PUBLICATIONS MATHÉMATIQUES DE L'I.H.É.S.

BARRY MAZUR

Modular curves and the Eisenstein ideal

Publications mathématiques de l'I.H.É.S., tome 47 (1977), p. 33-186

<http://www.numdam.org/item?id=PMIHES_1977__47__33_0>

MODULAR CURVES AND THE EISENSTEIN IDEAL

by B. MAZUR (1)

INTRODUCTION

Much current and past work on elliptic curves over number fields fits into this general program: Given a number field K and a subgroup H of $GL_2(\hat{\mathbf{Z}}) = \prod_p GL_2(\mathbf{Z}_p)$ classify all elliptic curves $E_{/K}$ whose associated Galois representation on torsion points maps $Gal(\bar{K}/K)$ into $H \subset GL_2(\hat{\mathbf{Z}})$. By a theorem of Serre [67], if we ignore elliptic curves with complex multiplication, we may take H to be a subgroup of finite index.

This program includes the problems of classifying elliptic curves over K with a point of given order N in its Mordell-Weil group over K, or with a cyclic subgroup of order N rational over K (equivalently: possessing a K-rational N-isogeny). These last two problems may be rephrased in diophantine terms: Find the K-rational points of the modular curves $X_1(N)$ and $X_0(N)$ (cf. I, § 1).

In this paper we study these diophantine questions mainly for $K=\mathbf{Q}$. In particular we shall determine the ($\mathbf{Q}$-)rational points of $X_1(N)$ for all N. The precise nature of our results (which require close control of a certain part of the Mordell-Weil group of $J=J_0(N)$, the jacobian of $X_0(N)$ when N is a prime number) may indeed be peculiar to the ground field $\mathbf{Q}$. There are other reasons why this ground field may be a reasonable one on which to focus. For example, the recent conjecture of Weil would have every elliptic curve over $\mathbf{Q}$ obtainable as a quotient of $J_0(N)$ for some N. Thus, a detailed analysis of the Mordell-Weil groups of these jacobians may be relevant to a systematic diophantine theory for elliptic curves over $\mathbf{Q}$.

We shall now describe the main arithmetic results of this paper (2).

Theorem (1) (conjecture 2 of Ogg [49]). — *Let* $N \geq 5$ *be a prime number, and* $n = \text{numerator}\left(\frac{N-1}{12}\right)$. *The torsion subgroup of the Mordell-Weil group of* J *is a cyclic group of order n, generated by the linear equivalence class of the difference of the two cusps* $(0)-(\infty)$ (chap. III, (1.2)).

---

(1) Some of the work for this paper was done at the Institut des Hautes Études scientifiques, whose warm hospitality I greatly appreciate. It was also partially supported by a grant from the National Science Foundation.

(2) See also [36], [38] which give surveys of these results.

Control of the 2-torsion part of this Mordell-Weil group presents special difficulties. Ogg has made use of theorem 1 to establish, by an elegant argument, that for prime numbers N such that the genus of $X_0(N)$ is ≥ 2 (*i.e.* $N \geq 23$), the only automorphisms of the curve $X_0(N)$ (defined over $\mathbf{C}$) are the identity and the canonical involution w, *except when* $N=37$ [51].

Ogg had also conjectured the precise structure of the maximal torsion sub-Galois module of J which is isomorphic to a sub-Galois module of $\mathbf{G}_m$:

Theorem **(2)** (conjecture 2 (twisted) of Ogg [49]). — *The maximal* μ*-type group* (chap. I, § 3) *is the Shimura subgroup* (chap. II, § 11) *which is cyclic of order n.*

Despite their " dual " appearance, theorem 2 lies somewhat deeper than theorem 1.

Decomposing the jacobian J by means of the canonical involution w, we may consider the exact sequence $0 \to J_+ \to J \to J^- \to 0$ where $J_+ = (1+w).J$. One finds a markedly different behavior in the Mordell-Weil groups of J_+ and J^- (as is predictable by the Birch-Swinnerton-Dyer conjectures).

Theorem **(3)**. — *The Mordell-Weil group of* J_+ *is a free abelian group of positive rank, provided* $g_+ = \dim J_+ > 0$ (i.e. $N \geq 73$ *or* $N = 37, 43, 53, 61, 67$) (chap. III, (2.8)).

As for the minus part of the jacobian, a quotient $\tilde{J}$ of J is constructed (chap. II, (10.4)), the *Eisenstein quotient.* It is shown that $\tilde{J}$ is actually a quotient of J^- (chap. II, (17.10)), and its Mordell-Weil group is computed:

Theorem **(4)**. — *The natural map* $J \to \tilde{J}$ *induces an isomorphism of the cyclic group of order n generated by the linear equivalence class of* $(0)-(\infty)$ *onto the Mordell-Weil group of* $\tilde{J}$. *We have:* $\tilde{J}(\mathbf{Q}) = \mathbf{Z}/n$ (chap. III, (3.1)).

Since $n > 1$ whenever the genus of $X_0(N)$ is > 0, it follows from theorem 4 that $\tilde{J}$ is nontrivial whenever J is, and one can obtain bounds on the dimension of simple factors of $\tilde{J}$ (chap. III, (5.2)). Here is a consequence, which is stated explicitly only because one has, at present, no other way of producing such examples:

Theorem **(5)**. — *There are absolutely simple abelian varieties of arbitrarily high dimension, defined over* $\mathbf{Q}$, *whose Mordell-Weil groups are finite* (chap. III, (5.3)).

Using theorem 4, one obtains:

Theorem **(6)**. — *Let* N *be a prime number such that* $X_0(N)$ *has positive genus* (i.e. $N \neq 2, 3, 5, 7,$ *and* 13). *Then* $X_0(N)$ *has only a finite number of rational points over* $\mathbf{Q}$ (chap. III, (4.1)).

One obtains theorem 6 from theorem 4 as follows: since the image of $X_0(N)$ in $\tilde{J}$ generates the nontrivial group variety $\tilde{J}$, it follows that $X_0(N)$ maps in a finite-to-one

manner to $\tilde{J}$. Finiteness of the Mordell-Weil group of $\tilde{J}$ then implies finiteness of the set of rational points of $X_0(N)$.

The purely qualitative result (finiteness of $\tilde{J}(\mathbf{Q})$) is comparatively easy to obtain. It uses extremely little modular information, and in an earlier write-up I collected the necessary input to its proof in a few simple axioms. To follow the proof of theorem 6, one need only read these sections: chap. I, § 1; chap. II, §§ 6, 8.10, prop. (14.1) and chap. III, § 3. See also the outline given in [39].

To be sure, the assertion of mere finiteness is not all that is wanted. One expects, in fact, that the known list of rational points on $X_0(N)$ (all N) exhausts the totality of rational points, and in particular that the *only* rational points of $X_0(N)$ for N any integer >163 are the two cusps (0) and (∞) [49].

In this direction, we prove the following result, conjectured by Ogg [1]:

Theorem **(7)** (conjecture 1 of Ogg [49]). — *Let m be an integer such that the genus of $X_1(m)$ is greater than zero* (i.e. $m=11$ *or* $m\geqslant 13$). *Then the only rational points of $X_1(m)$ are the rational cusps* (III, (5.3)).

This uses results of Kubert concerning the rational points of $X_1(m)$ for low values of composite numbers m [27]. Equivalently:

Theorem **(7')**. — *Let an elliptic curve over $\mathbf{Q}$ possess a point of order $m<+\infty$, rational over $\mathbf{Q}$. Then $m\leqslant 10$ or $m=12$.*

This result may be used to provide a complete determination of the possible torsion subgroups of Mordell-Weil groups of elliptic curves over $\mathbf{Q}$. Namely:

Theorem **(8)**. — *Let Φ be the torsion subgroup of the Mordell-Weil group of an elliptic curve defined over $\mathbf{Q}$. Then Φ is isomorphic to one of the following 15 groups:*

$$\mathbf{Z}/m.\mathbf{Z} \quad \textit{for} \quad m\leqslant 10 \quad \textit{or} \quad m=12$$

or:

$$(\mathbf{Z}/2.\mathbf{Z})\times(\mathbf{Z}/2\nu.\mathbf{Z}) \quad \textit{for} \quad \nu\leqslant 4.$$

(III, (5.1). By [27] theorems 7 and 8 are implied by theorem 7 for prime values of $m\geqslant 23$. See also the discussion of this problem in [49].)

Since theorems 7 and 8 may be of interest to readers who do not wish to enter into the detailed study of the Eisenstein quotient $\tilde{J}$, I have tried to present the proof of these theorems in as self-contained a manner as possible. For their complete proof one needs to know:

a) $\tilde{J}(\mathbf{Q})$ is a torsion group (see discussion after theorem 6 above) and

b) the cusp $(0)-(\infty)$ does not project to zero in $\tilde{J}$ if the genus of $X_0(N)$ is greater than zero (which is easy).

---

[1] Demjanenko has published [12] a proof of the following assertion: (?) For any number field k (and, in particular, for $k=\mathbf{Q}$), there is an integer $m(k)$ such that $X_1(m)$ has no noncuspidal points rational over k, if $m\geqslant m(k)$. However, the proof does not seem to be complete. See the discussion of this in (*Math. Reviews*, *44*, 2755) and in [27].

One then need only read § 5 of chapter III.

If $\mathscr{H} \subset GL_2(\mathbf{F}_N)$ is any subgroup such that $\det \mathscr{H} = \mathbf{F}_N^*$ there is a projective curve $X_{\mathscr{H}}$ over $\mathbf{Q}$ parametrizing elliptic curves with "level $\mathscr{H}$-structures" [9] (chap. IV). The determination of the rational points of $X_{\mathscr{H}}$ amounts to a classification of elliptic curves over $\mathbf{Q}$ satisfying the property that the associated representation of $Gal(\bar{\mathbf{Q}}/\mathbf{Q})$ on N-division points factors through a conjugate of $\mathscr{H}$. If $N \geqslant 5$ is a prime number, any proper subgroup $\mathscr{H} \subset GL_2(\mathbf{F}_N)$ is contained in one of the following four types of subgroups ([67], § 2):

(i) $\mathscr{H}$ = a *Borel* subgroup. Then $X_{\mathscr{H}} = X_0(N)$.

(ii) $\mathscr{H}$ = the normalizer of a *split Cartan* ("déployé" [67]) subgroup.

In this case, denote $X_{\mathscr{H}} = X_{split}(N)$. It is an elementary exercise to obtain a natural isomorphism between $X_{split}(N)$ and $X_0(N^2)/w_{N^2}$ as projective curves over $\mathbf{Q}$, where w_{N^2} is the canonical involution induced from $z \mapsto -1/N^2 z$ on the upper half-plane.

(iii) $\mathscr{H}$ = the normalizer of a *nonsplit Cartan* subgroup.

In this case write $X_{\mathscr{H}} = X_{nonsplit}(N)$.

(iv) $\mathscr{H}$ = an *exceptional* subgroup (or to keep to the terminology of [67] (2.5)), $\mathscr{H}$ is the inverse image in $GL_2(\mathbf{F}_N)$ of an *exceptional* subgroup of $PGL_2(\mathbf{F}_N)$. An exceptional subgroup of $PGL_2(\mathbf{F}_N)$ is a subgroup isomorphic to the symmetric group $\mathfrak{S}_4$, or alternating groups $\mathfrak{A}_4$ or $\mathfrak{A}_5$.

The further requirement $\det \mathscr{H} = \mathbf{F}_N^*$ insures that the image of $\mathscr{H}$ in $PGL_2(\mathbf{F}_N)$ be isomorphic to $\mathfrak{S}_4$. Moreover, if such an $\mathscr{H}$ (with surjective determinant) exists when $K = \mathbf{Q}$, then $N \equiv \pm 3 \bmod 8$. For such N write $X_{\mathscr{H}} = X_{\mathfrak{S}_4}(N)$.

We do not treat cases (iii) and (iv) in this paper. Of the four types of subgroups of $GL_2(\mathbf{F}_N)$ listed above, the normalizer of a nonsplit Cartan subgroup seems the least approachable by known methods. In particular (to my knowledge) there is no value of N for which $X_{nonsplit}(N)$ has been shown to have a finite number of rational points. As for case (ii) Serre remarked recently that for any fixed number field K there are very few $N \geqslant 5$ such that $X_{\mathscr{H}}(K)$ is nonempty when $\mathscr{H}$ is an *exceptional* subgroup of $GL_2(\mathbf{F}_N)$. Firstly, if the image of $\mathscr{H}$ in $PGL_2(\mathbf{F}_N)$ is $\mathfrak{A}_4$ or $\mathfrak{A}_5$, then $\det \mathscr{H} \subset (\mathbf{F}_N^*)^2$. Using the e_N-pairing of Weil, one sees that if $X_{\mathscr{H}}(N)$ has a K-rational point, then K contains the quadratic subfield of $\mathbf{Q}(\zeta_N)$. This can happen for only finitely many values of N for a given K, and not at all when $K = \mathbf{Q}$.

Secondly, Serre proves the following local result:

Let $\mathscr{K}$ be a finite extension of $\mathbf{Q}_N$, of ramification index e. Let E *be an elliptic curve over $\mathscr{K}$ with a semi-stable Néron model over the ring of integers $\mathcal{O}_{\mathscr{K}}$. Let* $r : Gal(\bar{\mathscr{K}}/\mathscr{K}) \to PGL_2(\mathbf{F}_N)$ *denote the projective representation associated to the action of Galois on* N*-division points of* E. *Then: if* $2e < N-1$, *the image of the inertia subgroup under r contains an element of order* $\geqslant (N-1)/e$.

Using this local result one sees that there is a bound $c(\mathscr{K})$ such that if $N > c(\mathscr{K})$ then $X_{\mathscr{H}}(\mathscr{K})$ is empty for all exceptional subgroups $\mathscr{H}$. In the case of $\mathscr{K} = \mathbf{Q}$, $X_{\mathfrak{S}_4}(N)$ has *no* points rational over $\mathbf{Q}_N$ if $N > 13$. Hence it has no points rational over $\mathbf{Q}$ for $N > 13$.

Serre constructs, however, a rational point on $X_{\mathfrak{S}_4}(11)$ and on $X_{\mathfrak{S}_4}(13)$ corresponding to elliptic curves with complex multiplication by $\sqrt{-3}$.

Concerning case (ii) (elliptic curves over $\mathbf{Q}$ such that the associated $Gal(\bar{\mathbf{Q}}/\mathbf{Q})$-representation on N-division points factors through the normalizer of a split Cartan subgroup of $GL_2(\mathbf{F}_N)$) we obtain the following result:

Theorem (**9**). — *If* $N = 11$ *or* $N \geqslant 17$ (i.e. *if* $X_{split}(N)$ *is of positive genus and* $N \neq 13$) *then* $X_{split}(N)$ *has only a finite number of rational points* (chap. III, § 6).

Remarks. — Since $X_{split}(13)$ is of genus 3, one expects it to have only a finite number of rational points as well. The proof of theorem 9 is given in Chapter II, § 9. It uses the following two facts:

a) $\tilde{J}(\mathbf{Q})$ is finite (see the discussion after theorem 6 above) and

b) $\tilde{J}$ factors through J^-.

It is interesting to note that when $N \equiv 1 \bmod 8$ fact *b)* seems to depend on the detailed study of $\tilde{J}$ (chap. II, (17.10)).

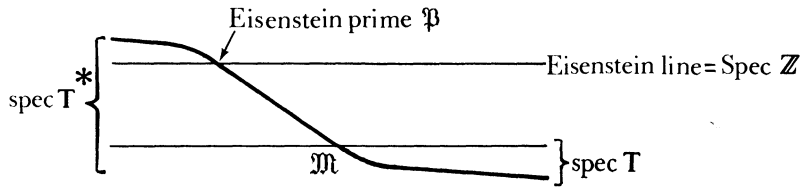
It is often an interesting problem to apply theorem 4 to obtain an effective determination of the rational points on $X_0(N)$ for a given (even relatively low) value of N, and, to that end, somewhat sharper results are useful.

Theorem **(10).** — *Let* $\rho : X_0(N)(\mathbf{Q}) \to \mathbf{Z}/n$ *denote the map obtained by projecting the linear equivalence class of* $x-(\infty)$ *to the Mordell-Weil group of* $\tilde{J}$ (cf. theorem 4). *Then* $\rho(x)$ *is equal to one of these five values in* $\mathbf{Z}/n$: 0, 1, 1/2 (*possible only if* $N \equiv -1 \bmod 4$), 1/3 *or* 2/3 (*the latter two being possible only if* $N \equiv -1 \bmod 3$) (chap. III, (4.2)).

Using these results, tables of Wada [70], Atkin, and Tingley, and work of Ogg [49], Brumer and Kramer [4], and Parry [73], one obtains the chart given at the end of this introduction where the rational points of $X_0(N)$ for $N < 250$, $N \neq 151$, 199, and 223 are determined explicitly (also see note added in proof (end of chap. III)).

The main technique of this paper involves a close study of the Hecke algebra $\mathbf{T}$ (chap. II, § 6) which we prove to be isomorphic to the full ring of $\mathbf{C}$-endomorphisms of J (mildly sharpening a result of Ribet). We establish a dictionary between maximal ideals $\mathfrak{M}$ in $\mathbf{T}$ and finite sub-Galois representations of J which are two-dimensional over the residue field of $\mathfrak{M}$ (cf. chap. II, (14.2), for a precise statement and precise hypotheses). The prime ideals that distinguish themselves as corresponding to *reducible* representations are the primes in the support of a certain ideal which we call the *Eisenstein ideal* $\mathfrak{I}$ (chap. II, § 9), and which is the central object of our investigation.

We like to view the Eisenstein ideal geometrically as follows: Let $\mathbf{T}^*$ denote the algebra generated by the action of the Hecke operators T_ℓ $(\ell \neq N)$ and by w, on the space of holomorphic modular forms of weight 2 for $\Gamma_0(N)$. The algebra $\mathbf{T}$ is the image of $\mathbf{T}^*$ in the ring of endomorphisms of *parabolic* forms. We envision the spectra of these rings schematically as follows:



where the extra irreducible component belonging to $\mathbf{T}^*$ *(the Eisenstein line)* corresponds to the action of $\mathbf{T}^*$ on the Eisenstein series of weight 2. The Eisenstein ideal is the ideal

defining the scheme-theoretic intersection of Spec $\mathbf{T}$ and the Eisenstein line. The Eisenstein quotient $\tilde{J}$ is the quotient of J associated to (chap. II, § 10) the union of irreducible components of Spec $\mathbf{T}$ which meet the Eisenstein line. One may think of the " geometric descent " argument of chapter III, § 3, as a technique of passing from knowledge of the arithmetic of the Eisenstein line (*i.e.* of Eisenstein series, and of $\mathbf{G}_m$) to knowledge of the arithmetic of irreducible components meeting the Eisenstein line (*i.e.* of $\tilde{J}$) by a " descent " performed at a common prime ideal. One might hope that for other prime ideals common to distinct irreducible components (primes of *fusion*) one might make an analogous passage (cf. [39], § 5, Prop. 4).

Control of the local structure of $\mathbf{T}$ is necessary for the more detailed work. For example, it is easily seen that the kernel of the ideal $\mathfrak{M} \subseteq \mathbf{T}$ in $J(\bar{\mathbf{Q}})$ is 2-dimensional as a vector space over the residue field of $\mathfrak{M}$ if and only if $\mathbf{T}_{\mathfrak{M}}$ (the completion at $\mathfrak{M}$) is a Gorenstein ring (chap. II, (15.1)). We prove that $\mathbf{T}_{\mathfrak{M}}$ is a Gorenstein ring, at least if $\mathfrak{M}$ is an Eisenstein prime, or if its residual characteristic is $\neq 2$, or if it is supersingular (chap. II, § 14). When $\mathfrak{M}$ is *not* an Eisenstein prime this is relatively easy to prove. When $\mathfrak{M}$ is an Eisenstein prime, it involves the structure theory of admissible group schemes developed in chapter I and a close study of modular forms mod p (chap. II). Using this work we prove:

Theorem (**11**). — *The Eisenstein ideal* $\mathfrak{I}$ *is locally principal in* $\mathbf{T}$. *If* $\mathfrak{P}=(\ell, p)$ *is an Eisenstein prime of residual characteristic* p, *then the element* $\eta_\ell = 1+\ell-T_\ell$ *is a local generator of the ideal* $\mathfrak{I}$ *at* $\mathfrak{P}$ *if and only if*:

(i) ℓ *is not a* p-th *power modulo* N
(ii) $\frac{\ell-1}{2} \not\equiv 0 \bmod p$

(*if not both* ℓ *and* p *are equal to* 2)

or (*when* $\ell = p = 2$) 2 *is not a quartic residue modulo* N (chap. II, (18.10)).

Most of this analysis of $\mathbf{T}_{\mathfrak{P}}$ is crucial for the proof of Ogg's conjectures 2 and 2 (twisted) (theorems 1 and 2) and for the more delicate descent needed to establish:

Theorem (**12**). — *If* $\mathfrak{P}$ *is an Eisenstein prime whose residue field is of odd characteristic, then the* $\mathfrak{P}$*-primary component of the Shafarevich-Tate group of* J *vanishes* (chap. III, (3.6)).

As described in the survey [36], theorems 4 and 10 may be used to prove a version of the Birch-Swinnerton-Dyer conjecture *relative to the prime ideal* $\mathfrak{P}$. In the last two sections of chapter III we pursue this theme obliquely by studying the $\mathfrak{P}$-adic L series [1]. Guided by formulas, and by conjectures, we are led to the following result, which we prove, independent of any conjectures:

Theorem (**13**). — *Let* $\mathfrak{P}$ *be an Eisenstein prime whose residual characteristic is an odd prime* p. *Let* $\mathbf{Q}^{(p)}$ *be the unique* $\mathbf{Z}_p$*-extension of* $\mathbf{Q}$. *Let* $\tilde{J}^{(p)}$ *be the* p*-Eisenstein quotient* (*the*

[1] Ref. [34].

abelian variety quotient of $\tilde{J}$ *corresponding to the union of all irreducible components of* Spec **T** *containing* $\mathfrak{P}=(\mathfrak{I}, p)$, chap. II, § 10).

Then $\tilde{J}^{(p)}(\mathbf{Q}^{(p)})$, *the group of points of* $\tilde{J}^{(p)}$ *rational over* $\mathbf{Q}^{(p)}$, *is a finitely generated group, and is finite if p is not a p-th power modulo* N.

We also obtain asymptotic control of the $\mathfrak{P}$-primary component of the Shafarevich-Tate group of J in the finite layers of $\mathbf{Q}^{(p)}$.

It would be interesting to develop the theory of the Eisenstein ideal in broader contexts (*i.e.* wherever there are Eisenstein series). Five special settings suggest themselves, with evident applications to arithmetic:

One might study $X_0(N)$ for N not necessarily prime (*e.g.*, N square-free). Although much will carry over (cf. Appendix) there is, as yet, no suitable analogue of the Shimura subgroup, and the " geometric descent " is bound not to be decisive without new ideas: (but see forthcoming work of Berkovich).

One might attempt the same with $X_1(N)$ (cf. [71]) and here one interesting new difficulty is that the endomorphism ring is nonabelian.

One might work with modular forms of higher weight k for $SL_2(\mathbf{Z})$, where a major problem will be to understand the action of inertia at p on the p-adic Galois representation associated to the modular form.

One might stretch the analogy somewhat and consider some important non-congruence modular curves (*e.g.*, the Fermat curves, following the forthcoming Ph d. Thesis of D. Rohrlich) where the " Eisenstein ideal " has no other definition than the annihilator, in the endomorphism ring, of the group generated by the cuspidal divisors in the jacobian of the curve.

One might also work over function fields in the context of Drinfeld's new theory [13].

Throughout this project, I have been in continual communication with A. Ogg and J.-P. Serre. It would be hard to completely document all the suggestions, conjectures and calculations that are theirs, or all that I learned from them in the course of things. I look back with pleasure on conversations and correspondence I had with them, and with Atkin, Brumer, Deligne, Katz, Kramer, Kubert, Lenstra, and Van Emde Boas, Ligozat, Rapoport, Ribet, and Tate.

We conclude this introduction with a chart describing the numerical situation for prime numbers $N<250$. The columns are as follows:

N: ranges through all primes less than 250 such that $g=\text{genus}(X_0(N))>0$.

$n=\text{num}\left(\frac{N-1}{12}\right)$.

$g_\pm=$ number of $\pm$ eigenvalues of w acting on parabolic modular forms of weight 2 for $\Gamma_0(N)$. Also $g_+=\dim J^+=\text{genus}(X_0(N))^+$; $g_-=\dim J^-$.

We write $g_\pm$ as a sum of the dimensions of the simple factors comprising $J^\pm$. When a simple factor is a quotient of the Eisenstein factor, it is boldface. When the

TABLE

N	n	g_+	g_-	ν	Values of $\rho(x)$	e_p
11	5	0	**1**	3	$0, \pm 1/3$	
17	4	0	**1**	2	$\pm 1/3$	
19	3	0	**1**	1	0	
23	11	0	**2**	0		
29	7	0	**2**	0		
31	5	0	**2**	0		$e_5 = 2$
37	3	1	**1**	2	± 1	
41	10	0	**3**	0		$e_2 = 3$
43	7	1	**2**	1	0	
47	23	0	**4**	0		
53	13	1	**3**	0		
59	29	0	**5**	0		
61	5	1	**3**	0		
67	11	2	$1+$**2**	1	0	
71	35	0	$\mathbf{3}_5+\mathbf{3}_7$	0		
73	6	2	$\mathbf{1}_2^*+\mathbf{2}_3$	0		
79	13	1	**5**	0		
83	41	1	**6**	0		
89	22	1	$\mathbf{1}_2^*+\mathbf{5}_{11}$	0		
97	8	3	**4**	0		
101	25	1	**7**	0		
103	17	2	**6**	0		
107	53	2	**7**	0		$e_{17} = 2$
109	9	3	$1+$**4**	0		
113	28	3	$\mathbf{1}_2^*+\mathbf{2}_2+\mathbf{3}_7$	0		$e_2 = 3$
127	21	3	**7**	0		$e_7 = 2$
131	65	1	**10**	0		$e_5 = 2$
137	34	4	**7**	0		$e_2 = 3$
139	23	3	$1+$**7**	0		
149	37	3	**9**	0		
151	25	3	$3+$**6**	??	??	
157	13	5	**7**	0		
163	27	$1+5$	**7**	1	0	
167	83	2	**12**	0		
173	43	4	**10**	0		
179	89	3	$1+$**11**	0		
181	15	5	**9**	0		$e_5 = 3$
191	95	2	**14**	0		
193	16	$2+5$	**8**	0		
197	49	$1+5$	**10**	0		
199	33	4	$2+\mathbf{10}_{3,11}$	??		$e_3 = 2$
211	35	$3+3$	$\mathbf{2}_5+\mathbf{9}_7$	0		$e_5 = 2$
223	37	$2+4$	**12**	0		
227	113	$2+3$	$2+2+$**10**	??	??	
229	19	$1+6$	**11**	0		
233	58	7	$\mathbf{1}_2^*+\mathbf{11}_{29}$	0		
239	119	3	**17**	0		
241	20	7	**12**	0		

Eisenstein factor is not simple, there is a subscript p to each boldface simple factor. If a factor has p as subscript, then it is a quotient of the p-Eisenstein quotient $\mathbf{J}^{(p)}$. An asterisk * signals a Neumann-Setzer curve (chap. III, § 7).

ν = the number of noncuspidal rational points on $X_0(N)$.

For ρ see theorem 7 above.

$e_p = \mathrm{rank}_{\mathbf{Z}_p} \mathbf{T}_{\mathfrak{P}}$, where $\mathfrak{P}$ is the Eisenstein prime associate to p and $\mathbf{T}_{\mathfrak{P}}$ is the completion at $\mathfrak{P}$. For the range of the table it is the case that $\mathbf{T}_{\mathfrak{P}}$ is a discrete valuation ring except when $N=113$ and $p=2$ (see chap. III, remark after (5.5) where this case is shown to be "forced" by the existence of a Neumann-Setzer factor).

Thus, for all entries of the table except $N=113$, $p=2$, e_p = absolute ramification index of $\mathbf{T}_{\mathfrak{P}}$. In the majority of cases $\mathbf{T}_{\mathfrak{P}} = \mathbf{Z}_p$ (equivalently: $e_p = 1$); therefore we only give e_p when it is greater than 1.

By forthcoming work of Brumer and Kramer [4] all the non-boldface elliptic curve factors of J^- (resp. J^+) on our table have Mordell-Weil rank 0 (resp. ≤ 1). The factorization of $J^{\pm}$ into simple components comes from tables of Atkin, Wada, and Tingley. The fact that $\mathbf{T}_{\mathfrak{P}}$ is integrally closed ($N \neq 113$) comes in part from a theorem (chap. II, (19.1)) and from Wada's tables, as do the calculations of e_p. The fact that the values of ρ given are the only possible involves work of Ogg, completed by Brumer and Parry (also see note added in proof at the end of chap. III, § 9).

TABLE OF CONTENTS

CONVENTIONS 43

I. — **Admissible groups** 43

1. Generalities 43
2. Extensions of μ_p by $\mathbf{Z}/\mathbf{p}$ over S 49
3. Etale admissible groups 54
4. Pure admissible groups 58
5. A special calculation for $p = 2$ 60

II. — **The modular curve $X_0(N)$** 62

1. Generalities 62
2. Ramification structure of $X_1(N) \to X_0(N)$ 64
3. Regular differentials 67
4. Parabolic modular forms 69
5. Nonparabolic modular forms 78
6. Hecke operators 87
7. Quotients and completions of the Hecke algebra 90
8. Modules of rank 1 92
9. Multiplicity one 93
10. The spectrum of $\mathbf{T}$ and quotients of J 97
11. The cuspidal and Shimura subgroups 98
12. The subgroup $D \subset J[P]$ ($p = 2$; n even) 103
13. The dihedral action on $X_1(N)$ 109
14. The action of Galois on the torsion points of J 112
15. The Gorenstein condition 123
16. Eisenstein primes (mainly $p \neq 2$) 124
17. Eisenstein primes ($p = 2$) 129
18. Winding homomorphisms 135
19. The structure of the algebra $\mathbf{T}_{\mathfrak{P}}$ 140

III. — **Arithmetic applications** 141

1. Torsion points 141
2. Points of complex multiplication 143
3. The Mordell-Weil group of J 148
4. Rational points on $X_0(N)$ 151
5. A complete description of torsion in the Mordell-Weil groups of elliptic curves over $\mathbf{Q}$ 156
6. Rational points on $X_{\text{split}}(N)$ 160
7. Factors of the Eisenstein quotient 161
8. The $\mathfrak{P}$-adic L series 164
9. Behavior in the cyclotomic tower 166

APPENDIX (*by* B. MAZUR and M. RAPOPORT). Behavior of the Néron model of the jacobian of $X_0(N)$ at bad primes 173

CONVENTIONS

N : a fixed *prime* number ≥ 5 (the level) [1].

n : numerator $\left(\frac{N-1}{12}\right)$.

S : Spec $\mathbf{Z}$.

S′ : Spec $\mathbf{Z}[1/N]$.

If p is a prime number we write $p^f || n$ when p^f is the highest power of p dividing n.

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

$J_{/S}$: the Néron model of the jacobian of $X_0(N)$.

$\mathbf{T}$: the Hecke algebra acting on $J_{/S}$ (chap. II, § 6).

$\mathfrak{I}$: the Eisenstein ideal in $\mathbf{T}$ (chap. II, § 9).

$\mathfrak{P}$: the Eisenstein prime associated to a prime number p (chap. II, § 9).

$\mathfrak{M}$: a general maximal prime ideal in $\mathbf{T}$ (not necessarily Eisenstein).

If $\mathfrak{a} \subset \mathbf{T}$ is an ideal, then $\mathbf{T}_{\mathfrak{a}}$ denotes completion with respect to $\mathfrak{a}$. If m is an integer and A an object of an abelian category, then $A[m]$ denotes the kernel of multiplication by m.

I. — ADMISSIBLE GROUPS

1. Generalities.

Consider quasi-finite separated commutative group schemes of finite presentation over the base $S = \operatorname{Spec} \mathbf{Z}$ which are finite flat group schemes over $S' = \operatorname{Spec} \mathbf{Z}[1/N]$. In this chapter we refer to such an object as a *group scheme* or (if there is no possible confusion) a *group* over S (or over whatever restriction of the base S concerns us). If $G_{/S}$ is such a group scheme, its *associated Galois module* is the (finite) $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-module $G(\bar{\mathbf{Q}})$ (of $\bar{\mathbf{Q}}$-rational points of G, where $\bar{\mathbf{Q}}$ is some fixed algebraic closure of $\mathbf{Q}$). By the *order* of $G_{/S}$ we mean the order of the finite abelian group $G(\bar{\mathbf{Q}})$, or, equivalently. the rank over $\mathbf{Z}[1/N]$ of the affine algebra of the scheme $G_{/S'}$ (*rank* meaning its rank as locally free $\mathbf{Z}[1/N]$-module). For the general properties of group schemes the reader

[1] In the appendix we consider more general N.

may consult [40], [9]. *We now fix a prime number p* different from N, and *suppose that the order of* $G_{/S}$ *is a power of p.* In this case, if $S''=\operatorname{Spec}\mathbf{Z}[1/p]$, $G_{/S''}$ is an *étale* quasi-finite group ([41], lemma 5) and consequently it is an étale *finite* group over:

$$S'\cap S''=\operatorname{Spec}\mathbf{Z}[1/p.N],$$

determined up to isomorphism by its associated Galois module, which is a representation of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on $G(\bar{\mathbf{Q}})$—unramified except possibly at p and N.

(a) *The structure of* G *away from p*:

Let us fix a choice of compatible algebraic closures:

$$\begin{array}{ccccccc} \bar{\mathbf{Q}} & \hookrightarrow & \bar{\mathbf{Q}}_N & \hookleftarrow & \bar{\mathbf{Z}}_N & \twoheadrightarrow & \bar{\mathbf{F}}_N \\ | & & | & & | & & | \\ \mathbf{Q} & \hookrightarrow & \mathbf{Q}_N & \hookleftarrow & \mathbf{Z}_N & \twoheadrightarrow & \mathbf{F}_N \end{array} \tag{1.1}$$

Let $G_{/S''}$ be a group scheme as above. It is given, over S'', by the following diagram of *compatible* Galois modules:

$$G(\bar{\mathbf{F}}_N) \xrightarrow{j} G(\bar{\mathbf{Q}}) \tag{1.2}$$

where $G(\bar{\mathbf{Q}})$ is the Galois module (the $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-module) associated to $G_{/\mathbf{Q}}$, $G(\bar{\mathbf{F}}_N)$ is the $\mathrm{Gal}(\bar{\mathbf{F}}_N/\mathbf{F}_N)$-module associated to $G_{/\mathbf{F}_N}$ and the homomorphism j maps $G(\bar{\mathbf{F}}_N)$ into the part of $G(\bar{\mathbf{Q}})$ which is fixed under the action of the inertia subgroup of $\mathrm{Gal}(\bar{\mathbf{Q}}_N/\mathbf{Q}_N)$. The homomorphism j is compatible with Galois action (compatibility being defined in an evident manner using (1.1)) and it is *injective* since G is assumed to be separated.

(b) *Extensions of group schemes from* S' *to* S:

Let $G'_{/S'}$ be a group scheme (as at the beginning). To give an *extension*, $G_{/S}$ of G' to the base S (up to canonical isomorphism) amounts to giving a sub-$\mathrm{Gal}(\bar{\mathbf{Q}}_N/\mathbf{Q}_N)$-module $H\subset G(\bar{\mathbf{Q}})$ whose elements are fixed under the inertia group at N. For the sub-$\mathrm{Gal}(\bar{\mathbf{Q}}_N/\mathbf{Q}_N)$-module H then inherits a $\mathrm{Gal}(\bar{\mathbf{F}}_N/\mathbf{F}_N)$-structure and $H\subset G(\bar{\mathbf{Q}})$ may be viewed as a compatible diagram of Galois modules of the form (1.2). This compatible diagram gives us an étale quasi-finite group scheme $G''_{/S''}$ and an isomorphism:

$$G''_{/S''\cap S'}\cong G'_{/S'\cap S''},$$

which, by patching, gives our extension $G_{/S}$.

For a given $G'_{/S'}$ there is a *minimal* and a *maximal* extension to the base S, which we shall denote $G^\flat$ and $G^\sharp$ respectively. The minimal extension (*extension-by-zero*; compare [33]) $G^\flat$ is defined by taking $H=\{0\}\subset G(\bar{\mathbf{Q}})$. The maximal extension $G^\sharp$ is defined by taking H to be the subgroup of $G(\bar{\mathbf{Q}})$ consisting in all elements invariant under the inertia group at N. If $G_{/S}$ is any extension of $G'_{/S'}$, we have $G^\flat\subset G\subset G^\sharp$.

From this discussion we have:

Proposition (**1.3**). — *These are equivalent*:

(i) $G'_{/S'}$ *admits an extension* $G_{/S}$ *which is a finite flat group scheme.*

(ii) *The inertia group at* N *operates trivially in the* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$*-module associated to* $G'_{/S'}$.

(iii) $G^{\sharp}_{/S}$ *is a finite flat group scheme.*

(c) *Subgroup scheme extensions*:

Let $G_{/S}$ be a group scheme as above, and let $H(\overline{\mathbf{Q}})$ be any sub-$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-module of $G(\overline{\mathbf{Q}})$. By the *subgroup scheme extension to* S, $H_{/S}$, of $H(\overline{\mathbf{Q}})$ we mean the scheme-theoretic closure of $H(\overline{\mathbf{Q}})$ in $G_{/S}$. To understand this, it is perhaps best to consider it over the bases S′ and S″ separately.

Over S′, we are taking the scheme-theoretic closure of $H(\overline{\mathbf{Q}})$ in the finite flat group scheme $G_{/S'}$ [55], which is a finite flat subgroup scheme $H_{/S'} \subset G_{/S'}$ whose associated Galois module is our $H(\overline{\mathbf{Q}})$ [55].

To describe it over S″ we must give its "diagram (1.2)" $H(\overline{\mathbf{F}}_N) \subset H(\overline{\mathbf{Q}})$; one sees easily that $H(\overline{\mathbf{F}}_N) = H(\overline{\mathbf{Q}}) \cap G(\overline{\mathbf{F}}_N)$, the intersection taking place in $G(\overline{\mathbf{Q}})$.

It follows that the subgroup scheme extension of $H(\overline{\mathbf{Q}})$ in $G_{/S}$ is a quasi-finite *closed* subgroup scheme $H_{/S} \subset G_{/S}$ which is finite and flat over S′, and whose associated Galois module is our original $H(\overline{\mathbf{Q}})$. Moreover, this construction provides a one-one correspondence between sub-$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules in $G(\overline{\mathbf{Q}})$ and closed subgroup schemes in $G_{/S}$.

If $H_{/S} \subset G_{/S}$ is a closed subgroup scheme, we may consider the *quotient* $(G/H)_{/S}$ ([SGA 3], exp. V, VI_B) first as sheaf for the *fppf* topology. This quotient is representable by a group scheme (of the type we are considering) as can be seen, again, by working separately over the bases S′ and S″: Over S′, $H_{/S}$ is a finite flat subgroup scheme of the finite flat group scheme $G_{/S}$, and the quotient is representable, by [57] theorem 1. Over S″, one easily constructs the "diagram (1.2)" of the quotient and one finds:

$$\begin{array}{ccc}
0 & & 0 \\
\downarrow & & \downarrow \\
H(\overline{\mathbf{F}}_N) & \xrightarrow{j_H} & H(\overline{\mathbf{Q}}) \\
\downarrow & & \downarrow \\
G(\overline{\mathbf{F}}_N) & \xrightarrow{j_G} & G(\overline{\mathbf{Q}}) \\
\downarrow & & \downarrow \\
(G/H)(\overline{\mathbf{F}}_N) & \xrightarrow{j_{G/H}} & (G/H)(\overline{\mathbf{Q}}) \\
\downarrow & & \downarrow \\
0 & & 0
\end{array}$$

where $j_{(G/H)}$ is injective because $H(\overline{\mathbf{F}}_N) = G(\overline{\mathbf{F}}_N) \cap H(\overline{\mathbf{Q}})$.

It follows from this discussion that there is a one-one correspondence between filtrations of $G_{/S}$ by closed subgroup schemes, and filtrations of $G(\overline{\mathbf{Q}})$ by sub-$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules. Moreover the successive quotients of any filtration of $G_{/S}$ by closed subgroup schemes are again group schemes (of the type we are considering), and their associated Galois modules are canonically isomorphic to the successive quotients of the corresponding filtration of $G(\overline{\mathbf{Q}})$.

(d) *Determining* $G_{/S'}$ *by its associated Galois module*:

Here is a consequence of the work of Fontaine.

Theorem **(1.4)** *(Fontaine).* — *Let* $G^{(1)}_{/S'}$, $G^{(2)}_{/S'}$ *be two finite flat p-primary group schemes with isomorphic associated Galois modules. If either*:

(a) $p \neq 2$ *or*

(b) $G^{(i)}_{/\mathbf{F}_2}$ *are both unipotent finite group schemes.*

Then $G^{(1)}_{/S'}$ *is isomorphic to* $G^{(2)}_{/S'}$.

Discussion. — By Fontaine's theorem 2 [14] and the subsequent remark (p. 1424), the isomorphism between the associated Galois modules extends to an isomorphism: $G^{(1)}_{/\mathbf{Z}_p} \cong G^{(2)}_{/\mathbf{Z}_p}$ (Fontaine works over the Witt vectors of a perfect field).

A standard patching argument gives the version of Fontaine's result quoted above.

(e) *Vector group schemes of rank* 1.

If $V_{/S'}$ is a finite flat group scheme killed by p, we may view $V_{/S'}$ in a natural way as admitting an $\mathbf{F}_p$-module structure. If k is any finite field and $V_{/S'}$ is endowed with a k-module structure, we shall call $V_{/S'}$ a *k-vector group scheme.* The *rank* of $V_{/S'}$ (as k-vector group scheme) is the dimension of the k-vector space $V(\overline{\mathbf{Q}})$. If $V_{/S'}$ is a k_1-vector group scheme and k_2/k_1 is a finite field extension, then by $V \otimes_{k_1} k_2$ the evident construction is meant (one takes the direct sum of as many copies of V as there are elements in a k_1-basis of k_2, and gives it the natural k_2-module structure).

Proposition **(1.5)**. — *Let k be a finite field of characteristic p. Let* $V_{/S}$ *be a finite flat k-vector group scheme of rank* 1. *Then either* $V_{/S} \cong (\mathbf{Z}/\mathbf{p})_{/S} \otimes_{\mathbf{F}_p} k$ *or*: $V_{/S} \cong \boldsymbol{\mu}_{p/S} \otimes_{\mathbf{F}_p} k$.

Proof. — The $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-representation of a k-vector group of rank 1 is given by a character $\chi : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to k^*$ and hence determines a cyclic abelian extension of $\mathbf{Q}$ of order dividing $p^f - 1$ ($p^f = \mathrm{card}(k)$) unramified except at p. Such an extension must be contained in $\mathbf{Q}(\zeta_p)$ (ζ_p a primitive p-th root of 1) and therefore has order dividing $p-1$. Consequently the character χ takes values in $\mathbf{F}_p^* \subset k^*$ and it follows that there is a sub-$\mathbf{F}_p$-vector group scheme of rank 1, $V_{0/S} \subset V_{/S}$ whose associated $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ representation is given by the character $\chi : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{F}_p^*$. By the Oort-Tate classification theorem ([54], Cor. to thm. 3) applied to the group scheme of order p, $V_{0/S}$,

one has that $V_{0/\mathbf{F}_p}$ is either of multiplicative type or étale (1). Replacing $V_{/S}$ by its Cartier dual, if necessary, we may suppose that $V_{0/S}$ is étale, and consequently the character χ is trivial.

Moreover, the group scheme $(V_{/\mathbf{F}_p})^{\text{ét}}$ has a k-module structure and is nontrivial since it contains $V_{0/\mathbf{F}_p}$. Its order is then $\geq q$, and at the same time $\leq q$ since the order of $V_{/S}$ is q. It follows that $V_{/S}$ is étale, and has trivial $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-action; it follows that as k-vector group scheme, $V_{/S} = (\mathbf{Z}/\mathbf{p}) \otimes_{\mathbf{F}_p} k$.

For a detailed study of k-vector group schemes, especially of rank 1, see Raynaud's [55].

Corollary (**1.6**). — *Let* $V_{/S}$ *be a group scheme of order* p.

(i) *Let* $p \neq 2$. *If the associated Galois module to* V *is* $\mathbf{Z}/p$, *then* $V_{/S'} \cong (\mathbf{Z}/\mathbf{p})_{/S'}$. *If the associated Galois module to* V *is* $\boldsymbol{\mu}_p$, *then* $V_{/S'} \cong \boldsymbol{\mu}_{p/S'}$.

(ii) *Let* $p = 2$. *Then* $V_{/S'}$ *is isomorphic either to* $(\mathbf{Z}/\mathbf{2})_{/S'}$ *or to* $\boldsymbol{\mu}_{2/S'}$.

(f) *Admissible* p*-groups.*

Definition. — *An admissible* (p-)*group* G *over* S (or *over* S′) is a group scheme (as usual in this chapter: commutative, quasi-finite, separated, flat, such that $G_{/S'}$ is finite and flat) which is killed by a power of p, and such that $G_{/S'}$ possesses a filtration by finite flat subgroup schemes such that the successive quotients are S′-isomorphic to one of the two group schemes: $\mathbf{Z}/\mathbf{p}$ or $\boldsymbol{\mu}_p$ (called an *admissible filtration*).

By (1.6) and (c) $G_{/S'}$ possesses an admissible filtration if and only if its associated $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-module possesses a filtration by sub-$\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-modules whose successive quotients are isomorphic to the $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-modules $\mathbf{Z}/p$ or $\boldsymbol{\mu}_p$ (called an *admissible filtration* of a $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-module).

Clearly a closed subgroup scheme of an admissible p-group is again admissible, as is the quotient group scheme of an admissible p-group by a closed subgroup scheme. We have the notion of *short exact sequence of* admissible p-groups:

$$0 \to G_1 \to G_2 \to G_3 \to 0$$

where G_1 is closed in G_2 and the morphism $G_2 \to G_3$ induces an isomorphism of *fppf* sheaves $G_2/G_1 \xrightarrow{\sim} G_3$.

To an admissible p-group we may attach the following numerical invariants:

$$\ell(G) = \log_p(\text{order of } G_{/S'}) \quad \text{(the } \textit{length} \text{ of G)}$$

$$\delta(G) = \log_p(\text{order of } G_{/S'}) - \log_p(\text{order of } G_{/\mathbf{F}_N}) \quad \text{(the } \textit{defect} \text{ of G)}$$

$\alpha(G) =$ the number of $(\mathbf{Z}/\mathbf{p})$'s occurring as successive quotients in an admissible filtration of $G_{/S'}$.

---

(1) We may deduce this from the following simple consequence of the theory of Oort-Tate, which may also be checked directly: The group scheme $\boldsymbol{\alpha}_p$ over the base Spec $(\mathbf{Z}/p)$ admits no extension to a finite flat group of order p over the base Spec $(\mathbf{Z}/p^2)$.

$h^i(G) = \log_p(\text{order}(H^i(S, G)))$, cohomology being taken for the *fppf* topology ([SGA 3], Exp IV, § 6).

Remarks. — The invariant $\ell(G) = \log_p(\text{order } G(\overline{\mathbf{Q}}))$ depends only on the Galois module associated to G. The invariant $\delta(G)$ is detectable from the structure of $G_{/\text{Spec}(\mathbf{Z}_N)}$. The invariant $\alpha(G)$ is detectable from the structure of $G_{/\mathbf{F}_p}$:

$$\alpha(G) = \log_p(\text{order } G(\overline{\mathbf{F}}_p)).$$

If $p \neq 2$, one can also determine $\alpha(G)$ from the $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-module structure of $G(\overline{\mathbf{Q}})$. This is, of course not the case if $p = 2$.

We are mainly interested, in this paper, in h^i for $i = 0, 1$. Note that:

$$H^0(S, G) = G(S),$$

while $H^1(S, G)$ may be given an appropriate " geometric " interpretation.

(g) *Elementary admissible p-groups.*

By an *elementary* admissible group G we shall mean an admissible group of *length one*. Up to isomorphism there are *four* elementary admissible p-groups:

$$\mathbf{Z}/\mathbf{p},\ \mathbf{Z}/\mathbf{p}^\flat,\ \mu_p,\ \mu_p^\flat$$

where $(\mathbf{Z}/\mathbf{p}^\flat)_{/S}$ is, as in (b), the extension-by-zero of $(\mathbf{Z}/\mathbf{p})_{/S'}$ and similarly with $\mu^\flat_{p/S'}$.

The invariants of these elementary groups are given by the following table:

	$\mathbf{Z}/\mathbf{p}^\flat$	$\mathbf{Z}/\mathbf{p}$	μ_p	$\mu_p^\flat$
δ	0	1	0	1
α	1	1	0	0
h^0	1	0	$0 (p \neq 2)$ $1 (p = 2)$	0
h^1	0	0	$0 (p \neq 2)$ $1 (p = 2)$	ε

where $\varepsilon = \begin{cases} 0 & \text{if } N \not\equiv 1 \bmod p \quad (p \text{ odd}) \\ & \text{or } N \equiv -1 \bmod 4 \quad (p = 2) \\ 1 & \text{otherwise.} \end{cases}$

It is straight forward to establish the first three lines of the above table. To compute $H^1(S, \mu_p)$ use the Kummer sequence (of *fppf* sheaves) $0 \to \mu_p \to \mathbf{G}_m \to \mathbf{G}_m \to 0$ giving: $H^1(S, \mu_p) = (\mathbf{Z}^*)/(\mathbf{Z}^*)^p$ since the ideal class group of $\mathbf{Z}$ is zero. Also, $H^1(S, \mathbf{Z}/\mathbf{p}) = 0$ because there are no unramified cyclic p-extensions of $\mathbf{Q}$.

The nontrivial class in $H^1(S, \mu_2)$ is represented by the S-scheme $\text{Spec } \mathbf{Z}[\sqrt{-1}]$, regarded as μ_2—principal homogeneous space (torseur) over S. Forming the exact sequences of *fppf* sheaves over S:

$$0 \to \mathbf{Z}/\mathbf{p}^b \to \mathbf{Z}/\mathbf{p} \to \varphi \to 0$$
$$0 \to \boldsymbol{\mu}_p^b \to \boldsymbol{\mu}_p \to \psi \to 0,$$

one computes $H^0(S, \varphi) = \mathbf{Z}/p$; $H^0(S, \psi) = \boldsymbol{\mu}_p(\mathbf{F}_N)$. The natural map:

$$H^1(S, \boldsymbol{\mu}_2) \to H^1(S, \psi)$$

is injective if and only if the principal homogeneous space Spec $\mathbf{Z}[\sqrt{-1}]$ for $\boldsymbol{\mu}_2$ over S does *not* split when restricted to the base Spec $\mathbf{F}_N$ (*i.e.* when $N \equiv -1 \bmod 4$). These facts establish the table.

Proposition (**1.7**). — *Let* $G_{/S}$ *be an admissible group. Then*:

$$h^1(G) - h^0(G) \leq \delta(G) - \alpha(G).$$

Proof. — The right hand side of the above inequality is additive for short exact sequences of admissible groups. The left hand side is *sub-additive* in the sense that if $0 \to G_1 \to G_2 \to G_2 \to 0$ is such a short exact sequence, then:

$$h^1(G_2) - h^0(G_2) \leq (h^1(G_1) - h^0(G_1)) + (h^1(G_3) - h^0(G_3)).$$

To see this, one simply uses the long exact sequence of *fppf* cohomology coming from our short exact sequence. One clearly has equality if, instead of $h^1(G_3)$ one inserts $h^1(G_3)' = \log_p(\text{order}(\text{image } H^1(G_2) \text{ in } H^1(G_3)))$ in the displayed line above. The asserted subadditivity follows.

Since any admissible group G has a filtration by closed subgroup schemes whose successive quotients are elementary admissible groups, the discussion above reduces the problem of checking the asserted inequality for *any* admissible group to the same problem for *elementary* admissible groups, where it follows from an inspection of the table above.

Remark. — When $\varepsilon = 1$ (which will be the case in our applications) the asserted inequality is, in fact, an equality for elementary admissible groups.

2. Extensions of μ_p by Z/p over S.

The point of this section is to show that there are no nontrivial such extensions.

Proposition (**2.1**). — *Let p be any prime number. Then*:

$$\text{Ext}^1_S(\boldsymbol{\mu}_p, \mathbf{Z}/\mathbf{p}) = 0.$$

Proof (1). — To begin, we reduce our problem to a calculation in étale cohomology. Let Sch $\boldsymbol{\mu}_{p/S}$ denote the underlying scheme (ignoring group structure) and let:

$$s : \text{Sch } \boldsymbol{\mu}_p \times \text{Sch } \boldsymbol{\mu}_p \to \text{Sch } \boldsymbol{\mu}_p,$$

be the group law.

---

(1) An alternate approach to the proof of (2.1) in the case of an odd prime p is to show that an element of $\text{Ext}^1_S(\boldsymbol{\mu}_p, \mathbf{Z}/\mathbf{p})$ must go to zero in $\text{Ext}^1_{\text{Spec } \mathbf{Q}}$, using Herbrand's theorem below, and the argument of chapter III, § 5. One then could apply Fontaine's theorem (1.4) to conclude.

Since Sch $\mu_{p/S}$ is connected, and $(\mathbf{Z}/\mathbf{p})_{/S}$ is étale, there are no nontrivial 2-cocycles for $\mu_{p/S}$ with coefficients in $(\mathbf{Z}/\mathbf{p})_{/S}$, and therefore $\mathrm{Ext}^1_S(\mu_p, \mathbf{Z}/\mathbf{p})$ is the kernel of:

$$\mathrm{H}^1(\mathrm{Sch}\ \mu_p, \mathbf{Z}/\mathbf{p}) \xrightarrow{s^*-\pi_1^*-\pi_2^*} \mathrm{H}^1(\mathrm{Sch}\ \mu_p \times \mu_p, \mathbf{Z}/\mathbf{p})$$

where π_i are the first and second projections $(i=1, 2)$ and cohomology is computed for the *fppf* topology or ([15], § 11) since $\mathbf{Z}/\mathbf{p}$ is étale, for the étale topology. To see the assertion made, the reader may verify it directly, following [12] and *(e.g.)* [SGA 3], exp. III, § 1.

If X, Y are any two schemes equipped with $\mathbf{F}_p$-valued points:

$$\begin{array}{ccc} & & \mathrm{X} \\ & \nearrow & \\ \mathrm{Spec}\ \mathbf{F}_p & & \\ & \searrow & \\ & & \mathrm{Y} \end{array} \tag{2.1}$$

we allow ourselves to use the symbol $\mathrm{X} \vee \mathrm{Y}$ to refer to *any* scheme-theoretic union of X and Y along (subschemes which are nilpotent extensions of) $\mathrm{Spec}(\mathbf{F}_p)$. Taking $\mathrm{Spec}(\mathbf{F}_p) \to \mathrm{X}$ to be one such scheme, and $\mathrm{Y} = \mathrm{S} = \mathrm{Spec}(\mathbf{Z})$ to be the other, denote by $\tilde{\mathrm{H}}^1(\mathrm{X})$ *the* étale cohomology group $\mathrm{H}^1(\mathrm{X} \vee \mathrm{Y}, \mathbf{Z}/\mathbf{p})$. One obtains an exact sequence:

$$0 \to \tilde{\mathrm{H}}^1(\mathrm{X}) \to \mathrm{H}^1(\mathrm{X}, \mathbf{Z}/\mathbf{p}) \to \mathrm{H}^1(\mathrm{Spec}(\mathbf{F}_p), \mathbf{Z}/\mathbf{p})$$

using: the Mayer-Vietoris exact sequence for étale cohomology, the fact that $\mathrm{Spec}(\mathbf{F}_p)$ is connected, and that $\mathrm{H}^1(\mathrm{S}, \mathbf{Z}/\mathbf{p}) = 0$. We learn, in particular, that the group $\tilde{\mathrm{H}}^1(\mathrm{X})$ is independent of *which* scheme-theoretic union of X and Y was made (provided that it is subject to the above conditions). A similar calculation gives an additivity formula for $\tilde{\mathrm{H}}^1$ (for any diagram (2.1)):

$$\tilde{\mathrm{H}}^1(\mathrm{X} \vee \mathrm{Y}) = \tilde{\mathrm{H}}^1(\mathrm{X}) \oplus \tilde{\mathrm{H}}^1(\mathrm{Y}). \tag{2.2}$$

We may write Sch $\mu_p = \mathrm{T} \vee \mathrm{S}$ where T denotes the " cyclotomic scheme ":

$$\mathrm{Spec}(\mathbf{Z}[x]/(x^{p-1} + x^{p-2} + \ldots + 1)).$$

If M denotes the p-primary component of the Galois group of the Hilbert class field extension of (the field of fractions of) $\mathbf{Z}[x]/(x^{p-1} + x^{p-2} + \ldots + 1)$, then:

$$\mathrm{H}^1(\mathrm{T}, \mathbf{Z}/\mathbf{p}) = \mathrm{Hom}(\mathrm{M}, \mathbf{Z}/p).$$

Therefore by (2.3), if $\tilde{\mathrm{M}}$ is the maximal quotient of M such that p splits completely in the field extension classified by $\tilde{\mathrm{M}}$, we have:

$$\tilde{\mathrm{H}}^1(\mathrm{T}) = \mathrm{Hom}(\tilde{\mathrm{M}}, \mathbf{Z}/p). \tag{2.5}$$

The automorphism group of $\mu_{p/S}$ maps to the automorphism group of the scheme T and we have canonical identifications:

$$\mathrm{Aut}(\mu_{p/S}) = \mathrm{Aut}(\mathrm{T}) = \mathbf{F}_p^*$$

where $a \in \mathbf{F}_p^*$ operates by $\sigma_a =$ " raising to the a-th power " in the group scheme μ_p. The isomorphism (2.5) is compatible with this action in the following sense:

If $a\in\mathbf{F}_p^*$ and $\varphi\in\mathrm{Hom}(\widetilde{M}, \mathbf{Z}/p)$, then $\varphi(m)=(\sigma_a.\varphi)(\sigma_a.m)$ where the action of σ_a on M is the natural action of the morphism $\sigma_a : T\to T$ on $M\subseteq H_1(T)$ (one-dimensional homology).

To decompose our spaces into eigenspaces for the action of $\mathbf{F}_p^*$ we need some terminology: If H is a $\mathbf{Z}_p[\mathbf{F}_p^*]$-module and $j\in\mathbf{Z}/(p-1)\mathbf{Z}$, let $H^{(j)}=\{h\in H \mid \sigma_a.h=a^j.h\}$ (where if $a\in\mathbf{F}_p^*$ we denote its operation on H by σ_a). Then $H=\bigoplus H^{(j)}$, the summation being taken over all $j\in\mathbf{Z}/(p-1)\,\mathbf{Z}$.

By the compatibility formula above, we get:

(2.6) $$\widetilde{H}^1(T)^{(j)}=\mathrm{Hom}(\widetilde{M}^{(-j)}, \mathbf{Z}/p)$$

for all $j\in\mathbf{Z}/(p-1)\mathbf{Z}$.

Note that $\mathrm{Sch}(\mu_p\times\mu_p)$ is *a* wedge (in the sense of $\vee$) of S with $p+1$ copies of T; these copies can be considered as the images:

$$T\subset \mathrm{Sch}\ \mu_p \overset{\tau}{\hookrightarrow} \mathrm{Sch}(\mu_p\times\mu_p)$$

where, to be noncanonical for a moment, we may take the maps τ to be given by the set of 2×1 matrices:

$$(a, 1) \text{ for } a=0, 1, \ldots, p-1 \text{ and } (1, 0).$$

Using (2.2) we obtain that $H^1(\mathrm{Sch}(\mu_p\times\mu_p))$ is a direct sum of $p+1$ copies of $\widetilde{H}^1(T)$. Let us describe this group in a more " choice-free " manner.

Consider *all* imbeddings $\tau : \mu_p\hookrightarrow\mu_p\times\mu_p$. The 2×1 matrices representing all imbeddings τ range through the set of nonzero elements of $\mathbf{F}_p\times\mathbf{F}_p$. Let Funct(A, B) denote the set of functions from A to B and form:

$$H^1(\mathrm{Sch}(\mu_p\times\mu_p)) \overset{\beta}{\to} \mathrm{Funct}(\mathbf{F}_p\times\mathbf{F}_p, \widetilde{H}^1(T))$$

by sending $h\in H^1(\mathrm{Sch}(\mu_p\times\mu_p))$ to the function $(\tau\mapsto\tau^*h)$. Let $\Phi_{\mathbf{F}^*}(\mathbf{F}_p\times\mathbf{F}_p, \widetilde{H}^1(T))$ denote those functions which send (0, 0) in $\mathbf{F}_p\times\mathbf{F}_p$ to 0 in $\widetilde{H}^1(T)$, and which are compatible with the natural action of $\mathbf{F}_p^*$ on domain and range.

From our noncanonical description of $H^1(\mathrm{Sch}(\mu_p\times\mu_p))$ it follows that β induces an *isomorphism* between $H^1(\mathrm{Sch}(\mu_p\times\mu_p))$ and $\Phi_{\mathbf{F}_p^*}(\mathbf{F}_p\times\mathbf{F}_p, \widetilde{H}^1(T))$.

By the analogous but easier construction for Sch μ_p we get an isomorphism:

$$\widetilde{H}^1(\mathrm{Sch}\ \mu_p) \xrightarrow{\sim} \Phi_{\mathbf{F}_p^*}(\mathbf{F}_p, \widetilde{H}^1(T))=\widetilde{H}^1(T)$$

and one can check the commutative diagram:

$$\begin{array}{ccc} H^1(\mathrm{Sch}\ \mu_p) & \xrightarrow{s^*-\pi_1^*-\pi_2^*} & H^1(\mathrm{Sch}(\mu_p\times\mu_p)) \\ \| & & \| \\ \Phi_{\mathbf{F}_p^*}(\mathbf{F}_p, \widetilde{H}^1(T)) & \xrightarrow{\delta} & \Phi_{\mathbf{F}_p^*}(\mathbf{F}_p\times\mathbf{F}_p, \widetilde{H}^1(T)) \end{array}$$

where δ is just the obstruction-to-linearity:

If $f \in \Phi_{\mathbf{F}_p^*}(\mathbf{F}_p, \tilde{H}^1(T))$ then $\delta f(x,y) = f(x+y) - f(x) - f(y)$.

We are reduced to analyzing the kernel of δ, the obstruction-to-linearity. Let Φ_j denote functions which bring 0 to 0 and are homogeneous of degree j, under the natural action of $\mathbf{F}_p^*$ on domain and range. Thus:

$$\begin{array}{ccc} \Phi_{\mathbf{F}_p^*}(\mathbf{F}_p, \tilde{H}^1(T)) & \xrightarrow{\delta} & \Phi_{\mathbf{F}_p^*}(\mathbf{F}_p \times \mathbf{F}_p, \tilde{H}^1(T)) \\ \cong \downarrow & & \cong \downarrow \\ \bigoplus_j \Phi_j(\mathbf{F}_p, \mathbf{F}_p) \otimes \tilde{H}^1(T)^{(j)} & \xrightarrow[\delta]{} & \bigoplus_j \Phi_j(\mathbf{F}_p \times \mathbf{F}_p, \mathbf{F}_p) \otimes \tilde{H}^1(T)^{(j)} \end{array}$$

where the summation is taken over $j \in \mathbf{Z}/(p-1)\mathbf{Z}$. We are led to consider the maps:

(2.7) $$\Phi_j(\mathbf{F}_p, \mathbf{F}_p) \xrightarrow[\delta]{} \Phi_j(\mathbf{F}_p \times \mathbf{F}_p, \mathbf{F}_p)$$

for each $j \in \mathbf{Z}/(p-1)\,\mathbf{Z}$. Clearly $\Phi_j(\mathbf{F}_p, \mathbf{F}_p)$ is a one-dimensional vector space over $\mathbf{F}_p$ generated by the function $x \mapsto x^j$, and δ applied to it is the function $(x+y)^j - x^j - y^j$. Thus (2.7) is injective if $j \neq 1$. To show that $\mathrm{Ext}^1_{\mathcal{S}}(\boldsymbol{\mu}_p, \mathbf{Z}/\mathbf{p}) = 0$ it therefore suffices to show that $\tilde{H}^1(T)^{(1)} = 0$.

Equivalently it suffices to show that $\tilde{M}^{(-1)} = 0$. In fact, $M^{(-1)}$ vanishes. This is a consequence of a theorem of Herbrand [20] together with the calculation of the second Bernoulli number.

For the convenience of the reader, we shall reprove the theorem of Herbrand, which follows from the theorem of Clausen-von Staudt, Kummer's congruence, a power summation congruence (cf. [72], chap. V, § 8) and Stickelberger's theorem (cf. [23]).

To prepare, let the Bernoulli numbers B_i be defined by:

$$t/(e^t - 1) = \sum_i B_i t^i / i! \quad (1)$$

and the Bernoulli polynomials:

$$B_n(X) = \sum_i \binom{n}{i} . B_i . X^{n-i}$$

(So $B_0 = 1$, $B_1 = -1/2$, ...).

We have these classical facts:

If p is a prime, $p . B_m$ is a p-integer, and B_m itself is a p-integer provided $m \not\equiv 0 \bmod (p-1)$ (Clausen-von Staudt).

If p is a prime, and $m \not\equiv 0 \bmod (p-1)$, then B_m/m is a p-integer whose residue class mod p *depends only on $m \bmod (p-1)$:*

$$B_m/m \equiv B_{m+p-1}/(m+p-1) \bmod p \quad \textit{(Kummer)}.$$

---

(1) This differs from Iwasawa's choice [22].

Let p be an odd prime number. Suppose k is a nonnegative integer such that $k+1 \not\equiv 0 \bmod p$, and $k-1 \not\equiv 0 \bmod (p-1)$. Then:

$$\sum_{a=0}^{p-1} a^k \equiv p.B_k \bmod p^2.$$

(*Power summation congruence* [72], chap. V (8.11) Cor. to theorem 4.)

To apply the Stickelberger theorem, we use the class field theory isomorphism to identify the Galois group of the Hilbert class field of $K=\mathbf{Q}[x]/(x^{p-1}+\ldots+1)$ with the ideal class group of K (1). Let Y denote the p-primary component of this ideal class group. Thus:

$$M \underset{\approx}{\overset{\theta}{\to}} Y.$$

It is important to check that θ commutes with the natural action of $\mathbf{F}_p^*$ on domain and range. The action on the domain may be viewed as follows: If L/K is the Hilbert class field extension, then L/$\mathbf{Q}$ is Galois and the natural action of G on itself by inner automorphisms $(\iota_g(x)=gxg^{-1})$ induces an action of $\mathbf{F}_p^*$ on M, which is equal to the action considered above.

The action on Y is induced by the natural action of $\mathbf{F}_p^* = \mathrm{Gal}(K/\mathbf{Q})$ on ideals.

The fact that θ commutes with these actions is, then, VII, theorem (11.5) (i) of [5].

Thus, we have:

$$M^{(j)} = Y^{(j)}.$$

In what follows we suppose that $p>2$ and j is *odd*. This makes sense because j is an integer $\bmod(p-1)$ and p is odd. For convenience, take j to be an ordinary integer in the range $0<j<p-1$. Write $\bar{j}=p-1-j$ (so $\bar{j}\equiv -j \bmod(p-1)$, and $0<\bar{j}<p-1$).

Let $\omega : \mathbf{F}_p^* \to \mathbf{Z}_p^*$ be the Teichmüller character.

We shall now quote (what is, in essence) Stickelberger's theorem (cf. Iwasawa's *p-adic* L *functions* [23]. Our " Y " replaces his " S_0 "):

Proposition **(2.8).** — $Y^{(1)}=0$. *If* $j\neq 1$, *then the p-adic number*:

$$\xi_j = (1/p)\sum_{a=0}^{p-1} a.\omega^{-j}(a)$$

is a p-adic integer, and $\xi_j.Y^{(j)}=0$.

Corollary **(2.9)** *(Herbrand).* — *Let j be odd and different from* 1. *If* $B_{p-j}\not\equiv 0 \bmod p$, *then* $Y^{(j)}=0$.

