{array}$$

where $u_p = u$ is the endomorphism of $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}^{\mu})$ studied in §3 of Chap. 3.

Let

$$\mathscr{D}^{(n)}_{\mathfrak{m},r'} \subseteq \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}_n)_{\mathfrak{m}}(k)$$

be the image of $\mathscr{C}^{(n)}_{\mathfrak{m},r'}$ under the natural projection

$$\mathrm{proj}_1 \colon \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}_n)_{\mathfrak{m}}(k) \times \mathrm{Pic}^0(\tilde{\Sigma}^{\mu}_n)_{\mathfrak{m}}(k) \to \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}_n)_{\mathfrak{m}}(k).$$

Set $$\mathscr{C}^{(n)}_{\mathfrak{m}} = \mathscr{C}^{(n)}_{\mathfrak{m},r}$$

and $$\mathscr{D}^{(n)}_{\mathfrak{m}} = \mathscr{D}^{(n)}_{\mathfrak{m},r}.$$

Lemma 1. *If*

$$(x, y) \in \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}_n)_{\mathfrak{m}}(k) \times \mathrm{Pic}^0(\tilde{\Sigma}^{\mu}_n)_{\mathfrak{m}}(k)$$

lies in $\mathscr{C}^{(n)}_{\mathfrak{m},r'}$, *then*

$$y = \sum_{k=0}^{\infty} p^k \langle n_p \rangle^k c_1(x).$$

Proof. This follows from the formula for u_p (Proposition 2 of §3 of Chap. 3; this is also where c_1 is defined) together with the relation $Fx = x$. Note that all but a finite number of terms in the above infinite sum vanish.

Lemma 2.

(i) $$\mathscr{D}^{(n)}_{\mathfrak{m},r'} = \prod_{\substack{q \mid r' \\ q \neq p}} (U_q - q[n_q]_{\mathfrak{m}}) \mathfrak{E}^{(n)}_{\mathfrak{m}}$$

(ii) *The homomorphisms*

$$\mathscr{D}^{(n)}_{\mathfrak{m},r'} \xrightarrow[u_p^{n-1}(u_p - p[n_p]_{\mathfrak{m}})]{} \mathscr{C}^{(n)}_{\mathfrak{m},r'}$$

and

$$\mathscr{C}^{(n)}_{\mathfrak{m},r'} \xrightarrow[proj_1]{} \mathscr{D}^{(n)}_{\mathfrak{m},r'}$$

are isomorphisms.

Proof. This follows easily from Proposition 2 of §3 of Chap 3. The right-hand side of (i) is contained in the first factor of $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}_n)_{\mathfrak{m}}(k) \times \mathrm{Pic}^0(\tilde{\Sigma}^{\mu}_n)_{\mathfrak{m}}(k)$. Moreover, $\mathrm{proj}_1 \circ u_p^{n-1}(u_p - p[n_p]_{\mathfrak{m}})$ is an automorphism of the right-hand side of (i). This proves (i). Assertion (ii) follows easily.

Let the subscript 0 denote the restriction of a divisor to the zero-cusps on $\tilde{\Sigma}^{\text{ét}}_n$, its "*zero-cuspidal part*". If h is any element of $\mathbf{Z}[(\mathbf{Z}/ap^n\mathbf{Z})^*/(\pm 1)]$, we have

Lemma 3. *The divisor*

$$h \cdot \prod_{\substack{q|r' \\ q \neq p}} (U_q - q\langle n_q \rangle) \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

is contained in the group of divisors $D^{(r/r')}$ *(introduced in the discussion of Proposition* $3^{(r')}$, *§2). The zero-cuspidal part is given by*

$$\left\{ h \cdot \prod_{\substack{q|r' \\ q \neq p}} (U_q - q\langle n_q \rangle) \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}_0 = h \cdot \prod_{\substack{q|r' \\ q \neq p}} (1 - q\langle n_q \rangle) \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Proof. The assertions follow immediately from the formulae for U_q.

Lemma 4. *If* $h \in R_{\mathfrak{m}}^{(n)}$ *annihilates the subgroup*

$$\mathscr{D}_{\mathfrak{m},r'}^{(n)} = \prod_{\substack{q|r' \\ q \neq p}} (U_q - q[n_q]_{\mathfrak{m}}) \mathfrak{E}_{\mathfrak{m}}^{(n)}$$

of $\mathrm{Pic}^0(\tilde{\Sigma}_n^{\text{ét}})(k)$ *then*

$$\prod_{\substack{q|r' \\ q \neq p}} (1 - q[n_q]_{\mathfrak{m}}) \cdot h \in \hat{S}_{\mathfrak{m}}^{(r/r')}(ap^n).$$

Proof. Using Lemma 3, the argument of Proposition 4, §2, may be adapted to prove Lemma 4.

Briefly, we may "approximate" h by an element $\tilde{h} \in \mathbf{Z}[(\mathbf{Z}/N\mathbf{Z})^*/(\pm 1)]$ such that

$$\delta = \tilde{h} \cdot \prod_{\substack{q|r' \\ q \neq p}} (U_q - q\langle n_q \rangle) \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

is a divisor of degree zero on $\tilde{\Sigma}_n^{\text{ét}}$ which is linearly equivalent to zero. It then follows by Lemma 4 and Proposition 3 of §2 that there is an integer e prime to p such that $e \cdot \delta = (f^m)$ for a suitable function f^m. But by (8) of §2, $\mathrm{div}_0(f_m)$ is given by $\sum_s m(s) \hat{\vartheta}_2^{(r/r')}(s; N) \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, while the zero-cuspidal part of δ is given by

$$h \cdot \prod_{\substack{q|r' \\ q \neq p}} (1 - q\langle n_q \rangle) \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Since $\hat{S}_m^{(r/r')}(ap^n)$ is a closed ideal, Lemma 4 follows.

(c) *Eisenstein maximal ideals.* If $\mathbf{T}^{(n)}$ denotes the Hecke algebra acting on A_{n/k_n}, note that we may also view $\mathbf{T}^{(n)}$ as a ring of endomorphisms of

$$\mathrm{Pic}^0(\tilde{\Sigma}_n^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}_n^{\mu}),$$

the action being compatible with the isogeny

$$\mathrm{Pic}^0(\tilde{\Sigma}_n^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}_n^{\mu}) \xrightarrow[\sigma_n]{} A_{n/k_n}.$$

Let $P_n \subseteq \mathbf{T}_{\mathfrak{m}}^{(n)}$ be the associated *Eisenstein "maximal"* ideal;[6]) that is, P_n is generated by

$$\{T_l - 1 - l\langle l\rangle, U_q - 1 \quad (\text{for } q|N), \quad \langle r\rangle - [r]_{\mathfrak{m}}, \mathfrak{p}_n\},$$

where $\mathfrak{p}_n$ is the image in $\mathbf{T}_{\mathfrak{m}}^{(n)}$ of the maximal ideal of $R_{\mathfrak{m}}^{(n)}$.

Consider the p-divisible group over $\mathcal{O} = \mathbf{Z}_p[\zeta_{p^n}]$:

$$A_{n,P_n} = \bigcup_{\nu=1}^{\infty} A_n[P_n^{\nu}]_{/\mathcal{O}};$$

and the étale p-divisible group over k,

$$\Gamma^{(n)\text{ét}} = \{\mathrm{Pic}^0(\tilde{\Sigma}_n^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}_n^{\mu})\}_{P_n}^{\text{ét}}$$

$$= \bigcup_{\nu=1}^{\infty} \{\mathrm{Pic}^0(\tilde{\Sigma}_n^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}_n^{\mu})\}[P_n^{\nu}]^{\text{ét}}.$$

The natural mappings induce a commutative diagram of étale p-divisible group schemes over k:

$$\begin{array}{ccccc} \Gamma^{(n)\text{ét}} & \xrightarrow{\sigma_n^{\text{ét}}} & A_{n,P_n/k}^{\text{ét}} & \xrightarrow{\cong} & B_{n,P_n/k}^{\text{ét}} \\ \uparrow & & \uparrow & & \uparrow \\ \Gamma^{(1)\text{ét}} & \xrightarrow{\sigma_1^{\text{ét}}} & A_{1,P_{1/k}}^{\text{ét}} & \xrightarrow{\cong} & B_{1,P_{1/k}}^{\text{ét}}. \end{array} \tag{4}$$

Lemma 5. *The vertical mappings in (4) are injections.*

Proof. For injectivity of the right-hand vertical map, see Chap. 6, § 6.

To see injectivity of the left-hand vertical mapping, consider the *étale* p-divisible part of $\{\mathrm{Pic}^0(\tilde{\Sigma}_n^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}_n^{\mu})\}_{P_n/k_n}$. By Proposition 3 of Chap. 3, § 3, the desired injectivity would follows if $\mathrm{Pic}^0(\tilde{\Sigma}_1^{\text{ét}})_{P/k_n}^{\text{ét}} \to \mathrm{Pic}^0(\tilde{\Sigma}_n^{\text{ét}})_{P/k_n}^{\text{ét}}$ were injective, or equivalently, if

$$\mathrm{Pic}^0(\tilde{\Sigma}_1^{\text{ét}})(\bar{k}_n) \to \mathrm{Pic}^0(\tilde{\Sigma}_n^{\text{ét}})(\bar{k}_n)$$

were injective. But by Proposition 1 of Chap. II, §8.1, the mapping β_0 identifies the above morphism with the mapping

$$\mathrm{Pic}^0(Igusa(ap))(\bar{k}_n) \to \mathrm{Pic}^0(Igusa(ap^n))(\bar{k}_n) \tag{5}$$

induced from the natural projection

$$Igusa(ap^n) \to Igusa(ap). \tag{6}$$

But (6) is totally ramified at the supersingular points, and therefore (5) is injective.

Lemma 6. *The p-divisible groups $\Gamma^{(n)\text{ét}}$ are nontrivial for $n \leqq 1$. The ideals P_n are proper for $n \geqq 1$.*

---

[6] The reason for the quotation marks around the word maximal is that it is not yet evident that P_n is a *proper* ideal. See Lemma 6 below

Proof. The second assertion follows from the first. Moreover, since $\Gamma^{(1)\text{ét}} \to \Gamma^{(n)\text{ét}}$ is injective by Lemma 5, it is enough to show that $\Gamma^{(1)\text{ét}} \neq 0$.

For this, let χ be a basic character belonging to $\mathfrak{m}$, and let us fix

$$r' = \prod_{\substack{q|r \\ \chi(n_q)\neq 1}} q$$

for the remainder of this proof. Lemma 6 follows from

Lemma 7.

(i) *$\mathscr{C}^{(n)}_{\mathfrak{m},r'}$ is annihilated by a power of P_n; $\mathscr{C}^{(n)}_{\mathfrak{m},r'} \subset \Gamma^{(n)\text{ét}}(k_n)$*

(ii) *the $R^{(1)}_{\mathfrak{m}}$-annihilator of $\mathscr{C}^{(1)}_{\mathfrak{m},r'}$ is contained in $\hat{S}^{(r/r')}_{\mathfrak{m}}(ap)$, and hence also in $\hat{S}'_{\mathfrak{m}}(ap)$.*

This will establish nontriviality of $\Gamma^{(1)\text{ét}}$, since by our hypothesis, $\hat{S}'_{\mathfrak{m}}(ap)$ is not the unit ideal.

Proof of (i): We must show that a power of P_n annihilates $\mathscr{C}^{(n)}_{\mathfrak{m},r'}$. But a power of $\mathfrak{p}_n$ annihilates $\mathscr{C}^{(n)}_{\mathfrak{m},r'}$ and the operators

$$\begin{aligned} &T_l - 1 - l\langle l\rangle && l \nmid N \\ &\langle x\rangle - [x]_{\mathfrak{m}} && (x, N) = 1. \end{aligned}$$

$$U_q - 1 \begin{cases} q = p & \text{(Lemma 1 (i))} \\ q \neq p \quad q \,\Big|\, \dfrac{ap}{r} & \text{(Lemma 1 (iii))} \\ q \mid r' & \text{(Lemma 1 (ii)} \end{cases}$$

all annihilate $\mathscr{C}^{(n)}_{\mathfrak{m},r'}$.

We now consider the operators $U_q - 1$ for $q \neq p$, $q \mid r$, and such that $\chi(n_q) = 1$. Since $\chi(n_q) = 1$, we have that $[n_q]_{\mathfrak{m}} - 1 \in \mathfrak{p}_n$. Recall that if $q \mid r$, then $q - 1$ is divisible by p. Therefore $(U_q - 1)(U_q - q[n_q]_{\mathfrak{m}})$, which annihilates $\mathscr{C}^{(n)}_{\mathfrak{m},r'}$, may be expressed as

$$(U_q - 1)(U_q - q[n_q]_{\mathfrak{m}}) = (U_q - 1)^2 + (U_q - 1) \circ x$$

where $x \in \mathfrak{p}_n$. It follows that a power of $U_q - 1$ annihilates $\mathscr{C}^{(n)}_{\mathfrak{m},r'}$.

Proof of (ii). By Lemma 2, it is equivalent to study the $R^{(1)}_{\mathfrak{m}}$-annihilator of $\mathscr{D}^{(n)}_{\mathfrak{m},r'}$. But by our choice of r' the element

$$\prod_{\substack{q|r' \\ q\neq p}} (1 - q[n_q]_{\mathfrak{m}})$$

is a unit in $R^{(1)}_{\mathfrak{m}}$, and so Lemma 4 implies (ii).

Proposition 2. *The mapping*

$$\sigma^{\text{ét}}_n : \quad \Gamma^{(n)\text{ét}} \to A^{\text{ét}}_{n, P_n/k}$$

is an isomorphism of p-divisible groups, for $n \geqq 1$.

Proof. Since $\sigma_n^{\text{ét}}$ is an isogeny, it suffices to show that

$$\sigma_n^{\text{ét}}: \quad \Gamma^{(n)\text{ét}}[P_n] \to A_{n/k}[P_n]^{\text{ét}} \tag{8}$$

is injective. But by the q-expansion principle (Chap. 3, §3, Prob. 4′) we have:

Lemma 8. *$\Gamma^{(n)\text{ét}}[P_n](\bar{k})$ is cyclic as a module over*

$$\mathbf{T}^{(n)}/P_n \cong R_{\mathfrak{m}}^{(n)}/\mathfrak{m}_n \cong R_{\mathfrak{m}}^{(1)}/\mathfrak{m}_1 .$$

Now, since $\Gamma^{(1)(\text{ét})} \to \Gamma^{(n)(\text{ét})}$ is injective, and $\Gamma^{(1)(\text{ét})}$ is nontrivial (Lemma 6) we have an isomorphism of (cyclic) $R_{\mathfrak{m}}^{(1)}/\mathfrak{p}_1$-modules:

$$\Gamma^{(1)(\text{ét})}[P_1](\bar{k}) \xrightarrow{\cong} \Gamma^{(n)\text{ét}}[P_n^n](\bar{k}).$$

It follows that it suffices to show injectivity of (8) for $n = 1$, but this comes from Proposition 4 of §2 of Chap. 3.

Corollary. *The mapping*

$$\mathscr{C}_{\mathfrak{m}}^{(n)} \xrightarrow{\sigma_n} C_{\mathfrak{m}}^{(n)}(k)$$

is an isomorphism for all $n \geqq 1$.

