Two-dimensional representations in the arithmetic of modular curves

B. Mazur K. A. Ribet

In the theory of automorphic representations of a reductive algebraic group G over a number field K, it is broadly — but not always — true that irreducible representations occurring in $L^2(G_{\mathbf{A}}/G_K)$ occur with multiplicity one. In a *classical special case* ($G = \mathbf{GL}(2)$, $K = \mathbf{Q}$, and where we restrict attention to automorphic representations which are holomorphic, cuspidal, and of weight 2), the Galois-theoretic counterpart of the above "multiplicity one phenomenon" is the assertion that given a newform of the above type, of level N, the (two-dimensional p-adic) $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-representation associated to it occurs *with multiplicity one* in the p-adic Tate module of $J_1(N)$.

For some important arithmetic applications, however, one is led to search for criteria guaranteeing certain analogues of the above "multiplicity one phenomenon" valid for the mod p Galois representations associated to newforms. The "mod p multiplicity" questions are somewhat more delicate than their p-adic counterparts. Indeed, to our knowledge, the main cases where the mod p Galois representation questions have been treated seriously so far are for cuspidal newforms of weight two which are either unramified at p [20, 30] or ordinary and nonspecial at p [25, 43].

The present article concerns itself with a "missing p-ordinary case," one for which the newform is "special" at p.[1] We assume, more precisely, that the level of the newform is divisible by p but not by p^2, and also that the Nebentypus character of the form is trivial. (Our method might also treat the more general case in which the character is unramified at p, but possibly non-trivial.) For the case where the character is ramified at p, see [12].

[1]We also require that the associated mod p Galois representation be absolutely irreducible, avoiding the important, but much more difficult, case of *Eisenstein primes* [20, 24].

This case arises in the second author's article [30] on Serre's conjectures. Assume that p is an odd prime, and suppose that ρ is an irreducible mod p representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ which arises from the space of weight-2 modular forms on $\Gamma_o(M)$. (We then say that ρ is *modular of level* M.) Assume that $\ell \neq p$ is a prime factor of M for which ρ is unramified at ℓ. Then Serre's conjectures [37] predict that ρ is modular of level M_o, where M_o is the prime-to-ℓ part of M. This statement was proved by the first author [22] in case ℓ "exactly divides M" (i.e., $M_o = M/\ell$) and the congruence $\ell \equiv 1 \bmod p$ is *not* satisfied. (See [30], Theorem 6.1.) It was proved by the second author if ℓ exactly divides M and the newform giving ρ is unramified at p, i.e., p is prime to M ([30], Theorem 8.2). The methods of [30] show, more generally, that ρ is modular of level M_o whenever ℓ exactly divides M and ρ occurs with multiplicity one in the Jacobian $J_o(M)$. This motivated our interest in the mod p multiplicity one question for Galois representations.

The mod p multiplicity-one question for Galois representations has an intriguing, and relatively complicated, answer for twisted forms of $\mathbf{GL}(2)$ [32]. It would be quite interesting to have even a conjectural picture telling us what to expect for multiplicities of mod p Galois representations in a more general context.

We would like to thank Bas Edixhoven for enlightening conversations on subjects related to this article and for detailed comments on our preliminary versions. We also thank the IHES for providing the congenial setting in which much of this work was done.

Contents

1 Introduction and statement of the main theorem

1.1 The representations V_φ

Let M be a positive integer. Let $\Gamma_o(M)$ be (as usual) the subgroup of $\mathbf{SL}(2,\mathbf{Z})$ which consists of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}(2,\mathbf{Z})$ with $c \equiv 0 \pmod{M}$. Let $X_o(M)$ be the associated modular curve over $\mathbf{Q}$. Finally, let T_n for $n \geq 1$ denote the standard Hecke correspondences on $X_o(M)$. (See, for example, [24], Chapter 2, §5 for a description of the Hecke operators T_q for q prime. When q divides M, our operator T_q is the "Atkin operator" denoted U_q in [24].)