Proof. — We show, under the hypotheses of the corollary, that ξ_j is a p-adic unit. For this, we examine:

$$\sum_{a=0}^{p-1} a.\omega^{-j}(a) = \sum_{a=0}^{p-1} a.\omega^{\bar{j}}(a) \bmod p^2.$$

(1) For definiteness, take the class field theory isomorphism θ to be the map induced from ψ^{-1} as in [5], VII, § 5.

Since $\omega(a) \equiv a^p \bmod p^2$, $\sum_{a=0}^{p-1} a.\omega^{\bar{j}}(a) \equiv \sum_{a=0}^{p-1} a^k \bmod p^2$, where $k = p\bar{j}+1$.

Since $p \neq 2$, $k+1 \not\equiv 0 \bmod p$. Since $j \neq 1$, $k-1 \not\equiv 0 \bmod (p-1)$. Therefore the power sum congruence (above) applies, giving:

$$\sum_{a=0}^{p-1} a^k \equiv p.B_k \bmod p^2.$$

To prove corollary (2.9) we show that if $B_{p-j} = B_{\bar{j}+1}$ is not congruent to zero mod p, then $B_k = B_{p\bar{j}+1}$ also is not. But $p\bar{j}+1 \equiv \bar{j}+1 \equiv 0 \bmod (p-1)$ and so Kummer's congruence applies; it proves the assertion since $p\bar{j}+1$ and $\bar{j}+1$ are both p-adic units.

Corollary **(2.10)**. — $Y^{(-1)} = 0$ (*also*: $Y^{(-3)} = Y^{(-5)} = Y^{(-7)} = Y^{(-9)} = 0$) *for all* p (*also*: $Y^{(-11)} = 0$ *for all* $p \neq 691, \ldots$).

Proof. — We may suppose p odd (this is the only place in this paper where $p = 2$ is significantly easier than its fellow primes).

Writing $Y^{(-i)} = Y^{(p-(i+1))}$ we see (2.9) that $Y^{(-i)} = 0$ if $B_{i+1} \not\equiv 0 \bmod p$ and $i+1 \not\equiv 0 \bmod p-1$ or (2.8) if $i+1 \equiv 0 \bmod p-1$. The Corollary then follows from Clausen-von Staudt, and determination of the first few Bernoulli numbers.

3. Etale admissible groups.

Fix a prime number p different from N. We consider only p-groups in this section.

By a *constant group* over any base we mean an étale finite flat group scheme with trivial (constant) Galois representation.

By a *μ-type group* we mean a finite flat group scheme whose Cartier dual is a constant group.

By a *pure (admissible) group* we mean a finite flat group scheme which is the direct product of a constant group by a μ-type group.

Proposition **(3.1)**. — *Any étale admissible finite flat group over* S *is constant. Any admissible finite flat group of multiplicative type over* S *is a μ-type group.*

Proof. — The second assertion follows from the first, by Cartier duality. To see the first, let G be an étale, finite flat admissible group over S. Proceed by induction on the length of G, and suppose $\ell(G) \geq 1$. Then, there is a finite flat subgroup $G_0 \subset G$ such that $G/G_0 = \mathbf{Z}/\mathbf{p}$, since G is both étale and admissible. By induction, G_0 is constant, and G represents an element in $\mathrm{Ext}^1_S(\mathbf{Z}/\mathbf{p}, G_0)$. Now consider the Ext^i exact sequence associated to $0 \to \mathbf{Z} \to \mathbf{Z} \to \mathbf{Z}/\mathbf{p} \to 0$ over S. Note that $\mathrm{Ext}^i_S(\mathbf{Z}, G_0) = H^i(S, G_0)$, and $H^1(S, G_0)$ vanishes since G_0 is a constant group and there are no nontrivial unramified (abelian) extensions of $\mathbf{Z}$. We obtain an isomorphism:

$$H^0(S, G_0)/p.H^0(S, G_0) \xrightarrow{\approx} \mathrm{Ext}^1_S(\mathbf{Z}/\mathbf{p}, G_0).$$

Performing the same calculation over *(e.g.)* Spec(**C**) rather than S, and comparing (using that S is connected) we get:

$$\mathrm{Ext}^1_S(\mathbf{Z}/\mathbf{p}, G_0) \xrightarrow[\approx]{} \mathrm{Ext}^1_{\mathrm{Spec}(\mathbf{C})}(\mathbf{Z}/\mathbf{p}, G_0)$$

which indeed implies that every extension of G_0 by $\mathbf{Z}/\mathbf{p}$ over S is constant. Q.E.D.

If G is a constant admissible group over S′, killed by p^e, it is sometimes convenient to write:

$$G = (\mathbf{Z}/\mathbf{p}^e) \otimes C$$

where C is an abstract finite group killed by p^e, and $\mathbf{Z}/\mathbf{p}^e$ is, to be sure, the constant S′-group scheme. The $\otimes$ construction is the evident one. We may take:

$$C = \mathrm{Hom}_{S'}(\mathbf{Z}/\mathbf{p}^e, G).$$

Similarly, if G is a μ-type group over S′, killed by p^e, we may write:

$$G = \boldsymbol{\mu}_{p^e} \otimes M$$

where M is the abstract finite group $\mathrm{Hom}_{S'}(\boldsymbol{\mu}_{p^e}, G)$.

Now let $G_{/S'}$ be an étale admissible group which is an extension of $\mathbf{A}_{/S'}$ by $\mathbf{B}_{/S'}$ where both **A** and **B** are constant groups over S′.

Write $\mathbf{A} \cong \mathbf{Z}/\mathbf{p}^e \otimes A$, $\mathbf{B} \cong \mathbf{Z}/\mathbf{p}^e \otimes B$, for an appropriate integer e, and abstract finite groups A, B killed by p^e. We may view $G_{/S'}$ as giving rise to an element:

$$g \in \mathrm{Ext}^1_{S'}(\mathbf{A}, \mathbf{B}).$$

To deal with $\mathrm{Ext}^1_{S'}(\mathbf{A}, \mathbf{B})$ it is useful to have the following fairly complete description. Let $p^\alpha \,||\, N-1$. Set $(\widehat{\mathbf{Z}/N})^* = \mathrm{Hom}((\mathbf{Z}/N)^*, \mathbf{Z}/p^\alpha)$ (the Pontrjagin p-dual).

Lemma (**3.2**). — *There is a canonical isomorphism*:

$$\mathrm{Ext}^1_{S'}(\mathbf{A}, \mathbf{B}) = \mathrm{Ext}(A, B) \oplus ((\widehat{\mathbf{Z}/N})^* \otimes_{(\mathbf{Z}/p^\alpha)} \mathrm{Hom}(A, B)[p^\alpha])$$

(to be described in the course of the proof below).

Proof. — By Ext(A, B), we mean Ext in the category of abelian groups. By Hom(A, B)[p^α] we mean the kernel of p^α in Hom(A, B).

The map $\mathrm{Ext}(A, B) \to \mathrm{Ext}^1_{S'}(\mathbf{A}, \mathbf{B})$ is the one which associates to an extension of abstract groups $0 \to B \to E \to A \to 0$ the corresponding extension of constant groups over S′. The map $\mathrm{Ext}^1_{S'}(\mathbf{A}, \mathbf{B}) \to \mathrm{Ext}(A, B)$ is " passage to underlying abstract group " (or equivalently: restriction of the base from S′ to Spec(**C**)). To establish the isomorphism, resolve **A** by free abelian groups (of finite rank): $0 \to \mathbf{R} \to \mathbf{F} \to \mathbf{A} \to 0$ and evaluate the long exact sequence of Ext's to get:

$$0 \to \mathrm{Ext}(A, B) \to \mathrm{Ext}^1_{S'}(\mathbf{A}, \mathbf{B}) \to \mathrm{Hom}(A, H^1(S', \mathbf{B})) \to 0.$$

Since **B** is a constant group scheme, an element in $H^1(S', \mathbf{B})$ is given by the following data: an abelian extension $K/\mathbf{Q}$ unramified outside N, and an injection $\mathrm{Gal}(K/\mathbf{Q}) \subset B$.

Since any such extension is isomorphic to a subfield of $\mathbf{Q}(\zeta_N)$ (recall: $p \nmid N$) we have the canonical isomorphism:

$$H^1(S', \mathbf{B}) = \mathrm{Hom}((\mathbf{Z}/N)^*, B)$$

(using the isomorphism $\mathrm{Gal}(\mathbf{Q}(\zeta_N)/\mathbf{Q}) \cong (\mathbf{Z}/N)^*$) and therefore, we have the canonical isomorphisms:

$$\begin{aligned}\mathrm{Hom}(A, H^1(S', \mathbf{B})) &= \mathrm{Hom}((\mathbf{Z}/N)^*, \mathrm{Hom}(A, B)) \\ &= \mathrm{Hom}((\mathbf{Z}/N)^*_p, \mathrm{Hom}(A, B)[p^\alpha]))\end{aligned}$$

where the subscript p above means p-primary component. Since $(\mathbf{Z}/N)^*_p$ is a free module of rank 1 over $\mathbf{Z}/p^\alpha$, we have:

$$\mathrm{Hom}(A, H^1(S', \mathbf{B})) = \widehat{(\mathbf{Z}/N)}^* \otimes_{\mathbf{Z}/p^\alpha} \mathrm{Hom}(A, B)[p^\alpha].$$

Remark **(3.3)**. — It is sometimes convenient to make a choice of a *generator* $\psi_N : (\mathbf{Z}/N)^* \to \mathbf{Z}/p^\alpha$ [1], in which case, an element $g \in \mathrm{Ext}^1_{S'}(\mathbf{A}, \mathbf{B})$ gives rise (under projection to the second factor of the formula of (3.2)) to a well-defined element $\psi_N \otimes \gamma$, where $\gamma \in \mathrm{Hom}(A, B)[p^\alpha]$. We refer to γ as the *classifying map* for g (dependent, of course, on the choice of ψ_N). The associated Galois module to the group scheme $G_{/S'}$ may be neatly described in terms of ψ_N and γ, as follows. Fix $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. For $x \in G(\bar{\mathbf{Q}})$ the mapping $x \mapsto \sigma(x) - x$ induces a homomorphism from $A = \mathbf{A}(\bar{\mathbf{Q}})$ to $B = \mathbf{B}(\bar{\mathbf{Q}})$ which is simply $\psi_N(\sigma).\gamma(\bar{x})$ where $\bar{x}$ is the image of x in A.

If G is an étale admissible group over S', let the *canonical sequence* of G denote the filtration of closed (étale admissible) subgroup schemes over S':

$$0 = G_0 \subset G_1 \subset \ldots \subset G$$

defined inductively as follows: G_{i+1} is the inverse image in G of the group generated by the S'-sections (*i.e.* the Galois invariant sections) of G/G_i. Thus, the successive quotients are constant groups and $G = G_m$ for some integer m. If m is the least such integer, say that G is an *étale* (admissible) *group of m stages.*

If $G_1 \subset G$ is the "first stage" then, by definition, G_1 is the largest constant subgroup of G.

If $G_2 \subset G$ is the "second stage", then G_2 is an extension of the constant group $\mathbf{A} = G_2/G_1$ by the constant group $\mathbf{B} = G_1$ and, furthermore, its classifying map γ is *injective* since G_1 is the maximal constant subgroup of G_2.

If G is an admissible group of multiplicative type over S', we may similarly define the *canonical sequence* for G, as follows: $G_{i+1} \subset G$ is the inverse image in G of the largest μ-type subgroup of G/G_i.

Note that if G is an admissible multiplicative type group then its canonical sequence

---

[1] Which we also view as a homomorphism from $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ to $\mathbf{Z}/p^\alpha$ by composition with:
$\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Gal}(\mathbf{Q}(\zeta_N)/\mathbf{Q}) \cong (\mathbf{Z}/N)^*$.

is not necessarily dual to the Cartier dual of the canonical sequence of the étale admissible group $G^\vee$. Rather, G_1 is dual to the largest *constant quotient* group of $G^\vee$, etc. The natural functor which passes from multiplicative type admissible groups to étale admissible groups, and which preserves canonical sequences is the functor: $G \mapsto \mathscr{H}om_{S'}(\mathscr{E}a\ \mu, G)$ where $\mathscr{E}a\ \mu = \varprojlim_m \mu_{p^m}$.

Lemma **(3.4)** *(Criterion for constancy).* — *Let* G *be an étale admissible group over* S'. *If* $N \not\equiv 1 \bmod p$, *then* G *is constant. In general,* G *is constant if and only if there is a prime number* $\ell \neq N$ *such that*:

a) ℓ *is not a* p*-th power modulo* N;

b) *The action of* φ_ℓ [1] *in the Galois representation of* G *is trivial.*

Proof. — Consider the canonical sequence (G_i) for G. We need only show that $G_2 = G_1$, under the above hypotheses. Thus we may assume $G = G_2$ is an étale admissible group of two stages. Let $\gamma : G_2(\overline{\mathbf{Q}}) \to G_1(\overline{\mathbf{Q}})$ be its classifying homomorphism which is *injective* by the above discussion. Thus, for any $\ell \neq N$ (even for $\ell = p$) the endomorphism $\varphi_\ell - 1$ of $G(\overline{\mathbf{Q}})$ induces a homomorphism $\psi_N(\ell).\gamma : G_2(\overline{\mathbf{Q}}) \to G_1(\overline{\mathbf{Q}})$ where ψ_N is the chosen homomorphism of remark (3.3). Also $p^\alpha.\gamma = 0$, where $p^\alpha \| N-1$. It follows that if $N \not\equiv 1 \bmod p$, $\gamma = 0$, and we are done. If ℓ is not a p-th power mod N, it is a generator of the p-part of the group $(\mathbf{Z}/N)^*$, and therefore $\psi_N(\ell)$ is a unit in the ring $\mathbf{Z}/p^\alpha$. Hypothesis b) then implies that $\gamma = 0$.

Lemma **(3.5)** *(A* μ*-type criterion).* — *Let* G *be an admissible multiplicative type group over* S'. *If* $N \not\equiv 1 \bmod p$, *then* G *is a* μ*-type group. In general,* G *is* μ*-type if and only if there is a prime number* $\ell \neq p$, N *such that*:

a) ℓ *is not a* p*-th power* mod N.

b) *The Frobenius element* φ_ℓ *acts as multiplication by* ℓ *in the Galois representation of* G.

Proof. — Pass to the étale admissible situation by applying $\mathscr{H}om_{S'}(\mathscr{E}a\ \mu, -)$ (or by Cartier duality) and then use lemma (3.4).

Lemma **(3.6).** — *Let* $\ell \neq p$, N *be a prime number not a* p*-th power* mod N. *If* G *is a multiplicative type group, then the Galois module of* G_1 *(the first stage in its canonical sequence) is the kernel of* $\varphi_\ell - \ell$ *in the Galois module of* G.

Proof. — Passing to the étale situation by the functor $\mathscr{H}om_{S'}(\mathscr{E}a\ \mu, -)$ we may replace G by an *étale* admissible group over S', and we must show that the Galois module of G_1 is the kernel of $\varphi_\ell - 1$.

Work by induction on the number of stages of G. Suppose that it is true for groups of $m-1$ stages and let G have m stages $(m \geq 2)$. Thus G/G_{m-2} has two stages

(1) ℓ-Frobenius.

and its "first stage subgroup" is, by construction, G_{m-1}/G_{m-2}. Using the formula (3.3) $\varphi_\ell(x)-x=\psi_N(\ell).\gamma(\bar{x})$ where γ is the classifying homomorphism for the 2-stage group G/G_{m-2}, $x\in(G/G_{m-2})(\bar{\mathbf{Q}})$ and $\bar{x}$ is its image in $(G/G_{m-1})(\bar{\mathbf{Q}})$, we see that the kernel of $\varphi_\ell-1$ in $(G/G_{m-2})(\bar{\mathbf{Q}})$ is the subgroup $(G_{m-1}/G_{m-2})(\bar{\mathbf{Q}})$ (since γ is injective, and $\psi_N(\ell)$ is a unit in the ring $\mathbf{Z}/p^\alpha$). Consequently, any element $x\in G(\bar{\mathbf{Q}})$ which is in the kernel of $\varphi_\ell-1$ must be contained in $G_{m-1}(\bar{\mathbf{Q}})\subset G(\bar{\mathbf{Q}})$.

But G_{m-1} is a group of $m-1$ stages, and therefore $x\in G_1(\bar{\mathbf{Q}})$, by induction.

4. Pure admissible groups.

Proposition (4.1). — *Let* $p\neq 2$. *Let* $\mathbf{A}$ *be a constant group and* M *a* μ*-type group. Then*:

$$\mathrm{Ext}^1_S(\mathbf{A}, M)=0.$$

Proof. — This reduces to showing $\mathrm{Ext}^1_S(\mathbf{Z}/\mathbf{p}, \mu_p)=0$. But applying $\mathrm{Ext}^i(-, \mu_p)$ to the exact sequence of *fppf* sheaves $0\to\mathbf{Z}\to\mathbf{Z}\to\mathbf{Z}/\mathbf{p}\to 0$ yields a long exact sequence which may be evaluated using the fact that $\mathrm{Ext}^1_S(\mathbf{Z}, \mu_p)=H^1(S, \mu_p)$. One gets the short exact sequence:

$$0\to H^0(S, \mu_p)\to \mathrm{Ext}^1_S(\mathbf{Z}/\mathbf{p}, \mu_p)\to H^1(S, \mu_p)\to 0.$$

From the Kummer sequence $0\to\mu_p\to\mathbf{G}_m\to\mathbf{G}_m\to 0$ of *fppf* sheaves, and the fact that the ideal class group of $\mathbf{Z}$ vanishes, one gets: $H^1(S, \mu_p)=(\mathbf{Z}^*)/(\mathbf{Z}^*)^p$. Thus we have a short exact sequence:

$$0\to(\mathbf{Z}^*)[p]\to\mathrm{Ext}^1_S(\mathbf{Z}/\mathbf{p}, \mu_p)\to(\mathbf{Z}^*)/(\mathbf{Z}^*)^p\to 0.$$

Now suppose $p\neq 2$, and one sees that the middle group must vanish. If $p=2$, we get:

Proposition (4.2). — *There are three nontrivial extensions of* $\mathbf{Z}/\mathbf{2}$ *by* μ_2 *over* S:

Extension 1: *an extension whose associated Galois representation is trivial, and whose underlying abelian group is cyclic of order* 4.

Extension 2: *the* unique *nontrivial extension over* S *killed by* 2:

$$0\to\mu_2\to D\to\mathbf{Z}/\mathbf{2}\to 0.$$

Its associated Galois representation factors through $\mathbf{Q}(\sqrt{-1})$. *If we let*:

$$\psi_{-1}: \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})\to\mathrm{Gal}(\mathbf{Q}(\sqrt{-1})/\mathbf{Q})\xrightarrow{\sim}\mathbf{Z}/2$$

be the composite where the first map is the natural projection, and the second an isomorphism, then the Galois representation associated to D *is given as follows*:

$$\sigma(x)-x=\psi_{-1}(\sigma).\gamma(\bar{x}) \tag{4.3}$$

where if $x\in D(\bar{\mathbf{Q}})$, *then* $\bar{x}$ *is its projection to* $\mathbf{Z}/2$, *and* γ *is the only surjective homomorphism* $D(\bar{\mathbf{Q}})\to\mu_2(\bar{\mathbf{Q}})$ *with kernel* $\mu_2(\bar{\mathbf{Q}})$.

As usual, identifying $\mathrm{Gal}(\mathbf{Q}(\sqrt{-1})/\mathbf{Q})$ *with* $(\mathbf{Z}/4)^*$, *if* φ_ℓ *denotes* ℓ*-Frobenius (in the Galois group of any extension field of* $\mathbf{Q}(\sqrt{-1})$ *which is Galois over* $\mathbf{Q}$, *and unramified over* ℓ*) then we also write* $\psi_{-1}(\ell)$ *for* $\psi_{-1}(\varphi_\ell)$. *One has:* $\psi_{-1}(\ell)=1$ *if and only if* $\ell \equiv -1 \bmod 4$.

Extension 3: (the sum in Ext^1 *of the above two elements) an extension whose underlying abelian group is cyclic of order* 4, *and whose Galois representation satisfies the same formula as above.*

Proof. — This is evident from the exact sequences in the proof of (4.1) except for the assertions concerning Galois representations. To see those, one must recall that the nontrivial μ_2-torseur representing the (nontrivial) element in $H^1(S, \mu_2)$ is the S-scheme $\mathrm{Spec}\ \mathbf{Z}[\sqrt{-1}]$.

Remark. — The group scheme $D_{/S}$ (Extension 2 of (4.2) above) will play a central role in our study of the prime 2. Since Fontaine's theorem does not apply to admissible 2-groups in general, the following result is useful:

Proposition **(4.4).** — *Let* $D'_{/S'}$ *be a finite flat group scheme, and* $\varphi : D_{/\mathbf{Q}} \xrightarrow{\approx} D'_{/\mathbf{Q}}$ *an isomorphism over* $\mathbf{Q}$ *(equivalently: an isomorphism of associated Galois modules). Then* φ *extends to an isomorphism* $\varphi : D_{/S'} \to D'_{/S'}$ *of group schemes over* S'.

Proof. — Since the associated Galois module to D' is admissible, $D'_{/S'}$ is admissible, and since the inertia group at N operates trivially in the Galois representation of D (and hence also of D'), D' extends to a finite flat group scheme over S. Since the Galois representation of D' satisfies (4.3), D' cannot be an extension of μ_2 by $\mathbf{Z}/2$ (2.1), nor of $\mathbf{Z}/2$ by $\mathbf{Z}/2$ (3.3), nor of μ_2 by μ_2 (applying (3.3) to its Cartier dual).

Therefore it must indeed be isomorphic to D, by (4.2).

Since there is only one nontrivial automorphism of the Galois module associated to D, and this automorphism extends to an automorphism of $D_{/S}$, our proposition follows.

Proposition **(4.5)** *(Criterion for purity:* $p \neq 2$*). — Let* $p \neq 2$, *and let* $G_{/S'}$ *be an admissible group. These are equivalent:*

a) G *is pure.*

b) *The associated Galois module to* G *is pure* (i.e. *it is the direct sum of a constant Galois module and the Cartier dual of a constant Galois module*).

c) *The action of inertia at* N *is trivial on the associated Galois module to* G.

d) G *extends to a finite flat group scheme over* S.

Proof. — Clearly a) $\Rightarrow$ b) $\Rightarrow$ c). By (1.3), c) $\Rightarrow$ d). To conclude, we must show that any finite flat admissible group over S is pure. Let G be such a group, and:

$$0 = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_r = G$$

an admissible filtration. Thus the successive quotients are isomorphic either to $\mathbf{Z}/\mathbf{p}$ or to μ_p over S.

Step 1: We may suppose all the successive quotients isomorphic to μ_p *precede* those isomorphic to $\mathbf{Z}/\mathbf{p}$. This follows immediately from proposition (2.1), and induction.

Therefore, for some s, $G_s \subset G$ is an admissible subgroup of multiplicative type, and G/G_s is an admissible étale group.

Step 2: G_s is a μ-type group and G/G_s is constant.

Proof: (3.1).

Step 3: G is a trivial extension of the constant group G/G_s by the μ-type group G_s.

Proof: (4.1).

Remark. — Demanding that the action of inertia at N be trivial in the Galois representation is clearly not sufficient to insure purity when $p=2$ (*e.g.*, consider the nontrivial extension D of (4.2)). Nevertheless, for admissible 2-groups over S killed by 2, purity is equivalent to the requirement that the action of $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$ be trivial in the associated Galois module. As it turns out in our ultimate applications, however, the notion of purity is not the relevant one when $p=2$.

The final proposition of this section will be used in studying the cuspidal subgroup (chap. II, § 11).

Proposition **(4.6).** — *Let* $C_{/S}$ *be a finite flat group whose underlying Galois module is a finite cyclic group with trivial Galois action. If* C *is of odd order, then* C *is a constant group. If* C *contains a subgroup isomorphic to* μ_2, *then the quotient* C/μ_2 *is a constant group.*

Proof. — The first assertion of (4.6) follows from (1.6) and (3.4). As for the second, we may suppose that C is killed by a power of 2 (say 2^α). If $\alpha=1$, we are done. Now suppose that $\alpha=2$. It suffices to show that C/μ_2 is étale over S. Clearly C/μ_2 cannot be isomorphic to μ_2, for then the Cartier dual of $C_{/S}$ would be étale, hence constant, and so the Galois action on C could not be trivial. Thus $C/\mu_2 \cong \mathbf{Z}/\mathbf{2}$.

Now let $\alpha>2$. We shall show that C/μ_2 is étale as follows: filtering C by the kernels of successive powers of 2, if C/μ_2 were not étale, using the result proved for $\alpha=2$, one could obtain a subquotient of C, whose underlying abelian group is cyclic of order 4, and which is an extension of μ_2 by $\mathbf{Z}/\mathbf{2}$, which is impossible by (2.1).

5. A special calculation for $p=2$.

Let $\mathrm{Ext}^1_{2\_S'}(A, B)$ denote the subgroup of elements in $\mathrm{Ext}^1_{S'}(A, B)$ which represent extensions of A by B which are killed by multiplication by 2.

Consider the (nonflat) surjective homomorphism $\mathbf{Z}/\mathbf{2} \to \mu_2$ (over S'). This induces a homomorphism:

$$\mathrm{Ext}^1_{2\_S'}(\mu_2, \mathbf{Z}/\mathbf{2}) \xrightarrow{\beta} \mathrm{Ext}^1_{2\_S'}(\mathbf{Z}/\mathbf{2}, \mathbf{Z}/\mathbf{2})$$

and we shall show that this map is *injective*. The full story, however, is the following:

Proposition **(5.1)**:

a) $\mathrm{Ext}^1_{2\_S'}(\mathbf{Z}/2, \mathbf{Z}/2)$ *is of order* 2.

b) *If* $N \not\equiv \pm 1 \bmod 8$, *then* $\mathrm{Ext}^1_{2\_S'}(\mu_2, \mathbf{Z}/2) = 0$.

c) *If* $N \equiv \pm 1 \bmod 8$, *then the homomorphism* β *is an isomorphism of groups of order* 2.

Proof. — a) Follows from $H^1(S', \mathbf{Z}/2) = \mathrm{Ext}^1_{2\_S'}(\mathbf{Z}/2, \mathbf{Z}/2)$.

As for an analysis of $\mathrm{Ext}^1_{2\_S'}(\mu_2, \mathbf{Z}/2)$ there are two ways to proceed. We may adapt the general method of (2.1) to the base S', or (since our group schemes have such small orders) we may work directly. We choose the latter course.

Consider the composition:

$$\bar{\beta} : \mathrm{Ext}^1_{2\_S'}(\mu_2, \mathbf{Z}/2) \xrightarrow{\beta} \mathrm{Ext}^1_{2\_S'}(\mathbf{Z}/2, \mathbf{Z}/2) \underset{\approx}{\to} H^1(S', \mathbf{Z}/2).$$

A " geometric " construction of $\bar{\beta}$ is the following:
If x is an element in $\mathrm{Ext}^1_{2\_S'}(\mu_2, \mathbf{Z}/2)$ represented by an extension:

(5.2) $$0 \to \mathbf{Z}/2 \to E \to \mu_2 \to 0,$$

let $r : S' \to \mu_{2/S'}$ denote the *nontrivial* section, and let $E_r \subset E$ denote the fiber-product:

$$\begin{array}{ccc} E_r & \longrightarrow & E \\ \downarrow & & \downarrow \\ S' & \xrightarrow{r} & \mu_2 \end{array}$$

Thus E_r is the " nontrivial " $\mathbf{Z}/2$-coset. It is a $\mathbf{Z}/2$-torseur over S' and represents the element $\bar{\beta}(x)$ in $H^1(S', \mathbf{Z}/2)$.

The scheme-theoretic intersection of E_r and $\mathbf{Z}/2$ in E consists in two points lying over $\mathrm{Spec}\, \mathbf{F}_2$. From this we deduce that the prime 2 *splits* in the S'-extension E_r.

If $\bar{\beta}(x) = 0$, E_r is a trivial $\mathbf{Z}/2$-torseur. Take the subgroup of E generated by the (unique) S'-section of E_r which meets (at $\mathrm{Spec}(\mathbf{F}_2)$) the zero-section of E. This is a group scheme which projects *isomorphically* to μ_2, and therefore gives a splitting of (5.2), showing that $x = 0$. Thus $\bar{\beta}$ (and hence β) is injective.

Now suppose that x is *nontrivial* (*i.e.* (5.2) does not split). The Galois representation associated to the group scheme E of (5.2) is *isomorphic* (to be sure) with the Galois representation associated to the pull-back via β. In particular (3.3):

If $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ and $z \in E(\bar{\mathbf{Q}})$, we have $\sigma(z) - z = \psi_N(z) \cdot \gamma(\bar{z})$ where $\bar{z}$ is the image of z in $\mu_2(\bar{\mathbf{Q}})$ and $\gamma : \mu_2(\bar{\mathbf{Q}}) \underset{\approx}{\to} \mathbf{Z}/2$ is an isomorphism.

This Galois representation factors through the unique quadratic number field in $\mathbf{Q}(\zeta_N)$, namely:

$$K = \begin{cases} \mathbf{Q}(\sqrt{-N}) & \text{if} \quad N \equiv -1 \bmod 4 \\ \mathbf{Q}(\sqrt{N}) & \text{if} \quad N \equiv \ 1 \bmod 4. \end{cases}$$

Note that if $N \not\equiv \pm 1 \bmod 8$, then 2 does not split in K, whence b). As for c) we need only construct a nontrivial extension (5.2) when $N \equiv \pm 1 \bmod 8$. We omit

the details (noting that no use of c) is made in this paper) and merely sketch this construction: Since 2 does split in K, when $N \equiv \pm 1 \bmod 8$, one can *glue* the S'-scheme $\mathbf{Z}/2$ and the nontrivial $\mathbf{Z}/2$-torseur over S' transversally at their closed points of characteristic 2, and check that the evident group law away from characteristic 2 extends to a group-scheme structure of S'.

II. — THE MODULAR CURVE $X_0(N)$

1. Generalities.

We shall be reading closely in two sources of information concerning moduli stacks, their associated coarse moduli schemes, and the theory of modular forms: [9], [24]. Our ultimate object is to derive as complete a description as possible of $J_{/S}$, the Néron model of the jacobian of $X_0(N)$ over S ($N \geq 5$, a prime number; $X_0(N)$ the modular curve associated to $\Gamma_0(N)$). Technically, reduction to characteristics 2, 3, and N (in that order) produce the thorniest problems, and we shall spend *most* of our time dealing with them.

We keep to most of the conventions of [9]. Thus, for m any integer, and $H \subset GL_2(\mathbf{Z}/m)$ we have the algebraic moduli stack $\mathscr{M}_H$ ([9], IV, (3.3)) proper over S, which may be interpreted over Spec $\mathbf{Z}[1/m]$ as the fine moduli stack classifying *generalized* elliptic curves with a level H-structure ([9], IV, (3.1)). Its associated *coarse* moduli stack ([9], I, (8.1)) may be denoted M_H. If H is the trivial subgroup of $GL_2(\mathbf{Z}/m)$ we write $\mathscr{M}_m$ for $\mathscr{M}_H$. If $H = \Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| c \equiv 0 \bmod N \right\}$ write:

$$\mathscr{M}_H = \mathscr{M}_0(N); \qquad M_H = M_0(N).$$

Given a pair $(E_{/T}, h)$ where E is an elliptic curve (or a *generalized* elliptic curve [9], chap. II) over the scheme T, and h is a level H-structure of $E_{/T}$, then the T-valued point of M_H determined by this pair will be denoted $j(E_{/T}, h)$.

In relating modular forms to differential forms, and in other arguments as well, we shall have use for certain refinements of $M_0(N)$, associated to level structures H, where $\mathscr{M}_H = M_H$ (*i.e.* where the fine moduli stack " exists " as an algebraic space). Two notable refinements having this property are ([9], IV, th. (2.7)):

a) Take $m = N$, and $H = \Gamma_{00}(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| c \equiv 0 \bmod N, a \equiv 1 \bmod N \right\}$ (recall: $N \geq 5$) in which case we write $M_H = M_1(N)$.

b) Take $m = 3N$ and $H = \Gamma_0(N; 3) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 3;\ c \equiv 0 \bmod N \right\}$ in which case we write $M_H = M_0(N; 3)$.

The schemes $M_N \to M_1(N) \to M_0(N)$ are smooth when restricted to:

$$S' = \mathrm{Spec}(\mathbf{Z}[1/N]).$$

As in [9], the superscript h ($\mathcal{M}_0(N)^h$, $M_0(N)^h$, etc.) refers to the open substack or subscheme obtained by removing the " supersingular points " of characteristic N. The precise geometric structure of $M_0(N)_{/S}$ is given by [9], IV, th. (6.9). In particular, $M_0(N)_{/\mathbf{F}_N}$ is a union of two copies of $\mathbf{P}^1_{/\mathbf{F}_N}$ (the j-line) intersecting transversally at the " supersingular points ", where a point x on the second copy gets glued to the image under N-Frobenius $x^{(N)}$ on the first. One has that $M_0(N)^h_{/S}$ is smooth, and if j is a supersingular point of characteristic N (using [9], IV, (6.9) (iii) and the fact that $N \geq 5$) then $M_0(N)_{/S}$ is regular at j if $j \neq 0$, 1728. In the latter two cases, $M_0(N)$ is formally isomorphic to :

$$W(\overline{\mathbf{F}}_N)[x,y]/(x.y - N^3) \quad \text{if} \quad j = 0$$
$$W(\overline{\mathbf{F}}_N)[x,y]/(x.y - N^2) \quad \text{if} \quad j = 1728.$$

In any case, $M_0(N) \to S$ is locally a complete intersection, hence Gorenstein, and hence also Cohen-Macaulay [3]. By suitable blow-up of the points $j = 0$, 1728 in characteristic N, when they are supersingular, we may arrive at the minimal regular resolution of $M_0(N)_{/S}$, *which we call* $X_0(N)_{/S}$. See the appendix for a study of these minimal regular resolutions in a somewhat broader context. The structure of the " bad fiber " (*i.e.* over $\mathbf{F}_N$) of $X_0(N)$ may be schematized as follows:

blow-up of $j = 1728$ when supersingular ($\Leftrightarrow N \equiv -1 \bmod 4$)

transversal intersection at $j \neq 1728, 0$, supersingular cusps

blow-up of $j = 0$ when supersingular ($\Leftrightarrow N \equiv -1 \bmod 3$)

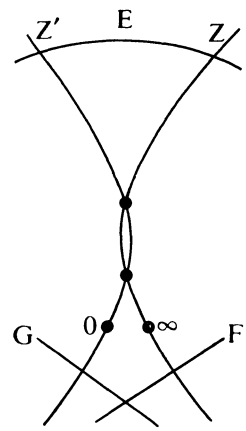


Diagram 1

The irreducible components E (which occurs if and only if $N \equiv -1 \bmod 4$) and F, G (which occur if and only if $N \equiv -1 \bmod 3$) are the " results " of the appropriate blow-ups, and are all isomorphic to $\mathbf{P}^1_{/\mathbf{F}_N}$. See appendix for further discussion.

The morphism $X_0(N) \to S$ is a local complete intersection, and, again therefore a Gorenstein morphism, and hence Cohen-Macaulay. Clearly $M_0(N)_{/S'} = X_0(N)_{/S'}$, and therefore (over any base extension of S') we have *two* possible names for the same thing. We try to keep to this usage: it will be called $M_0(N)_{/S'}$ when we are interested primarily in questions of modular forms, and $X_0(N)_{/S'}$ when we are interested in more

geometric questions. Also, for reasons of consistency, and compatibility with other authors, we allow ourselves the same double notation $M_1(N)_{/S'} = X_1(N)_{/S'}$ in dealing with $H = \Gamma_{00}(N)$, and likewise: $M_0(N; 3)_{/\mathrm{Spec}(\mathbf{Z}[1/3N])} = X_0(N; 3)_{/\mathrm{Spec}(\mathbf{Z}[1/3N])}$.

The usual names (0 and ∞) are given to the two cusps of $M_0(N)$. We view these as (nowhere intersecting) sections of $M_0(N)_{/S}$ ([9], VII, § 2). They also give rise to sections of $X_0(N)_{/S}$ (denoted by the same symbols) and, after arbitrary base change $T \to S$, to T-sections of $X_0(N)_{/T}$.

The cuspidal sections 0 and ∞ distinguish themselves as follows: The morphism of stacks $\mathscr{M}_0(N) \to \mathscr{M}_0(1)$ induced by the rule $(E_{/T}, H) \mapsto E_{/T}$ is unramified at ∞ and ramified at 0.

2. Ramification structure of $X_1(N) \to X_0(N)$.

As always, let N be a prime number ≥ 5. Let k be a field which is algebraically closed and of characteristic different from N. The map (2.1) $X_1(N) \to X_0(N)$ over k is unramified at the cusps, and has precisely these points as ramification points:

TABLE 1

Char k	Name of point in $X_0(N)$	Value of j	Occurs if and only if	Structure of inertia group
$\neq 2, 3, N$	$(i)_+, (i)_-$	1728	$N \equiv 1 \bmod 4$	cyclic of order 2
	$(\rho)_+, (\rho)_-$	0	$N \equiv 1 \bmod 3$	cyclic of order 3
2	$(\rho)_+, (\rho)_-$	$0 = 1728$	$N \equiv 1 \bmod 3$	cyclic of order 3
	(i)		$N \equiv 1 \bmod 4$	cyclic of order 2: "wild ramification of *first* type"
3	$(i)_+, (i)_-$	$0 = 1728$	$N \equiv 1 \bmod 4$	order 2
	(ρ)		$N \equiv 1 \bmod 3$	order 3: "wild ramification of *first* type"

Definition **(2.2).** — *A Galois p-cyclic extension of local fields whose residue fields are of characteristic p will be said to be wildly ramified of the* ν*-th type if the higher ramification sequence* (G_i) (cf. [60], chap. IV) *of subgroups of its Galois group* G *has the following structure*:

$$G = G_0 = G_1 = \ldots = G_\nu$$
$$G_{\nu+1} = G_{\nu+2} = \ldots = 0.$$

We shall establish the facts of the above table. Recall that (since k is of characteristic different from N) the cusps are unramified in the mapping (2.1). If (E, C)

is a pair representing a point $j(E, C) \in X_0(N)$ [1], then the automorphism group Aut(E, C) denotes the stabilizer of C in Aut(E); since $N \geq 5$, the natural homomorphism:

$$\mathrm{Aut}(E, C) \to \mathrm{Aut}(C) = (\mathbf{Z}/N)^*$$

is injective [2]. Passing to the quotient:

$$\mathrm{Aut}(E, C)/(\pm 1) \to (\mathbf{Z}/N)^*/(\pm 1) = \mathrm{Gal}(X_1(N)/X_0(N))$$

the above homomorphism identifies $\mathrm{Aut}(E, C)/(\pm 1)$ with the inertia group of the point $j(E, C)$.

If $j(E) \neq 0, 1728$ then $\mathrm{Aut}(E) = (\pm 1)$, and therefore $j(E, C)$ is not a point of ramification.

Characteristic $k \neq 2, 3, N$. — $j(E) = 1728$: The group Aut(E) is cyclic of order 4. It can stabilize no cyclic subgroup of order N, $C \subset E$ if $N \not\equiv 1 \bmod 4$. On the other hand, if $N \equiv 1 \bmod 4$ there is a 4-th root of unity in $\mathbf{F}_N$ and consequently Aut(E) stabilizes precisely two cyclic subgroups of order N. Call them $C^{\pm}$ and write $(i)^{\pm} = j(E, C^{\pm})$. We have $(i)^+ \neq (i)^-$ since no element of Aut(E) interchanges C^+ and C^-. This establishes the first line of the table.

$j(E) = 0$: The group Aut(E) is cyclic of order 6 and reasoning similar to the above establishes the second line of the table.

Characteristic $k = 2$. — Let E be an elliptic curve with $j(E) = 1728 = 0$. We may take E to be the curve $y^2 + y = x^3$. The endomorphism ring of E is the ring of Hurwitz quaternions and its automorphism group is of order 24. The quotient $\mathrm{Aut}(E)/(\pm 1)$ is isomorphic to $\mathfrak{A}_4$, the alternating group on 4 letters. The cyclic subgroups of $\mathfrak{A}_4$ have orders 1, 2, 3 and any two cyclic subgroups of the same order are conjugate. Fix cyclic subgroups $H_2, H_3 \subset \mathrm{Aut}(E)/(\pm 1)$ of orders 2 and 3 respectively. Note that the inverse images of these in Aut(E) are cyclic groups of orders 4 and 6 respectively.

As above, then, H_3 stabilizes precisely *two* cyclic subgroups of order N (call them $C^{\pm} \subset E$) if $N \equiv 1 \bmod 3$ and *none* if $N \not\equiv 1 \bmod 3$. Write $(\rho)^{\pm} = j(E, C^{\pm})$. Since H_3 is its own normalizer in $\mathrm{Aut}(E)/(\pm 1)$, $(\rho)^+ \neq (\rho)^-$ and we have established the third line of the table.

The subgroup H_2 stabilizes *two* cyclic subgroups of order N (call them, again, $C^{\pm} \subset E$) if $N \equiv 1 \bmod 4$ and *none* if $N \not\equiv 1 \bmod 4$. But the normalizer of H_2 in $\mathrm{Aut}(E)/(\pm 1)$ is isomorphic to the Klein 4-group. Since the entire Klein 4-group cannot stabilize $C^{\pm}$, any element in the normalizer of H_2 which is not in H_2 must *interchange* C^+ and C^-. Consequently $j(E, C^+) = j(E, C^-)$. Denote this point (i). Clearly, (i) is a point of wild ramification. We shall show it to be of *first* type, using an argument

---

[1] Here C is a cyclic subgroup of order N in the elliptic curve E, giving the "level $\Gamma_0(N)$ structure".

[2] If $a \neq \pm 1$ is an automorphism of any elliptic curve over any field k, then a is of order 4 or 6, and generates a ring of endomorphisms isomorphic to the ring of cyclotomic integers of that order. See the discussion in Appendix 1 of [29] concerning endomorphism rings, and automorphisms. The assertion concerning injectivity above then follows, for there is no homomorphism of the ring of cyclotomic integers of order 4 or 6 to $\mathbf{F}_N$, which sends a to 1, provided $N \geq 5$.

communicated to us by Serre: For *any* field k of characteristic different from N, one has the short exact sequence:

$$0 \to f^*\Omega^1_{X_0(N)/k} \to \Omega^1_{X_1(N)/k} \to \Omega^1_{X_1(N)/X_0(N)} \to 0$$

where the zero on the right comes from the fact that $X_0(N)$ is smooth, and $f: X_1(N) \to X_0(N)$ is generically separable. Note that $\dim_k H^0(\Omega^1_{X_1(N)/X_0(N)})$ is the degree of the global different ([60], chap. III, § 7, Prop. 14) giving us the *Hurwitz Formula.* Namely, the degree of the global different of $X_1(N)/X_0(N)$ is:

$$2 \cdot g_1(N) - 2 - \left(\frac{N-1}{2}\right) \cdot (2g_0(N) - 2)$$

where $g_i(N)$ is the genus of the curve $X_i(N)$. It follows that the degree of the global different of $X_1(N)/X_0(N)$ is independent of the characteristic of the field k (provided that it is different from N). From the first two lines of our table, choosing k to be of characteristic different from 2, 3 and N, we compute the degree of the global different to be:

$$2 \cdot \left\langle \frac{N-1}{4} \right\rangle + 2 \cdot \left\langle \frac{N-1}{3} \right\rangle$$

where if r is a rational number we let the symbol $\langle r \rangle$ be r if r is an integer and 0 if not.

On the other hand, if k is of characteristic two and if (i) is wildly ramified of the ν-th type, using prop. 4 of [60] chapter IV, from what we have established concerning the ramification structure of $X_1(N)/X_0(N)$ we compute the degree of the global different to be:

$$(1+\nu) \cdot \left\langle \frac{N-1}{4} \right\rangle + 2 \cdot \left\langle \frac{N-1}{3} \right\rangle.$$

Consequently, $\nu = 1$, and the third and fourth lines of our table have been established.

Characteristic $k = 3$. — Here, again, we take E to be an elliptic curve with $j(E) = 0 = 1728$; for example: $y^2 = x^3 - x$. The group of automorphisms Aut(E) is of order 12 and has the following structure: it contains a normal subgroup of order 3, $\mathfrak{A}_3 \subset \mathrm{Aut}(E)$ such that the quotient of Aut(E) by $\mathfrak{A}_3$ is a cyclic group of order 4, which acts in the unique nontrivial way on $\mathfrak{A}_3$ ([29], App. 1, § 2). The center of Aut(E) is (± 1) and $\mathrm{Aut}(E)/(\pm 1)$ is isomorphic to $\mathfrak{S}_3$, the symmetric group on 3 letters. Again we have that the cyclic subgroups of $\mathfrak{S}_3$ have orders 1, 2, 3 and any two cyclic subgroups of the same order are conjugate. Fix cyclic subgroups $H_2, H_3 \subset \mathrm{Aut}(E)/(\pm 1)$ of orders 2 and 3 respectively. It is again true that the inverse images of these in Aut(E) are cyclic groups of orders 4 and 6 respectively.

From this point on, to establish the last two lines of our table, we proceed exactly as in the case of characteristic 2, with the one important difference that now it is H_2 which is its own normalizer in $\mathrm{Aut}(E)/(\pm 1)$ while H_3 is normal in $\mathrm{Aut}(E)/(\pm 1)$.

Our table is established.

Corollary (**2.3**). — *Let* $n = \text{numerator}\left(\frac{N-1}{12}\right)$. *Let* $S' = \mathrm{Spec}(\mathbf{Z}[1/N])$. *Let* $X_2(N)_{/S'} \to X_0(N)_{/S'}$ *denote the unique covering intermediate to* $X_1(N)_{/S'} \to X_0(N)_{/S'}$ *which is a Galois covering, cyclic of order n.*

Then $X_2(N)_{/S'} \to X_0(N)_{/S'}$ *is étale.*

We shall refer to the above étale covering as the *Shimura covering*.

3. Regular differentials.

Deligne and Rapoport [9] work out Grothendieck's duality theory in the case of a Cohen-Macaulay morphism $\pi : X \to T$ (purely of dimension d). We shall recall the contents of [9] in the case $d=1$, with some change of notation.

Definition (**3.1**). — *If* $\pi : X \to T$ *is a Cohen-Macaulay morphism purely of dimension* 1, *where* T *is a noetherian scheme, the sheaf* of regular differentials *is*:

$$\Omega_{X_{/T}} = \mathscr{H}^{-1}(R\pi^! \mathcal{O}_T) \ (^1) \ ([9], \text{ chap. I, } (2.1.1)).$$

The sheaves $\Omega_{X_{/T}}$ are flat over T, their formation commutes with arbitrary base change $T' \to T$ and with étale localization of X. If $X_{/T}$ is smooth, then $\Omega_{X_{/T}} = \Omega^1_{X_{/T}}$. If X is a reduced curve over an algebraically closed field k which has only ordinary double point singularities $x_1, \ldots, x_t$ and if (x_i', x_i'') denotes the inverse image of x_i in X^*, the normalization of X, then *the regular differentials* on X consist in meromorphic differential forms on X^* regular outside of the x_i', x_i'', having at worst a simple pole at the x_i' and x_i'', and verifying:

$$\mathrm{res}_{x_i'} = -\mathrm{res}_{x_i''} \qquad (i = 1, \ldots, t).$$

The duality theorem gives an isomorphism.

If $\mathscr{F}$ is a locally free $\mathcal{O}_T$-Module, and if the $R^j\pi_*\mathscr{F}$ are locally free $\mathcal{O}_T$-Modules, the duality theorem (*loc. cit.* (2.2.3)) gives:

$$(3.2) \qquad R^{1-j}\pi_*(\mathscr{F}^\vee \otimes \Omega_{X_{/T}}) \xrightarrow{\approx} (R^j\pi_*\mathscr{F})^\vee$$

where $\vee$ denotes $\mathcal{O}_T$-dual.

We prepare to apply the duality theorem to the morphisms π_T, π_T', which are the base changes to $T \to S$ of the morphisms occuring in the diagram:

$$\begin{array}{ccc} X_0(N) & \xrightarrow{\ i\ } & M_0(N) \\ & {\scriptstyle\pi}\searrow \quad \swarrow{\scriptstyle\pi'} & \\ & S & \end{array}$$

where i is the minimal regular resolution introduced in § 1.

---

(1) Deligne-Rapoport call this $\omega_{X_{/T}}$. We often omit the subscript $X_{/T}$ when no confusion can arise.

Let $\Omega_{M_0(N)/S}(\text{cusps})$ denote the locally free sheaf, which when restricted to the complement of the cuspidal divisor, is equal to the sheaf of regular differentials and whose sections in a neighborhood of the cuspidal divisor are meromorphic differentials with, at worst, a simple pole along the cuspidal divisor. Let $\mathcal{O}_{M_0(N)/S}(\text{cusps})$ be the subsheaf of functions in $\mathcal{O}_{M_0(N)/S}$ which are zero along the cuspidal divisor. An easy computation gives that $R^j\pi'_{T*}\mathcal{O}_{M_0(N)/T}(\text{cusps})$ vanishes when $j \neq 1$, and is an extension of $R^1\pi'_{T*}\mathcal{O}_{M_0(N)/T}$ by $\mathcal{O}_T$, when $j=1$. Consequently, the $R^j\pi'_{T*}\mathcal{O}_{M_0(N)}(\text{cusps})$ are locally free $\mathcal{O}_T$-Modules, when the $R^j\pi'_{T*}\mathcal{O}_{M_0(N)/T}$ are.

Lemma **(3.3)**. — *Let* T *be a noetherian scheme flat over* $S=\mathrm{Spec}(\mathbf{Z})$, *or over the spectrum of a field. Then*:

$$R^j\pi'_{T*}\mathcal{O}_{M_0(N)/T}$$
$$R^j\pi'_{T*}\mathcal{O}_{M_0(N)/T}(\text{cusps})$$
$$R^j\pi_{T*}\mathcal{O}_{X_0(N)/T}$$

are locally free $\mathcal{O}_T$*-Modules.*

Remark. — The duality isomorphism (3.2) then applies in these cases.

Proof. — By the preceding discussion we need only prove the assertion for $R^jf_*\mathcal{O}_Y$ where $f: Y \to T$ stands for either the morphism π or π'. Formation of $R^jf_{T*}\mathcal{O}_{Y/T}$ commutes with flat base change $T' \to T$ ([EGA], III, (1.4.15)), which reduces us to considering the unique case $T=\mathrm{Spec}(\mathbf{Z})$. Also, $j=1$ is the only nonobvious dimension. Let p be any prime. Since $\mathcal{O}_Y$ is flat over $\mathbf{Z}$, we have the exact sequence:

$$0 \to R^0f_*\mathcal{O}_Y \xrightarrow{p} R^0f_*\mathcal{O}_Y \to R^0(f_{/\mathbf{F}_p})_*\mathcal{O}_{Y/\mathbf{F}_p} \to R^1f_*\mathcal{O}_Y \xrightarrow{p} R^1f_*\mathcal{O}_Y.$$

The only global functions on $Y_{/\mathbf{F}_p}$ are constant functions. This is evident for $p \neq N$, since $Y_{/\mathbf{F}_p}$ is then smooth and irreducible, and follows for $p=N$ from the explicit description of the fibers $X_0(N)_{/\mathbf{F}_N}$ and $M_0(N)_{/\mathbf{F}_N}$ (§ 1). It follows that $R^1f_*\mathcal{O}_Y$ has no nontrivial p-torsion.

Proposition **(3.3)** *(commutation with base change). — Consider the category of rings which are flat over* $\mathbf{Z}/m$ *for some* m, *or over* $\mathbf{Z}$. *Let* $R \to R'$ *be a homomorphism in this category, then*:

$$H^0(M_0(N)_{/R}, \Omega) \otimes_R R' \xrightarrow{\sim} H^0(M_0(N)_{/R'}, \Omega)$$

and:

$$H^0(M_0(N)_{/R}, \Omega(\text{cusps})) \otimes_R R' \xrightarrow{\sim} H^0(M_0(N)_{/R'}, \Omega(\text{cusps}))$$

are isomorphisms.

Proof. — The assertion holds for $R \to R'$ flat, by [EGA], III, (1.4.15). This allows one to reduce the question to the base changes $\mathbf{Z} \to \mathbf{Z}/m$ (for m an arbitrary integer); for these the assertion is true since $H^1(M_0(N)_{/\mathbf{Z}}, \Omega)$ and $H^1(M_0(N)_{/\mathbf{Z}}, \Omega(\text{cusps}))$ are torsion-free $\mathbf{Z}$-modules, by (3.3) and the duality isomorphism (3.2).

Proposition (3.4). — *Let* T *be a (noetherian) scheme flat over* S *or over a field. The natural map induces an isomorphism*:

$$R^0\pi_{T^*}\Omega_{X_0(N)/T} \xrightarrow{\iota}_{\approx} R^0\pi'_{T^*}\Omega_{M_0(N)/T}.$$

Proof. — This is evident if N is invertible in T. Thus, since formation of $R^j f_{T^*}\Omega_{Y/T}$ commutes with flat base change, we are reduced to the cases $T=\mathrm{Spec}(\mathbf{Z})$, and $T=\mathrm{Spec}(\mathbf{F}_N)$. For the latter case, we must check that the regular differentials on $M_0(N)_{/\mathbf{F}_N}$ and on $X_0(N)_{/\mathbf{F}_N}$ coincide. But this is elementary, taking account of the explicit description (diagram 1 of § 1) of $X_0(N)_{/\mathbf{F}_N}$ in terms of $M_0(N)_{/\mathbf{F}_N}$ and using the fact that a meromorphic differential on $\mathbf{P}^1$ with at worst simple poles at two points $a, b\in\mathbf{P}^1$ is uniquely determined by its residue (at a, say).

For $T=\mathrm{Spec}(\mathbf{Z})$, we have:

$$i : H^0(X_0(N), \Omega_{X_0(N)}) \to H^0(M_0(N), \Omega_{M_0(N)})$$

is a morphism of free $\mathbf{Z}$-modules of finite rank (3.3), (3.2). Since $i\otimes_{\mathbf{Z}}\mathbf{Z}[1/N]$ is an isomorphism, it follows that i is injective, with cokernel $\mathscr{C}$ a finite N-primary abelian group.

Since by (3.3), (3.2) $H^1(X_0(N), \Omega_{X_0(N)})$ and $H^1(M_0(N), \Omega_{M_0(N)})$ are free $\mathbf{Z}$-modules, we have the diagram:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & H^0(X_0(N), \Omega_{X_0(N)}) & \longrightarrow & H^0(M_0(N), \Omega_{M_0(N)}) & \longrightarrow & \mathscr{C} & \longrightarrow & 0 \\
 & & \downarrow N & & \downarrow N & & \downarrow N & & \\
0 & \longrightarrow & H^0(X_0(N), \Omega_{X_0(N)}) & \longrightarrow & H^0(M_0(N), \Omega_{M_0(N)}) & \longrightarrow & \mathscr{C} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \\
 & & H^0(X_0(N)_{/\mathbf{F}_N}, \Omega_{X_0(N)/\mathbf{F}_N}) & \xrightarrow{\approx} & H^0(M_0(N)_{/\mathbf{F}_N}, \Omega_{M_0(N)/\mathbf{F}_N}) & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

giving that $\mathscr{C}=0$.

4. Parabolic modular forms.

In this section R will denote a ring *flat over* $\mathbf{Z}$, *or over* $\mathbf{Z}/m$ for some m. We shall be interested in comparing three different points of view concerning *holomorphic modular forms of weight* 2 *over* $\Gamma_0(N)$, *defined over* R.

1. *q-expansions of classical modular forms* (Serre [47]).

If $R\subset\mathbf{Q}$, let $B(R)\subset R[[q]]$ be the R-submodule of q-expansions (at ∞) of (classical) modular forms of the above type (1) (whose q-expansion coefficients (at ∞)

(1) Holomorphic, of weight 2, over $\Gamma_0(N)$.

lie in R). Let $B^0(R) \subset B(R)$ be the subspace generated by parabolic forms. We do not require that the q-expansion coefficients at the *other* cusp o lie in R. Using ([9], VII, (3.18)) and the discussion of § 6, (1) below one sees, however, that these " other " coefficients lie in $N^{-1}.R \subset \mathbf{Q}$. The unspecified term *q-expansion* will mean: at ∞. It follows from the work of Igusa and Deligne or ([69], p. 85, th. (3.52)) that:

$$B(\mathbf{Z}) \otimes R \cong B(R) \quad \text{and} \quad B^0(\mathbf{Z}) \otimes R \cong B^0(R) \quad \text{for} \quad R \subset \mathbf{Q}$$

(formation " commutes with base change ") and we *define* the R-submodules:

$$B^0(R) \subset B(R) \subset R[[q]]$$

for an arbitrary ring R by the above isomorphisms.

2. *Sections of the sheaf $\omega^{\otimes 2}$ over the moduli stack (which are holomorphic at the cusps)* (Katz [24]; Deligne-Rapoport [9]).

Let A(R) (resp. $A^0(R)$) denote the R-module of modular forms (resp. *parabolic* modular forms) of the above sort, as defined in [24], (1.3) (compare [9], VII, § 3). We also refer to an element of A(R) as a *modular form in* $\omega^{\otimes 2}$. Thus, an element $\alpha \in A(R)$ is a rule which assigns to each pair $(E_{/T}, H)$, where E is an elliptic curve over an R-scheme T, and H a finite flat subgroup scheme of $E_{/T}$ of order N, a section $\alpha(E_{/T}, H)$ of $\omega_{E_{/T}}^{\otimes 2}$ where $\omega_{E_{/T}}$ is the sheaf of invariant differentials.

The *rule* α must depend only on the isomorphism class of the pair $(E_{/T}, H)$ and its formation must commute with arbitrary base change $T' \to T$. Finally, it must satisfy the condition of holomorphy at the two cusps.

The *q-expansion morphism*:

$$q\text{-exp} : A(R) \to R[[q]] \quad \alpha \mapsto \tilde{\alpha}$$

defined by:

$$\alpha(\text{Tate curve}_{/R((q))}, \mu_N) = \tilde{\alpha}.\text{square of canonical differential } (1)$$

is *injective*, if R is flat over $\mathbf{Z}$ or if $1/N \in R$ (2) and allows us to identify A(R) with an R-submodule of R[[q]] in these cases.

We shall be especially interested in A(R) for rings R containing 1/N. In this case one has an alternate description of A(R) as the space of holomorphic modular forms of level N, defined over R ([24], (1.2)) which are invariant under the action of the appropriate Borel subgroup.

The question of whether formation of A(R) commutes with base change is a difficult one, and may be viewed as the main technical problem of this paragraph (3).

---

(1) Compare [9], VII, (1.16); [24], A 1.2, p. 161.
(2) This follows from the argument of VII, (3.9) of [9], or, if $1/N \in R$, [24], (1.6.1).
(3) Compare [24], (1.7) and (1.8).

3. *q-expansions of regular differentials.*

The pair (Tate curve$_{/\mathbf{Z}[[q]]}$, μ_N) gives rise to a morphism:

$$\tau : \operatorname{Spec} \mathbf{Z}[[q]] \to M_0(N)_{/\mathbf{Z}}$$

as in [9] VII, Th. (2.1) and τ identifies $\mathbf{Z}[[q]]$ with the formal completion of $M_0(N)_{/\mathbf{Z}}$, along the section over $S = \operatorname{Spec} \mathbf{Z}$ corresponding to the cusp ∞. For any ring R, τ induces a morphism:

$$t : \operatorname{Spec} R((q)) \to M_0(N)_{/R}$$

where $R((q)) = R[[q]][1/q]$ is the ring of " finite-tailed " Laurent-series.

Suppose U is an open subscheme of $M_0(N)_{/R}$ through which the above morphism t factors, and such that $U_{/\mathrm{Spec}(R/N)}$ is contained in the irreducible component of the Hasse domain $M_0(N)^h_{/\mathrm{Spec}(R/N)}$ to which the cusp ∞ belongs. If γ is a regular differential on U, we refer to γ as a *meromorphic* differential on $M_0(N)_{/R}$. Define the *q-expansion* of γ to be that element $\tilde{\gamma}$ of $R((q))$ such that $t^*\gamma = \tilde{\gamma} \cdot \frac{dq}{q}$.

The q-expansion morphism is an *injection* of the space of meromorphic differentials over R to $R((q))$. The reason for this is, briefly, as follows. If γ is defined on U and $\tilde{\gamma} = 0$, then γ is defined, and vanishes, on a formal neighborhood of the section in $M_0(N)_{/R}$ corresponding to the cusp ∞. Since Ω is an invertible sheaf, and the support of γ intersects each geometric fiber of U in a finite number of points, $\gamma = 0$ (cf. argument of [9], VII, th. (3.9); or of [24], (1.6.2)).

The q-expansion morphism also induces an injection:

$$q\text{-exp} : H^0(M_0(N)_{/R}, \Omega(\text{cusps})) \to R[[q]].$$

To prove this when $R = \mathbf{Z}/N$ use the structure of the fiber in characteristic N and the fact that a differential on $\mathbf{P}^1_{/\mathbf{F}_N}$, which possesses at worst simple poles, is known when its poles and (all but one of) its residues are known. It then follows for $R = \mathbf{Z}/N^m$ ($m \geq 1$) by an argument using (3.3). If $1/N \in R$, the argument of the preceding paragraph gives injectivity; if R is flat over $\mathbf{Z}$ one must use that $M_0(N)$ is Cohen-Macaulay.

By means of the map q-exp, we identify $H^0(M_0(N)_{/R}, \Omega(\text{cusps}))$ with a sub-R-module of $R[[q]]$.

The relation between A(R) and $H^0(M_0(N)_{/R}, \Omega(\text{cusps}))$ is given by the " Kodaira-Spencer style morphism " of [24], (1.5) and A, (1.3.17). For our purposes, the following statement is convenient.

Lemma (**4.1**). — *The natural mapping* ([24], A, (1.3.17)):

$$\omega^{\otimes 2} \to \Omega^1$$

a) *is an isomorphism on the complement of the cuspidal sections in* $X_1(N)_{/R}$, *for any* R, *as above, which contains* $1/N$;

b) *is defined on the complement of the cuspidal sections and the supersingular points of characteristic* N *in* $X_0(N;3)$, *for any* R, *as above, which contains* $1/6$.

Now when R contains $1/N$, let:

$U_1(N)_{/R}$ = the open subscheme of $X_1(N)_{/R}$ obtained by removing the discriminant locus of $X_1(N) \to X_0(N)$.

$U_0(N)_{/R}$ = the image of $U_1(N)_{/R}$ in $X_0(N)_{/R}$. The Galois covering $U_1(N)_{/R} \to U_0(N)_{/R}$ is a finite étale Galois extension with Galois group $(\mathbf{Z}/N)^*/(\pm 1)$ [1].

When R contains $1/6$, let:

$V_0(N;3)_{/R}$ = the open subscheme of $X_0(N;3)_{/R}$ obtained by removing the discriminant locus of $X_0(N;3) \to X_0(N)$ and the " supersingular points " in characteristic N.

$V_0(N)_{/R}$ = the image of $V_0(N;3)_{/R}$ in $M_0(N)_{/R}$. If G is the covering group of $X_0(N;3) \to X_0(N)$, then $V_0(N;3) \to V_0(N)$ is a finite étale Galois extension with covering group G.

Lemma (**4.2**). — *The Kodaira-Spencer morphism induces*:

an imbedding: $A(R) \to H^0(U_0(N)_{/R}, \Omega(\text{cusps}))$ *if* $1/N \in R$;

a morphism: $A(R) \to H^0(V_0(N)_{/R}, \Omega(\text{cusps}))$ *if* $1/6 \in R$.

Moreover, these morphisms bring $A^0(R)$ *to the subspace of* regular *differentials on the respective bases.*

Proof. — Suppose $1/N \in R$. Modular forms for $\Gamma_0(N)$ on $\omega^{\otimes 2}$ ([24], (1.3)) are modular forms for $\Gamma_1(N)$ which are invariant under the action of the covering group. Using lemma (4.1), the Kodaira-Spencer morphism associates to an element α in A(R) a regular differential a_1 on the complement of the cuspidal sections in $U_1(N)_{/R}$, which is invariant under the action of the covering group. Since $U_1(N)_{/R} \to U_0(N)_{/R}$ is étale, a_1 descends to a regular differential a on the complement of the cuspidal sections in $U_0(N)_{/R}$. By Cor. A, (1.3.18) of [24], the q-expansions of a coincide with the q-expansions of α. The condition of holomorphy (resp. parabolicity) at the cusps then insures that a have at worst a simple pole (resp. is regular) at the cusps; consequently a is a section of $\Omega(\text{cusps})$ (resp. Ω) on all of $U_0(N)_{/R}$.

Similarly, if $1/6 \in R$, one constructs a differential on $V_0(N)_{/R}$.

Note that both $U_0(N)_{/R}$ and $V_0(N)_{/R}$, when defined, are open dense subschemes of $M_0(N)_{/R}$. Also, the construction which associates to α differentials on these open subschemes yields the *same* differential on the intersection (same q-expansion).

Consequently, to any $\alpha \in A(R)$, and for any ring R as considered in this section, we may associate a *meromorphic* differential on $M_0(N)_{/R}$, a, with the same q-expansion as α.

---

[1] To avoid confusion with various Galois actions we refer to this group as *covering group.*

To compare differentials with elements of B(R), we begin with:

Lemma **(4.3)**:

$$H^0(M_0(N)_{/R}, \Omega) \subset B^0(R) \subset R[[q]]$$
$$H^0(M_0(N)_{/R}, \Omega(\text{cusps})) \subset B(R) \subset R[[q]].$$

Proof. — If $R = \mathbf{Z}$, the first inclusion follows since $H^0(M_0(N)_{/\mathbf{Z}}, \Omega)$ is a subspace of $H^0(M_0(N)_{/\mathbf{Q}}, \Omega)$ having integral q-expansions. Consequently we obtain the desired inclusion for any R of the type considered in this section, since formation of both range and domain commute with base change $\mathbf{Z} \to R$ (3.3). The second inclusion follows similarly.

Lemma **(4.4)**:

(1) *If* R *is a field of characteristic* $p \neq N$, *then*:

$$A^0(R) = H^0(M_0(N)_{/R}, \Omega)$$

and:

$$A(R) = H^0(M_0(N)_{/R}, \Omega(\text{cusps}, (i))) \quad \textit{if} \quad p = 2 \quad \textit{and} \quad N \equiv 1 \bmod 4$$
$$A(R) = H^0(M_0(N)_{/R}, \Omega(\text{cusps}, (\rho))) \quad \textit{if} \quad p = 3 \quad \textit{and} \quad N \equiv 1 \bmod 3$$
$$A(R) = H^0(M_0(N)_{/R}, \Omega(\text{cusps})) \quad \textit{otherwise}$$

(i.e. $p \geq 5$, *or* $p = 2$, $N \equiv -1 \bmod 4$ *or* $p = 3$, $N \equiv -1 \bmod 3$). *(See Table* 1.*)*

(2) *If* $R = \mathbf{Z}[1/m]$ *for some integer m, then*:

$$A(R) \subset H^0(M_0(N)_{/R}, \Omega(\text{cusps}))$$
$$A^0(R) \subset H^0(M_0(N)_{/R}, \Omega).$$

Note. — By $\Omega(\text{cusps}, (i))$ is meant the sheaf of meromorphic differentials which have, at worst, simple poles at the cusps and at the point (i) of Table 1.

Proof. — Let $\alpha \in A(R)$ and let a be its associated meromorphic differential.

(1) R *a field of characteristic* $p \neq N$:

Here a is a meromorphic differential on $M_0(N)_{/R}$ which is regular on $U_0(N)_{/R}$, except for possible simple poles at the cusps, and which lifts to a differential on $X_1(N)_{/R}$ regular except at the cusps.

We shall make a local calculation to determine when a meromorphic differential can become regular, after finite extension. Explicitly, let k be an (algebraically closed) field of characteristic p and $D_1 \subset D_2$ a finite extension of k-algebras, which are discrete valuation rings, with residue field k.