(d) *Proof of the theorem*: Collecting what has already been proven, we have the surjections and isomorphisms

$$\mathfrak{E}_{\mathfrak{m}}^{(n)} \xrightarrow[\substack{\prod_{q|r,\ q\neq p} (U_q - q[n_q]_{\mathfrak{m}})}]{} \mathscr{D}_{\mathfrak{m}}^{(n)} \xrightarrow[\cong]{} \mathscr{C}_{\mathfrak{m}}^{(n)} \cong C_{\mathfrak{m}}^{(n)}(k) \cong C_{\mathfrak{m}}^{(n)}(\mathscr{O})$$

(Lemma 2, the corollary to Proposition 2, and Proposition 1).

To prove (i) we simply apply Lemma 4 with $r' = r$, and use that (by definition) $\mathfrak{b}_{\mathfrak{m}}^{(n)}$ is the annihilator of $C_{\mathfrak{m}}^{(n)}(\mathscr{O})$. As for part (ii), we must show that $C_{\mathfrak{m}}^{(n)}(k)[P_n]$ is of dimension $\leqq 1$ over $\mathbf{T}_{\mathfrak{m}}^{(n)}/P_n$ (Lemma 8). But $C_{\mathfrak{m}}^{(n)}(k)[P_n] \cong \mathscr{D}_{\mathfrak{m}}^{(n)}[P_n] \subseteq \Gamma^{(n)\text{ét}}[P_n](\bar{k})$ which is of dimension one over $\mathbf{T}_{\mathfrak{m}}^{(n)}/P_n$.

Chapter 5. The kernel of the Eisenstein ideal

§ 1. The basic sequence

The stabilized cuspidal group $C_{\mathfrak{m}}^{(n)}$ defined in Chap. 4, §3 is stable under the action of $\mathbf{T}_{\mathfrak{m}}^{(n)}$ by Proposition 1 of §3 of Chap. 4.

Define the *(stabilized) Eisenstein ideal* $I_{\mathfrak{m}}^{(n)} \subset \mathbf{T}_{\mathfrak{m}}^{(n)}$ to be the annihilator ideal of $C_{\mathfrak{m}}^{(n)}$. Thus, by the proposition just quoted, $I_{\mathfrak{m}}^{(n)}$ is the ideal generated by $T_l - 1 - l\langle l\rangle$

for $l \nmid N$, $U_q - 1$ for $q \mid N$, $\langle r \rangle - [r]_{\mathfrak{m}}$, and the image of the "basic ideal" $\mathfrak{b}_{\mathfrak{m}}^{(n)}$ in $\mathbf{T}_{\mathfrak{m}}^{(n)}$. (For the definition of this ideal see Chap. 4, §3).

If $C_{\mathfrak{m}}^{(n)}$ is nontrivial, then $I_{\mathfrak{m}}^{(n)}$ is not the unit-ideal and is primary to the maximal Eisenstein ideal P_n.

Note that the natural mapping $R_{\mathfrak{m}}^{(n)}/\mathfrak{b}_{\mathfrak{m}}^{(n)} \to \mathbf{T}_{\mathfrak{m}}^{(n)}/I_{\mathfrak{m}}^{(n)}$ is an isomorphism.

To simplify our notation, we fix an n such that $C_{\mathfrak{m}}^{(n)} \neq 0$, and we drop the sub- or superscript (n), in most cases. Thus $I_{\mathfrak{m}}^{(n)} = I_{\mathfrak{m}} = I$, $P_n = P$, etc.

Let $\mathrm{E}_{\mathfrak{m}}$ denote the kernel of the Eisenstein ideal $I = I_{\mathfrak{m}}$ in the $\bar{\mathbf{Q}}$-rational points of the p-divisible group scheme B_p associated to the abelian variety $B/_{\mathbf{Q}}$. We may write:

$$\mathrm{E}_{\mathfrak{m}} = B_P[I] = B_p[I] = B_p[I \cdot \mathbf{T}_p]$$

and we view the above finite abelian p-group as endowed with its natural structure as a bimodule (I, §8). More precisely, it has a natural module structure over the ring

$$\mathbf{T}_p/I \cdot \mathbf{T}_p = R_{\mathfrak{m}}^{(n)}/\mathfrak{b}_{\mathfrak{m}}^{(n)}$$

and it also has a natural action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ which commutes with its $R_{\mathfrak{m}}^{(\infty)}$-action.

Let F and S be as in Chap. 3, §7, i.e. $F = \mathbf{Q}(\zeta_{pn})$ and $S = \mathcal{O}(F)[1/a]$. If we restrict the $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ action to $\mathrm{Gal}(\bar{\mathbf{Q}}/F)$, the Galois module $\mathrm{E}_{\mathfrak{m}}$ over F extends to a finite flat group scheme over S (since A and hence also B acquired good reduction over S), and we denote this finite flat group scheme $\mathrm{E}_{\mathfrak{m}/S}$.

The $\mathfrak{m}$-part of the cuspidal group $C_{\mathfrak{m}}^{(n)}$ is contained in $\mathrm{E}_{\mathfrak{m}}$. Let $M_{\mathfrak{m}/S}$ denote the cokernel of the morphism $C_{\mathfrak{m}/S} \to \mathrm{E}_{\mathfrak{m}/S}$ and let $M_{\mathfrak{m}}$ denote the finite abelian group of $\bar{\mathbf{Q}}$-rational points of the group scheme $M_{\mathfrak{m}/S}$.

We then have an exact sequence of finite abelian groups

$$0 \to C_{\mathfrak{m}} \to \mathrm{E}_{\mathfrak{m}} \to M_{\mathfrak{m}} \to 0 \tag{*}$$

and $M_{\mathfrak{m}}$ may be given the structure of a *bimodule* in such a way that (*) becomes an exact sequence of bimodules. These groups are just the $\bar{\mathbf{Q}}$-rational points of the corresponding exact sequence of finite flat group schemes over S:

$$0 \to C_{\mathfrak{m}/S} \to \mathrm{E}_{\mathfrak{m}/S} \to M_{\mathfrak{m}/S} \to 0. \tag{**}$$

We refer to (**) as the *basic sequence.*

§ 2. The étale part of the kernel of the Eisenstein ideal

Let $s = \mathrm{Spec}(\mathbf{F}_p)$ be the point of S of characteristic p, and let $\bar{s} = \mathrm{Spec}(\bar{\mathbf{F}}_p)$ be a geometric point lying above s.

Let $\Gamma = \{\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}^{\mu})\}_p$ denote the P-divisible group scheme over s associated to the abelian variety $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}^{\mu})$.

By Proposition 3 of Chap. 3, §3, Γ is ordinary.

Lemma 1. *The group scheme over s, $\Gamma^{\text{ét}}[P]$ is a $\mathbf{T}/P$-"vector space" group scheme of "$\mathbf{T}/P$-rank" $\leqq 1$.*

Proof. This follows from the q-expansion principle, (Prop. 4′, in §3, of Chap. 3) and the fact that $u_p^* - 1 \in P$.

Lemma 2. *The Tate module* $\mathrm{Ta}^*(\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})_p^{\text{ét}})$ *is a* cyclic $\mathbf{T}_p$*-module. The étale group scheme* $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})^{\text{ét}}[\mathrm{I}]$ *is of order* $\leqq$ *the cardinality of* $\mathbf{T}/\mathrm{I}$.

Proof. We remind the reader that $\tilde{\Sigma}^{\text{ét}}$ is the normalization of one of the two good components of the special fibre of $X_1(ap^n)$, that $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})_P$ is the P-divisible group over s associated to $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})$, and that $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})_P^{\text{ét}}$ is the canonical étale quotient of $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})_P$.

Lemma 2 follows directly from Lemma 1 since the Pontrjagin dual of the group of $\bar{s}$-valued points of $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})_P^{\text{ét}}[P]$ is isomorphic to $Ta^*(\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})_P^{\text{ét}})/P \cdot Ta^*(\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})_P^{\text{ét}})$.

Let $\mathscr{C}_{\mathfrak{m}/s}$ denote the stabilized cuspidal group on $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}^{\mu})$, that is the image of the cuspidal group $\mathscr{D}_{\mathfrak{m},r}$ on $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})(\bar{k})$ under $(U_p)^{n-1}(U_p - p\langle n_p\rangle)$. Since this image is in the kernel of $(U_p - 1)$ the formula of Proposition 3 of Chap. 3, §3, shows that $\mathscr{C}_{\mathfrak{m}/s}$ lies on the first factor $\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})^{\text{ét}}$. Consider the following line of morphisms of group schemes over s:

$$\begin{array}{ccccc} \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})^{\text{ét}}[I] & \longrightarrow & (A_n[I]_{/s})^{\text{ét}} & \xrightarrow{\gamma} & (B[I]_{/s})^{\text{ét}} \\ \uparrow & & \uparrow & & \\ \mathscr{C}_{\mathfrak{m}/s} & \longrightarrow & C_{\mathfrak{m}/s} & & \end{array} \tag{3}$$

where the left-hand horizontal maps are induced by σ_n (cf. Prop. 2 of §3 of Chap. 4). We also have the morphisms of Tate modules of P-divisible groups over s:

$$Ta^*(B_{P/s}^{\text{ét}}) \xrightarrow{\delta} Ta^*(A_{P/s}^{\text{ét}}) \longrightarrow Ta^*(\mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})_P^{\text{ét}}).$$

Lemma 3. *All the morphisms of (3) and (4) are isomorphisms. In particular* $C_{\mathfrak{m}/s} = (B[I]_{/s})^{\text{ét}}$.

Proof. We know that γ is an isomorphism since the isogeny $A_{/S} \to B_{/S}$ has a kernel a group scheme of multiplicative type by construction of B (cf. Chap. 3, §7). Recall that $C_{\mathfrak{m}/S}$ is étale (Proposition 1 of §3 of Chap. 4). The mapping $\mathscr{C}_{\mathfrak{m}/S} \to C_{\mathfrak{m}/S}$ is an isomorphism by the corollary of Proposition 2, §3, of Chap. 4. Since the Eisenstein ideal I is the annihilator of $C_{\mathfrak{m}/S}$, the injection $\mathscr{C}_{\mathfrak{m}/s} \hookrightarrow \mathrm{Pic}^0(\tilde{\Sigma}^{\text{ét}})^{\text{ét}}[I]$ is an isomorphism by Lemma 2. The top left-hand morphism in (3) is an isomorphism by Proposition 2 of §3 of Chap. 4. One proves that the mappings in (4) are isomorphisms similarly.

Heaving just proved that $C_{\mathfrak{m}/s} = B[I]_{/s}^{\text{ét}}$ we immediately deduce the following.

Lemma 4. *The finite flat group scheme* $M_{\mathfrak{m}/s}$ *is of multiplicative type.*

Proof. The finite flat group scheme $B[I]_{/s}$ is ordinary and its étale part is $C_{\mathfrak{m}/s}$.

Let F_s denote the completion of the field F at s, and let $\mathcal{O}_s = \mathcal{O}(F_s)$ denote its ring of integers. Consider the multiplicative-type parts of the p-divisible groups $A_{P/\mathcal{O}_s}$ and $B_{P/\mathcal{O}_s}$, and denote them, as usual, $A_{P/\mathcal{O}_s}^{\text{m.t.}}$, and $B_{P/\mathcal{O}_s}^{\text{m.t.}}$ respectively.

Notation. *Set* $\mathfrak{X} = Ta^*(B_{P/F_s}^{\text{m.t.}})$, *and view* $\mathfrak{X}$ *as a module over the ring* $\mathbf{T}_P$. *We also consider* $\mathrm{Hom}(M_{\mathfrak{m}}; \mathbf{Q}_p/\mathbf{Z}_p)$ *as* $\mathbf{T}_p$*-module in the natural way; namely, if* $f \in \mathrm{Hom}(M_{\mathfrak{m}}; \mathbf{Q}_p/\mathbf{Z}_p)$, $t \in \mathbf{T}_p$, *then* $(tf)(m) = f(tm)$.

Proposition 1. *The $\mathbf{T}_p$-module $\mathfrak{X}$ is faithful. We have an isomorphism of $\mathbf{T}_p$-modules*

$$\mathfrak{X}/I_p \cdot \mathfrak{X} = \mathrm{Hom}(M_{\mathfrak{m}}, \mathbf{Q}_p/\mathbf{Z}_p).$$

Proof. The faithfulness of $\mathfrak{X}$ as a $\mathbf{T}_p$-module follows from Corollary 2 of §2 of Chap. 3. The asserted isomorphism comes from the identification of the group scheme $M_{\mathfrak{m}/\mathcal{O}_S}$ with the maximal multiplicative-type subgroup scheme in $B_p[I]_{/\mathcal{O}_S}$, using Lemma 4. More precisely, since

$$M_{\mathfrak{m}/\mathcal{O}_S} = (B_p[I]_{/\mathcal{O}_S})^{\mathrm{m.t.}} = B^{\mathrm{m.t.}}_{P/\mathcal{O}_S}[I]$$

our assertion follows from the elementary fact that if A is a p-divisible group over F which is also a $\mathbf{T}_p$-module, then the modules

$$Ta^*(A_{/F})/I_p \cdot Ta^*(A_{/F})$$

and $A(\bar{F})[I_p]$ (the kernel of I_p in $A(\bar{F})$) are in perfect Pontrjagin duality.

We end this paragraph with a comparison of the kernel of the Eisenstein maximal ideal in various cuspidal groups. For this, let

$$r' = \prod_{\substack{q|r \\ \chi(n_q)\neq 1}} q \tag{5}$$

and let n be large enough to that $C^{(n)}_{\mathfrak{m}} \neq 0$, cf. the corollary to the Theorem of §8 of Chap. 4. Consider the natural map

$$i_n\colon\ C^{(1)}_{\mathfrak{m},r'}[P_1] \to C^{(n)}_{\mathfrak{m},r'}[P_n]$$

which is injective.

Proposition 2. *The mapping i_n is an isomorphism and the group $C^{(n)}_{\mathfrak{m},r'}[P_n] = i_n \cdot C^{(1)}_{\mathfrak{m},r'}[P_1]$ is equal to $C^{(n)}_{\mathfrak{m}}[P_n]$, these being $\mathbf{T}^{(n)}_{\mathfrak{m}}/P_n$-vector spaces of dimension one.*

Proof. The three groups referred to in the statement of our proposition have trivial Galois action and are contained in $B[P_n]$. Since the étale part of $B[P_n]_{/S}$ is $C^{(n)}_{\mathfrak{m}}[P_n]_{/S}$, for any $\mathbf{Q}$-valued point c of $C^{(n)}_{\mathfrak{m},r'}[P_n]$, there is a $\mathbf{Q}$-valued point d of $C^{(n)}_{\mathfrak{m}}[P_n]$ such that $c-d$, when lifted to the base S, specializes to zero at the point s. If $c \neq d$, the section $c-d$ then generates a subgroup scheme of $B[P_n]$ of order p, necessarily of multiplicative type. But B is μ-deprived and consequently $c = d$. It follows that

$$0 \neq i_n C^{(n)}_{\mathfrak{m},r'}[P_1] \subset C^{(n)}_{\mathfrak{m},r'}[P_n] \subset C^{(n)}_{\mathfrak{m}}[P_n].$$

But $C^{(n)}_{\mathfrak{m}}[P_n]$ is a $\mathbf{T}^{(n)}_{\mathfrak{m}}/P_n$-vector space of dimensional 1. The Proposition follows.