These operators induce endomorphisms on the space $S_2(\Gamma_o(M))$ of weight-2 cusp forms on the group $\Gamma_o(M)$ and on the Jacobian

$$J = J_o(M) = \mathrm{Pic}^o(X_o(M))$$

of $X_o(M)$. We write simply T_n for each of these endomorphisms. (The endomorphism T_n of $J_o(M)$ is denoted T_n^* in [18].) The subrings of $\mathrm{End}(J_o(M))$ and of $\mathrm{End}(S_2(\Gamma_o(M)))$ which these operators generate are the "same." More precisely, the faithful operation of $\mathrm{End}(J_o(M))$ on $S_2(\Gamma_o(M))$ (coming from the fact that this latter space is the cotangent space of the abelian variety dual to $J_o(M)$) maps the endomorphism labeled T_n of $J_o(M)$ to the endomorphism of $S_2(\Gamma_o(M))$ labeled T_n. We let $\mathbf{T}_M$ be the subring of $\mathrm{End}(J_o(M))$

generated by the T_n, viewing this ring, when convenient, as operating on $S_2(\Gamma_o(M))$.

Let $\varphi : \mathbf{T}_M \to \overline{\mathbf{F}}_p$ be a ring homomorphism. The kernel of φ is a maximal ideal $\mathfrak{m} = \mathfrak{m}_\varphi$ of $\mathbf{T}_M$. As usual, we denote by $J[\mathfrak{m}]$ the "kernel of $\mathfrak{m}$ on J," i.e., the intersection of the kernels of all elements of $\mathfrak{m}$ acting on $J(\overline{\mathbf{Q}})$. This subgroup of the finite group $J[p]$ has natural commuting actions of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ and of the residue field $k_\mathfrak{m} = T_M/\mathfrak{m}$. Further, the field $k_\mathfrak{m}$ is embedded in $\overline{\mathbf{F}}_p$ by φ. Let

$$V_\varphi := J[\mathfrak{m}] \otimes_{k_\mathfrak{m}} \overline{\mathbf{F}}_p.$$

Then V_φ is a finite-dimensional (continuous) representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $\overline{\mathbf{F}}_p$. The vector space V_φ is easily seen to be non-zero.

The representations $J[\mathfrak{m}]$ and V_φ may be compared with the canonical two-dimensional representation $\rho_\mathfrak{m}$ of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ which is associated to $\mathfrak{m}$ ([11], Th. 6.7 or [30], Prop. 5.1). Recall that this is the semisimple representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $k_\mathfrak{m}$, unique up to isomorphism, which is unramified outside the set of primes dividing pM and which satisfies

$$\mathrm{trace}(\rho_m(\sigma_r)) \equiv T_r \bmod \mathfrak{m}, \qquad \det(\rho_\mathfrak{m}(\sigma_r)) \equiv r \bmod \mathfrak{m}$$

for all primes r not dividing pM. (Here σ_r is a Frobenius element for r in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.) We define ρ_φ to be the representation $\rho_\mathfrak{m} \otimes_{k_\mathfrak{m}} \overline{\mathbf{F}}_p$, i.e., the representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ deduced from $\rho_\mathfrak{m}$ by the base change $k_\mathfrak{m} \to \overline{\mathbf{F}}_p$ induced by φ.

These two-dimensional representations are said to be *modular of level M*. More generally, suppose that $\mathbf{F}$ is an algebraic extension of $\mathbf{F}_p$. We say that a semisimple representation $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \mathbf{F})$ is modular of level M if there is an embedding $\iota : \mathbf{F} \hookrightarrow \overline{\mathbf{F}}_p$ so that ρ, when viewed over $\overline{\mathbf{F}}_p$ via ι, is isomorphic to some ρ_φ. It is equivalent to ask that the representation $\rho \otimes_\mathbf{F} \overline{\mathbf{F}}_p$ be of the form ρ_φ for *each* embedding $\iota : \mathbf{F} \hookrightarrow \overline{\mathbf{F}}_p$.