Let a_1 denote a *meromorphic* differential on D_1 relative to k, and let a_2 denote the induced differential on D_2, relative to k.

Sublemma. — *If* $D_1 \subset D_2$ *is (étale, or) tamely ramified, then the meromorphic differential* a_2 *is a regular differential* (resp. *has a simple pole*) *if and only if* a_1 *is a regular differential* (resp. *has a simple pole*) *on* D_1.

If $D_1 \subset D_2$ *is wildly ramified of the first type* (2.2), *then* a_2 *is a regular differential if and only if* a_1 *has (at worst) a simple pole on* D_1.

Proof. — Since there are no nontrivial étale extensions in our situation, we may assume $D_1 \subset D_2$ a totally ramified Galois extension of degree r. Write $D_2 = k[[y]]$ for a choice of uniformizer y of D_2, and $D_1 = k[[x]]$, where x is a uniformizer, chosen so that $x = \varphi(y)$, where $\varphi(Y) \in k[Y]$ is a polynomial.

Using ([60], III, 7, Cor. 2) one calculates the different of $D_1 \subset D_2$ to be $(\varphi'(y))$. If v_2 is the valuation on D_2 such that $v_2(y) = 1$, then $v_2(x) = r$, and $v_2(\varphi'(y))$ can be calculated in terms of the orders of the higher ramification groups of $D_1 \subset D_2$ ([60], IV, § 2, Prop. 4: $v_2(\varphi'(y)) = \sum_{i=0}^{\infty} (\mathrm{Card}(G_i) - 1)$) and consequently:

$$v_2(\varphi'(y)) = r - 1 \qquad \text{(tamely ramified case)}$$

$$v_2(\varphi'(y)) = 2p - 2 \qquad \text{(wild ramification of first type).}$$

Up to multiplication by a unit in D_1, we may write a_1 as $x^s . dx$ for some $s \in \mathbf{Z}$. Thus, a_2 is, up to a unit, of the form $x^s . \varphi'(y) . dy$, and:

$$v_2(x^s . \varphi'(y)) = rs + r - 1 \qquad \text{(tame ramification of degree } r\text{)}$$

$$= ps + 2(p-1) \qquad \text{(wild ramification of first type).}$$

The assertions of the lemma can now be read off from the above formulae (*e.g.*, in the case of wild ramification of first type, $s \geq -1$ if and only if $ps + 2(p-1) \geq 0$).

Now return to the case (1) of lemma (4.4), and the meromorphic differential a. By Table 1, $X_1(N)_{/R} \to X_0(N)_{/R}$ has *at most one point of wild ramification*, and none if characteristic $R \neq 2, 3$. Moreover, if there is a point of wild ramification, it is of first type.

By the sublemma, the meromorphic differential a is regular with the exception of possible simple poles at 0, ∞, and (i) and (ρ), *if they occur* (see Table 1). Conversely, any meromorphic differential which is regular, except for such simple poles will (by the sublemma) lift to a differential on $X_1(N)$ with, at worst, simple poles at cusps. This gives us the identification of $A(R)$ with the appropriate space of meromorphic differentials, as in the statement of (1). The subspace $A^0(R)$ is then identified with the space of differentials on $M_0(N)$ which are regular everywhere with the exception of a possible simple pole at (i) (if $p = 2$, and $N \equiv 1 \bmod 4$) or at (ρ) (if $p = 3$, and $N \equiv 1 \bmod 3$). Since the sum of the residues of a differential over a complete curve is zero, it follows that $A^0(R)$ is identified with the space of everywhere regular differentials.

(2) $R = \mathbf{Z}[1/m]$:

We show $A^0(R) \subset H^0(M_0(N)_{/R}, \Omega)$; the other inclusion is proved in the same way.

Recall that $M_0(N)^h_{/R}$ denotes the complement of the characteristic N supersingular points, in $M_0(N)_{/R}$. The meromorphic differential a is regular on an open dense subscheme of $M_0(N)^h_{/R}$.

Let D_∞ (resp. D_0) denote the *divisor of poles* (resp. *of zeroes*) of a, on $M_0(N)^h_{/R}$. Recall their definition: if x is a point of the scheme $M_0(N)^h_{/R}$, and $\mathcal{O}_x$ the local ring at x, let φ_x be a local generator of $\Omega_{M_0(N)^h_{/R}}$ at x. Since $\mathcal{O}_x$ is a unique factorization domain, one can find $g_x, h_x \in \mathcal{O}_x$ with no common factors such that $g_x . a = h_x . \varphi_x$. A local equation at x for D_∞ (resp. for D_0) is given by: $g_x = 0$ (resp. $h_x = 0$).

Now let p be a prime number with these properties:

a) $p \nmid 2.3.N.m$;

b) D_∞ and D_0 have disjoint support in characteristic p : $|D_\infty \otimes \mathbf{F}_p| \cap |D_0 \otimes \mathbf{F}_p| = \emptyset$.

It follows from the definition of polar divisor and *a), b)* that $a \otimes \mathbf{F}_p$ is definitely nonholomorphic at $D_\infty \otimes \mathbf{F}_p$. Therefore part (1) of our proposition implies that the support of D_∞ is disjoint from the fibre of $M_0(N)^h_{/R} \xrightarrow{\pi} \mathrm{Spec}(R)$ in characteristic p. Since D_∞ contains no irreducible component of any fibre of π, it follows that $D_\infty = 0$; therefore a is regular on $M_0(N)^h_{/R}$. To see that a is, in fact, regular on $M_0(N)_{/R}$, use that the supersingular points of characteristic N are of codimension 2 in $M_0(N)_{/R}$, and Ω is an invertible sheaf, and $M_0(N)_{/R}$ is Cohen-Macaulay (SGA 2, Exp. III, Cor. (3.5)).

Lemma **(4.5)**. — *Let* R *be flat over* $\mathbf{Z}[1/N]$. *Then*:

$$A(R) = H^0(M_0(N)_{/R}, \Omega(\text{cusps})) = B(R)$$
$$A^0(R) = H^0(M_0(N)_{/R}, \Omega) = B^0(R).$$

Proof. — We establish the first line above; the second may be obtained by essentially the same argument.

First let $R = \mathbf{Z}[1/N]$. By the previous two lemmas, we have inclusions:

$$A(R) \subset H^0(M_0(N)_{/R}, \Omega(\text{cusps})) \subset B(R)$$

and so we must prove that $A(R) = B(R)$. But this follows from the *q-expansion principle* ([24], Cor. (1.6.2)). To be more precise, using the notation of (1.6.2), take f to be any element in B(R), $n = N$, $K = \mathbf{Q}$, $L = R$. Katz's corollary (1.6.2) then gives us that f is a holomorphic modular form (in $\omega^{\otimes 2}$) of level N, defined over R. Since f, viewed as a modular form of level N, is invariant under the appropriate Borel subgroup of $GL_2(\mathbf{F}_N)$, it is in A(R).

Now let R be flat over $\mathbf{Z}[1/N]$. Lemma (4.5) will follow from what we have done, provided we show that:

$$A(R) = A(\mathbf{Z}[1/N]) \otimes_{\mathbf{Z}[1/N]} R.$$

Even this " commutation with base change " is not totally trivial. If one takes the point of view that A(R) is the space of $(\mathbf{Z}/N)^*/(\pm 1)$-invariant differentials (regular, with the possible exception of simple poles at cusps) on $X_1(N)_{/R}$, however, it is an easy exercise (1).

---

(1) If G is a group and M a $\mathbf{Z}[1/N][G]$-module, flat over $\mathbf{Z}[1/N]$, and R a flat $\mathbf{Z}[1/N]$-module, then $M^G \otimes_{\mathbf{Z}[1/N]} R$ is isomorphic to $(M \otimes_{\mathbf{Z}[1/N]} R)^G$. (The superscript G denotes invariants under G.)

Lemma (4.6):

$$H^0(M_0(N)_{/R}, \Omega(\text{cusps})) = B(R)$$
$$H^0(M_0(N)_{/R}, \Omega) = B^0(R).$$

Proof. — We show the second equality; the first is done similarly. It suffices to prove this equality for $R=\mathbf{Z}$, since formation of both sides of the equation commutes with base change from $\mathbf{Z}$ to any of the rings R we consider.

By lemmas (4.3) and (4.5), $H^0(M_0(N)_{/\mathbf{Z}}, \Omega)$ is a subgroup of $B^0(\mathbf{Z})$, and the quotient $\underset{\sim}{Q}$ is an N-primary finite abelian group. Since:

$$H^0(M_0(N)_{/\mathbf{F}_N}, \Omega) \subset B^0(\mathbf{F}_N) \subset \mathbf{F}_N[[q]]$$

one checks that multiplication by N is an isomorphism on $\underset{\sim}{Q}$.

Lemma (4.7). — *Let m be an integer prime to* N *and* $R=\mathbf{Z}/m$. *Then*:

$$H^0(M_0(N)_{/R}, \Omega(\text{cusps})) \subset A(R)$$
$$H^0(M_0(N)_{/R}, \Omega) \subset A^0(R).$$

Proof. — These inclusions follow from (4.5) and the fact that the morphisms:

$$H^0(M_0(N)_{\mathbf{Z}[1/N]}, \Omega(\text{cusps})) \to H^0(M_0(N)_{/R}, \Omega(\text{cusps}))$$
$$H^0(M_0(N)_{\mathbf{Z}[1/N]}, \Omega) \to H^0(M_0(N)_{/R}, \Omega)$$

are surjective (3.3).

Lemma (4.8). — *Let m be prime to* N, *and* $R=\mathbf{Z}/m$. *Then*:

$$A^0(R) = H^0(M_0(N)_{/R}, \Omega) = B^0(R)$$

and:

$$A(R) = H^0(M_0(N)_{/R}, \Omega(\text{cusps})) = B(R)$$

if m and N *satisfy the following properties*:

(a) *either* $m \not\equiv 0 \bmod 2$, *or* $N \not\equiv 1 \bmod 4$ *and*

(b) *either* $m \not\equiv 0 \bmod 3$, *or* $N \not\equiv 1 \bmod 3$.

Proof. — In the light of (4.6), what must be shown is that the inclusions of (4.7) are equalities, under the hypotheses above. Lemma (4.4) (1) assures us that they are if m is a prime number. We now proceed by induction. Let p be a prime dividing m; $m=m'.p$. Let $R' \subset R$ be the sub-R-module consisting in multiples of p ($R' \cong \mathbf{Z}/m'$).

Consider:

$$\begin{array}{ccccc} A(R') & \longrightarrow & A(R) & \longrightarrow & A(\mathbf{F}_p) \\ \uparrow & & \uparrow & & \uparrow \\ H(R') & \longrightarrow & H(R) & \longrightarrow & H(\mathbf{F}_p) \longrightarrow 0 \end{array}$$

where $H(*)$ stands for $H^0(M_0(N)_{/*}, \Omega(\text{cusps}))$. The bottom line is exact since formation of $H(*)$ commutes with the type of base change which occurs in that line (3.3). The top line is exact, by an application of the q-expansion principle ([24], (1.6.2)). The two flanking vertical inclusions are isomorphisms by induction, since if m and N satisfy (a), (b), then m' and N also satisfy (a), (b). Therefore the central vertical inclusion is an equality, as well. This establishes the assertion of lemma (4.8) concerning $A(R)$; the assertion concerning $A^0(R)$ is established by a similar argument.

Summary and convention **(4.9)**. — We shall be chiefly concerned with modular forms of weight 2, over $\Gamma_0(N)$, for some (usually fixed) prime number $N \geq 5$. Except when indicated explicitly to the contrary, a *parabolic modular form* (*over* $\Gamma_0(N)$, *defined over* R) will mean an element of $B^0(R)$; or, equivalently, a regular differential on $M_0(N)_{/R}$; or, equivalently (if R is flat over $\mathbf{Z}$ or over a field) a regular differential on $X_0(N)_{/R}$; or (if $R = \mathbf{Z}/m$ with $(m, N) = 1$ (4.8); or R flat over $\mathbf{Z}[1/N]$ (4.5)) an element of $A^0(R)$.

For holomorphic (nonparabolic) modular forms it is true that elements of $B(R)$ coincide with differentials defined over R, regular with the possible exception of simple poles at cusps (4.6). Nevertheless, for certain rings R, $A(R)$ may differ from $B(R)$ (*e.g.*, Remark below). Thus we shall always make clear, in what follows, whether we are dealing with an element of $A(R)$ (*a modular form in* $\omega^{\otimes 2}$) or of $B(R)$, and both notions will be useful.

Remark (concerning the distinction between $A(R)$ and $B(R)$). — The Riemann-Roch Theorem and the description given in (4.4) (1) show that $B(R)$ is of *codimension* 1 in $A(R)$, if R is a field of characteristic 2 and $N \equiv 1 \bmod 4$; or of characteristic 3 and $N \equiv 1 \bmod 3$.

In certain cases one can exhibit an element of $A(R)$, not in $B(R)$. For example, if $\operatorname{char} R = 2$, and $N \equiv 5 \bmod 8$, it follows from the description in (5.12) below that the power series δ modulo 2 is (the q-expansion of) such an element; the power series δ modulo 3 is such an element if $\operatorname{char} R = 3$, and $N \equiv 4$ or $7 \bmod 9$.

On the other hand, the Eisenstein series e' (§ 5) is in $B(\mathbf{Z})$ but not $A(\mathbf{Z})$, since its q-expansion coefficients *at the cusp* 0 can be seen to lie in $N^{-1}.\mathbf{Z}$ but not in $\mathbf{Z}$.

Proposition **(4.10)**. — *There are no nonvanishing parabolic modular forms over* $\Gamma_0(1)$ (*in* $\omega^{\otimes 2}$), *defined over any ring* R *flat over* $\mathbf{Z}$ *or over* $\mathbf{Z}/m$.

Remark. — There *are* nontrivial *holomorphic* modular forms over $\Gamma_0(1)$ (in $\omega^{\otimes 2}$), defined over certain rings R (cf. (5.6)).

Proof. — If $1/5 \in R$, lift to $M_0(5)_{/R}$. This is a curve of genus 0, and therefore has no nonvanishing regular differentials on it. Since $1/5 \in R$ there are no parabolic modular forms (in $\omega^{\otimes 2}$) over $\Gamma_0(5)$, as well. Therefore there are none over $\Gamma_0(1)$.

If $1/7 \in R$, lift to $X_0(7)$ and use the same argument.

The general ring R (as considered in this section) is then treated by patching.

5. Nonparabolic modular forms.

(5.1)

Consider the following three power series in $\mathbf{Z}[[q]]$.

$$e = 1 - 24 \sum_{m=1}^{\infty} \sigma(m) q^m$$

where $\sigma(m)$ is the sum of the positive divisors of m.

$$e' = 1 - N - 24 \sum_{m=1}^{\infty} \sigma'(m) q^m$$

where $\sigma'(m)$ is the sum of the positive divisors of m which are prime to N (as usual, N is a fixed prime number ≥ 5).

$$\delta = \sum_{m=1}^{\infty} \sigma'(m) q^m.$$

The power series e is the q-expansion of the *Eisenstein series of weight* 2 of level 1 [1]. It is the logarithmic derivative of the q-expansion of the normalized modular form (of level 1) of weight 12:

$$\Delta = q \prod_{m=1}^{\infty} (1-q^m)^{24} \text{ [2]}.$$

The power series $e'(q) = e(q) - N.e(q^N)$ is the q-expansion of the *Eisenstein series of weight* 2 *on* $\Gamma_0(N)$ [3]. It may be regarded, as meromorphic differential, as the logarithmic derivative of the function $\Delta(q)/\Delta(q^N)$ on $M_0(N)_{/\mathbf{Q}}$. Since this functions has zeroes and poles only at the cusps, e' is (the q-expansion of) a differential whose only poles are (simple) poles, occurring at the cusps. Since e' has integral coefficients, we have $e' \in B(\mathbf{Z})$. *Viewed as modular form in* $\omega^{\otimes 2}$ *over* $\mathbf{Q}$, the q-expansion of e' *at the cusp* o may be seen to be (using [9], VII, (3.18)):

$$1/N.(N - 1 + 24 \sum_{m=1}^{\infty} \sigma'(m) q^{m/N})$$

and therefore e' is not in $A(\mathbf{Z})$.

The power series δ is simply e', *deprived of its constant term and conveniently normalized.* It will be of interest to consider those rings R over which δ is a modular form.

It is proved in [24], (4.5.4) (also (A.2.4) if $p \geq 5$) that e is a *p-adic modular form* ([24], (2.2)) for every p. Thus, if $R = \mathbf{F}_p$, e is the q-expansion of a meromorphic differential on the Hasse domain $X_0(1)^h_{/R}$. This differential may have poles at the

---

(1) It is the q-expansion of $\left(\frac{3}{\pi^2}\right).G_2(\tau; 0, 0, 1)$ in Hecke's terminology ([19], p. 474). It is denoted P in [24].

(2) Cf. [24], A 1.4.4 for a proof of this fact, which does *not* use the Jacobi identity.

(3) The q-expansion of $\left(-\frac{3}{\pi^2}\right).E(\tau, N)$ in HECKE [19], p. 474.

supersingular points. Our first object will be to study e, both as section of $\omega^{\otimes 2}$ over the moduli stack, restricted to the Hasse domain, and as meromorphic differential.

Lemma **(5.1)**. — *The power series e is the q-expansion of the meromorphic differential*:

$$\frac{-dj}{j} \text{ modulo } 2^4.3^2.5$$

and of:

$$-\frac{dj}{j-1728} \text{ modulo } 2^4.3^2.7$$

on $X_0(1)$.

Remarks. — In the above, j is the elliptic modular function, which is a rational parameter for $X_0(1)$, and has q-expansion beginning $1/q+744+\ldots$. If:

$$e_4 = 1 + 240 \sum_{m=1}^{\infty} \sigma_3(m) q^m$$

$$e_6 = 1 - 504 \sum_{m=1}^{\infty} \sigma_5(m) q^m$$

are the normalized Eisenstein series of weight 4 and 6 respectively, we have:

(5.2) $$j = e_4^3/\Delta = 1728 + e_6^2/\Delta.$$

It would be interesting to study the poles and residues of e at the supersingular points of $X_0(1)_{/\mathbf{Z}/p^r}$ for p^r any power of a prime. O. A. L. Atkin, M. Ashworth, and (independently) N. Koblitz have some interesting formulae, algorithms, and machine computations which suggest some precise conjectures in this direction.

Proof of lemma (5.1). — Take logarithmic derivatives of formulas (5.2), regarded as identities in power series in q, noting that:

$$d\log(e_4^3) \equiv 0 \text{ modulo } 3.240 = 2^4.3^2.5$$

$$d\log(e_6^2) \equiv 0 \text{ modulo } 2.504 = 2^4.3^2.7.$$ Q.E.D.

To study e as a section of $\omega^{\otimes 2}$ over the moduli stack, recall the standard formulas giving elliptic curves in " generalized Weierstrass form " over arbitrary bases (we use the notation and conventions of Tate. Cf. Appendix 1 [29]). Thus, if $(E_{/T}, \pi)$ is an elliptic curve over the base scheme T, equipped with an invariant differential, π, we may represent $(E_{/T}, \pi)$ locally for the Zariski topology over T as a curve:

(5.3)
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$\pi = dx/(2y + a_1x + a_3) = dy/(3x^2 + 2a_2x + a_4 - a_1y)$$

where, if $f : E \to T$ is the structure map, and $\varepsilon : T \to E$ the zero-section, then $(1, x)$ is a basis of $f_*\mathcal{O}(2\varepsilon)$ and $(1, x, y)$ is a basis of $f_*\mathcal{O}(3\varepsilon)$.

This representation may be modified by making a different choice (π', x', y') to

obtain a new equation (5.3)′. The relation between the old and new choices is given by the " data ":

$$(u, r, s, t) \quad \text{where} \quad u \in \Gamma(T, \mathcal{O}_T^*)$$
$$r, s, t \in \Gamma(T, \mathcal{O}_T)$$

defined by the formulas:

$$\pi' = u\pi$$
$$x = u^2x' + r$$
$$y = u^3y' + su^2x' + t$$

and, conversely, any such data gives us a new choice. The new formula (5.3)′ is related to the old by:

$$ua_1' = a_1 + 2s$$
$$u^2a_2' = a_2 - sa_1 + 3r - s^2$$
$$u^3a_3' = a_3 + ra_1 + 2t$$
$$u^4a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st$$
$$u^6a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1.$$

Following Tate, define:

$$b_2 = a_1^2 + ra_2; \qquad b_4 = a_1a_3 + 2a_4.$$

For the new formula (5.3)′ one has:

(5.4) $$u^2b_2' = b_2 + 12r; \qquad u^4b_4' = b_4 + rb_2 + 6r^2.$$

Lemma **(5.5).** — *Let* $R = \mathbf{Z}/72$ $(72 = 2^3 \cdot 3^2)$. *Let* T *be an* R*-scheme. Let* $(E_{/T}, \pi)$ *be a pair consisting in an elliptic curve* $E_{/T}$ *and an invariant differential* π *such that* b_2 *is invertible in* $\Gamma(T, \mathcal{O}_T)$. *Then the function* $\varepsilon = b_2 - 12b_4/b_2$ *depends only on the isomorphism class of the pair* $(E_{/T}, \pi)$ *and not on the representation* (5.3) *chosen. It defines a section of* $\omega^{\otimes 2}$ *over the open substack of the moduli stack of level* 1 *over* R *obtained by removing the cusps and " inverting* b_2 ". *The q-expansion of* ε *is e, modulo* 72.

Proof. — One checks, using (5.4) and working modulo 72, that the relation between ε and ε' (under a change of representation given by the " data " (u, r, s, t)) is $u^2\varepsilon' = \varepsilon$ which establishes everything but the last sentence of lemma (5.5). For this, we evaluate ε on the Tate curve whose equation is ([63], IV, 30):

$$y^2 - xy = x^3 + a_4x + a_6 \qquad \left(a_4 = -5\sum_n \frac{n^3q^n}{1-q^n}\right)$$

Thus, $b_2 = 1$ and $b_4 = -10\sum_n \frac{n^3q^n}{1-q^n}$, giving $\varepsilon = 1 + 120\sum_{m=1}^{\infty} \frac{m^3q^m}{1-q^m}$. Since $120m^3 \equiv -24m \bmod 72$, we conclude that $\varepsilon = e$.

Remark. — This lemma gives the first two terms of an " asymptotic expansion " of e in terms of the parameter b_2 (which cuts out the supersingular locus, 2-adically

and 3-adically). Using his algorithm and machine computation, N. Koblitz has obtained the first 40 terms.

Proposition **(5.6)**. — (*Holomorphic modular forms of level* 1):

(a) *There are no nontrivial holomorphic modular forms of level* 1 (*in* $\omega^{\otimes 2}$) *defined over a field* R *of characteristic* $\neq 2, 3$.

(b) *The "square of the Hasse invariant" is a holomorphic modular form* mod 4, *with q-expansion equal to e.*

The "Hasse invariant" is a holomorphic modular form mod 3, *with q-expansion equal to e.*

(c) *If* φ *is a holomorphic modular form* (*of level* 1; *in* $\omega^{\otimes 2}$), *defined over* $R = \mathbf{Z}/m$, *with q-expansion beginning with the constant* 1, *then*:

(i) *m divides* 12;

(ii) $\varphi = e$.

Summary. — Every holomorphic modular form of level 1, defined over $R = \mathbf{Z}/m$ has q-expansion *equal to a constant.*

Proof:

(a) R *a field of characteristic* $\neq 2, 3$

Let φ be such a holomorphic modular form defined over R, and denote by the same letter the meromorphic differential on $X_0(1)_{/R}$ associated to φ. Since the moduli stack associated to $\Gamma_0(1; 3)$ "exists" (§ 1), lifting φ to $X_0(1; 3)$ yields a meromorphic differential, with at worst, simple poles at the cusps. Since $X_0(1; 3) \to X_0(1)$ is a tamely ramified Galois extension, the sublemma in the proof of (4.4) assures us that φ has, at worst a simple pole at the cusp ∞ of $X_0(1)_{/R}$. Since $X_0(1)_{/R}$ is of genus 0, φ must vanish.

(b) Going back to (5.5) one sees that, modulo 12, e is given by b_2, and is therefore a holomorphic modular form modulo 12. Its q-expansion is the constant 1. Modulo p (any p) the Hasse invariant is a holomorphic modular form of weight $p-1$, and q-expansion *equal to* 1 ([24], (2.0)).

Thus, modulo 2, the Hasse invariant is of weight 1 and can be taken to be a_1. By "the square of Hasse invariant mod 4" we mean a_1^2, which is a section of $\omega^{\otimes 2}$, mod 4. But, $e \equiv b_2 \equiv a_1^2 \bmod 4$.

Working modulo 3, the Hasse invariant is a modular form of weight 2, with the same q-expansion as e. It coincides, therefore, with e.

(c) Let φ be a holomorphic modular form mod m, such that the constant term of its q-expansion is 1. By (a) $m = 2^a.3^b$. To show that m divides 12, it suffices to show that no such φ can exist mod 8 or mod 9.

Let φ be such a modular form mod 8 (resp. mod 9). Note that $\varphi \equiv e \bmod 4$ (resp. mod 3), because, by (b) $\varphi - e$ is a holomorphic modular form mod 4 (resp. mod 3);

it is parabolic by our assumptions on φ, and therefore must be zero by (4.8). Let $R=\mathbf{Z}/8$ (resp. $\mathbf{Z}/9$).

We may write $\varphi=r(j).e$, where $r(j)$ is a rational function in j (viewed as rational parameter of $X_0(1)$) with coefficients in R. If we view both φ and e as meromorphic differentials, and use (5.1) that $e=-\frac{dj}{j}$, and (4.2) that φ is a regular differential on the open subscheme Spec $R[j,j^{-1}]$ of $X_0(1)_{/R}$, we obtain that $r(j)$ is in $R[j,j^{-1}]$. By the above, we may write $r(j)=1+4L(j)$ (resp. $1+3L(j)$) where $L(j)$ is a "Laurent polynomial" in $R[j,j^{-1}]$. We now use holomorphicity of φ about the point $j=0$, together with the above description of $r(j)$.

If $R=\mathbf{Z}/8$, consider the following elliptic curve E over the power series ring $R[[t]]$.

$$E: y^2+txy+y=x^3, \qquad \pi=dx/(2y+tx+1)$$

One computes:

$$\begin{aligned} &b_2=t^2 \\ &b_4=t \qquad e=b_2-12b_4/b_2=t^2-12/t\in R[[t]][t^{-1}] \\ &j=t^{12}(t^3-27)^{-1}\in R[[t]]. \end{aligned}$$

We now compute the value of the section φ of $\omega^{\otimes 2}$ on the pair (E,π) over the ring of finite-tailed Laurent series $R[[t]]\,[t^{-1}]$.

$$\begin{aligned} \varphi(E,\pi)&=(1+4L(j))(t^2-12/t)\in R[[t]]\,[t^{-1}] \\ &=t^2-12/t+4t^2.L(j). \end{aligned}$$

Since φ is holomorphic, and (E,π) is defined over $R[[t]]$, $\varphi(E,\pi)$ must lie in $R[[t]]\subset R[[t]]\,[t^{-1}]$. That is:

(5.7) $$12/t-4t^2.L(j)\in R[[t]].$$

Let j^b be the *lowest* power of j occuring in the Laurent polynomial $L(j)$ with coefficient a unit mod 8. Writing $4t^2\,L(j)$ as a finite-tailed Laurent series in t, one has that t^{12b+2} is the lowest power of t occuring with nonzero coefficient. One reasons now, that if b is nonnegative, the $12/t$ term in (5.7) cannot be cancelled by any term in $4t^2L(j)$, while if b is negative, t^{12b+2} is the lowest power of t occurring in the expression of (5.7). In either case, one has a contradiction.

If $R=\mathbf{Z}/9$, it is convenient to work with the elliptic curve E given by the representation:

$$a_1=a_3=1; \qquad a_2=(t-1)/4; \qquad a_4=0; \qquad a_6=-1/4.$$

Then:

$$\begin{aligned} &b_2=t \\ &b_4=1 \qquad e=b_2-12b_4/b_2=t-12/t\in R[[t]][t^{-1}] \\ &j=4t^6(t^2-32)^{-1}\in R[[t]]. \end{aligned}$$

Again: $\varphi(E, \pi) = (1 + 3L(j))(t - 12/t)$

(5.8) $\qquad = t - 12/t + 3t.L(j) \in R[[t]]\ [t^{-1}].$

If j^b is the lowest power of j occurring with unit coefficient in the Laurent polynomial L, then t^{6b+1} is the lowest power of t occurring with nonzero coefficient in $3t.L(j) \in R[[t]][t^{-1}]$, and, as above, (5.8) leads to a contradiction. Q.E.D.

We now prepare to study the status of the q-expansion " 1 " as a modular form over $\Gamma_0(N)$. The following lemma, which is in the spirit of the theory of Atkin-Lehner, and which was suggested to me by J.-P. Serre, will be helpful.

Lemma **(5.9)** (reduction of level). — *Let* $1/N \in R$. *Let* φ *be a holomorphic modular form in* $\omega^{\otimes k}$ *over* $\Gamma_0(N)$, *defined over* R $(k \geq 2)$.

Suppose, further, that the q-expansion (at ∞*) of* φ *is a power series in* $q^N : \widetilde{\varphi} = \widetilde{f}(q^N)$, $\widetilde{f} \in R[[q]]$.

Then $\widetilde{f}$ *is the q-expansion of a holomorphic modular form over* $\Gamma_0(1)$ *(again in* $\omega^{\otimes k}$, *and defined over* R).

To obtain an analogue of (5.9) in characteristic N, we return to the setting of interest to us:

Lemma **(5.10)**. — *Let* $N \geq 5$ *be a prime number and* φ *a holomorphic modular form over* $\Gamma_0(N)$, *in* $B(\mathbf{F}_N)$ (§ 4). *Suppose, further, that the q-expansion of* φ *is a power series in* $q^N : \widetilde{\varphi} = \widetilde{f}(q^N)$.

Then $\varphi = 0$.

Proof of lemma (5.9). — Let $\mathcal{N}$ denote the stack $\mathcal{M}_0(N)$ over R and $\mathcal{N}^0 = \mathcal{M}_0(N)^0$. Thus, if one is given a pair $(E_{/T}, H)$ where T is an R-scheme, E is an elliptic curve over T, and $H \subset E$ is a subgroup of order N, defined over T, one may associate to $(E_{/T}, H)$ a T-valued section of the stack $\mathcal{N}$. There are maps:

$$\mathcal{M}_N^0 \xrightarrow{\alpha} \mathcal{N}^0 \xrightarrow{\beta} \mathcal{M}_1^0$$

where $\mathcal{M}_N^0$ and $\mathcal{M}_1^0$ are the moduli stacks of level N and 1 respectively, defined over R.

These maps are determined by the rules:

$$(E_{/T}, \gamma) \xrightarrow{\alpha} (E'_{/T}, H)$$

where $\gamma : \mathbf{Z}/N \times \mathbf{Z}/N \xrightarrow{\sim} E[N]$ is an isomorphism of group schemes over T, and: E′ is taken to be $E/\gamma(0 \times \mathbf{Z}/N)$; H is taken to be the image of $\gamma(\mathbf{Z}/N \times 0)$.

$$(E_{/T}, H) \xrightarrow{\beta} (E/H).$$

The map $\beta\alpha : \mathcal{M}_N^0 \to \mathcal{M}_1^0$ is a Galois, étale morphism of stacks. The Galois (covering) group may be identified with $GL_2(\mathbf{F}_N)$ acting in the natural way (by composition with γ) on $\mathcal{M}_N^0$. The intermediate stack $\mathcal{N}^0$ is fixed under the Borel subgroup

$B=\begin{pmatrix}*&*\\0&*\end{pmatrix}\subset GL_2(\mathbf{F}_N)$. We may view φ as either a section of the sheaf $\omega^{\otimes k}$ over the stack $\mathscr{N}^0$, or as a section over $\mathscr{M}_N^0$, invariant under the action of B.

A "formal neighborhood of the cusp ∞" in $\mathscr{N}^0$ is induced from the pair $(\mathrm{Tate}(q)_{/R((q))}, \mu_N)$ while a "formal neighborhood of the (unique) cusp ∞" in $\mathscr{M}_1$ is induced from the Tate curve over $R((q))$ ([24], (1.3)). We have the following commutative diagram:

$$\begin{array}{ccc}\mathrm{Spec}\, R((q)) & \xrightarrow{\iota} & \mathscr{N}^0 \\ \downarrow{\scriptstyle q\mapsto q^N} & & \downarrow{\scriptstyle \beta} \\ \mathrm{Spec}\, R((q)) & \xrightarrow{\iota} & \mathscr{M}_1^0\end{array}$$

where we can check that the left-hand vertical map *is* given by $q\mapsto q^N$ as follows: By ([24], (1.11), p. 91) we have $\mathrm{Tate}(q)/\mu_N=\mathrm{Tate}(q^N)$, and $\mathrm{Tate}(q^N)$ is induced from $\mathrm{Tate}(q)$ by extension of scalars $R((q))\to R((q))$; $q\mapsto q^N$.

By the above discussion we may give the following geometric interpretation to our hypothesis concerning φ: the restriction $\tilde{\varphi}$ of φ to $\mathrm{Spec}\, R((q))$ *descends* to a section of $\omega^{\otimes k}$ over the "formal neighborhood of the cusp" in $\mathscr{M}_1^0$.

We now consider the cusps of $\mathscr{M}_N$, and for this we make the base change from R to $R_0=R[\zeta_N]$. Note that the map $\mathscr{M}_N\to\mathscr{N}$ is *étale* over the cusp ∞. Let:

$$U=\pm\begin{pmatrix}1&0\\*&1\end{pmatrix}\subset GL(2,\mathbf{F}_N)$$

$$A=\begin{pmatrix}*&0\\0&1\end{pmatrix}\subset GL(2,\mathbf{F}_N).$$

The inertia groups in $GL_2(\mathbf{F}_N)$ of the cusps in $\mathscr{M}_N$ consist in the *conjugates* of the group U (cf. [9] Cor. (2.5) of VII). From the definition of the map α one sees that the inertia groups of those cusps lying above $\infty\in\mathscr{N}$ consist in those N conjugates of U which do *not* lie in B. Let $\overline{\infty}$ be a cusp in $\mathscr{M}_N$, lying over ∞, whose inertia group (for the Galois extension $\mathscr{M}_N\to\mathscr{M}_1$) is U. Since the group A normalizes U, it follows that, for all $a\in A$, $a.\overline{\infty}$ also has U as inertia group.

Viewing φ as a section of $\omega^{\otimes k}$ over $\mathscr{M}_N^0$, the Fourier expansions $\tilde{\varphi}_{a.\overline{\infty}}$ *descend* to a formal neighborhood of the cusp in $\mathscr{M}_1^0$, and therefore $\tilde{\varphi}_{a.\overline{\infty}}$ is invariant under the action of the inertia group of $a.\overline{\infty}$ (namely U). Thus, for any $u\in U$, $\varphi^u-\varphi$ has *zero* q-expansions at each of the cusps $a.\overline{\infty}$ for $a\in A$. Since the group A operates transitively on the $N-1$ distinct connected components of $\mathscr{M}_N$ we have that $\varphi^u-\varphi$ has zero q-expansion at (at least) one cusp belonging to each of the $N-1$ distinct connected components of the geometric fiber of $\mathscr{M}_N$. Therefore theorem (1.6.1) of [24] applies, giving that $\varphi^u-\varphi=0$. It follows that φ is invariant under *both* B and U. Since B

and U generate $GL_2(\mathbf{F}_N)$, φ descends to a modular form over $\Gamma_0(1)$, defined over $R_0 = R[\zeta_N]$. Since its q-expansion has coefficients in R, [9], VII, th. (3.9) (ii) insures that φ is defined over R.

Proof of lemma (5.10). — Suppose that φ is a *nonzero* holomorphic modular form satisfying the hypotheses of our lemma. Since φ is the reduction modulo N of a modular form of weight 2 over $\Gamma_0(N)$ with integral q-expansion, we use [61], th. 11 (c), and regard φ as the reduction modulo N of a modular form over $SL_2(\mathbf{Z})$, of weight $N+1$. In the terminology of [61], φ is of *filtration* $\leq N+1$, as a modular form over $SL_2(\mathbf{Z})$. Since the filtration of φ is congruent to $N+1$ modulo $N-1$ ([66], th. 2) and since it cannot be 2, the filtration of φ is $N+1$. On the other hand, our hypotheses may be interpreted as saying $\theta\varphi = 0$, where θ is the derivation $q.\frac{d}{dq}$. Since $N \geq 5$, we may apply lemma 1 (a) of [61], which gives an *absurd* equality for the filtration of $\theta\varphi = 0$. Consequently, there are no nonzero modular forms φ satisfying the hypotheses of (5.10).

Corollary **(5.11)**. — *Let* $\tilde{\varphi}(q) = 1 + a_N q^N + a_{2N} a^{2N} + \ldots$ *be a power series in* q^N, *with integral coefficients, beginning with constant term* 1. *Then*:

(i) $\tilde{\varphi}$ *reduced modulo* N *is not a holomorphic modular form* (*for* $\Gamma_0(N)$) *in* $B(\mathbf{F}_N)$ (§ 4).

(ii) *If m is prime to* N, *and* $\tilde{\varphi}$, *reduced modulo m, is a holomorphic modular form* (*in* $\omega^{\otimes 2}$, *over* $\Gamma_0(N)$), *then m divides* 12, *and* $\varphi \equiv 1$ *modulo m.*

Proof. — (i) is a repetition of (5.10), while (ii) follows from (5.9) and (5.6) and (4.10).

We now consider the status of the power series $\delta(q) = \sum_m \sigma'(m) q^m$ (see beginning of § 5), as modular form, when reduced modulo integers *m.*

Proposition **(5.12)**:

(i) *The power series* δ *is not the q-expansion of a holomorphic modular form of weight* 2 *over* $\Gamma_0(N)$, *modulo* N (" *holomorphic modular form* " *in* $B(\mathbf{F}_N)$ (§ 4)).

(ii) *Let m be prime to* N. *The power series* $\delta(q)$ *is the q-expansion of a holomorphic modular form over* $\Gamma_0(N)$ *modulo m* (*in* $\omega^{\otimes 2}$) *if and only if m divides* $\frac{N-1}{2}$ [1].

(iii) *Let m be any integer. The power series* $\delta(q)$ *is the q-expansion of a parabolic modular form if and only if m divides* $n = \text{numerator}\left(\frac{N-1}{12}\right)$.

Proof. — Consider the formula:

$$-e' = (N-1) + 24\,\delta$$

[1] See also KOIKE [26] when m is a prime ≥ 5.

from which it follows that if δ were a modular form modulo N (in $B(\mathbf{F}_N)$) then the constant 1 would be the q-expansion of such a modular form as well. This is not true by (5.11) (i), whence (i).

We shall now prove (ii). But first we need a fact about modular forms (in $\omega^{\otimes 2}$) which is not totally obvious: Let $\tilde{\varphi}$ be a power series in q with integral coefficients. Let a, b be integers. Then $\tilde{\varphi}$ is a holomorphic modular form mod b if and only if $a\tilde{\varphi}$ is a holomorphic modular form mod ab.

To prove this, we invoke the q-expansion principle ([9], VII, (3.9) (ii); [24], (1.6.2)). We view $a.\mathbf{Z}/b$ as submodule of $\mathbf{Z}/ab$ and note that $a\varphi$ has all q-expansion coefficients lying in the above submodule.

Now, suppose that δ is a holomorphic modular form modulo m with $(m, N)=1$. From the formula quoted above, it follows that $N-1$ is (the q-expansion of) a holomorphic modular form, modulo $24m$. By (5.11) (ii) and the fact proved above, if m' is any integer prime to N such that $N-1$ is a holomorphic modular form modulo m', then m' divides $12(N-1)$. It follows that $24m$ divides $12(N-1)$, or m divides $\left(\frac{N-1}{2}\right)$. Conversely, e is a holomorphic modular form (in $\omega^{\otimes 2}$) modulo 12. Therefore $(N-1).e$ is a holomorphic modular form modulo $12(N-1)$. Moreover:

(5.13) $$-e' \equiv (N-1).e + 24\,\delta \quad \text{modulo } 24(N-1),$$

from which it follows that δ is a holomorphic modular form modulo $\left(\frac{N-1}{2}\right)$. This proves (ii).

As for (iii), it suffices to consider integers m which divide $\left(\frac{N-1}{2}\right)$, by (ii). Consider (5.13) as an equation of meromorphic differential forms, and we shall compute the residues of each term appearing in it, at the sections ∞ and 0.

To do this, consider the involution w of $X_0(N)$ induced by the rule:

$$(E, H) \mapsto (E/H, E[N]/H)$$

operating on sections of the moduli stack $\mathcal{N}^0$ and on modular forms (cf. terminology and discussion in proof of lemma (5.9) above; for a discussion of w cf. § 6) below. If φ is a (holomorphic) modular form, defined over R, *of level* 1, and if we denote by φ, again lifting to $\mathcal{N}^0$ defined by the rule $\varphi(E, H)=\varphi(E)$, then the q-expansions of φ and $\varphi.w$ are related by:

$$\tilde{\varphi}.w(q)=\tilde{\varphi}(q^N)$$

as follows from the discussion in the proof of lemma (5.9). Since w interchanges the cuspidal sections ∞ and 0, we have the following

Sublemma. — *Let* $1/N \in R$. *If* φ *is a holomorphic modular form (in* $\omega^{\otimes 2}$*) of level* 1, *defined over* R, *regarded as meromorphic differential, and if the same letter* φ *denotes its lifting to* $M_0(N)_{/R}$ *as above, we have the formula for residues*:

$$\mathrm{Res}_0(\varphi)=N.\mathrm{Res}_\infty(\varphi).$$

Thus:

$$\text{(5.14)}\qquad \begin{aligned} &\mathrm{Res}_\infty((N-1).e) \equiv N-1 \bmod 24(N-1) \\ &\mathrm{Res}_0((N-1).e) \equiv N(N-1) \bmod 24(N-1) \end{aligned} \quad (1).$$

Since e' is an eigenvector for w with eigenvalue -1, we have:

$$\text{(5.15)}\qquad \begin{aligned} &\mathrm{Res}_\infty(-e') = N-1 \\ &\mathrm{Res}_0(-e') = 1-N \end{aligned} \quad (1).$$

Formula (5.15) would also follow from the fact that the *only* poles of e' occur at 0 and ∞.

Combining (5.13), (5.14) and (5.15) we get:

$$\text{(5.16)}\qquad \begin{aligned} &\mathrm{Res}_\infty(\delta) = 0 \quad \text{(as it should)} \\ &\mathrm{Res}_0(\delta) \equiv \frac{1-N^2}{24} \text{ modulo } N-1. \end{aligned}$$

Assertion (iii) then follows from (ii), (5.16), and the following elementary fact: $n = \text{g.c.d.}\left(\frac{N-1}{2}, \frac{1-N^2}{24}\right)$.

6. Hecke operators.

1) *The involution w* (induced by $(z \mapsto -1/Nz)$ on the upper half-plane).

This is defined on $M_0(N)_{/\mathbf{Z}[1/N]}$ by the rule $(E, H) \mapsto (E/H, E[N]/H)$; it extends to an involution of $M_0(N)_{/\mathbf{Z}}$ (by [9], IV, (3.19)), and of $X_0(N)_{/\mathbf{Z}}$.

We denote this involution (as well as the involutions induced by it on the moduli schemes $M_0(N.N')$, where N and N' are relatively prime) by w_N, or by w, if no confusion can arise. In the terminology of [9], IV, (3.16), w is induced by conjugation of $\Gamma_0(N)$ by the matrix $g = \begin{pmatrix} 0 & 1 \\ N & 0 \end{pmatrix}$. It *interchanges* the cuspidal sections ∞ and 0.

By " transport of structure " (*i.e.* functoriality of the sheaf of regular differentials) the involution w induces an involution on the space of regular differentials (on $B^0(R)$) and also on B(R). Care should be taken to distinguish this involution w (which is indeed the " classical " one) from the mapping on *modular forms in* $\omega^{\otimes 2}$ defined by Deligne and Rapoport ([9], VII, (3.18)). Referring to their w by the bold letter $\mathbf{w}$, one can show that for a modular form in $\omega^{\otimes 2}$ over $\mathbf{Q}$, $\mathbf{w}\varphi = N.w\varphi$. Our mapping w does not necessarily " preserve " A(R).

If $f \in H^0(M_0(N)_{/\mathbf{Z}}, \Omega)$ has q-expansion $\tilde{f} = \sum_m a_m q^m$, the q-expansion of $w.f$ is given by $\widetilde{w.f} = -\sum_m a_{N.m} q^m$ ([61], (2.1), and (3.3), th. 11 (a)).

2) T_ℓ *for prime numbers* $\ell \neq N$.

---

(1) In these formulas e and e' are regarded as *meromorphic differentials*.

These are correspondences determined by the diagram of morphisms:

(*)
$$\begin{array}{ccc} & M_0(N.\ell) & \\ {\scriptstyle c}\swarrow & & \searrow{\scriptstyle c.w_\ell} \\ M_0(N) & \xrightarrow[T_\ell]{} & M_0(N) \end{array}$$

where c, on the moduli stack, is determined by the rule: $(E, H_N, H_\ell) \mapsto (E, H_N)$. Here $H_N \subset E$ is a subgroup scheme of order N, $H_\ell \subset E$ of order ℓ. Compare [9], VI, (6.11). The morphisms c, cw_ℓ are finite *(loc. cit.)* (1).

If $x = j(E_{/K}, H_N)$ is a point on the curve $X_0(N)$ with values in a field K, then $T_\ell x$ is the divisor:

(6.1) $$\sum_H j(E/H, (H_N + H)/H)$$

where the summation is taken over all cyclic subgroups H of order ℓ of E, defined over $\bar{K}$.

Define morphisms:

(a) $$c^* : H^1(M_0(N)_{/\mathbf{Z}}, \mathcal{O}_{M_0(N)}) \to H^1(M_0(N.\ell)_{/\mathbf{Z}}, \mathcal{O}_{M_0(N\ell)})$$

(b) $$c^* : H^0(M_0(N)_{/\mathbf{Z}}, \Omega) \to H^0(M_0(N.\ell)_{/\mathbf{Z}}, \Omega)$$

as follows: *(a)* is induced from the natural map:

$$\mathcal{O}_{M_0(N)} \to c_* \mathcal{O}_{M_0(N.\ell)}.$$

As for *(b)*, let U denote the open subscheme of $M_0(N.\ell)$ which is the complement of the supersingular points of characteristics N and ℓ (the *smooth* locus of $M_0(N.\ell) \to \mathrm{Spec}(\mathbf{Z})$) and let V be the image of U under c. The restriction of Ω to U (resp. to V) is $\Omega^1_{U/S}$ (resp. $\Omega^1_{V/S}$). One has the natural map:

$$\Omega^1_{V/S} \to c_* \Omega^1_{U/S}$$

which induces a morphism $c^* : H^0(V, \Omega) \to H^0(U, \Omega)$. But since Ω is an invertible sheaf on $M_0(N.\ell)$ and the complement of U in $M_0(N.\ell)$ consists in a finite set of points of codimension two, whose local rings are Cohen-Macaulay, we have:

$$H^0(U, \Omega) = H^0(M_0(N.\ell), \Omega)$$

whence the mapping in *(b)* above.

Applying the Grothendieck duality isomorphism $^\vee$ $((3.3)+(3.2))$ to *(a)* and *(b)*, we obtain morphisms:

(a$^\vee$) $$c_* = (c^*)^\vee : H^0(M_0(N.\ell)_{/\mathbf{Z}}, \Omega) \to H^0(M_0(N), \Omega)$$

(b$^\vee$) $$c_* = (c^*)^\vee : H^1(M_0(N.\ell)_{/\mathbf{Z}}, \mathcal{O}_{M_0(N.\ell)}) \to H^1(M_0(N)_{/\mathbf{Z}}, \mathcal{O}_{M_0(N)}).$$

---

(1) They are not necessarily flat. To determine the (finite) set of points at which they are nonflat is an easy exercise, using [62], IV, Prop. 22; [9], V, (6.9).

We now define the endomorphism T_ℓ on $H^0(M_0(N)_{/\mathbf{Z}}, \Omega)$ and on:

$$H^1(M_0(N)_{/\mathbf{Z}}, \mathcal{O}_{M_0(N)})$$

by the formula:

$$T_\ell = c_*.(cw_\ell)^* = (cw_\ell)_*.c^*.$$

From the definition one sees that the action of T_ℓ on $H^1(M_0(N), \mathcal{O}_{M_0(N)})$ and on $H^0(M_0(N), \Omega)$ are adjoint with respect to Grothendieck duality. The correspondence T_ℓ also induces endomorphisms of:

(i) The Hodge filtration on 1-dimensional de Rham cohomology:

$$0 \to H^0(X_0(N)_{/\mathbf{Z}[1/N.\ell]}, \Omega^1) \to H^1_{DR}(X_0(N)_{/\mathbf{Z}[1/N.\ell]}) \to H^1(X_0(N)_{/\mathbf{Z}[1/N.\ell]}, \mathcal{O}_{X_0(N)}) \to 0.$$

(This action is *hermitian* – $(T_\ell x, y) = (x, T_\ell y)$ – with respect to the cup-product self-duality on H^1_{DR} and it exhibits the adjointness of the action of T_ℓ on the two flanking members of the above exact sequence) (1).

(ii) The jacobian of $X_0(N)_{/\mathbf{Q}}$; its Néron model $J_{/\mathbf{Z}}$; the " connected component " of the Néron model $J^0_{/\mathbf{Z}}$; the singular cohomology groups of $X_0(N)_{/\mathbf{C}}$ with coefficients in $\mathbf{Z}$; the p-divisible (Barsotti-Tate) groups $J_{p/\mathbf{Z}[1/N]}$.

The endomorphisms T_ℓ are hermitian with respect to the cup-product self-duality of 1-dimensional singular cohomology of $X_0(N)_{/\mathbf{C}}$ and the auto-duality of the Barsotti-Tate groups $J_{p/\mathbf{Z}[1/N]}$.

The effect of T_ℓ on the q-expansions of elements in $H^0(M_0(N), \Omega)$ may be computed over the base $\mathbf{Q}$ (or $\mathbf{C}$) and one finds (applying (6.1)) the classical formula:

If the q-expansion of f is given by $\tilde{f} = \sum_m a_m q^m$ then:

(6.2) $$\widetilde{T_\ell f} = \sum_m b_m q^m, \quad \text{where} \quad b_m = \ell . a_{m/\ell} + a_{\ell . m}$$

(with the convention that $a_{m/\ell} = 0$ unless $\ell \mid m$).

Consider the action of T_ℓ on the Néron model $J_{/\mathbf{Z}}$ and restrict to characteristic ℓ. The Eichler-Shimura relation on the level of correspondence, (whose proof in [7] works mutatis mutandis for $\Gamma_0(N)$) gives the formula:

Eichler-Shimura:

$$T_\ell = \mathrm{Frob}_\ell + \ell/\mathrm{Frob}_\ell \quad \text{on} \quad J_{/\mathbf{F}_\ell} \ (\ell \nmid N).$$

Here Frob_ℓ is the Frobenius endomorphism of the group scheme $J_{/\mathbf{F}_\ell}$, and ℓ/Frob_ℓ may be regarded as the canonical " Verschiebung " of the group scheme $J_{/\mathbf{F}_\ell}$. It follows that Frob_ℓ satisfies the quadratic *Eichler-Shimura* equation:

$$X^2 - T_\ell . X + \ell = 0$$

in the endomorphism ring of $J_{/\mathbf{F}_\ell}$.

---

(1) Duality for de Rham cohomology is compatible with (indeed: constructed by means of) duality for coherent sheaves (cf. [18]).

Definition. — *By the* Hecke Algebra **T** *we shall mean the subring of* $\mathrm{End}(J_{/\mathbf{Q}})$ *generated by the Hecke operators* T_ℓ $(\ell \nmid N)$ *and by* w.

The algebra **T** operates, by definition, on $J_{/\mathbf{Q}}$. It also operates (via the previously defined actions of T_ℓ and w) on the following list of objects:

$J_{/\mathbf{Z}}$; $J^0_{/\mathbf{Z}}$;
$\mathrm{Pic}^0(X_0(N)_{/\mathbf{Z}}) \cong J^0_{/\mathbf{Z}}$;
$H^1(X_0(N)_{/\mathbf{Z}}, \mathcal{O}_{X_0(N)}) = $ Tan. space $\mathrm{Pic}^0(X_0(N)_{/\mathbf{Z}})$;
$H^0(X_0(N)_{/\mathbf{Z}}, \Omega)$ (which is the dual of the above);
$H^1_{\mathrm{DR}}(X_0(N)_{/\mathbf{Q}})$ (which is the Lie algebra of the universal extension of $J_{/\mathbf{Q}}$ [37]);
$H^1_{\mathrm{sing}}(X_0(N)_{/\mathbf{C}}, \mathbf{Z})$.

Clearly, **T** is a free **Z**-module of finite rank. It is known that $\mathbf{T}\otimes\mathbf{Q}$ is a commutative **Q**-algebra of rank $g = \mathrm{genus}(X_0(N))$, and that it is isomorphic to a product of totally real algebraic number fields:

$$\mathbf{T}\otimes\mathbf{Q} = \prod_{\alpha = 1, \ldots, t} k_\alpha \quad (1). \tag{6.3}$$

(6.4) Say that a **T**-module M (of finite type) is of *rank* r (as opposed to *free* or *locally free of rank* r) if, equivalently:

(a) $M\otimes\mathbf{Q}$ is free over $\mathbf{T}\otimes\mathbf{Q}$ of rank r.

(a') For some, or any, field K of characteristic 0, $M\otimes K$ is free of rank r over $\mathbf{T}\otimes K$.

(b) $M\otimes k_\alpha$ is a vector space of dimension r, over k_α, for $\alpha = 1, \ldots, t$.

(c) M contains a free **T**-module of rank r, of finite index.

Note that if M is a **T**-module of rank r, then the **Z**-dual **T**-module $M^\vee = \mathrm{Hom}(M, \mathbf{Z})$ is again a **T**-module of rank r (2).

Since $H^0(X_0(N)_{/\mathbf{C}}, \Omega^1)$ is known to be a free $\mathbf{T}\otimes\mathbf{C}$ module of rank 1 (as follows from lemma 27 of [2]), one has:

$$H^0(X_0(N)_{/\mathbf{Z}}, \Omega) \quad \text{and} \quad H^1(X_0(N)_{/\mathbf{Z}}, \mathcal{O}_{X_0(N)}) \tag{6.5}$$

are **T**-modules of rank 1.

$H^1_{\mathrm{sing}}(X_0(N)_{/\mathbf{C}}, \mathbf{Z})$ is a **T**-module of rank 2.

---

(1) This follows from lemmas 13, 27 of [2].

(2) It is not at all evident, however, that the operation $\vee$ preserves the category of locally free **T**-modules. This latter assertion is equivalent to saying that **T** is a *Gorenstein ring* (but see §§ 15-17 below).

7. Quotients and completions of the Hecke algebra.

Let m be an integer. Let $J[m]_{/\mathbf{Z}}$ denote the scheme-theoretic kernel of multiplication by m in the Néron model $J_{/\mathbf{Z}}$. Since J is semi-stable (cf. appendix) $J[m]_{/\mathbf{Z}}$ is a quasi-finite flat group scheme, whose restriction to $S'=\operatorname{Spec}\mathbf{Z}[1/N]$ is finite and flat.

Let $\mathfrak{a}\subset\mathbf{T}$ be an ideal containing m. By $J[\mathfrak{a}]_{/\mathbf{Q}}$ we shall mean the kernel of the ideal $\mathfrak{a}$ in the jacobian $J_{/\mathbf{Q}}$. That is:

$$J[\mathfrak{a}]_{/\mathbf{Q}}=\bigcap_{\alpha\in\mathfrak{a}}(\text{kernel of }\alpha\text{ in }J/\mathbf{Q})$$
$$=\bigcap_{\alpha\in\mathfrak{a}}(\text{kernel of }\alpha\text{ in }J[m]/\mathbf{Q}).$$

From the second description it is clear that $J[\mathfrak{a}]_{/\mathbf{Q}}$ is a finite subgroup scheme of $J[m]_{/\mathbf{Q}}$. Now define $J[\mathfrak{a}]_{/\mathbf{Z}}$ to be the Zariski-closure of $J[\mathfrak{a}]_{/\mathbf{Q}}$ in $J_{/\mathbf{Z}}$. It is the subgroup scheme extension of $J[\mathfrak{a}]_{/\mathbf{Q}}$ in $J[m]_{/\mathbf{Z}}$, as in chapter I, § 1; $J[\mathfrak{a}]_{/\mathbf{Z}}$ is a quasi-finite flat group, which is, by construction, a closed subgroup scheme of $J_{/\mathbf{Z}}$, and killed by $\mathfrak{a}$. The quotient $\mathbf{T}/\mathfrak{a}$ operates naturally on $J[\mathfrak{a}]_{/\mathbf{Z}}$.

Caution. — The group scheme $J[\mathfrak{a}]_{/\mathbf{Z}}$ is not necessarily the full scheme-theoretic kernel of $\mathfrak{a}$ in $J_{/\mathbf{Z}}$. This kernel is not necessarily flat over $\mathbf{Z}$.

Fix a prime p. Let $\mathfrak{a}\subset\mathbf{T}$ be any ideal containing p. Let $\mathbf{T}_{\mathfrak{a}}=\varprojlim_m \mathbf{T}/\mathfrak{a}^m$ denote the completion of $\mathbf{T}$ at $\mathfrak{a}$. Denote by $\mathbf{T}_p$ the completion of $\mathbf{T}$ at the ideal generated by p. Thus $\mathbf{T}_p=\mathbf{T}\otimes\mathbf{Z}_p$. Since $\mathbf{T}$ is a finite $\mathbf{Z}$-module, $\mathbf{T}_{\mathfrak{a}}$ is a *direct factor* of the semi-local ring $\mathbf{T}_p$. Write:

(7.1) *(a)* $\mathbf{T}_p=\mathbf{T}_{\mathfrak{a}}\times\mathbf{T}'_{\mathfrak{a}}$

(b) $1=\varepsilon_{\mathfrak{a}}+\varepsilon'_{\mathfrak{a}}$

where $\mathbf{T}'_{\mathfrak{a}}$ is our notation for the factor complementary to $\mathbf{T}_{\mathfrak{a}}$, and (7.1) *(b)* is the associated idempotent decomposition of 1 in $\mathbf{T}_p$.

Form the inductive limits of the quasi-finite group schemes:

(7.2)
$$J_{p/\mathbf{Z}}=\varinjlim_m J[p^m]_{/\mathbf{Z}}$$
$$J_{\mathfrak{a}/\mathbf{Z}}=\varinjlim_m J[\mathfrak{a}^m]_{/\mathbf{Z}}.$$

Thus, $J_{p/\mathbf{Z}}$ is an ind-quasi-finite group scheme, whose restriction to:

$$S'=\operatorname{Spec}(\mathbf{Z}[1/N])$$

is a p-divisible (Barsotti-Tate)group admitting a natural continuous action of $\mathbf{T}_p$. We may use the idempotent decomposition (7.1) to write $J_{\mathfrak{a}}$ as a direct factor of J_p:

(7.3) $$J_p=J_{\mathfrak{a}}\times J'_{\mathfrak{a}}.$$

Restricting to the base S', (7.3) becomes a product decomposition of Barsotti-Tate groups. Moreover, since the action of $\mathbf{T}$ is hermitian with respect to the auto-duality of $J_{p/S'}$, one obtains an induced auto-duality on $J_{\mathfrak{a}/S'}$.

To pass to pro-p-groups, one uses the *Tate construction.* We recall this in the category of modules.

The functor $M \mapsto M \otimes (\mathbf{Q}_p/\mathbf{Z}_p)$ is an equivalence between the categories of free $\mathbf{Z}_p$-modules of rank r, and p-divisible torsion $\mathbf{Z}_p$-modules of *corank* r. The Tate construction $W \mapsto \mathrm{Hom}(\mathbf{Q}_p/\mathbf{Z}_p, W) = \mathcal{T}a(W)$ provides an essential inverse to the above functor.

There is a perfect $\mathbf{Z}_p$-pairing between $\mathcal{T}a(W)$ and the Pontrjagin p-dual of W, $W^* = \mathrm{Hom}(W, \mathbf{Q}_p/\mathbf{Z}_p)$.

The isomorphism $W^* \xrightarrow{\sim} \mathcal{T}a(W)^\vee = \mathrm{Hom}(\mathcal{T}a(W), \mathbf{Z}_p)$ takes $\varphi \in W$ to:

$$\mathcal{T}a(\varphi) : \mathcal{T}a(W) \to \mathcal{T}a(\mathbf{Q}_p/\mathbf{Z}_p) \cong \mathbf{Z}_p.$$

Let $X_0(N)_{\mathbf{C}}$ denote the analytic curve associated to $X_0(N)_{/\mathbf{C}}$, and $J_{\mathbf{C}}$ the complex Lie group associated to $J_{/\mathbf{C}}$. We may identify the singular homology group $H_1(X_0(N)_{\mathbf{C}}, \mathbf{Z})$ with the kernel of the homomorphism of the universal covering group of $J_{\mathbf{C}}$ to $J_{\mathbf{C}}$. By means of this identification, we obtain an isomorphism:

$$\mathbf{(7.4)} \qquad J_p(\mathbf{C}) = H_1(X_0(N)_{\mathbf{C}}, \mathbf{Z}) \otimes \mathbf{Q}_p/\mathbf{Z}_p = H_1(X_0(N)_{\mathbf{C}}, \mathbf{Q}_p/\mathbf{Z}_p)$$

where the left-hand group is the group of $\mathbf{C}$-valued points of J_p. Applying the Tate construction:

$$\mathbf{(7.5)} \qquad \mathcal{T}a(J_p)(\mathbf{C}) = \mathcal{T}a(J_p(\mathbf{C})) = H_1(X_0(N)_{\mathbf{C}}, \mathbf{Z}_p)$$

and this isomorphism is compatible with the action of $\mathbf{T}_p$. Applying the idempotent ε_a to (7.5) gives:

$$\mathbf{(7.6)} \qquad \begin{aligned} \mathcal{T}a(J_a)(\mathbf{C}) = \mathcal{T}a(J_a(\mathbf{C})) &= H_1(X_0(N)_{\mathbf{C}}, \mathbf{Z}_p) \otimes_{\mathbf{T}_p} \mathbf{T}_a \\ &= H_1(X_0(N)_{\mathbf{C}}, \mathbf{Z}) \otimes_{\mathbf{T}} \mathbf{T}_a. \end{aligned}$$

The last equality, together with (7.5) gives:

Lemma **(7.7).** — *Let* K *be an algebraically closed field of characteristic* 0. *Then* $\mathcal{T}a(J_a(K))$ *is of rank* 2 *over* $\mathbf{T}_a$. (That is: $\mathcal{T}a(J_a(K)) \otimes \mathbf{Q}$ is free of rank 2 over $\mathbf{T}_a \otimes \mathbf{Q}$).

8. Modules of rank 1.

If M is a $\mathbf{T}_a$-module of rank 2 (6.4) and there is an exact sequence of $\mathbf{T}_a$-modules (up to torsion):

$$0 \to M_1 \to M \to M_2 \to 0$$

where M_1 and M_2 are $\mathbf{Z}_p$-dual (up to torsion), then they are each of rank 1. We use this elementary assertion three times in this section.

1. *The defect sequence.*

Suppose $p \neq N$. Then J_p is an ind-étale (quasi-finite) group scheme over the base $\mathrm{Spec}(\mathbf{Z}_N)$. Consider the natural imbedding:

$$J_p(\overline{\mathbf{F}}_N) \to J_p(\overline{\mathbf{Q}}_N)$$

which induces an imbedding on Tate constructions. Form the exact sequence:

(8.1) $$0 \to \mathcal{E}a(J_p(\overline{\mathbf{F}}_N)) \to \mathcal{E}a(J_p(\overline{\mathbf{Q}}_N)) \to \Delta \to 0$$

where Δ is the cokernel *(the module of defect)*. The sequence (8.1) is compatible with the action of $\mathbf{T}_p$. By the " théorème d'orthogonalité " (th. (2.4) of exp. IX, SGA 7), the *toric* part of $\mathcal{E}a(J_p(\overline{\mathbf{Q}}_N))$ is orthogonal to itself. On the other hand, the fiber $J_{/\overline{\mathbf{F}}_N}$ is isomorphic to $\mathbf{G}_m^g$ where g is the genus of $X_0(N)$ (cf. appendix). It follows by computing ranks over $\mathbf{Z}_p$ that the self-duality of $\mathcal{E}a(J_p(\overline{\mathbf{Q}}_N))$ induces, up to torsion, a $\mathbf{Z}_p$-duality between $\mathcal{E}a(J_p(\overline{\mathbf{F}}_N))$ and Δ. Applying ε_α (7.1) *(b)* to (8.1) yields an exact sequence:

(8.2) $$0 \to \mathcal{E}a(J_\alpha(\overline{\mathbf{F}}_N)) \to \mathcal{E}a(J_\alpha(\overline{\mathbf{Q}}_N)) \to \Delta_\alpha \to 0$$

where $\Delta_\alpha = \Delta \otimes_{\mathbf{T}_p} \mathbf{T}_\alpha$, and where Δ_α is dual to $\mathcal{E}a(J_\alpha(\overline{\mathbf{F}}_N))$, up to torsion. Applying lemma (7.7), we have:

Proposition **(8.3)**. — $\mathcal{E}a(J_\alpha(\overline{\mathbf{F}}_N))$ *and* Δ_α *are* $\mathbf{T}_\alpha$*-modules of rank* 1.

2. *Etale and Multiplicative type parts, in the ordinary case.*

Now suppose that $p \neq N$, and J_α is an *ordinary* Barsotti-Tate group. This means that over $\mathrm{Spec}(\mathbf{Z}_p)$ it admits a filtration:

(8.4) $$0 \to J_\alpha^{\text{mult. type}} \to J_\alpha \to J_\alpha^{\text{étale}} \to 0$$

where $J_\alpha^{\text{étale}}$ is an étale Barsotti-Tate group (the *étale part* of J_α) and $J_\alpha^{\text{mult. type}}$ is the connected component of J_α, and is a group of *multiplicative type* (the dual of an étale Barsotti-Tate group). The self-duality of J_α induces a duality between $J_\alpha^{\text{mult. type}}$ and $J_\alpha^{\text{étale}}$. Applying $\mathcal{E}a$ to (8.4), and using lemma (7.7) one obtains:

Proposition **(8.5)**. — $\mathcal{E}a(J_\alpha^{\text{mult. type}}(\overline{\mathbf{Q}}_p))$ *and* $\mathcal{E}a(J_\alpha^{\text{étale}}(\overline{\mathbf{Q}}_p))$ *are* $\mathbf{T}_\alpha$*-modules of rank* 1.

3. *Eigenspaces for complex conjugation.*

Complex conjugation σ on the topological space $X_0(N)_{\mathbf{C}}$ commutes with cup-product and induces multiplication by -1 on H^2. Consequently the cup-product pairing induces (up to torsion) a duality between the $+1$-eigenspace of σ operating on $H^1(X_0(N)_{\mathbf{C}}, \mathbf{Z})$ and the -1-eigenspace. Using (6.5) it follows that these eigenspaces are $\mathbf{T}$-modules of rank 1.

9. Multiplicity one.

Let R be any commutative ring. Consider operators $T_\ell : R[[q]] \to R[[q]]$ ($\ell \neq N$) and $U : R[[q]] \to R[[q]]$ defined purely formally by the appropriate equations:

If $f = \sum_m a_m q^m$, then:

(9.1) $$T_\ell f = \sum_m a_{\ell m} q^m + \ell \cdot \sum_m a_m q^{\ell \cdot m} \ (\ell \neq N), \quad \text{and} \quad Uf = \sum_m a_{N \cdot m} q^m.$$

Let $\mathscr{L}$ be any set of prime numbers, and $\mathscr{L}'$ the set of all positive *integers* which are not divisible by any member of $\mathscr{L}$ (so 1 is always in $\mathscr{L}'$). Let :

$$f = a_1 q + a_2 q^2 + \ldots \in \mathrm{R}[[q]]$$

be a power series with no constant term, which is an eigenvector for T_ℓ (all $\ell \in \mathscr{L}$, $\ell \neq \mathrm{N}$) with eigenvalue $c_\ell \in \mathrm{R}$, and, if $\mathrm{N} \in \mathscr{L}$, an eigenvector for U, with eigenvalue $c_\mathrm{N} \in \mathrm{R}$.