§ 3. The multiplicative-type part of the kernel of the Eisenstein ideal

Recall the morphism

$$\eta_1\colon\ \mathbf{Z}_p[\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})] \to R^{(\infty)}_{\mathfrak{m}}$$

which sends the l-Frobenius element Φ_l to $l \cdot [l]_{\mathfrak{m}}$ (see Chap. 1, §4).

Let

$$\mathfrak{x}\colon \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to k_{\mathfrak{m}}^*$$

be the $k_{\mathfrak{m}}$-valued character obtained by composition of η_1 with the natural morphism to $k_{\mathfrak{m}}^*$:

$$\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \xrightarrow[\eta_1]{} R_{\mathfrak{m}}^{(\infty)*} \longrightarrow k_{\mathfrak{m}}^*.$$

Note that $B[I]$ and hence also $M_{\mathfrak{m}}$ satisfies the Eichler-Shimura formula ([13, 67]). Since I annihilates $M_{\mathfrak{m}}$, the Eichler-Shimura formula can be expressed in the following way:

$$(\Phi_l - 1)(\Phi_l - \eta_1(\Phi_l)) = 0 \tag{1}$$

for l any prime number not dividing ap, and Φ_l any choice of l-Frobenius element in $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$.

Definition. *A bimodule will be called simple if it is simple as an $R_{\mathfrak{m}}^{(\infty)}$-module; equivalently, if it is annihilated by the maximal ideal in $R_{\mathfrak{m}}^{(\infty)}$ and is of dimension one as a $k_{\mathfrak{m}}$-vector space.*

Any simple bimodule has the property that its $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-action is given by a $k_{\mathfrak{m}}$-valued character on $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, $y\colon \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to k_{\mathfrak{m}}^*$. Such a simple bimodule will be called of type y. We refer to the trivial character as 1.

We begin with some preliminaries on bimodules.

Lemma 1. *Suppose X is a bimodule having a filtration such that every subquotient is of type 1. Suppose further that X is annihilated by I. Then the action of* $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ *on X is trivial.*

Proof. Consider the subgroup $G_0 \subset \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ consisting of elements g such that $\mathfrak{x}(g) = 1$. Then G_0 is an open and closed proper subgroup. Its complement D in $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ generates $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ as a group. If l is a prime number not dividing ap such that there is an l-Frobenius element which lies in D, one sees that the endomorphism $\Phi_l - \eta_1(\Phi_l)$ of X must have trivial kernel. (This is because on any element of the kernel $\Phi_l - 1$ is nilpotent by the hypothesis on X.) So $\Phi_l - \eta_1(\Phi_l)$ is an automorphism of X and then by the Eichler-Shimura relation (1) $\Phi_l = 1$ on X. By the Cebotarev density theorem every element of D acts trivially on X. Since D generates $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, X has trivial Galois action, and the lemma is proved.

If we impose the stronger condition that X is annihilated by P we obtain that $X \xrightarrow{\sim} \bigoplus_{i=1}^{t} k_{\mathfrak{m}}$ with trivial Galois action. A similar proof to the above in the case where each successive subquotient is of type $\mathfrak{x}$ yields the following:

Lemma 2. *Suppose X is a bimodule having a filtration such that every subquotient is of type $\mathfrak{x}$. Suppose further that X is annihilated by I. Then*

$$gx = \eta_1(g)\mathrm{x} \quad \textit{for every} \quad x \in X, g \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}). \tag{2}$$

Again we note that if we impose the condition that X is annihilated by P we obtain that $X \xrightarrow{\sim} \bigoplus_{i=1}^{t} k_{\mathfrak{m}}$ where the action on each $k_{\mathfrak{m}}$ is via the character $\mathfrak{x}$.

From the argument of ([47], p. 114) or ([67], §4), using the Brauer-Nesbitt theorem, one sees that $M_{\mathfrak{m}}$ admits a filtration by sub-bimodules of type 1 and $\mathfrak{x}$. A priori both types could occur for successive quotients of the same filtration.

Ideally we would like to prove that $M_{\mathfrak{m}}$ has a filtration by simple bimodules of type $\mathfrak{x}$. In this case we say that $M_{\mathfrak{m}}$ is *pure* (or more precisely pure of type $\mathfrak{x}$). Unfortunately we have been unable to prove this for all components $\mathfrak{m}$ and we have to make do with a weaker result in some cases. To distinguish these cases let ψ be the basic character associated to $\mathfrak{m}$ and write

$$\psi = \psi_{p'} \omega^k$$

where $\psi_{p'}$ is a character of conductor prime to p, ω is the Teichmüller character of conductor p and k is an integer, $0 \leqq k < p-1$. We say that we are in case (1) if any of the following three conditions hold

(a) the greatest common divisor of k and $(p-1)$ is greater than 1,
(b) $\chi_{p'}(p) \neq 1$,
(c) k is odd and $\neq -1$.

We say that we are in case (2) if none of the above hold.

Proposition 1. *In case (1) $M_{\mathfrak{m}}$ is pure of type $\mathfrak{x}$.*

Corollary. *In case (1) $M_{\mathfrak{m}}$ is an η_1-yoked bimodule.*

For the definition of a yoke see Chap. 1, §4. Here it simply expresses the relation (2) above and it holds in this case by Lemma 2.

Proof of Proposition 1 in case 1 (a). Note that this includes the powers of the Teichmüller character since ψ is necessarily even.

Using the notation of §2 of Chap. 3, $A_{n,\mathfrak{m}}$ achieves good reduction over $\mathcal{O}_{n,\mathfrak{m}}$ whose field of fractions is the subfield of $\mathbf{Q}_p(\zeta_{p^n})$ which is of degree $(p-1)p^{n-1}/d$ over $\mathbf{Q}_p$.

If we denote by $A_{n,\mathfrak{m}/\mathcal{O}_{n,\mathfrak{m}}}$ the $\hat{p}$-divisible group scheme prolongation, there is no ambiguity in the notation, for (using Tate's theorem; see Chap. 0) $A_{n,\mathfrak{m}/\mathbf{Z}_p[\zeta_{p^n}]}$ is naturally isomorphic to the base change of $A_{n,\mathfrak{m}/\mathcal{O}_{n,\mathfrak{m}}}$ to $\mathbf{Z}_p[\zeta_{p^n}]$. It follows that $M_{\mathfrak{m}/\mathcal{O}_{n,\mathfrak{m}}}$ is of multiplicative type, since $M_{\mathfrak{m}/\mathbf{Z}_p[\zeta_{p^n}]}$ is. But then $M_{\mathfrak{m}/\mathcal{O}_{n,\mathfrak{m}}}$ can have no subquotients of type 1 by the proposition of Chap. 0.

Now we prove the key lemma for case (1) which will enable us to prove Proposition 1 also in cases (*b*) and (c).

Lemma 3. *In case (1) $B[I]$ has no submodule of type $\mathfrak{x}$.*

Proof. The idea is to use the fact that B is μ-deprived. (For the definition of this see Chap. 3, §7). Thus it is sufficient to show that the existence of a sub-bimodule M of type $\mathfrak{x}$ implies the existence of a multiplicative type subgroup of B.

In case 1 (a) let F be the unique subfield of $\mathbf{Q}(\zeta_{p^n})$ of degree $p^{n-1}(p-1)/d$ and let $\mathcal{O}_{n,\mathfrak{m}}$ denote the completion of its ring of integers $\mathcal{O}_F$ at the prime above p. (Here $d = \text{g.c.d.}(p-1, k)$). Then the Zariski closure of the simple bimodule M in $B_{n,\mathfrak{m}}$ is a finite flat group scheme (see Corollary 2 to Proposition 2 of Chap. 3 which applies also to $B_{n,\mathfrak{m}}$ since A and B are isogenous over $\mathbf{Q}$). As a $\text{Gal}(\bar{F}/F)$-module M is

isomorphic to an unramified twist of $\mu_p \otimes k_{\mathfrak{m}}$ and consequently $M_{/\mathcal{O}_{n,\mathfrak{m}}}$ is of multiplicative type since $d > 1$ and $M_{/\mathcal{O}_{n,\mathfrak{m}}}$ is ordinary. (This follows easily from the classification theorem of Oort-Tate or of Raynaud cf. [52, 55] and Chap. 0.) But this contradicts the fact that B is μ-deprived.

In case 1(b) let $S = \mathcal{O}_F[1/a]$and suppose that $M_{/S}$ were étale. Then $M(\overline{\mathbf{F}}_p)$ is in the kernel of I and hence by Lemma 3 of §2 it is contained in the cuspidal group $C_{\mathfrak{m}/S}$. But this has a trivial action of the Frobenius element of $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ whereas the condition $\psi_{p'}(p) \neq 1$ means that a Frobenius at p acts non-trivially on $M(\overline{F})$. This is a contradiction if $M_{/S}$ is étale, whence $M_{/S}$ is of multiplicative type. But this again contradicts B being μ-deprived.

In case 1(c) we use a similar argument but this time we keep track of the action of the inertia group at p. If $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_{p^n})/\mathbf{Q})$ then σ induces an action of $B_{/\mathbf{Q}} \otimes \mathbf{Q}(\zeta_{p^n})$ which by the functoriality of the Néron model extends uniquely to $B_{/\mathbf{Z}[\zeta_{p^n}]}$. The induced action on the fibre $B_{/S}$ is *algebraic* (cf. [69], proof of Theorem 2). Now the action of any such σ on $C_{\mathfrak{m}/S}$ is trivial. If $M_{/S}$ were étale, $M(\mathbf{F}_p)$ would be in the kernel of I and so as above it would be contained in $C_{\mathfrak{m}/S}$. Thus the action of σ on $M(\overline{\mathbf{F}}_p)$, and so also on $M(\overline{F})$, would be trivial. But in case 1(c) the action of the inertia group at p is via the character $\varepsilon\omega^k$ which is non-trivial mod p if $k \neq -1$. (The action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is given by η_1 on $M(\overline{F})$ since M has type $\mathfrak{x}$). This is a contradiction, so $M_{/S}$ is of multiplicative type and this then contradicts B being μ-deprived as before.

Proof of Proposition 1. Recall the sequence (**) of §1,

$$0 \to C_{\mathfrak{m}/S} \to E_{\mathfrak{m}/S} \to M_{\mathfrak{m}/S} \to 0 \qquad (**)$$

where $S = \mathcal{O}_F(1/a)$ and $F = \mathbf{Q}(\zeta_{p^n})$. We may pass to the completion $\mathcal{O} = \mathbf{Z}_p[\zeta_{p^n}]$ of S at p and obtain the corresponding sequence of finite flat group schemes over $\mathcal{O}$:

$$0 \to C_{\mathfrak{m}/\mathcal{O}} \to E_{\mathfrak{m}/\mathcal{O}} \to M_{\mathfrak{m}/\mathcal{O}} \to 0. \qquad (3)$$

Since $\mathcal{O}$ is a complete local ring there is a canonical exact sequence decomposing the finite flat group scheme $E_{\mathfrak{m}/\mathcal{O}}$ onto its connected and étale parts:

$$0 \to E^0_{\mathfrak{m}/\mathcal{O}} \to E_{\mathfrak{m}/\mathcal{O}} \to E^{\text{ét}}_{\mathfrak{m}/\mathcal{O}} \to 0.$$

On the other hand, Lemma 3 and Lemma 4 of 2 show that $C_{\mathfrak{m}/\mathcal{O}}$ is étale and $M_{\mathfrak{m}/\mathcal{O}}$ is of multiplicative type. Thus the sequence (3) splits canonically:

$$E_{\mathfrak{m}/\mathcal{O}} \xrightarrow{\sim} C_{\mathfrak{m}/\mathcal{O}} \times M_{\mathfrak{m}/\mathcal{O}}.$$

In particular the sequence (**) splits as a sequence of Hecke modules whence the sequence of Hecke modules

$$0 \to C_{\mathfrak{m}}[P] \to E_{\mathfrak{m}}[P] \to M_{\mathfrak{m}}[P] \to 0$$

is exact. Since the actions of Galois and of Hecke commute they are also Galois modules.

To prove the proposition it will be sufficient to show that $M_{\mathfrak{m}}[P]$ admits a filtration by sub-bimodules in which the successive quotients are all simple bimodules of type $\mathfrak{x}$. For then if we pick any basis $\{t_1, \ldots, t_s\}$ for the $K_{\mathfrak{m}}$ vector space

P^s/P^{s+1} the map

$$M_{\mathfrak{m}}[P^{s+1}]/M_{\mathfrak{m}}[P^s] \to \bigoplus_{i=1}^{s} M_{\mathfrak{m}}[P]$$

given by $x \mapsto xt_1 \oplus \ldots \oplus xt_s$ is injective. Since this is true for each s, and since $M_{\mathfrak{m}} = M_{\mathfrak{m}}[P^t]$ for some t, the proposition will follow.

We assume then that $M_{\mathfrak{m}}[P]$ admits a filtration with some subquotient of type 1. (Recall that in any filtration by bimodules each simple subquotient is either of type 1 of $\mathfrak{x}$.) We pick a sub-bimodule Z of $E_{\mathfrak{m}}$ containing $C_{\mathfrak{m}}$ and of minimal order subject to the condition that $Z/C_{\mathfrak{m}}$ has a subquotient of type 1. This Z has a filtration

$$0 \subset C_{\mathfrak{m}}[P] \subset Z^0 \subset Z$$

with $Z^0/C_{\mathfrak{m}}[P]$ of type $\mathfrak{x}$ and Z/Z^0 of type 1. Since Z is annihilated by P it is a $k_{\mathfrak{m}}$-vector space and we may pick a basis. If $\dim(Z^0/C_{\mathfrak{m}}[P]) = s$ the Galois representation on Z may be represented in $GL_{s+2}(k_{\mathfrak{m}})$ by matrices of the form

$$g \mapsto \rho(g) = \begin{pmatrix} 1 & \mathbf{a}(g) & \gamma(g) \\ \mathbf{o} & \mathfrak{x}(g) & \mathbf{b}(g) \\ 0 & \mathbf{o} & 1 \end{pmatrix} \in GL_{s+2}(k_{\mathfrak{m}})$$

where $\mathbf{a}$ and $\mathbf{b}$ are $(1 \times s)$ and $(s \times 1)$ matrices respectively and $\mathfrak{x}(g)$ is an $s \times s$ matrix with the values $\mathfrak{x}(g)$ on the diagonal and zero elsewhere. That we may choose $\mathfrak{x}(g)$ to be of this form follows from the remark following Lemma 2.

First we show that $s > 0$. For if $s = 0$ then by Lemma 1 Z has trivial Galois action. Its closure in $E_{\mathfrak{m}/S}$ is a finite flat group scheme and we can pick a subgroup scheme which is of multiplicative type. We simply take the kernel of reduction mod p, which is nontrivial because by Lemma 3 of §2, $C_{\mathfrak{m}}[P]_{/s} = (B[P]_{/s})^{\text{ét}}$. But this contradicts the hypothesis that B is μ-deprived.