Assume that the two-dimensional representation $\rho_\mathfrak{m}$ is irreducible. Then by the Eichler-Shimura relations, the Cebotarev Density Theorem, and the Brauer-Nesbitt Theorem, one sees that the semisimplification of $J[\mathfrak{m}]$ as a $k_\mathfrak{m}[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module is a direct sum of some number of copies of $\rho_\mathfrak{m}$ ([20], Chapter II,§14 or [30], Th. 5.2). Also, the representation ρ_φ is automatically an irreducible representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $\overline{\mathbf{F}}_p$, provided that $p \neq 2$.[2]

[2]According to a recent theorem of Boston, Lenstra and the second author [6], $J[\mathfrak{m}]$ is semisimple whenever ρ_φ is irreducible over $\overline{\mathbf{F}}_p$.

1.2 Questions of multiplicity

Definition 1 The *multiplicity* of $\rho_{\mathfrak{m}}$ in the representation $J[\mathfrak{m}]$ is the multiplicity of $\rho_{\mathfrak{m}}$ in the semisimplification of $J[\mathfrak{m}]$. We denote this integer by $\mu_{\mathfrak{m}}$ or μ_φ. We have $\mu_\varphi = \dim V_\varphi/2$.

The multiplicity $\mu_{\mathfrak{m}}$ is "typically" equal to 1. To cite the simplest possible example, take $M = 11$. Then $J_o(11)$ is an elliptic curve, $\mathbf{T} = \mathbf{Z}$, and the ideals $\mathfrak{m}$ are the prime ideals (p) of $\mathbf{Z}$. The kernel $J_o(11)[p]$ is then an $\mathbf{F}_p$-vector space of dimension two. In [20], the first author showed more generally that $\mu_{\mathfrak{m}} = 1$ when M is a *prime*, except perhaps in a small number of special situations when $p = 2$. (In these special situations, no example has been found where $\mu_{\mathfrak{m}} \neq 1$.) In [30] (Th. 5.2b), the second author employed the techniques of [20] to prove a theorem valid when M is not necessarily prime, but p does not divide $2M$.

MAIN THEOREM *Let $M = pN$, where N is prime to p. Let $\mathfrak{m}$ be a maximal ideal of the Hecke ring $\mathbf{T}_M$ with $\mathbf{T}/\mathfrak{m}$ of characteristic p. Suppose that $\rho_{\mathfrak{m}}$ is an absolutely irreducible representation of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Assume further that $\rho_{\mathfrak{m}}$ is not modular of level N. Then $\mu_{\mathfrak{m}} = 1$.*

The absolute irreducibility of $\rho_{\mathfrak{m}}$, is equivalent to the irreducibility of $\rho_{\mathfrak{m}}$ as a representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $\mathbf{T}/\mathfrak{m}$ whenever p is odd. This follows from the fact that $\rho_{\mathfrak{m}}(c)$, where c is a complex conjugation in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, then has the distinct eigenvalues $+1$, -1 in $\mathbf{T}/\mathfrak{m}$.

The condition that $\rho_{\mathfrak{m}}$ is not modular of level N may be examined from varied perspectives. Serre conjectured in 1985 that $\rho_{\mathfrak{m}}$ is *finite* at p ([37], p. 189) if and only if $\rho_{\mathfrak{m}}$ is modular of level N ([36], Conjecture C_2, cf. [37]). This conjecture was proved by the first author soon afterwards: see [22], or [30], Theorem 6.1.