The recursive relations:

$$a_{\ell . m} = c_\ell . a_m + \ell . a_{m/\ell} \qquad \ell \in \mathscr{L}, \quad \ell \neq \mathrm{N}$$
$$a_{\mathrm{N} . m} = c_\mathrm{N} . a_m \qquad \text{if} \quad \mathrm{N} \in \mathscr{L}$$

show immediately that f is *determined* by the eigenvalues c_ℓ for $\ell \in \mathscr{L}$, and its coefficients a_m for $m \in \mathscr{L}'$ (1).

In particular, given $c_\ell \in \mathrm{R}$ for *all* prime numbers ℓ, there is a unique power series $f = 1 . q + a_2 q^2 + \ldots$ in $\mathrm{R}[[q]]$ such that $\mathrm{T}_\ell . f = c_\ell . f$ for all $\ell \neq \mathrm{N}$, and $\mathrm{U} . f = c_\mathrm{N} . f$. Moreover, any eigenvector in $\mathrm{R}[[q]]$ possessing the same eigenvalues for all these operators must be a scalar multiple of f. Call f the *generating eigenvector* (for the eigenvalues $\{c_\ell\}$.)

Proposition **(9.2).** — *Let* R *and* $\mathrm{B}^0(\mathrm{R})$ *be as in* § 4. *Let elements* $c_\ell \in \mathrm{R}$ *be given, for each prime number* ℓ.

If $\beta \in \mathrm{B}^0(\mathrm{R})$ *is a parabolic modular form such that*:

$$(*) \qquad \begin{aligned} &\mathrm{T}_\ell . \beta = c_\ell . \beta \quad \ell \neq \mathrm{N} \\ &\mathrm{U} . \beta = c_\mathrm{N} . \beta \end{aligned}$$

then the q-expansion of β *is a scalar multiple of the generating eigenvector f. The* R*-submodule of* $\mathrm{B}^0(\mathrm{R})$ *consisting in all elements which satisfy* (*) *is a submodule of a free* R*-module of rank* 1.

Now let $\mathfrak{M} \subset \mathbf{T}$ be a maximal ideal, with $k_\mathfrak{M}$ as residue field, of characteristic p. Let $\mathrm{B}^0(\mathbf{F}_p)[\mathfrak{M}]$ denote the *kernel* of the ideal $\mathfrak{M}$. This may be viewed, in a natural way, as a $k_\mathfrak{M}$-vector space.

Proposition **(9.3).** — $\mathrm{B}^0(\mathbf{F}_p)[\mathfrak{M}]$ *is of dimension* 1 *over* $k_\mathfrak{M}$.

Proof. — Let $\mathrm{R} = k_\mathfrak{M}$, or any *field* of characteristic p, which is large enough. Let M denote the $k_\mathfrak{M}$-vector space $\mathrm{B}^0(\mathbf{F}_p)[\mathfrak{M}]$. Clearly $\mathrm{M} \neq 0$, since $\mathbf{T}$ operates faithfully on $\mathrm{B}^0(\mathbf{Z})$. Since:

$$\mathrm{M} \otimes_{\mathbf{F}_p} \mathrm{R} \subset \mathrm{B}^0(\mathrm{R})$$

---

(1) A (perhaps too) succinct way of expressing this determination is by the use of *formal Dirichlet series with coefficients in* R. Once one defines the evident rules of manipulation of these formal Dirichlet series, one has:

$$\sum_m a_m . m^{-s} = \Big(\sum_{m \in \mathscr{L}'} a_m . m^{-s} \Big) . \prod_{\ell \in \mathscr{L}} \mathrm{D}_\ell$$

where: $\mathrm{D}_\ell = (1 - c_\ell . \ell^{-s} + \ell^{1-2s})^{-1}$ if $\ell \neq \mathrm{N}$, and $\mathrm{D}_\mathrm{N} = (1 - c_\mathrm{N} . \mathrm{N}^{-s})^{-1}$.

the proposition will follow, if we show that $B^0(R)$ is an R-vector space of dimension less than or equal to $[k_{\mathfrak{M}} : \mathbf{F}_p]$. The action of $\mathbf{T}$ on $B^0(R)$ induces an action of $k_{\mathfrak{M}}$ on $B^0(R)[\mathfrak{M}]$ which commutes with the action of R. Since R contains $k_{\mathfrak{M}}$, $B^0(R)$ possesses an R-basis of $k_{\mathfrak{M}}$-eigenvectors. To each eigenvector in this basis, we may associate a homomorphism $k_{\mathfrak{M}} \to R$ (by passing to eigenvalues). By the previous proposition, no two eigenvectors in this basis are associated to the same homomorphism. The proposition follows.

Proposition **(9.4)**. — $H^1(X_0(N)_{/\mathbf{Z}}, \mathcal{O})$ *is a locally free* $\mathbf{T}$*-module, of rank* 1 (1).

Proof. — Note that if M is a $\mathbf{T}$-module of rank 1, it is *locally free* of rank 1 provided $M/\mathfrak{M}.M$ is a $k_{\mathfrak{M}}$-vector space of dimension 1, for all maximal primes $\mathfrak{M} \subset \mathbf{T}$.

Letting $M = H^1(X_0(N)_{/\mathbf{Z}}, \mathcal{O})$, it is of rank 1 over $\mathbf{T}$, by (6.5). Also:

$$M/\mathfrak{M}.M = H^1(X_0(N)_{/\mathbf{F}_p}, \mathcal{O})/\mathfrak{M}.H^1(X_0(N)_{/\mathbf{F}_p}, \mathcal{O})$$

and the right-hand side of the above equality is isomorphic to the ($\mathbf{F}_p$-vector space) dual of $H^0(X_0(N)_{/\mathbf{F}_p}, \Omega)[\mathfrak{M}] = B^0(\mathbf{F}_p)[\mathfrak{M}]$, which is of dimension 1 by (9.3).

Proposition **(9.5)**. — *The Hecke algebra* $\mathbf{T}$ *is the full ring of endomorphisms of* $J_{/\mathbf{C}}$.

Remark. — This is a mild sharpening of a result of Ribet: that:

$$\mathbf{T} \otimes \mathbf{Q} = \mathrm{End}(J_{/\mathbf{Q}}) \otimes \mathbf{Q} = \mathrm{End}(J_{/\mathbf{C}}) \otimes \mathbf{Q} \quad [58]$$

which is, in fact, used in the proof below.

Proof. — Let $\mathbf{T}' = \mathrm{End}(J_{/\mathbf{C}})$. By Ribet's result, any element of $\mathbf{T}'$ is defined over $\mathbf{Q}$, and therefore acts on the Néron model of $J_{/\mathbf{Q}}$; hence on the connected component $J^0_{/\mathbf{Z}}$ which is $\mathrm{Pic}^0(X_0(N)_{/\mathbf{Z}})$; hence on the tangent space to $\mathrm{Pic}^0(X_0(N)_{/\mathbf{Z}})$, which is $H^1(X_0(N)_{/\mathbf{Z}}, \mathcal{O})$. It also follows by Ribet's result that $\mathbf{T}'$ is a subring of $\mathbf{T} \otimes \mathbf{Q}$ and hence is a commutative ring, and its action commutes with the action of the Hecke algebra $\mathbf{T}$. We get, then, a homomorphism:

$$\mathbf{T}' \to \mathrm{End}_{\mathbf{T}}(H^1(X_0(N)_{/\mathbf{Z}}, \mathcal{O})) = \mathbf{T}''$$

which is injective, since $\mathbf{T} \otimes \mathbf{Q}$ acts faithfully on $H^1(X_0(N)_{/\mathbf{Q}}, \mathcal{O})$. Since $H^1(X_0(N)_{/\mathbf{Z}}, \mathcal{O})$ is a locally free $\mathbf{T}$-module of rank 1 (9.4), $\mathbf{T}'' = \mathbf{T}$. The proposition is established.

Definition. — *The* Eisenstein ideal $\mathfrak{I} \subset \mathbf{T}$ *is the ideal generated by the elements*: $1 + \ell - T_\ell$ (*all* $\ell \neq N$) *and by* $1 + w$.

If R is any ring, any element in $B^0(R)[\mathfrak{I}]$, the kernel of $\mathfrak{I}$ in $B^0(R)$, is an eigenvector for the T_ℓ's and for U, satisfying equation (*) above, where:

$$c_\ell = 1 + \ell \quad \text{if} \quad \ell \neq N$$
$$c_N = 1.$$

(1) It follows that $B^0(\mathbf{Z}) = H^0(X_0(N)_{/\mathbf{Z}}, \Omega)$ is the $\mathbf{Z}$-dual of a locally free $\mathbf{T}$-module of rank 1. The assertion that $B^0(\mathbf{Z})$ is locally free over $\mathbf{T}$ is therefore equivalent to the assertion that $\mathbf{T}$ is a Gorenstein ring (see § 15 below).

In $R[[q]]$, the generating eigenvector for the above package of eigenvalues c_ℓ is the power series δ of (5.1). Consequently, the q-expansion of any element of the R-module $B^0(R)[\mathfrak{I}]$ must be a scalar multiple of δ.

Proposition **(9.6).** — *Let m be any integer divisible by $n = \mathrm{num}\left(\frac{N-1}{12}\right)$. Then $B^0(\mathbf{Z}/m)[\mathfrak{I}]$ is a cyclic group of order n, generated by $(m/n).\delta$.*

Proof. — This follows from the above discussion and (5.12).

Proposition **(9.7).** — $\mathbf{T}/\mathfrak{I} = \mathbf{Z}/n$; *the Eisenstein ideal $\mathfrak{I}$ contains the integer n* [1].

Proof. — We have a natural map $\mathbf{Z} \to \mathbf{T}/\mathfrak{I}$ which is surjective, since, modulo $\mathfrak{I}$, the operators T_ℓ ($\ell \neq N$) and w are all congruent to integers. We cannot have $\mathbf{T}/\mathfrak{I} = \mathbf{Z}$, for then δ would be the q-expansion of a modular form (of weight 2 for $\Gamma_0(N)$) over $\mathbf{C}$, which it is not. Therefore, $\mathbf{T}/\mathfrak{I} = \mathbf{Z}/m$ for some integer m, which must be divisible by n, since $\delta \in B^0(\mathbf{Z}/n)$ is of order n, and is annihilated by $\mathfrak{I}$. We prepare to use the previous proposition. Since:

$$B^0(\mathbf{Z}/m) = H^0(X_0(N)_{/(\mathbf{Z}/m)}, \Omega)$$

is the $\mathbf{Z}/m$-dual of $H^1(X_0(N)_{/(\mathbf{Z}/m)}, \mathcal{O})$ (3.2) we have that $B^0(\mathbf{Z}/m)[\mathfrak{I}]$ is the $\mathbf{Z}/m$-dual of:

$$H^1(X_0(N)_{/(\mathbf{Z}/m)}, \mathcal{O})/\mathfrak{I}.H^1(X_0(N)_{/(\mathbf{Z}/m)}, \mathcal{O}) = H^1(X_0(N)_{/\mathbf{Z}}, \mathcal{O})/\mathfrak{I}.H^1(X_0(N)_{/\mathbf{Z}}, \mathcal{O})$$

where, we have the equality above since $m \in \mathfrak{I}$. By the previous proposition, then, the cokernel of $\mathfrak{I}.H^1(X_0(N)_{/\mathbf{Z}}, \mathcal{O})$ in $H^1(X_0(N)_{/\mathbf{Z}}, \mathcal{O})$ is cyclic of order n. Since (9.4) $H^1(X_0(N)_{/\mathbf{Z}}, \mathcal{O})$ is a locally free $\mathbf{T}$-module of rank 1, it follows that $\mathbf{T}/\mathfrak{I}$ is cyclic of order n. Q.E.D.

Definition. — *A prime ideal $\mathfrak{P} \subset \mathbf{T}$ in the support of the Eisenstein ideal is called an* Eisenstein prime.

The Eisenstein primes $\mathfrak{P}$ are in one-one correspondence with the prime numbers p which divide n by (9.7). If p is such a prime number, then the Eisenstein prime corresponding to p (which is the unique Eisenstein prime whose residue field is of characteristic p) is given by:

$$\mathfrak{P} = (\mathfrak{I}, p).$$

Clearly:

$$\mathbf{T}/\mathfrak{P} = \mathbf{F}_p.$$

One checks easily that $n > 1$ if and only if the genus of $X_0(N)$ is greater than 0. Thus:

Proposition **(9.8).** — *If the genus of $X_0(N)$ is greater than 0, the Eisenstein ideal $\mathfrak{I}$ is a proper ideal in $\mathbf{T}$; there* are *Eisenstein primes.*

---

[1] This vague result is sufficient for our purposes. It appears to be significantly more difficult to give an expression for n in terms of the operators T_ℓ, in $\mathbf{T}$. This would be particularly useful in questions related to § 19 below.

10. The spectrum of T and quotients of J.

As follows from the result of Ribet [58], there are one-to-one correspondences:

$$\begin{array}{ccc} \left\{\begin{array}{c}\text{isogeny classes of}\\ \mathbf{C}\text{-simple}\\ \text{abelian variety}\\ \text{factors of } J_{/\mathbf{C}}\end{array}\right\} & \longleftrightarrow & \left\{\begin{array}{c}\text{isogeny classes of}\\ \mathbf{Q}\text{-simple}\\ \text{abelian variety}\\ \text{factors of } J_{/\mathbf{Q}}\end{array}\right\} \\ \updownarrow & & \updownarrow \\ \left\{\begin{array}{c}\text{fields } k_\alpha \text{ occurring}\\ \text{in the product de-}\\ \text{composition (6.3)}\\ \text{of } \mathbf{T}\otimes\mathbf{Q}\end{array}\right\} & \longleftrightarrow & \left\{\begin{array}{c}\text{irreducible}\\ \text{components}\\ \text{of Spec } \mathbf{T}\end{array}\right\} \end{array} \tag{10.1}$$

Define $J_+=(1+w).J\subset J$; $J_-=(1-w).J\subset J$. These are sub-abelian varieties, defined over $\mathbf{Q}$. Form the quotients indicated in the diagram below:

$$\begin{array}{ccccccccc} & & & & 0 & & & & \\ & & & & \downarrow & & & & \\ & & & & J_+ & & & & \\ & & & & \downarrow & \searrow & & & \\ 0 & \to & J_- & \to & J & \to & J^+ & \to & 0 \\ & & & \searrow & \downarrow & & & & \\ & & & & J_- & & & & \\ & & & & \downarrow & & & & \\ & & & & 0 & & & & \end{array} \tag{10.2}$$

Thus J^+, J^- are quotients of J on which w acts as $+1$, and -1 respectively. We let $J^{\pm}_{/\mathbf{Z}}$ denote the Néron model of $J^{\pm}_{/\mathbf{Q}}$ over the base $\mathbf{Z}$. By the criterion of Néron-Ogg-Shafarevitch, $J^{\pm}_{/\mathbf{Z}[1/N]}$ is an abelian scheme, as are $J_{\pm/\mathbf{Z}[1/N]}$.

The abelian variety $J_{+/\mathbf{Q}}$ can be identified with the jacobian of the quotient curve $X^+=X_0(N)/w$. One sees this as follows: since the map $X_0(N)\to X^+$ is ramified (w has fixed points), the induced map on Pic^0 is injective and identifies the jacobian of X^+ with the connected component of the identity in the $+$-eigenspace of w in J. But the diagram (10.2) identifies $(1+w).J=J_+$ with this same connected component.

To any ideal $\mathfrak{a}\subset\mathbf{T}$ we may associate an abelian variety $J^{(\mathfrak{a})}_{/\mathbf{Q}}$ which is a quotient of $J_{/\mathbf{Q}}$, whose $\mathbf{C}$-simple factors are in one to one correspondence under (10.1) with those irreducible components of Spec $\mathbf{T}$ which *meet* the support of the ideal $\mathfrak{a}$. To define $J^{(\mathfrak{a})}$, let $\gamma_\mathfrak{a}\subset\mathbf{T}$ be the kernel of $\mathbf{T}\to\mathbf{T}_\mathfrak{a}=\varprojlim_m \mathbf{T}/\mathfrak{a}^m$; let $\gamma_\mathfrak{a}.J\subset J$ be the sub-abelian variety (defined over $\mathbf{Q}$) generated by the images $\alpha.J$ for $\alpha\in\gamma_\mathfrak{a}$. Take $J^{(\mathfrak{a})}_{/\mathbf{Q}}$ to be the quotient abelian variety:

$$0\to\gamma_\mathfrak{a}.J\to J\to J^{(\mathfrak{a})}\to 0. \tag{10.3}$$

Let $J^{(\mathfrak{a})}_{/\mathbf{Z}}$ denote the Néron model of $J^{(\mathfrak{a})}_{/\mathbf{Q}}$ over the base $\mathbf{Z}$. By the criterion of Néron-Ogg-Shafarevitch one has that $J^{(\mathfrak{a})}_{/\mathbf{Z}[1/N]}$ is an abelian scheme.

Definitions **(10.4)**:

1) *If* $\mathfrak{a}=\mathfrak{I}$, *the Eisenstein ideal, call* $J^{(\mathfrak{a})}$ *the* Eisenstein quotient *of* J, *and denote it* $\tilde{J}$.

2) *If* $\mathfrak{a}=\mathfrak{P}$, *the Eisenstein ideal at p, call* $J^{(\mathfrak{a})}$ *the p*-Eisenstein quotient *and denote it* $\tilde{J}^{(p)}$.

Note that, for any p, the p-Eisenstein quotient is a quotient of the Eisenstein quotient. Conversely, any $\mathbf{C}$-simple factor of $\tilde{J}$ is a factor of $\tilde{J}^{(p)}$ for some prime p dividing n.

It is also true (but not at all evident when n is even; cf. (17.10) below) that $\tilde{J}$ is a quotient of J^-.

Definitions **(10.5)**:

$$g=\dim(J_{/\mathbf{Q}})$$
$$g^{\pm}=\dim(J^{\pm}_{/\mathbf{Q}})=\dim(J_{\pm/\mathbf{Q}})$$
$$\tilde{g}=\dim(\tilde{J}_{/\mathbf{Q}})$$
$$\tilde{g}^{(p)}=\dim(\tilde{J}^{(p)}_{/\mathbf{Q}}).$$

So $g=g^+ + g^-$, and $g^+=\text{genus}(X^+)$. The Hurwitz formula computed for the map $X_0(N)\to X^+$ yields the well known relation: $2(g^- - g^+)=h-2$, where h is the number of fixed points of w.

Proposition **(10.6)**. — *The scheme* Spec $\mathbf{T}$ *is connected.*

Proof. — Suppose not. It would follow that $J_{/\mathbf{C}}$ could be expressed as a nontrivial *direct* product $J_{/\mathbf{C}}=A\times B$. Let us show that the principal polarization $\lambda : J \xrightarrow[\approx]{} \hat{J}$ ($\hat{}$ denotes the dual abelian variety and λ is the θ-polarization ([43], chapter 6; [44])) induces principal polarizations $\lambda_A : A \xrightarrow[\approx]{} \hat{A}$ and $\lambda_B : B \xrightarrow[\approx]{} \hat{B}$. By Ribet's theorem [58], since J decomposes *(up to isogeny)* into a product of simple factors, each occurring with multiplicity one, the simple factors of A are non-isogenous to simple factors of B, and consequently there are no nontrivial homomorphisms from A to $\hat{B}$ and from B to $\hat{A}$. Our assertion follows. But a jacobian (taken with its natural principal polarization) cannot decompose as a nontrivial direct product of principally polarized abelian varieties. This follows from the irreducibility of its θ-divisor.

Remark. — When $g^+>0$, the above proposition insures the existence of " primes of fusion " (see introduction) relating J^+ to J^-. It would be interesting to understand these primes.

11. The cuspidal and Shimura subgroups.

Let c be the linear equivalence class of the divisor $(0)-(\infty)$ in $J(\mathbf{Q})$.

Proposition **(11.1)**. — *The element* $c\in J(\mathbf{Q})$ *is annihilated by the Eisenstein ideal* $\mathfrak{I}$. *It is of order n.*

Proof. — Since the correspondence T_ℓ ($\ell \neq N$) takes the cusp (0) to $(1+\ell).(0)$ and (∞) to $(1+\ell).(\infty)$, one has:

$$T_\ell . c = (1+\ell).c \quad \text{for all} \quad \ell \neq N.$$

Since w interchanges the cusps 0 and ∞, one has:

$$(1+w).c = 0.$$

It follows that $\mathfrak{I}.c = 0$. From proposition we conclude that the order of c divides n. But since (Appendix A.1) the specialization of c to the Néron fibre $J_{/\mathbf{F}_N}$ generates the cyclic group of connected components, which is of order n, it follows that the order of c must also be divisible by n. Q.E.D.

Remark. — The fact that order$(c) = n$ was proved originally by Ogg [36]. He shows that the order of c divides n by exhibiting a function f on $X_0(N)$ whose divisor is $n.(0) - n.(\infty)$. Namely, if ν is the g.c.d. of $N-1$ and 12:

$$\textbf{(11.2)} \qquad f(z) = \left(\frac{\Delta(z)}{\Delta(Nz)}\right)^{1/\nu} = q^n \prod_{m=1}^{\infty} (1-q^{mN})^{-24/\nu} . (1-q^m)^{24/\nu}$$

can be shown to be invariant under $\Gamma_0(N)$, and clearly has the indicated divisor.

Let C denote the subgroup of $J(\mathbf{Q})$ generated by c. Thus, C is a cyclic group of order n, with a distinguished generator. Denote by $C_{/\mathbf{Z}}$ the finite flat subgroup scheme of $J_{/\mathbf{Z}}$ generated by $C \subset J(\mathbf{Q})$. Let $\overline{C}$ = the $\mathbf{F}_N$-valued points of $C_{/\mathbf{Z}}$ (" the specialization " of C to $J_{/\mathbf{F}_N}$). By the appendix, one has that $\overline{C}$ is, again, of order n (the specialization map $C \to \overline{C}$ is an *isomorphism*) and:

$$\textbf{(11.3)} \qquad J_{/\mathbf{F}_N} = J^0_{/\mathbf{F}_N} \times \overline{C}$$

where $J^0_{/\mathbf{F}_N}$ is the connected component of the identity.

The retraction of $J(\mathbf{Q})$ *to* C. — If $x \in J(\mathbf{Q})$, denote the section over Spec $\mathbf{Z}$ induced by x in $J_{/\mathbf{Z}}$ by the same letter.

Let $x_{/\mathbf{F}_N}$ denote the restriction of this section to an $\mathbf{F}_N$-valued section of $J_{/\mathbf{F}_N}$. Let $\bar{x}$ be the image of $x_{/\mathbf{F}_N}$, under projection, to $\overline{C}$, using the product decomposition (11.3). Let $\rho(x) \in C$ denote the unique element of C which maps to $\bar{x} \in \overline{C}$, under the " specialization map " described above. If $M = J(\mathbf{Q})$ (the *Mordell-Weil group* of J), we have just described a retraction $\rho : M \to C \subset M$, giving a product decomposition.

$$\textbf{(11.4)} \qquad M = M^0 \times C$$

where ρ is projection to the second factor; projection to $M^0 = \ker \rho$ is given by $x \mapsto x - \rho(x)$.

The Shimura subgroup. — The Shimura covering (2.3):

$$\textbf{(11.5)} \qquad X_2(N)_{/S'} \to X_0(N)_{/S'}$$

is the maximal étale extension intermediate to $X_1(N) \to X_0(N)$ and is a finite, étale, Galois extension, whose covering group U is the (unique) quotient group of $(\mathbf{Z}/N)^*$

which is (cyclic) of order n. Applying Pic^0 to the morphism (11.5), we obtain a morphism $J_{/S'} \to \mathrm{Pic}^0 X_2(N)_{/S'}$ whose group scheme kernel we denote $\Sigma_{/S'}$.

Definition. — *The* Shimura subgroup $\Sigma_{/S} \subset J_{/S}$ *is the group scheme extension* (i.e. *Zariski closure*) *of* $\Sigma_{/S'}$ *in* $J_{/S}$.

Let $U^*_{/S} = \mathscr{H}om_S(U, \mu_N)$ be the Cartier dual of U (where U is viewed as constant group scheme over S).

Proposition (**11.6**). — *There is a natural isomorphism* $U^*_{/S} \cong \Sigma_{/S}$. *The Shimura subgroup is a* μ*-type group* (*chapter* I, § 3) *over* S; *in particular it is finite and flat.*

Proof. — We establish this first *over the base* S'.

Consider the Hochschild-Serre Spectral sequence (for the étale topology ([1], III (4.7))) associated to the (finite étale Galois) Shimura covering $X_2(N)_{/T} \to X_0(N)_{/T}$ and the sheaf $\mathbf{G}_m$ where we have made the base change to an (arbitrary) S'-scheme T. We obtain the exact sequence:

$$0 \to H^1(U, \mathbf{G}_m(T)) \xrightarrow[i]{} H^1(X_0(N)_{/T}, \mathbf{G}_m) \to H^1(X_2(N)_{/T}, \mathbf{G}_m).$$

Passing to associated sheaves, the morphism i induces an isomorphism, $U^*_{/S'} \xrightarrow{i} \Sigma_{/S'}$. Since U^* is a finite *étale* group scheme over the base S', this isomorphism *extends* to a homomorphism $U^*_{/S} \xrightarrow{i} \Sigma_{/S}$ (by the universal property of the Néron model). It follows that $\Sigma_{/S}$ is a finite flat group scheme. Restricting to the base S', one has that the morphism i is a homomorphism of locally constant groups, which is an isomorphism on generic fibers. Hence i is an *isomorphism* over S'; hence i is an isomorphism over S.

Proposition (**11.7**). — *The Shimura subgroup* Σ *is annihilated by the Eisenstein ideal* $\mathfrak{I}$.

Proof. — We must show that w acts as -1 on Σ, and T_ℓ acts as $1+\ell$ for $\ell \neq N$. As for the action of w, note that $\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$ induces an involution w' on $X_1(N)$ which projects to the involution w on $X_0(N)$. If $\alpha \in \Gamma_0(N)$, one computes conjugation by w', and obtains: $w' \alpha w' \equiv \alpha^{-1} \bmod \Gamma_1(N)$, which yields what we wish.

The operators T_ℓ " act " as well on $X_1(N)$, by the formula:

$$T_\ell : (z) \mapsto (\ell . z) + \sum_{j=0}^{\ell-1} \left(\frac{z+j}{\ell}\right).$$

In the above formula, as in the rest of this proof, we view the modular curves $X_i(N)$ $(i = 1, 2, 0)$ as analytic manifolds, parametrized by the extended upper half-plane.

If α, β are points in the extended uper half-plane, let $\{\alpha, \beta\}$ denote the (relative) homotopy class of paths in the extended upper half-plane beginning at α and ending at β. Recall Ogg's convenient terminology for the cusps of $\Gamma(N)$: Let:

$$\left(\tfrac{a}{b}\right) = \{p/q \in \mathbf{P}^1(\mathbf{Q}) \mid p \equiv a \bmod N,\ q \equiv b \bmod N;\ (p, q) = 1\}.$$

With this notation, $\binom{a}{b}$ is an equivalence class of $\mathbf{P}^1(\mathbf{Q})$ mod $\Gamma(N)$. Therefore it gives rise to a well-defined cusp of $X_i(N)$ $(i=1, 2, 0)$. One shows $\binom{a}{b} \equiv \binom{0}{b} \bmod \Gamma_1(N)$, provided $(b, N)=1$.

If $\pi \in \{\alpha, \beta\}$ is a path in the extended upper half-plane, let $\gamma(\pi) \in U$ be the (unique) element of U which maps the image of α in $X_2(N)$ to the image of β in $X_2(N)$.

Let π_b be a path in $\{\binom{0}{1}, \binom{0}{b}\}$, for b an integer relatively prime to N. Then one checks that $\gamma(\pi_b)$ is the image of b^{-1} in U, while $\gamma(T_\ell . \pi_b)$ is the $(1+\ell)$-th power of this image, as follows from the formula:

$$T_\ell\{\tbinom{0}{1}, \tbinom{0}{b}\} = \{\tbinom{0}{1}, \tbinom{0}{b}\} + \sum_{j=0}^{\ell=1} \{\tbinom{j}{\ell}, \tbinom{j}{\ell . b}\}$$

The proposition follows.

The Shimura subgroup over the base $\mathbf{F}_N$. — Note that $\Sigma(\mathbf{F}_N) = \mathrm{Hom}(U, \mu_n(\mathbf{F}_N))$, and that there is a *natural* generator of this group. Namely:

$$\begin{array}{ccc} (\mathbf{Z}/N)^* = \mathbf{F}_N^* & \longrightarrow & \mathbf{F}_N^* \\ \downarrow & & \uparrow \\ U & \xrightarrow[s]{} & \mu_n(\mathbf{F}_N) \end{array}$$

where the unlabeled horizontal map is raising to the ν-th power $(\nu = (N-1, 12))$.

The natural projection $J(\mathbf{F}_N) = J^0(\mathbf{F}_N) \times \bar{C} \to \bar{C}$ induces a homomorphism:

(11.8) $\qquad \Sigma(\mathbf{F}_N) \to \bar{C}$

which sends the canonical generator s to some multiple ξ of the canonical generator $\bar{c} \in \bar{C}$. Thus ξ is a well-defined integer modulo n.

Question. — *What is* ξ?

Proposition **(11.9)**. — *The homomorphism* (11.8) *is an isomorphism. The scheme-theoretic intersection* $\Sigma_{/\mathbf{F}_N} \cap J^0_{/\mathbf{F}_N}$ *is the trivial group scheme over* $\mathbf{F}_N$. *The integer (modulo n)* ξ *is relatively prime to n* [1].

Proof. — The three assertions of the proposition are equivalent. We prove them by showing that:

(11.10) $\qquad \mathrm{Pic}^0(X_0(N)_{/\mathbf{F}_N}) \to \mathrm{Pic}^0(X_1(N)_{/\mathbf{F}_N})$

is *injective*. For this, we may identify $\mathrm{Pic}^0(X_0(N)_{/\mathbf{F}_N})$ as group-scheme over $\bar{\mathbf{F}}_N$ with the $\mathbf{G}_m$-dual of the singular one-dimensional homology group of the topological graph (Appendix, § 3) associated to $X_0(N)_{/\bar{\mathbf{F}}_N}$ (homology with $\mathbf{Z}$ coefficients).

---

[1] In the light of this, it is hard to imagine that ξ is anything other than ± 1. We have not, however, succeeded in answering our question.

By inspecting (diagram 1 of chap. II, § 1) it is clear that this is the same as the $\mathbf{G}_m$-dual of $H_1(\mathrm{Graph}(M_0(N)_{/\bar{\mathbf{F}}_N}), \mathbf{Z})$. To prove injectivity of (11.10) it suffices to show that the map:

$$\mathrm{Graph}\ M_1(N)_{/\bar{\mathbf{F}}_N} \to \mathrm{Graph}\ M_0(N)_{/\bar{\mathbf{F}}_N}$$

induces a *surjection* on one-dimensional homology. But the above map of *graphs* is an *isomorphism* as follows from [9], V, th. (2.12) and VI, Cor. (6.10).

The relation between C *and* Σ. — By the cuspidal subgroup $C_{/\mathbf{Z}} \subset J_{/\mathbf{Z}}$ we mean the Zariski closure of $C \subset J(\mathbf{Q})$ in the group scheme $J_{/\mathbf{Z}}$. By the universal property of Néron models, the isomorphism $\mathbf{Z}/n \to C$ (of group schemes over $\mathbf{Q}$; $1 \mapsto c$) extends to a homomorphism $\mathbf{Z}/\mathbf{n}_{/S} \to C_{/S}$, and shows that $C_{/S}$ is a finite flat group.

Proposition (**11.11**). — *If n is odd, the group scheme* C *is a constant (étale) group over* S; *the scheme-theoretic intersection of* C *and* Σ *over* S *is the trivial group*; *the natural map* $C \oplus \Sigma \to J[\mathfrak{I}]$ *is an* injection.

If n is even, the group scheme $C_{/S}$ *contains a subgroup scheme isomorphic to* $\boldsymbol{\mu}_2$ (*and which we shall call* μ_2). *The cokernel of* μ_2 *in* C *is a constant (étale) group. The scheme-theoretic intersection of* C *and* Σ *in* $J_{/S}$ *is* μ_2. *The natural map* $C \oplus \Sigma \to J[\mathfrak{I}]$ *has "the diagonal"* $\boldsymbol{\mu}_2$ *as kernel, and induces an isomorphism of* $(C \oplus \Sigma)/\boldsymbol{\mu}_2$ *with the finite flat subgroup of order* $n^2/2$ *in* $J[\mathfrak{I}]$ *generated by* C *and* Σ (*call it* $C + \Sigma$).

Proof. — *(a)* We show first that the *odd* part of Σ has trivial intersection with (the odd part of) C. For by consideration of Galois modules, the odd part of Σ is a $\boldsymbol{\mu}$-type group and the odd part of C is a constant group.

(b) If *n* is even, the group $\Sigma(\mathbf{Q})$ (the rational points of Σ) is of order 2.

Lemma. — $\Sigma(\mathbf{Q}) \subset C$.

Proof. — Suppose that *n* is even, or, equivalently, $N \equiv 1 \bmod 8$. Then there is an étale double covering $X_0^\sharp(N) \to X_0(N)$ intermediate to the Shimura covering (2.3). This we shall call *the Nebentypus (double) covering.* Applying the functor Pic^0 to the Nebentypus covering (over $\mathbf{Q}$), we obtain a morphism of jacobians $J_{/\mathbf{Q}} \to \mathrm{Jac}(X_0^\sharp(N)_{/\mathbf{Q}})$ whose kernel is the group $\Sigma(\mathbf{Q})$. To prove the lemma, it suffices to show that the image, $c^\sharp$, of c in $\mathrm{Jac}(X_0^\sharp(N)_{/\mathbf{Q}})$ is of order $n/2$. For this, it suffices to show that if f is the function (11.2) whose divisor is $n.(0) - n.(\infty)$, then $f^{1/2}$ is a rational function on the Nebentypus curve $X_0^\sharp(N)$:

$$f^{1/2} = q^{n/2} \prod_{m=1}^{\infty} (1 - q^{mN})^{-12/\nu} . (1 - q^m)^{12/\nu}$$

as follows from Dedekind's transformation formulas for the η-function. (Cf. discussion of this in [48], § 3.)

The Zariski closure of $\Sigma(\mathbf{Q})$ in $J_{/S}$ (which is its Zariski closure in $\Sigma_{/S}$) is a $\boldsymbol{\mu}$-type group of order 2. Thus it is canonically isomorphic to $\boldsymbol{\mu}_{2/S}$ and we shall denote it $\mu_{2/S}$.

By the lemma, $\mu_2 \subset C_{/S}$. Since $C_{/S}$ is a finite flat group scheme, whose associated Galois module is a cyclic group with trivial Galois action, by (chap. I (4.6)) we have that the cokernel of μ_2 in C is a *constant (étale)* group scheme over S. It follows by an easy argument that $\Sigma \cap C_{/S}$ is the finite flat group scheme μ_2.

There is a canonical auto-duality:

(11.12) $$J[n] \underset{\approx}{\to} \mathscr{H}om(J[n], \mu_n) \text{ (over } \mathbf{Q})$$

and the section $c \in C \subset J[n](\mathbf{Q})$ determines, by (11.12), a homomorphism:

$$c^\sharp : J[n] \to \mu_n \text{ (over } \mathbf{Q}).$$

Restricting $c^\sharp$ to Σ, we obtain a homomorphism:

$$c^\sharp : U^* \to \mu_n$$

which, in turn, may be identified with an *element* $u \in U$ (1).

Question. — What is this element u?

This element has been evaluated in no case where $n > 1$. One can show that if p is an odd prime dividing n, then u projects to a generator of the p-primary component of U *if and only if* $\mathbf{T}_{\mathfrak{P}}$ (the completion of $\mathbf{T}$ at the Eisenstein prime $\mathfrak{P}$ associated to p) is isomorphic to $\mathbf{Z}_p$ (cf. (19.2) below) (2). In the light of the table of the introduction, it then follows that *u does* project to a generator of the p-primary component of $U(p \neq 2, p \mid n)$ for all $N < 250$ except when $N = 31$, 103, 127, 131, 181, 199 and 211.

12. The subgroup $D \subset J[\mathfrak{P}]$ ($p = 2$; n even).

Suppose $n \equiv 0 \bmod 4$ (equivalently: $N \equiv 1 \bmod 16$). Choose $y \in \Sigma(\mathbf{Q}(\sqrt{-1}))$ an element of order 4. Let $x = (n/4).c$, which is an element of order 4 in C. Thus x, y are elements of $C + \Sigma$ rational over $\mathbf{Q}(\sqrt{-1})$. By (11.11), $2x = 2y$. Let $D \subset (C+\Sigma)_{/S}$ be the closed subgroup scheme generated by the points $x - y$, and $2y$. In $(C+\Sigma)(\mathbf{Q}(\sqrt{-1}))$ these two points are a basis of an $\mathbf{F}_2$-vector space (of dimension two) which is stable under the action of $\mathrm{Gal}(\mathbf{Q}(\sqrt{-1})/\mathbf{Q})$. If τ is the nontrivial element of $\mathrm{Gal}(\mathbf{Q}(\sqrt{-1})/\mathbf{Q})$, then the matrix of τ computed with respect to the basis $x - y$, $2y$ is $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Since $\mathbf{Q}(\sqrt{-1})/\mathbf{Q}$ is unramified at N, the group scheme D is finite and flat over S (chap. I (1.3)), and it follows from the above discussion and (chap. I (4.4)) that D is isomorphic to the unique nontrivial extension of $\mathbf{Z}/2_{/S}$ by $\mu_{2/S}$ killed by 2.

---

(1) Since there are *two* natural choices of sign of the above autoduality (or equivalently, of the e_n-pairing), the pair of elements $u^{\pm 1}$ has, perhaps, greater significance than the element u.

(2) Which explains why we might be interested in some reasonable direct method of computation of u.

The purpose of this section is to consider the case where $n \equiv 2 \bmod 4$ (equivalently: $N \equiv 9 \bmod 16$) and to construct a subgroup scheme of $J[\mathfrak{P}]$, which is isomorphic to D. In this case, the 2-primary components of C and of Σ *coincide* with μ_2. The group scheme D, which we construct, will contain μ_2, but (necessarily) will not be contained in $C+\Sigma$.

The construction of D. — If n is even, the Nebentypus covering (§ 11) $X_0^\sharp(N) \to X_0(N)$ is étale (over S′) with Galois group U/U^2. Let ν be the nontrivial element in U/U^2, and $J \to J^\sharp$ the induced morphism on jacobians. Using the Leray Spectral sequence (over the base $\bar{\mathbf{Q}}$) for $\mathbf{G}_m$-cohomology of the Nebentypus covering, one has:

$$\textbf{(12.1)} \qquad 0 \to \mu_2(\bar{\mathbf{Q}}) \to J(\bar{\mathbf{Q}}) \to (J^\sharp(\bar{\mathbf{Q}}))^\nu \to 0$$

where the superscript ν means the part fixed under the involution ν.

To describe the Galois module associated to D, we shall construct a point of order 2 in $J^\sharp(\bar{\mathbf{Q}})$, and $D(\bar{\mathbf{Q}})$ will be, by definition, the subgroup of $J(\bar{\mathbf{Q}})$ generated by the inverse image of this point.

There are *four* cusps on $X_0^\sharp(N)$. Let 0, $\bar{0}$ denote the cusps lying over 0 in $X_0(N)$, and ∞, $\bar{\infty}$ those lying over ∞. Thus ν interchanges 0 and $\bar{0}$ (and ∞ and $\bar{\infty}$). The cusps 0 and $\bar{0}$ are rational over $\mathbf{Q}$, while ∞ and $\bar{\infty}$ are conjugate over $\mathbf{Q}$ and defined over $\mathbf{Q}(\sqrt{N})$. Compare [48], § 1.

Proposition **(12.2)** *(Ogg, Ligozat).* — *Let* χ *be the Legendre symbol of conductor* N, $\chi(a) = \left(\frac{a}{N}\right)$, *and let* $B_{2,\chi}$ *be the generalized second Bernoulli number associated to* χ ([22] *a)). Then the divisor class of* $(0)-(\bar{0})$ (*and of* $(\infty)-(\bar{\infty})$) *in* $J^\sharp$ *is of order* $B_{2,\chi}/4$. *There is a rational function* f *on* $X_0(N)_{/\mathbf{Q}}$ *having the properties*:

(a) $$(f) = (B_{2,\chi}/4) \cdot ((0)-(\bar{0}))$$

(b) $$\nu . f = -1/f.$$

The function f, and the proof of the proposition of Ligozat and Ogg are discussed below. We now prepare to apply their proposition in the construction of D.

Lemma **(12.3)**. — If $N \equiv 1 \bmod 8$, *then* $B_{2,\chi} \equiv 0 \bmod 8$.

Proof. — $B_{2,\chi} = N . \sum_{u=1}^{N-1} \chi(u) . B_2\left(\frac{u}{N}\right)$ where $B_2(X)$ is the second Bernoulli polynomial, $X^2 - X + 1/6$. Thus:

$$B_{2,\chi} = N . \sum_{u=1}^{N-1} \left(\frac{u}{N}\right) \cdot \left(\frac{u^2}{N^2} - \frac{u}{N}\right)$$

and since $N \equiv 1 \bmod 8$:

$$B_{2,\chi} \equiv \sum_{u=1}^{N-1} \binom{u}{N}(u^2-u) \mod 8$$

$$\equiv \sum_{\substack{u \text{ odd} \\ 1 \le u \le N-2}} \binom{u}{N}(u^2-u+(N-u)^2-(N-u))$$

$$\equiv \sum_{\substack{u \text{ odd} \\ 1 \le u \le N-2}} \binom{u}{N}(2u^2-2u) \equiv 4. \sum_{\substack{u \text{ odd} \\ 1 \le u \le N-2}} \binom{u}{N}.u.\left(\frac{u-1}{2}\right)$$

$$\equiv 4. \sum_{\substack{u \text{ odd} \\ 1 \le u \le N-2}} (u-1)/2 \mod 8$$

Writing $u = 1+2j$ $(j = 0, 1, 2, \ldots, (N-3)/2)$ we get:

$$B_{2,\chi} \equiv 4.\frac{(N-3)/2.((N-3)/2+1)}{2} \mod 8$$

$$\equiv 4.(N-3).\frac{N-1}{8} \mod 8.$$

But $N \equiv 1 \bmod 8$. Q.E.D.

We conclude from (12.2) and (12.3) that $(0)-(\bar{0})$ and $(\infty)-(\bar{\infty})$ are of *even* order $(1/4)B_{2,\chi} = n^\#$ in $J^\#$.

Set:

$$A = (n^\#/2).\mathscr{C}\ell((0)-(\bar{0}))$$

$$B = (n^\#/2).\mathscr{C}\ell((\infty)-(\bar{\infty}))$$

so $2A = 2B = 0$. Since A and B are fixed under ν, they are in the image of J.

Suppose that $N \equiv 9$ *mod* 16. — The image of c in $J^\#$ is the divisor class of $(0)+(\bar{0})-(\infty)-(\bar{\infty})$ which is of *odd* order $m = n/2$. Thus:

$$A+B = m.A+m.B = n^\#/2.\mathscr{C}\ell(m.((0)+(\bar{0})-(\infty)-(\bar{\infty}))) = 0$$

and therefore A=B. Denote by $D \subset J(\bar{\mathbf{Q}})$ the inverse image (in $J(\bar{\mathbf{Q}})$) of the group generated by A. Since A is fixed by w and $w\nu$ (acting on $J^\#$), D is stable under the action of w (acting on J). Also, D is stable under Galois. Let $\alpha \in \mu_2(\bar{\mathbf{Q}})$ be the non-trivial element, and let $\beta \in D$ be an element in the inverse image of A.

Lemma **(12.4)**. — D *is a Klein four group. The action of* $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ *on* D *is the action which factors through* $\mathrm{Gal}(\mathbf{Q}(\sqrt{-1})/\mathbf{Q})$ *where the conjugation* τ *acts on the basis* α, β *by the matrix* $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Proof. — Using (12.2), the above lemma is an exercise in Galois theory. To emphasize this, let K be the function field of $X_0(N)_{/\mathbf{Q}}$ and L the function field of $X_0^\#(N)_{/\mathbf{Q}}$.

Thus L/K is a quadratic extension with ν as conjugation. By (12.2) f is not a square in $L\otimes\mathbf{C}$. The extension $L(f^{1/2})/K$ is a quartic extension. Since $\nu(f)=-1/f$, (12.2) *(b)*, the extension $L(f^{1/2},\sqrt{-1})/K(\sqrt{-1})$ is Galois. Let G denote its Galois group. Fix $\bar{\nu}$, a lifting of ν to G, and let τ denote complex conjugation in $L(f^{1/2},\sqrt{-1})$. By (12.2) *(b)*, $\bar{\nu}(f^{1/2})=\pm\sqrt{-1}.f^{-1/2}$. Therefore $\bar{\nu}^2(f^{1/2})=f^{1/2}$, and consequently $\bar{\nu}^2=1$. It follows that G is a Klein four-group and therefore so is D, for D is the Cartier dual of G. Let ρ denote the automorphism of $L(f^{1/2},\sqrt{-1})/L(\sqrt{-1})$, given by $\rho(f^{1/2})=-f^{1/2}$. One checks:

$$\tau\nu\tau^{-1}=\rho.\nu$$

$$\tau\rho\tau^{-1}=\rho$$

which yields the Galois action on D asserted in the lemma. Let $D_{/S}$ denote the group scheme extension (Zariski closure) of $D_{/\mathbf{Q}}$ in $J_{/S}$. Let $D_{1/S}$ denote the finite flat group which is the unique extension of $\mathbf{Z}/\mathbf{2}_{/S}$ by $\mu_{2/S}$ killed by 2 (*extension* 2 of chapter I (4.2)).

Lemma (**12.5**). — $D_{/S}\cong D_{1/S}$.

Proof. — The two groups have isomorphic Galois modules. Therefore, if $D_{/S}$ is a finite flat group over S, then (12.5) follows from chapter I (4.4). Consider an isomorphism $D_{1/\mathbf{Q}}\xrightarrow{\approx}D_{/\mathbf{Q}}\subset J_{/\mathbf{Q}}$ and extend it to an isomorphism:

$$D_{1/\mathbf{Z}[1/2]}\xrightarrow{\approx}D_{/\mathbf{Z}[1/2]}\subset J_{/\mathbf{Z}[1/2]}$$

by the universal property of Néron models. In particular, $D_{/\mathbf{Z}[1/2]}$ is finite. Since $D_{/S'}$ is clearly finite, it follows that $D_{/S}$ is a finite flat group.

Lemma (**12.6**). — D *is annihilated by the Eisenstein ideal* $\mathfrak{I}$.

Proof. — By the formulas giving the action of T_ℓ on the cusps of $X_0^\sharp(N)$ one has, as in (11.1), $T_\ell.A=(1+\ell).A$ $(\ell\neq N)$. As already mentioned, A is fixed under w, and since it is of order 2, $(1+w).A=0$. It follows that D is annihilated by $\mathfrak{I}^2$. Any element $\gamma\in\mathfrak{I}$ operates as an upper triangular matrix in terms of the basis α, β. To show that D is annihilated by $\mathfrak{I}$, we show that $\gamma\in I$ operates *semi-simply* on the vector space D. For this, we choose a prime lying above N in $\mathbf{Z}[\sqrt{-1}]$, and consider the specialization map $D(\mathbf{Z}[\sqrt{-1}])\to D(\mathbf{F}_N)$, which is an isomorphism of **T**-modules. Let $D(\mathbf{F}_N)^0=D(\mathbf{F}_N)\cap J^0(\mathbf{F}_N)$. Note that $D(\mathbf{F}_N)$ is canonically a direct sum:

$$D(\mathbf{F}_N)=D(\mathbf{F}_N)^0\oplus\mu_2(\mathbf{F}_N)$$

(for the subgroup $\mu_2\subset C$ maps isomorphically to the image of $D(\mathbf{F}_N)$ in $\bar{C}$ (11.3)). Since the action of **T** " preserves J^0 " it follows that the action of **T** preserves the above direct sum decomposition. Since each summand is an $\mathbf{F}_2$-vector space of dimension 1, **T** does act semi-simply on $D(\mathbf{Z}[\sqrt{-1}])$.

Discussion of proof of the proposition of Ligozat and Ogg. — Ligozat constructs the function f using the " Klein forms " of Kubert and Lang [28], which are essentially Eisenstein series of weight 1. Ogg has a different point of view; he works with products of differences of Eisenstein series of weight 2. In the end, from either point of view, one emerges with a function f on $X_0(N)_{/\mathbf{Q}}$ whose divisor is $B_{2,\chi}/4.((0)-(\overline{0}))$ and which has the property that $f(\infty).f(\overline{\infty})=-1$. Assertion *(b)* of our proposition follows from this equation since $(\gamma f).f$ must be a constant. It also follows that, up to sign, Ligozat's function and Ogg's function must agree (this identity is nontrivial). Both Ligozat and Ogg check that their function f is " smallest possible " and thus $B_{2,\chi}/4$ is indeed the order of the divisor class of $((0)-(\overline{0}))$ in $J^{\#}$. Nevertheless, in the light of the use we make of $(0)-(\overline{0})$ it is worth noticing that the equation $f(\infty)f(\overline{\infty})=-1$ immediately implies that this divisor class is *not* killed by $B_{2,\chi}/8$ [1]. For if it were, there would be a function g on $X_0(N)_{/\mathbf{Q}}$ such that $g^2=r.f$ where r is a rational (nonzero) number. This is impossible, for $g(\infty).g(\overline{\infty})$ would then be a rational number whose square is negative.

In the remainder of this section, although we do not prove the proposition in full, we present an account of the *construction* of Ligozat's function and some of its salient properties [2].

Ligozat's construction. — We may take $N\equiv 1 \bmod 4$, $N>5$.

Let ζ be a primitive N-th root of 1; set:

$$S_{\pm}=\{\,1\leq a\leq (N-1)/2 \mid \chi(a)=\pm 1\,\}$$

and:

$$g_{\pm}(z)=\prod_{m=1}^{\infty}\frac{\prod_{a\in S_{\pm}}(1-\zeta^a.q^m)(1-\zeta^{-a}.q^m)}{(1-q^m)^{(N-1)/2}}.$$

The functions $g_{\pm}(z)$ $(q=e^{2\pi iz})$ are expressible as products of Klein forms of level N [28].

Explicitly, let $\rho_{\pm}$ be the constant:

$$\rho_{\pm}=(-2\pi i)^{(N-1)/4}.\exp\left(\frac{2\pi i}{2N}.\sum_{a\in S_{\pm}}a\right).\prod_{a\in S_{\pm}}(1-\zeta^a)^{-1}$$

then, using the notation of [28]:

$$g_{\pm}(z)=\rho_{\pm}.\prod_{a\in S_{\pm}}\mathbf{k}_{(0,a)}(z).$$

One checks:

$$g_{+}(z).g_{-}(z)=\prod_{m=1}^{\infty}(1-q^{Nm})(1-q^m)^{-N}=\frac{\eta(Nz)}{\eta(z)^N}$$

---

(1) An integer, by lemma (12.3).

(2) Here I have simply copied a part of a manuscript that Ligozat provided for me, and for which I am extremely grateful. It is to be hoped that Ligozat will present the full story in his future publications.

and therefore (by Hecke [19], p. 924) $g_+ . g_-$ is a modular form of weight $-(N-1)/2$ on $\Gamma_0(N)$, of Nebentypus, whose associated character is the Legendre character χ.

Definition. — $f(z)=\dfrac{g_+(z)}{g_-(z)}$.

Lemma. — *$f(z)$ is a modular form on $\Gamma_1(N)$.*

Proof. — This follows from the transformation laws for the Klein forms $\mathbf{k}$ of [28]. If $v=\begin{pmatrix} 1+N\alpha & N\beta \\ N\gamma & 1+N\delta \end{pmatrix} \in \Gamma(N)$ one has:

$$\mathbf{k}_{(0,a)}(vz)=(N\gamma z+N\delta).\varepsilon_a(\gamma,\delta).\mathbf{k}_{(0,a)}(z)$$

where $-\varepsilon_a(\gamma,\delta)=(-1)^{(\gamma a+1)(\delta a+1)} \exp\left(2\pi i \dfrac{(-\gamma a^2)}{2N}\right)$ and therefore $f(z)$ is invariant under $\Gamma(N)$ if and only if:

$$(-1)^{\frac{N-1}{2}} \prod_{1\leq a\leq (N-1)/2} \varepsilon_a(\gamma,\delta)^{(a)}=1$$

for any choice of γ, δ. Since $N>5$, $\sum_a \chi(a).a^2 \equiv 0 \bmod N$ and therefore we may rewrite the condition of invariance of $f(z)$ as:

$$(\gamma+\delta)\Big(\sum_{1\leq a\leq (N-1)/2} \chi(a).a\Big)+\gamma(1+N\delta)\sum_{1\leq a\leq (N-1)/2} \chi(a)a^2 \equiv 0 \bmod 2.$$

Now note that if γ is even, so is δ, in which case the above congruence holds. If γ is odd, it also holds since $\sum_{1\leq a\leq (N-1)/2} \chi(a)(a+a^2)\equiv 0 \bmod 2$. Therefore f is invariant under $\Gamma(N)$. To see that it is invariant under $\Gamma_1(N)$, note that $\mathbf{k}_{(0,a)}(z+i)=\mathbf{k}_{(0,a)}(z)$ for $i\in\mathbf{Z}$.

Definition. — *If* $u=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, *define* $\varepsilon(u)=f(uz).f(z)^{-\chi(d)}$.

Thus ε is a *character* of $\Gamma_0(N)$, trivial on $\Gamma_1(N)$, and takes values in the group of $(2N)$-th roots of 1.

Lemma. — $\varepsilon(u)=\chi(d)$.

Proof. — Clearly $\varepsilon^2=1$, since the index of $\Gamma_1(N)$ in $\Gamma_0(N)$ is relatively prime to N. To establish the lemma, one must show that $\varepsilon \neq 1$.

If $\begin{pmatrix} a & b \\ c & d \end{pmatrix}=u$ is in $\Gamma_0(N)$, and $\chi(d)=-1$ then:

$$g_\pm(uz)=\varepsilon_\pm(u).(cz+d)^{(N-1)/4}.g_\mp(z)$$

where $\varepsilon_\pm(u)$ are $2N$-th roots of 1 and $\varepsilon(u)=\varepsilon_+(u)/\varepsilon_-(u)$. But since $g_+g_-=\eta(Nz)/\eta(z)^N$ is of Nebentypus with character χ, $\varepsilon_+.\varepsilon_-=\chi(d)=-1$. It follows that $\varepsilon(u)=-1$.

Corollary. — $\gamma f=-1/f$.

By the properties of Klein forms [28] the zeroes of f are concentrated at (0), $(\bar{0})$ and an elementary computation (compare [48], § 2) gives their order.

13. The dihedral action on $X_1(N)$.

We shall be working with the covering $X_1(N) \to X_0(N)$ of curves over $\mathbf{Q}$, and with certain subcoverings. Abbreviate the notation to $X_1 \to X_0$, and set:

$$U = (\mathbf{Z}/N)^*/(\pm 1).$$

So, U operates on X_1 with quotient curve X_0; it operates freely on the open curve $Y_1 = X_1 - \text{cusps}$.

As in [40] form a " dihedral " group Δ containing U as follows:

$$\Delta = U \cup \{w_\zeta\}_\zeta$$

where the w_ζ are " symbols " indexed by the primitive N-th roots of 1, $\zeta \in \bar{\mathbf{Q}}$, where, by convention, the element $w_{\zeta^{-1}}$ is taken to be equal to the element w_ζ. Impose a group law on Δ by:

$$(13.1) \qquad (w_\zeta)^2 = 1; \quad u.w_\zeta = w_{\zeta^u} = w_\zeta.u^{-1}$$

for all $u \in U$, and primitive N-th roots of 1, ζ. Here $\zeta^u = \zeta^a$ for a an integer (mod N) projecting to $u \in U$.

The dihedral group Δ acts in a natural way as a group of automorphisms of X_1 (cf. [40] § 2). The compatibility of the action of Δ and of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on $X_1(\bar{\mathbf{Q}})$ is most conveniently described as follows: Define an action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on Δ by the rules $u^\alpha = u$; $(w_\zeta)^\alpha = w_{\zeta^\alpha}$, for $\alpha \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, $u \in U$, and ζ a primitive N-th root of 1. Then, for $\delta \in \Delta$, and $x \in X_1(\bar{\mathbf{Q}})$, we have: $(\delta.x)^\alpha = \delta^\alpha.x^\alpha$ [1].

The action of Δ on X_1 " covers the action of the canonical involution w on X_0 ", in the following sense: If $\pi : X_1 \to X_0$ is the projection, then $\pi(w_\zeta.x) = w.\pi(x)$; $\pi(u.x) = \pi(x)$.

Let $\varphi_0 \subset X_0(\bar{\mathbf{Q}})$ be the fixed point set of the canonical involution w. Using the modular definition of w, one sees that a point in φ_0 is given by an elliptic curve defined over $\bar{\mathbf{Q}}$ together with an endomorphism whose square is $-N$ (note: $N \geq 5$). That is, the fixed point set is in one-one correspondence with isomorphism classes of elliptic curves over $\bar{\mathbf{Q}}$ which possess a complex multiplication by $\sqrt{-N}$. *Suppose that* $N \equiv 1 \bmod 4$. Then $\mathbf{Z}[\sqrt{-N}]$ is the full ring of integers in $\mathbf{Q}(\sqrt{-N})$ and φ_0 is a principal homogeneous set under the natural action of $\mathcal{Cl}$, the ideal class group of the field $\mathbf{Q}(\sqrt{-N})$.

Let $\varphi_1 \subset X_1(\bar{\mathbf{Q}})$ be the full inverse image of φ_0, and let $\varphi_1(\zeta) \subset \varphi_1$ be the fixed point set of w_ζ, for each ζ.

---

[1] In [40] we call Δ, with its $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ action, the *twisted* dihedral group.

If $x_1 \in \varphi_1$, and ζ is a primitive N-th root of 1, there is a unique element of U, which we denote $u_{(x_1, \zeta)}$ satisfying:

$$w_\zeta . x_1 = u_{(x_1, \zeta)} . x_1 .$$

Clearly, for $v \in U$, $u_{(x_1, \zeta)} v = v . u_{(x_1, \zeta)}$ from which one gets

Lemma **(13.2)**. — φ_1 *decomposes into the disjoint union*:

$$\varphi_1 = \coprod_\zeta \varphi_1(\zeta)$$

where ζ *runs through the set of primitive* N*-th roots of* 1, *with the convention that we have* identified ζ *and* ζ^{-1}.

Let x_0 denote the image of x_1 in X_0. An elementary computation gives, for any element $u . x_1$ in the inverse image of x_0, that:

(13.3) $$u_{(u . x_1, \zeta)} = u^{-2} . u_{(x_1, \zeta)}$$

and consequently the question of whether or not $u_{(x_1, \zeta)}$ is a *square* in U depends on x_0 and ζ but not on x_1. Write $u_{(x_0, \zeta)} \in U/U^2$ for the image of $u_{(x_1, \zeta)}$.

Lemma **(13.4)**. — *These are equivalent*:

a) $u_{(x_0, \zeta)}$ *is trivial in* U/U^2.

b) w_ζ *possesses a fixed point in the inverse image of* x_0.

Moreover, if these conditions hold, then w_ζ *will have exactly two fixed points in the inverse image of* x_0, *and these fixed points will be multiples of each other by the unique element* $v \in U$ *which is of precise order two.*

Proof. — This is essentially immediate: If a) holds, choose an x_1 mapping to x_0, and let $u \in U$ be such that $u^2 = u_{(x_1, \zeta)}$. Then (13.3) shows that $u . x_1$ is a fixed point of w_ζ. The other direction is totally trivial. Finally, if x_1 is a fixed point of w_ζ, from (13.3) the action of w_ζ on the inverse image of x_0 is:

$$w_\zeta (u . x_1) = u^{-1} . x_1$$

giving the last assertion of our lemma.

Since $(w_\zeta . x)^\alpha = w_{\zeta^\alpha} . x^\alpha$ for $\alpha \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, it follows that α induces a 1 : 1 correspondence $\varphi_1(\zeta) \to \varphi_1(\zeta^\alpha)$, giving:

Lemma **(13.5)**. — *Let* h *be the class number of* $\mathbf{Q}(\sqrt{-N})$. *Then, for any primitive* N*-th root of* 1, ζ, w_ζ *has exactly* h *fixed points in* $X_1(\bar{\mathbf{Q}})$.

Proof. — The cardinality of φ_1 is $h . (N-1)/2$. By (13.5), φ_1 is the disjoint union of the $(N-1)/2$ sets $\varphi_1(\zeta)$, which are put in 1 : 1 correspondence, one with another, by the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. It follows that each of these sets has cardinality h.

Comparing lemmas (13.5) and (13.4) it follows that, for a given ζ, precisely

half of the elements of φ_0 have the property that w_ζ has a fixed point in their inverse image. It is reasonable to expect that the elements of φ_0 with this property, for a given ζ, forms a principal homogeneous space under the action of $\mathscr{C}l^2 \subset \mathscr{C}l$ (squares of ideal classes).

Now pass to the Nebentypus curve $X^\# \to X_0$ which fits into a diagram:

$$\begin{array}{l} U \left\{ \begin{array}{l} X_1 \\ \downarrow \\ X^\# \\ \downarrow \\ X_0 \end{array} \right. \begin{array}{l} \} U^2 \\ \\ \} (1, \nu) \end{array} \end{array}$$

where ν denotes the involution of $X^\#$ such that $X^\#/\nu = X_0$, induced from the action of any $u \in U$ such that $u \notin U^2$. From (13.1) one sees that the $(N-1)$ involutions w_ζ induce precisely *two* distinct involutions of $X^\#$ which we arbitrarily call $w^\#$ and $\nu.w^\#$. These are conjugate over $\mathbf{Q}$ and defined over $\mathbf{Q}(\sqrt{N})$. From (13.1) we have that ν and $w^\#$ commute. Also, from (13.4) it follows that if w_ζ induces $w^\#$, then $\varphi_1(\zeta)$ projects bijectively to the fixed point set of $w^\#$. Consequently, both $w^\#$ and $\nu.w^\#$ have exactly h fixed points in $X^\#(\bar{\mathbf{Q}})$.

Now suppose $N \equiv 1 \bmod 8$, so $X^\# \to X_0$ is unramified. Consider the diagram:

(13.6)

$$\begin{array}{ccccc} & & X^\# & & \\ & \swarrow^{\alpha} & & \searrow & \\ X^\#/w^\# & & & & X^\#/\nu = X_0 \\ & \searrow_{\beta} & & \swarrow & \\ & & X^+ = X_0/w & & \end{array}$$

Lemma **(13.7)**. — *Both α and β are ramified.*

Proof. — As for α, this follows since $w^\#$ has h fixed points. To compute the number of fixed points of β, we use the Euler characteristic χ:

$$\begin{array}{ll} \chi(X^\#) = 2.\chi(X_0) & \text{(since } X^\# \to X_0 \text{ is unramified)} \\ \chi(X^\#) = 2.\chi(X^\#/w^\#) - h & (w^\# \text{ has } h \text{ fixed points}) \\ \chi(X_0) = 2.\chi(X^+) - h & (w \text{ has } h \text{ fixed points}) \end{array}$$

which gives: $\chi(X^\#/w^\#) = 2.\chi(X^+) - h/2$ and therefore β has $h/2$ fixed points.

Lemma **(13.8)**. — *We continue to suppose* $N \equiv 1 \bmod 8$. *The subgroup* $D \subset J_{/\mathbf{Q}}$ (cf. § 12) *has trivial intersection with the sub-abelian variety* $J_+ = (1+w).J$.

Proof. — We work with group schemes over $\mathbf{Q}$. We first show that the subgroup μ_2 of the Shimura subgroup has trivial intersection with J_+. If $Y \to Z$ is any double covering of (smooth projective) curves, then the induced map on their jacobians (regarded

as Pic^0) is injective if and only if the double covering is ramified. Since $X_0 \to X^+$ is ramified, we may identify the jacobian of X^+ with the sub-abelian variety $J_+ \subset J$. The subgroup $\mu_2 \subset D$ is the kernel of the map $J \to J^\#$ on jacobians induced by $X^\# \to X_0$ (12.1).

To show that μ_2 is not contained in J_+, it suffices to show that the composition $J_+ \to J \to J^\#$ is injective. But the map $J_+ \to J^\#$ is induced from the covering of degree 4, $X^\# \to X^+$. Returning to diagram (13.6) we have that this map is the composite $\beta\alpha$ where by (13.7) both β and α are ramified double coverings. Injectivity of $J_+ \to J^\#$ follows. Since J_+ is defined over $\mathbf{Q}$, and $D \cap J_+$ is a subgroup scheme of D (over $\mathbf{Q}$) not containing μ_2, it must vanish. Q.E.D.

Corollary **(13.9).** — *The subgroup scheme* $D_{/S'} \subset J_{/S'}$ *maps isomorphically onto a subgroup scheme of* $\bar{J}_{/S'}$ *under the natural projection of abelian schemes* $J_{/S'} \to \bar{J}_{/S'}$ (cf. § 10).

Proof. — Let $\bar{D}_{/S'} \subset \bar{J}_{/S'}$ be the subgroup scheme extension of the image of $D_{/\mathbf{Q}}$ in $\bar{J}_{/\mathbf{Q}}$. Then we have a map $D_{/S'} \to \bar{D}_{/S'}$ which induces an isomorphism on Galois modules. It must be an isomorphism, by chapter I (4.4).

For later purposes:

Corollary **(13.10).** — *The subgroup* $(D_{/\mathbf{F}_2})^{\text{ét}} \subset J_{/\mathbf{F}_2}$ *is not in the image of* $1 + w$.

Proof. — The image of $J_{/\mathbf{F}_2}$ under $1 + w$ goes to zero in $\bar{J}_{/\mathbf{F}_2}$, but $(D_{/\mathbf{F}_2})^{\text{ét}}$ does not, by (13.9).

14. The action of Galois on torsion points of J.

Let m be an integer $\neq 0$, and consider $J[m](\bar{\mathbf{Q}})$ as a $\mathbf{T}/(m.\mathbf{T})[G]$-module (the group ring of G with coefficients in $\mathbf{T}/(m.\mathbf{T})$ where G is some finite quotient of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ through which the natural action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on $J[m](\bar{\mathbf{Q}})$ factors). Say that the $\mathbf{T}/(m.\mathbf{T})[G]$-module V is a *constituent* of $J[m](\bar{\mathbf{Q}})$ if it is a constituent of a $\mathbf{T}/(m.\mathbf{T})[G]$-Jordan-Hölder filtration of $J[m](\mathbf{Q})$. Since a constituent V is irreducible (as $\mathbf{T}/(m.\mathbf{T})[G]$-module), its annihilator in $\mathbf{T}$ is a maximal ideal $\mathfrak{M}$. Say that V *belongs to* $\mathfrak{M}$. Thus, V is a $k_{\mathfrak{M}}[G]$-module where $k_{\mathfrak{M}}$ is the residue field $\mathbf{T}/\mathfrak{M}$. By the *dimension* of V we mean its dimension as *$k_{\mathfrak{M}}$-vector space.*

Note that any constituent V belonging to $\mathfrak{M}$ is a constituent of the sub-module $J[\mathfrak{M}^r](\bar{\mathbf{Q}}) \subset J[m](\bar{\mathbf{Q}})$ for suitable integers r, m. Note also that given a generating set of elements $(a_1, \ldots, a_t)$ of the $k_{\mathfrak{M}}$-vector space $\mathfrak{M}^r/\mathfrak{M}^{r+1}$, the map $x \mapsto a_1.x \oplus \ldots \oplus a_t.x$ is an injection of the module $J[\mathfrak{M}^r]/J[\mathfrak{M}^{r+1}](\bar{\mathbf{Q}})$ into the direct sum of t copies of $J[\mathfrak{M}](\bar{\mathbf{Q}})$, and therefore V is isomorphic to a constituent in $J[\mathfrak{M}](\bar{\mathbf{Q}})$. Regarding V as a specific subquotient of $J[m](\bar{\mathbf{Q}})$ we may use (chap. I, § 1 (6)) to obtain a quasi-finite group scheme subquotient $V_{/S}$ of $J[m]_{/S}$ which is finite and flat over S′, and whose associated Galois module is the subquotient V.