We have seen (Lemma 3) that since B is μ-deprived Z does not contain a simple sub-bimodule of type $\mathfrak{x}$. This implies the following condition on the set $\mathscr{A} = \{\mathbf{a}(g) \colon \mathfrak{x}(g) = 1\}$,

$$\mathscr{A} \overset{\text{defn.}}{=} \{\mathbf{a}(g) \colon \mathfrak{x}(g) = 1\} = (k_{\mathfrak{m}})^s. \tag{I}$$

To see this first observe that $\mathscr{A}$ is indeed a $k_{\mathfrak{m}}$-subspace of $(k_{\mathfrak{m}})^s$. It is certainly a subgroup since $\mathbf{a}(gh) = \mathbf{a}(g) + \mathbf{a}(h)$. On the other hand conjugation of a matrix $\rho(g)$ lying in $\mathscr{A}$ by any other matrix $\rho(g')$ multiplies $\mathbf{a}(g)$ by $\mathfrak{x}(g')$. Since the $\{\mathfrak{x}(g')\}$ span $k_{\mathfrak{m}}$ over $\mathbf{F}_p$ we see that $\mathscr{A}$ is indeed a subspace. If $\dim \mathscr{A} < s$, then we could find a subspace W of Z^0 of dimension 2, containing $C_{\mathfrak{m}}$, and with the property that ρ restricted to W has the form

$$\rho|W(g) = \begin{pmatrix} 1 & a_1(g) \\ 0 & \mathfrak{x}(g) \end{pmatrix} \in GL_2(k_{\mathfrak{m}})$$

with $a_1(g) = 0$ whenever $\mathfrak{x}(g) = 1$. Thus the kernel of this representation is $\ker \mathfrak{x}$ which has degree prime to p. It follows easily that the representation is diagonalizable and hence that Z^0 contains a simple sub-bimodule of type $\mathfrak{x}$, which is false. Hence $\dim \mathscr{A} = s$.

A similar argument, this time using the fact that Z was chosen with minimal order, implies that

$$\mathscr{B} \overset{\text{defn.}}{=} \{\mathbf{b}(g) : \mathfrak{x}(g) = 1\} = (k_{\mathfrak{m}})^s. \tag{II}$$

Now let us consider the subgroup $\mathscr{K}$ of $\rho(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}))$ given by

$$\mathscr{K} = \{k = \rho(g) : \mathfrak{x}(g) = 1\}.$$

By the Eichler-Shimura relation (1) we have that $(k-1)^2 = 0$ for all $k \in \mathscr{K}$. (Note that $\eta_1(g) = \mathfrak{x}(g)$ on Z since it is annihilated by P). Furthermore $\mathscr{K}$ is an abelian group. If k and k' are any two elements of $\mathscr{K}$ then from the identity

$$2(k'-1)(k-1) = (k'-1)^2 + (k-1)^2 - k^2(k'k^{-1} - 1)^2$$

we see that $(k'-1)(k-1) = 0$. But this obviously contradicts (I) or (II) for a suitable choice of k and k'. For if, in the obvious notation, $\mathbf{a} = \mathbf{a}(k)$ and $\mathbf{b}' = \mathbf{b}(k')$ we would have that $\mathbf{a} \cdot \mathbf{b}' = 0$ for any pair k, k'.

Thus there is no filtration of $M_{\mathfrak{m}}[P]$ with a subquotient of type 1 and Proposition 1 is now proved.

We turn now to case (2) i.e. where $k = -1$ and $\psi_{p'}(p) = 1$. It will be convenient to redefine the cuspidal group in this case as follows. Pick an $l \equiv 1\,(ap)$ such that $l \not\equiv 1\,(p^2)$. Then set

$$C_{\mathfrak{m}}^* = C_{\mathfrak{m}}^{*(n)} = (-l < l >)^{\kappa} C_{\mathfrak{m}}^{(n)}$$

for some integer κ which will be chosen later. Then $C_{\mathfrak{m}}^*$ is again a module over $R_{\mathfrak{m}}$ and $\mathbf{T}_{\mathfrak{m}}$ and we let $I_{\mathfrak{m}}^* = Ann(C_{\mathfrak{m}}^*)$ be the annihilator ideal of $C_{\mathfrak{m}}^*$ in $\mathbf{T}_{\mathfrak{m}}$. We need a lemma.

Lemma 4. *For any sufficiently large* κ, $(I_{\mathfrak{m}}^*, 1 - l\langle l \rangle) \subseteq P_{\mathfrak{m}}^s$ *for some integer* s *independent of* n.

Proof. We note first that although we have dropped it from our notation $I_{\mathfrak{m}}^*$ and $P_{\mathfrak{m}}$ depend on n. By Proposition 4 of Chap. 4, §2, $\vartheta_{\mathfrak{m}}^{(r)}(1) \in I_{\mathfrak{m}}$. Hence the ideal $\mathfrak{a}_n$ defined by

$$\mathfrak{a}_n = \{r \in R_{\mathfrak{m}}^{(n)} : (1 - l\langle l \rangle)^{\kappa} \cdot r \in (\hat{\vartheta}_{\mathfrak{m}}^{(r)}(1))\}$$

is contained in $I_{\mathfrak{m}}^*$. The map

$$R_{\mathfrak{m}}^{(n)}/(\mathfrak{a}_n, 1 - l\langle l \rangle) \to \mathbf{T}_{\mathfrak{m}}^{(n)}/(I_{\mathfrak{m}}^*, 1 - l\langle l \rangle)$$

is surjective so it will be sufficient to show that the left hand side has order bounded independent of n. We consider the following projective limits over n:

$$y = \varprojlim (1 - l\langle l \rangle), \qquad \hat{\vartheta} = \varprojlim \hat{\vartheta}_{\mathfrak{m}}^{(r)}(1).$$

These are then elements of $R_{\mathfrak{m}}^{(\infty)} = \varprojlim R_{\mathfrak{m}}^{(n)}$. It will be enough to show that $R_{\mathfrak{m}}^{(\infty)}/(\mathfrak{a}_{\infty}, y)$ is finite where $\mathfrak{a}_{\infty}$ is the ideal of $R_{\mathfrak{m}}^{(\infty)}$ defined by

$$\mathfrak{a}_{\infty} = \{r \in R_{\mathfrak{m}}^{(\infty)} : y^{\kappa} r \in (\hat{\vartheta})\}.$$

For any sheet σ attached to $\mathfrak{m}$ there is a natural map $R_{\mathfrak{m}}^{(1)} \twoheadrightarrow R_{\sigma}^{(1)}$ which induces a map $R_{\mathfrak{m}}^{(\infty)} \to R_{\sigma}^{(1)}$ [64]. (See Chap. 1, §3 for the definition of a sheet; see also formula

(5) of that section. If χ is a character belonging to σ then composition with the natural map $R_\sigma^{(1)} \to \mathcal{O}_\chi$ induces the homomorphism $\alpha_{\mathfrak{m},\chi}$ if (4) of Chap. 1, §6). Let $y_\sigma(T)$ and $\hat{\vartheta}_\sigma(T)$ be the images of y and $\hat{\vartheta}$ under this map. Then for suitably large κ we can find an element $\alpha_\sigma(T) \in R_\sigma^{(1)}$ [64] such that

i) $\alpha_\sigma(T)$ and $y_\sigma(T)$ have no common factor,

ii) $$y_\sigma(T)^\kappa \alpha_\sigma(T) \in (\hat{\vartheta}_\sigma(T)).$$

This simply amounts to removing whatever zeroes $\hat{\vartheta}_\sigma(T)$ has in common with $y_\sigma(T)$. Note that neither of these power series is zero, the former by, for example, the corollary to Proposition 4 of Chap. 4, §2 and the finiteness of the cuspidal group.

There is an isomorphism

$$R_{\mathfrak{m}}^{(\infty)} \otimes \mathbf{Q}_p \xrightarrow{\sim} \prod_{\sigma \in \mathfrak{m}} R_\sigma^{(1)}[[T]] \otimes \mathbf{Q}_p$$

and it follows easily that $p^i \alpha_\sigma(T)$ is in the image of $R_{\mathfrak{m}}^{(\infty)}$ for some i. (This is the element which maps to $p^i \alpha_\sigma(T)$ in $R_\sigma^{(1)}[\![T]\!]$ and to zero in $R_{\sigma'}^{(1)}[\![T]\!]$ if $\sigma' \neq \sigma$). We can then find a j (depending on σ) such that $p^j \alpha_\sigma(T) \in \mathfrak{a}_\infty$. Since $p \nmid y$ it follows from (i) above that the ideal

$$\{y, p^j \alpha_\sigma(T) : \sigma \in \mathfrak{m}\}$$

has finite index in $R_{\mathfrak{m}}^{(\infty)}$, whence the same is also true of $\mathfrak{a}_\infty$.

We now fix a choice of κ satisfying the above lemma, and so also of $C_{\mathfrak{m}}^*$ and $I_{\mathfrak{m}}^*$.

Lemma 5. *In case (2), suppose that $B_n[I^*]$ has a finite submodule X which is pure of type $\mathfrak{x}$. Then the order of X is bounded independent of n.*

Proof. First we observe that if X is pure of type $\mathfrak{x}$ then by Lemma 2 the relation $g = \eta_1(g)$ holds on X for every $g \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Hence a splitting field for the Galois action on X is given by $F = \mathbf{Q}(\zeta_{ap^n})$ for some m. As in the proof of case 1(c) in Lemma 3 we can define an action of the inertia group at a prime above p on X. Suppose that $x \in X(F)$ is of order p^n. Then for some prime $\mathfrak{p}$ of F above p, $p^{n-1}x$ is not in the kernel of reduction mod p, for otherwise it would generate a subgroup scheme of multiplicative type over F, contradicting the hypothesis that B is μ-deprived. Hence any element of $I_\mathfrak{p}$ acts trivially on x since the action of $I_\mathfrak{p}$ on $C_{\mathfrak{m}}$ is trivial and since $x/_{\mathbf{F}_p}$ is in $B/_{\mathbf{F}_p}[I]^{\text{ét}}$ so it is in $C_{\mathfrak{m}}$ by Lemma 3 of §2. But for the prime $\mathfrak{p}$, $I_\mathfrak{p}$ is the subgroup of $\mathrm{Gal}(F|\mathbf{Q})$ consisting of those Φ_l with $l \equiv 1 (a)$ and $(l,p) = 1$. Thus for any such l

$$1 = \Phi_l = \eta_1(\Phi_l) = l\langle l \rangle \quad \text{on} \quad X.$$

By Lemma 4 the ideal $(I^*, 1 - l\langle l \rangle)$ contains P^s for some s independent of n (and l chosen as in Lemma 4). It is sufficient then to prove that $X[P]$ is finite since picking a basis $t_1, \ldots, t_j$ for P^i/P^{i+1} we get an injection

$$X[P^{i+1}]/X[P^i] \hookrightarrow \bigoplus_{i=1}^{j} X[P]$$

given by $a \to at_1 \oplus \ldots \oplus at_j$. But $X[P]$ is a direct sum of simple bimodules of type $\mathfrak{x}$ (by the remark after Lemma 2) and so a splitting field for it is given by $\mathbf{Q}(\zeta_{ap})$. Over this field $X[P]$ has trivial Galois action and we let $V_\mathfrak{p}$ be the kernel of reduction

mod $\mathfrak{p}$ in $X[P]$ where $\mathfrak{p}$ is a prime above p in $\mathbf{Q}(\zeta_{ap})$. Then $V_{\mathfrak{p}}$ is of codimension $\leqq 1$, as follows from Lemma 3 and Proposition 2 to §2. Thus $V = \cap V_{\mathfrak{p}}$ has codimension in $X[P]$ at most equal to the number of primes above p in $\mathbf{Q}(\zeta_{ap})$. But $V = 0$ since B is μ-deprived, and this completes the proof.

Now let X denote the maximal submodule of $B_n[I^*]$ which is pure of type $\mathfrak{x}$, and let $E_{\mathfrak{m}}^* = B_n[I^*]/X$. Let $C_{\mathfrak{m}}^{**}$ be the maximal submodule of $E_{\mathfrak{m}}^{**}$ which is pure of type 1. We consider the following exact sequence, where $M_{\mathfrak{m}}^{**}$ is by definition the cokernel in the sequence,

$$0 \to C_{\mathfrak{m}}^{**} \to E_{\mathfrak{m}}^{**} \xrightarrow{\varphi} M_{\mathfrak{m}}^{**} \to 0.$$

Proposition 1*. *$M_{\mathfrak{m}}^{**}$ is pure of type $\mathfrak{x}$, and is therefore an η_1-yoked bimodule.*

Proof. It will be enough to prove that $M_{\mathfrak{m}}^{**}[P]$ is pure of type $\mathfrak{x}$. Assume that it is not. For simplicity of notation we will drop the subscript $\mathfrak{m}$ during this proof. From the filtration

$$0 \subset C^{**} \subset C^{**} + E^{**}[P] \subset \varphi^{-1}(M^{**}[P])$$

we see that we can assume that we have a filtration of bimodules

$$0 \subset E_1 = C^{**} \subset E_2 \subset E_3$$

in which E_2/E_1 is of pure $\mathfrak{x}$-type and E_3/E_2 is a simple bimodule of type 1. Furthermore we may assume that E_3 has minimal order with this property. Note that E_2/E_1 cannot be zero since C^{**} was the maximal type 1 sub-bimodule of E^{**}. Also we know that E_2 contains no $\mathfrak{x}$-type sub-bimodule since X was chosen to be maximal of $\mathfrak{x}$-type in $B_n[I^*]$.

Thus we are in a situation similar to that of case (1) except that we do not have that $pE_3 = 0$. We do however that $p(E_3/E_1) = 0$. We need a more elaborate argument in this case (which also works in case (1)). Let z be an element of E_3 which generates E_3/E_2. Let $x_1, \ldots, x_s$ be elements of E_2 which form a basis for the $k_{\mathfrak{m}}$-vector space E_2/E_1 (cf. the remark following Lemma 2).

Step 1. There exists a σ_0 with $\mathfrak{x}(\sigma_0) \neq 1$ such that $\sigma_0 z - z \in C^{**}$.
There is certainly some element τ with $\mathfrak{x}(\tau) \neq 1$. Suppose that $\tau z = z + x$ with $x \in E_2$. Then as in (II) of case (1) there exists a ρ with $\mathfrak{x}(\rho) = 1$ and $\rho z \equiv z + x \bmod C^{**}$. Let $\sigma = \tau\rho^{-1}$.

Step 2. $\sigma_0 z = z$.
Applying the Eichler-Shimura relation we have

$$(\sigma_0 - \eta_1(\sigma_0))\,(\sigma_0 - 1)\,z = 0.$$

But on C^{**} σ_0 acts trivially, whence the result follows since $\mathfrak{x}(\sigma_0) \neq 1$ ($\eta_1(\sigma_0) \equiv \mathfrak{x}(\sigma_0)$ modulo the maximal ideal of $R_{\mathfrak{m}}$).