The condition may also be expressed in terms of newforms of weight 2. To say that $\rho_{\mathfrak{m}}$ is modular of level pN means, concretely, that it is a mod p representation attached to a weight-2 newform f, having trivial character, whose level divides pN. To say that it is not modular of level N then means that every f giving rise to $\rho_{\mathfrak{m}}$ has level divisible by p. In the language of representation theory, f is "special" at p in the sense that the component at p of the adelic representation of $\mathbf{GL}(2)$ associated to f is a special representation of $\mathbf{GL}(2, \mathbf{Q}_p)$. (See [25] for results in the case of weight-two p-ordinary modular forms which are not special at p.)

Suppose, more generally, that $\mathfrak{m} \subset \mathbf{T}_M$ is a maximal ideal, and assume that ρ_m is absolutely irreducible. What is the multiplicity of ρ_m in $J_o(M)[\mathfrak{m}]$?

In cases where the residue characteristic p of $\mathfrak{m}$ divides the integer M, we have little information other than that provided by the Main Theorem. For example, we have not been able to determine the multiplicity in all cases when $M = pN$ is as in the Main Theorem, but $\rho_{\mathfrak{m}}$ is modular of level N. We have been able to show, at least, that there are some cases where the multiplicity exceeds 1; those which we have discovered have M divisible by p^3 and $\rho_{\mathfrak{m}}$ modular of level M/p^2 (see §13 below).

The reader may wish to consult also [32], which gives a systematic construction of multiplicity-two examples for Jacobians of Shimura curves.

1.3 mod p Galois representations ρ and homomorphisms φ

The discussion of this section records some thoughts on placing the Main Theorem in a somewhat larger context. It will not be used in the rest of the article. For simplicity, we suppose throughout this discussion that p is a prime number different from 2 and 3.

We shall be concerned with mod p Galois representations arising from weight-two eigenforms with Nebentypus, whose associated Dirichlet characters have conductor prime to p. In other words, we shall consider cusp forms of weight two on groups of the form $\Gamma_1(N) \cap \Gamma_o(p^\nu)$, where N an integer prime to p and where $\Gamma_1(N)$ is, as usual, the subgroup of $\mathbf{SL}(2, \mathbf{Z})$ which is represented by matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ which satisfy the congruences $a \equiv d \equiv 1$ and $c \equiv 0 \pmod{N}$.

There is a standard operation of $(\mathbf{Z}/N\mathbf{Z})^*$ on the space of such forms. For each $a \in (\mathbf{Z}/N\mathbf{Z})^*$, the corresponding automorphism of the space of cusp forms is the "diamond bracket operator" $\langle a \rangle$. This operator arises from an automorphism, again denoted $\langle a \rangle$, of the modular curve over $\mathbf{Q}$ which is associated with the subgroup $\Gamma_1(N) \cap \Gamma_o(p^\nu)$ of $\mathbf{SL}(2, \mathbf{Z})$. (See, for example, [18] for a discussion of $\langle a \rangle$ in varied guises.) In the context of $\Gamma_1(N) \cap \Gamma_o(p^\nu)$, we include the operators $\langle a \rangle$, for $a \in (\mathbf{Z}/N\mathbf{Z})^*$, along with the Hecke operators T_n, in defining $\mathbf{T}_{p^\nu N}$. A semisimple representation $\rho_\varphi\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \overline{\mathbf{F}}_p)$ is again associated to each ring homomorphism $\varphi : \mathbf{T}_{p^\nu N} \to \overline{\mathbf{F}}_p$. This representation satisfies

$$\mathrm{trace}(\rho_\varphi(\sigma_r)) = \varphi(T_r), \qquad \det(\rho_\varphi(\sigma_r)) = \varphi(\langle r \rangle) r$$

for all prime numbers r which are prime to pN.

Similarly, for each $M \geq 1$, we have a diamond bracket operation of $(\mathbf{Z}/M\mathbf{Z})^*$ on the space of cusp forms of weight two on $\Gamma_1(M)$.