Note however that the isomorphism type of $V_{/S}$ *may* depend on the way we view V as subquotient of $J[m](\bar{\mathbf{Q}})$ and is not necessarily predictable from the isomorphy type of V.

By Fontaine's theorem, chapter I (1.4), however, it *is* determined (over S') by the isomorphy type of V provided the characteristic of $k_{\mathfrak{M}}$ is different from 2.

Let p be the characteristic of $k_{\mathfrak{M}}$ and $V_{/\mathbf{F}_q}$ the fibre of $V_{/S}$ reduced to characteristic p. Consider the two possibilities:

a) $T_p \in \mathfrak{M}$. Then, by the Eichler-Shimura relations (§ 6), both the *Frobenius* and the *Verschiebung* satisfy the relation $X^2 - T_p X + p = 0$, and therefore, since $\mathfrak{M}$ annihilates $V_{/\mathbf{F}_p}$ they satisfy the relation: $X^2 = 0$. That is, both *Frobenius* and *Verschiebung* are nilpotent on $V_{/\mathbf{F}_p}$. Consequently, $V_{/\mathbf{F}_p}$ has the property that both it and its Cartier dual are unipotent finite group schemes. Equivalently, it has a Jordan-Hölder filtration by finite subgroup schemes, all constituents being isomorphic to α_p ([9], IV, § 4 (3.14)). In this case say that $\mathfrak{M}$ is *supersingular.*

b) $T_p \notin \mathfrak{M}$. Then, as above, *Frobenius* and *Verschiebung* satisfy $X.(X - T_p) = 0$, where T_p is an automorphism of $V_{/\mathbf{F}_p}$ and it follows that:

$$V_{/\mathbf{F}_p} = V^{\text{m.t.}}_{/\mathbf{F}_p} \times V^{\text{ét}}_{/\mathbf{F}_p}.$$

(The product decomposition arising, if you wish, from the fact that T_p^{-1}. *Frobenius* and T_p^{-1}. *Verschiebung* are *orthogonal* idempotents whose sum is the identity.)

Thus $V_{/\mathbf{F}_p}$ is, as we shall say, an *ordinary* group scheme over $\mathbf{F}_p$. In this case we say that $\mathfrak{M}$ is *ordinary.*

Proposition (**14.1**). — *Let* V *be a constituent belonging to* $\mathfrak{M}$. *Then* V *is of dimension* 1 *if and only if* $\mathfrak{M}$ *is an Eisenstein prime. If* $\mathfrak{P}$ *is an Eisenstein prime, then* $J[\mathfrak{P}^r]_{/S}$ *is admissible* (cf. chap. I, § 1 *(f)*).

Proof. — We first show that if V is of dimension 1, then it belongs to an Eisenstein prime. Consider $V_{/S}$, which is a finite flat group scheme if and only if the inertia group at N operates trivially on the $k_{\mathfrak{M}}$-vector space V (chap. I (1.3)). Since the inertia group operates unipotently (SGA 7, exp. IX (3.5) (critère galoisien de réduction semi-stable) which applies since (appendix) $J_{/S}$ has semi-stable reduction at N) and semi-simply (since V is of dimension 1 over $k_{\mathfrak{M}}$), it *does* operate trivially (1).

Thus $V_{/S}$ is a *finite* flat one-dimensional $k_{\mathfrak{M}}$-vector group scheme. By chapter I (1.5), either:

$$V_{/S} = \boldsymbol{\mu}_p \otimes_{\mathbf{F}_p} k_{\mathfrak{M}}$$

or:

$$V_{/S} = \mathbf{Z}/\mathbf{p} \otimes_{\mathbf{F}_p} k_{\mathfrak{M}}$$

and in either case, the Eichler-Shimura relations (§ 6) give us the following facts about the image of T_ℓ ($\ell \neq N$) in $k_{\mathfrak{M}}$ which we can think of as *contained in* $\text{End}(V_{/\mathbf{F}_\ell})$:

$$T_\ell \equiv 1 + \ell \mod \mathfrak{M} \quad (\ell \neq N).$$

(1) This was pointed out to me by K. Ribet.

As for the image of w in $k_{\mathfrak{M}}$, since w is or order 2, this image *must* be ± 1. If the image of w is -1, then $\mathfrak{M}$ is visibly the Eisenstein prime of residual characteristic p.

To conclude the first part of this proof, one must show that if p is odd, the case $w \mapsto +1$ cannot occur. We show that the ideal $\mathfrak{M}$ generated by: p, $1-w$, and $1+\ell-T_\ell$ (all $\ell \neq N$) is the *unit* ideal in $\mathbf{T}$. Suppose not; then it is a maximal ideal with residue field $\mathbf{F}_p$. By (9.3) the kernel of its action on $H^0(X_0(N)_{/\mathbf{F}_p}, \Omega)$ is of dimension 1 over $\mathbf{F}_p$.

This kernel is generated by a parabolic modular form mod p, g, whose q-expansion is entirely determined (9.2) by the above package of eigenvalues, and the fact that it begins with the term $1.q$. Comparing the coefficients of g with that of the Eisenstein series e' (5.1) one sees that $f=e'+24.g$ is a modular form modulo $24p$ whose q-expansion (modulo $24p$) is a function of q^N:

$$\tilde{f}=(1-N)-48.q^N+\dots$$

If $p \geq 5$, such a modular form does not exist [1] by lemma (5.10) (if $p=N$), by lemmas (4.10), (5.9) (if $p \mid N-1$) and corollary (5.11) (if $p \neq N$, $p \nmid N-1$). If $p=3$, and $N \equiv 1 \bmod 3$, then $\tilde{f}/3=\left(\frac{N-1}{3}\right)+16.q^N+\dots$ does not exist mod 3, as a holomorphic modular form, by corollary (5.11) (ii) (if $N \not\equiv 1 \bmod 9$) and by (4.10) and (5.9) (if $N \equiv 1 \bmod 9$). Finally, if $p=3$, and $N \equiv -1 \bmod 3$, f does not exist mod 9 by corollary (5.11).

To conclude the proof of our proposition, we show that if $\mathfrak{P}$ is an Eisenstein prime, then $J[\mathfrak{P}^r]$ is admissible (any r) and consequently any of its constituents is, indeed, of dimension 1. In the light of (chap. I, § 1 *(f)*) and remarks made at the beginning of this section, it suffices to show that $J[\mathfrak{P}](\bar{\mathbf{Q}})$ possesses an admissible filtration by sub-Galois modules. Let W denote the $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-module which is the direct sum of $J[\mathfrak{P}](\bar{\mathbf{Q}})$ and its Cartier dual. Thus W is a self-dual $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-module, annihilated by $\mathfrak{P}$, of dimension $2d$, say, over $\mathbf{F}_p$. We let G denote a finite quotient of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ through which the action on W factors. Since T_ℓ acts as $1+\ell$ on W, $(\ell \neq N)$, the Eichler-Shimura relations (§ 6) impose the relation:

$$\varphi_\ell^2-(1+\ell).\varphi_\ell+\ell=0$$

on the action of the Frobenius *automorphism* φ_ℓ $(\ell \neq N, p)$ on W. Thus, the only eigenvalues possible for the action of φ_ℓ on W are: 1 and ℓ. Since Cartier duality " interchanges " these eigenvalues, and since W has been devised to be self-dual under Cartier duality, it follows that the characteristic polynomial of φ_ℓ acting on W *must* be $(X-1)^d(X-\ell)^d$.

Now consider the $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-module $(\mathbf{Z}/p)^d \oplus (\mu_p)^d$, which we also regard as a G-module (the natural action on this module factors through G, and if it did not, we would have augmented G appropriately). It also has the property that the characteristic

(1) This has been proven independently by K. Ribet.

polynomial of φ_ℓ acting on it is: $(X-1)^d(X-\ell)^d$. By the Čebotarev theorem any element in G is the image of some φ_ℓ ($\ell \neq p$, N).

Thus, any element $g \in G$ has the same characteristic polynomial for the representation W as for $(\mathbf{Z}/p)^d \oplus (\mu_p)^d$. By the Brauer-Nesbitt theorem ([6], (30.16)), the semi-simplification of the representation W is isomorphic to (the already semi-simple) $(\mathbf{Z}/p)^d \oplus (\mu_p)^d$. Thus W has an admissible filtration and therefore, so does $J[\mathfrak{P}](\bar{\mathbf{Q}})$.

Proposition **(14.2).** — *Let* $\mathfrak{M}$ *be a prime which is not an Eisenstein prime, and which is supersingular if* $\operatorname{char} k_{\mathfrak{M}} = 2$. *Then* $J[\mathfrak{M}]$ *is an irreducible two-dimensional* $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$*-representation over* $k_{\mathfrak{M}}$ [1].

Proof. — By theorem (6.7) (and (3.2)) of [10], there is a unique semi-simple representation $\rho : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(k_{\mathfrak{M}})$ such that for every $\ell \neq p$, N, if $a_\ell = \text{image}(T_\ell) \subset k_{\mathfrak{M}}$:

$$\operatorname{Trace}(\varphi_\ell) = a_\ell$$
$$\det(\varphi_\ell) = \ell.$$

Denote by V the associated semi-simple $k_{\mathfrak{M}}[\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})]$-module. Let:

$$d = \dim_{k_{\mathfrak{M}}}(J[\mathfrak{M}](\bar{\mathbf{Q}})).$$

As in the previous proposition, form the $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-module W: the direct sum of $J[\mathfrak{M}](\bar{\mathbf{Q}})$ with its Cartier dual. Let $W' =$ the direct sum of d copies of V. By the Eichler-Shimura relations, the eigenvalues of φ_ℓ are constrained to be solutions of the quadratic equation $X^2 - a_\ell X + \ell = 0$, and since Cartier duality " interchanges the roots of the above equation " the characteristic polynomial of φ_ℓ operating on the self-dual $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-module W is: $(X^2 - a_\ell X + \ell)^d$.

But this is also the characteristic polynomial of φ_ℓ acting on the semi-simple $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-module W'. It follows that W' *is* the semi-simplification of W. By proposition (14.1) (and the fact that $\mathfrak{M}$ is not an Eisenstein prime) it follows that V is an irreducible $k_{\mathfrak{M}}[\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})]$-module. Therefore, W has a Jordan-Hölder filtration of sub-$k_{\mathfrak{M}}[\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})]$-modules all of whose successive quotients are isomorphic to V. It follows that $J[\mathfrak{M}](\bar{\mathbf{Q}})$ *also* has such a filtration. In particular, considering the first stage of such a filtration, we have an injection $V \subset J[\mathfrak{M}](\bar{\mathbf{Q}})$. We must prove that $V = J[\mathfrak{M}](\bar{\mathbf{Q}})$. We do this by studying $V_{/S} \subset J[\mathfrak{M}]_{/S}$, the quasi-finite group scheme extension of V.

Case 1. — $\operatorname{Char} k_{\mathfrak{M}} \neq N$ *and either*:

a) $\mathfrak{M}$ *supersingular or*

b) $\mathfrak{M}$ *ordinary and* $\operatorname{char} k_{\mathfrak{M}} \neq 2$.

---

[1] We also establish (cf. (16.3) below) that $J[\mathfrak{P}]$ is a 2-dimensional $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-representation, when $\mathfrak{P}$ is an Eisenstein prime.

Here we make use of the contravariant Dieudonné module functor of Oda [47], denoted $M(-)$. Its relation to De Rham cohomology is given by corollary (5.11) of [47]. Namely, if A is an abelian variety over a perfect field k, of characteristic p then there is a functorial isomorphism of Dieudonné modules:

$$M(A[p]) \overset{\psi}{\underset{\approx}{\rightarrow}} H^1_{DR}(A_{/k}).$$

Moreover, under ψ, the Hodge filtration:

$$0 \to H^0(A, \Omega^1) \to H^1_{DR}(A_{/k}) \to H^1(A, \mathcal{O}_A) \to 0$$

corresponds to the filtration:

$$0 \to M(A[\mathrm{Frob}])' \to M(A[p]) \to M(A[\mathrm{Ver}]) \to 0$$

where [ ] means, as usual, kernel, Frob means the *Frobenius* endomorphism, Ver means the *Verschiebung*, and the prime superscript has the following significance:

$$M(A[\mathrm{Frob}])' = (k, \sigma^{-1}) \otimes_k M(A[\mathrm{Frob}])$$

where (k, σ^{-1}) is the abelian group k, regarded as k-algebra by the morphism $k^{\sigma^{-1}} \to k$ where σ is the p-th power map.

Moreover:

$$M(A[p])[\mathrm{Frob}] = \mathrm{Ver}.M(A[p]) \cong M(A[\mathrm{Frob}])'$$

where Ver and the first Frob denote the V and F operators of the Dieudonné module $M(A[p])$.

If G is a finite group scheme over k equipped with a homomorphism:

$$\mathbf{T}/p\mathbf{T} \to \mathrm{End}(G_{/k}),$$

we induce a $\mathbf{T}/p\mathbf{T}$-module structure on $M(G)$ commuting with its module-structure over the Dieudonné ring. Since $M(-)$ is an exact contravariant functor, we have $M(G)/\mathfrak{M}.M(G) = M(G[\mathfrak{M}])$.

Consequently:

$$\begin{aligned} M(J[\mathfrak{M}]_{/\mathbf{F}_p}) &= M(J[p]_{/\mathbf{F}_p})/\mathfrak{M}.M(J[p]_{/\mathbf{F}_p}) \\ &= H^1_{DR}(J_{/\mathbf{F}_p})/\mathfrak{M}.H^1_{DR}(J_{/\mathbf{F}_p}) \cong H^1_{DR}(X_0(N)_{/\mathbf{F}_p})/\mathfrak{M}.H^1_{DR}(X_0(N)_{/\mathbf{F}_p}) \end{aligned}$$

where the last isomorphism comes by the identification of J with the Albanese of $X_0(N)$, and all isomorphisms are isomorphisms of $\mathbf{T}/p\mathbf{T}$-Dieudonné modules. Make these abbreviations: $M(V_{/\mathbf{F}_p}) = M$; $H^1_{DR}(X_0(N)_{/\mathbf{F}_p}) = H^1_{DR}$.

The inclusion $V_{/\mathbf{F}_p} \subset J[\mathfrak{M}]_{/\mathbf{F}_p}$ induces a surjection of the $k_{\mathfrak{M}}$-Dieudonné modules:

$$H^1_{DR}/\mathfrak{M}.H^1_{DR} \to M \to 0.$$

Passing to the cokernel of Verschiebung, one has a diagram:

$$\begin{array}{ccccc} H^1_{DR}/\mathfrak{M}.H^1_{DR} & \longrightarrow & M & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow \\ H^1(\mathcal{O}_X)/\mathfrak{M}.H^1(\mathcal{O}_X) & \longrightarrow & M/\mathrm{Ver}.M & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \\ 0 & & 0 & & \end{array}$$

where we have written $H^1(\mathcal{O}_X)$ for $H^1(X_0(N)_{/\mathbf{F}_p}, \mathcal{O})$.

By (9.4), $H^1(\mathcal{O}_X)/\mathfrak{M}.H^1(\mathcal{O}_X)$ is a $k_{\mathfrak{M}}$-vector space of dimension 1. Thus:

(14.3) $\qquad \dim_{k_{\mathfrak{M}}}(M/\mathrm{Ver}.M) \leq 1.$

We now use the hypothesis that either $\mathfrak{M}$ is supersingular or the characteristic of $k_{\mathfrak{M}}$ is different from 2.

Lemma **(14.4)**. — *With the above hypotheses,* $V_{/S'}$ *is an auto-dual finite flat group scheme with respect to Cartier duality. Neither* Frob *nor* Ver *vanish identically, nor are they isomorphisms, on the Dieudonné module* M.

Proof. — The $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-module V is auto-dual under Cartier duality. Therefore $V_{/S'}$ and its Cartier dual $V^{\vee}_{/S'}$ have isomorphic associated $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules. Under our hypotheses, Fontaine's theorem, chapter I (1.4), applies. Thus $V_{/S'}$ is auto-dual.

Consequently, M is a self-dual Dieudonné module. Since $\mathrm{Frob}.\mathrm{Ver} = p = 0$ on M, it is clear that not *both* Frob and Ver can be automorphisms of M, and by self-duality, *neither* are. Also, by self-duality, if one of the two operators Frob and Ver are identically zero, then both are.

In particular, Ver would be zero, which is impossible, since its cokernel is of dimension less than or equal to 1 by (14.3).

An immediate consequence of Lemma (14.4) and (14.3) is:

Lemma **(14.5)**. — $H^1(\mathcal{O}_X)/\mathfrak{M}.H^1(\mathcal{O}_X) \to M/\mathrm{Ver}.M$ *is an isomorphism of* 1*-dimensional* $k_{\mathfrak{M}}$*-vector spaces.*

Lemma **(14.6)**. — *Let* $0 \to M_1 \to M_2 \to M_3 \to 0$ *be a short exact sequence of (finite)* $k_{\mathfrak{M}}$*-Dieudonné modules satisfying these properties*:

a) *the cokernel of* Ver *on* M_2 *is of dimension* 1 *over* $k_{\mathfrak{M}}$;

b) Frob *is nonzero on* M_3.

Then Ver *is an* isomorphism *of* M_1 *onto itself.*

Proof. — We show that $\mathrm{Ver} : M_1 \to M_1$ is surjective, by showing:

(i) $M_2/\mathrm{Ver}.M_2 \to M_3/\mathrm{Ver}.M_3$ is *injective,*

(ii) $M_2[\mathrm{Ver}] \to M_3[\mathrm{Ver}]$ is *surjective.*

and applying the snake-lemma. Since the morphism (i) is surjective, and $M_2/\mathrm{Ver}.M_2$ is of dimension 1 over $k_{\mathfrak{M}}$, it suffices to show that $\mathrm{Ver}.M_3 \neq M_3$ to obtain injectivity of (i). But Ver annihilates $\mathrm{Frob}.M_3$ which is nonzero, by b). Therefore Ver is not an automorphism of M_3.

To show (ii), note first that since M_i is finite-dimensional over $k_{\mathfrak{M}}$ ($i=2, 3$), $\dim_{k_{\mathfrak{M}}}(M_2[\mathrm{Ver}])=1$ (as follows from a)); also $\dim_k(M_3[\mathrm{Ver}])=1$ (as follows from the isomorphism (i)). Therefore all that must be shown is that the morphism (ii) is nonzero. But this follows from the diagram:

$$\begin{array}{ccccc} M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \\ M_2[\mathrm{Ver}] & \xrightarrow[\text{(ii)}]{} & M_3[\mathrm{Ver}] & & \end{array}$$

and hypothesis b).

To apply lemma (14.6) to our situation, take $M_2 = H^1_{DR}/\mathfrak{M}.H^1_{DR}$ and $M_3 = M$. Both hypotheses a) and b) hold, by lemmas (14.4) and (14.5). We obtain the following conclusion: If M_1 is the kernel of the homomorphism $H^1_{DR}/\mathfrak{M}.H^1_{DR} \to M$, then Ver is an isomorphism on M_1. That is, M_1 is the Dieudonné module of a group scheme of multiplicative type. Therefore the cokernel of $V_{/S'} \subset J[\mathfrak{M}]_{/S'}$ has multiplicative type reduction in characteristic p. But, by the discussion at the beginning of this proof, and by Fontaine's theorem, this cokernel has a filtration by finite flat subgroup schemes all of whose nontrivial successive quotients are isomorphic to $V_{/S'}$, which does not have multiplicative type reduction in characteristic p. We conclude that this cokernel is zero.

Case 2. — (A digression) $\mathfrak{M}$ ordinary and char $k_{\mathfrak{M}} \neq N$.

There is another more direct way of putting the above argument, when $\mathfrak{M}$ is ordinary. This alternate method does not use Dieudonné modules, but rather depends upon an important isomorphism due to Cartier and Serre ([64], § 11, Prop. 10). By means of this isomorphism, one may deduce (14.8) below, which will also be useful to us in the case where $\mathfrak{M}$ is an Eisenstein prime (cf. (14.9), (14.10)). Thus, in the present case we let $\mathfrak{M}$ be *any* ordinary prime in **T**, Eisenstein or not, with char $k_{\mathfrak{M}} \neq N$. Recall the canonical isomorphism:

$$\delta : J[p](\overline{\mathbf{F}}_p) \to H^0(X_0(N)_{/\overline{\mathbf{F}}_p}, \Omega^1)^{\mathscr{C}}$$

of [64], § 11, Prop. 10, where the superscript $\mathscr{C}$ means fixed elements under the Cartier operator. (Note: this isomorphism is defined for any smooth projective curve and not just $X_0(N)$.) The definition of δ is as follows: an element x of the domain is represented by a divisor D on $X_0(N)_{/\overline{\mathbf{F}}_p}$ such that $p.D=(f)$. One takes $\delta(x)=df/f$.

Proposition **(14.7).** — *The isomorphism above induces an injection:*

$$\delta : (J[p](\overline{\mathbf{F}}_p)) \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p \hookrightarrow H^0(X_0(N)_{/\overline{\mathbf{F}}_p}, \Omega^1)$$

which commutes with the action of $\mathbf{T}/p.\mathbf{T}$ *on domain and range.*

Proof. — By ([64], § 11, Prop. 10) injectivity follows from injectivity of the natural map:

$$(H^0(X_0(N), \Omega^1)^{\mathscr{C}}) \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p \to H^0(X_0(N)_{/\overline{\mathbf{F}}_p}, \Omega^1)$$

which is an elementary exercise, using σ^{-1}-linearity of $\mathscr{C}$: Let $x_1, \ldots, x_s$ be the smallest number $(s>0)$ of $\mathbf{F}_p$-linearly independent elements of $H^0(X_0(N), \Omega^1)^{\mathscr{C}}$ such that $x_1+\lambda_2.x_2+\ldots+\lambda_s.x_s=0$, where $\lambda_j \in \overline{\mathbf{F}}_p$. Applying $1-\mathscr{C}$ to this equation gives a smaller relation.

That δ commutes with the action of w is evident. To check that it commutes with T_ℓ boils down, in the end, to checking commutativity of the (two) squares:

$$\begin{array}{ccc} L^* & \xrightarrow{d\log} & \Omega^1_{L/\overline{\mathbf{F}}_p} \\ {\scriptstyle i}\uparrow\downarrow{\scriptstyle N_{L/K}} & & {\scriptstyle i}\uparrow\downarrow{\scriptstyle \mathrm{Tr}_{L/K}} \\ K^* & \xrightarrow[d\log]{} & \Omega^1_{K/\overline{\mathbf{F}}_p} \end{array}$$

where K is a function field in one variable over $\overline{\mathbf{F}}_p$ and L is a finite K-algebra.

Corollary **(14.8).** — *Let* $\mathfrak{M}$ *be an ordinary prime ideal in* $\mathbf{T}$ *with* $\mathrm{char}\, k_{\mathfrak{M}} \neq N$. *Let* $(J[p]_{/\overline{\mathbf{F}}_p})^{\text{ét}}$ *denote the étale part of the group scheme* $J[p]_{/\overline{\mathbf{F}}_p}$, *and let* $(J[p]^{\text{ét}}_{/\overline{\mathbf{F}}_p})[\mathfrak{M}]$ *denote the kernel of the ideal* $\mathfrak{M}$ *in this group scheme. Then* $(J[p]^{\text{ét}}_{/\overline{\mathbf{F}}_p})[\mathfrak{M}]$ *is a* $k_{\mathfrak{M}}$*-vector group scheme of rank* 1. *One has the* equality:

$$J[\mathfrak{M}]^{\text{ét}}_{/\overline{\mathbf{F}}_p} = (J[p]^{\text{ét}}_{/\overline{\mathbf{F}}_p})[\mathfrak{M}] \quad \textit{if} \quad p>2.$$

Proof. — The rank of $(J[p]^{\text{ét}}_{/\overline{\mathbf{F}}_p})[\mathfrak{M}]$ is at most 1 as follows immediately from the previous proposition and proposition (9.3). To obtain the equality asserted, we must show that $J[\mathfrak{M}]^{\text{ét}}_{/\overline{\mathbf{F}}_p}$ is nontrivial. If it were trivial, then $J[\mathfrak{M}]_{/\overline{\mathbf{F}}_p}$ would be of multiplicative type. Since $p>2$, Fontaine's theorem, and the remarks at the beginning of this section, apply, giving us that any constituent of $J[\mathfrak{M}^r]_{/\overline{\mathbf{F}}_p}$ is a constituent of $J[\mathfrak{M}]_{/\overline{\mathbf{F}}_p}$. It would then follow that the p-divisible (Barsotti-Tate) group $J_{\mathfrak{M}/\overline{\mathbf{F}}_p}$ is of multiplicative type, which is impossible, since it is auto-dual under Cartier duality.

If p divides n, let $J_p[\mathfrak{I}]_{/S}$ denote (as usual) the group scheme extension to S of the kernel of the Eisenstein ideal $\mathfrak{I}$ in the Barsotti-Tate group $J_{p/\mathbf{Q}}$. This group scheme is also $J[\mathfrak{I}, p^f]_{/S}$ where $p^f \| n$. Let $C_{p/S}$ denote the p-primary component of the cuspidal subgroup C (regarded as constant group over S). If $p=2$, let $D_{/S}$ denote the subgroup scheme of $J_{/S}$ constructed in § 12.

Proposition **(14.9)**. — *If p is an odd prime dividing n, then*:

$$C_{p/\mathbf{F}_p} = (J_p[\mathfrak{I}]_{/\mathbf{F}_p})^{\text{ét}} = (J^{\text{ét}}_{p/\mathbf{F}_p})[\mathfrak{I}]$$

and, if $p=2$, divides n:

$$D^{\text{ét}}_{/\mathbf{F}_2} = J[\mathfrak{P}]^{\text{ét}}_{/\mathbf{F}_2} = (J^{\text{ét}}_{2/\mathbf{F}_2})[\mathfrak{P}].$$

Remarks and proof. — The right-hand group scheme on the first line of our proposition is the kernel of $\mathfrak{I}$ in the étale part of the p-Barsotti-Tate group over $\mathbf{F}_p$ associated to J. All of the asserted *equalities* of the proposition are known *inclusions* (reading from left to right).

To establish the proposition, note that Corollary (14.8) gives that:

$$(J^{\text{ét}}_{p/\mathbf{F}_p})[\mathfrak{P}] = (J[p]^{\text{ét}}_{/\mathbf{F}_p})[\mathfrak{P}]$$

is a group scheme of order p. The assertion of the proposition for $p=2$ then follows simply by noting that $(D_{/\mathbf{F}_2})^{\text{ét}}$ is also a group scheme of order p. To obtain the assertion when $p>2$, let $p^f \| n$. Note that $(J^{\text{ét}}_{p/\mathbf{F}_p})[\mathfrak{I}]$ is annihilated by p^f by (9.7), and since the kernel of multiplication by p in this group scheme is of order p, it follows that $(J^{\text{ét}}_{p/\mathbf{F}_p})[\mathfrak{I}]$ is of order p^f. So is C_p, by (11.1). The proposition follows.

Corollary **(14.10)**. — *If p is an odd prime dividing n, then one has a short exact sequence*:

(i) $$0 \to C_p \to J_p[\mathfrak{I}] \to M \to 0 \quad (\textit{over } S)$$

where M *is an admissible group scheme of* multiplicative type.

If $p=2$ divides n, then one has a short exact sequence:

(ii) $$0 \to D \to J[\mathfrak{P}] \to M \to 0 \quad (\textit{over } S)$$

where M *is an admissible group scheme of* multiplicative type.

Proof. — In either of the exact sequences above, the cokernel is admissible by (14.1), and of multiplicative type by the previous proposition.

Corollary **(14.11)**. — *Let p be a prime dividing n. Let* W *denote the $\mathbf{Z}_p$-dual of $\mathscr{Ea}(J_{\mathfrak{P}}(\overline{\mathbf{F}}_p))$. The $\mathbf{T}_{\mathfrak{P}}$-module* W *is free of rank* 1.

Proof. — By proposition (8.4) it is of rank 1 (*i.e.* $W \otimes \mathbf{Q}$ is free of rank 1 over $\mathbf{T}_{\mathfrak{P}} \otimes \mathbf{Q}$). It suffices to show that $W/\mathfrak{P}.W$ is of order p. But (§ 7) W is the Pontrjagin dual of $J_{\mathfrak{P}}(\overline{\mathbf{F}}_p)$ and therefore we must show that $J_{\mathfrak{P}}(\overline{\mathbf{F}}_p)[\mathfrak{P}]$ is of order p, which follows from (14.9).

As for the *alternate argument*: suppose $\mathfrak{M}$ is ordinary, not an Eisenstein prime, and such that char $k_{\mathfrak{M}} \neq N, 2$. By Fontaine's theorem, and the discussion at the beginning of this section, $V_{/\mathbf{F}_p}$ cannot be of multiplicative type. Thus, the $k_{\mathfrak{M}}$-rank of $(V_{/\mathbf{F}_p})^{\text{ét}}$ is ≥ 1, and (by (14.8)) the $k_{\mathfrak{M}}$-rank of $(J[\mathfrak{M}]_{/\mathbf{F}_p})^{\text{ét}}$ is ≤ 1. It follows that $V = J[\mathfrak{M}]$.

Case 3. — Char $k_{\mathfrak{M}} = N$.

This case parallels the " alternate argument " in case 2. Note that if char $k_{\mathfrak{M}} = N$, then $\mathfrak{M}$ is not an Eisenstein prime. Also, $J[\mathfrak{M}]_{/S'}$ is a finite *étale* group scheme, admitting a Jordan-Hölder filtration by finite étale subgroup schemes all successive quotients being isomorphic to the finite étale group scheme $V_{/S'}$. Consider the first layer in such a filtration $V \subset J[\mathfrak{M}]$, and note that we have exact sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J[\mathfrak{M}]^0(\bar{\mathbf{Q}}_N) & \longrightarrow & J[\mathfrak{M}](\bar{\mathbf{Q}}_N) & \longrightarrow & J[\mathfrak{M}](\bar{\mathbf{F}}_N) & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & V^0(\bar{\mathbf{Q}}_N) & \longrightarrow & V(\bar{\mathbf{Q}}_N) & \longrightarrow & V(\bar{\mathbf{F}}_N) & \longrightarrow & 0 \end{array}$$

where the superscript ^{0} may be viewed as denoting either the connected component over Spec $\mathbf{Z}_N$, or the intersection of the (appropriate) group scheme over Spec $\mathbf{Z}_N$ with $J^0_{/\mathbf{Z}_N}$.

Since V is self-dual, we cannot have $V(\bar{\mathbf{Q}}_N) = V^0(\bar{\mathbf{Q}}_N)$ (for then it would be of multiplicative type over $\mathbf{F}_N$). Therefore $\dim_{k_{\mathfrak{M}}}(V(\bar{\mathbf{F}}_N)) \geq 1$. As in case 2, we must show $\dim_{k_{\mathfrak{M}}} J[\mathfrak{M}](\bar{\mathbf{F}}_N) \leq 1$. For this, we extend Serre's mapping δ to cover our present case. Let D represent a divisor class x in $J[N](\bar{\mathbf{Q}}_N) = \mathrm{Pic}^0(X_0(N)_{/\bar{\mathbf{Q}}_N})[N]$. Assume D is an *eigenvector* for w. Let f be a rational function on $M_0(N)_{/\bar{\mathbf{Z}}_N}$ ($\bar{\mathbf{Z}}_N$ = ring of integers in $\bar{\mathbf{Q}}_N$) such that $(f) = N.D$ on $X_0(N)_{/\bar{\mathbf{Q}}_N}$, and such that f does not vanish identically on $M_0(N)_{/\bar{\mathbf{F}}_N}$. Since f satisfies an equation of the type $f \circ w = \pm f^{\pm 1}$, and w interchanges the two irreducible components of $M_0(N)_{/\bar{\mathbf{F}}_N}$, f vanishes on neither component of $M_0(N)_{/\bar{\mathbf{F}}_N}$. Form df/f in $H^0(M_0(N)^h_{/\bar{\mathbf{Z}}_N}, \Omega^1)$ where the superscript h denotes the smooth locus. Note that:

$$H^0(M_0(N)^h_{/\bar{\mathbf{Z}}_N}, \Omega^1) = H^0(M_0(N)_{/\bar{\mathbf{Z}}_N}, \Omega) = H^0(X_0(N)_{/\bar{\mathbf{Z}}_N}, \Omega)$$

(the second equality comes from (3.4); for the first, since $M_0(N)$ is Cohen-Macaulay, Ω is invertible, and the supersingular points of characteristic N are of codimension 2 in $M_0(N)_{/\bar{\mathbf{Z}}_N}$).

Set $\delta(x)$ = image of df/f in $H^0(X_0(N)_{/\bar{\mathbf{F}}_N}, \Omega)$.

Since the function f is unique up to a possible multiple $u.g^N$ where u is a unit in $\bar{\mathbf{Z}}_N$ and g is a rational function on $M_0(N)_{/\bar{\mathbf{Z}}_N}$, the mapping $x \mapsto \delta(x)$ is well-defined. Also, $\delta(x) = 0$ if and only if f, reduced modulo N, is an N-th power (or, equivalently, x goes to zero in $J[N](\bar{\mathbf{F}}_N)$). Extending the definition of δ, by linearity, to all divisor classes $x \in J[N](\bar{\mathbf{Q}}_N)$, we have:

$$\delta : J[N](\bar{\mathbf{F}}_N) \hookrightarrow H^0(X_0(N)_{/\bar{\mathbf{F}}_N}, \Omega).$$

Since the theory of the Cartier operator ([64], § 10) is local, it applies to the smooth quasi-projective curve $X_0(N)^h_{/\overline{\mathbf{F}}_N}$ and one has, as before, that the image of δ is *contained* in the fixed part: $H^0(X_0(N)^h_{/\overline{\mathbf{F}}_N}, \Omega^1)^{\mathscr{C}}$, and by the argument of (14.7), one deduces an injection:

$$\delta : J[N](\overline{\mathbf{F}}_N) \otimes_{\mathbf{F}_N} \overline{\mathbf{F}}_N \hookrightarrow H^0(X_0(N)_{/\overline{\mathbf{F}}_N}, \Omega).$$

At this point one uses (9.3) as in the proof of (14.8) to conclude that:

$$\dim_{k_{\mathfrak{M}}} J[\mathfrak{M}](\overline{\mathbf{F}}_N) \leq 1.$$

What is the minimal field of definition of the $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ representation determined by $J[\mathfrak{M}]$?

Proposition **(14.12).** — *Let $\mathfrak{M}$ be a prime which is not an Eisenstein prime, and which is supersingular if* $\operatorname{char} k_{\mathfrak{M}} = 2$.

Then $k_{\mathfrak{M}}$ is generated over $\mathbf{F}_p$ by the images of the operators T_ℓ $(\ell \neq \operatorname{char} k_{\mathfrak{M}})$, and $J[\mathfrak{M}]$ is an irreducible $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$*-module.*

Proof. — Before we begin the proof, let us note that the last assertion is stronger than the assertion of Proposition (14.2).

We are saying that the *abelian group* $J[\mathfrak{M}](\overline{\mathbf{Q}}) = V$ is irreducible as $\mathbf{F}_p[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module. Let E be the image of $\mathbf{F}_p[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$ in the endomorphism ring of $J[\mathfrak{M}](\overline{\mathbf{Q}})$. Let $k \subset k_{\mathfrak{M}}$ be the subfield generated by the T_ℓ (for all $\ell \neq p$, N). Using the Eichler-Shimura relations for $J[\mathfrak{M}]_{/\mathbf{F}_\ell}$ and the fact that $J[\mathfrak{M}]$ is *étale* in characteristic $\ell \neq p$, N, we obtain a natural imbedding of k in the center of the ring E, which we therefore view as k-algebra; in fact we take k systematically as our base field. Note that $k_{\mathfrak{M}} = k[\tau_p]$ ($\tau_p = \text{image } T_p$), if $p \neq N$. If $p = N$ then $k = k_{\mathfrak{M}}$.

Let V_1 be a two-dimensional $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-representation over k such that $V_1 \otimes_k k_{\mathfrak{M}} = V$. Such a representation exists by [10], Theorem (6.7).

Viewing $V_1 \subset V$ as sub-Galois module, and taking the subgroup scheme extension (Chap. I, § 1 *(c)*) of V_1 in $V_{/S} = J[\mathfrak{M}]_{/S}$, we obtain a closed ($k$-vector space) subgroup scheme $V_{1/S} \subset V_{/S}$.

Let $V_1 \otimes_k k_{\mathfrak{M}/S}$ denote the associated $k_{\mathfrak{M}}$-vector group scheme, which one can "construct" simply by taking:

$$V_{1/S} \oplus \tau_p . V_{1/S} \oplus \tau_p^2 . V_{1/S} \oplus \ldots \oplus \tau_p^{d-1} . V_{1/S}$$

where $d = [k_{\mathfrak{M}} : k]$, and giving it the natural $k_{\mathfrak{M}}$-structure.

We have a homomorphism of $k_{\mathfrak{M}}$-vector group schemes:

$$V_1 \otimes_k k_{\mathfrak{M}/S} \to V_{/S}$$

which is an isomorphism on associated Galois modules. Since, by our hypothesis, Fontaine's theorem (chap. I (1.4)) applies, this is an *isomorphism of group schemes over* S', and hence also when restricted to characteristic p. Note that *over* $\mathbf{F}_p$, the endomorphism

Frob $+$Ver preserves the above direct sum decomposition. By the Eichler-Shimura relations, T_p must also preserve the above direct sum decomposition (over $\mathbf{F}_p$), which is possible only if $d=1$. The proposition follows.

Proposition **(14.13).** — *Let* $\mathfrak{M}$, $\mathfrak{M}'$ *be primes such that* $\operatorname{char} k_{\mathfrak{M}} = \operatorname{char} k_{\mathfrak{M}'} \neq 2$ *or:* $\mathfrak{M}$ *and* $\mathfrak{M}'$ *are supersingular.*

Then the $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$*-modules* $J[\mathfrak{M}](\bar{\mathbf{Q}})$ *and* $J[\mathfrak{M}'](\bar{\mathbf{Q}})$ *are isomorphic if and only if* $\mathfrak{M}=\mathfrak{M}'$.

Proof. — By (14.1) we may suppose neither prime is an Eisenstein prime. Suppose $J[\mathfrak{M}](\bar{\mathbf{Q}})$ and $J[\mathfrak{M}'](\bar{\mathbf{Q}})$ are isomorphic as $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-modules. By Fontaine's theorem $J[\mathfrak{M}]_{/S'}$ is isomorphic to $J[\mathfrak{M}']_{/S'}$, and the Eichler-Shimura relations together with Proposition (14.12) enable us to get an isomorphism $k_{\mathfrak{M}} \overset{\approx}{\underset{i}{\to}} k_{\mathfrak{M}'}$ such that if τ_ℓ is the image of T_ℓ in $k_{\mathfrak{M}}$ (resp. $\tau'_\ell =$ image of T_ℓ in $k_{\mathfrak{M}'}$) then $i(\tau_\ell)=\tau'_\ell$ for all $\ell \neq N$. To show that $\mathfrak{M}=\mathfrak{M}'$, it suffices to show that w has the same image in $k_{\mathfrak{M}}$ as it does in $k_{\mathfrak{M}'}$. Suppose not (*i.e.* w goes to $+1$ in $k_{\mathfrak{M}}$ and -1 in $k_{\mathfrak{M}'}$). Then consider the q-expansions of generating eigenvectors (§ 9) in $H^0(X_0(N)_{/k}, \Omega)[\mathfrak{M}]$ and in $H^0(X_0(N)_{/k}, \Omega)[\mathfrak{M}']$.

These q-expansions are the *same* except for the coefficients of powers of q^N. Applying (4.10), (5.9), (5.10) to the difference of these generating eigenvectors, we obtain that the generating eigenvectors are equal. Therefore $\mathfrak{M}=\mathfrak{M}'$.

15. The Gorenstein condition.

Let R be a local $\mathbf{Z}_p$-algebra, free of finite rank as a module over $\mathbf{Z}_p$. Then R is a *Gorenstein ring* [3] if and only if the $\mathbf{Z}_p$-dual to R, $R^* = \mathrm{Hom}_{\mathbf{Z}_p}(R, \mathbf{Z}_p)$, is free (of rank 1) as a module over R.

Lemma **(15.1).** — *Let* $\mathfrak{M} \subset \mathbf{T}$ *be a maximal ideal. We have the indicated implications of the assertions below:*

1) $J[\mathfrak{M}](\bar{\mathbf{Q}})$ *is of dimension* 2 *over* $k_{\mathfrak{M}}$.

$\Updownarrow$

2) $\mathscr{T}a(J_{\mathfrak{M}}(\bar{\mathbf{Q}}))$ *is free of rank* 2 *over* $\mathbf{T}_{\mathfrak{M}}$.

$\Downarrow$

3) $\mathbf{T}_{\mathfrak{M}}$ *is a Gorenstein ring.*

$\Updownarrow$

4) $H^0(X_0(N)_{/\mathbf{Z}_p}, \Omega) \otimes_{\mathbf{T}} \mathbf{T}_{\mathfrak{M}}$ *is free of rank* 1 *over* $\mathbf{T}_{\mathfrak{M}}$.

Proof. — 1) $\Rightarrow$ 2): Assuming 1) we have that the kernel of $\mathfrak{M}$ in $J_{\mathfrak{M}}(\bar{\mathbf{Q}})$ is of dimension two over $k_{\mathfrak{M}}$. Hence the cokernel of $\mathfrak{M}$ in $\mathrm{Hom}(J_{\mathfrak{M}}(\bar{\mathbf{Q}}), \mathbf{Q}_p/\mathbf{Z}_p) = H^*_{\mathfrak{M}}$ is also of dimension two. But $H^*_{\mathfrak{M}}$ is the $\mathbf{Z}_p$-dual of the Tate group (cf. § 7):

$$\mathscr{T}a(J_{\mathfrak{M}}(\bar{\mathbf{Q}})) = H_1(X_0(N)_{\mathbf{C}}, \mathbf{Z}) \otimes_{\mathbf{T}} \mathbf{T}_{\mathfrak{M}} = H_{\mathfrak{M}}.$$

Since $H_{\mathfrak{M}}$ is its own $\mathbf{Z}_p$-dual, we have that $H_{\mathfrak{M}} \otimes_{\mathbf{T}_{\mathfrak{M}}} k_{\mathfrak{M}}$ is of dimension two. But since (7.7) $H_{\mathfrak{M}} \otimes \mathbf{Q}$ is free of rank two over $\mathbf{T}_{\mathfrak{M}} \otimes \mathbf{Q}$, it follows that for any homomorphism $\mathbf{T}_{\mathfrak{M}} \to K$ (where K is any field) $H_{\mathfrak{M}} \otimes_{\mathbf{T}_{\mathfrak{M}}} K$ is of dimension two, and $H_{\mathfrak{M}}$ is therefore free of rank 2 over $\mathbf{T}_{\mathfrak{M}}$.

2) $\Rightarrow$ 3): Write $H_{\mathfrak{M}} = F_1 \oplus F_2$, the direct sum of two free $\mathbf{T}_{\mathfrak{M}}$-modules of rank 1. Since $H_{\mathfrak{M}} = H_{\mathfrak{M}}^*$ (* denotes $\mathbf{Z}_p$-dual) we have an isomorphism $F_1^* \oplus F_2^* \to F_1 \oplus F_2$.

Consider the four projections $\pi_{i,j} : F_i^* \to F_j$ $(i, j = 1, 2)$. At least one is a surjection, for if not the image of $\pi_{i,j}$ would be contained in the maximal proper submodule $\mathfrak{M} \cdot F_j$ for all i, j, contradicting our isomorphism.

Suppose $\pi_{i,j} : F_i^* \to F_j$ is surjective. It is also injective since it induces an isomorphism after tensoring with $\mathbf{Q}$, and the domain is $\mathbf{Z}$-torsion free. Thus, F_i is a free $\mathbf{T}_{\mathfrak{M}}$-module of rank 1, whose $\mathbf{Z}$-dual is also free and therefore $\mathbf{T}_{\mathfrak{M}}$ is Gorenstein.

3) $\Leftrightarrow$ 4): By (9.4) $H^1(X_0(N)_{/\mathbf{Z}_p}, \mathcal{O}) \otimes_{\mathbf{T}} \mathbf{T}_{\mathfrak{M}}$ is free of rank 1 over $\mathbf{T}_{\mathfrak{M}}$, and using the idempotents $\varepsilon_{\mathfrak{M}}$, $\varepsilon'_{\mathfrak{M}}$ of (7.1), and the fact that $\mathbf{T}$ act in a hermitian manner with respect to the duality (3.2) one sees that $H^0(X_0(N)_{/\mathbf{Z}}, \Omega) \otimes_{\mathbf{T}} \mathbf{T}_{\mathfrak{M}}$ is its $\mathbf{Z}_p$-dual.

2) $\Rightarrow$ 1): An easy reversal of the argument that 1) $\Rightarrow$ 2).

Corollary **(15.2).** — *Let $\mathfrak{M}$ be a maximal ideal in $\mathbf{T}$ which is not an Eisenstein prime, and such that, if* $\operatorname{char} k_{\mathfrak{M}} = 2$, *then $\mathfrak{M}$ is supersingular.*

Then all four assertions of (15.1) *hold and in particular $\mathbf{T}_{\mathfrak{M}}$ is a Gorenstein ring.*

Remark. — In the next two sections, we shall establish this Corollary for Eisenstein primes as well. This is significantly harder. We shall have use for the following (elementary) sufficient condition for Gorenstein-ness.

Proposition **(15.3).** — *If* $R = \mathbf{Z}_p[\eta]$ *is generated by* one *element over* $\mathbf{Z}_p$, *then* R *is Gorenstein* [3].

16. Eisenstein primes (mainly $p \neq 2$).

Fix p a prime number dividing n.

Definition. — *A prime number $\ell \neq N$ will be called* good (relative to the pair (p, N), *usually unmentioned and understood) if either*:

a) *not both ℓ and p are equal to* 2, *and*

(i) *ℓ is not a p-th power modulo* N *and*

(ii) $\dfrac{\ell - 1}{2} \not\equiv 0 \bmod p$

or (the somewhat special "degenerate" case):

b) $\ell = p = 2$, *and* 2 *is not a quartic residue modulo* N.

The set of good primes has Dirichlet density $\left(\frac{p-2}{p-1}\right)$ if $p>2$, and $\frac{1}{4}$ if $p=2$. In particular, there are some good primes.

For any ℓ set $\eta_\ell = 1+\ell-T_\ell$.

The object of this section and the next is to establish the following proposition and to derive some important consequences:

Proposition **(16.1)**. — *The Eisenstein prime* $\mathfrak{P}.\mathbf{T}_\mathfrak{P} \subset \mathbf{T}_\mathfrak{P}$ *is generated by the elements* p *and* η_ℓ, *where* ℓ *is any good prime* [1].

Although some finer consequences of the above proposition will be developed later, note these corollaries.

Corollary **(16.2)**. — *The* $\mathbf{Z}_p$*-algebra* $\mathbf{T}_\mathfrak{P}$ *is generated by* η_ℓ *for* ℓ *any good prime.*

Therefore, by (15.3):

Corollary **(16.3)**. — *The ring* $\mathbf{T}_\mathfrak{P}$ *is Gorenstein. The* $\mathbf{F}_p$*-vector group* $J[\mathfrak{P}]$ *is two-dimensional. If* $p>2$, *then*:

$$J[\mathfrak{P}] = C[p] \oplus \Sigma[p].$$

If $p=2$, *then* $J[\mathfrak{P}] = D$.

The $\mathbf{T}_\mathfrak{P}$*-module* $H_\mathfrak{P} = \mathcal{E}a(J_\mathfrak{P}(\overline{\mathbf{Q}}))$ *is free of rank* 2.

Corollary **(16.4)**. — *If* $p>2$, $J_p[\mathfrak{I}] = J_\mathfrak{P}[\mathfrak{I}] = C_p \oplus \Sigma_p$ (*recall*: $C_p = p$*-primary component of* C, *and the same for* Σ_p).

Proof. — $C_p \oplus \Sigma_p$ is contained in $J_\mathfrak{P}[\mathfrak{I}]$ ((11.1), (11.7)).

But $J_\mathfrak{P}[\mathfrak{I}](\overline{\mathbf{Q}})$ is the Pontrjagin dual of $H^*_\mathfrak{P}/\mathfrak{I}.H^*_\mathfrak{P}$ (* means $\mathbf{Z}_p$-dual) and therefore, by the previous corollary, it has the same order as $C_p(\overline{\mathbf{Q}}) \oplus \Sigma_p(\overline{\mathbf{Q}})$.

We begin by establishing a lemma needed to control the action of inertia.

Lemma **(16.5)**. — *Let* B *be a subgroup of either the cuspidal or the Shimura subgroup of* J. *If the superscript* ^{1} *denotes the module of fixed elements under the action of inertia, we have an exact sequence*:

$$0 \to B \to J_p(\overline{\mathbf{Q}}_N)^1 \to (J_p(\overline{\mathbf{Q}}_N)/B)^1 \to 0$$

(*where* J_p *is the p-divisible (Barsotti-Tate) group associated to* J).

Proof. — What must be shown is that $J_p(\overline{\mathbf{Q}}_N) \to J_p(\overline{\mathbf{Q}}_N)/B$ induces a surjection on elements fixed under inertia. By the appendix we know:

$$J_p(\overline{\mathbf{Q}}_N)^1 = J_p^0(\overline{\mathbf{F}}_N) \times C \qquad (J_p^0 = p\text{-divisible group associated to } J^0_{/\mathbf{F}_N}).$$

---

[1] Carefully stated, our proof even works for $\ell = p$, if p happens to be a good prime. This is hardly relevant for the main corollaries; moreover, our *second* proof of this proposition (by the theory of modular symbols (cf. (18.10) below)) makes no distinction whatsoever between the cases $\ell = p$ and $\ell \neq p$. Nevertheless, the fact that our proposition is true when $\ell = p$ is a good prime has significance for the $\mathfrak{P}$-adic analytic number theory of J, and for the study of the arithmetic of the p-Eisenstein factor $\tilde{J}^{(p)}$ in the p-cyclotomic tower over $\mathbf{Q}$ (cf. chap. III, 9).

By SGA 7, exp. IX (3.5) (critère galoisien de réduction semi-stable) we know that if β, γ are in the inertia group at N, then $(1-\beta)(1-\gamma)$ acts trivially on $J_p(\overline{\mathbf{Q}}_N)$. Hence, if γ is in the inertia subgroup, $(1-\gamma).J_p(\overline{\mathbf{Q}}_N) \subset J_p(\overline{\mathbf{Q}}_N)^i$. But since $J_p(\overline{\mathbf{Q}}_N)$ is a p-divisible group, $(1-\gamma).J_p(\overline{\mathbf{Q}}_N)$ must be contained in the *p-divisible* part of $J_p(\overline{\mathbf{Q}}_N)^i$, which is $J_p^0(\overline{\mathbf{F}}_N) \subset J_p(\overline{\mathbf{Q}}_N)^i$, by the above direct product decomposition.

Now, take an element e in $J_p(\overline{\mathbf{Q}}_N)$ which maps to $\bar{e}$ in $(J_p(\overline{\mathbf{Q}}_N)/B)^i$. Let γ be any element in the inertia subgroup. Since $(1-\gamma).e$ goes to $(1-\gamma)\bar{e}=0$ in $J_p(\overline{\mathbf{Q}}_N)/B$, $(1-\gamma).e \in B$. Therefore, by the above discussion, $(1-\gamma).e$ is in $B \cap J_p^0(\overline{\mathbf{F}}_N)$ which is the trivial group, as is clear from the displayed direct product, if $B \subset C$ and as follows from (11.9) if $B \subset \Sigma$. Thus $(1-\gamma).e=0$, for all γ in the inertia subgroup. Q.E.D.

From now on, in this section, let $p \neq 2$. — In this case, proposition (16.1) will follow from a direct proof of the stronger proposition (16.6) below. When $p=2$, we shall reverse the order of proofs of these propositions.

Proposition **(16.6).** — *The ideal* $\mathfrak{I}.\mathbf{T}_{\mathfrak{P}}$ *is a principal ideal in* $\mathbf{T}_{\mathfrak{P}}$, *generated by* η_ℓ *for* ℓ *any good prime.*

Proof. — We shall be working with subgroup schemes (closed quasi-finite) in $J_{\mathfrak{P}}$ (hence admissible by (14.1)). In particular, consider $J_{\mathfrak{P}}[\mathfrak{I}]=J_p[\mathfrak{I}]$. We make extensive use of the tools developed in chapter I.

Lemma **(16.7).** — *The admissible group* $J_p[\mathfrak{I}]$ *is a* pure *group* [1].

Proof. — Consider the exact sequence (14.10):

$$0 \to C_p \to J_p[\mathfrak{I}] \to M \to 0$$

over S′, where C_p is the p-primary component of the cuspidal subgroup, and M is of multiplicative type. We first show that M is a μ-type group [1]. Since $\mathfrak{I}$ annihilates $J[\mathfrak{I}]$, for any prime number $\ell \neq N$, T_ℓ acts as $1+\ell$ on $J[\mathfrak{I}]$. Thus, by the Eichler-Shimura relations, for any $\ell \neq p$, N, the ℓ-Frobenius φ_ℓ satisfies $\varphi_\ell^2-(1+\ell).\varphi_\ell+\ell=0$, or:

$$(\varphi_\ell-1)(\varphi_\ell-\ell)=0.$$

If $\ell \equiv 1 \bmod p$, then φ_ℓ acts as multiplication by ℓ on $M(\overline{\mathbf{Q}})$. The reason for this is as follows. Since the Galois module $M(\overline{\mathbf{Q}})$ is admissible, of multiplicative type, the only eigenvalue that φ_ℓ possesses (when acting on $M(\overline{\mathbf{Q}})$) is ℓ. Consequently, $(\varphi_\ell-1)$ maps $M(\overline{\mathbf{Q}})$ isomorphically onto itself, and the above formula then implies that $(\varphi_\ell-\ell)$ annihilates $M(\overline{\mathbf{Q}})$. If $M^\vee$ denotes the Cartier dual of M, then $M^\vee$ is an étale admissible group over S′ such that φ_ℓ acts trivially in its Galois representation

[1] Chapter I, § 3.

for every $\ell \neq p$, N such that $\ell \equiv 1 \bmod p$. An elementary density argument (or chap. I (3.4)) implies that $M^\vee$ is constant, and therefore M is a μ-type group.

Since M is a μ-type group, the inertia subgroup at N operates trivially on $M(\overline{\mathbf{Q}}_N)$ (M extends to a finite flat subgroup over S, of order prime to N). Applying lemma (16.5) with $B = C_p$, we obtain that inertia at N operates trivially on $J_p[\mathfrak{I}]$ which is therefore a pure group by chapter I (4.5).

Thus $J_p[\mathfrak{I}]_{/S}$ is a finite flat group and, over S:

$$J_p[\mathfrak{I}] = C_p \times M.$$

It follows that:

$$J[\mathfrak{P}] = C[p] \times M[p].$$

Let r be a nonnegative integer.

Claim 1. — *The quotient group scheme* $J_p[\mathfrak{I}.\mathfrak{P}^{r+1}]/J_p[\mathfrak{I}.\mathfrak{P}^r]$ *over* S′ *is pure.*

Proof. — Set $t = \dim_{\mathbf{F}_p} \mathfrak{I}.\mathfrak{P}^r/\mathfrak{I}.\mathfrak{P}^{r+1}$. As in the discussion at the beginning of § 14, one may obtain an injection of the associated Galois module to $J_p[\mathfrak{I}.\mathfrak{P}^{r+1}]/J_p[\mathfrak{I}.\mathfrak{P}^r]$ into the associated Galois module to the direct sum of t copies of $J[\mathfrak{P}]$.

Consequently, by lemma (16.7), the inertia group at N operates trivially on the $\overline{\mathbf{Q}}_N$-valued points of $J_p[\mathfrak{I}.\mathfrak{P}^{r+1}]/J_p[\mathfrak{I}.\mathfrak{P}^r]$ and therefore it is pure, by chapter I (4.5).

Now fix a good prime number ℓ.

Claim 2. — *The group scheme* $J_p[\mathfrak{I}.\mathfrak{P}^r, \eta_\ell] = G_r$ *is pure for all r, and:*

$$G_r = C_p \times M^{(r)}$$

where $M^{(r)}$ *is a* μ*-type group.*

Proof. — By the above group scheme we mean, as usual, the subgroup scheme extension in $J_{/S}$ of the intersection of the kernels of $\mathfrak{I}.\mathfrak{P}^r$ and η_ℓ in $J_{p/\mathbf{Q}}$ (or, equivalently, in $J_{\mathfrak{P}/\mathbf{Q}}$). We proceed by induction, the first case $r = 0$ being already established (lemma (16.7)).

Suppose G_r is of the desired type: a pure group with étale part C_p and μ-type part $M^{(r)}$. Since its étale and μ-type parts are canonically determined, the operation of the Hecke algebra $\mathbf{T}$ must preserve these parts; in particular it preserves $M^{(r)}$.

Now we work over the base S′. Since η_ℓ annihilates G_{r+1}, the Eichler-Shimura relations give us the equation:

$$(\varphi_\ell - 1)(\varphi_\ell - \ell) = 0$$

on G_{r+1}, if $\ell \neq p$ and hence also on any subquotient of G_{r+1}. If $\ell = p$ we have the above equation on any subquotient of G_{r+1} which is *étale.*

By claim 1, and chapter I (4.5), it follows that G_{r+1}/G_r is pure. So we may write:

(16.8) $$0 \to G_r \to G_{r+1} \to (\mathbf{Z}/\mathbf{p})^\alpha \times M' \to 0$$

where α is some nonnegative integer, and M' is a μ-type group.

We first show that $\alpha = 0$. — Form the pullback:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G_r & \longrightarrow & G_{r+1} & \longrightarrow & (\mathbf{Z}/\mathbf{p})^\alpha \times M' & \longrightarrow & 0 \\ & & = \uparrow & & \subseteq \uparrow & & \subseteq \uparrow & & \\ 0 & \longrightarrow & G_r & \longrightarrow & G & \longrightarrow & (\mathbf{Z}/\mathbf{p})^\alpha & \longrightarrow & 0 \end{array}$$

and set $\overline{G} = G/M^{(r)}$. Thus we have a short exact sequence:

$$0 \to C_p \to \overline{G} \to (\mathbf{Z}/\mathbf{p})^\alpha \to 0.$$

That is, $\overline{G}$ is an admissible étale group. Moreover, since $(\varphi_\ell - 1)(\varphi_\ell - \ell) = 0$, and $\ell \not\equiv 1 \bmod p$, it follows that $\varphi_\ell = 1$ on $\overline{G}$. By the " criterion for constancy " (chap. I (3.4)), $\overline{G}$ is a constant group. By the manner in which $\overline{G}$ was constructed, there is a natural induced action of the Hecke algebra $\mathbf{T}$ on $\overline{G}$. But the ideal $\mathfrak{I} \subset \mathbf{T}$ annihilates $\overline{G}$. To see this, use the fact that the action of $\mathrm{Frob}_{\ell'}$ on $\overline{G}$ is trivial (for any prime number $\ell' \neq N$, including $\ell' = p$) since $\overline{G}$ is a constant group over S'. From the Eichler-Shimura relations one then sees that $T_{\ell'} = 1 + \ell'$ (for all $\ell' \neq N$). By construction of $\overline{G}$, $(1+w)^2$ annihilates $\overline{G}$. Since w is an involution, and $p \neq 2$, it follows that $1 + w = 0$ on $\overline{G}$. Thus the ideal $\mathfrak{I}$ annihilates $\overline{G}$.

Now reduce to characteristic p. From our exact sequences one sees that $\overline{G}_{/\mathbf{F}_p}$ is *equal* to $(G_{r+1/\mathbf{F}_p})^{\text{ét}}$. It follows from what we have just shown that $(G_{r+1/\mathbf{F}_p})^{\text{ét}}$ is annihilated by $\mathfrak{I}$. But by (14.10), C_p equals the kernel of $\mathfrak{I}$ in $(J_{p/\mathbf{F}_p})^{\text{ét}}$. Therefore $\alpha = 0$.

Return to our exact sequence (16.8), which now may be written:

$$0 \to G_r \to G_{r+1} \to M' \to 0.$$

Also we have the exact sequence:

(16.9) $$0 \to C_p \to G_{r+1} \to M'' \to 0$$

where M'' is an admissible group of multiplicative type which is an extension of M' by $M^{(r)}$. Since $\eta_\ell = 0$, applying the Eichler-Shimura relations to the Cartier dual $(M'')^\vee$ which is an étale admissible group, we have that $(\varphi_\ell - 1)(\varphi_\ell - \ell) = 0$ on $(M'')^\vee$.

Since ℓ is a good prime number, we use, again, the above quadratic equation, and the " Criterion of constancy " (chap. I (3.4)) to deduce that $(M'')^\vee$ is a constant group; thus M'' is of μ-type. In particular, the inertia group at N operates trivially on $M''(\overline{\mathbf{Q}}_N)$, and hence also on $G_{r+1}(\overline{\mathbf{Q}}_N)$, using the exact sequence (16.9) and lemma (16.5) with $B = C_p$. Thus, by the criterion of purity (chap. I (4.5)), G_{r+1} is a pure group, whose étale part is C_p.

Claim 3. — $C_p=(J_{\mathfrak{P}/\mathbf{F}_p})^{\text{ét}}[\eta_\ell]$.

Proof. — By Claim 2, the kernel of η_ℓ in $J_{\mathfrak{P}/S'}$ has the following structure:

$$J_{\mathfrak{P}}[\eta_\ell]=C_p\times M^{(\infty)}$$

where $M^{(\infty)}=\bigcup_r M^{(r)}$ is a union of μ-type groups.

Consequently $C_p=((J_{\mathfrak{P}}[\eta_\ell])_{/\mathbf{F}_p})^{\text{ét}}$. Our claim will follow from a lemma (which we also use later when $p=2$):

Lemma (**16.10**). — *Let p be* any *prime dividing n, and ℓ any prime number different from* N. *Then*:

$$J_{\mathfrak{P}}[\eta_\ell](\overline{\mathbf{F}}_p)=J_{\mathfrak{P}}(\overline{\mathbf{F}}_p)[\eta_\ell].$$

One sees easily that η_ℓ is an isogeny of J onto itself, for if it were not, then, by the Eichler-Shimura relations, φ_ℓ would have an eigenvalue equal to 1 or to ℓ in its representation of $J_{\ell'}(\overline{\mathbf{Q}})$ (ℓ' any prime different from ℓ or N) which is impossible for various reasons. Thus, η_ℓ is a surjective endomorphism on all groups of the exact sequence:

$$0\to J^0_{\mathfrak{P}}(\overline{\mathbf{Q}}_p)\to J_{\mathfrak{P}}(\overline{\mathbf{Q}}_p)\to J_{\mathfrak{P}}(\overline{\mathbf{F}}_p)\to 0$$

giving us surjectivity of $J_{\mathfrak{P}}(\overline{\mathbf{Q}}_p)[\eta_\ell]\to J_{\mathfrak{P}}(\overline{\mathbf{F}}_p)[\eta_\ell]\to 0$ by the snake-lemma. It follows that $J_{\mathfrak{P}}[\eta_\ell](\overline{\mathbf{F}}_p)=J_{\mathfrak{P}}(\overline{\mathbf{F}}_p)[\eta_\ell]$ [1].

Conclusion of the proof of Proposition (16.6) *for* $p\neq 2$. — Let W denote the $\mathbf{Z}_p$-dual of $\mathcal{E}a(J_{\mathfrak{P}}(\overline{\mathbf{F}}_p))$ (or, equivalently, the $\mathbf{Q}_p/\mathbf{Z}_p$-dual of $J_{\mathfrak{P}}(\overline{\mathbf{F}}_p)$; cf. § 7). By (14.11) W is a free $\mathbf{T}_{\mathfrak{P}}$-module of rank 1. By Claim 3, and (14.9), $W/\eta_\ell.W=W/\mathfrak{I}.W$. Therefore $\eta_\ell.\mathbf{T}_{\mathfrak{P}}=\mathfrak{I}.\mathbf{T}_{\mathfrak{P}}$.

17. Eisenstein primes ($p=2$).

We now begin to study the case where $p=2$ divides n. Our first goal is to prove:

Proposition (**17.1**). — *The Eisenstein prime $\mathfrak{P}.\mathbf{T}_{\mathfrak{P}}\subset\mathbf{T}_{\mathfrak{P}}$ is generated by the elements p and η_ℓ, where ℓ is any good prime different from* 2.

---

(1) To help the reader see this, it may be worth discursively reviewing the "brackets" terminology at this point. By definition, the group scheme $J_{\mathfrak{P}}[\eta_\ell]_{/S'}$ is the subgroup scheme extension in $J_{/S'}$ of the sub-Gal($\overline{\mathbf{Q}}/\mathbf{Q}$)-module in $J_{\mathfrak{P}}(\overline{\mathbf{Q}})$ consisting in the kernel of η_ℓ. Thus, since η_ℓ is an isogeny and $J_{/S'}$ is an abelian scheme, $J_{\mathfrak{P}}[\eta_\ell]_{/S'}$ is a finite flat group scheme (it is, in fact, admissible) whose associated Galois module is $J_{\mathfrak{P}}(\overline{\mathbf{Q}})[\eta_\ell]=J_{\mathfrak{P}}(\overline{\mathbf{Q}}_p)[\eta_\ell]$. By $J_{\mathfrak{P}}[\eta_\ell](\overline{\mathbf{F}}_p)$ we mean, to be sure, the $\overline{\mathbf{F}}_p$-valued points of the group scheme $J_{\mathfrak{P}}[\eta_\ell]_{/S'}$. We have a natural map (a surjection in fact) from the $\overline{\mathbf{Q}}_p$-valued points of the finite flat group $J_{\mathfrak{P}}[\eta_\ell]$ to the $\overline{\mathbf{F}}_p$-valued points (reduction to characteristic p): $J_{\mathfrak{P}}[\eta_\ell](\overline{\mathbf{Q}}_p)\to J_{\mathfrak{P}}[\eta_\ell](\overline{\mathbf{F}}_p)$, the range being naturally contained in $J_{\mathfrak{P}}(\overline{\mathbf{F}}_p)[\eta_\ell]$ (the kernel of η_ℓ in $J_{\mathfrak{P}}(\overline{\mathbf{F}}_p)$). The asserted equality then follows from the previous discussion.

Discussion. — The case $p=2$ differs from $p\neq 2$ in many respects, the major ones being:

a) Fontaine's theorem does not apply.

b) The equation $(\varphi_\ell-\ell)(\varphi_\ell-1)=0$ (for ℓ a good prime) on an étale or multiplicative type admissible group does *not* imply that the group is constant or of μ-type.

c) Where we have dealt in § 16 with the cuspidal subgroup, we must now deal, systematically, with the group D.

d) C_p and Σ_p have a nontrivial intersection (when $p=2$) and therefore it will turn out that $J_{\mathfrak{P}}[\mathfrak{I}_{\mathfrak{P}}]$ is *larger* than $C_p+\Sigma_p$. If $N\equiv 1 \bmod 16$ we give no direct construction of $J_{\mathfrak{P}}[\mathfrak{I}_{\mathfrak{P}}]$.

We deal with *a)* by keeping strict control of the étale part of our group scheme. We are forced by *b)* and *c)* to work with groups which are roughly " twice the size " (in terms of lengths of various filtrations) as in the case $p\neq 2$. In particular, the *pure* groups of § 16 are replaced by $*$-type groups (see below). We " pay for " *d)* by not being able to give a complete account of the Galois representation on $J_{\mathfrak{P}}[\mathfrak{I}_{\mathfrak{P}}]$.