Now write $\sigma_0 x_i = \eta_1(\sigma_0)\, x_i + c_i$ with $c_i \in C^{**}$. Let $\mathbf{c}_0 = (c_1, \ldots, c_s)$. Also for any $g \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ with $\mathfrak{x}(g) = 1$ we write

$$\begin{aligned} gz &= z + \mathbf{b} \cdot \mathbf{x} + c \quad \text{with} \quad \mathbf{b} = (b_1, \ldots, b_s) \in (R_{\mathfrak{m}})^s,\ c \in C^{**} \\ gx_i &= x_i + d_i \quad \text{with} \quad d_i \in C^{**}, \end{aligned} \tag{4}$$

Here, even for fixed g, the choice of b_i and c are not unique but we make a choice. We note also that b_i, c and d_i all depend on g but for the moment we suppress this in our notation.

Step 3. Suppose that $\eta_1(g)=1$. Then

$$\mathbf{b}\cdot\mathbf{d}=\sum_{i=1}^{s} b_i d_i=0$$

as an element of C^{**}.
Applying the Eichler-Shimura relation to g we get that $(g-1)^2 z=0$. The above relation now follows immediately from (4).

Step 4. Suppose that $\eta_1(g)=1$. Then

$$\mathbf{b}\cdot\mathbf{c}_0+(1-\eta_1(\sigma_0))\,c=0\,. \tag{5}$$

We apply the Eichler-Shimura relation to $\sigma_0 g$. First we have

$$(\sigma_0 g-1)\,z=\sigma_0(\mathbf{b}\cdot\mathbf{x}+c)=\eta_1(\sigma_0)\,\mathbf{b}\cdot\mathbf{x}+\mathbf{b}\cdot\mathbf{c}_0+c\,.$$

Then applying $(\sigma_0 g-\eta_1(\sigma_0))$ to this we get zero by the Eichler-Shimura relation:

$$\eta_1(\sigma_0)\,\mathbf{b}\cdot\mathbf{d}+\mathbf{b}\cdot\mathbf{c}_0+(1-\eta_1(\sigma_0))\,c=0\,.$$

Now applying the result of step 3 gives the required relation.

Note that (5) uniquely determines c in terms of $\mathbf{b}$.

Step 5. For any $\mathbf{b}\in(R_{\mathfrak{m}})^s$, there exist a g with $\eta_1(g)=1$ and for which we may choose $\mathbf{b}=\mathbf{b}(g)$.
By adjusting our choice of c we see that we only have to prove that

$$\mathscr{B}=\{\mathbf{b}(g)\bmod \mathfrak{m}\colon\ \eta_1(g)=1\}$$

is equal to $(k_{\mathfrak{m}})^s$, where $\mathfrak{m}$ is the maximal ideal of $R_{\mathfrak{m}}$. This is a slight generalization of property (II) of case (1) where it was seen to hold if the condition $\eta_1(g)=1$ was replaced by $\mathfrak{x}(g)=1$. To see that we can make this generalization let K be the splitting field of E_3/E_1, F the fixed field of $\ker\mathfrak{x}$ and L the fixed field of $\ker\eta_1$. Then L and K are abelian extensions of F. Furthermore $L\cap K=F$ because the action of $\mathrm{Gal}(F/\mathbf{Q})$ on $\mathrm{Gal}(L/F)$ is trivial whereas the action on $\mathrm{Gal}(K/F)$ is via the character $\mathfrak{x}$. The assertion now follows easily.

Step 6. For all g with $\eta_1(g)=1$ we have $\mathbf{d}(g)=\mathbf{0}$.
We consider two elements g and g' for which $\eta_1(g)=\eta_1(g')=1$. With formula (4) for g and g' we get, in the obvious notation,

$$(gg')\,z=\ g(z+\mathbf{b}'\cdot\mathbf{x}+c')=\ z+(\mathbf{b}+\mathbf{b}')\cdot\mathbf{x}+\mathbf{b}'\cdot\mathbf{d}+\mathbf{c}+\mathbf{c}'\,.$$

Now apply the relation (5) to g, g' and gg'. By combining these relations we deduce that $\mathbf{b}'\cdot\mathbf{d}=0$. By the result of step 5 this holds for every $\mathbf{b}'$ in $(R_{\mathfrak{m}})^s$ whence $\mathbf{d}=0$.

We now obtain a contradiction from this. We have shown that E_2 has trivial Galois action over the fixed field of $\ker\eta_1$, and hence over an abelian extension of $\mathbf{Q}$. Let g be any element of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ for which $\mathfrak{x}(g)\neq 1$. Then $\ker(g-\eta_1(g))$ is a sub-bimodule of E_2. A simple sub-bimodule of it must be of $\mathfrak{x}$-type, but there are none of this type by our choice of X. Hence $\ker(g-\eta_1(g))=0$, whence $g-\eta_1(g)$ is

an automorphism of E_2. But this is impossible because E_2/E_1 is non-trivial and pure of $\mathfrak{x}$-type. The only possibility is that $M^{**}[P]$ was of pure $\mathfrak{x}$-type and this completes the proof of the proposition.

Let us now review our construction in case (2). We have now two related exact sequences which we can put into a commutative diagram

$$\begin{array}{ccccccc} 0 \to & C_{\mathfrak{m}}^{*} & \to & E_{\mathfrak{m}}^{*} = B_{\mathfrak{m}}[I^{*}] & \to & M_{\mathfrak{m}}^{*} & \to 0 \\ & \cap & & \downarrow \varphi & & \downarrow \psi & \\ 0 \to & C_{\mathfrak{m}}^{**} & \to & E_{\mathfrak{m}}^{**} & \longrightarrow & M_{\mathfrak{m}}^{**} & \to 0\,. \end{array} \tag{6}$$

In the top sequence, if we take the Zariski closures over $\mathcal{O}$, $C_{\mathfrak{m}/\mathcal{O}}^{*}$ is identified with the étale part of $B_{\mathfrak{m}}[I^{*}]_{/\mathcal{O}}$ (See Lemma 6 below) and $M_{\mathfrak{m}/\mathcal{O}}^{*}$ with the multiplicative part just as in the discussion after 3. On the other hand $C_{\mathfrak{m}}^{**}$ is of type 1 and $M_{\mathfrak{m}}^{**}$ is of type $\mathfrak{x}$. We now show that these two sequences are not too different (as expressed in Proposition 2* below). First we need a lemma.

Lemma 6. *$C_{\mathfrak{m}}^{*}$ is the maximal type 1 sub-bimodule of $E_{\mathfrak{m}}^{*}$, and $C_{\mathfrak{m}/\mathcal{O}}^{*}$ is the étale part of $E_{\mathfrak{m}/\mathcal{O}}^{*}$.*

Proof. The Pontrjagin dual of $C_{\mathfrak{m}}$ is a cyclic $\mathbf{T}_{\mathfrak{m}}$-module (see the beginning of § 2). This is therefore also the case for $C_{\mathfrak{m}}[I^{*}]$. By construction, $C_{\mathfrak{m}}^{*}$ is also cyclic. Since $C_{\mathfrak{m}}^{*}$ and $C_{\mathfrak{m}}[I^{*}]$ have the same annihilator ideal $I^{*} \subset \mathbf{T}_{\mathfrak{m}}$ it follows that they have the same order.

Consequently the inclusion $C_{\mathfrak{m}}^{*} \subset C_{\mathfrak{m}}[I^{*}]$ is an equality. It follows that $C_{\mathfrak{m}/\mathcal{O}}^{*}$ is the étale part of $E_{\mathfrak{m}/\mathcal{O}}^{*}$, using Lemma 3 of § 2.

Now suppose that T is the maximal type 1 sub-bimodule of $E_{\mathfrak{m}}^{*}$. The action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on T is trivial by Lemma 1. The kernel of reduction in $T(F)$ (to characteristic p) is zero because $E_{\mathfrak{m}/s}$ has no subgroup of multiplicative type (being μ-deprived). Hence $T_{/\mathcal{O}}$ is étale. But $C_{\mathfrak{m}/\mathcal{O}}^{*}$ *is* the étale part of $E_{\mathfrak{m}/\mathcal{O}}^{*}$, whence $C_{\mathfrak{m}}^{*} = T$.

Proposition 2*. *The vertical maps in (6) have kernels and cokernels of order bounded independent of n.*

Proof. Since by definition $E_{\mathfrak{m}}^{**} = E_{\mathfrak{m}}^{*}/X$ the statement for φ follows from Lemma 5. Thus we only have to prove that the order of the cokernel of the natural injection $C_{\mathfrak{m}}^{*} \to C_{\mathfrak{m}}^{**}$ is bounded independent of n.

We define a map

$$\varphi^{-1}(C_{\mathfrak{m}}^{**}) \to H^{1}(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), X)$$

by $e \to \{\sigma \to \sigma e - e\}$. By Lemma 5 and the fact that the image of the above mapping lies in a finite subgroup of the range of order independent of n, it will be sufficient to prove that the kernel is $C_{\mathfrak{m}}^{*} + X$. Clearly, $C_{\mathfrak{m}}^{*} + X$ is contained in the kernel. The converse follows immediately from Lemma 6.

§ 4. The splitting fields $L_{\mathfrak{m}}^{(n)}$

We continue the notation of § 3. In particular we often omit the n from the notation. Also for the time being we only consider case (1).

Let $K_{\mathfrak{m}}$ denote the smallest field extension of $\mathbf{Q}$ which

(i) is a splitting field for *all* Dirichlet characters χ of conductor ap^r (any r) belonging to the component $\mathfrak{m}$, and

(ii) contains $\mathbf{Q}(\zeta_{p^\infty})$.

It is evident from (1) of § 1 that $K_{\mathfrak{m}}$ is a splitting field for $C_{\mathfrak{m}}^{(n)}$. It follows from the corollary to Proposition 1 of § 3 that $K_{\mathfrak{m}}$ is also a splitting field for $M_{\mathfrak{m}}$. Let $L_{\mathfrak{m}}^{(n)} = L_{\mathfrak{m}}$ denote the minimal field extension of $K_{\mathfrak{m}}$ contained in $\bar{\mathbf{Q}}$ which is a splitting field for the Galois module $E_{\mathfrak{m}}$. It is evident that $L_{\mathfrak{m}}$ is a Galois extension of $\mathbf{Q}$, and that $L_{\mathfrak{m}}/K_{\mathfrak{m}}$ is a finite Galois extension, whose Galois group $G_{\mathfrak{m}}$ is a finite p-abelian group. We have a pairing

$$\begin{aligned} G_{\mathfrak{m}} \times M_{\mathfrak{m}} &\to C_{\mathfrak{m}} \\ (g, x) &\to \langle g, x \rangle \end{aligned} \tag{1}$$

defined as follows. Let $\tilde{x} \in E_{\mathfrak{m}}$ be any lifting of x, and let

$$\langle g, x \rangle = g(\tilde{x}) - \tilde{x} \in C_{\mathfrak{m}}.$$

Since $L_{\mathfrak{m}}/\mathbf{Q}$ is a Galois extension we obtain an action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on $G_{\mathfrak{m}}$ in the standard way: if $\alpha \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ and $g \in G_{\mathfrak{m}}$ then, denoting the action exponentially, we have

$$g^\alpha = \tilde{\alpha} g \tilde{\alpha}^{-1} \text{ where } \tilde{\alpha} \text{ is the image of } \alpha \text{ in } \mathrm{Gal}(L_{\mathfrak{m}}/Q).$$

Denoting the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on $M_{\mathfrak{m}}$ and $C_{\mathfrak{m}}$ exponentially also, we have:

$$\langle g^\alpha, x^\alpha \rangle = \langle g, x \rangle^\alpha = \langle g, x \rangle. \tag{2}$$

The compatibility with the diamond operators is given by the formula

$$\langle g, \langle r \rangle m \rangle = \langle r \rangle \langle g, m \rangle. \tag{3}$$

Lemma 1. *The pairing (1) is nondegenerate.*

Proof. That it is left-nondegenerate follows directly from the choice of $L_{\mathfrak{m}}$ as the *minimal* splitting field of $E_{\mathfrak{m}}$ over $K_{\mathfrak{m}}$.

We shall prove that the pairing (1) is right-nondegenerate. Suppose not. We may then find a submodule (as a Galois module and also as a Hecke module) $M_{\mathfrak{m}}^0 \subset M_{\mathfrak{m}}$ such that $\langle g, x \rangle = 0$ for all $g \in G_{\mathfrak{m}}$ and $x \in M_{\mathfrak{m}}^0$. Form the exact sequence of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ modules:

$$0 \to C_{\mathfrak{m}} \to E_{\mathfrak{m}}^0 \to M_{\mathfrak{m}}^0 \to 0 \tag{4}$$

by pullback from the basic sequence (*) of § 1. By the defining property of $M_{\mathfrak{m}}^0$ we have that $K_{\mathfrak{m}}$ is a splitting field for the Galois module $E_{\mathfrak{m}}^0$. Recall that $K_{\mathfrak{m}}$ is an *abelian* extension of $\mathbf{Q}$. Consequently, for any prime number l not dividing ap, and for any l-Frobenius element $\Phi_l \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ the endomorphism $\Phi_l - 1$ may be viewed as an endomorphism of the sequence (4) of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-modules. Fix a prime number l not dividing ap such that $\mathfrak{x}(\Phi_l) \neq 1$. Let $\tilde{M}_{\mathfrak{m}}^0 \subset E_{\mathfrak{m}}^0$ denote the kernel of $\varphi_l - \eta_1(\varphi_l)$ in $E_{\mathfrak{m}}^0$. Since $\varphi_l - \eta_1(\varphi_l)$ is an automorphism of $C_{\mathfrak{m}}$ we see that $\tilde{M}_{\mathfrak{m}}^0 \cap C_{\mathfrak{m}} = \{0\}$. Since $\varphi_l - \eta_1(\varphi_l)$ is zero on $M_{\mathfrak{m}}^0$, it cannot be an automorphism of $E_{\mathfrak{m}}^0$ and therefore $\tilde{M}_{\mathfrak{m}}^0$ is nontrivial. It follows that $\tilde{M}_{\mathfrak{m}}^0$ is a Galois-invariant lifting of $M_{\mathfrak{m}}^0$ to $E_{\mathfrak{m}}$ and is therefore of type $\mathfrak{x}$. This contradicts Lemma 3 of § 3.

The pairing (1) determines an inclusion

$$\lambda\colon\ G_{\mathfrak{m}} \to \mathrm{Hom}_{R_{\mathfrak{m}}^{(\infty)}}(M_{\mathfrak{m}}, C_{\mathfrak{m}})$$

(in the light of Lemma 1 and (4)).

The module $\mathrm{Hom}_{R_{\mathfrak{m}}^{(\infty)}}(M_{\mathfrak{m}}, C_{\mathfrak{m}})$ is naturally endowed with the structure of a bimodule. We see from the corollary to Proposition 1 of § 3 that it is an $\bar{\eta}_{-1}$-yoked bimodule, in the sense that its Galois action is derived from its $R_{\mathfrak{m}}^{(\infty)}$-module structure via the ring homomorphism:

$$\bar{\eta}_{-1}\colon\ \mathbf{Z}_p[\![\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})]\!] \twoheadrightarrow R_{\mathfrak{m}}^{(\infty)}. \tag{5}$$

By (2), the morphism λ commutes with the $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-action and consequently, the image of $G_{\mathfrak{m}}$ in $\mathrm{Hom}_{R_{\mathfrak{m}}^{(\infty)}}(M_{\mathfrak{m}}, C_{\mathfrak{m}})$ is stable under the action of the ring $\mathbf{Z}_p[\![\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})]\!]$.