Let $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \overline{\mathbf{F}}_p)$ be a continuous, irreducible representation with odd determinant. Serre ([37],§3) has associated to such a representation three invariants: $N = N(\rho)$, $k = k(\rho)$, and $\epsilon = \epsilon(\rho)$. Here N is a positive integer prime to p (which we shall call *the tame level* of ρ), k is an integer ≥ 2 (the *weight* of ρ), and ϵ is a homomorphism from $(\mathbf{Z}/N\mathbf{Z})^*$ to $\overline{\mathbf{F}}_p^*$ (the *character* of ρ).

Given such a homomorphism $\epsilon : (\mathbf{Z}/N\mathbf{Z})^* \to \overline{\mathbf{F}}_p^*$, we have its multiplicative (or "Teichmüller") lifting $\epsilon_o : (\mathbf{Z}/N\mathbf{Z})^* \to \overline{\mathbf{Q}}_p^*$, the unique character of finite order prime to p which lifts ϵ.

Serre conjectures ([37] 3.2.3, 3.2.4) that there exists a classical (parabolic) newform over $\overline{\mathbf{Q}}_p$, on $\Gamma_o(N)$, with weight k and character ϵ_o, such that the mod p Galois representation associated to it (by the construction of Shimura when $k = 2$ and Deligne for $k > 2$) is equivalent to ρ. (As Serre has noted [38], his conjectures must be modified slightly in the cases $p = 2$ and $p = 3$. These cases have been excluded in our discussion.)

Suppose, now, that ρ is given with invariants (N, k, ϵ) and that Serre's conjecture holds for ρ, i.e., that there is a newform with invariants (N, k, ϵ_o) whose associated mod p Galois representation is equivalent to ρ. Suppose further that

$$k \equiv 2 \bmod p{-}1.$$

The determinant of ρ is then the product $\chi\epsilon$, where χ is the mod p cyclotomic character of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. This suggests that ρ arises from an eigenform of weight two on $\Gamma_1(N) \cap \Gamma_o(p^\nu)$ for some integer $\nu \geq 0$. If this is the case for a given ν, we shall refer to p^ν as a *wild level* for ρ.

PROPOSITION 1 *There is a newform with invariants $(p^\nu N, \epsilon_o, 2)$ whose associated mod p Galois representation is equivalent to ρ, for some $\nu \leq 2$.*

Proof. Using Theorem 3.5(d) of [4], we can find an integer j such that the twist of ρ by the j^{th} power of the mod p cyclotomic character arises from an eigenvector g in the space of weight-two cusp forms on $\Gamma_1(pN)$ over $\overline{\mathbf{F}}_p$. This eigenform may be chosen so that the diamond bracket operation of $(\mathbf{Z}/pN\mathbf{Z})^*$ on g is given as follows: the group $(\mathbf{Z}/N\mathbf{Z})^*$ operates via the character ϵ, and the group $(\mathbf{Z}/p\mathbf{Z})^*$ operates as the $(2j)^{\text{th}}$ power of the identity character $(\mathbf{Z}/p\mathbf{Z})^* \to \mathbf{F}_p^*$. Equivalently, $(\mathbf{Z}/N\mathbf{Z})^*$ operates via (the mod p reduction of the character) ϵ_o, while $(\mathbf{Z}/p\mathbf{Z})^*$ operates via ω^{2j}, where ω is the unique Dirichlet character $(\mathbf{Z}/p\mathbf{Z})^* \to \overline{\mathbf{Q}}_p^*$ which lifts the identity character. After twisting g by ω^{-j}, we obtain a weight-two eigenform on the group $\Gamma_1(p^2N)$, with character ϵ, whose associated Galois representation is ρ. (For a convenient discussion of the behavior of characters and levels of eigenforms under twisting, see [3], §3.) This eigenform is a modular form over $\overline{\mathbf{F}}_p$.