Recall the terminology of chapter I, § 3, and especially lemma (3.5):

Lemma **(17.2).** — *Let* $M_{/S'}$ *be a multiplicative type admissible group. Let* ℓ *be a prime number which is not a quadratic residue* mod N (e.g. *a good prime*) $(\ell\neq 2)$ *such that* $(\varphi_\ell-\ell)(\varphi_\ell-1)=0$ *on* M. *Let* $M_1\subset M$ *be the "first stage" in the canonical sequence of* M (cf. chap. I, § 3) (i.e. *the largest* μ*-type subgroup of* M). *Then* $M_1(\mathbf{Q})$ *is the kernel of* $\varphi_\ell-\ell$ *and* φ_ℓ *acts trivially on* $(M/M_1)(\bar{\mathbf{Q}})$.

Proof. — The first assertion is a repetition of chapter I (3.6). The second assertion is then evident since $\varphi_\ell-1$ brings $M(\bar{\mathbf{Q}})$ into the kernel of $(\varphi_\ell-\ell)$.

$*$-type groups.

We work with a fixed *good* prime number $\ell\neq 2$, and certain admissible subgroup schemes $G_{/S'}\subset J_{\mathfrak{P}}[\eta_\ell]_{/S'}$ (*i.e.* in $J_{\mathfrak{P}}$ and killed by η_ℓ). Say that such a group scheme is a $*$*-type group* if it can be expressed as a " push-out " (or " amalgamated direct sum ") of the following form:

$$(*)\qquad \begin{array}{ccccccccc} & & & & 0 & & & & \\ & & & & \downarrow & & & & \\ 0 & \longrightarrow & \boldsymbol{\mu}_2 & \longrightarrow & D & \longrightarrow & \mathbf{Z/2} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \subset} & & \downarrow{\scriptstyle \subset} & & \downarrow{\scriptstyle =} & & \\ 0 & \longrightarrow & G^0 & \longrightarrow & G & \longrightarrow & \mathbf{Z/2} & \longrightarrow & 0 \end{array}$$

where: $D\subset J[\mathfrak{P}]$ is *the* subgroup scheme of § 12, and $G^0\subset J_{\mathfrak{P}}[\eta_\ell]$ is some (admissible) subgroup scheme of *multiplicative type*, containing the subgroup $\boldsymbol{\mu}_2\subset D$.

We also denote the " amalgamated sum " as follows: $G=G^0\vee_{\boldsymbol{\mu}_2} D$.

Since D is fixed, a $*$-type group is *determined by* its multiplicative part $G^0 \subset G$, and conversely: G^0 is the connected component containing the identity of the *scheme* $G_{/S'}$.

Lemma (**17.3**). — *If* G *is* $*$*-type, and*:

$$0 \to (G_{/\mathbf{Z}_2})^0 \to G_{/\mathbf{Z}_2} \to (G_{/\mathbf{Z}_2})^{\text{ét}} \to 0$$

is the natural sequence displaying the connected *and* étale *parts of* $G_{/\mathbf{Z}_2}$, *then*:

$$(G_{/\mathbf{Z}_2})^0 = G^0_{/\mathbf{Z}_2}.$$

Remark. — In particular, the $\bar{\mathbf{Q}}_2$-rational points of $(G_{/\mathbf{Z}_2})^0$ (which is, *a priori*, only stable under the action of $\mathrm{Gal}(\bar{\mathbf{Q}}_2/\mathbf{Q}_2)$) is stable under the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ as subgroup of $G(\bar{\mathbf{Q}}) = G(\bar{\mathbf{Q}}_2)$; here we fix *any* imbedding $\bar{\mathbf{Q}} \subset \bar{\mathbf{Q}}_2$.

Applying (17.2) to G^0/μ_2 we obtain a subgroup scheme $G^{00} \subset G^0$ containing μ_2, such that G^{00}/μ_2 is the " first stage " in the canonical sequence for G^0/μ_2. In particular, G^{00}/μ_2 is a μ-type group and its Galois module is the kernel of $\varphi_\ell - \ell$ in the Galois module of G^0/μ_2. Also φ_ℓ acts trivially on the Galois module of G^0/G^{00}.

Lemma (**17.4**). — G^{00} *is a* μ*-type group.*

Proof. — Since the inertia group at N operates trivially on G^{00}/μ_2 lemma (16.5) (where we take $B = \mu_2$) assures us that it operates trivially on G^{00}. We then apply chapter I (3.1).

The key lemma enabling us to construct $*$-type groups is the following:

Lemma (**17.5**). — *Let* ℓ *be a good prime number different from* 2. *Let* $G \subset G' \subset J_{\mathfrak{P}}[\eta_\ell]$ *be (admissible) subgroups stable under the action of* **T** *such that*:

a) G *is a* $*$*-type group.*

b) G'/G *is of order* 2.

c) 2 *kills the étale part of* $G'_{/\mathbf{F}_2}$.

Then G′ *is a* $*$*-type group.*

Proof. — In the calculations of Claims 1 and 2 below, we deal exclusively with Galois modules. For simplicity we let the symbol of the group-scheme stand for the associated $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-module, in the proof of those claims. Thus G′ would stand for $G'(\bar{\mathbf{Q}})$, etc.

Claim 1: $(\varphi_\ell - 1)(G'/D) \subset (G^{00} \vee_{\mu_2} D)/D = G^{00}/\mu_2$.

Proof. — We have a filtration:

$$0 \subset (G^{00} \vee_{\mu_2} D)/D \subset G/D \subset G'/D$$

$$\| \qquad\qquad \|$$

$$G^{00}/\mu_2 \qquad G^0/\mu_2$$

Since $(\varphi_\ell - 1)$ annihilates G'/G and leaves D stable, we have that $(\varphi_\ell - 1)(G'/D)$ is in G/D. But note that $(\varphi_\ell - \ell) : G^0/G^{00} \to G^0/\mu_2$ is *injective* (17.2), and consequently, if $(\varphi_\ell - 1)(G'/D)$ were *not* contained in G^{00}/μ_2 we could *not* have $(\varphi_\ell - \ell)(\varphi_\ell - 1) = 0$.

Claim 2: $(\varphi_\ell - 1)\, G' \subset G^{00}$.

Proof. — By Claim 1, $(\varphi_\ell - 1)\, G' \subset G^{00} \vee_{\mu_2} D$. But $\varphi_\ell - \ell$ maps $G^{00} \vee_{\mu_2} D$ onto μ_2, with kernel G^{00} (since $\psi_{-1}(\ell) = 1$, $\varphi_\ell - \ell$ maps D onto μ_2; cf. chap. I (4.3)).

Again, since $(\varphi_\ell - \ell)(\varphi_\ell - 1) = 0$, Claim 2 follows.

Claim 3. — *The extension of* group schemes *over* S':

$$0 \to \mathbf{Z}/2 \to G'/G^0 \to G'/G \to 0$$

splits.

Proof. — By Claim 2, φ_ℓ acts trivially on G'/G^0. There are two possibilities:

Case I. — $G'/G = \mathbf{Z}/2$ (as group scheme over S').

Then hypothesis c) insures that the étale group scheme G'/G^0 is killed by 2, and since φ_ℓ acts trivially on it, it is indeed a product, by chapter I (3.4).

Case II. — $G'/G = \mu_2$.

It is also true in this case that G'/G^0 is killed by 2. The reason is that *any* extension $\mathscr{E}$ of μ_2 by $\mathbf{Z}/2$ *splits* over Spec $\mathbf{Z}_2$ (the splitting is obtained by showing that $\mathscr{E}^0$, the connected component of $\mathscr{E}$, must project isomorphically to μ_2). Therefore, in particular, 2 kills $\mathscr{E}(\overline{\mathbf{Q}}_2) = \mathscr{E}(\mathbf{Q})$, and hence it also kills $\mathscr{E}$. Again since φ_ℓ acts trivially on it, it is a product, by chapter I (5.1).

We now show that Case I cannot occur. That is, G'/G^0 cannot be the constant group scheme $\mathbf{Z}/2 \times \mathbf{Z}/2$. Note first that the Hecke algebra $\mathbf{T}$ induces a natural action on G'/G^0. For it leaves G' and G stable by hypothesis. We must show that it leaves G^0 stable. But by Lemma (17.3), the Galois submodule $G^0(\overline{\mathbf{Q}})$ of $G(\overline{\mathbf{Q}})$ is determinable as the sections which specialize to zero in characteristic 2 (the sections of the connected component $(G_{/\mathbf{Z}_2})^0$) and is therefore left stable under the action of $\mathbf{T}$. We follow the proof for p odd, quite closely. For all primes $\ell' \neq 2$, N, the Eichler-Shimura relations assure us that $T_{\ell'} = 1 + \ell'$ on the constant group scheme G'/G^0. Reducing to $\mathbf{F}_2$, one has that $T_2 = 1 (\equiv 1 + 2)$ on $(G'/G^0)_{/\mathbf{F}_2}$, again by the Eichler-Shimura relations.

We have to check that $w + 1 = 0$, in order to conclude that $(G'_{/\mathbf{F}_2})^{\text{ét}} = (G'/G^0)_{/\mathbf{F}_2}$ is in $(J_{/\mathbf{F}_2})^{\text{ét}}[\mathfrak{P}]$. But since $(w+1)^2 = 0$ (because $w+1$ is certainly nilpotent on $G' \subset J_{\mathfrak{P}}$ and (G'/G^0) is an $\mathbf{F}_2$-vector group of rank 2) and since $w+1$ annihilates $\mathbf{Z}/2 = G/G^0$, it suffices to show that $(G_{/\mathbf{F}_2})^{\text{ét}} = (D_{/\mathbf{F}_2})^{\text{ét}}$ *is not in the image of* $w+1$, which is true by (13.10).

Thus $(G'_{/\mathbf{F}_2})^{\text{ét}} \subset (J_{/\mathbf{F}_2})^{\text{ét}}[\mathfrak{P}]$ which *contradicts* (14.9). Therefore we have:

$$G'/G^0 = \mathbf{Z}/2 \times \mu_2.$$

Defining G'^0 to be the kernel of the natural projection of G' onto the first factor $\mathbf{Z}/2$ in the above product, we have that G'^0 is a subgroup of G', of multiplicative type, and $G'=G'^0 \vee_{\mu_2} D$ is therefore a $*$-type group. Q.E.D.

Let $r \geq 1$ be an integer. Consider the exact sequences of $\mathrm{Gal}(\bar{\mathbf{Q}}_2/\mathbf{Q}_2)$-modules:

$$0 \to J_{\mathfrak{P}}[2^r, \eta_\ell]^0(\bar{\mathbf{Q}}_2) \to J_{\mathfrak{P}}[2^r, \eta_\ell](\bar{\mathbf{Q}}_2) \to J_{\mathfrak{P}}[\eta_\ell](\bar{\mathbf{F}}_2)$$

where the superscript ^{0} denotes the connected component (containing the identity) of a group scheme over $\mathrm{Spec}\ \mathbf{Z}_2$.

Since $J_{\mathfrak{P}}[2^r, \eta_\ell](\bar{\mathbf{Q}}_2)=J_{\mathfrak{P}}[2^r, \eta_\ell](\bar{\mathbf{Q}})$, this group is (in a fixed way) a $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-module.

Let $G(r) \subset J_{\mathfrak{P}}[2^r, \eta_\ell](\bar{\mathbf{Q}}_2)$ denote the full inverse image of $(J_{\mathfrak{P}}[\eta_\ell](\bar{\mathbf{F}}_2))[2]$ in $J_{\mathfrak{P}}[2^r, \eta_\ell](\bar{\mathbf{Q}}_2)$. It is clear that $G(r)$ inherits a $\mathrm{Gal}(\bar{\mathbf{Q}}_2/\mathbf{Q}_2)$-module structure. It is *not* clear that $G(r)$ is stable under $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Write $G^0(r)=J_{\mathfrak{P}}[2^r, \eta]^0(\bar{\mathbf{Q}}_2)$.

We have:

(17.6) (i) $$0 \to G^0(r) \to G(r) \to (J_{\mathfrak{P}}[\eta_\ell](\bar{\mathbf{F}}_2))[2]$$

and, *if r is sufficiently large*:

(17.6) (ii) $$0 \to G^0(r) \to G(r) \to (J_{\mathfrak{P}}[\eta_\ell](\mathbf{F}_2))[2] \to 0.$$

We formulate two hypotheses:

$\mathrm{I}(r)$: The subgroup $G(r) \subset J_{\mathfrak{P}}[2^r, \eta_\ell](\bar{\mathbf{Q}})$ is stable under the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$.

$\mathrm{I}^0(r)$: The subgroup $G^0(r) \subset J_{\mathfrak{P}}[2^r, \eta_\ell](\bar{\mathbf{Q}})$ is stable under the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$.

Lemma **(17.7)**. — *Hypotheses* $\mathrm{I}(r)$ *and* $\mathrm{I}^0(r)$ *hold for all* $r>0$. *The group scheme* $G(r)$ *is a* $*$*-type group for all* $r>0$.

Proof of Lemma (17.7). — Our inductive proof consists in five steps. Set:

$$G(0)=D \subset J[\mathfrak{P}] \quad (\S\ 12).$$

Step 1. — *For* $r \geq 0$, *if* $\mathrm{I}(r)$ *and* $\mathrm{I}(r+1)$ *hold, and if* $G(r)$ *is a* $*$*-type group, then* $G(r+1)$ *is a* $*$*-type group.*

Proof. — Since the groups $G(r) \subset G(r+1)$ are both stable under the action of $\mathbf{T}$, we may find a filtration:

$$G(r)=H_0 \subset H_1 \subset \ldots \subset H_j \subset \ldots \subset H_t = G(r+1)$$

by $\mathbf{T}_{\mathfrak{P}}[\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})]$-submodules H_j such that the successive quotients H_j/H_{j-1} are irreducible $\mathbf{T}_{\mathfrak{P}}[\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})]$-modules. Since H_j/H_{j-1} is therefore a module over:

$$\mathbf{T}_{\mathfrak{P}}/\mathfrak{P}.\mathbf{T}_{\mathfrak{P}}[\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})]$$

and since $\mathbf{T}_{\mathfrak{P}}/\mathfrak{P}.\mathbf{T}_{\mathfrak{P}}=\mathbf{F}_2$, H_j/H_{j-1} is an irreducible $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-module. Since $G(r)$ is admissible, it follows that H_j/H_{j-1} is of order two. By upwards induction on j, applying Lemma (17.5) to $G=H_{j-1}$, $G'=H_j$, one obtains that $G(r+1)$ a $*$-type group.

Step 2. — *If* $I(r)$ *holds, and* $G(r)$ *is a* $*$*-type group, then* $I^0(r)$ *holds.*

Proof. — Apply Lemma (17.3) with $G(r)=G$.

Step 3. — $I^0(r) \Rightarrow I(r+1)$.

Proof. — If $x \in J_{\mathfrak{P}}[2^{r+1}, \eta_\ell](\overline{\mathbf{Q}})$, then (since $2^r.2x=0$) by the defining property of $G(r+1)$, $x \in G(r+1)$ if and only if $2x \in G^0(r)$. Now, if $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, and $x \in G(r+1)$ we must show that $\sigma(x) \in G(r+1)$. Equivalently, we must show that $2.\sigma(x) \in G^0(r)$. But this is true since (by $I^0(r)$) σ leaves $G^0(r)$ stable, and $\sigma(2x)=2.\sigma(x)$.

Step 4. — *If* $I(r)$ *holds, and* $G(r)$ *is a* $*$*-type group, then* $I(r+1)$ *holds and* $G(r+1)$ *is a* $*$*-type group* $(r \geq 1)$.

Proof. — Combine the first three steps.

Step 5. — *Conclusion*: Clearly $D=G(0)$ is a $*$-type group, and, since:

$$G(1)=J[2, \eta_\ell](\overline{\mathbf{Q}}),$$

$I(1)$ holds. By Step 1 it follows that $G(1)$ is a $*$-type group. This allows us to apply Step 4 (inductively) to conclude the proof of Lemma (17.7).

Proposition **(17.8).** — *The following groups (of order 2) are equal*:

$$D(\overline{\mathbf{F}}_2)=J[\mathfrak{P}](\overline{\mathbf{F}}_2)=J_{\mathfrak{P}}(\overline{\mathbf{F}}_2)[\mathfrak{P}]=J_{\mathfrak{P}}(\overline{\mathbf{F}}_2)[2, \eta_\ell].$$

Proof. — It is only the last equality that is new, but they will all follow if we show that the right-most group is of order 2. By Lemma (17.7) and the exact sequence (17.6) (ii) for r sufficiently large, we deduce that $(J_{\mathfrak{P}}[\eta_\ell](\overline{\mathbf{F}}_2))[2]$ is of order 2 [1]. To conclude the proposition, we need that $J_{\mathfrak{P}}[\eta_\ell](\overline{\mathbf{F}}_2)=J_{\mathfrak{P}}(\overline{\mathbf{F}}_2)[\eta_\ell]$ which is true by (16.10).

Proof of Proposition (17.1). — We follow the proof for p odd. By (14.11), the Pontrjagin dual, W, of $J_{\mathfrak{P}}(\overline{\mathbf{F}}_2)$ is free over $\mathbf{T}_{\mathfrak{P}}$ of rank 1. By Proposition (17.8), $W/(\eta_\ell, 2)=W/\mathfrak{P}.W$.

Therefore $\mathfrak{P}=(\eta_\ell, 2)$. Q.E.D.

One has these immediate consequences (15.1):

(17.9)
(i) $\mathbf{T}_{\mathfrak{P}}$ *is a Gorenstein ring*;
(ii) $J[\mathfrak{P}]=D$;
(iii) $H_{\mathfrak{P}}$ *is free of rank 2 over* $\mathbf{T}_{\mathfrak{P}}$.

Proposition **(17.10).** — *The Eisenstein quotient* $J \to \tilde{J}$ *factors through* J^- (cf. § 4).

Proof. — Let us work over the base $\mathbf{Q}$.

---

(1) The point here is that the étale part of a $*$-type group reduced to characteristic 2 is of *order* 2. This is *all* we need.

The fact that for p odd, the p-Eisenstein quotient factors through J^- is fairly evident: the kernel of $\mathfrak{P}$ in J_+ is zero, since w acts as -1 on $J[\mathfrak{P}]$ and as $+1$ on $J_+ = (1+w).J = \ker(J \to J^-)$.

For $p=2$ (if $2 \mid n$) we must also show that $J_+[\mathfrak{P}]=0$. But by (17.9) $J[\mathfrak{P}]=D$, and by (13.10) $D \cap J_+ = 0$.

18. Winding homomorphisms.

If R is a commutative ring with unit let $R[\sigma]$ denote the commutative R-algebra $1.R \oplus \sigma.R$ where σ is a symbol satisfying the law $\sigma^2=1$. If M is a free $R[\sigma]$-module of rank 1, then σ is an involution on M; forming the (± 1)-eigen-subspaces $M_\pm \subset M$ associated to σ, and the corresponding eigenquotient spaces $M^\pm$, we have the diagram of exact sequences:

(18.1)

$$\begin{array}{ccccccccc} & & & & 0 & & & & \\ & & & & \downarrow & & & & \\ & & & & M_+ & & & & \\ & & & & \downarrow & \searrow^{\text{“2”}} & & & \\ 0 & \to & M_- & \to & M & \to & M^+ & \to & 0 \\ & & & \searrow^{\text{“2”}} & \downarrow & & & & \\ & & & & M^- & & & & \\ & & & & \downarrow & & & & \\ & & & & 0 & & & & \end{array}$$

where all four R-modules $M_\pm$, $M^\pm$ are free of rank 1. In fact they may be canonically identified with R and in terms of these canonical identifications, the diagonal homomorphisms above are " multiplication by 2 ".

Lemma **(18.2)**. — *Let* R *be a commutative local ring with maximal ideal* $\mathfrak{m}$. *Let* M *be a free* R*-module of rank* 2 *endowed with an* (R*-linear*) *involution* σ *which is* not *a scalar modulo* $\mathfrak{m}$. *Then* M *is free of rank* 1 *over* $R[\sigma]$.

Proof. — Let $k=R/\mathfrak{m}$. Then $\overline{M}=M/\mathfrak{m}.M$ is a 2-dimensional vector space over k on which the involution σ does not act as a scalar. In particular, there is an element $x \in M$ such that $\bar{x} \in \overline{M}$ is a generator of $\overline{M}$ as $k[\sigma]$-module. Applying Nakayama's Lemma to M over R, one deduces that x is a generator of M as $R[\sigma]$-module. Moreover, since the $R[\sigma]$-homomorphism $R[\sigma] \xrightarrow{i} M$ $(\alpha \mapsto \alpha.x)$ is an isomorphism of R-modules modulo $\mathfrak{m}$, and M is a free R-module, it follows that i is an isomorphism.

Proposition **(18.3)**. — *Let* $H = H_1(X_0(N)_{\mathbf{C}}, \mathbf{Z})$ *and let* $\sigma : H \to H$ *be the involution induced from complex conjugation of the manifold* $X_0(N)_{\mathbf{C}}$.

Let $\mathfrak{M}$ *be any maximal ideal in* $\mathbf{T}$ *such that* $\operatorname{char} k_{\mathfrak{M}} \neq 2$. *Then* $H_{\mathfrak{M}}$ *is a free* $\mathbf{T}_{\mathfrak{M}}[\sigma]$*-module of rank* 1.

Let $\mathfrak{P}$ be (any) Eisenstein prime. Then $H_{\mathfrak{P}}$ is a free $\mathbf{T}_{\mathfrak{P}}[\sigma]$-module of rank 1.

Let $\mathbf{T}_{\mathfrak{Z}}$ denote the completion of $\mathbf{T}$ with respect to the (full) Eisenstein ideal. Then $H_{\mathfrak{Z}}$ is a free $\mathbf{T}_{\mathfrak{Z}}[\sigma]$-module of rank 1.

Proof. — Let $\mathfrak{M}$ be a maximal ideal such that $p = \operatorname{char} k_{\mathfrak{M}} \neq 2$. By (15.2) $H_{\mathfrak{M}} = \mathscr{E}a(J_{\mathfrak{M}})(\mathbf{C})$ is free over $\mathbf{T}_{\mathfrak{M}}$ of rank two. On the other hand, one has a perfect duality:

$$\mathscr{E}a(J_{\mathfrak{M}})(\mathbf{C}) \times \mathscr{E}a(J_{\mathfrak{M}})(\mathbf{C}) \to \mathscr{E}a(\mu)(\mathbf{C}) \tag{18.4}$$

(where $\mu = \bigcup_{r=1}^{\infty} \mu_{p^r} \subset \mathbf{G}_m$). Since σ acts as -1 on $\mathscr{E}a(\mu)(\mathbf{C})$ and since $p \neq 2$, we have that $H_{\mathfrak{M}} = H_{\mathfrak{M}+} \oplus H_{\mathfrak{M}-}$ where (18.4) puts $H_{\mathfrak{M}+}$ and $H_{\mathfrak{M}-}$ in duality. Since (again) $p \neq 2$ it follows that σ does not act as a scalar modulo $\mathfrak{M}.\mathbf{T}_{\mathfrak{M}}$ and consequently $H_{\mathfrak{M}}$ is free over $\mathbf{T}_{\mathfrak{M}}[\sigma]$.

Now let $\mathfrak{P}$ be an Eisenstein prime associated to p. By (16.3) and (17.9) $H_{\mathfrak{P}}$ is free over $\mathbf{T}_{\mathfrak{P}}$ of rank 2, and by (16.3) the action of σ is evident. Namely, when $p \neq 2$ σ acts as $+1$ on C and as -1 on Σ. Therefore it does not act as a scalar modulo $\mathfrak{P}.\mathbf{T}_{\mathfrak{P}}$. If $p = 2$, σ does not act as a scalar on $D(\mathbf{C})$ (cf. chap. I (4.3)). Therefore Lemma (18.2) applies again.

Since $\mathbf{T}_{\mathfrak{Z}} = \prod_{p|n} \mathbf{T}_{\mathfrak{P}}$, $H_{\mathfrak{Z}} = \prod_{p|n} H_{\mathfrak{P}}$, the final assertion follows, as well. Q.E.D.

Let $J_{\mathbf{C}}$ denote the complex Lie group underlying the jacobian of $X_0(N)$, and U its universal covering group. We have an exact sequence of topological groups:

$$0 \to H \to U \xrightarrow{\pi} J_{\mathbf{C}} \to 0 \tag{18.5}$$

where the discrete subgroup $H \subset U$ is identified with $H = H_1(X_0(N)_{\mathbf{C}}, \mathbf{Z})$. Moreover, the Hecke algebra $\mathbf{T}$ and complex conjugation σ both operate naturally on the above exact sequence. The Lie group U is isomorphic to $H \otimes \mathbf{R}$, as real Lie group: The real Lie group $J_{\mathbf{C}}$ is canonically isomorphic to $H \otimes (\mathbf{R}/\mathbf{Z})$.

Consider the *fundamental arc* $[0, i\infty] = \{iy \mid 0 \leq y \leq i\infty\}$ in the extended upper-half plane. We regard the fundamental arc as an oriented topological interval (orientation from $i\infty$ to 0). The parametrization of $X_0(N)_{\mathbf{C}}$ by the upper-half plane induces a natural homeomorphic injection:

$$[0, i\infty] \xrightarrow{\bar{h}} J_{\mathbf{C}} \qquad (\bar{h}(i\infty) = \text{origin}).$$

The continuous map $\bar{h}$ lifts uniquely to a continuous map to the universal covering group:

$$h : [0, i\infty] \to U \qquad (h(i\infty) = \text{origin}).$$

Definition. — *Set $e = h(0) \in U$. Call e the* winding element.

Lemma (18.6). — *We have $\mathfrak{I}.e \subset H_+ \subset U$. The winding element e is in $H_+ \otimes \mathbf{Q}$.*

Proof. — The fundamental arc maps to the real locus of $X_0(N)$ and, from the definition it is clear that $\pi(e)=c=\mathscr{C}\ell((0)-(\infty))$ in J_C. Therefore, since $\mathfrak{I}.c=0$ (11.1), it follows that $\mathfrak{I}.e\subset H$, and since e is fixed under σ, $\mathfrak{I}.e\subset H_+$. Since $n\in\mathfrak{I}$, $e\in(1/n).H_+$.

Definition. — *Let*:

$$e_+ : \mathfrak{I}\to H_+$$

be the **T**-*homomorphism* $\alpha\mapsto\alpha.e$.

If $\mathfrak{a}$ *is any ideal in* **T**, *let*:

$$e_+ : \mathfrak{I}.\mathbf{T}_\mathfrak{a}\to H_{\mathfrak{a}+}$$

denote, as well, the induced $\mathbf{T}_\mathfrak{a}$ *homomorphism.*

If $H_\mathfrak{a}$ *is free over* $\mathbf{T}_\mathfrak{a}$ *of rank* 1, *let*:

$$e^+ : \mathfrak{I}.\mathbf{T}_\mathfrak{a}\to H_\mathfrak{a}^+$$

be the $\mathbf{T}_\mathfrak{a}$-*homomorphism defined by*: $2.e^+(\alpha)=$ image in $H_\mathfrak{a}^+$ of $e_+(\alpha)$ (*using diagram* (18.1)).

We shall call the homomorphisms e_+ and e^+ *winding homomorphisms.* The winding homomorphisms are (conveniently normalized) " generalizations " of the *winding numbers* of [39].

We shall be especially interested in the winding homomorphism e^+ for $\mathfrak{a}=\mathfrak{I}$:

$$e^+ : \mathfrak{I}.\mathbf{T}_\mathfrak{I}\to H_\mathfrak{I}^+.$$

By means of the theory of modular symbols ([32], [35], [39]) we shall be able to completely determine this homomorphism modulo $\mathfrak{I}$, and deduce a number of implications. As we do this it is of interest to keep track of how *little* use we shall make of all our previous work. We use only the assertions of Proposition (18.3) (those having to do with Eisenstein primes). These, in turn, are easy corollaries of the *(hard)* result: $\mathbf{T}_\mathfrak{P}$ is a Gorenstein ring, for $\mathfrak{P}$ an Eisenstein prime.

Lemma **(18.7)**. — $H^+/\mathfrak{I}.H^+$ *is a cyclic group of order* n. *There is a canonical* [1] *surjection* $\varphi : (\mathbf{Z}/N)^*\to H^+/\mathfrak{I}.H^+$ *which identifies* $H^+/\mathfrak{I}.H^+$ *with the Galois group of the Shimura covering* ((2.3); cf. § 11):

$$\frac{(\mathbf{Z}/N)^*}{(\pm 1)}\left\{\begin{array}{c}X_1(N)\\ \downarrow\\ X_2(N)\\ \downarrow\\ X_0(N)\end{array}\right\}H^+/\mathfrak{I}.H^+$$

Proof. — Since $H^+/\mathfrak{I}.H^+=H_\mathfrak{I}^+/\mathfrak{I}.H_\mathfrak{I}^+$ and since $H_\mathfrak{I}^+/\mathfrak{I}.H_\mathfrak{I}^+$ is free of rank 1 over $\mathbf{T}_\mathfrak{I}/\mathfrak{I}.\mathbf{T}_\mathfrak{I}$ by Proposition (18.3) and the discussion involving Diagram (18.1), it follows that $H^+/\mathfrak{I}.H^+$ is, indeed, a cyclic abelian group of order n (9.7).

---

(1) To *make* it canonical, one must make, somewhere, a specific choice of sign. Compare the next footnote and relevant text.

Let $\mathscr{S}$ denote the unique quotient of $(\mathbf{Z}/N)^*$ of order n. Thus $\mathscr{S}$ is a cyclic group which is canonically the Galois (covering) group of the Shimura covering (2.3). Since the Shimura covering is unramified (2.3) there is a canonical surjection $H \to \mathscr{S}$. Since $X_2(N) \to X_0(N)$ is defined over $\mathbf{Q}$ (and hence over $\mathbf{R}$) this canonical surjection factors, to give a surjection $H^+ \to \mathscr{S}$. Since (Proposition (11.7)) the Shimura subgroup is annihilated by $\mathfrak{I}$, this surjection factors to yield a surjection $H^+/\mathfrak{I}.H^+ \to \mathscr{S}$, which must be an isomorphism, since both domain and range have the same order. Q.E.D.

If a/b is a fraction where b is an integer relatively prime to N, let $\{a/b\} \in H$ denote the *modular symbol* [32], [35], ([39], § 6).

Proposition **(18.8).** — *(Congruence formula for the modular symbol.)*
Let a, b be integers with b relatively prime to N. *Let $\bar{b}$ denote the image of b in* $(\mathbf{Z}/N)^*$. *Let $\Phi(a/b) \in H^+/\mathfrak{I}.H^+$ denote the image of the modular symbol $\{a/b\}$ in $H^+/\mathfrak{I}.H^+$. Then:*

$$\Phi(a/b) = \varphi(\bar{b}^{-1}) \in H^+/\mathfrak{I}.H^+.$$

(Compare footnote in Section (6.15) of [32].)

Proof. — Here we again (as in the Proof of (11.7)) make use of Ogg's terminology for the cusps of $\Gamma(N)$.

$$\begin{pmatrix} a \\ b \end{pmatrix} = \{p/q \in \mathbf{P}^1(\mathbf{Q}) \mid p \equiv a \bmod N;\ q \equiv b \bmod N;\ (p, q) = 1\}.$$

From the definition of the modular symbol, one sees that if $(b, a.N) = 1$, $\Phi(a/b)$ is that unique element of $\mathscr{S} \cong H^+/\mathfrak{I}.H^+$ which sends (the image in $X_2(N)$ of) the cusp $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ to (the image in $X_2(N)$ of) the cusp $\begin{pmatrix} a \\ b \end{pmatrix}$. Since an element $c \in (\mathbf{Z}/N)^*$ acts as the matrix $\begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix}$ (1) and since $\begin{pmatrix} a \\ b \end{pmatrix} \equiv \begin{pmatrix} 0 \\ b \end{pmatrix} \bmod \Gamma_1(N)$ provided $(b, N) = 1$, it follows that $\Phi(a/b)$ is the image of $\bar{b}^{-1}$ in $H^+/\mathfrak{I}.H^+$. Q.E.D.

Proposition **(18.9).** — *(Congruence formula for the winding homomorphism.)*
Let $\eta_\ell = 1 + \ell - T_\ell$. Let $\varepsilon^+ : \mathfrak{I}/\mathfrak{I}^2 \to H^+/\mathfrak{I}.H^+$ be the homomorphism induced from the winding homomorphism $e^+ : \mathfrak{I} \to H^+_{\mathfrak{I}}$.
Then:

$$\varepsilon^+(\eta_\ell) = \left(\frac{\ell - 1}{2}\right)\varphi(\bar{\ell}) \quad (\textit{in } H^+/\mathfrak{I}.H^+)$$

where ℓ is any prime number different from N.

Remarks. — First note that the right-hand side makes sense. For if $\ell = 2$, and $p = 2$ divides n, then $N \equiv 1 \bmod 8$. By the quadratic reciprocity theorem $\bar{2} \in (\mathbf{Z}/N)^*$

(1) We follow Ogg in making this choice.

is then a quadratic residue ($\bar{2}=x^2$), and consequently $\left(\frac{\ell-1}{2}\right)\varphi(\bar{\ell})=\varphi(x)$. In any other case, the 2 in the denominator is harmless.

The assertion of (18.9) may be viewed as a congruence formula for numbers of rational points over $\mathbf{F}_\ell$. For example, in the first nontrivial case, $N=11$, it was first proved by Serre, and takes the following shape: Let N_ℓ denote the number of rational points of the elliptic curve $X_0(11)$ over $\mathbf{F}_\ell$ ($\ell\neq 11$). Let $\xi : (\mathbf{Z}/11)^*\to\mathbf{Z}/5$ be the homomorphism which sends $-3\in(\mathbf{Z}/11)^*$ to 2 mod 5. Then:

$$N_\ell\equiv -5(\ell-1).\xi(\ell) \bmod 25.$$

Proof of (18.9). — Our proposition follows immediately from the formula:

$$(1+\ell-T_\ell).e=-\sum_{k \bmod \ell}\{k/\ell\}$$

(formula (8), § 6 of [39], compare (5.5) of [32]), together with Proposition (18.8), (18.3), and the definition of e^+.

Theorem **(18.10).** — *(Local principality of the Eisenstein ideal.)*

Let p be a prime number dividing n. Let $\mathfrak{P}$ be the associated Eisenstein prime. Let ℓ be a prime number different from N. *Then η_ℓ is a generator of the ideal $\mathfrak{I}_\mathfrak{P}=\mathfrak{I}.\mathbf{T}_\mathfrak{P}\subset\mathbf{T}_\mathfrak{P}$ if and only if ℓ is a good prime number (with respect to p).*

The winding homomorphism $e^+ : \mathfrak{I}_\mathfrak{P}\to H^+_\mathfrak{P}$ is an isomorphism of $\mathbf{T}_\mathfrak{P}$-modules.

Proof. — Reducing the above winding homomorphism mod $\mathfrak{I}_\mathfrak{P}$ one gets the homomorphism $\varepsilon^+ : \mathfrak{I}_\mathfrak{P}/\mathfrak{I}_\mathfrak{P}^2\to H^+_\mathfrak{P}/\mathfrak{I}_\mathfrak{P}.H^+_\mathfrak{P}$ and by Proposition (18.9), the element η_ℓ maps to a generator of $H^+_\mathfrak{P}/\mathfrak{I}_\mathfrak{P}.H^+_\mathfrak{P}$ if and only if $\left(\frac{\ell-1}{2}\right)$ is not congruent to 0 mod p and ℓ is not a p-th power mod N (if we are not in the special case $\ell=p=2$). In the case $\ell=p=2$, Proposition (18.9) assures us that ℓ maps to a generator if and only if ℓ is not a quartic residue mod N. Thus, η_ℓ maps to a generator if and only if ℓ is a good prime. Since good primes do, indeed, exist, we deduce that $e^+ : \mathfrak{I}_\mathfrak{P}\to H^+_\mathfrak{P}$ is surjective, by Nakayama's lemma. By counting dimensions over $\mathbf{Q}_p$, we obtain that:

$$e^+\otimes\mathbf{Q}_p : \mathfrak{I}_\mathfrak{P}\otimes_{\mathbf{Z}_p}\mathbf{Q}_p\to H^+_\mathfrak{P}\otimes_{\mathbf{Z}_p}\mathbf{Q}_p$$

is an isomorphism. Since $\mathfrak{I}_\mathfrak{P}$ is torsion-free as a $\mathbf{Z}_p$-module, it follows that $e^+ : \mathfrak{I}_\mathfrak{P}\to H^+_\mathfrak{P}$ is an isomorphism. Since $H^+_\mathfrak{P}$ is free of rank 1 over $\mathbf{T}_\mathfrak{P}$, our theorem follows.

Remark. — Except for the " only if " part of the theorem and the assertion concerning the winding homomorphism, the " new " information conveyed by (18.10) is for $p=2$. For odd p, it is a curious alternate to the methods of § 16, for (starting with Corollary 16.3. The Gorenstein property for $\mathbf{T}_\mathfrak{P}$) it enables us to quickly retrieve the results of § 16 in their full strength.

If $\mathfrak{M}$ is a maximal non-Eisenstein prime in $\mathbf{T}$, then the winding element e is naturally

contained in $H_{\mathfrak{M}+}$. Thus if $\mathfrak{M}$ is such that $H_{\mathfrak{M}+}$ is free over $\mathbf{T}_{\mathfrak{M}}$ of rank 1 (*e.g.*, if char $k_{\mathfrak{M}} \neq 2$; cf. (18.3)) then, choosing some identification between the $\mathbf{T}_{\mathfrak{M}}$-modules $H_{\mathfrak{M}+}$ and $\mathbf{T}_{\mathfrak{M}}$, e will correspond to some element in $\mathbf{T}_{\mathfrak{M}}$. The principal ideal $e_{\mathfrak{M}} \subset \mathbf{T}_{\mathfrak{M}}$ generated by this element is independent of the choice made and shall be called the *winding ideal associated to* $\mathfrak{M}$.

19. The structure of the algebra $\mathbf{T}_{\mathfrak{P}}$.

Fix p a prime dividing n, and $\mathfrak{P}$ the associated Eisenstein prime. We know (18.10) that if ℓ is any good prime number, η_ℓ generates the Eisenstein ideal $\mathfrak{I}_{\mathfrak{P}} \subset \mathbf{T}_{\mathfrak{P}}$, and $\mathfrak{I}_{\mathfrak{P}} = \mathbf{Z}_p[\eta_\ell]$. Let $R_\ell(x) \in \mathbf{Z}_p[x]$ be the minimal monic polynomial satisfied by η_ℓ over $\mathbf{Z}_p$. Thus $\mathbf{T}_{\mathfrak{P}} = \mathbf{Z}_p[x]/(R_\ell)$. Denote by g_p the rank of $\mathbf{T}_{\mathfrak{P}}$ as $\mathbf{Z}_p$-module, or equivalently, the degree of $R_\ell(x)$. Since $\mathbf{T}_{\mathfrak{P}}$ is local and η_ℓ is in $\mathfrak{P}$, R_ℓ is a " distinguished polynomial " (*i.e.* $R_\ell(x) \equiv x^{g_p} \bmod p\mathbf{Z}_p[x]$). Since $\mathbf{T}_{\mathfrak{P}}/\eta_\ell . \mathbf{T}_{\mathfrak{P}} \cong \mathbf{Z}/p^f$ where $p^f \| n$, the constant term of $R_\ell(x)$ has p-adic valuation f. Since, if ℓ and ℓ' are *two* good prime numbers, η_ℓ and $\eta_{\ell'}$ are associate in the ring $\mathbf{T}_{\mathfrak{P}}$, the Newton polygons of $R_\ell(x)$ and $R_{\ell'}(x)$ are equal. One might call the common Newton polygon of $R_\ell(x)$ for ℓ any good prime number, *the Newton polygon of* $\mathbf{T}_{\mathfrak{P}}$ (or, more strictly speaking, of $\mathfrak{I}_{\mathfrak{P}}$).

Is there anything general that can be said about the Newton polygon of $\mathbf{T}_{\mathfrak{P}}$, or even about g_p?

One has hardly enough numerical data to begin serious speculation about this question. As far as my calculations go ($N < 250$) there is only one instance where $\mathbf{T}_{\mathfrak{P}}$ is not a discrete valuation ring ($N = 113, p = 2$) [1]. In this case $f = 2$, $g_p = 3$, and the Newton polygon is the only *possible* one conforming to this data.

There is no practical difficulty in computing the Newton polygon of $\mathbf{T}_{\mathfrak{P}}$, using *(e.g.)* the tables of Wada [70]. Wada gives the characteristic polynomial of T_ℓ (call it $S_\ell(x)$) acting on the parabolic modular forms for $\Gamma_0(N)$. The most straightforward thing to do is to look for the smallest good prime number ℓ such that $S_\ell(1+\ell)$ has p-adic valuation f [2]. For such a prime number ℓ, $R_\ell(x)$ is simply the " Weierstrass-prepared part " of $S_\ell(1+\ell-x)$.

Proposition (**19.1**). — *Suppose* $p \| n$ (i.e. $f = 1$). *Then* $\mathbf{T}_{\mathfrak{P}}$ *is a discrete valuation ring, totally ramified over* $\mathbf{Z}_p$, *of ramification index* g_p.

Proof. — In this case, the maximal ideal $\mathfrak{P} = \mathfrak{I}_{\mathfrak{P}}$, and is principal, by (18.10).

Proposition (**19.2**). — *Let* $p \neq 2$, $p^f \| n$ ($f \geq 1$). *The natural auto-duality of* $J[p^f]$ *restricts to a nondegenerate auto-duality of* $C_p \oplus \Sigma_p$ *(the direct sum of the p-primary components*

(1) As we shall see (chap. III, § 5) if we avail ourselves of certain standard conjectures, this instance is the *first* of an infinite series of analogous instances (all with $p = 2$).

(2) In practice one does not have to go far to find one, at least when $N < 250$.

of the cuspidal and Shimura subgroups) if and only if $\mathbf{T}_{\mathfrak{P}} = \mathbf{Z}_p$ (i.e. $g_p = 1$). *In particular, the element u (end of* § 11) *is a generator of the p-primary component of* U *if and only if* $g_p = 1$.

Proof. — If $\mathbf{T}_{\mathfrak{P}} = \mathbf{Z}_p$, then $C_p \oplus \Sigma_p = J_{\mathfrak{P}}[p^f]$, and on the latter group the natural auto-duality (11.12) is nondegenerate. Conversely, suppose the natural auto-duality of $J_{\mathfrak{P}}[p^f]$ restricts to a nondegenerate auto-duality of $C_p \oplus \Sigma_p$. Then the natural auto-duality of $J_{\mathfrak{P}}[p]$ would restrict to a non-degenerate pairing of $C[p]$ with $\Sigma[p]$. By (18.3) $J_{\mathfrak{P}}[p](\overline{\mathbf{Q}})$ is free of rank 2 over $\mathbf{T}_{\mathfrak{P}}/p.\mathbf{T}_{\mathfrak{P}}$, which by the above discussion is isomorphic to $\mathbf{F}_p[\eta_\ell]$ where η_ℓ satisfies the relation $\eta_\ell^{g_p} = 0$ (over $\mathbf{F}_p$). One sees immediately that $J_{\mathfrak{P}}[p, \eta_\ell](\overline{\mathbf{Q}})$ (which is the kernel of η_ℓ in $J_{\mathfrak{P}}[p](\overline{\mathbf{Q}})$) is the image of $\eta^{g_p - 1}$. If $g_p - 1 > 0$, the relation $(\eta^{g_p - 1}x, y) = (x, \eta^{g_p - 1}y)$ gives us that the natural auto-duality restricts to zero on $C[p] \oplus \Sigma[p]$, contrary to assumption.

Remark. — The only instances ($N < 250$, $p \neq 2$) where $g_p > 1$ are: $N = 31$, 103, 127, 131, 181, 199 and 211.

III. — ARITHMETIC APPLICATIONS

1. Torsion points.

Lemma (1.1). — *Let* $A_{/\mathbf{Q}}$ *be any quotient abelian variety of* $J_{/\mathbf{Q}}$. *Let p be a prime number dividing the order of the torsion subgroup* $A(\mathbf{Q})_{\text{tors}}$ *of the Mordell-Weil group of* $A_{/\mathbf{Q}}$. *Then p divides n.*

If $A_{/\mathbf{Q}}$ *is a quotient abelian variety of* $J_{/\mathbf{Q}}$ *on which* **T** *operates in a manner compatible with its action on* $J_{/\mathbf{Q}}$, *then* $A(\mathbf{Q})_{\text{tors}}$ *is annihilated by a power of the Eisenstein ideal* $\mathfrak{I}$.

Let $A_{/\mathbf{Q}}$ *be a simple (equivalently:* **C***-simple or* **Q***-simple*; cf. chap. II (10.1)) *quotient abelian variety of* $J_{/\mathbf{Q}}$ *such that the prime number p divides the order of* $A(\mathbf{Q})_{\text{tors}}$. *Then* $A_{/\mathbf{Q}}$ *is a quotient of the p-Eisenstein quotient* $\tilde{J}^{(p)}$ (10.4).

Proof. — Start with the first assertion. Consider the surjective morphism of associated p-divisible groups over $\mathbf{Q}$, $J_p \to A_p$. If r is large enough, the image of the finite group scheme $J[p^r]$ in A_p contains $A[p]$. Find a Jordan-Hölder filtration of $J[p^r]$, as $\mathbf{T}[\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module. Since, by hypothesis, there is a point of $A[p]$, defined over $\mathbf{Q}$, some successive quotient of the Jordan-Hölder filtration must have trivial $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-action. By (chap. II (14.1)), this subquotient of $J[p^r]$ belongs to [1] an Eisenstein prime $\mathfrak{P}$, necessarily associated to p. Therefore p divides n (chap. II (9.7)).

The second assertion is similar, but easier. Every successive quotient of a Jordan-Hölder filtration of the $\mathbf{T}[\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$ module $A(\mathbf{Q})_{\text{tors}}$ must belong to some Eisenstein prime, by chapter II (14.1). By the Mordell-Weil theorem, $A(\mathbf{Q})_{\text{tors}}$ is a finite group, and is therefore annihilated by some (finite) power of $\mathfrak{I}$.

---

[1] In the terminology of § 14.

The third assertion depends upon the one-to-one correspondence of chapter II (10.1) where isogeny classes of simple abelian variety factors of J are " identified " with irreducible components of Spec **T**. Since p divides the order of $A(\mathbf{Q})_{\text{tors}}$, by what we have already shown, the irreducible component of Spec **T** corresponding to the (isogeny class of the) simple abelian variety quotient A must contain the Eisenstein prime $\mathfrak{P} \in \text{Spec } \mathbf{T}$ associated to p.

Since $\tilde{J}^{(p)} = J/\gamma_{\mathfrak{P}} \cdot J$ where $\gamma_{\mathfrak{P}} = \bigcap_r \mathfrak{P}^r$ (chap. II (10.4)) it follows that, up to isogeny, $\tilde{J}^{(p)}$ is a product of those simple factors corresponding to irreducible components of Spec(**T**) containing $\mathfrak{P}$. Since $\tilde{J}^{(p)}$ is the quotient of J by a *connected* subgroup scheme, it follows that $J \to A$ factors through $\tilde{J}^{(p)}$.

Theorem (**1.2**). — (Conjecture of Ogg):

$$C = J(\mathbf{Q})_{\text{tors}}.$$

(*Any rational torsion point of* J *is a multiple of* $c = \mathcal{C}\ell((0) - (\infty))$.)

Proof. — Set $M = J(\mathbf{Q})$ (the Mordell-Weil group of J) and recall the retraction $\rho : M \to C \subset M$ of chapter II, § 11, giving rise to the direct product decomposition $M = M^0 \times C$ (chap. II (11.4)). It follows that C is a direct factor of $M_{\text{tors}} = J(\mathbf{Q})_{\text{tors}}$. By (1.1) it suffices to show $M^0[\mathfrak{P}] = 0$ for all Eisenstein primes $\mathfrak{P}$. But this follows from the inclusion $C[\mathfrak{P}] \times M^0[\mathfrak{P}] \subset J[\mathfrak{P}]$, and the determination of $J[\mathfrak{P}]$ (chap. II (16.3) or (for $p \neq 2$) (14.10)).

Theorem (**1.3**). — *The Shimura subgroup* Σ *is the maximal* μ*-type subgroup in* $J_{/S'}$.

Proof. — The sum of two (finite) μ-type subgroups of J is again a (finite) μ-type group. It suffices to show that if Σ' is a (finite) μ-type subgroup of J containing Σ, then $\Sigma' = \Sigma$. We first show that Σ is a direct summand in Σ'. Using the universal property of the Néron model $J_{/S}$ (and the fact that the inertia group at N operates trivially in the Galois module associated to Σ') one has that the subgroup scheme extension $\Sigma'_{/S} \subset J_{/S}$ is a finite flat (μ-type) subgroup scheme. Consider specialization to characteristic N, where one obtains a diagram:

$$\begin{array}{ccc} \overline{\Sigma}' & \longrightarrow & J_{/\mathbf{F}_N} = J^0_{/\mathbf{F}_N} \times \overline{C} \\ \uparrow & & \downarrow \\ \overline{\Sigma} & \xrightarrow{\approx} & \overline{C} \end{array}$$

(the left arrow is $\subseteq$, the right arrow is proj_2)

where $^-$ denotes specialization, and where the bottom horizontal map is an isomorphism, by chapter II (11.9).

It follows that $\overline{\Sigma}$ is a direct summand of $\overline{\Sigma}'$ and one easily obtains from this that

Σ is a direct summand in Σ'. Write $\Sigma' = \Sigma \oplus B$ where B is a μ-type group. Applying chapter II (14.1), one has that every successive quotient of a Jordan-Hölder filtration of B belongs to an Eisenstein prime. It suffices to show that $B[\mathfrak{P}] = 0$ for all Eisenstein primes. But $\Sigma[\mathfrak{P}] \oplus B[\mathfrak{P}] \subset J[\mathfrak{P}]$, and $B[\mathfrak{P}]$ must therefore vanish, by chapter II (16.3).

Remarks. — Theorem (1.3) was also conjectured by Ogg [48]. Although (1.2) and (1.3) have the appearance of being of comparable difficulty, there are notable differences between them. Ignoring 2-torsion, Theorem (1.3) is far easier than Theorem (1.2) (it uses only chap. II (14.10), and does not depend on the Gorenstein condition). In dealing with the 2-torsion subgroup of $J(\mathbf{Q})$, however, one must control subgroup schemes of $J_{/\mathbf{S}}$ isomorphic to $\mathbf{Z}/2$ as well as subgroup schemes isomorphic to μ_2 (since either will contribute to a point of order 2 in $J(\mathbf{Q})$). Consequently, this requires the full strength of chapter II (16.3), *e.g.*, all of chapter II, § 17.

Corollary **(1.4).** — *The natural maps induce isomorphisms of torsion subgroups of Mordell-Weil groups*:

$$C = J(\mathbf{Q})_{\text{tors}} \to J^-(\mathbf{Q})_{\text{tors}} \to \tilde{J}(\mathbf{Q})_{\text{tors}}$$

(cf. chap. II, § 10).

Proof. — By (1.1) one has that $J^-(\mathbf{Q})_{\text{tors}}$ and $J(\mathbf{Q})_{\text{tors}}$ are annihilated by a power of the Eisenstein ideal $\mathfrak{I}$. We shall show that the natural maps:

$$J_{\mathfrak{I}} \to J^-_{\mathfrak{I}} \to \tilde{J}_{\mathfrak{I}}$$

are isomorphisms. The map $J_{\mathfrak{I}} \to J^-_{\mathfrak{I}}$ is an isomorphism since $((1+w).J)[\mathfrak{I}] = 0$ (chap. II (17.10)). The map $J_{\mathfrak{I}} \to \tilde{J}_{\mathfrak{I}}$ is an isomorphism since its kernel is $\gamma_{\mathfrak{I}} . J_{\mathfrak{I}}$ and the supports of $\mathbf{T}/\mathfrak{I}$ and of $\gamma_{\mathfrak{I}} = \bigcap_r \mathfrak{I}^r$ are disjoint.

Corollary **(1.5).** — *The Mordell-Weil group of* $J_+ = (1+w).J$ *is torsionfree.*

2. Points of complex multiplication.

In this section we examine a set of points of $X_0(N)$ defined over fields of particularly low degree. A somewhat larger class has been studied by Birch and Stephens (called *Heegner points*).

Fix N (a prime number ≥ 5, as usual) and work over the field of complex numbers. If $E_{/\mathbf{C}}$ is an elliptic curve, an N-*isogeny by complex multiplication* $\pi : E \to E$ is an endomorphism such that $\ker \pi$ is of order N. Thus, π is a complex multiplication of E such that if R is the ring of complex multiplications of E, $\pi . \bar{\pi} = u . N$ where u is a unit in R. Let $a_{E,\pi} = j(E, \ker \pi) \in X_0(N)(\mathbf{C})$, which we will refer to as a *point of complex multiplication.*

If $a = a_{E,\pi}$ is a point of complex multiplication, set:

$R(a)$ = the ring of endomorphisms of E. The ring $R(a)$ is an order in a quadratic imaginary field $k(a)$ which may be viewed as naturally imbedded in $\mathbf{C}$ (since

$\mathrm{End}(\mathrm{Tan}(E_{/\mathbf{C}}))=\mathbf{C}$ and $R(a)$ acts faithfully on $\mathrm{Tan}(E_{/\mathbf{C}})$, the tangent space of $E_{/\mathbf{C}}$.

$\Lambda(a)=$ a sublattice of $\mathbf{C}$ such that $\mathbf{C}/\Lambda(a)\cong E$. It is well known (cf. [29]) that $\Lambda(a)$ is a locally free $R(a)$-module of rank 1.

$\pi(a)=\pi$. It is an element in $R(a)$ of norm N.

Given a triple (R, Λ, π) where $R\subset\mathbf{C}$ is an order in a quadratic imaginary field, Λ is a locally free R-module of rank 1, taken up to isomorphism, and π is an element of R of norm N, given up to multiplication by a unit in R, then we may construct a unique point of complex multiplication $a=a_{(R,\Lambda,\pi)}\in X_0(N)(\mathbf{C})$ such that $R=R(a)$, $\Lambda=\Lambda(a)$, and $\pi=\pi(a)$. Let $\mathscr{A}\subset X_0(N)(\mathbf{C})$ denote the set of all points of complex multiplication. It is easy enough to produce elements of $\mathscr{A}$. Consider equations:

$$N=r^2+D.s^2$$

where D is a positive integer not necessarily square-free and r, s are either both positive integers, or both positive half-integers (1). If $D=1$, suppose $r>s$. Let $\pi=r\pm\sqrt{-D}.s$ and let R be an order in $\mathbf{Q}(\sqrt{-D})$ containing π. Finally let Λ be a locally free R-module of rank 1 (*e.g.*, R itself).

The points of complex multiplication are defined over algebraic number fields which are studied in detail by the classical theory of complex multiplication (cf. [29], chap. 10, § 3, theorem 5 and remarks 1, 2 following it). We give a synopsis of this theory below:

(2.1) Let R be an order in a quadratic imaginary field $k\subseteq\mathbf{C}$ and $(\pi)\subset R$ a principal ideal of norm N. Let $\Lambda_1, \ldots, \Lambda_{h(R)}$ run through a system of representatives of isomorphism classes of locally free R-modules of rank 1. Set $a_i=a_{(R,\Lambda_i,\pi)}\in\mathscr{A}$. Then the points $a_1, \ldots, a_{h(R)}\in X_0(N)(\mathbf{C})$ are rational over $\bar{\mathbf{Q}}=\bar{k}$ and are a full set of conjugates over k. Let G denote the quotient of $\mathrm{Gal}(\bar{k}/k)$ which acts faithfully on the above set of conjugate points. There is an isomorphism $(\sigma\mapsto\Lambda_\sigma)$ of G onto H(R), the group of isomorphism classes of locally free R-modules of rank 1, such that if $\sigma\in G$, then $\sigma(a_1)=a_i$, where $\Lambda_1\underset{R}{\otimes}\Lambda_\sigma=\Lambda_i$.

The group G cuts out that ray class field L of k whose conductor is the conductor of R. The field extension $L/\mathbf{Q}$ is Galois, with Galois group $\tilde{G}$. We may write $L=k(j(R))\subset\mathbf{C}$ in which case the real subfield $L^+=L\cap\mathbf{R}$ is given by $L^+=\mathbf{Q}(j(R))$. Let ρ denote the nontrivial element of $\mathrm{Gal}(L/L^+)=\mathrm{Gal}(k/\mathbf{Q})$. Then $\tilde{G}$ is a semi-direct product of G and the group $\{1, \rho\}$ where the action of ρ is given by $\rho g\rho^{-1}=g^{-1}$ for $g\in G$. Thus $\tilde{G}$ is a dihedral extension of G. One has:

(2.2) $$\rho.a_{(R,\Lambda,\pi)}=a_{(R,\Lambda^{-1},\bar{\pi})}.$$

(1) H. Lenstra and P. Van Emde Boas have tables of the smallest such D for a given $N<500{,}000$.

The action of the canonical involution w on $\mathscr{A}$ is easily determined:

(2.3) $$w.a_{(R,\Lambda,\pi)} = a_{(R,\Lambda,\bar{\pi})}.$$

Let $a \in X_0(N)(\mathbf{C})$ be a fixed point of w. Then a is represented by an isogeny $E \xrightarrow{\pi} E'$ which is isomorphic to $E' \xrightarrow{\bar{\pi}} E$ (its dual). It follows that $E' \cong E$ and consequently the isogeny must be a complex multiplication $E \xrightarrow{\pi} E$ and $\pi^2 = u.N$ where u is a unit in $R(a)$. Multiplying π by a unit in $R(a)$, if necessary, we may suppose that $\pi = \sqrt{-N}$. Consequently, R is either $\mathbf{Z}[\sqrt{-N}]$ or $\mathbf{Z}\left[\frac{1+\sqrt{-N}}{2}\right]$, where the latter case may occur only if $N \equiv -1 \bmod 4$.

Using classical facts concerning the class numbers of the orders $\mathbf{Z}[\sqrt{-N}]$ and $\mathbf{Z}\left[\frac{1+\sqrt{-N}}{2}\right]$ ([28], chap. 8, § 1, th. 7) we may give the following description of the fixed point set of w. Let $h(N)$ be the class number of $\mathbf{Q}(\sqrt{-N})$. If $N \equiv 1 \bmod 4$, then the fixed point set of w consists in one $\mathbf{Q}$-conjugacy class of $h(N)$ points. If $N \equiv -1 \bmod 4$ it consists in two distinct $\mathbf{Q}$-conjugacy classes, the first containing $h(N)$ points and the second containing $h(N)$ or $3h(N)$ points according as $N \equiv -1 \bmod 8$ or $N \equiv 3 \bmod 8$.

Proposition **(2.4)**. — *Let a be a point of complex multiplication and let $a^+ \in X_0(N)^+(\mathbf{C})$ be its image in $X_0(N)^+ = X_0(N)/w$. Then a^+ is defined over $\mathbf{Q}$ if and only if the class number of $R(a)$ is 1.*

Proof. — This follows immediately from (2.1) and (2.3).

Such points $a^+ \in X^+$ are examples of rational noncuspidal points. It is natural to refer to them as *points of class number one.* One obtains a point a^+ of class number one for *each* order R (in a quadratic imaginary field) of class number one, in which N splits or ramifies.

Note that if N splits or ramifies in any one of the 9 quadratic imaginary fields of class number one, there *are* some points of class number one on the associated X^+. This is the case, for example, for all prime numbers $N < 7000$ except for $N = 3167$, as was communicated to me by H. Lenstra and P. Van Emde Boas. The Dirichlet density of primes N whose associated X^+ possesses no point of class number 1 is $1/512$.

What *further* noncuspidal rational points does the curve X^+ possess?

This diophantine question (when the genus $g^+ > 0$) is extremely interesting, since no known method appears to be applicable to it, for *any* value of N. In the first nontrivial case ($N = 67$) the genus of X^+ is 2. A. Brumer has obtained its hyperelliptic representation, and has begun a numerical study.

When $h(N) = 1$, the description of the fixed point set of w given above shows that there is a (unique) rational point $a \in X_0(N)(\mathbf{Q})$ fixed under w.

Proposition **(2.5)** (*compare* [48]). — *Let* $N=11, 19, 43, 67,$ *or* 163. *Then* $X_0(N)$ *possesses a rational point fixed under the action of* w. *Moreover* (*when* $g=$ *genus* $X_0(N)>0$) *these are all the points of complex multiplication in* $X_0(N)(\mathbf{C})$ *which are rational.*

Recall that $J_+=(1+w).J\subset J$ may be identified with the jacobian of $X_0(N)^+$ (cf. chap. II, proof of (13.8)). We shall produce some rational points in J_+.

If $R\subset\mathbf{C}$ is a fixed order in a quadratic imaginary number field such that the ideal generated by N splits into a product of conjugate principal ideals:

$$(N)=(\pi)(\bar{\pi}),$$

let $a_R^+\in J_+$ be the linear equivalence class containing the divisor:

$$\sum_{\Lambda\in H(R)} a^+_{(R,\Lambda)}-h(R).(\infty)$$

where $a^+_{(R,\Lambda)}$ is the common image of $a_{(R,\Lambda,\pi)}$ and $a_{(R,\Lambda,\bar{\pi})}$ in X^+, $\infty\in X^+$ is the unique cusp and $h(R)$ is the order of $H(R)$.

By (2.1-3) a_R^+ is defined over $\mathbf{Q}$, and therefore represents an element in the Mordell-Weil group of J_+.

To study these points we use a modification of an elegant trick due to Ogg: [49].

Lemma **(2.6)**. — *Let* d *be an integer.*

If the dimension of $H^0(X_0(N)^+_{/\mathbf{Q}};\mathcal{O}(d.\infty))$ *is* >1, *then* $d<N/96$.

Proof. — Suppose d is as in the assertion above. Using (chap. II, § 10), $J_{+/S'}$ is an abelian scheme. By ([9], VI, 6.7) one sees easily that $X_0(N)^+$ has a smooth model over S' (which we call $X^+_{/S'}$). Consider the base change $\operatorname{Spec}\mathbf{F}_4\to S'$. Using the upper-semi-continuity property (EGA III (7.7.5), I) one obtains that the dimension over $\mathbf{F}_4$ of $H^0(X^+_{/\mathbf{F}_4},\mathcal{O}(d.\infty))$ is also >1. Thus there is a morphism $f: X^+_{/\mathbf{F}_4}\to\mathbf{P}^1_{/\mathbf{F}_4}$ of degree d, such that the inverse image of the point ∞ of $\mathbf{P}^1$ is the divisor $d.\infty$ of X^+. Composing f with the projection $X\to X^+$, we obtain a map $g: X_{/\mathbf{F}_4}\to\mathbf{P}^1_{/\mathbf{F}_4}$ of degree $2d$ such that the inverse image of the point ∞ of $\mathbf{P}^1$ consist in the cusps. This gives us the upper bound $8d$ for the number of rational (noncuspidal) $\mathbf{F}_4$-valued points of $X_0(N)$. But, as Ogg remarked [49], all the supersingular points of $X_0(N)_{/\bar{\mathbf{F}}_2}$ are rational over $\mathbf{F}_4$ and there are more than $N/12$ of them.

Corollary **(2.7)**. — *If* R *is an order in a quadratic imaginary field such that the ideal generated by* N *splits into a product of conjugate principal ideals, and such that* $h(R)<N/96$, *then* a_R^+ *is a point of infinite order in the Mordell-Weil group of* J_+.

Proof. — By (1.5), the Mordell-Weil group of J_+ is torsion-free. Therefore it suffices to prove that $a_R^+\neq 0$. Suppose $a_R^+=0$. Then there would be a function f

on $X_{/\mathbf{Q}}^+$ whose divisor of poles is $h(R).(\infty)$. By (2.6) $h(R)>N/96$ contrary to assumption.

Proposition **(2.8)**. — *Suppose* $g^+>0$ (*which is the case for all* $N>73$, *as well as* $N=37, 43, 53, 61, 67$). *Then the Mordell-Weil group of* J_+ *is a torsion-free group of infinite order* (i.e. *of positive rank*).

Proof. — Write $4N=a^2+Db^2$ with a, b integers, $D>0$ and a^2 largest possible. One obtains $N=\pi.\bar{\pi}$ with π in R, the ring of integers of $\mathbf{Q}(\sqrt{-D})$ and if Δ is the discriminant of R, then $|\Delta|<4\sqrt{N}$. By a standard upper estimate for the class number $h(R)$, we have $h(R)\leq(1/3)|\Delta|^{1/2}.\log|\Delta|<(1/3)N^{1/4}\log(16N)$ if $|\Delta|>4$. A calculation shows that $(1/3).N^{1/4}\log(16N)<N/96$ when $N^{1/4}\geq 7$, or $N\geq 2401$. Thus by (2.7) a_R^+ is a point of infinite order when $N>2401$. But by the calculations of Lenstra and Van Emde Boas, $X_0(N)^+$ possesses a point of class number 1 (hence defined over $\mathbf{Q}$ (2.2)) for all $N<3167$ and therefore (2.8) follows.

Remarks. — 1. Using the estimates in the proof above one may show that if N is sufficiently large, each of the points $a_R^+\in X_0(N)^+$ is of infinite order.

2. The above theorem depends on the fact that $J_+(\mathbf{Q})$ is torsion-free, which, in turn, depends on the full strength of chapter II, § 17. It is significantly easier to show that $2.J_+(\mathbf{Q})$ is torsion-free (for one has far less to do with Eisenstein primes associated to 2). If one wishes to obtain the above proposition using only this weaker fact, one must prove that for same R, $2.a_R^+\neq 0$. The estimates give this for R as in the proof above, provided $N<7000$. We may then use the calculations of Lenstra and Van Emde Boas quoted above to reduce considerations to the one case: $N=3167$. But, quoting their tables, $3167=56^2+31.1^2$ and $\mathbf{Q}(\sqrt{-31})$ has class number 3. For:

$$R=\mathbf{Z}\left[\frac{1+\sqrt{-31}}{2}\right]$$

the estimates above enable us to conclude that $2.a_R^+\neq 0$.

3. Let $V^+=J_+(\mathbf{Q})\otimes\mathbf{Q}$ which we regard as a $\mathbf{T}^+\otimes\mathbf{Q}$ module, where:

$$\mathbf{T}^+=\mathbf{T}/(1-w)\mathbf{T}.$$

We have shown that V^+ is a $\mathbf{Q}$-vector space of positive dimension if $g^+>0$. Let V_e^+ (resp. $V_{c.m.}^+$) be the sub-$\mathbf{T}^+\otimes\mathbf{Q}$ of V^+ module generated by the point a_R^+ where R is the ring of integers in $\mathbf{Q}(\sqrt{-N})$ (resp. by all points of complex multiplication). Consideration of Dirichlet L-series and the Birch Swinnerton-Dyer conjectures might lead one to suspect that V_e^+ will play a significant role in studies of the Mordell-Weil group of J_+. It is tempting to hope that V_e^+ is always a free $\mathbf{T}^+\otimes\mathbf{Q}$ module of rank 1. Numerical evidence is too slim to make any conjectures yet, but Atkin has recently produced some interesting tables which bear on the problem.

3. The Mordell-Weil group of J.

The object of this section is to prove

Theorem (3.1). — *The natural projection* $J \to \tilde{J}$ *induces an isomorphism of the cuspidal subgroup* C *onto the Mordell-Weil group* $\tilde{J}(\mathbf{Q})$.

We shall also obtain complementary information concerning a part of the Shafarevich-Tate group of J. Our method will be to use " geometric descent " together with much of the information we have accumulated up to this point.

Let $\mathfrak{P}$ be an Eisenstein prime and $J^0 \subset J_{/S}$ the connected component containing the identity (which differs from J only in its fibre at N). Let $J^0[p^m]$ be the kernel of p^m, and $J^0[p^m]_{\mathfrak{P}}$ its $\mathfrak{P}$-*component* (which is the image of $J^0[p^m]$ under the idempotent $\varepsilon_{\mathfrak{P}}$ for the Eisenstein ideal, as discussed in chap. II, § 7).

Lemma (3.2). — $J^0[p^m]_{\mathfrak{P}}$ *is an admissible group* (chap. I, § 1(f)) *and when m varies, the order of* $H^1(S, J^0[p^m]_{\mathfrak{P}})$ *remains bounded.*

Proof. — It is admissible as can be easily seen by chapter II (14.1). Since $H^0(S, J^0[p^m]_{\mathfrak{P}})$ is a subgroup of the torsion part of the Mordell-Weil group of J, it is a finite group which has bounded order as m varies. Thus, to prove the lemma, it suffices to show that $h^1 - h^0$ has bounded order. But by chapter I, Prop. (1.7) it suffices, then, to prove that $\delta(J^0[p^m]_{\mathfrak{P}}) - \alpha(J^0[p^m]_{\mathfrak{P}})$ has bounded order.