Since the ring-homomorphism of (5) is surjective, it follows that the image of λ is also stable under the action of $R_{\mathfrak{m}}^{(\infty)}$. Since λ is injective, we may *endow* $G_{\mathfrak{m}}$ with the structure of an $R_{\mathfrak{m}}^{(\infty)}$-module in a unique manner such that λ is a homomorphism of bimodules. We shall henceforth regard $G_{\mathfrak{m}}$ as being endowed with *this* bimodule structure. Note that it is a sub-bimodule of a yoked bimodule, and therefore it is itself "yoked" (in fact, $\bar{\eta}_{-1}$-yoked).

The field extension $L_{\mathfrak{m}}/K_{\mathfrak{m}}$ is a Galois extension of type $\mathfrak{m}$ unramified except possibly at one of the primes $q_i \neq p$, $i = 1, \ldots, \nu$ (for the notation, see the beginning of this chapter).

Proposition 1. *In case (1), if* $\mathfrak{m}$ *is pseudo-primitive, then the extension* $L_{\mathfrak{m}}/K_{\mathfrak{m}}$ *is a virtually unramified Galois extension of type* $\mathfrak{m}$.
(For the definitions of type $\mathfrak{m}$ and virtually unramified, see Chap. I, § 7 and § 8).

Proof. The extension $L_{\mathfrak{m}}/K_{\mathfrak{m}}$ is Galois of type $\mathfrak{m}$ by construction, and is unramified at primes not dividing N. It suffices to show that it is unramified at primes dividing p. For this, we return to the basic sequence (**) of § 1 and pass to the completion $\mathcal{O} = \mathbf{Z}_p[\zeta_{p^n}]$ of $\mathbf{Z}[\zeta_{p^n}, \frac{1}{a}]$:

$$0 \to C_{\mathfrak{m}/\mathcal{O}} \to E_{\mathfrak{m}/\mathcal{O}} \to M_{\mathfrak{m}/\mathcal{O}} \to 0. \tag{6}$$

Since $C_{\mathfrak{m}/\mathcal{O}}$ is étale and $M_{\mathfrak{m}/\mathcal{O}}$ is of multiplicative type, and $\mathcal{O}$ is a complete local ring, a comparison of (6) with the canonical exact sequence decomposing the finite flat group scheme $E_{\mathfrak{m}/\mathcal{O}}$ into connected and étale parts shows that the sequence (6) splits canonically:

$$E_{\mathfrak{m}/\mathcal{O}} \xrightarrow{\sim} C_{\mathfrak{m}/\mathcal{O}} \times M_{\mathfrak{m}/\mathcal{O}}$$

which, in turn, shows that $L_{\mathfrak{m}}/K_{\mathfrak{m}}$ splits completely (and is therefore unramified) for the primes of $K_{\mathfrak{m}}$ dividing p.

In case (2) we use $M_{\mathfrak{m}}^{**}$ and $C_{\mathfrak{m}}^{**}$ in place of $M_{\mathfrak{m}}$ and $C_{\mathfrak{m}}$, and we define $L_{\mathfrak{m}}$ to be the splitting field of $E_{\mathfrak{m}}^{**}$. (The notation is as in § 3.) The non-degeneracy of the pairing (1) is still valid (for $M_{\mathfrak{m}}^{**}$, $C_{\mathfrak{m}}^{**}$ and and $G_{\mathfrak{m}}$). However Proposition 1 must be weakened slightly.

Proposition 1*. *In case (2), if* $\mathfrak{m}$ *is pseudo-primitive, then* $L_{\mathfrak{m}}/K_{\mathfrak{m}}$ *is a Galois extension of type* $\mathfrak{m}$ *unramified outside primes dividing* N.

Furthermore the inertia groups at the primes above p all lie in an $R_{\mathfrak{m}}^{(\infty)}$-submodule which is annihilated by a power of the maximal ideal, $\mathfrak{m}^c$, with c independent of n.

Proof. The idea is to compare the two sequences in (6) of § 3:

$$\begin{array}{ccccccc} 0 \to & C_{\mathfrak{m}}^* & \to & E_{\mathfrak{m}}^* = B_{\mathfrak{m}}[I^*] & \to & M_{\mathfrak{m}}^* & \to 0 \\ & \downarrow & & \downarrow \varphi & & \downarrow \psi & \\ 0 \to & C_{\mathfrak{m}}^{**} & \to & E_{\mathfrak{m}}^{**} & \longrightarrow & M_{\mathfrak{m}}^{**} & \to 0\,. \end{array}$$

Let $K'_{\mathfrak{m}}$ be the minimal splitting field of $\varphi^{-1}(C_{\mathfrak{m}}^{**})$ containing $K_{\mathfrak{m}}$. One checks that $K'_{\mathfrak{m}}$ is a finite extension of $K_{\mathfrak{m}}$ of degree bounded independent of n. Let $K_{\mathfrak{m}}^*$ be the minimal splitting field of $M_{\mathfrak{m}}^*$ containing $K'_{\mathfrak{m}}$.

Now pick a prime $\mathfrak{P}$ above p in $L_{\mathfrak{m}}^*$, the splitting field of $E_{\mathfrak{m}}^*$ (again assumed to contain $K'_{\mathfrak{m}}$), and primes $\mathfrak{p}$ and $\mathfrak{q}$ lying under $\mathfrak{P}$ in $L_{\mathfrak{m}}$ and $K_{\mathfrak{m}}^*$ respectively. We form a diagram in which all the squares are commutative:

$$\begin{array}{l} I_{\mathfrak{P}} \subseteq \mathrm{Gal}\,(L_{\mathfrak{m}}/L_{\mathfrak{m}} \cap K'_{\mathfrak{m}}) \\ \uparrow \qquad\qquad \uparrow \\ I_{\mathfrak{P}} \subseteq \mathrm{Gal}\,(L_{\mathfrak{m}}^*/K'_{\mathfrak{m}}) \\ \wr\downarrow \qquad\qquad \downarrow \\ I_{\mathfrak{q}} \subseteq \mathrm{Gal}\,(K_{\mathfrak{m}}^*/K'_{\mathfrak{m}}) \to \mathrm{Hom}_{R_{\mathfrak{m}}^{(\infty)}}(M_{\mathfrak{m}}^*,\ \varphi^{-1}(C_{\mathfrak{m}}^{**})/(C_{\mathfrak{m}}^*))\,. \end{array}$$

On the left the group $I_{\mathfrak{P}}$ is the inertia group at $\mathfrak{P}$ and similarly for $\mathfrak{p}$ and $\mathfrak{q}$. The horizontal map is defined by

$$\sigma \to \{e \to \tilde{\sigma}\, e - e\}$$

where $\tilde{\sigma}$ is a lifting of σ to $\mathrm{Gal}\,(L_{\mathfrak{m}}^*/K'_{\mathfrak{m}})$. The fact that the restriction map $I_{\mathfrak{P}} \to I_{\mathfrak{q}}$ is an isomorphism comes from the fact that $L_{\mathfrak{m}}^*/K_{\mathfrak{m}}^*$ is unramified. This is proved in the same way as Proposition 1.

To prove the proposition we just observe that $\varphi^{-1}(C_{\mathfrak{m}}^{**})/C_{\mathfrak{m}}^*$ is of finite order bounded independent of n (Proposition 2* of § 3). Hence the image of $I_{\mathfrak{q}}$ is annihilated by a fixed power of p. The same is then true of $I_{\mathfrak{P}}$. Since $K'_{\mathfrak{m}}$ is a finite extension of $K_{\mathfrak{m}}$ of order bounded independent of n, the same is true for the inertia groups in $L_{\mathfrak{m}}/K_{\mathfrak{m}}$. Finally, using the theorem of Ferrero and Washington [19] on the vanishing of Iwasasawa's μ-invariant we obtain our proposition.

§ 5. *The basic mapping*

We begin by considering case (1) in the sense of § 3. The pairing (1) of § 4 gives rise to a homomorphism

$$M_{\mathfrak{m}} \xrightarrow[\rho]{} \mathrm{Hom}_{R_{\mathfrak{m}}^{(\infty)}}(G_{\mathfrak{m}}, C_{\mathfrak{m}})$$

as follows. For $x \in M_{\mathfrak{m}}$, define $\rho(x)$: $G_{\mathfrak{m}} \to C_{\mathfrak{m}}$ by $\rho(x)(g) = \langle x, g \rangle$. If we wish to indicate that we are working at level $n \geqq 1$ ($N = ap^n$) at the component $\mathfrak{m}$ we denote this morphism $\rho = \rho_{\mathfrak{m}}^{(n)}$. The mapping $\rho_{\mathfrak{m}}^{(n)}$ is injective for all components in case (1).

Lemma 1. *Let* $\mathfrak{m}$ *be a pseudo-primitive component in case (1). There is an isomorphism of* $R_{\mathfrak{m}}^{(\infty)}$*-modules*:

$$\mathrm{Hom}_{R_{\mathfrak{m}}^{(\infty)}}(G_{\mathfrak{m}}, C_{\mathfrak{m}}) \xrightarrow[\delta]{\cong} \mathrm{Hom}_{\mathbf{Z}}(G_{\mathfrak{m}}, \mathbf{Q}_p/\mathbf{Z}_p)$$

well defined up to multiplication by a unit in $R_{\mathfrak{m}}^{(\infty)}$.

Proof. We use Proposition 4 of the appendix, nothing that $C_{\mathfrak{m}}$ is isomorphic to $R_{\mathfrak{m}}^{(n)}/\mathfrak{b}_{\mathfrak{m}}^{(n)}$ which is a Gorenstein ring. (The theorem of Chap. 4, § 3).

There is a mapping of $R_{\mathfrak{m}}^{(\infty)}$-modules

$$\xi\colon\ G_{\mathfrak{m}} \to \mathscr{X}/I_P\cdot\mathscr{X} = \mathrm{Hom}(M_{\mathfrak{m}}, \mathbf{Q}_p/\mathbf{Z}_p)$$

well-defined up to multiplication by a unit in $R_{\mathfrak{m}}^{(\infty)}$ given by the dual of $\delta\rho$, making use of Proposition 1 of § 2. If we wish to indicate that we are working at level n, we write $\xi = \xi^{(n)}$. From Lemma 1 and the injectivity of ρ we deduce the following Lemma.

Lemma 2. *The mapping* ξ *is surjective for any component* $\mathfrak{m}$ *in case (1).*

Proposition 1. *In case (1) of § 3 the Fitting ideal of the* $R_{\mathfrak{m}}^{(n)}$*-module* $G_{\mathfrak{m}}^{(n)} = \mathrm{Gal}(L_{\mathfrak{m}}^{(n)}/K_{\mathfrak{m}})$ *is contained in* $\mathfrak{b}_{\mathfrak{m}}^{(n)}$.

Proof. The surjection of $R_{\mathfrak{m}}^{(n)}$-modules of Lemma 2 gives an inclusion of Fitting ideals

$$F_{R_{\mathfrak{m}}^{(n)}}(G_{\mathfrak{m}}) \subseteq F_{R_{\mathfrak{m}}^{(n)}}(\mathscr{X}/I_P\mathscr{X}),$$

by Remark 1 of the appendix. It suffices then by Remark 4 of the Appendix to show that

$$F_{R_{\mathfrak{m}}^{(n)}/\mathfrak{b}_{\mathfrak{m}}^{(n)}}(\mathscr{X}/I_P\mathscr{X}) = 0.$$

But $R_{\mathfrak{m}}^{(n)}/\mathfrak{b}_{\mathfrak{m}}^{(n)} \cong \mathbf{T}_P^{(n)}/I_P^{(n)}$ and therefore, using Remark 4 again, it suffices to show that

$$F_{\mathbf{T}_P}(\mathscr{X}/I_P\mathscr{X}) \subseteq I_P.$$

This follows from the faithfulness of $\mathscr{X}$ as a $\mathbf{T}_P$-module (Proposition 1 of § 2) and Remark 7 of the appendix.

Now we turn to case (2). We define $\mathfrak{b}_{\mathfrak{m}}^{*(n)}$ to be the intersection of $I_{\mathfrak{m}}^{*(n)}$ with $R_{\mathfrak{m}}^{(n)}$. Thus $\mathfrak{b}_{\mathfrak{m}}^{*(n)}$ is the annihilator ideal of $C_{\mathfrak{m}}^* = C_{\mathfrak{m}}^{*(n)}$ in $R_{\mathfrak{m}}^{(n)}$. Since $C_{\mathfrak{m}}^*$ is cyclic as an $R_{\mathfrak{m}}^{(n)}$-module,

$$C_{\mathfrak{m}}^* \xrightarrow{\sim} R_{\mathfrak{m}}^{(n)}/\mathfrak{b}_{\mathfrak{m}}^{*(n)}.$$

The same analysis used in the proof of the theorem of Chap. 4 § 3 shows that $R_{\mathfrak{m}}^{(n)}/\mathfrak{b}_{\mathfrak{m}}^{*(n)}$ is a Gorenstein ring. Furthermore

$$(1 - l\langle l\rangle)^{\kappa}\cdot \prod_{\substack{q_i \neq p \\ q_i | r}} (q_i[n_{q_i}] - 1)\,\mathfrak{b}_{\mathfrak{m}}^{*(n)} \subseteq \hat{S}'_{\mathfrak{m}}(N).$$

We also have the natural isomorphism

$$R_{\mathfrak{m}}^{(n)}/\mathfrak{b}_{\mathfrak{m}}^{*(n)} \xrightarrow{\sim} \mathbf{T}_P^{(n)}/I_P^{*(n)}$$

An analysis as in case (1) gives a diagram

$$\begin{array}{ccccc} M_{\mathfrak{m}}^{**} & \xrightarrow[\rho]{} & \mathrm{Hom}_{R_{\mathfrak{m}}^{(\infty)}}(G_{\mathfrak{m}}, C_{\mathfrak{m}}^{**}) & & \\ \uparrow\subseteq & & \uparrow\subseteq & & \\ \tilde{M}_{\mathfrak{m}} & \longrightarrow & \mathrm{Hom}_{R_{\mathfrak{m}}^{(\infty)}}(G_{\mathfrak{m}}, C_{\mathfrak{m}}^{*}) & \xrightarrow{\sim} & \mathrm{Hom}_{\mathbf{Z}}(G_{\mathfrak{m}}, \mathbf{Q}_p/\mathbf{Z}_p) \end{array}$$

where $\tilde{M}_{\mathfrak{m}}$ is defined as the inverse image of $\mathrm{Hom}_{R_{\mathfrak{m}}^{(\infty)}}(G_{\mathfrak{m}}, C_{\mathfrak{m}}^{*})$ under ρ. Here we recall that in case (2) $G_{\mathfrak{m}} = \mathrm{Gal}(L_{\mathfrak{m}}/K_{\mathfrak{m}})$ where $L_{\mathfrak{m}}$ is the splitting field of $E_{\mathfrak{m}}^{**}$. We have the following maps of $R_{\mathfrak{m}}^{(\infty)}$-modules, the first two being surjective and the last injective:

$$G_{\mathfrak{m}} \twoheadrightarrow \mathrm{Hom}(\tilde{M}_{\mathfrak{m}}, \mathbf{Q}_p/\mathbf{Z}_p),$$

$$\mathrm{Hom}_{\mathbf{Z}}(M_{\mathfrak{m}}^{**}, \mathbf{Q}_p/\mathbf{Z}_p) \twoheadrightarrow \mathrm{Hom}_{\mathbf{Z}}(\tilde{M}_{\mathfrak{m}}, \mathbf{Q}_p/\mathbf{Z}_p),$$

$$\mathrm{Hom}_{\mathbf{Z}}(M_{\mathfrak{m}}^{**}, \mathbf{Q}_p/\mathbf{Z}_p) \to \mathrm{Hom}_{\mathbf{Z}}(M_{\mathfrak{m}}^{*}, \mathbf{Q}_p/\mathbf{Z}_p) = \mathcal{X}/I_P^{*}\,\mathcal{X}.$$

The second mapping has kernel of order bounded independent of n using the vanishing of Iwasawa's μ-invariant [19] as can be seen from the Cartesian square above. The third mapping has cokernel bounded independent of n (Prop. 2* of § 3).