This is done by showing:

(a) $$\delta(J^0[p^m]_{\mathfrak{P}}) = m.g_{\mathfrak{P}} + O(1)$$

(b) $$\alpha(J^0[p^m]_{\mathfrak{P}}) = m.g_{\mathfrak{P}} + O(1)$$

where $g_{\mathfrak{P}}$ is the rank of $\mathbf{T}_{\mathfrak{P}}$ over $\mathbf{Z}_p$.

Proof of (a). — Letting J_p denote the p-divisible group associated to J over S, and $J_{\mathfrak{P}}$ its $\mathfrak{P}$-component (*i.e.* the image of the idempotent $\varepsilon_{\mathfrak{P}}$) then $J[p^m]_{\mathfrak{P}} = J_{\mathfrak{P}}[p^m]$ and $J^0[p^m]_{\mathfrak{P}} = J^0_{\mathfrak{P}}[p^m]$ where the superscript 0 denotes, as usual, the inverse image of J^0. We now make use of the results and terminology of chapter I, § 8. Consider, in particular, the exact sequence chapter I (8.2):

$$0 \to \mathcal{E}a(J_{\mathfrak{P}}(\overline{\mathbf{F}}_N)) \to \mathcal{E}a(J_{\mathfrak{P}}(\overline{\mathbf{Q}}_N)) \to \Delta_{\mathfrak{P}} \to 0$$

where (8.3) $\Delta_{\mathfrak{P}}$ is a $\mathbf{T}_{\mathfrak{P}}$-module " of rank 1 " (*i.e.* it contains a free $\mathbf{T}_{\mathfrak{P}}$-module of rank 1 as a subgroup of finite index). One checks that:

$$\delta(J^0_{\mathfrak{P}}[p^m]) = \log_p(\text{order}(\Delta^{\vee}_{\mathfrak{P}}/p^m \Delta^{\vee}_{\mathfrak{P}})) + O(1)$$

where $^{\vee}$ denotes $\mathbf{Z}_p$-dual. Since $\Delta^{\vee}_{\mathfrak{P}}$ is also a $\mathbf{T}_{\mathfrak{P}}$-module of rank 1, we have:

$$\delta(J^0_{\mathfrak{P}}[p^m]) = \log_p(\text{order } \mathbf{T}_{\mathfrak{P}}/p^m \mathbf{T}_{\mathfrak{P}}) + O(1).$$

Proof of (b). — This follows the same lines as *(a)* above. One need only note that $\alpha(J^0_{\mathfrak{P}}[p^m]) = \log_p(\text{order}(J^0_{\mathfrak{P}}[p^m](\overline{\mathbf{F}}_p))) = \log_p(\text{order}(J^0_{\mathfrak{P}}[p^m]^{\text{ét}}_{/\mathbf{F}_p}))$ and since $\mathfrak{P}$ is an

ordinary prime, we have the exact sequence of chapter II, § 4 and chapter II, Proposition (8.5).

Lemma **(3.3).** — *Let* $M=J(\mathbf{Q})$ *be the Mordell-Weil group of* J, *regarded as* $\mathbf{T}$*-module. Then* $\mathbf{T}_{\mathfrak{P}}\otimes_{\mathbf{T}} M$ *and* $Ш_{\mathfrak{P}}$ (*the* $\mathfrak{P}$*-component of the Shafarevich-Tate group* Ш *of* J) *are finite groups.*

Proof. — Set $M^0=H^0(S, J^0)$ and note that $M=H^0(S, J)$. The quotient M/M^0 is finite. Therefore to show that $\mathbf{T}_{\mathfrak{P}}\otimes_{\mathbf{T}} M$ is finite it suffices to show that $\mathbf{T}_{\mathfrak{P}}\otimes_{\mathbf{T}} M^0$ is finite. The long exact sequence of cohomology associated to the exact sequence of *fppf* sheaves over S:

$$0\to J^0[p^m]\to J^0_{/S}\xrightarrow{p^m} J^0_{/S}\to 0$$

yields:
$$0\to M^0/p^m.M^0\to H^1(S, J^0[p^m])\to H^1(S, J^0)[p^m]\to 0$$

and, by passage to the limit as m tends to ∞, using the maps:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J^0[p^m] & \longrightarrow & J^0 & \xrightarrow{p^m} & J^0 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \subseteq} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle p} & & \\ 0 & \longrightarrow & J^0[p^{m+1}] & \longrightarrow & J^0 & \xrightarrow{p^{m+1}} & J^0 & \longrightarrow & 0 \end{array}$$

we obtain an exact sequence of $\mathbf{T}_p$-modules:

$$0\to \mathbf{Q}_p/\mathbf{Z}_p\otimes M^0\to \varinjlim_m H^1(S, J^0[p^m])\to H^1(S, J^0)_p\to 0$$

where the subscript p on the right means p-primary component. Passing to $\mathfrak{P}$-component (by applying the idempotent $\varepsilon_{\mathfrak{P}}$) we obtain:

$$0\to \mathbf{T}_{\mathfrak{P}}\otimes_{\mathbf{T}_p}(\mathbf{Q}_p/\mathbf{Z}_p\otimes M^0)\to \varinjlim_m H^1(S, J^0[p^m]_{\mathfrak{P}})\to H^1(S, J^0)_{\mathfrak{P}}\to 0.$$

Since the middle group is finite, by Lemma (3.2), the two flanking groups are. Since M^0 is a finitely generated group (by the theorem of Mordell-Weil), finiteness of $\mathbf{T}_{\mathfrak{P}}\otimes_{\mathbf{T}_p}(\mathbf{Q}_p/\mathbf{Z}_p\otimes M^0)$ implies finiteness of $\mathbf{T}_{\mathfrak{P}}\otimes_{\mathbf{T}_p} M^0$.

To see that $Ш_{\mathfrak{P}}$ is finite we use that (working modulo the category of groups whose order is a power of two) Ш may be identified with the image of $H^1(S, J^0)$ in $H^1(S, J)$ (Appendix of [34]), and the 2-primary component of Ш is a subgroup of the 2-primary component of this image. Finiteness of $Ш_{\mathfrak{P}}$ then follows from finiteness of $H^1(S, J^0)_{\mathfrak{P}}$.

To use (3.3) conveniently, we make a digression and recall the terminology of chapter II, § 10. Let $\mathfrak{a}\subset\mathbf{T}$ be any ideal of finite index in $\mathbf{T}$, $\gamma_{(\mathfrak{a})}=\bigcap_r \mathfrak{a}^r$, $\mathbf{T}^{(\mathfrak{a})}=\mathbf{T}/\gamma_{(\mathfrak{a})}$ (so $\mathbf{T}^{(\mathfrak{a})}$ maps injectively to the completion $\mathbf{T}_{\mathfrak{a}}$) and $J^{(\mathfrak{a})}=J/\gamma_{(\mathfrak{a})}.J$, the quotient associated to J (chap. II, § 10). Let $V=J(\mathbf{Q})\otimes\mathbf{Q}$ as $\mathbf{T}\otimes\mathbf{Q}$ module, and $V^{(\mathfrak{a})}=J^{(\mathfrak{a})}(\mathbf{Q})\otimes\mathbf{Q}$ as $\mathbf{T}^{(\mathfrak{a})}\otimes\mathbf{Q}$-module.

Lemma **(3.4).** — $V^{(\mathfrak{a})}=V/\gamma_{(\mathfrak{a})}.V=\mathbf{T}^{(\mathfrak{a})}\otimes_{\mathbf{T}}V$.

Proof. — On the category of abelian varieties over $\mathbf{Q}$, the functor $A\mapsto A(\mathbf{Q})\otimes\mathbf{Q}$ is exact since $A(\mathbf{Q})$ is finitely generated and $H^1(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), A)$ is a torsion group, for all A in the category. The lemma then follows by applying this exact functor to the diagram:

$$\begin{array}{ccccccccc} & & & & 0 & & & & \\ & & & & \uparrow & & & & \\ 0 & \longrightarrow & \gamma_{(\mathfrak{a})}.J & \longrightarrow & J & \longrightarrow & J^{(\mathfrak{a})} & \longrightarrow & 0 \\ & & & & \uparrow{\scriptstyle (\alpha,\ldots,\alpha_t)} & & & & \\ & & & & J\times J\times\ldots\times J & & & & \end{array}$$

where $\alpha_1, \ldots, \alpha_t$ is a system of generators of the ideal $\mathfrak{a}$.

Corollary **(3.5).** — *If* $\mathbf{T}_{\mathfrak{a}}\otimes_{\mathbf{T}}V=0$, *then the Mordell-Weil group of* $J^{(\mathfrak{a})}$ *is finite.*

Proof. — Let W be the torsion-free quotient of the Mordell-Weil group $J(\mathbf{Q})$. Thus W is a free $\mathbf{Z}$-module of finite rank and gives rise to a coherent sheaf over Spec $\mathbf{T}$. By hypothesis, the support of $\mathbf{T}_{\mathfrak{a}}\otimes_{\mathbf{T}}W$ contains no irreducible component of Spec $\mathbf{T}_{\mathfrak{a}}$. Since the support of $\mathfrak{a}$ meets every irreducible component of Spec $\mathbf{T}^{(\mathfrak{a})}$ it follows that the support of W contains no irreducible component of Spec $\mathbf{T}^{(\mathfrak{a})}$. The support of W then meets Spec $\mathbf{T}^{(\mathfrak{a})}$ in a finite union of closed points and (3.5) follows from Lemma (3.4).

Proof of Theorem (3.1). — Applying (3.3) for all Eisenstein primes we obtain that $\mathbf{T}_{\mathfrak{I}}\otimes_{\mathbf{T}}M$ is finite, where $\mathfrak{I}$ denotes the Eisenstein ideal. It then follows from (3.5) that $\tilde{J}(\mathbf{Q})$ is finite. The theorem follows from Corollary (1.4).

Proposition **(3.6).** — *Let* $\mathfrak{P}$ *be an Eisenstein prime associated to an odd prime number p. Then* $Ш_{\mathfrak{P}}=0$.

Proof. — We shall perform a more delicate descent to establish this. Let ℓ be a good prime number and $\eta=\eta_\ell$ (using the terminology of chap. II, § 16). Then η is an isogeny (cf. Proof of (16.10)); we consider:

$$\mathbf{(3.7)} \qquad 0\to\ker\eta\to J\xrightarrow{\eta}J\to\mathrm{coker}\,\eta\to 0$$

as an exact sequence of *fppf* sheaves of $\mathbf{T}$-modules over S. Let Δ denote a finite set of points in Spec $\mathbf{T}$, not containing $\mathfrak{P}$, but containing all other points in the support of the $\mathbf{T}$-modules $\ker\eta(\bar{\mathbf{Q}})$ and $\mathrm{coker}\,\eta(\bar{\mathbf{Q}})$. We shall work in the category of $\mathbf{T}$-modules, modulo the category of $\mathbf{T}$-modules whose supports lie in Δ (*modulo* Δ).

By chapter II (16.6) and (16.4) it follows that:

$$\ker\eta\equiv C_p\oplus\Sigma_p \quad \text{modulo } \Delta$$

and cok η is a skyscraper sheaf concentrated in characteristic N, whose stalk in characteristic N is isomorphic to the **T**-module C_p, modulo Δ.

Since C_p is a constant group over S and Σ_p is a μ-type group, we have (*e.g.*, chap. I (1.7)) that $H^1(S, C_p \oplus \Sigma_p) = 0$, and therefore $H^1(S, \ker \eta) \equiv 0$ modulo Δ. One obtains then the following exact sequence modulo Δ of *fppf* cohomology from the exact sequence (3.7):

$$0 \to C_p \to H^0(S, J) \xrightarrow{\eta} H^0(S, J) \xrightarrow{i} H^0(S, \text{coker } \eta).$$

Since $H^0(S, \text{coker } \eta) \equiv C_p$ modulo Δ, the above exact sequence shows that i is surjective modulo Δ. It also shows that η is automorphism, modulo Δ, of the torsion-free quotient of the Mordell-Weil group, which can be used as an alternative to the proof of Theorem (3.1), at least as it concerns odd Eisenstein primes. Reconsidering the exact sequence (3.7), surjectivity (modulo Δ) of the mapping i, gives that:

$$\eta : H^1(S, J) \to H^1(S, J)$$

is injective, modulo Δ. Since Ш is a submodule of $H^1(S, J)$, multiplication by η is also injective modulo Δ on Ш, which establishes our proposition.

Combining this with recent results of Brumer and Kramer [4] we may obtain:

Proposition **(3.8)**. — *Let* $N < 250$. *The natural map* $J \to J^-$ *induces an isomorphism of* C *onto the Mordell-Weil group* $J^-(\mathbf{Q})$ *except possibly in cases* $N = 151$, 199 *and* 227.

Proof. — From the table of the introduction, one sees that for $N < 250$, $J^- = \tilde{J}$ except for the following values of N:

$$N = 67, 109, 139, 151, 179, 199, 227$$

and when $N = 67, 109, 139, 179$, J^- differs from $\tilde{J}$ by an elliptic curve factor. Brumer and Kramer have shown (1) that these elliptic curve factors have finite Mordell-Weil groups over $\mathbf{Q}$. It then follows that $J^-(\mathbf{Q})$ is finite, using (3.1), for all values of N considered in Proposition (3.8). The assertion then follows from (1.4).

Recently, Atkin communicated to me that J^- is a simple abelian variety (and hence equal to $\tilde{J}$) for $N = 383, 419, 479, 491$, and consequently (3.8) holds for these values of N, as well.

4. Rational points on $X_0(N)$.

Theorem **(4.1)**. — *Let* $N \neq (2, 3), 5, 7$ *and* 13 (i.e. *the genus of* $X_0(N)$ *is* > 0). *Then* $X_0(N)(\mathbf{Q})$ *is finite.*

Proof. — Work over $\mathbf{Q}$, and consider the projection $X_0(N) \to \tilde{J}$ defined by $x \mapsto \text{image}(x - \infty)$ in $\tilde{J}$. Since $\tilde{J}$ is nontrivial and the image of $X = X_0(N)$ generates $\tilde{J}$

(1) See their forthcoming publication [4].

as a group variety, if $\tilde{X}$ is the image of X in $\tilde{J}$, then $\tilde{X}_{/\mathbf{Q}}$ is a curve, and $X \xrightarrow{\beta} \tilde{X}$ is a finite morphism. Since $\tilde{X}(\mathbf{Q}) \subset \tilde{J}(\mathbf{Q}) = C$ (3.1), $\tilde{X}(\mathbf{Q})$ is a finite set and therefore $X(\mathbf{Q})$ is also finite. To be sure, we have little control over this set if we know nothing concerning the structure of the finite morphism β. What is its degree? What are the singular points of the image?

Remark. — It is a theorem of Manin ([31], [65]) that for every number field K and integer $m \geq 1$, there is an integer $e(m, K)$ such that $X_0(m^e)(K)$ is finite for all $e \geq e(m, K)$, but no effective bound for $e(m, K)$ is obtained. I understand that the Russian mathematician Berkovich has recently obtained such effective bounds using the techniques of this paper, and in particular the techniques of the proof of (4.1).

To analyze the finite set $X(\mathbf{Q})$ we make use of the retraction $\rho : J(\mathbf{Q}) \to \mathbf{Z}/n$ of chapter II, § 11.

Proposition **(4.2).** — *If* $x \in X_0(N)(\mathbf{Q})$, *the element* $\rho(x)$ *of* $\mathbf{Z}/n$ *is equal to one of the following values*:

$$(4.2)\ \text{i)} \quad \begin{cases} 0 \text{ or } 1 \\ 1/2 \ (\textit{possible only if } N \equiv -1 \bmod 4) \\ 1/3 \text{ or } 2/3 \ (\textit{possible only if } N \equiv -1 \bmod 3). \end{cases}$$

Remarks. — 1. If $N \equiv -1 \bmod 3$, the integer n is not divisible by 3 and $1/3$ has a sense in $\mathbf{Z}/n$; similarly $1/2$ has a sense in $\mathbf{Z}/n$ when n is odd, which is the case if $N \equiv -1 \bmod 4$.

2. $\rho(0) = 1$ and $\rho(\infty) = 0$.

Proof of (4.2). — The point x extends (by Zariski closure) to a section of $X_0(N)_{/S}$. This section must lie in the smooth locus of $X_0(N) \to S$ and hence, if $\bar{x}$ is its pullback to $\mathrm{Spec}(\mathbf{F}_N)$, $\bar{x}$ must lie in exactly one irreducible component of the fiber $X_0(N)_{/\mathbf{F}_N}$ (see diagram 1 of chap. II, § 1). Thus, $\bar{x}$ lies on one of these:

$$(4.2)\ \text{ii)} \quad \begin{cases} Z' \text{ or } Z \\ E \text{ (possible only if } N \equiv -1 \bmod 4) \\ G \text{ or } F \text{ (possible only if } N \equiv -1 \bmod 3). \end{cases}$$

But the natural map $X_0(N)^{\text{smooth}}_{/\mathbf{F}_N} \to J_{/\mathbf{F}_N} \to C = \mathbf{Z}/n$ sends the five components listed in (4.2) ii) to the corresponding values listed in (4.2) i) as follows from the table of the appendix.

Let $J_- = (1 - w)J \subset J$. One obtains a map:

$$r : X_0(N) \to J_-$$

by the rule $x \mapsto cl((x) - (wx))$. If $x \in X_0(N)(\mathbf{Q})$, set $\lambda(x) = \rho(r(x)) \in \mathbf{Z}/n$.

Corollary **(4.3).** — *One has* $\lambda(x) = \pm 1, 0, \text{ or } \pm 1/3$.

Proof. — This follows from (4.2) and the fact that $\lambda(x) = 2\rho(x) - 1$.

Corollary **(4.4)**. — *Suppose* $J_-(\mathbf{Q})$ *is finite. Then*:

a) *One has* $J_-(\mathbf{Q})=C$.

b) *For all* $x\in X_0(N)(\mathbf{Q})$, *one has* $r(x)=\lambda(x).c$ *with* $\lambda(x)=\pm 1, 0,$ *or* $\pm 1/3$.

Proof. — Assertion a) comes from the fact that C is contained in $J_-(\mathbf{Q})$ and it is the torsion subgroup of $J(\mathbf{Q})$ (1.2). Assertion b) follows from (4.3) and the fact that ρ is the identity on C.

Remark. — By (3.8) and the remarks after it, (4.4) applies to at least these values: $N<250$, with the possible exceptions of $N=151, 199, 227$ and $N=383, 419, 479, 491$.

The next proposition is due mainly to Ogg and includes work of Parry and of Brumer.

Proposition **(4.5)**. — a) *If* $N\geq 23$ *and* $N=37$ *then the morphism* $r : X_0(N)\to J_-$ *is injective off the locus of fixed points of w.*

b) *If* $J_-(\mathbf{Q})$ *is finite, and* $x\in X_0(N)(\mathbf{Q})$, *one has*:

$$\lambda(x)=\pm 1/3 \Rightarrow N=11, 17$$

$$\lambda(x)=\ 0\ \Rightarrow N=11, 19, 43, 67, \text{ or } 163.$$

Discussion of the proposition. — The following is Ogg's proof of a). Suppose $x, y\in X_0(N)(\mathbf{C})$ such that $r(x)=r(y)$, $x\neq y$, and x is not fixed under w. Write $z=w(y)$ and we have:

$$x+z\equiv w(x)+w(z)$$

where $\equiv$ denotes linear equivalence on $X_0(N)$. Since $x+z$ is not invariant under w, it follows that $X_0(N)$ is a hyperelliptic curve, and moreover, the involution w is *not* the hyperelliptic involution. But Ogg ([38], theorem 1) has determined that $N=37$ is the only value of N such that $X_0(N)$ admits such a description. As for b), let $x\in X_0(N)(\mathbf{Q})$ be a point such that $\lambda(x)=\pm 1/3$. Then $N\equiv -1 \bmod 3$, and (replacing x by $w(x)$ if necessary) we may assume:

$$3x+(\infty)\equiv 3w(x)+(0).$$

By an elegant argument (end of [49]) Ogg shows that $n<240$. We recall the argument and sharpen this upper estimate a bit. Let $\bar{}$ denote specialization of a section over S to Spec $\mathbf{F}_4$. Then we have:

$$3\bar{x}+(\bar{\infty})\equiv 3w(\bar{x})+(\bar{0}),$$

yielding a function f on $X_0(N)_{/\mathbf{F}_4}$ such that the inverse image of the point $\infty\in\mathbf{P}^1(\mathbf{F}_4)$ is the divisor $3\bar{x}+(\bar{\infty})$ and the inverse image of $0\in\mathbf{P}^1(\mathbf{F}_4)$ is $3w(\bar{x})+(\bar{0})$.

Since the points of $X_0(N)(\mathbf{F}_4)$ different from $\bar{x}$, $w(\bar{x})$, $\bar{\infty}$, $\bar{0}$ must lie in the fibers of f above the 3 points of $\mathbf{P}^1(\mathbf{F}_4)$ different from ∞ and 0, we have:

$$\#\, X_0(N)(\mathbf{F}_4)\leq 16.$$

But Ogg has constructed [49] at least N/12 noncuspidal rational points in $X_0(N)(\mathbf{F}_4)$, so:

$$N/12+2\leq 16 \quad \text{or} \quad N\leq 168.$$

Let us now consider an argument which helps to eliminate many low values of N.

Find f a function from $X_0(N)_{/\mathbf{Q}}$ to $\mathbf{P}^1_{/\mathbf{Q}}$ whose divisor is $3x+\infty-3wx-0$. Define f^w by $f^w(z)=f(wz)$. Since $f.f^w$ has neither zeroes nor poles, it is a constant ε. Define an involution $w:\mathbf{P}^1\to\mathbf{P}^1$ by the formula $y\mapsto\varepsilon/y$. We obtain a commutative square:

$$\begin{array}{ccc} X & \xrightarrow{w} & X \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ \mathbf{P}^1 & \xrightarrow{w} & \mathbf{P}^1 \end{array}$$

and consequently f induces a rational map on quotients by w:

$$\begin{array}{ccccc} X & \xrightarrow{\pi} & X/w=X^+ & & \\ {\scriptstyle f}\downarrow & & \downarrow & & \downarrow{\scriptstyle f^+} \\ \mathbf{P}^1 & \xrightarrow{\pi} & \mathbf{P}^1/w=\mathbf{P}^{1+} & & \end{array}$$

The double covering $\mathbf{P}^1\to\mathbf{P}^{1+}$ has precisely 2 ramification points $y=\pm\sqrt{\varepsilon}$. Also, the map f^+ is of degree 4. Consequently, the double covering $\pi:X\to X^+$ can have *at most* $2.4=8$ ramification points. That is, the number of fixed points of w is ≤ 8. This condition is easily shown to be equivalent to the condition $g^- - g^+\leq 3$, by the Hurwitz formula applied to the covering $X\to X^+$, and one checks (*e.g.*, consult the table of introduction) that those N such that *a)* $N\leq 168$, *b)* $N\equiv -1 \bmod 3$, *c)* $g^- - g^+\leq 3$, are:

$$N=11,\ 17,\ 23,\ 29,\ 41,\ 53,\ 113, \text{ and } 137.$$

When $N=11,\ 17$, $X_0(N)$ is of genus 1, and there is a (unique) point $x\in X_0(N)(\mathbf{Q})$ such that $\lambda(x)=1/3$.

When $N=23,\ 29,\ 41$, $X_0(N)^+$ is of genus 0, and Ogg has special arguments to show that there are no rational points such that $\lambda(x)=1/3$ [49].

The remaining three cases have been ruled out by work of W. Parry and A. Brumer.

Finally, note that if $x\in X_0(N)(\mathbf{C})$, $\lambda(x)=0\Leftrightarrow x$ is a fixed point of w, and so the final assertion of (4.5) follows from (2.2) and the solution of the class number one problem (Heegner-Baker-Stark).

Remarks. — 1. By (3.8) and (4.5) we have determined all the rational points on all curves $X_0(N)$ for $N<250$, with the exception of $N=151$, 199 and 227.

2. *(Fields of low odd degree.)*

If $J_-(\mathbf{Q})$ is finite, Ogg's trick has strong implications concerning rational points of $X_0(N)$ in the *totality* of fields of a given degree. Brumer has some computations for degree 2, and we shall give a fragmentary result for degree 3. By a point on $X_0(N)$ *of degree d* we mean a point of $X_0(N)(\bar{\mathbf{Q}})$ defined over *any* extension field of degree d over $\mathbf{Q}$.

Proposition **(4.6).** — *If* $N=383, 419, 479,$ *or* 491, *then* $X_0(N)$ *has only a finite number of cubic points (points of degree* 3*).*

Proof. — Let d be any odd positive number. Let K_d be the set of all $\mathbf{Q}$-conjugacy classes of points of degree d in $X_0(N)(\bar{\mathbf{Q}})$ not containing a fixed point of w.

Define a mapping $\iota : K_d \to J_-(\mathbf{Q})$ by:

$$\kappa \mapsto \mathrm{cl}\Big(\sum_{x\in\kappa} x - \sum_{x\in\kappa} w(x)\Big).$$

Lemma **(4.7).** — *If (d is an odd positive number, and)* $N>120.d$, *then* $\iota : K_d \to J_-(\mathbf{Q})$ *is injective.*

Proof. — Suppose $\iota(\kappa)=\iota(\kappa')$ where $\kappa\neq\kappa'$. Writing $\kappa''=w(\kappa')$ we get a relation:

$$\textbf{(4.8)} \qquad \sum_{x\in\kappa} x + \sum_{y\in\kappa''} y \equiv \sum_{x\in\kappa} w(x) + \sum_{y\in\kappa''} w(y).$$

The above linear equivalence cannot be an identity of divisors, for by hypothesis w does not interchange the conjugacy classes κ and κ'', nor does w stabilize either conjugacy class. The reason for the latter assertion is that an involution of a finite set of odd cardinality must have a fixed point and the conjugacy classes containing fixed points of w are excluded from K_d.

Thus there is a nonconstant function f on $X_0(N)$ whose divisor of zeroes is the left-hand side of (4.8) and whose divisor of poles is the right-hand side.

Letting D be the Cartier divisor in $X_0(N)_{/S'}$ obtained by taking the closure of the right-hand side of (4.8), we have that $H^0(X_0(N)_{/\mathbf{F}_4}, \mathcal{O}(D))$ is of dimension >1, using (EGA III (7.7.5), I) as in the proof of Lemma (2.6). It follows that there is a mapping $f : X_0(N)_{/\mathbf{F}_4} \to \mathbf{P}^1_{/\mathbf{F}_4}$ of degree $2d$ and therefore $10.d$ is an upper bound for the cardinality of $X_0(N)(\mathbf{F}_4)$. Since this cardinality is greater than $N/12$, the lemma follows.

The proposition then follows by taking $d=3$, and using the *remark* after (4.4).

It is interesting to consider the problem of showing finiteness of $X_0(m)(\mathbf{Q})$ when $\mathrm{genus}(X_0(m))>0$, for *all* integers m. By (4.1) we may restrict attention to composite numbers m, and it is evident that it suffices to treat those composite numbers m such that $\mathrm{genus}\, X_0(d)=0$ for all proper divisors d of m. There are 17 such values of m, of which 9 are of genus 1 and have been shown to have finite Mordell-Weil groups, by various people, including Ligozat ([30], and see discussion in [48]). The case $m=26$

is treated in [41]. The cases $m=35, 50$ have been taken care of by Kubert [27]; the case $m=50$ was also done independently by Birch. The case $m=39$ has been settled by a descent argument on the elliptic curve quotient of $X_0(39)$ using an explicit equation given for this curve which can be found in an extensive table compiled by Kiepert. This equation (formula 631*b* on page 391 of [25]) and these useful tables were pointed out to me by Kubert. Re-writing the curve as a quotient defined over $\mathbf{Q}$, its minimal model is $y^2+xy=x^3+x^2-4x-5$ and the descent follows the lines of the case $m=35$ ([27], [34], § 9). Sixteen of the seventeen cases (all m above except $m=125$) have been covered by the recent work of Berkovich (cf. remark following (4.1)).

5. A complete description of torsion in the Mordell-Weil group of elliptic curves over Q.

In this section we shall prove the following theorem, first conjectured by Ogg [49]:

Theorem (5.1). — *Let* Φ *be the torsion subgroup of the Mordell-Weil group of an elliptic curve* E, *over* $\mathbf{Q}$. *Then* Φ *is isomorphic to one of the following 15 groups*:

$$\mathbf{Z}/m\mathbf{Z} \quad \textit{for} \quad m\leq 10 \quad \textit{or} \quad m=12$$

or:

$$\mathbf{Z}/2.\mathbf{Z}\times\mathbf{Z}/2\nu\mathbf{Z} \quad \textit{for} \quad \nu\leq 4.$$

Remark. — All these groups do occur. The fifteen curves:

$$X_1(m) \quad \text{and} \quad X(2)\times_{X_1(2)}X_1(2\nu)$$

for m, ν in the above range are all isomorphic to $\mathbf{P}^1_{/\mathbf{Q}}$. Consequently, the elliptic curves $E_{/\mathbf{Q}}$ whose Mordell-Weil group contains a given group Φ (chosen from among the 15 above) occur in an infinite (rationally parametrized) family. These fifteen explicit rational parametrizations are given in the table of [27], chapter IV.

Corollary (5.2). — *Let an elliptic curve, defined over* $\mathbf{Q}$, *possess a point of order* m *rational over* $\mathbf{Q}$. *Then* $m\leq 10$ *or* $m=12$.

Equivalently:

Corollary (5.3). — *Let* m *be an integer such that the genus of* $X_1(m)$ *is greater than* 0 (i.e. $m=11$ *or* $m>13$). *Then the only rational points of* $X_1(m)$ (*over* $\mathbf{Q}$) *are the rational cusps.*

We shall begin the proof of (5.1-3) with a series of reduction steps.

First reduction. — *To prove* (5.1-3) *it suffices to prove* (5.2) *in the special case where* $m=N$, *a prime number such that the genus of* $X_0(N)$ *is* >0 (*i.e.* $N\neq 2, 3, 5, 7,$ *and* 13).

This is so by virtue of the close study of the above conjecture of Ogg, made by Kubert, for low values of composite numbers m.

In particular, Kubert has shown ([27], chap. IV) that it suffices to consider only prime values of m, greater than or equal to 23. For $m=13$, see [40].

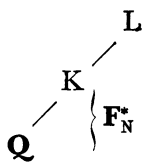
For the duration of the proof, let, then, N denote a prime number $\neq 2, 3, 5, 7$ or 13,

and let $\mathbf{Z}/N \subset E$ be an elliptic curve over $\mathbf{Q}$ with a point of order N, rational over $\mathbf{Q}$ (generating the subgroup $\mathbf{Z}/N$). The object of the proof will be to show that $\mathbf{Z}/N \subset E$ does not exist. As usual, $E_{/S}$ will denote the Néron model of E over S and $\mathbf{Z}/N_{/S} \subset E_{/S}$ is the étale constant subgroup scheme over S generated by our point of order N.

Let $K = \mathbf{Q}(\zeta_N)$, where ζ_N is a primitive N-th root of unity, and let L be the field extension of $\mathbf{Q}$ generated by the N-division points of E. By considering the short exact sequence of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$-modules:

$$\textbf{(5.4)} \qquad 0 \to \mathbf{Z}/N \to E[N] \to \mu_N \to 0$$

one sees that $\mathrm{Gal}(L/K)$ has a faithful representation into $GL_2(\mathbf{F}_N)$ of the form $\begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix}$ where $\chi : \mathrm{Gal}(L/\mathbf{Q}) \twoheadrightarrow \mathrm{Gal}(K/\mathbf{Q}) \twoheadrightarrow \mathbf{F}_N^*$ is the cyclotomic character. Thus, one has the diagram of field extensions:



where L/K is either an N-cyclic extension, or is the trivial extension. Moreover, an elementary computation gives that the natural action of $\mathrm{Gal}(K/\mathbf{Q})$ on $\mathrm{Gal}(L/K)$ (conjugation in $\mathrm{Gal}(L/\mathbf{Q})$) is by multiplication by χ^{-1}. This computation uses the existence of the faithful representation of $\mathrm{Gal}(L/\mathbf{Q})$ of the form $\begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix}$, and, as Serre remarked, can be most conveniently seen by noting that the $*$ in the upper right corner takes its values, canonically, in the vector space $\mathrm{Hom}(\mu_N, \mathbf{Z}/N)$.

It is clear that the exact sequence (5.4) splits if and only if $L = K$.

Second reduction. — *It suffices to prove that* (5.4) *splits, or equivalently, that* $L = K$.

For we would then have the following result from which we easily derive a contradiction: Given any elliptic curve $\mathscr{E}_{/\mathbf{Q}}$ and a sub-Galois module $\mathbf{Z}/N \subset \mathscr{E}$, there is a sub-Galois module $\mu_n \subset \mathscr{E}$.

Let us obtain a contradiction from this.

Forming the quotient $\mathscr{E}' = \mathscr{E}/\mu_N$, we get another elliptic curve over $\mathbf{Q}$ and the image of $\mathbf{Z}/N$ provides $\mathscr{E}'$ with, again, a sub-Galois module $\mathbf{Z}/N \subset \mathscr{E}'$. We may then apply the above result inductively to obtain a chain of such elliptic curves over $\mathbf{Q}$, related by μ_N-isogenies, rational over $\mathbf{Q}$:

$$\mathscr{E} \to \mathscr{E}' \to \mathscr{E}'' \to \dots$$

all containing sub-Galois modules isomorphic to $\mathbf{Z}/N$. This is impossible for various reasons. Firstly, the members of the above chain cannot be all mutually nonisomorphic. For, if they were, they would represent an infinite number of elliptic curves over $\mathbf{Q}$ with good reduction outside a given finite set of primes. This would contradict the

theorem of Shafarevitch (cf. [63], IV (1.4)). Alternatively (and more in the spirit of the present work), it would provide an infinite number of distinct rational points on $X_0(N)$; and this would contradict Theorem (4.1). We have therefore shown that for suitable $i \neq j$, $\mathscr{E}^{(i)} \approx \mathscr{E}^{(j)}$, and consequently there is a non-scalar endomorphism of $\mathscr{E}^{(i)}$ defined over $\mathbf{Q}$. In particular, $\mathscr{E}^{(i)}$ possesses a complex multiplication over $\mathbf{Q}$, which is impossible.

Third reduction. — It suffices to show that L/K *is unramified (at all places).*

For suppose that L/K is unramified, and *nontrivial.* Then it is an N-cyclic (unramified) extension, and consequently N must be an irregular prime. Since $L/\mathbf{Q}$ is Galois and the natural action of $\mathrm{Gal}(K/\mathbf{Q})$ on $\mathrm{Gal}(L/K)$ is χ^{-1} it would then follow, by Herbrand's theorem (chap. I (2.9)), that the Bernoulli number B_2 must have numerator divisible by N. Since $B_2 = 1/6$, L/K must be the trivial extension.

We shall now prove that L/K is unramified. Although this is a local question at each place v of K, it is unlikely that one can prove this by local arguments. Indeed, the essential *step 3* below is global. We proceed by 4 steps, analyzing the structure of the putative $\mathbf{Z}/N \subset E$.

Step 1. — $E_{/S}$ *is semi-stable. That is,* E *has semi-stable* (i.e. *good or multiplicative*) *reduction at all points of* S.

Proof. — Let q be a (rational) prime of nonsemi-stable (*i.e.* additive) reduction for E. Thus the connected component of the fibre $E_{/\mathbf{F}_q}$, $(E_{/\mathbf{F}_q})^0$, is an additive group, and, as is well known, the index of $(E_{/\mathbf{F}_q})^0$ in $E_{/\mathbf{F}_q}$ is $2^a \cdot 3^b$ for suitable integers a, b. It follows that the specialization $\mathbf{Z}/\mathbf{N}_{/\mathbf{F}_q}$ must be contained in $(E_{/\mathbf{F}_q})^0$. Consequently, $q = N$.

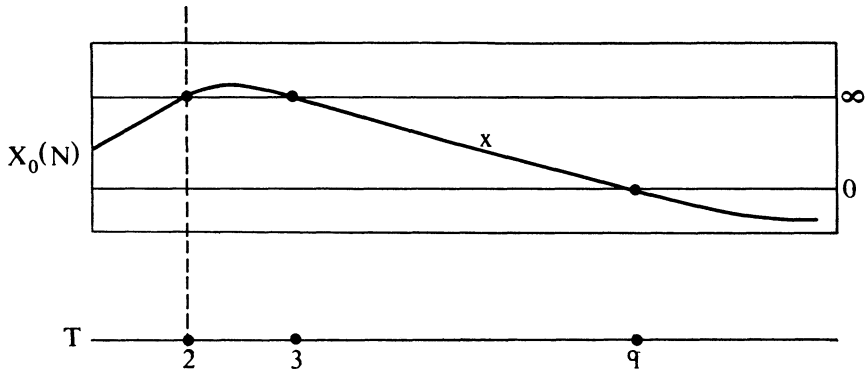
Using ([72], § 2, Cor. 3) one sees that there is a finite extension field $\mathscr{K}/\mathbf{Q}_N$ such that $E_{/\mathscr{K}}$ has semi-stable reduction at the maximal ideal of the ring of integers $\mathscr{O} = \mathscr{O}_{\mathscr{K}}$, and if $e = e(\mathscr{K} : \mathbf{Q}_N)$ is the absolute ramification index, we may choose $\mathscr{K}$ so that $e \leq 6$. If $E_{/\mathscr{O}}$ is the Néron model of E over the base $\mathscr{O}$, and $E_{/\mathbf{Z}} \otimes \mathscr{O}$ is the pullback to $\mathscr{O}$ of the Néron model over $\mathbf{Z}$, there is a natural morphism $E_{/\mathbf{Z}} \otimes \mathscr{O} \to E_{/\mathscr{O}}$ which is trivial on the connected component of the closed fiber, since there are no nontrivial maps from an additive group over a field to a multiplicative group, or to an elliptic curve. If $G_{/\mathscr{O}} \subset E_{/\mathscr{O}}$ is the closed subgroup scheme generated by $\mathbf{Z}/\mathbf{N}_{/\mathscr{K}} \subset E_{/\mathscr{K}}$, we have a natural morphism $\mathbf{Z}/\mathbf{N}_{/\mathscr{O}} \to G_{/\mathscr{O}}$ which is an isomorphism on generic fibers, and *not* an isomorphism on the special fibers, by the above discussion. From this, one sees that $G_{/\mathscr{O}}$ is a finite flat group scheme. But since $e \leq 6 < N-1$, by [55] a finite flat group scheme of order N over $\mathscr{O}$ is determined by its generic fiber. In other words, $G_{/\mathscr{O}}$ must be isomorphic to $\mathbf{Z}/\mathbf{N}_{/\mathscr{O}}$, which is a contradiction.

Step 2. — If $q = 2$, *or* 3, *then* E *has bad (hence multiplicative) reduction at* q, *and the specialization* $\mathbf{Z}/\mathbf{N}_{/\mathbf{F}_q}$ *is* not *contained in the connected component of the identity* $(E_{/\mathbf{F}_q})^0$.

Proof. — If $E_{/\mathbf{F}_q}$ were an elliptic curve, and $\mathbf{Z}/N \subset E_{/\mathbf{F}_q}$, then by the " Riemann hypothesis " $N \leq 1+q+2\sqrt{q}$, which is impossible for $q=2, 3$. Therefore, E has bad reduction at q $(=2, 3)$ necessarily of multiplicative type, by step 1. But, by Tate's theory ([63], IV, A.1.1), $(E_{/\mathbf{F}_{q^2}})^0$ is isomorphic to $\mathbf{G}_{m/\mathbf{F}_{q^2}}$ which has q^2-1 points. Again, we cannot have $\mathbf{Z}/N \subset \mathbf{G}_{m/\mathbf{F}_{q^2}}$, for $q=2, 3$, by virtue of our hypotheses on N.

Step 3. — If q is any prime of bad (hence multiplicative) reduction for E, *then the specialization* $\mathbf{Z}/\mathbf{N}_{/\mathbf{F}_q}$ *is* not *contained in the connected component of the identity,* $(E_{/\mathbf{F}_q})^0$.

Proof. — Let q be a prime of multiplicative reduction such that $\mathbf{Z}/\mathbf{N}_{/\mathbf{F}_q} \subset (E_{/\mathbf{F}_q})^0$. By steps 1 and 2 we may assume $q \neq 2, 3$ or N. Consider the base $T = \operatorname{Spec} \mathbf{Z}[1/2.N]$ and let x be the T-valued point of $X_0(N)_{/T}$ determined by the couple $(E_{/T}, \mathbf{Z}/\mathbf{N}_{/T})$. That is, $x = j(E_{/T}, \mathbf{Z}/\mathbf{N}_{/T})$. It is illuminating to draw the scheme-theoretic diagram:



where ∞ and 0 are the cuspidal sections over T. We are justified in drawing the intersections: $x_{/\mathbf{F}_2} = \infty_{/\mathbf{F}_2}$, $x_{/\mathbf{F}_N} = 0_{/\mathbf{F}_N}$ because, by ([7], VI, § 5), the modular interpretation of $\infty_{/\mathbf{F}_\ell}$ is the " generalized elliptic curve ":

$$(\mathbf{G}_m \times \mathbf{Z}/N, \mathbf{Z}/N)_{\mathbf{F}_\ell}$$

(*i.e.* the cyclic subgroup of order N which gives the $\Gamma_0(N)$-structure is *not* contained in the connected component containing the identity) while the interpretation of $0_{/\mathbf{F}_\ell}$ is the " generalized elliptic curve ":

$$(\mathbf{G}_m \times \mathbf{Z}/N, \mu_N)_{/\mathbf{F}_\ell}$$

(*i.e.* the cyclic subgroup of order N which gives the $\Gamma_0(N)$-structure *is* contained in the connected component containing the identity).

Now consider the natural projection to the Eisenstein quotient $X_0(N)_{/T} \to \tilde{J}_{/T}$. By (3.1) we know that $\tilde{J}(\mathbf{Q}) = C$. For the present proof, however, it suffices to know that $\tilde{J}(\mathbf{Q})$ is a torsion group. Thus $\tilde{J}(T) = \tilde{J}(\mathbf{Q})$ is a torsion group. Let $\sim$ denote the image of sections of $X_0(N)$ in $\tilde{J}$. Since T is an open subscheme of Spec $\mathbf{Z}$ over which 2 is invertible, if A is any abelian scheme over T, and ℓ any rational prime representing

a closed point of T, the specialization map $A(T)_{tors} \to A(\mathbf{F}_\ell)$ is injective (1). Applying this fact to $A = \tilde{J}$, one sees that $\tilde{J}(T) \to \tilde{J}(\mathbf{F}_\ell)$ is injective. But the equations $\tilde{x}_{/\mathbf{F}_3} = \tilde{\infty}_{/\mathbf{F}_3}$, and $\tilde{x}_{/\mathbf{F}_q} = \tilde{0}_{/\mathbf{F}_q}$, then imply that $\tilde{0} = \tilde{\infty}$. Since $\tilde{0} - \tilde{\infty}$ is of order n in $\tilde{J}$, this can only be true if $n = 1$, or equivalently, if $N \leq 7$ or $N = 13$. Since N is constrained to be > 7 and $\neq 13$, we obtain the contradiction that we seek.

Step 4. — L/K *is unramified.*

Proof. — (i) *q a rational prime of good reduction for* E; $q \neq N$: Since $E[N]_{/\mathbf{Z}_q}$ is an étale, finite flat group scheme, L/K is unramified over all places of K lying over q.

(ii) $q = N$; E *has good reduction at* N: Again $E[N]_{/\mathbf{Z}_N}$ is a finite flat group scheme. Applying the " connected component of the identity " functor to (4.4) one sees that $(E_{/\mathbf{Z}_N})^0 = \mu_N$, and therefore we get a splitting: $E[N]_{/\mathbf{Z}_N} = \mathbf{Z}/\mathbf{N}_{/\mathbf{Z}_N} \times \mu_{N/\mathbf{Z}_N}$, which again shows that L/K is unramified at all places of K lying above N.

(iii) *q a rational prime of bad reduction for* E: Since $\mathbf{Z}/\mathbf{N}_{/\mathbf{F}_q} \not\subset (E_{/\mathbf{F}_q})^0$ by step 3, one obtains, as in (ii), $E[N]_{/\mathbf{Z}_q} \cong \mathbf{Z}/\mathbf{N}_{/\mathbf{Z}_q} \times \mu_{N/\mathbf{Z}_q}$, giving us the same conclusion: that all places of K above q are unramified in L/K.

6. Rational points on $X_{split}(N)$.

Keeping to the terminology of the Introduction (cf. discussion preceding Theorem 9) elliptic curves with a normalizer-of-split-Cartan structure on their N-division points are classified by noncuspidal rational points on $X_{split}(N) = X_0(N^2)/w_{N^2}$.

Theorem **(6.1).** — *If* $N \neq 2, 3, 5, 7$ *and* 13, *then* $X_{split}(N)$ *has only a finite number of rational points.*

Note. — If $N \leq 7$, then $X_{split}(N)$ is isomorphic to $\mathbf{P}^1_{/\mathbf{Q}}$ and therefore its set of rational points form a rationally parametrized infinite set. The curve $X_{split}(13)$ is of genus 3. It is to be expected that $X_{split}(13)$ has only a finite number of rational points, but my methods have not been able to establish this.

Proof of theorem (6.1). — Consider the two natural morphisms:

$$f, g : X_0(N^2) \to X_0(N).$$

The map f is defined by the prescription $f : (E, C_{N^2}) \mapsto (E, C_N)$ where, if E is an elliptic curve, and C_{N^2} is a subgroup of E of order N^2, then $C_N = N.C_{N^2} \subset E$. It induces a map from parabolic modular forms (of weight 2) on $\Gamma_0(N)$ to parabolic modular forms on $\Gamma_0(N^2)$ with the same q-expansion.

The map g is defined by the prescription $g : (E, C_{N^2}) \mapsto (E', C'_N)$ where $E' = E/C_N$ and $C'_N = C_{N^2}/C_N$.

---

(1) This is a standard application of the Oort-Tate classification theorem [54] to the group scheme over T generated by an element of order p in the kernel of the above specialization map. If A is an elliptic curve, then this result is due to Nagel-Lutz.

If ω is a parabolic modular form (of weight 2) and $\tilde{\omega}(q)$ denotes its q-expansion at ∞, then $(\widetilde{g\omega})(q)=\tilde{\omega}(q^N)$. We denote the canonical involution (chap. II, § 6) of $X_0(N)$ by w_N to distinguish it from the canonical involution of $X_0(N^2)$, denoted w_{N^2}. As usual, J is the jacobian of $X_0(N)$. Let $h : X_0(N^2)\to J$ be the map which associates to x the divisor class of $f(x)-g(x)$. A straightforward calculation yields the formula $h.w_{N^2}=-w_N.h$ (and the minus sign will be of importance to our proof). It follows from this formula that the composition $X_0(N^2) \xrightarrow[h]{} J \xrightarrow[\text{proj.}]{} J^-=J/(1+w_N).J$ factors through $X_0(N^2)\to X_0(N^2)/w_{N^2}=X_{\text{split}}(N)$ and thereby induces a map:

$$h^- : X_{\text{split}}(N)\to J^-.$$

The map $X_0(N^2)\to J$ induces a surjection on the jacobian $J_0(N^2)\to J$ as can be seen as follows. The induced map from parabolic modular forms of weight 2 under $\Gamma_0(N)$ to parabolic modular forms under $\Gamma_0(N^2)$ is injective. This latter assertion is true since a modular form of weight 2 under $\Gamma_0(N)$ which is sent to zero by the map in question must have its first N q-expansion coefficients equal to zero. Hence it is zero.

It follows that the map $h^- : X_{\text{split}}(N)\to J^-$ induces a surjection from the jacobian of $X_{\text{split}}(N)$ to J^-. Let $\tilde{h} : X_{\text{split}}(N)\to\tilde{J}$ denote the composition of h^- with the projection map to the Eisenstein quotient (chap. II (17.10)). Since $N=11$ or $N\geq 17$, it follows that $X_0(N)$ is of positive genus, and that $\tilde{J}$ is nontrivial. Letting $\tilde{X}_{\text{split}}(N)\subset\tilde{J}$ denote the image of $X_{\text{split}}(N)$ under $\tilde{h}$, one sees that $\tilde{X}_{\text{split}}(N)$ must be a curve, and $X_{\text{split}}(N)\to\tilde{X}_{\text{split}}(N)$ a finite morphism. Since $J(\mathbf{Q})=C$ is a finite group, the proof of Theorem (6.1) is completed.

Remark. — We have made essential use of the fact that $\tilde{J}$ factors through J^- (chap. II (17.10)). This fact (when $N\equiv 1 \bmod 8$) seems to depend on some of the more delicate aspects of the theory developed in chapter II.

7. Factors of the Eisenstein quotient.

Consider a surjective morphism defined over $\mathbf{Q}$, $J\to A$ where $A_{/\mathbf{Q}}$ is a $\mathbf{Q}$-simple (equivalently: $\mathbf{C}$-simple) abelian variety.

Let $p\,|\,n$ be a prime number such that this morphism factors through the p-Eisenstein quotient (such a prime number p must exist, but may not be unique) and let $a=\dim A$.

Replacing A by an abelian variety isogenous to it, if necessary, we may suppose that the Hecke algebra $\mathbf{T}$ leaves the kernel of $J\to A$ stable, and consequently that we can induce a natural action of $\mathbf{T}$ on A. Since the Eisenstein prime $\mathfrak{P}$ associated to p is contained in the irreducible component of Spec $\mathbf{T}$ which corresponds to A (chap. II (10.1)) it follows that $A[\mathfrak{P}]$ (the kernel of $\mathfrak{P}$ in A) is nontrivial. Consequently, by admissibility of the kernel of $\mathfrak{P}$ (chap. II (14.1)) it follows that there is an abelian variety $A'_{/\mathbf{Q}}$ isogenous to A over $\mathbf{Q}$ such that A' possesses a point of order p in its Mordell-Weil group. (More precisely, we may take $A'_{/S}$ to contain a subgroup scheme isomorphic to $\mathbf{Z}/\mathbf{p}_{/S}$.)

Using the criterion of Néron-Ogg-Shafarevich, one sees that $A \to A'$ extends to an isogeny of abelian schemes over S'. Reduce to characteristic 2 and obtain an isogeny $A_{/\mathbf{F}_2} \to A'_{/\mathbf{F}_2}$ of abelian varieties where $A'(\mathbf{F}_2)$ contains a point of order p. Standard estimates for the number of rational point of an abelian variety over a finite field (the Weil conjectures) give:

$$p \leq \#A'(\mathbf{F}_2) \leq (1+\sqrt{2})^{2a}$$

or:

$$a \geq \frac{\log p}{2.\log(1+\sqrt{2})}. \tag{7.1}$$

We obtain:

Proposition (7.2). — *Every simple factor of the p-Eisenstein quotient* $\tilde{J}^{(p)}$ *has dimension* $\geq \frac{\log p}{2.\log(1+\sqrt{2})}$.

Corollary (7.3). — *There are absolutely simple abelian varieties of arbitrarily high dimension, defined over* $\mathbf{Q}$, *whose Mordell-Weil group is finite.*

Proof. — For any positive integer a_0, find a prime number $p \geq 5$ such that $\log p \geq 2a_0.\log(1+\sqrt{2})$ and, by Dirichlet's theorem, choose a prime number N such that $N \equiv 1 \bmod p$. Then (7.2) every simple factor of the p-Eisenstein quotient of $J=J_0(N)$ has dimension $\geq a_0$ and (4.1) has finite Mordell-Weil group.

What are the elliptic curve factors of the Eisenstein quotient $\tilde{J}$? If $E_{/\mathbf{Q}}$ is a quotient elliptic curve of $\tilde{J}^{(p)}$, then E has (prime) conductor N, and by the above discussion, after modification of E by $\mathbf{Q}$-isogeny if necessary, we may suppose that the Mordell-Weil group of E possesses a point of order p. There has been some recent work ([68], [46], [42], [16]) on elliptic curves of prime conductor N possessing a torsion point of order p over $\mathbf{Q}$. In particular, one has that $p \leq 5$ (using the Weil estimates to the reduction of E in characteristic 2) and by [42] one has, further, if $p=5$, then $N=11$ and E is isogenous to $X_0(11)$; if $p=3$, then $N=19$, or 37 and E is isogenous to $X_0(19)$ or to the Eisenstein quotient of $J_0(37)$.

Thus we are reduced to the case $p=2$. In this case, either $N=17$ and E is isogenous to $X_0(17)$, or it is a *Neumann-Setzer curve* (which, by definition, is an elliptic curve over $\mathbf{Q}$ of prime conductor $N \neq 17$ possessing a point of order 2 in its Mordell-Weil group). The facts concerning Neumann-Setzer curves are these ([68], [46]):

A Neumann-Setzer curve of conductor N exists if and only if N is of the form $64+u^2$ (u an integer). If N is of the above form there are precisely two isomorphism classes of Neumann-Setzer curves of conductor N, given by the equations:

$$y^2 = x^3 + ux^2 - 16x$$
$$y^2 = x^3 - 2ux^2 + Nx.$$

One may pass from one curve to the other by the 2-isogeny obtained by division by the rational point of order 2.

Proposition **(7.4)**. — i) *Let* $p>2$. *The* p*-Eisenstein quotient has no elliptic curve factor unless* $p=5$, $N=11$ *or* $p=3$ *and* $N=19$ *or* 37.

ii) *The 2-Eisenstein quotient* $\tilde{J}^{(2)}$ *has no elliptic curve factor unless* $N=17$, *or* $N=64+u^2$ *with* u *an integer. If the 2-Eisenstein quotient has an elliptic curve factor, then this factor is unique up to isogeny and if* $N\neq 17$ *its isogeny class is that of the Neumann-Setzer curves of conductor* N. *If the (two) Neumann-Setzer curves of conductor* N *are parametrized by modular functions for* $\Gamma_0(N)$ (i.e. *if they occur as quotients of* J, *a special case of the conjecture of Weil) then they are quotients of* $\tilde{J}^{(2)}$.

Proof. — This combines the work of [68], [46] as in the discussion above, and chapter II (14.1).

The following gives (granted conjectures of Weil and Hardy-Littlewood) an infinite number of values of N for which the estimate of (7.2) is sharp for the 2-Eisenstein quotient.

Proposition **(7.5)**. — *Let* N *be a prime number of the form* $64+u^2$ *such that* $N\not\equiv 1 \bmod 16$. *Suppose that the (two) Neumann-Setzer curves are parametrized by modular functions for* $\Gamma_0(N)$. *Then* $\tilde{J}^{(2)}$ *is of dimension* 1, *and is a Neumann-Setzer curve of conductor* N.

Proof. — Let $\mathfrak{P}$ be the Eisenstein prime associated to 2. By our hypothesis on N, $2\,||\,n$. Therefore, by chapter II (19.1), $\mathbf{T}_{\mathfrak{P}}$ is a discrete valuation ring. Since the irreducible components of Spec $\mathbf{T}_{\mathfrak{P}}$ map surjectively to the (isogeny classes of) factors of $\tilde{J}^{(2)}$, it follows that $\tilde{J}^{(2)}$ is a simple abelian variety. But, by the hypothesis of (7.5) and by (7.4) ii) the Neumann-Setzer curves are factors of $\tilde{J}^{(2)}$. Our proposition follows.

Remark. — Let N be a prime number of the form $64+u^2$ such that $N\equiv 1 \bmod 16$. The 2-Eisenstein quotient contains a point of order 4 (at least). It must have dimension greater than 1, for if it were an elliptic curve, it would be a Neumann-Setzer curve and a Neumann-Setzer curve does not possess a point of order 4 [68].

Suppose, further, that the Neumann-Setzer curves of conductor N are parametrized by modular functions for $\Gamma_0(N)$. It then follows that $\tilde{J}^{(2)}$ is not a simple abelian variety, since it has a Neumann-Setzer curve as a proper factor. Consequently the completion of the Hecke algebra $\mathbf{T}_{\mathfrak{P}}$ is *not an integral domain.* Conjectures of Weil and of Hardy-Littlewood would give that this occurs for infinitely many values of N.

The only case of a pair (N, p) where $N<250$ and $\mathbf{T}_{\mathfrak{P}}$ is not a discrete valuation ring, for $\mathfrak{P}$ the Eisenstein prime associated to p, is: $N=113$, $p=2$. This is the first instance of the (conjecturally infinite) family of examples described in the paragraph above.

8. The $\mathfrak{P}$-adic L-series.

Fix $\mathfrak{P}$ an Eisenstein prime associated to a prime number $p \neq 2$.

In this section and the next we shall examine the analytically-defined $\mathfrak{P}$-adic L series [39] and the arithmetically-defined $\mathfrak{P}$-adic characteristic polynomial [34]. We recall terminology and results from the papers cited.

Since both p and $\eta_p = 1 + p - T_p$ are in the ideal $\mathfrak{P}$, we have $T_p \equiv 1 \bmod \mathfrak{P}$ [1] and therefore T_p is a unit in $\mathbf{T}_{\mathfrak{P}}$.

The standard recursive process (*e.g.*, p. 47 of [39]) gives two roots of the quadratic equation:

$$X^2 - T_p . X + p = 0$$

in $\mathbf{T}_{\mathfrak{P}}$. Call the unit root π and the other one $\bar{\pi}$ to be consistent with the terminology of [39]. Let $\{\ \} : \mathbf{Q}/\mathbf{Z}' \to H = H_1(X_0(N), \mathbf{Z})$ denote the modular symbol, where $\mathbf{Q}/\mathbf{Z}'$ means rationals with denominator prime to N, modulo 1 ([22], [29]). Let $f : \mathbf{Q}/\mathbf{Z}' \to H_{\mathfrak{P}}$ be the composition of $\{\ \}$ with $H \to H_{\mathfrak{P}} = \mathbf{T}_{\mathfrak{P}} \otimes_{\mathbf{T}} H$. For any fixed choice of integer Δ_0 prime to p, set $\Delta_n = \Delta_0 . p^n$ and $\mathbf{Z}_\Delta = \varprojlim_n \mathbf{Z}/\Delta_n$ regarded as topological ring. $\mathbf{Z}_\Delta^*$ is then the topological group of its units.

We now wish to use the construction of [39], § 8, to obtain an $H_{\mathfrak{P}}$-valued measure on $\mathbf{Z}_\Delta^*$ from the function f. This may be done, for f is an eigenfunction for the Hecke operator T_p with eigenvalue a *unit* in $\mathbf{T}_{\mathfrak{P}}$. One remark, however, must be made: in the terminology of [39], § 8, we take $\mathbf{T}_{\mathfrak{P}} = D$, $H_{\mathfrak{P}} = W$. Note, however, that in [39] (8.1) the hypothesis on D is that it be the ring of integers in a finite extension of $\mathbf{Q}_p$. This is not needed. All that is used is that D is a local ring with maximal ideal $\mathfrak{m}$ containing the prime p and that D is p-adically complete.

Let μ^Δ, then, denote the $H_{\mathfrak{P}}$-valued measure associated to the eigenfunction f ([39] (8.1)). Let (chap. II (18.1)) $0 \to H_{\mathfrak{P}}^- \to H_{\mathfrak{P}} \to H_{\mathfrak{P}}^+ \to 0$ be the decomposition of $H_{\mathfrak{P}}$ into $-$ and $+$ eigen (sub- and quotient-) spaces. Let χ be a continuous multiplicative character on $\mathbf{Z}_\Delta^*$ whose values lie in (and generate) the $\mathbf{T}_{\mathfrak{P}}$-algebra $\mathbf{T}_{\mathfrak{P}}[\chi]$. We consider the Fourier transform of the measure μ^Δ:

$$L_{\mathfrak{P}}(\chi) = \int_{Z_\Delta^*} \chi . \mu^\Delta \in H_{\mathfrak{P}}[\chi] = \mathbf{T}_{\mathfrak{P}}[\chi] \otimes_{\mathbf{T}_{\mathfrak{P}}} H_{\mathfrak{P}} .$$

If the formula $\chi(-1) = (\text{sign } \chi) . 1$ defines sign χ, $L_{\mathfrak{P}}(\chi)$ lies in the (sign χ)-eigenspace of the complex conjugation involution and, if χ is even, it is natural to let $L_{\mathfrak{P}}(\chi)$ take its value in $H_{\mathfrak{P}}^+[\chi]$, by projection.

We refer to $L_{\mathfrak{P}}$ as *the* $\mathfrak{P}$*-adic* L*-series*, and the general theory of [39] applies to it. In particular we have its various developments as analytic function in the s- and T-planes, keeping the conventions of [39].

---

[1] We think of this relation as expressing the fact that Eisenstein primes are *anomalous*, in the spirit of the notion introduced for elliptic curves in [34].

Let $\mu^{\Delta,+}$ be the projection of the measure μ^{Δ} to $H^+_{\mathfrak{P}}$. Then the $\mathfrak{P}$-adic L-series restricted to *even* characters is the Fourier transform of $\mu^{\Delta,+}$.

Proposition **(8.1)** *(divisibility).* — $\mu^{\Delta,+}$ *takes its values in* $\mathfrak{I}.H^+_{\mathfrak{P}} \subset H^+_{\mathfrak{P}}$.

Proof. — By chapter II (18.8), $f(b/\Delta_m)$ depends only on $\Delta_m \bmod \mathfrak{I}.H^+_{\mathfrak{P}}$, if b is prime to Δ_m. By formula (2) of (8.1) of [39], $\mu^{\Delta,+}$ evaluated on the fundamental open set $a+\Delta_n \mathbf{Z}_\Delta \subset \mathbf{Z}^*_\Delta$ (for a prime to Δ) is given by:

$$\lim_{\substack{m \geq n \\ m \to \infty}} \pi^{-m} \sum_{b \equiv a \bmod \Delta_n} f(b/\Delta_m),$$

from which our proposition is seen to follow.

Corollary **(8.2)**. — *If* χ *is an even character,* $L_{\mathfrak{P}}(\chi) \in \mathfrak{I}.H^+_{\mathfrak{P}}[\chi]$.

The proposition also implies that if we develop $L_{\mathfrak{P}}$ in a power series expansion about an *even* character χ_0 in either the s- or the T-plane (cf. [39], § 9) then every coefficient of these power series will lie in $\mathfrak{I}.H^+_{\mathfrak{P}}[\chi_0]$.

To evaluate the *constant term* $L_{\mathfrak{P}}(\chi_0)$ of the $\mathfrak{P}$-adic L-series, where χ_0 is the principal character of conductor p, we use [39] (8.2).

Take $\Delta_0 = 1$. We work in the ring $D = \mathbf{T}_{\mathfrak{P}}$. The proposition of [39] (8.2) gives:

$$L_{\mathfrak{P}}(\chi_0) = \frac{-\eta_p . S}{(\pi^2 - p)(1-\bar{\pi})^2}$$

where S is $\sum_{a=0}^{p-1} \{a/p\}$ projected to $H^+_{\mathfrak{P}}$.

If $e^+_{\mathfrak{P}}$ denotes the image of the winding element in $H^+_{\mathfrak{P}} \otimes \mathbf{Q}$ (chap. II, § 18), formula (8) of page 35 of [39] yields $\eta_p . e^+_{\mathfrak{P}} = -S$, giving:

$$\textbf{(8.3)} \qquad L_{\mathfrak{P}}(\chi_0) = \frac{\eta_p^2 . e^+_{\mathfrak{P}}}{(\pi^2 - p)(1-\bar{\pi})^2} \in H^+_{\mathfrak{P}}$$

(compare with the formula at top of page 55 of [39]).

To analyze this constant term more closely, fix ℓ a *good* prime number (relative to p, N) as in chapter II, § 16. For convenience, if p itself is good (*i.e.* if p is not a p-th power modulo N), take $\ell = p$. Let $\eta = \eta_\ell$, which is a generator in $\mathbf{T}_{\mathfrak{P}}$ of the ideal $\mathfrak{I}_{\mathfrak{P}}$ by chapter II (16.6). Write $\eta_p = \delta . \eta$. Therefore $\delta \in \mathbf{T}_{\mathfrak{P}}$ and δ is a unit ($=1$) if and only if p is good. Since η, η_p are units in the ring $\mathbf{T}_{\mathfrak{P}} \otimes \mathbf{Q}$ (*e.g.*, as in chap. II, proof of (16.10)) so is δ.

Corollary **(8.4)**. — *There is a suitable generator* y *of the* $\mathbf{T}_{\mathfrak{P}}$*-module* $H^+_{\mathfrak{P}}$ *such that*:

$$L_{\mathfrak{P}}(\chi_0) = \delta^2 . \eta . y$$

where δ *is a unit in* $\mathbf{T}_{\mathfrak{P}} \otimes \mathbf{Q}$. *Furthermore,* δ *is a unit in* $\mathbf{T}_{\mathfrak{P}}$ *if and only if* p *is not a* p*-th power* mod N.

Proof. — This follows from the above discussion, and (8.3), by taking:

$$y = \eta . e_{\mathfrak{P}}^{+}/(\pi^2 - p)(1-\bar{\pi})^2.$$

Now make a choice of a 1-unit $\gamma \in \mathbf{Z}_{\Delta}^{*} = \mathbf{Z}_p^{*}$ and form ([39], § 9) the $\mathfrak{P}$-adic L-series in the T-plane about χ_0:

$$L(T) = L_{\mathfrak{P}}(\chi_0, T)_{(\gamma)} \in H_{\mathfrak{P}}^{+} \otimes_{\mathbf{T}_{\mathfrak{P}}} \mathbf{T}_{\mathfrak{P}}[[T]].$$

The constant term is just $L_{\mathfrak{P}}(\chi_0)$, and by (8.2) each of its coefficients is divisible by η, and therefore we may write $L(T) = g(T).\eta.y$, where $g(T) \in \mathbf{T}_{\mathfrak{P}}[[T]]$ is a power series whose constant term is δ^2. Thus

Corollary **(8.5)**. — *Identify* $\mathbf{T}_{\mathfrak{P}}$ *with* $H_{\mathfrak{P}}^{+}$ *by the map* $\tau \mapsto \tau.y$. *Then*:

$$\eta^{-1}.L_{\mathfrak{P}}(\chi_0, T)_{(\gamma)} \in \mathbf{T}_{\mathfrak{P}}[[T]]$$

is a power series with constant term δ^2. *It is a unit in* $\mathbf{T}_{\mathfrak{P}}[[T]]$ *if and only if* p *is not a* p*-th power modulo* N.

Remark. — When p is a p-th power modulo N, we have then a " secondary " analogue to the phenomenon of anomalous primes studied in [34], [39]. Namely, either $L_{\mathfrak{P}}(\chi_0, T)_{(\gamma)}$ is divisible by more than η, or it has at least one zero in the open unit $\mathbf{T}_{\mathfrak{P}}$-disc (or both).

9. Behavior in cyclotomic towers.

Guided by conjectures made in [39], the results concerning the $\mathfrak{P}$-adic L-series (§ 6) suggest that the following proposition is true. We prove it below (independent of any conjectures). We shall also take the opportunity to correct an erroneous assertion made in [34].

Proposition **(9.1)**. — *Let* $p \neq 2$ *be a divisor of* n. *Let* $\mathbf{Q}^{(p)}/\mathbf{Q}$ *denote the unique Galois extension with Galois group isomorphic to* $\mathbf{Z}_p$ (*the* p*-cyclotomic* Γ*-extension*). *The group* $\tilde{J}^{(p)}(\mathbf{Q}^{(p)})$ *of rational points of the* p*-Eisenstein quotient with values in the* p*-cyclotomic* Γ*-extension is a finitely generated group. If* p *is not a* p*-th power modulo* N, *then it is a finite group.*

One has an accompanying assertion about the $\mathfrak{P}$-primary component of the Shafarevich-Tate group. Namely, let $\Gamma = \mathrm{Gal}(\mathbf{Q}^{(p)}/\mathbf{Q})$, and for every positive integer m, let $\Gamma_m \subset \Gamma$ be the subgroup of index p^m. Set $\mathbf{Q}_m^{(p)} \subset \mathbf{Q}^{(p)}$ to be the fixed field of Γ_m, and $Ш_m$ the $\mathfrak{P}$-primary component of the Shafarevich-Tate group of $\tilde{J}^{(p)}$ (or of J: it is the same) over $\mathbf{Q}_m^{(p)}$.

Set $\Lambda = \varprojlim \mathbf{T}_{\mathfrak{P}}[\Gamma/\Gamma_m]$ (the projective limit of topological rings, where $\mathbf{T}_{\mathfrak{P}}[\Gamma/\Gamma_m]$ is given the natural topology) and $Ш_{\infty} = \varinjlim_{m \to \infty} Ш_m$ regarded as Λ-module.

Proposition **(9.2)**. — *The kernel and cokernel of the natural map*:

$$Ш_m \to (Ш_{\infty})^{\Gamma_m}$$

are finite groups whose orders are bounded (independent of n). That is, the above sequence is controlled *in the sense of* [24], [34].

The Λ*-module* $Ш_\infty$ *is isomorphic, modulo finite groups, to the Pontrjagin dual of the* Λ*-module* $\Lambda/\mathfrak{I}_\mathfrak{P}.\Lambda \cong \mathbf{T}_\mathfrak{P}/\mathfrak{I}_\mathfrak{P}[[T]]$. *There is a constant* $c_0 > 0$ *such that if* $p^f || n$, *then*:

$$|\log_p(\text{order } Ш_m) - f.p^m| \leq c_0$$

for all $m > 0$.

Remarks. — Guided by the same conjectures of [39] (6.5), one would expect that if p ($\neq 2$) *is* a p-th power modulo N, then either $\mathfrak{J}^{(p)}(\mathbf{Q}^{(p)})$ is a finitely generated group of positive rank, or $Ш_m$ grows more rapidly than the bound of (9.2).

The proof of these propositions may be regarded as a " generalization " of the case $N = 11$, treated in [34]. It proceeds closely along the lines of argument used for the case $N = 11$, but incorporates work we have already done concerning Eisenstein primes, and uses a recent result:

Theorem (Imai [21]). — *Let* K *be a number field (a finite extension of* $\mathbf{Q}$) *and* L/K *the p-cyclotomic extension* $(L = \bigcup_r K(\zeta_{p^r}))$. *Let* $A_{/L}$ *be an abelian variety. Then the torsion subgroup* $A(L)_{tors}$ *of the group of rational points of* A *over* L *is a finite group.*

Correction. — I am thankful to Ito for pointing out that an assertion I made in [34] (labelled (6.18)) is incorrect (for abelian varieties of CM-type of dimension greater than 1). Therefore, my proof that $A(L)_{tors}$ is finite when A is of CM-type ([34] (6.12 (i))) is incomplete. The theorem of Imai [21] shows, however, that the result is valid for *all* abelian varieties.

Discussion. — Imai proves a local result based on Sen's analysis of the structure of the Lie algebra of a Galois group acting on a Hodge-Tate module [59]. Serre has communicated to me a proof along rather different (global) lines by means of which he obtains finiteness of the group of rational torsion points of the abelian variety A with values in many Γ-extensions over K not only the p-cyclotomic Γ-extension.

We now prepare to prove (9.1) and (9.2) by the method of [34].

Let Y_m denote the spectrum of the ring of integers in $\mathbf{Q}_m^{(p)}$ and let Y be the spectrum of the ring of integers in $\mathbf{Q}^{(p)}$. Thus $Y_0 = S = \text{Spec}(\mathbf{Z})$.

If $J_{/Y_m}$ is the base change of the Néron model $J_{/S}$ then it is the Néron model of the jacobian of $X_0(N)_{/\mathbf{Q}_m^{(p)}}$ since p is the only ramified prime, and J has good reduction at p.

Let η (as in § 6) be a generator of the ideal $\mathfrak{I}_\mathfrak{P} \subset \mathbf{T}_\mathfrak{P}$ (chap. II (16.6)). So:

$$J_\mathfrak{P} = \varinjlim_r J_\mathfrak{P}[\eta^r]_{/S}$$

is represented in this way as an inductive limit of quasi-finite group schemes over S, and is naturally endowed with the structure of $\mathbf{T}_\mathfrak{P}$-module.

We have the analogue of diagram (6.6) of [34], which may be written:

(9.3)

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & J_{\mathfrak{P}}(\mathbf{Q}_m^{(p)})_{\Gamma_m} & \xrightarrow{\gamma_m} & E_m & & \\
 & & & & \downarrow & & \downarrow & \searrow^{\delta_m} & \\
0 & \longrightarrow & H^1(Y_m, J_{\mathfrak{P}}) & \longrightarrow & H^1(Y_m - p_m, J_{\mathfrak{P}}) & \longrightarrow & H^2_{\bullet}(Y_{m,p_m}, J_{\mathfrak{P}}) & \longrightarrow & H^2(Y_m, J_{\mathfrak{P}}) \\
 & & \downarrow{\scriptstyle \alpha_m} & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H^1(Y, J_{\mathfrak{P}})^{\Gamma_m} & \longrightarrow & H^1(Y - p_\infty, J_{\mathfrak{P}})^{\Gamma_m} & \longrightarrow & H^2_{\bullet}(Y_{p_\infty}, J_{\mathfrak{P}})^{\Gamma_m} & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array}$$

where p_m is the unique closed point of characteristic p in Y_m, p_∞ is the unique closed point of characteristic p in Y; Y_{m,p_m} is the completion of Y_m at p_m, and Y_{p_∞} is the completion of Y at p_∞; the superscript Γ_m means invariants under the action of Γ_m and the subscript mean coinvariants; $H^2_{\bullet}$ denotes cohomology with supports at the closed point. We view the above diagram, whose horizontal and vertical lines are exact, as a diagram of $\mathbf{T}_{\mathfrak{P}}$-modules.

There are three necessary calculations that must be made, in order to prove (9.1) and (9.2) and we collect them in the following lemma:

Lemma **(9.4)**:

1. $J_{\mathfrak{P}}(\mathbf{Q}^{(p)})$ *is isomorphic to* $\mathbf{T}_{\mathfrak{P}}/\mathfrak{I}_{\mathfrak{P}}$.
2. $H^1(\mathrm{Spec}(\mathbf{Z}), J_{\mathfrak{P}}) = 0$.
3. *For any* m, *the* $\mathbf{T}_{\mathfrak{P}}$*-module* E_m *is (noncanonically) isomorphic to* $(\mathbf{T}_{\mathfrak{P}}/\mathfrak{I}_{\mathfrak{P}}) \oplus (\mathbf{T}_{\mathfrak{P}}/\mathfrak{I}_{\mathfrak{P}})$.

Granted the lemma, we shall prove our propositions. Let H denote $H^1(Y, J_{\mathfrak{P}})$ regarded as Λ-module. The lemma enables us to " evaluate " the above diagram for $m = 0$:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
 & & \mathbf{T}_{\mathfrak{P}}/\mathfrak{I}_{\mathfrak{P}} & \longrightarrow & (\mathbf{T}_{\mathfrak{P}}/\mathfrak{I}_{\mathfrak{P}}) \oplus (\mathbf{T}_{\mathfrak{P}}/\mathfrak{I}_{\mathfrak{P}}) & & \\
 & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H^1(Y_0 - p_0, J_{\mathfrak{P}}) & \longrightarrow & H^2_{\bullet}(Y_{0,p_0}, J_{\mathfrak{P}}) & & \\
\downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H^{\Gamma} & \longrightarrow & H^1(Y - p_\infty, J_{\mathfrak{P}})^{\Gamma} & \longrightarrow & H^2_{\bullet}(Y_{p_\infty}, J_{\mathfrak{P}})^{\Gamma} \\
 & & & & \downarrow & & \downarrow \\
 & & & & 0 & & 0
\end{array}$$

Note that $\mathbf{T}_{\mathfrak{P}}/\mathfrak{I}_{\mathfrak{P}}$ is a cyclic group of order p^f. From the above diagram, it follows that H^{Γ} is a cyclic abelian group, hence, as $\mathbf{T}_{\mathfrak{P}}$-module, a quotient of $\mathbf{T}_{\mathfrak{P}}$ by some ideal $\mathfrak{a} \subset \mathbf{T}_{\mathfrak{P}}$. It also follows from the above diagram that $\mathfrak{I}_{\mathfrak{P}} \subset \mathfrak{a}$.

From this, we obtain the analogous information about H^*, the Pontrjagin dual. Namely, $H^* \otimes_{\Lambda} \mathbf{T}_{\mathfrak{P}}$ is isomorphic to $\mathbf{T}_{\mathfrak{P}}/\mathfrak{a}$, as $\mathbf{T}_{\mathfrak{P}}$-module.

Now consider the " descent sequence ":

(9.5)
$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_p \oplus \Sigma_p & \longrightarrow & J_{\mathfrak{P}} & \longrightarrow & J^0_{\mathfrak{P}} & \longrightarrow & 0 \\ & & & & \downarrow & \searrow^{\eta} & \downarrow & & \\ 0 & \longrightarrow & J^0_{\mathfrak{P}} & \longrightarrow & J_{\mathfrak{P}} & \longrightarrow & \Phi & \longrightarrow & 0 \end{array}$$

which is a sequence of sheaves of $\mathbf{T}_{\mathfrak{P}}$-modules for the *fppf* topology over $\mathrm{Spec}(\mathbf{Z}) = Y_0$, or, after base change, over the schemes Y_n, and Y. Here $C_p \cong \mathbf{Z}/p^f$ is the p-primary component of the cuspidal subgroup and Σ_p ($\cong \mu_{p^f}$ noncanonically) is the p-primary component of the Shimura subgroup (chap. II (16.4)). The sheaf Φ is representable by a *nonseparated* but finite étale group (pre-)scheme whose support is concentrated at the prime of characteristic N, and whose fiber at N is a free $\mathbf{T}_{\mathfrak{P}}/\mathfrak{I}_{\mathfrak{P}}$-module of rank 1.

Noting that by (1) of the lemma the group $H^0(Y, J_{\mathfrak{P}})$ is generated by the appropriate multiple of the point $(0)-(\infty)$, and as $\mathbf{T}_{\mathfrak{P}}$-module is isomorphic to $\mathbf{T}_{\mathfrak{P}}/\mathfrak{I}_{\mathfrak{P}}$, one obtains that $H^0(Y, J^0_{\mathfrak{P}}) = 0$. A consequence of the above diagram is, then, that:

(9.6) $$H^1(Y, C_p \oplus \Sigma_p) \to H$$

is an injection of Λ-modules.

By a result of Iwasawa, the p-primary components of the ideal class group of the fields $\mathbf{Q}_n^{(p)}$ vanish. It follows that:

$$H^1(Y, \mathbf{Z}/p^f) = 0$$

and, by " Kummer theory ":

$$H^1(Y_m, \mu_{p^f}) = U_m/U_m^{p^f} \qquad \text{(all these cohomology groups being}$$
$$H^2(Y_m, \mu_{p^f}) = 0 \qquad \textit{fppf}\text{-cohomology)}$$

where U_m is the group of units in the ring of integers of $\mathbf{Q}_m^{(p)}$. By the Dirichlet unit theorem, $U_m/U_m^{p^f}$ is a free $(\mathbf{Z}/p^f)$-module of rank $p^m - 1$. Replacing $\tilde{A}$ by μ_{p^f} in the diagram (7.3) and evaluating (using that $\mu_{p^f}(\mathbf{Q}_m^{(p)}) = 0$, $H^2(Y_m, \mu_{p^f}) = 0$ and that $H^2_{\cdot}(Y_{m,p_m}, \mu_{p^f})$ is dual to $H^1(Y_{m,p_m}, \mathbf{Z}/p^f)$), one finds that:

$$H^1(Y_m, \mu_{p^f}) \to H^1(Y, \mu_{p^f})^{\Gamma_m}$$

is injective, for each m, with cokernel cyclic of order p^f. It follows that $H^1(Y, \mu_{p^f})^{\Gamma_m}$ is a free $(\mathbf{Z}/p^f)$-module of rank p^m. An application of Nakayama's lemma gives that the Pontrjagin dual of $H^1(Y, \mu_{p^f})$ is a free module of rank one over $Z/p^f[[\Gamma]] = \Lambda/\eta.\Lambda$.

Taking the Pontrjagin dual of (9.6), one gets a surjective map of Λ-modules:

$$H^* \twoheadrightarrow \Lambda/\eta.\Lambda.$$

Let R denote the kernel of the above homomorphism. Form the long exact sequence:

$$\mathrm{Tor}_1^{\Lambda}(\Lambda/\eta.\Lambda, \mathbf{T}_{\mathfrak{P}}) \to R\otimes_{\Lambda}\mathbf{T}_{\mathfrak{P}} \to H^*\otimes_{\Lambda}\mathbf{T}_{\mathfrak{P}} \to \mathbf{T}_{\mathfrak{P}}/\mathfrak{I}_{\mathfrak{P}} \to 0.$$

By the resolution $0\to\Lambda\xrightarrow{\eta}\Lambda\to\Lambda/\eta\Lambda\to 0$, one sees that the Tor^1 term in the above sequence vanishes. Since $H^*\otimes_{\Lambda}\mathbf{T}_{\mathfrak{P}}$ is isomorphic to $\mathbf{T}_{\mathfrak{P}}/\mathfrak{a}$ where $\mathfrak{a}$ contains $\mathfrak{I}_{\mathfrak{P}}$, it follows that $R\otimes\mathbf{T}_{\mathfrak{P}}$ vanishes as well. By Nakayama's lemma one has $R=0$, and therefore:

$$H^*\cong\Lambda/\eta.\Lambda\cong\mathbf{Z}/p^f[[\Gamma]]$$

as Λ-module.

Proposition (9.2) is an immediate consequence of this, and Proposition (9.1) follows from Proposition (6.11) of [39] and the theorem of Imai and Serre quoted above.

Proof of Lemma (9.4). — *Part 1*: Consider the filtration of $J_{\mathfrak{P}}$ over the base $\mathrm{Spec}(\mathbf{Z}_p)$ (chap. II (8.4)):

$$0\to J_{\mathfrak{P}}^{\text{mult. type}}\to J_{\mathfrak{P}}\to J_{\mathfrak{P}}^{\text{ét}}\to 0.$$

We show that the specialization map $J_{\mathfrak{P}}(\mathbf{Q}^{(p)})\to J_{\mathfrak{P}}(\overline{\mathbf{F}}_p)$ is injective by noting that $J_{\mathfrak{P}}(\mathbf{Q}^{(p)})\cap J_{\mathfrak{P}}^{\text{mult. type}}(\overline{\mathbf{Q}}_p)$ vanishes. But the kernel of $\mathfrak{I}$ in the latter intersection is just $\Sigma(\mathbf{Q}^{(p)})$ by chapter II (16.4). It is zero, since Σ is a μ-type group, and $\mathbf{Q}^{(p)}$ does not contain the p-th roots of 1. Since $J_{\mathfrak{P}}(\mathbf{Q}^{(p)})\cap J_{\mathfrak{P}}^{\text{mult. type}}(\overline{\mathbf{Q}}_p)$ is also killed by a power of $\mathfrak{I}$, it must vanish. We shall conclude Part 1 by noting that $J_{\mathfrak{P}}(\mathbf{F}_p)=C_p$, the p-primary component of the cuspidal subgroup.

Since p is not a p-th power mod N (and $p\neq 2$), η_p is a generator of $\mathfrak{I}_{\mathfrak{P}}\subset\mathbf{T}_{\mathfrak{P}}$ (chap. II (18.10)). If π is the unit root of $X^2-T_pX+p=0$ in $\mathbf{T}_{\mathfrak{P}}$ and $\bar{\pi}$ is the non-unit root, using the Eichler-Shimura relations and well known arguments (repeated in [39], § 4 *d)* and *e)*) one deduces that $J_{\mathfrak{P}}(\mathbf{F}_p)$ is the kernel of $1-\pi$ in $J_{\mathfrak{P}}(\overline{\mathbf{F}}_p)$. But $\eta_p=(1-\pi)(1-\bar{\pi})$ and therefore $J_{\mathfrak{P}}(\mathbf{F}_p)$ is the kernel of $\mathfrak{I}_{\mathfrak{P}}$ in $J_{\mathfrak{P}}(\overline{\mathbf{F}}_p)$.

Part 2: Write out the descent sequence [39] (3.3) for the isogeny η_p^r on J:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & J[\eta_p^r] & \longrightarrow & J & \longrightarrow & J^0 & \longrightarrow & 0 \\
 & & & & \downarrow & \searrow^{\eta_p^r} & \downarrow & & \\
0 & \longrightarrow & J^0 & \longrightarrow & J & \longrightarrow & \Phi & \longrightarrow & 0
\end{array}$$

and the related long exact sequences for *fppf* cohomology. These latter we regard as exact sequences of $\mathbf{T}$-modules and we tensor them with $\mathbf{T}_{\mathfrak{P}}$, which preserves exactness. We get:

$$\begin{array}{ccccccccccccc}
0 & \to & C_p & \to & M\otimes_{\mathbf{T}}\mathbf{T}_{\mathfrak{P}} & \to & M^0\otimes_{\mathbf{T}}\mathbf{T}_{\mathfrak{P}} & \to & H^1(S, J_{\mathfrak{P}}[\eta_p^r]) & \to & H^1(S, J)_{\mathfrak{P}} & \to & H^1(S, J^0)_{\mathfrak{P}} \to H^2(S, J_{\mathfrak{P}}[\eta_p^r]) \\
 & & \downarrow & & \downarrow & \searrow^{\eta^r} & \downarrow & & & & \downarrow & \searrow^{\eta^r} & \downarrow \\
0 & \to & M^0\otimes_{\mathbf{T}}\mathbf{T}_{\mathfrak{P}} & \to & M\otimes_{\mathbf{T}}\mathbf{T}_{\mathfrak{P}} & \to & H^0(S, \Phi) & \to & H^1(S, J^0)_{\mathfrak{P}} & \to & H^1(S, J)_{\mathfrak{P}} & &
\end{array}$$

By (3.3), $M\otimes_{\mathbf{T}}\mathbf{T}_{\mathfrak{P}}$ and $M^0\otimes_{\mathbf{T}}\mathbf{T}_{\mathfrak{P}}$ are finite, and therefore by (1.2) we may evaluate them as follows: $M\otimes_{\mathbf{T}}\mathbf{T}_{\mathfrak{P}}=C_p$ and $M^0\otimes_{\mathbf{T}}\mathbf{T}_{\mathfrak{P}}=0$.

By chapter II (16.4), we have $J_{\mathfrak{P}}[\eta_p]=(C_p\oplus\Sigma_p)_{/S}$. Using the facts:

$$H^i(S, C_p)=H^i(S, \Sigma_p)=0 \quad \text{for} \quad i=1, 2$$

and: $H^0(S, \Phi)$ is free of rank 1 over $\mathbf{T}_{\mathfrak{P}}/\mathfrak{I}_{\mathfrak{P}}$,

we may evaluate the above diagram for $r=1$ and obtain the fact that η induces an isomorphism $H^1(S, J)_{\mathfrak{P}}\xrightarrow{\sim}H^1(S, J^0)_{\mathfrak{P}}$ (from the top line) and the kernel of η_p in $H^1(S, J)_{\mathfrak{P}}$ is zero (from the bottom line). Consequently, $H^1(S, J)_{\mathfrak{P}}=H^1(S, J^0)_{\mathfrak{P}}=0$.

If we now consider the top line for general r, we have that $H^1(S, J_{\mathfrak{P}}[\eta_p^r])$ is flanked by groups which vanish and hence must vanish itself.

Had [39] (5.7) been written in appropriate generality we would apply it directly to obtain what we wish.

Part 3: As it is, we reconsider its proof. Let $\mathscr{J}_p$ denote the formal completion of $J_{/\mathrm{Spec}(\mathbf{Z}_p)}$. Since $\mathscr{J}_p$ is naturally a $\mathbf{T}_p=\mathbf{T}\otimes\mathbf{Z}_p$-module, we have the decomposition (chap. II (7.1)) $\mathscr{J}_p=\mathscr{J}_{\mathfrak{P}}\times\mathscr{J}'_{\mathfrak{P}}$ using the idempotent decomposition $1=\varepsilon_{\mathfrak{P}}+\varepsilon'_{\mathfrak{P}}$.

We now prepare to copy the exact sequence of [39], Corollary (4.6). To convert to the notation of that Corollary, set $A=J$, $L_m=$ the completion of $\mathbf{Q}_m^{(p)}$ at the prime $\mathfrak{p}_m$, $D_m=$ the ring of integers in L_m, and, for some fixed m_0 set $K=L_{m_0}$, $D=D_{m_0}$. Then, for $m=m_0+h$ $(h\geq 0)$, Corollary (4.6) of [39] reads:

$$\mathscr{J}_p(D)/N_{L_m/K}\mathscr{J}_p(D_m)\to J(K)/N_{L_m/K}J(L_m)\to J(\mathbf{F}_p)/J(\mathbf{F}_p)^{p^h}\to 0$$

which is an exact sequence of $\mathbf{T}$-modules. Tensoring with $\mathbf{T}_{\mathfrak{P}}$ gives:

$$\mathscr{J}_{\mathfrak{P}}(D)/N_{L_m/K}\mathscr{J}_{\mathfrak{P}}(D_m)\to J(K)/N_{L_m/K}J(L_m)\otimes_{\mathbf{T}}\mathbf{T}_{\mathfrak{P}} \to J(\mathbf{F}_p)/J(\mathbf{F}_p)^{p^h}\otimes_{\mathbf{T}}\mathbf{T}_{\mathfrak{P}}\to 0 \tag{9.7}$$

But $\mathscr{J}_{\mathfrak{P}}$ is a formal group of multiplicative type to which Corollary (4.33) of [39] applies, giving:

The subgroups $N_{L_m/K}\mathscr{J}_{\mathfrak{P}}(D_m)\subset\mathscr{J}_{\mathfrak{P}}(D)$ stabilize for large m, and:

$$\mathscr{J}_{\mathfrak{P}}(D)/N_{L_m/K}\mathscr{J}_{\mathfrak{P}}(D_m)\cong[\Gamma/\Gamma_m]\otimes_{\mathbf{Z}_p}\mathbf{T}_{\mathfrak{P}}/(1-\pi).[\Gamma/\Gamma_m]\otimes_{\mathbf{Z}_p}\mathbf{T}_{\mathfrak{P}} \tag{9.8}$$

where $\Gamma_m=\mathrm{Gal}(\mathbf{Q}^{(p)}/\mathbf{Q}_m^{(p)})$ and π is the unit root (which is the twist matrix [39], § 4 for $\mathscr{J}_{\mathfrak{P}}$).

Since the ideal in $\mathbf{T}_{\mathfrak{P}}$ generated by $(1-\pi)$ is just $\mathfrak{I}_{\mathfrak{P}}$, the above isomorphism yields that the left-hand $\mathbf{T}_{\mathfrak{P}}$-module of (9.8) is free of rank 1 over $\mathbf{T}_{\mathfrak{P}}/\mathfrak{I}_{\mathfrak{P}}$ for large enough m. Also, by the discussion of Part 1, $J(\mathbf{F}_p)/J(\mathbf{F}_p)^{p^h}\otimes_{\mathbf{T}}\mathbf{T}_{\mathfrak{P}}$ is a free $\mathbf{T}_{\mathfrak{P}}/\mathfrak{I}_{\mathfrak{P}}$-module of rank 1, if h is large enough.

We now check that the left-hand map of exact sequence (9.7) is *injective*. This is as in Proposition (4.42) of [39]. Form the short exact sequence of Γ_{m_0}/Γ_m-modules:

$$0\to\mathscr{J}_{\mathfrak{P}}(D_m)\to J(L_m)\otimes_{\mathbf{T}}\mathbf{T}_{\mathfrak{P}}\to J(\mathbf{F}_p)\otimes_{\mathbf{T}}\mathbf{T}_{\mathfrak{P}}\to 0 \tag{9.9}$$

and note that $J(\mathbf{F}_p)\otimes_{\mathbf{T}}\mathbf{T}_{\mathfrak{P}}$ is generated by the specialization of C_p which is contained in $J(K)\otimes_{\mathbf{T}}\mathbf{T}_{\mathfrak{P}}\subset J(L_m)\otimes_{\mathbf{T}}\mathbf{T}_{\mathfrak{P}}$.

It follows that (9.9) splits as an exact sequence of $\mathbf{T}_{\mathfrak{P}}[\Gamma_{m_0}/\Gamma_m]$-modules. But the left-hand map of the exact sequence (9.7) is the map induced on 0-dimensional Tate cohomology by the map of Γ_{m_0}/Γ_m-modules $\mathscr{J}_p(D_m)\otimes_{\mathbf{T}}\mathbf{T}_{\mathfrak{P}}\to J(L_m)\otimes_{\mathbf{T}}\mathbf{T}_{\mathfrak{P}}$ appearing in the split exact sequence (9.9). Putting all the information we now have into the exact sequence (9.7) we obtain the following split exact sequence of $\mathbf{T}_{\mathfrak{P}}$-modules:

$$0\to\mathbf{T}_{\mathfrak{P}}/\mathfrak{I}_{\mathfrak{P}}\to J(K)/N_{L_m/K}J(L_m)\otimes_{\mathbf{T}}\mathbf{T}_{\mathfrak{P}}\to\mathbf{T}_{\mathfrak{P}}/\mathfrak{I}_{\mathfrak{P}}\to 0$$

for m large.

We now apply Corollary (5.4) (p. 225 of [39]) and the discussion on page 226 to conclude that the kernel of:

$$H^2_{\bullet}(Y_m, J_{\mathfrak{P}})\to H^2_{\bullet}(Y, J_{\mathfrak{P}})$$

is a free module over $\mathbf{T}_{\mathfrak{P}}/\mathfrak{I}_{\mathfrak{P}}$ of rank 2.

Added in proof (August 1977):

1. Using results of the present paper, and some new techniques, the ($\mathbf{Q}$-) rational points of $X_0(N)$ can be completely determined for all prime numbers N. One finds that there are no noncuspidal rational points on $X_0(N)$, and hence no $\mathbf{Q}$-rational N-isogenies, when N is a prime number $\geqslant 23$, such that $N\neq 37$, 43, 67, and 163. In particular the question-marks occuring in the TABLE of the introduction have been resolved. See: *Rational isogenies of prime degree* to appear in *Invent. math.*

2. An incorrect entry in a previous table of mine ([38], § 4) is corrected in the TABLE of the introduction to the present paper. Namely, when $N=199$, the data for g_- (in the table at the end of [38]) should read: $2+\mathbf{10}$ and not: $\mathbf{2}+\mathbf{10}$. In particular, when $N=199$, $\tilde{J}$ is not equal to J^-. Therefore, remark 2 of [38], 2.5 should be amended to read: $\tilde{J}=J^-$ for $N<250$, except when $N=67$, 109, 139, 151, 179, 221 *and* 199.

APPENDIX

Behavior of the Néron model of the jacobian of $X_0(N)$ at bad primes

by B. MAZUR *and* M. RAPOPORT

Throughout this appendix we depart from the convention of the rest of this paper and let N denote a *square free* number not divisible by 2 or 3, and p a prime divisor of N.

The connected component of the fibre at p of the Néron model J of the jacobian of the modular curve $M_0(N)$ (chap. II, § 1) was determined in [9]. Our purpose here is to get somewhat finer information about J, in particular about the finite abelian group:

$$\Phi = \Phi_p$$

of the connected components of the fibre at p of J.

The following theorem, which is the main result of this appendix, is due to P. Deligne:

Theorem (**A.1**). — *Let* $N = p$ *be a prime number.*

a) *The connected component* J_p^0 *of the fibre at* $\mathbf{F}_p$ *of* J *is a group of multiplicative type; considering it over* $\overline{\mathbf{F}}_p$, *the Frobenius endomorphism acts on the p-adic Tate module*:

$$\mathscr{T}a_p(J^0)$$

as: $$F^* = -p.w,$$

where w is induced from the canonical involution $(z \mapsto -1/pz)$.

b) *We have a canonical decomposition of the fibre at p of* J:

$$J_p = J_p^0 \times C$$

where C *is a cyclic group of order* $\mathrm{num}((p-1)/12)$ *generated by the class of the divisor* $(0)-(\infty)$.

More generally, write:

$$N = p.q_1, \ldots, q_\nu$$

(allowing for $\nu = 0$ to include the case $N = p$). The connected component of the fibre at p of J is an extension of $J^0(q_1, \ldots, q_\nu)_p \times J^0(q_1, \ldots, q_\nu)_p$ by a group of multiplicative type (cf. [9] and section 1 below).

As for the group $\Phi = \Phi_p$ of connected components of the fibre at p of J one has table 2 below:

TABLE 2

(u, v)	Order of $(0)-(\infty)$ in Φ	Structure of $\Phi/(0)-(\infty)$	Order of Φ	Structure of Φ	Relations satisfied by "standard" elements of Φ
$(0, 0)$	$\mathbf{Q}.\frac{p-1}{12}$	trivial	$\mathbf{Q}.\frac{p-1}{12}$	$\mathbf{Z}\Big/\Big(\mathbf{Q}.\frac{p-1}{12}\Big)\mathbf{Z}$	$\overline{\mathrm{Z}}=(0)-(\infty)$ is a generator
$(1, 0)$	$\mathbf{Q}.\frac{p-1}{6}$	$\mathbf{Z}/2^{2\nu-1}\mathbf{Z}$	$\mathbf{Q}.\frac{p-1}{12}2^{2\nu}$	$\mathbf{Z}\Big/\Big(\mathbf{Q}.\frac{p-1}{3}\Big).\mathbf{Z}$ $\oplus\mathbf{Z}/2^{2\nu-2}\mathbf{Z}$	Φ is generated by the $\overline{\mathrm{E}}_i$ $(i=1, \ldots, 2^\nu)$; relations: $\sum_i \overline{\mathrm{E}}_i=-\mathrm{S}'.\overline{\mathrm{Z}}$ $\overline{\mathrm{Z}}=2\overline{\mathrm{E}}_i$ $(i=1, \ldots, 2^\nu)$
$(0, 1)$	$\mathbf{Q}.\frac{p-1}{4}$	$\mathbf{Z}/3^{2\nu-1}\mathbf{Z}$	$\mathbf{Q}.\frac{p-1}{12}.3^{2\nu}$	$\mathbf{Z}\Big/\Big(\mathbf{Q}.\frac{p-1}{4}\Big)\mathbf{Z}$ $\oplus\mathbf{Z}/3^{2\nu-1}\mathbf{Z}$	Φ is generated by the $\overline{\mathrm{G}}_i$ $(i=1, \ldots, 2^\nu)$; relations: $\sum_i \overline{\mathrm{G}}_i=-\mathrm{S}'.\overline{\mathrm{Z}}$ $\left.\begin{matrix}\overline{\mathrm{F}}_i=2\overline{\mathrm{G}}_i\\ \overline{\mathrm{Z}}=3\overline{\mathrm{G}}_i\end{matrix}\right\}(i=1, \ldots, 2^\nu)$
$(1, 1)$	$\mathbf{Q}.\frac{p-1}{2}$	$\mathbf{Z}/6^{2\nu-1}\mathbf{Z}$	$\mathbf{Q}.\frac{p-1}{12}.6^{2\nu}$	$\mathbf{Z}/(\mathbf{Q}.p-1)\mathbf{Z}$ $\oplus\mathbf{Z}/2^{2\nu-2}\mathbf{Z}$ $\oplus\mathbf{Z}/3^{2\nu-1}\mathbf{Z}$	Φ is generated by the $\overline{\mathrm{E}}_i, \overline{\mathrm{G}}_j$ $(i, j=1, \ldots, 2^\nu)$; relations: $\sum_i \overline{\mathrm{E}}_i+\sum_j \overline{\mathrm{G}}_j=-\mathrm{S}'\overline{\mathrm{Z}}$ $\overline{\mathrm{Z}}=2\overline{\mathrm{E}}_i$ $(i=1, \ldots, 2^\nu)$ $\left.\begin{matrix}\overline{\mathrm{Z}}=3\overline{\mathrm{G}}_j\\ \overline{\mathrm{F}}_j=2\overline{\mathrm{G}}_i\end{matrix}\right\}(i, j=1, \ldots, 2^\nu)$

Notation:

a) Set $u=1$ if:

$$p\equiv 7 \text{ or } 11 \pmod{12}$$

and: all $q_i\equiv 1 \pmod 4$ $\quad i=1, \ldots, \nu$

otherwise set $u=0$.

b) Set $v=1$ if:

$$p\equiv 5 \text{ or } 11 \pmod{12}$$

and: all $q_i\equiv 1 \pmod 3$ $\quad i=1, \ldots, \nu$;

otherwise set $v=0$.

c) Set $Q=\prod_{i=1}^{\nu}(q_i+1)$ $(=1$ if $\nu=0)$.

d) The last column gives information about "standard elements" in Φ (cf. section 2). In particular $\overline{Z}=(0)-(\infty)$.

Remarks. — 1) In table 2, $\overline{Z}$ is an element (but not necessarily a generator) of the first cyclic group occurring in the column labelled "structure of Φ". $\overline{Z}$ *is* a generator of this cyclic group if $\nu=0$ or if (u, v) is $(0, 0)$ or $(0, 1)$. In all other cases $\overline{Z}$ is twice a generator.

2) The table shows that, ignoring 2- *and* 3-*primary components*, Φ_p is a cyclic group generated by the image of the divisor class $(0)-(\infty)$. Its order (again ignoring products of powers of 2 and 3) equals $Q.(p-1)$.

The order of $(0)-(\infty)$ in J is divisible by the l.c.m. of the orders of Φ_p, for all p dividing N. G. Ligozat has computed this order (as yet unpublished).

The plan of exposition is the following.

In section 1 we recall relevant results from [9] about the moduli schemes of interest. After recalling results of Raynaud [56] about the relation between the jacobian of the minimal model of a smooth curve over a discretely valued field and the Néron model of its jacobian, we reduce our problem to a computation.

This computation is outlined in section 2.

The final section 3 proves *a)* of Theorem 1.

1. Relation between minimal model and Néron model.

The following is a somewhat simplified version of ([9], VI (5.9)). Set $N'=N/p$.

Theorem **(1.1).** — a) $M_0(N)$ *is smooth over* $\mathbf{Z}[1/N']$ *outside the supersingular points in characteristic* p.

b) $M_0(N)\otimes\overline{\mathbf{F}}_p$ *is the union of two copies of* $M_0(N')\otimes\overline{\mathbf{F}}_p$ *crossing transversally at the supersingular points. If* $x=j(E, H)$ *is a supersingular point of* $M_0(N')\otimes\overline{\mathbf{F}}_p$ (i.e. $E=$*supersingular elliptic curve and* $H\subset E[N']$ *a cyclic subgroup of order precisely* N'), *then* x *on the second copy is glued to the point* $x^{(p)}$ *of the first copy of* $M_0(N')\otimes\overline{\mathbf{F}}_p$.

c) *Let* $x=j(E, H)$ *be a supersingular point of* $M_0(N')\otimes\overline{\mathbf{F}}_p$ *and set*:

$$k=\frac{1}{2}|\mathrm{Aut}(E, H)|.$$

At the corresponding point of $M_0(N)\otimes\overline{\mathbf{F}}_p$ *the scheme* $M_0(N)$ *has a singularity whose strict localization is isomorphic to*:

$$W(\overline{\mathbf{F}}_p)[[X, Y]]/(X.Y-p^k)$$

(i.e. *is of type* A_{k-1}).

d) *In particular, the reduction modulo p of the minimal model* $X_0(N)$ *of* $M_0(N)$ *(over* $\mathbf{Z}[1/N']$*) is obtained by glueing two copies of* $M_0(N')\otimes\overline{\mathbf{F}}_p$ *at corresponding supersingular points, and then replacing a crossing point by a chain of* $k-1$ *projective lines. If* $p\neq 2, 3$ *(which we will always assume), then*:

$$k>1$$

implies either:

$$j(x)=0, \quad \textit{and then} \quad k=3$$

or:

$$j(x)=1728, \quad \textit{and then} \quad k=2.$$

Those projective lines, considered as divisors on the minimal model, have self-intersection -2.

Our next task is to determine the number of supersingular points explicitly. Let:

$S'=$ the number of supersingular curves E over $\overline{\mathbf{F}}_p$ with $j(E)\neq 0, 1728$.

$$I=\begin{cases}1 & \text{if there exists a supersingular curve E over } \overline{\mathbf{F}}_p \text{ with } j(E)=1728.\\ 0 & \text{otherwise.}\end{cases}$$

$$R=\begin{cases}1 & \text{if there exists a supersingular curve E over } \overline{\mathbf{F}}_p \text{ with } j(E)=0.\\ 0 & \text{otherwise.}\end{cases}$$

Recall [1, VI (4.9)] that:

$$S'+\frac{1}{2}.I+\frac{1}{3}.R=\frac{p-1}{12}.$$

Recall from the introduction that $Q=\prod_{i=1}^{\nu}(q_i+1)$.

Proposition **(1.2).** — (i) *The number of points in* $M_0(N)\otimes\overline{\mathbf{F}}_p$ *lying above a supersingular point* $x\in M_0(p)\otimes\overline{\mathbf{F}}_p$ *is*:

$$Q \quad \textit{if} \quad j(x)\neq 0, 1728$$

$$\frac{1}{2}Q \quad \textit{if} \quad j(x)=1728 \quad \textit{but not all} \quad q_i\equiv 1 \pmod 4$$

$$\frac{1}{2}(Q-2^{\nu}) \quad \textit{if} \quad j(x)=1728 \quad \textit{and all} \quad q_i\equiv 1 \pmod 4$$

$$\frac{1}{3}Q \quad \textit{if} \quad j(x)=0 \quad \textit{but not all} \quad q_i\equiv 1 \pmod 3$$

$$\frac{1}{3}(Q-2^{\nu}) \quad \textit{if} \quad j(x)=0 \quad \textit{and all} \quad q_i\equiv 1 \pmod 3.$$

Hence:

(ii) $S'=$ *number of supersingular points x in* $M_0(N)\otimes\overline{\mathbf{F}}_p$ *with* $j(x)\neq 0, 1728$

$$=Q\frac{p-1}{12}-2^{\nu}\left(\frac{u}{2}+\frac{v}{2}\right)$$

(for u, v consult the introduction to this appendix).

Proof. — (i) is a consequence of the following facts:

a) The morphism $M_0(N)\otimes\overline{\mathbf{F}}_p \to M_0(p)\otimes\overline{\mathbf{F}}_p$ is a covering of degree Q.

b) Let $j(E)=1728$ and let (E, H) correspond to a point in $X_0(N')\otimes\overline{\mathbf{F}}_p$. If $\mathrm{Aut}(E, H)\neq\{\pm 1\}$, there is a primitive 4-th root of unity in $(\mathbf{Z}/q_i)^*$ (the automorphism group of the q_i-primary component of H) for each $i=1, \ldots, \nu$, *i.e.*:

$$q_i\equiv 1 \pmod 4 \qquad i=1, \ldots, \nu.$$

c) Similarly, if (E, H) corresponds to a point in $M_0(N')\otimes\overline{\mathbf{F}}_p$ with $j(E)=0$, and if $\mathrm{Aut}(E, H)\neq\{\pm 1\}$, then there is a primitive 6-th root of unity in $(\mathbf{Z}/q_i)^*$ for each $i=1, \ldots, \nu$, *i.e.*:

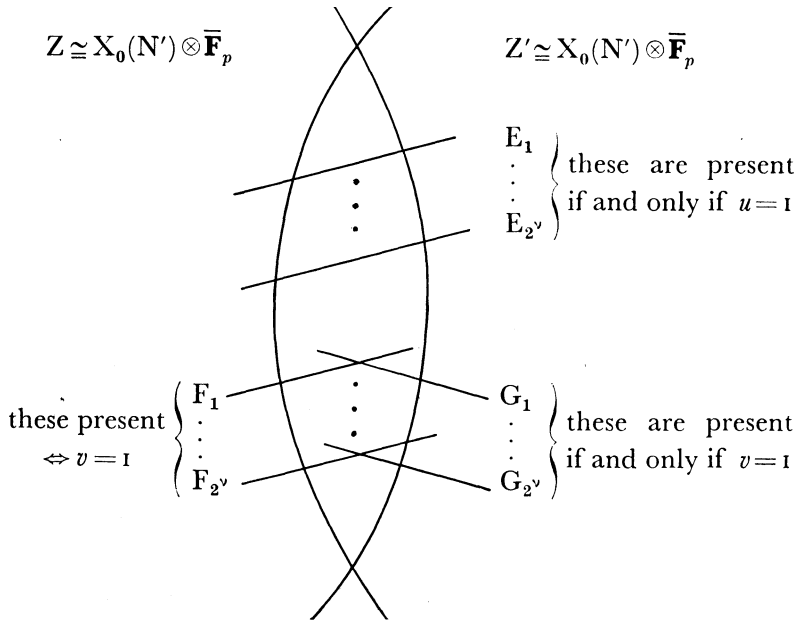
$$q_i\equiv 1 \pmod 3 \qquad i=1, \ldots, \nu.$$

(ii) follows from (i) by taking into account the formula recalled shortly before the statement of the proposition and the fact that:

$j=0$ is supersingular if $p\equiv 1 \pmod 6$

$j=1728$ is supersingular if $p\equiv 1 \pmod 4$. Q.E.D.

We obtain the following picture for the reduction modulo p of $X_0(N)$:



We now recall results of Raynaud [56] which will allow us to pass from Theorem (1.1) to Theorem (A.1) and its variants.

Let:

K = discretely valued field, complete for the valuation.
R = ring of integers in K, $k = R/(\pi)$ = residue field (assumed algebraically closed).
$S = \mathrm{Spec}(R)$, η and s its generic and closed points respectively.
C = a curve, smooth, geometrically irreducible and proper over K.
$f : \mathscr{C} \to S$ = minimal model of C over R. (Recall that $\mathscr{C}$ is the (unique) regular scheme, proper and flat over R, with generic fibre $\mathscr{C}_\eta = C$ such that for any other regular scheme $\mathscr{C}'$ flat over R with generic fibre $\mathscr{C}'_\eta = C$, the birational map $\mathscr{C}' \to \mathscr{C}$ is a morphism.)
$\mathscr{J}$ = jacobian variety of $C = \mathrm{Pic}^0(C)$.
J = Néron model of $\mathscr{J}$. (Recall that J is the (unique) group scheme smooth over R such that for every other smooth group scheme J' smooth over R, any K-morphism $J'_\eta \to J_\eta$ comes from a unique R-morphism $J' \to J$.)

The following result of Raynaud gives the connection between $\mathscr{C}$ and J:

Theorem (**1.3**). — *With the above notations, assume that* $d = \mathrm{g.c.d.}$ *of all multiplicities* d_i *of the irreducible components* C_i *of* $\mathscr{C}_s$ *is equal to* 1.

Then:

$$J \simeq \mathrm{Pic}^{[0]}_{\mathscr{C}/S}/E,$$

where:

$$\mathrm{Pic}^{[0]}_{\mathscr{C}/S} = \textit{kernel of the morphism ``degree''} \deg : \mathrm{Pic}_{\mathscr{C}/S} \to \mathbf{Z}$$

and: $E = \textit{scheme-theoretic closure of the unit section in } \mathrm{Pic}_{\mathscr{C}/S}$.

(This result is not stated in this form in [56]; it is a consequence of the results in that paper (we adhere to the terminology of [56]):

a) f verifies condition (N) and we have:

$$f_*(\mathscr{O}_{\mathscr{C}}) = \mathscr{O}_S,$$

hence f is cohomologically flat in dimension 0 ([56] (7.2.1)).

b) $\mathrm{Pic}_{\mathscr{C}/S}$ is representable by a formally smooth algebraic space in groups; and $\mathrm{Pic}^0_{\mathscr{C}/S}$ is represented by a separated smooth group scheme ([54] (8.2.1)). The quotient:

$$Q = \mathrm{Pic}_{\mathscr{C}/S}/E$$

is representable by a separated smooth group scheme over S ([56] (8.0.1)).

c) The group scheme:

$$Q^\tau = \text{inverse image in } Q \text{ of the torsion part of } Q/Q^0$$

is the Néron model of $\mathscr{J} = \mathrm{Pic}^0_{\mathscr{C}_\eta/\eta}$.

d) The morphism:

$$\mathrm{Pic}^{[0]}_{\mathscr{C}/S} \to Q^\tau$$

is surjective, with kernel E (cf. [56] (8.1.2)); hence $\mathrm{Pic}^{[0]}_{\mathscr{C}/S}/E \simeq \mathbf{Q}^r$ is the Néron model of $\mathscr{J}$.)

We extract from [56] (8.1.2) the following additional information:

Proposition **(1.4).** — *Let* $D \simeq \mathbf{Z}^n$ *be the free abelian group generated by the irreducible components* C_i *of* $\mathscr{C}_s$. *Let* $D^* = \mathrm{Hom}(D, \mathbf{Z})$ *be the dual group. Define:*

$$\alpha : D \to D^*$$

$$C \mapsto \sum_{i=1}^{n} \frac{I}{d_i}(C.C_i).C_i$$

and:

$$\beta : D^* \to \mathbf{Z}$$

$$\sum_i a_i.C_i^* \mapsto \sum_i a_i.d_i.$$

Then $\beta \circ \alpha = 0$; *and, sending* $\mathscr{L} \in \mathrm{Pic}(\mathscr{C})$ *to* $\sum_i \frac{I}{d_i}.\deg(\mathscr{L} \mid C_i).C_i^*$, *identifies:*

$$J_s/J_s^0 \simeq \ker(\beta)/\mathrm{Im}(\alpha).$$

To apply these results in our case we note that we may pass to the algebraic closure $\overline{\mathbf{F}}_p$ of $\mathbf{F}_p$ since formation of Néron models (respectively of minimal models of curves) commutes with étale base change ($\mathbf{F}_p$ is perfect).

2. Calculation of the table.

We use the Proposition (1.4) of section 1.

The irreducible components of the reduction modulo p of $X_0(N)$, the minimal model of $M_0(N)$, are Z, Z', E_i, F_i, G_i $(i = 1, \ldots, 2^\nu)$ (with the convention that E_i, respectively F_i and G_i, are missing if $u = 0$, respectively $v = 0$). They all have multiplicities equal to one.

Hence:

(2.1) $D =$ free abelian group generated by Z, Z', E_i, F_i, G_i.

Let $D_0 = \ker(\beta) =$ elements in D of degree 0 (cf. section 1, Proposition (1.4)). Let D^* and D_0^* be their respective dual groups.

Then:

(2.2) A basis of D_0^* is given by:

$$\overline{Z} = Z^* - Z'^*$$

$$\overline{E}_i = E_i^* - Z'^*$$

$$\overline{F}_i = F_i^* - Z'^*$$

$$\overline{G}_i = G_i^* - Z'^*.$$

The intersection products, as read off from the configuration of divisors given in section 1, determine the self-intersection numbers:

(2.3) $$Z.Z = -(S' + 2^{\nu}.u + 2^{\nu}.v)$$
$$Z'.Z' = -(S' + 2^{\nu}.u + 2^{\nu}.v).$$

Hence, since $\Phi = D_0^*/\mathrm{Im}(\alpha)$:

(2.4) $\Phi = D_0$/modulo the relations

$$m.\sum_i \bar{E}_i + n.\sum_i \bar{F}_i - (S' + 2^{\nu}m + 2^{\nu}n).\bar{Z} \equiv 0$$
$$m.\sum_i \bar{E}_i + n.\sum_i \bar{G}_i + S'.\bar{Z} \equiv 0$$
$$\bar{Z} - 2.\bar{E}_i \equiv 0$$
$$n.\bar{Z} - 2n\bar{F}_i + n\bar{G}_i \equiv 0$$
$$2n\bar{G}_i - n\bar{F}_i \equiv 0.$$

(2.5) The order of Φ equals the absolute value of the determinant of the intersection matrix of Z', E_i, F_i, G_i.

To fill in the table we distinguish cases:

1st case: $(u, v) = (0, 0)$

Here $\Phi = \mathbf{Z}.\bar{Z}/S'\bar{Z}$, hence its order is $S' = Q.\frac{p-1}{12}$; Φ is generated by $\bar{Z}$.

2nd case: $(u, v) = (0, 1)$

The order of Φ equals the absolute value of the determinant of the following intersection matrix:

	Z'	F_1	G_1	F_2	G_2	. . .	$F_{2^{\nu}}$	$G_{2^{\nu}}$
Z'	$-(S' + 2^{\nu})$	0	1	0	1		0	1
F_1	0	−2	1	0	0		0	0
G_1	1	1	−2	0	0		0	0
F_2	0	0	0	−2	1		0	0
G_2	1	0	0	1	−2		0	0
.							0	0
.							0	0
.							0	0
$F_{2^{\nu}}$	0	0	0	0	0		−2	1
$G_{2^{\nu}}$	1	0	0	0	0		1	−2

Adding to the Z′-row:

$$\frac{1}{3}(\text{sum over } F_i\text{-rows})+\frac{2}{3}(\text{sum over } G_i\text{-rows})$$

gives as new Z′-row:

$$-S'-2^{\nu}.\frac{2}{3},\ 0,\ 0,\ \ldots,\ 0;$$

hence the determinant equals:

$$\det=-\left(S'+\frac{1}{3}.2^{\nu}\right)3^{2^{\nu}}=-3^{2^{\nu}-1}(3.S'+2^{\nu}).$$

The relations (2.4) allow us to eliminate $\bar{F}_i$, and the $\bar{E}_i$ are absent:

$$\Phi=\left(\mathbf{Z}.\bar{Z}\oplus\bigoplus_{i=1}^{2^{\nu}}\mathbf{Z}.\bar{G}_i\right)\Big/(\sum_i\bar{G}_i+S'.\bar{Z},\ \bar{Z}-3.\bar{G}_i).$$

Hence $\Phi/(\text{cyclic subgroup generated by } \bar{Z})\cong\mathbf{Z}/3^{2^{\nu}-1}\mathbf{Z}$. The order of $\bar{Z}$ in Φ is thus:

$$3.Q.(p-1)/12;$$

since this number is prime to 3 (because, if $\nu=1$, then $p\equiv 5$ or 7 (mod 12) and $q_i\equiv 1$ (mod 3), $i=1,\ \ldots,\ 2^{\nu}$), the cyclic subgroup of Φ generated by $\bar{Z}$ is a direct summand.

3rd case: $(u, v)=(1, 0)$

The order of Φ equals the absolute value of the determinant of the following intersection matrix:

	Z′	E_1	E_2	. . .	$E_{2^{\nu}}$
Z′	$-(S'+2^{\nu})$	1	1	. . .	1
E_1	1	−2	0		0
E_2	1	0	−2		0
.					
.					
.					
$E_{2^{\nu}}$	1	0	0		−2

Adding the Z′-row to $\frac{1}{2}.$(sum of the E_i-rows) one obtains as new Z′-row:

$$-S'-\frac{1}{2}.2^{\nu},\ 0,\ 0,\ \ldots,\ 0,$$

hence: $$\det=-2^{2^{\nu}}\left(S'+\frac{1}{2}2^{\nu}\right).$$

The relations (2.4) become in this case:

$$\sum_i \bar{E}_i(S'+2^\nu).Z \equiv 0$$
$$\sum_i \bar{E}_i + S'.\bar{Z} \equiv 0$$
$$-2\bar{E}_i + Z \equiv 0.$$

Hence $\Phi/(\text{cyclic subgroup generated by } \bar{Z}) \cong \mathbf{Z}/2^{2^\nu-1}\mathbf{Z}$. The order of $\bar{Z}$ is thus $2.Q.(p-1)/12$. If $\nu \geq 1$, then the cyclic subgroup generated by $\bar{Z}$ is *not* a direct summand of Φ but is of index 2 in a direct summand.

4th case: $(u, v)=(1, 1)$

The order of Φ equals the absolute value of the determinant of the following intersection matrix:

	Z'	E_1	. . .	E_{2^ν}	F_1	G_1	. . .	F_{2^ν}	G_{2^ν}
Z'	$-(S'+2^{\nu+1})$	1	. . .	1	0	1	. . .	0	1
E_1	1	−2	0 . . .	0	0	0	. . .	0	0
.	.	0	−2	0	0	0	. . .	0	0
.	.	.	.	.	.	.		.	.
.	.	.	.	.	.	.	. . .	.	.
		.	.	.	.	.		.	.
E_{2^ν}	1	0	. . .	−2	0	0	. . .	0	0
F_1	0	0	. . .	0	−2	1	. . .	0	0
G_1	1	0		0	1	−2		0	0
.	.	.		.					
.	.	.		.					
.	.	.		.					
F_{2^ν}	0	0		0	0	0		−2	1
G_{2^ν}	1	0		0	0	0		1	−2

Add to the Z'-row:

$$\frac{1}{2}(\text{sum of } E_i\text{-rows}) + \frac{1}{3}(\text{sum of } F_i\text{-rows}) + \frac{2}{3}(\text{sum of } G_i\text{-rows})$$

to get as new Z'-row:

$$-S' + \frac{5}{6}2^\nu = -S' - 2^{\nu+1} + \frac{1}{2}.2^\nu + \frac{2}{3}.2^\nu, \quad 0, 0, \ldots, 0.$$

Hence:

$$\det = -6^{2^\nu}\left(S' + \frac{5}{6}.2^\nu\right).$$

The relations (2.4) become:

$$\left.\begin{aligned} &\bar{Z} \equiv 2.\bar{E}_i \equiv 3.\bar{G}_j \\ &\sum_i \bar{E}_i + \sum_j \bar{G}_j \equiv -S'.\bar{Z} \end{aligned}\right\} \quad (i,j = 1, \ldots, 2^\nu).$$

Hence $\Phi/(\text{cyclic subgroup generated by } \bar{Z}) \cong \mathbf{Z}/6^{2^\nu - 1}\mathbf{Z}$. The order of $\bar{Z}$ in Φ is thus $6.Q.(p-1)/12$. If $\nu \geq 1$, the cyclic subgroup of Φ generated by $\bar{Z}$ is *not* a direct summand of Φ but is of index 2 in a direct summand.

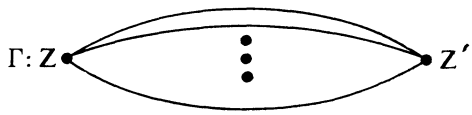
In conclusion, we have filled in all entries of the table; sections 1 and 2 also prove Theorem (A.1) except for the statement about the action of Frobenius on $J^0 \otimes \bar{\mathbf{F}}_p$.

3. The Frobenius action.

Let $N = p$ be a prime number. Denote by Γ the following graph:

vertices = components Z, Z′

edges = supersingular points (joining Z and Z′)



There is a canonical isomorphism (cf. [9]):

$$J^0 \otimes \mathbf{F}_p \simeq H^1(\Gamma, \mathbf{Z}) \otimes \mathbf{G}_m.$$

The action of the Frobenius endomorphism of $J^0 \otimes \mathbf{F}_p$ may be identified with:

$$\alpha \otimes F_{G_m} : H^1(\Gamma, \mathbf{Z}) \otimes \mathbf{G}_m \to H^1(\Gamma, \mathbf{Z}) \otimes \mathbf{G}_m$$

where $\alpha : \Gamma \to \Gamma$ is the map which fixes the vertices and which sends a supersingular point x (corresponding to an " edge " of Γ) to the unique supersingular point $x' = \alpha(x)$ such that $j(x') = j(x)^p$. But the map α induces the endomorphism $-w$ on $H^1(\Gamma, \mathbf{Z})$, because α is the composition of w with the automorphism of Γ which interchanges the vertices and keeps the edges fixed. Hence:

$$F = \alpha \otimes F_{G_m} = -p.w.$$

This proves part *a)* of Theorem (A.1).

REFERENCES

[1] ARTIN (M.), *Grothendieck topologies*, Mimeographed notes, Harvard University, 1962.

[2] ATKIN (A. O. L.), LEHNER (J.), Hecke operators on $\Gamma_0(m)$, *Math. Ann.*, **185** (1970), 134-160.

[3] BASS (H.), On the ubiquity of Gorenstein rings, *Math. Zeitschrift*, **82** (1963), 8-28.

[4] BRUMER (A.), KRAMER (K.), *On the rank of elliptic curves*, I (in preparation).

[5] CASSELS (J. W. S.), FRÖHLICH (A.) (eds.), *Algebraic Number Theory*, London-New York, Academic Press, 1967.

[6] CURTIS (C. W.), REINER (I.), *Representation theory of finite groups and associative algebras*, New York, Interscience, 1962.

[7] DELIGNE (P.), Formes modulaires et représentations l-adiques. Séminaire Bourbaki 68/69, no. 355, *Lecture Notes in Mathematics*, **179,** Berlin-Heidelberg-New York, Springer, 1971, 136-172.

[8] DELIGNE (P.), MUMFORD (D.), The irreducibility of the space of curves of given genus, *Publications Mathématiques I.H.E.S.*, **36** (1969), 75-109.

[9] DELIGNE (P.), RAPOPORT (M.), Schémas de modules des courbes elliptiques. Vol. II of The Proceedings of the International Summer School on Modular Functions, Antwerp (1972), *Lecture Notes in Mathematics*, **349,** Berlin-Heidelberg-New York, Springer, 1973.

[10] DELIGNE (P.), SERRE (J.-P.), Formes modulaires de poids 1, *Ann. Scient. Éc. Norm. Sup.*, 4e série, t. **7** (1974), 507-530.

[11] DEMAZURE (M.), GABRIEL (P.), *Groupes algébriques*, t. I, Amsterdam, North-Holland Publishing Co., 1970.

[12] DEMJANENKO (V. A.), Torsion of elliptic curves [in Russian], *Izv. Akad. Nauk. CCCP*, **35** (1971), 280-307 [MR 44, 2755].

[13] DRINFELD (G. I.), Elliptic modules [in Russian], *Mat. Sbornik*, **94** (136) (1974), No. 4. Engl. Trans.: *A.M.S.*, vol. **23** (1976), 561-592.

[14] FONTAINE (J.-M.), Groupes finis commutatifs sur les vecteurs de Witt, *C. R. Acad. Sc. Paris*, t. **280** (1975), série A, 1423-1425.

[15] GROTHENDIECK (A.), Le groupe de Brauer III : exemples et compléments (a continuation of Bourbaki exposés: 200, 297). Published in *Dix exposés sur la cohomologie des schémas*, Amsterdam, North-Holland Publ. Co., 1968,

[16] HADANO (T.), On the conductor of an elliptic curve with a rational point of order 2, *Nagoya Math. J.*, **53** (1974), 199-210.

[17] HARTSHORNE (R.), Residues and Duality, *Lecture Notes in Mathematics*, **20,** Berlin-Heidelberg-New York. Springer, 1966.

[18] HARTSHORNE (R.), On the De Rham cohomology of algebraic varieties, *Publications Mathématiques I.H.E.S.*, **45** (1975), 1-99.

[19] HECKE (E.), *Mathematische Werke*, 2nd edition, Göttingen, Vandenhoeck & Ruprecht, 1970.

[20] HERBRAND (J.), Sur les classes des corps circulaires, *Journal de Math. pures et appliquées*, 9e série, **11** (1932), 417-441.

[21] IMAI (H.), A remark on the rational points of abelian varieties with values in cyclotomic $\mathbf{Z}_p$-extensions, *Proc. Japan Acad.*, **51** (1975), 12-16.

[22] IWASAWA (K.), *Lectures on p-adic L-functions*, Princeton, Princeton University Press and University of Tokyo Press, 1972.

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

[24] 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*, **350,** Berlin-Heidelberg-New York, Springer, 1973, 69-190.

[25] KIEPERT (L.), Ueber gewisse Vereinfachungen der Transformationsgleichungen in der Theorie der elliptischen Functionen, *Math. Ann.*, **37** (1890), 368-398.

[26] KOIKE (M.), On the congruences between Eisenstein series and cusp forms (to appear).

[27] KUBERT (D.), Universal bounds on the torsion of elliptic curves, *Proc. London Math. Soc.* (3), **33** (1976), 193-237.
[28] KUBERT (D.), LANG (S.), Units in the modular function field, I, II, III, *Math. Ann.*, **218** (1975), 67-96, 175-189, 273-285.
[29] LANG (S.), *Elliptic Functions*, Addison Wesley, Reading, 1974.
[30] LIGOZAT (G.), Fonctions L des courbes modulaires, *Séminaire Delange-Pisot-Poitou*, Jan. 1970. Thesis: Courbes modulaires de genre 1, *Bull. Soc. math. France*, mémoire 43, 1975.
[31] MANIN (Y.), A uniform bound for p-torsion in elliptic curves [in Russian], *Izv. Akad. Nauk. CCCP*, **33** (1969), 459-465.
[32] MANIN (Y.), Parabolic points and zeta functions of modular forms [in Russian], *Izv. Akad. Nauk. CCCP*, **36** (1972), 19-65.
[33] MAZUR (B.), Notes on étale cohomology of number fields, *Ann. Scient. Éc. Norm. Sup.*, 4e série, t. **6** (1973), 521-556.
[34] MAZUR (B.), Rational points on abelian varieties with values in towers of number fields, *Inventiones Math.*, **18** (1972), 183-266.
[35] MAZUR (B.), Courbes elliptiques et symboles modulaires. Séminaire Bourbaki, No. 414, *Lecture Notes in Mathematics*, No. **317**, Berlin-Heidelberg-New York, Springer, 1973.
[36] MAZUR (B.), p-adic analytic number theory of elliptic curves and abelian varieties over $\mathbf{Q}$, *Proc. of International Congress of Mathematicians at Vancouver*, 1974, vol. I, 369-377, Canadian Math. Soc. (1975).
[37] MAZUR (B.), MESSING (W.), Universal extensions and one dimensional crystalline cohomology, *Lecture Notes in Mathematics*, No. **370**, Berlin-Heidelberg-New York, Springer, 1974.
[38] MAZUR (B.), SERRE (J.-P.), Points rationnels des courbes modulaires $X_0(N)$. Séminaire Bourbaki, No. 469, *Lecture Notes in Mathematics*, No. **514**, Berlin-Heidelberg-New York, Springer, 1976.
[39] MAZUR (B.), SWINNERTON-DYER (P.), Arithmetic of Weil curves, *Inventiones math.*, **25** (1974), 1-61.
[40] MAZUR (B.), TATE (J.), Points of order 13 on elliptic curves, *Inventiones math.*, **22** (1973), 41-49.
[41] MAZUR (B.), VÉLU (J.), Courbes de Weil de conducteur 26, *C. R. Acad. Sc. Paris*, t. **275** (1972), série A, 743-745.
[42] MIYAWAKA (I.), Elliptic curves of prime power conductor with $\mathbf{Q}$-rational points of finite order, *Osaka J Math.*, **10** (1973), 309-323.
[43] MUMFORD (D.), Geometric invariant theory, *Ergebnisse der Math.*, **34**, Berlin-Heidelberg-New York, Springer, 1965.
[44] MUMFORD (D.), *Curves and their jacobians*, Ann Arbor, The University of Michigan Press, 1975.
[45] NÉRON (A.), Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, *Publ. Math. I.H.E.S.*, **21** (1964), 361-483 [MR 31, 3424].
[46] NEUMANN (O.), Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten, I, II, *Math. Nachr.*, **49** (1971), 107-123; *Math. Nachr.*, **56** (1973), 269-280.
[47] ODA (T.), The first De Rham cohomology group and Dieudonné modules, *Ann. scient. Éc. Norm. Sup.*, 4e série, t. **2** (1969), 63-135.
[48] OGG (A.), Rational points on certain elliptic modular curves, *Proc. Symp. Pure Math.*, **24** (1973), 221-231, A.M.S., Providence.
[49] OGG (A.), Diophantine equations and modular forms, *Bull. A.M.S.*, **81** (1975), 14-27.
[50] OGG (A.), Hyperelliptic modular curves, *Bull. Soc. Math. France*, **102** (1974), 449-462.
[51] OGG (A.), Automorphismes des courbes modulaires, *Séminaire Delange-Pisot-Poitou*, déc. 1974 (mimeo. notes distributed by Secrétariat mathématique, 11, rue Pierre-et-Marie-Curie, 75231 Paris, Cedex 05).
[52] OHTA (M.), On reductions and zeta functions of varieties obtained from $\Gamma_0(N)$ (to appear).
[53] OORT (F.), Commutative group schemes, *Lecture Notes in Mathematics*, No. **15**, Berlin-Heidelberg-New York, Springer, 1966.
[54] OORT (F.), TATE (J.), Group schemes of prime order, *Ann. Scient. Éc. Norm. Sup.*, série 4, **3** (1970), 1-21.
[55] RAYNAUD (M.), Schémas en groupes de type $(p, \ldots, p)$, *Bull. Soc. Math. France*, **102** (1974), 241-280.
[56] RAYNAUD (M.), Spécialisation du foncteur de Picard, *Publ. Math. I.H.E.S.*, **38** (1970), 27-76.
[57] 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*, 133-157, Berlin-Heidelberg-New York, Springer, 1967.
[58] RIBET (K.), Endomorphisms of semi-stable abelian varieties over number fields, *Ann. of Math.*, **101** (1975), 555-562.

[59] SEN (S.), Lie algebras of Galois groups arising from Hodge-Tate modules, *Ann. of Math.*, **97** (1973), 160-170.
[60] SERRE (J.-P.), *Corps locaux*, Paris, Hermann, 1962.
[61] SERRE (J.-P.), Formes modulaires et fonctions zêta p-adiques, vol. III of the Proceedings of the International Summer School on Modular Functions, Antwerp (1972), *Lecture Notes in Mathematics*, **350,** 191-268, Berlin-Heidelberg-New York, Springer, 1973.
[62] SERRE (J.-P.), Algèbre locale. Multiplicités, *Lecture Notes in Mathematics*, No. **11** (3rd edition), Berlin-Heidelberg-New York, Springer, 1975.
[63] SERRE (J.-P.), *Abelian l-adic representations and elliptic curves*, Lectures at McGill University, New York-Amsterdam, W. A. Benjamin Inc., 1968.
[64] SERRE (J.-P.), Quelques propriétés des variétés abéliennes en caractéristique p, *Amer. J. Math.*, **80** (1958), 715-739.
[65] SERRE (J.-P.), p-torsion des courbes elliptiques (d'après Y. Manin). Séminaire Bourbaki, 69-70, No. 380, *Lecture Notes in Mathematics*, No. **180,** Berlin-Heidelberg-New York, Springer, 1971.
[66] SERRE (J.-P.), Congruences et formes modulaires (d'après H. P. F. Swinnerton-Dyer). Séminaire Bourbaki, 71-72, No. 416, *Lecture Notes in Mathematics*, No. **317,** Berlin-Heidelberg-New York, Springer, 1973.
[67] SERRE (J.-P.), Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Inventiones math.*, **15** (1972), 259-331.
[68] SETZER (B.), Elliptic curves of prime conductor, *J. Lond. Math. Soc.* (2), **10** (1975), 367-378.
[69] SHIMURA (G.), Introduction to the arithmetic theory of automorphic functions, *Publ. Math. Soc. Japan*, No. **11,** Tokyo-Princeton, 1971.
[70] WADA (H.), A table of Hecke operators, *Proc. Japan Acad.*, **49** (1973), 380-384.
[71] YAMAUCHI (M.), On the fields generated by certain points of finite order on Shimura's elliptic curves, *J. Math. Kyoto Univ.*, **14** (2) (1974), 243-255.
[72] BOREVICH (Z. I.), SHAFAREVICH (I. R.), *Number theory*, London-New York, Academic Press, 1966.
[73] PARRY (W. R.), A determination of the points which are rational over **Q** of three modular curves (unpublished).
[74] SERRE (J.-P.), TATE (J.), Good reduction of abelian varieties, *Ann. of Math.*, **88** (1968), 492-517.
[75] TATE (J.), Algorithm for determining the type of a singular fiber in an elliptic pencil, vol. IV of The Proceedings of the International Summer School on Modular Functions, Antwerp (1972), *Lecture Notes in Mathematics*, **476,** Berlin-Heidelberg-New York, Springer, 1975.
[SGA 3] Séminaire de Géométrie algébrique du Bois-Marie, 62-64. Directed by M. DEMAZURE and A. GROTHENDIECK, *Lecture Notes in Mathematics*, Nos. **151, 152, 153,** Berlin-Heidelberg-New York, Springer, 1970.
[SGA 7] Séminaire de Géométrie algébrique du Bois-Marie, 67-69. P. DELIGNE and N. KATZ, *Lecture Notes in Mathematics*, Nos. **288, 340,** Berlin-Heidelberg-New York, Springer, 1972, 1973.

Manuscrit reçu le 16 avril 1976.