Let $\mathfrak{m}_n$ be the maximal ideal of $R_{\mathfrak{m}}^{(\infty)}$. From Remarks 1, 8 and 9 of the appendix we easily deduce that there is an integer c independent of n such that

$$(\mathfrak{m}_n)^c \cdot F_{R_{\mathfrak{m}}^{(n)}}(G_{\mathfrak{m}}) \subseteq F_{R_{\mathfrak{m}}^{(n)}}(\mathcal{X}/I_P^{*}\,\mathcal{X}).$$

By the argument of the proof of Proposition 1 we obtain the following version in case (2).

Proposition 1*. *There is an integer c independent of n such that*

$$(\mathfrak{m}_n)^c \cdot F_{R_{\mathfrak{m}}^{(n)}}(G_{\mathfrak{m}}) \subseteq \mathfrak{b}_{\mathfrak{m}}^{*(n)}.$$

Appendix: Fitting ideals

Let R be a commutative ring with identity, and M an R-module of finite presentation. We refer the reader to Northcott's excellent book [50] for a self-contained elementary account of the theory of *Fitting invariants* of M. We will only have use for the "*zero*-th" (or the "*initial*") Fitting invariant.

If $h\colon R^a \to R^b$ is an R-homomorphism given by h', an $a \times b$ matrix with entries in R, the *Fitting ideal of h over R* is, by definition, the ideal $F_R(h) \subset R$ prescribed as follows: If $a < b$, then $F_R(h) = R$. If $a \geqq b$, then $F_R(h)$ is the ideal in R generated by all $b \times b$ minors of the matrix h'. [Compare *Bourbaki*, Comm. Alg. VII exercise 10 p. 573.]

By Theorem 1 of [50], the Fitting ideal of h over R depends only upon the R-isomorphy class of the cokernel of h. Thus, if M is a finitely presentable R-module, we define the *Fitting ideal of M over R*, denoted $F_R(M)$, to be $F_R(h)$, where

$$R^a \xrightarrow{h} R^b \longrightarrow M \longrightarrow 0$$

is any finite presentation of M over R.

These relations are evident, from the definition of Fitting ideal, in light of Theorem 1.

1. If $M \twoheadrightarrow M'$ is a surjection of R-modules, then

$$F_R(M) \subset F_R(M').$$

Note. It is not necessarily the case for general R that if M' is a submodule of M, then we have an inclusion of Fitting ideals. (For an example where R is a polynomial ring in three variables over a field, see *Bourbaki Commutative Algebra* VII Ex. 10 (g)) but see the corollaries to Propositions 1 and 3 below.

2. If $M \cong M_1 \times M_2$ is a direct product of finitely presented R-modules, then

$$F_R(M) = F_R(M_1) \cdot F_R(M_2).$$

3. If $\mathrm{Ann}_R(M)$ is the annihilator ideal of the R-module M, then

$$F_R(M) \subset \mathrm{Ann}_R(M).$$

4. If $I \subset R$ is any ideal, then

$$F_{R/I}(M/I \cdot M) = \text{image of } F_R(M) \text{ in } R/I.$$

From the above one deduces

5. If M is a direct sum of cyclic R-modules, $M = R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_t$, then

$$F_R(M) = \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_t.$$

6. If $I \subset R$ is a finitely generated ideal, then

$$F_R(M/I \cdot M) \subset (F_R(M), I) \subset R.$$

Proof. If

$$R^a \xrightarrow{h} R^b \longrightarrow M \longrightarrow 0$$

is a presentation of M, and $I = (x_1, \ldots, x_m) \subset R$, then an R-presentation of $M/I \cdot M$ is given by

$$R^a \times \underbrace{R^b \times R^b \times \ldots \times R^b}_{n} \xrightarrow{h^*} R^b \longrightarrow M/I \cdot M \longrightarrow 0$$

where $h^* = h \times x_1 \cdot \times x_2 \cdot \times \cdots \times x_n$. Any $b \times b$ minor of the matrix associated to h^* is either a minor of h, or a multiple of one of the x_j's.

A special case of 6 using that the Fitting ideal of a faithful module is trivial is:

7. If $I \subset R$ is a finitely generated ideal and M is a faithful R-module, then $F_R(M/I\,M) \subset I$.

The proofs of the next two assertions are easy, and may be found in [50]:

8. If M can be generated by n elements over R, then

$$\mathrm{Ann}_R(M)^n \subset F_R(M)$$

(cf. [50], Chap. 3, Theorem 5).

9. If $0 \to M_1 \to M_2 \to M_3 \to 0$ is an exact sequence of R-modules, then

$$F_R(M_1) \cdot F_R(M_3) \subset F_R(M_2)$$

(cf. [50], Chap. 3, Exercise 2: solution on pp. 90, 91).

Now suppose that R is a complete local noetherian ring with maximal ideal $\mathfrak{m}$.

10. If R is a complete local noetherian ring, and M an R-module of finite presentation expressed as a projective limit of quotient R-modules:

$$M \cong \varprojlim_n M_n \qquad n = 1, 2, \ldots.$$

Then

$$F_R(M) = \bigcap_{n=1}^{\infty} F_R(M_n).$$

From 9. one easily deduces:

11. Let M be an R-module of finite length. Then

$$\mathfrak{m}^{\mathrm{length}_R(M)} \subset F_R(M).$$

We now establish some results for the ring $R = \mathbf{Z}[X]$.

Let N be a finitely generated abelian group endowed with an endomorphism $T: N \to N$. We view N as an R-module, where $R = \mathbf{Z}[X]$ by: $X \cdot n = T(n)$ for any $n \in N$, and denote by N_0 the underlying group.

Lemma 1 (Auslander-Buchsbaum; [4] p. 392). *The sequence*

$$\mathbf{Z}[X] \otimes N_0 \xrightarrow{\gamma} \mathbf{Z}[X] \otimes N_0 \xrightarrow{e} N \longrightarrow 0$$

is an exact sequence of $\mathbf{Z}[X]$ *modules where*

$$e(P(X) \otimes n) = P(T) \cdot n$$

$$\gamma(P(X) \otimes n) = X \cdot P(X) \otimes n - P(X) \otimes T \cdot n$$

for $P(X)$ *a polynomial in* $\mathbf{Z}[X]$, *and* $n \in N$.

Proof. The sequence is evidently compatible with the action of $\mathbf{Z}[X]$, e is surjective, and $e \cdot \gamma = 0$. We must show that $\operatorname{Ker} e \subset \operatorname{image} \gamma$. It would suffice to show that for any $y \in \mathbf{Z}[X] \otimes N_0$ there is a $z \in \mathbf{Z}[X] \otimes N_0$ such that

$$y = \gamma(z) + 1 \otimes e(y). \tag{$*$}$$

But to check $(*)$ it suffices to check it for elements y of the form $y = X^k \otimes n$ for $k \geqq 0$ and $n \in N$. This we do inductively in k.

For $k = 0$, $y = 1 \otimes e(y)$ and we may take $z = 0$.

For $k = 1$, $y = X \otimes n = X \otimes n - 1 \otimes T(n) + 1 \otimes T(n)$ and we may take $z = 1 \otimes n$.

Suppose the assertion $(*)$ established for $k-1$, and let $y = X^k \otimes n$. Then

$$y = X \cdot X^{k-1} \otimes n - X^{k-1} \otimes T(n) + X^{k-1} \otimes T(n).$$

By the inductive hypothesis, $X^{k-1} \otimes T(n) = \gamma(z') + 1 \otimes T^k(n)$, and therefore we may take $z = X^{k-1} \otimes n + z'$.

Lemma 2. *If* N *is a free abelian group of finite rank endowed with an endomorphism* $T: N \to N$, *then we have the finite presentation of* N, *viewed as* $\mathbf{Z}[X]$ *module*:

$$0 \longrightarrow \mathbf{Z}[X] \otimes N_0 \xrightarrow{\gamma} \mathbf{Z}[X] \otimes N_0 \xrightarrow{e} N \longrightarrow 0.$$

Proof. In this case, $\mathbf{Z}[X] \otimes N_0$ is a free $\mathbf{Z}[X]$ module of finite rank. Injectivity of γ is also easily established.

Now let M be a finite abelian group endowed with an endomorphism $T: M \to M$. If $N = \mathbf{Z}^r$ for a suitably large r, we may construct a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{\varphi} & N & \xrightarrow{\psi} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle T_2} & & \downarrow{\scriptstyle T_1} & & \downarrow{\scriptstyle T} & & \\ 0 & \longrightarrow & N & \xrightarrow[\varphi]{} & N & \xrightarrow[\psi]{} & M & \longrightarrow & 0 \end{array}$$

where the rows are exact, and where ψ is given by a diagonal matrix. We may identify T_1 and T_2 with matrices in terms of the given standard $\mathbf{Z}$-basis of $\mathbf{Z}^r$. Let N_i $(i = 1, 2)$ denote the $\mathbf{Z}[X]$ module whose underlying abelian group is N, and where multiplication by X is given by the endomorphism T_i. Consider the resolutions of Lemma 2 for N_i:

$$0 \longrightarrow \mathbf{Z}[X] \otimes N \xrightarrow{\gamma_i} \mathbf{Z}[X] \otimes N \xrightarrow{e_i} N_i \longrightarrow 0$$

which yield the following $\mathbf{Z}[X]$ presentation of the module M;

$$\mathbf{Z}[X] \otimes N \oplus \mathbf{Z}[X] \otimes N \xrightarrow{1 \otimes \varphi \oplus \gamma_1} \mathbf{Z}[X] \otimes N \longrightarrow M \longrightarrow 0. \tag{1}$$

We are thankful to David Buchsbaum for providing us with the proof of

Proposition 1. *Let* M^* *denote the Pontrjagin dual of* M, *endowed with the natural* $\mathbf{Z}[X]$ *module structure induced from that of* M. *Then*

$$F_{\mathbf{Z}[X]}(M) = F_{\mathbf{Z}[X]}(M^*).$$

Proof. In the resolution (1) for M, we identify N with its $\mathbf{Z}$-dual, using the standard inner product. Then the analogous resolution of M^* is

$$\mathbf{Z}[X]\otimes N\oplus \mathbf{Z}[X]\otimes N \xrightarrow{1\otimes\varphi^t\oplus\gamma_2^t} \mathbf{Z}[X]\otimes N \longrightarrow M^* \longrightarrow 0 \tag{2}$$

where the superscript t denotes the transpose matrix. Of course, under our hypotheses, $\varphi^t=\varphi$.

We may view the resolutions (1) and (2) as given by $r\times 2r$ matrices $\mathcal{M}_1$ and $\mathcal{M}_2$ respectively, with values in $\mathbf{Z}[X]$. For suitable entries $a_1,\ldots,a_r$ and x_{ij}: $1\leqq i,j\leqq r$, these $r\times 2r$ matrices have the form

$$\mathcal{M}_1=\begin{pmatrix} a_1 & & x_{11} & x_{12} & \cdots & x_{1r}\\ & a_2 & x_{21} & x_{22} & \cdots & x_{2r}\\ & & \ddots & & & \\ & & a_r & x_{r1} & x_{r2} & \cdots & x_{rr}\end{pmatrix},$$

$$\mathcal{M}_2=\begin{pmatrix} a_1 & & X_{11} & a_1/a_2\cdot X_{21} & \cdots & a_1/a_r\cdot X_{r1}\\ & a_2 & a_2/a_1\cdot X_{12} & X_{22} & & a_2/a_r\cdot X_{r2}\\ & & \vdots & \vdots & & \vdots\\ & & a_r & a_r/a_1\cdot X_{1r} & a_r/a_2\cdot X_{2r} & & X_{rr}\end{pmatrix}.$$

The proposition will follow if we prove that there is a one: one correspondence between the $r\times r$ minor submatrices of $\mathcal{M}_1$ and those of $\mathcal{M}_2$ so that corresponding minor submatrices have the same determinant up to sign. This will be true in the field of rational functions (over $\mathbf{Q}$, say) in the variables $a_1,\ldots,a_r,x_{11},\ldots,x_{r,r}$.

The minor submatrices of size $r\times r$ in an $r\times 2r$ matrix $\mathcal{M}$ are in one: one correspondence with pairs of subsets S_1,S_2 in $[1,r]\subset N$ of the same cardinality. The minor matrix $\mathcal{M}(S_1,S_2)$ associated to such a pair (S_1,S_2) is given by taking the r columns of M indexed by the subset

$$S_1\cup([r+1,2r]-S_2')\subset[1,2r]$$

where $s\in S_2'$ if and only if $s-r\in S_2$.

An easy exercise:

$$\det\mathcal{M}_1(S_1,S_2)=\pm\det\mathcal{M}_2(S_2,S_1)$$

for any pair S_1, S_2 of subsets of $[1,r]$ of the same cardinality.

Corollary. *If $M'\subset M$ is an inclusion of $\mathbf{Z}[X]$ modules of finite cardinality, then*

$$F_{\mathbf{Z}[X]}(M)\subseteq F_{\mathbf{Z}[X]}(M').$$

Proof. The inclusion is converted to a surjection after application of Pontrjagin duality, and then we may apply 1.

We now pass to rings of particular interest to us: Let D be a finite discrete valuation ring extension of $\mathbf{Z}_p$ and $\Lambda=D[\![X]\!]$, the power series ring in the variable X over D.

The results proved for the ring $\mathbf{Z}[X]$ carry over to Λ quite easily. One has

Proposition 2. *If N is a Λ-module, free of finite type over D, and if N_0 denotes the underlying D-module of N, we have the finite free Λ-resolution*:

$$0\longrightarrow \Lambda\otimes_D N_0 \xrightarrow{\gamma} \Lambda\otimes_D N_0 \xrightarrow{e} N\longrightarrow 0.$$

(The Auslander-Buchsbaum resolution) where $e(\lambda\otimes n)=\lambda\cdot n$, $\gamma(\lambda\otimes n)=X\cdot\lambda\otimes n-\lambda\otimes X\cdot n$. The Fitting ideal of N is $\det_\Lambda(\gamma)$.

Recall that if M is any Λ-torsion Λ-module of finite type over Λ, Iwasawa has defined a polynomial $f_M(X)\in D[X]$, the "*characteristic polynomial*" of M, which is, in general, a power of the uniformizer of D times a distinguished polynomial. Now assume that M is of finite type over D and let $\tau(M)\subset M$ denote the D-torsion submodule. Since $\tau(M)$ is stable under the action of Λ, we have an exact sequence of Λ-modules

$$0\to\tau(M)\to M\to N\to 0$$

where N is free of finite rank over D. In this case $\tau(M)$ is finite, and therefore $f_M(X) = f_N(X)$ is the characteristic polynomial of the endomorphism induced by multiplication by X on N. Note that this characteristic polynomial is simply $\det_\Lambda(\gamma)$ where γ is as in the Auslander-Buchsbaum resolution for N.

Corollary. *The Λ-module N has "restricted projective dimension" equal to one* (cf. [50]). *The Fitting ideal $F_\Lambda(N)$ is the principal ideal generated by the characteristic polynomial $f_N(X)$. If M is a Λ-module which is of finite type over $\mathbf{Z}_p$, as above, then*

$$f_M(X) \cdot \mathfrak{m}^{\text{length}_\Lambda(M)} \subset F_\Lambda(M) \subset f_M(X) \cdot \Lambda$$

where $\mathfrak{m} \subset \Lambda$ is the maximal ideal.

Proof. Use the above discussion and Proposition 2; by 11, $\mathfrak{m}^{\text{length}_\Lambda(M)}$ is contained in $F_\Lambda(\tau(M))$; by 1, $F_\Lambda(M) \subset F_\Lambda(N) = f_M(X) \cdot \Lambda$; by 9. the other asserted inclusion holds.

In applying this corollary, it is useful to note the following elementary fact.

Lemma 3. *Let $\mathfrak{a} \subset \Lambda$ be an ideal of finite index. Let $f, g \in \Lambda$. Suppose that*

$$\mathfrak{a} \cdot (f) \subset (g).$$

Then g divides f.

Proof. The ring Λ is a unique factorization domain, and $\mathfrak{a}$ contains two nonzero elements α, β with no common irreducible factors. Since g divides αf and βf, one sees that g divides f, by considering the irreducible factors of g.

We also immediately obtain the analogues of Proposition 1 and its Corollary:

Proposition 3. *If M is a Λ-module of finite cardinality, and M^* is the Pontrjagin dual of M, with its naturally induced Λ-module structure, then*

$$F_\Lambda(M) = F_\Lambda(M^*).$$

Corollary. *If $M' \subset M$ is an inclusion of Λ-modules of finite cardinality, then $F_\Lambda(M) \subset F_\Lambda(M')$.*

The following result was explained to us by David Eisenbud.

Proposition 4. *Let R be a nontrivial local $\mathbf{Z}_p$-algebra of finite cardinality with maximal ideal denoted $\mathfrak{m}_R$. Then the following conditions are equivalent.*

1. *The kernel of $\mathfrak{m}_R$ in R, viewed as vector space over $R/\mathfrak{m}_R$ is of dimension* 1.
2. *The R-module $R^* = \text{Hom}_{\mathbf{Z}}(R, \mathbf{Q}_p/\mathbf{Z}_p)$ is free of rank* 1.
3. *For any R-module W of finite cardinality, there is an R-module isomorphism*

$$\delta_W\colon \text{Hom}_R(W, R) \xrightarrow[\cong]{} \text{Hom}_{\mathbf{Z}}(W, \mathbf{Q}_p/\mathbf{Z}_p)$$

4. *(Definition) R is a Gorenstein ring.*

Remark. If we are given a generator $h \in \text{Hom}_{\mathbf{Z}}(R, \mathbf{Q}_p/\mathbf{Z}_p)$ we may determine a *canonical* R-isomorphism δ_W for all such R-modules W. Without the choice of such an h, the R-isomorphisms δ_W are canonically determined up to multiplication by a unit in R.

Proof. 1) $\Rightarrow$ 2): If $R[\mathfrak{m}_R]$ is of length 1, then $R^*/\mathfrak{m}_R \cdot R^*$ is of length 1. By Nakayama's lemma we then have a surjection of R-modules $R \twoheadrightarrow R^*$ which must be an isomorphism since domain and range have the same (finite) cardinality.

2) $\Rightarrow$ 1): If R^* is free over R of rank 1, then $R^*/\mathfrak{m}_R R^*$ is of length 1 and therefore so is $R[\mathfrak{m}_R]$.

2) $\Leftrightarrow$ 3): This follows immediately from the "adjointness" isomorphism

$$\text{Hom}_{\mathbf{Z}}(W, \mathbf{Q}_p/\mathbf{Z}_p) \cong \text{Hom}_R(W, \text{Hom}_{\mathbf{Z}}(R, \mathbf{Q}_p/\mathbf{Z}_p)).$$

References

1. Artin, M.: Algebraization of formal moduli I. Global Analysis. Papers in honor of K. Kodaira Spencer, D.C., Iyanaga, S., (eds.) Univ. of Tokyo Press and Princeton Univ. Press, 21–71 1969
2. Atkin, A.O.L., Lehner, J.: Hecke operators on $\Gamma_0(m)$. Math. Ann. **185,** 134–160 (1970)
3. Atkin, A.O.L., Li, W.: Twists of newforms and pseudo-eigenvalues of W-operators. Invent. Math. **43,** 221–244 (1978)
4. Auslander, M., Buchsbaum, D.: Groups, Rings, Modules. New York, Evanston, San Francisco, London: Harper & Row 1974
5. Bayer, P., Neukirch, J.: On values of zeta functions and l-adic Euler characteristics. Invent Math. **50,** 35–64 (1978)
6. Casselman, W.: On representations of GL_2 and the arithmetic of modular curves. (International Summer School on Modular functions, Antwerp 1972) Modular functions of one variable II. Lecture Notes in Mathematics Vol. 349, pp. 109–141. Berlin-Heidelberg-New York: Springer 1973
7. Cassels, J.W.S., Fröhlich, A.: Algebraic number theory. London-New York: Academic Press 1967
8. Coates, J.: p-adic L-functions and Iwasawa's theory. In: Algebraic Number Fields, Fröhlich, A., (ed.) London-New York: Academic Press 1977
9. Coates, J.: The Work of Mazur and Wiles on Cyclotomic Fields. Séminaire Bourbaki No. 575, Lecture Notes in Mathematics Vol. 901. Berlin-Heidelberg-New York: Springer 1981
10. Coates, J.: K-theory and Iwasawa's analogue of the Jacobian, in Algebraic K-theory II. Lecture Notes in Mathematics Vol. 342. Berlin-Heidelberg-New York: Springer 1973
11. Coates, J., Lichtenbaum, S.: On l-adic zeta functions. Ann. of Math. **98,** 498–550 (1973)
12. Coates, J., Sinnott, W.: An analogue of Stickelberger's theorem for the higher K-groups. Invent. Math. **24,** 149–161 (1974)
13. Deligne, P.: Formes modulaires et représentations l-adiques, Séminaire Bourbaki 68/69 no. 355. Lecture Notes in Mathematics Vol. 179, pp. 136–172. Berlin-Heidelberg-New York: Springer 1971
14. Deligne, P., Mumford, D.: The irreducibility of the space of curves of given genus. Publications Mathématiques I.H.E.S., **36,** 75–109 (1969)
15. Deligne, P., Rapoport, M.: Schémas de modules de courbes elliptiques. Lecture Note in Mathematics Vol. 349. Berlin-Heidelberg-New York: Springer 1973
16. Demazure, M.: Lectures on p-divisible groups. Lecture Notes in Mathematics Vol. 302. Berlin-Heidelberg-New York: Springer 1972
17. Federer, L., Gross, B.: Regulators and Iwasawa Modules. Invent. Math. **62**, 443–457 (1981)
18. Ferrero, B., Greenberg, R.: On the behavior of the p-adic L-function at $s=0$. Invent. Math. **50,** 91–102 (1978)
19. Ferrero, B., Washington, L.: The Iwasawa invariant μ_p vanishes for abelian number fields. Ann. of Math. **109**, 377–396 (1979)
20. Fontaine, J.-M.: Groupes finis commutatifs sur les vecteurs de Witt. C.R. Acad. Sc. Paris t. **280**, (serie A) 1423–1425 (1975)
21. Gras. G.: Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés. Ann. Inst. Fourier **27**, 1–66 (1977)
22. Greenberg, R.: On a certain l-adic representation. Invent. Math., **21**, 198–205 (1973)
23. Greenberg, R.: On p-adic L-functions and cyclotomic fields. Nagoya Math. J. **56**, 61–77 (1974)
24. Greenberg, R.: On p-adic L-functions and cyclotomic fields II. Nagoya Math. J. **67**, 139–158 (1977)
25. Greenberg, R.: On the structure of certain Galois groups. Invent. Math. **47**, 85–99 (1978)
26. Grothendieck, A.: Modéles de Néron et monodromie. SGA7 I exposé IX. Lecture Notes in Mathematics, Vol. 288. Berlin-Heidelberg-New York: Springer 1972
27. Hartshore, R.: Algebraic Geometry. Berlin-Heidelberg-New York: Springer 1977
28. Igusa, J.: Kroneckerian model of fields of elliptic modular functions. Amer. J. Math. **81**, 561–577 (1959)
29. Igusa, J.: On the algebraic theory of elliptic modular functions. J. Math. Soc. Japan **20**, 96–106 (1968)
30. Iwasawa, K.: On p-adic L-functions. Ann. Math. **89**, 198–205 (1969)
31. Iwasawa, K.: Lectures on p-adic L-functions. Princeton: Princeton Univ. Press and Univ. of Tokyo Press 1972
32. Iwasawa, K.: On $\mathbf{Z}_l$-extensions of algebraic number fields. Ann. of Math. **98**, 246–326 (1973)
33. Kamienny, S.: On $J_1(p)$ and the arithmetic of the kernel of the Eisenstein ideal. Harvard Ph.D. Thesis, 1980
34. Katz, N.: p-adic properties of modular schemes and modular forms, vol. III of The Proceedings of

the International Summer School on Modular Functions, Antwerp (1972), Lecture Notes in Mathematics, Vol. 350, pp. 69–190 Berlin-Heidelberg-New York: Springer 1973
35. Katz, N.: Higher congruences between modular forms. Ann. of Math. **101,** (no. 2) 332–367 (1975)
36. Katz, N., Mazur, B.: Arithmetic moduli of elliptic curves. To appear in Annals of Math. Studies, Princeton U. Press.
37. Knutson, D.: Algebraic spaces. Lecture Notes in Mathematics, Vol. 203. Berlin-Heidelberg-New York: Springer 1971
38. Kubert, D.: Quadratic relations for generators of units in the modular function field. Math. Ann. **225**, 1–20 (1977)
39. Kubert, D., Lang, S.: Modular Units. Berlin-Heidelberg-New York: Springer 1981
40. Lang, S.: Introduction to modular forms. Berlin–Heidelberg-New York: Springer 1976
41. Lang, S.: Cyclotomic fields. Berlin-Heidelberg-New York: Springer 1978
42. Lang, S.: Cyclotomic fields II. Berlin-Heidelberg-New York: Springer 1980
43. Lang, S.: Units and class numbers in Number theory and algebraic Geometry. Lecture notes distributed in conjunction with the colloquium lectures given at the 85-th summer meeting of the A.M.S., University of Pittsburgh, Pittsburgh, Pennsylvania, August 17–20, 1981
44. Langlands, R.P.: Modular forms and l-adic representations. (International Summer School on Modular Functions, Antwerp, 1972) Modular functions of one variable II, Lecture Notes in Mathematics, Vol. 349, pp. 361–500, Berlin-Heidelberg-New York: Springer 1973
45. Li, W.: Newforms and functional equations. Math. Ann. **212**, 285–315 (1975)
46. Lichtenbaum, S.: On the values of zeta and L-functions I. Ann. of Math. **96**, (no. 2) 338–360 (1972)
47. Mazur, B.: Modular curves and the Eisenstein ideal. Publ. Math. I.H.E.S. **47**, (1948)
48. Mazur, B., Tate, J.: Points of order 13 on elliptic curves. Invent. Math. **22**, 41–49 (1973)
49. Mazur, B.: Rational isogenies of prime degree. Invent. Math. **44**, 129–162 (1978)
50. Northcott, D.G.: Finite free resolutions. Cambridge Univ. Press, Cambridge-New York 1976
51. Oort, F.: Commutative group schemes. Lecture Notes in Mathematics Vol. 15. Berlin-Heidelberg-New York: Springer 1966
52. Oort, F., Tate, J.: Group schemes of prime order. Ann. Scient. Ec. Norm. Sup. (serie 4) **3**, 1–21 (1970)
53. Raynaud, M.: Passage au quotient par une relation d'équivalence plate. Proc. of a Conference on Local Fields, NUFFIC Summer School held at Driebergen in 1966, pp. 133–157, Berlin-Heidelberg-New York: Springer 1967
54. Raynaud, M.: Spécialisation du foncteur de Picard. Publ. Math. I.H.E.S. **38**, 27–76 (1970)
55. Raynaud, M.: Schémas en groupes de type $(p, \ldots, p)$. Bull. Soc. Math. France **102**, 241–280 (1974)
56. Ribet, K.: A modular construction of unramified p-extensions of $\mathbf{Q}(\mu_p)$. Invent. Math. **34**, 151–162 (1976)
57. Serre, J-P.: Sur la topologie des variétés algébriques en caractéristique p. Symp. Int. de Top. Alg., Mexico, 1958
58. Serre, J-P.: Classes des corps cyclotomiques, Séminaire Bourbaki. Exp. **174** (1958-9)
59. Shafarevitch, I.R.: Lectures on minimal models and birational transformations of two-dimensional schemes. Tata Institute of fundamental research: Bombay 1966
60. Shimura, G.: Introduction to the arithmetic theory of automorphic forms. Publ. Math. Soc. Japan **11**, Tokyo-Princeton (1971)
61. Sinnott, W.: On the Stickelberger ideal and the circular units of a cyclotomic field. Ann. Math. **108**, 107–134 (1978)
62. Sinnott, W.: On the Stickelberger ideal and the circular units of an abelian field. Invent. Math. **62**, 181–234 (1980)
63. Soulé, C.: K-theorie des anneaux d'entiers de corps de nombres et cohomologie étale. Invent. Math. **55**, 251–295 (1979)
64. Tate, J.: p-divisible groups. Proceedings of a conference on local fields (Driebergen 1966). Berlin-Heidelberg-New York: Springer 1967
65. Tate, J.: Relations between K_2 and Galois cohomology. Invent. Math. **36**, 257–274 (1976)
66. Tate, J.: Number theoretic background. Proceedings of Symposia in Pure Mathematics **33**, (part II) 3–26 (1979)
67. Wiles, A.: Modular curves and the class group of $\mathbf{Q}(\zeta_p)$. Invent. Math. **58**, 1–35 (1980)
68. Yu, J.: A cuspidal class number formula for the modular curves $X_1(N)$. Math. Ann. **252**, 197–216 (1980)
69. Serre, J-P., Tate, J.: Good reduction of abelian varieties. Ann. of Math. **88**, 492–517 (1968)

Oblatum 17-I-1983