It follows by a well known lemma ([11], lemme 6.11) that ρ arises from a weight-two eigenform on $\Gamma_1(L)$, for some level L dividing p^2N. Further, the associated Dirichlet character of $(\mathbf{Z}/L\mathbf{Z})^*$ is a lift of the character ϵ. By [8], Prop. 3 (which applies because we have supposed $p \geq 5$), we may assume that this lift is ϵ_o. Also, we may suppose that the eigenform is a newform, possibly after replacing L by a divisor of L. (A short summary of the theory of newforms is presented in [28], §1.) The Proposition now follows from the fact that L is necessarily divisible by N ([8], §1.1 or [19], Proposition 0.1). $\square$

Let $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \overline{\mathbf{F}}_p)$ be an irreducible representation as above, i.e., one of tame level N for which Serre's conjecture holds. Suppose that p^ν is a wild level for ρ.

Definition 2 A homomorphism $\varphi : \mathbf{T}_{p^\nu N} \to \overline{\mathbf{F}}_p$ is *associated* to ρ if the representations ρ and ρ_φ are isomorphic. The homomorphism $\varphi : \mathbf{T}_M \to \overline{\mathbf{F}}_p$ is *(p-)ordinary* if $\varphi(T_p) \neq 0$. It is *(p)-singular* if $\varphi(T_p) = 0$.

For each homomorphism φ associated to ρ, a multiplicity μ_φ is defined as above. The methods presented below should show that we have $\mu_\varphi = 1$ in the case where $\nu = 1$ and where p^ν is a minimal wild level for ρ, i.e., where ρ is not modular of level N. Similarly, the argument of [20], Chapter II, Proposition 14.2 (cf. [30], Proposition 5.1b) should prove that $\mu = 1$ whenever $\nu = 0$. (In both cases, one needs only to check that arguments given for forms on $\Gamma_o(N)$ work equally well for $\Gamma_1(N)$.) This suggests that the multiplicity μ_φ should be 1 in the remaining case where p^ν is a minimal wild level for ρ, i.e., that for which $\nu = 2$ and ρ does not arise from weight-2 forms on $\Gamma_1(N) \cap \Gamma_o(p)$. It would be very interesting to investigate this question.

We next discuss the extent to which φ is determined by ρ.

PROPOSITION **2** *There is at most one p-singular homomorphism φ associated to ρ.*

Proof. Let φ be a p-singular homomorphism φ associated to ρ. By definition, the image of T_p under φ is 0. The images of the diamond bracket operators $\langle a \rangle$, for $a \in (\mathbf{Z}/N\mathbf{Z})^*$, are the character values $\epsilon(a)$, where $\epsilon = \epsilon(\rho)$. Similarly, for each prime number r not dividing pN, $\varphi(T_r) = \mathrm{trace}(\rho_\varphi(\sigma_r))$. It remains to show that the quantity $\varphi(T_r)$ is uniquely determined when r is a prime dividing N.

Let V be a two-dimensional $\overline{\mathbf{F}}_p$-vector space which is furnished with a continuous $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-action equivalent to ρ. For each prime $r \neq p$, let $I_r \subset \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ be an inertia group for r. We shall prove the formula

$$\varphi(T_r) = \mathrm{trace}(\sigma_r \mid V^{I_r}), \tag{1}$$

where V^{I_r} is the space of I_r-invariants on V.

For this, we recall that the formal power series $\sum_{n\geq 1} \varphi(T_n)q^n$ is a weight-two cusp form on $\Gamma_1(N)\cap\Gamma_o(p^\nu)$, with coefficients in $\overline{\mathbf{F}}_p$ (cf. [30], §5). This means that there is a cusp form on this group, with coefficients in the "integer ring" $\mathcal{O}$ of $\mathbf{Q}_p$, whose q-expansion reduces to $\sum_{n\geq 1} \varphi(T_n)q^n$ modulo the maximal ideal $\mathfrak{p}$ of $\mathcal{O}$. The form $\sum_{n\geq 1} \varphi(T_n)q^n$ is an eigenform for the Hecke operators T_n, with eigenvalues $\varphi(T_n)$.

By a well known lemma ([11], 6.11), one may find an eigenform $f = \sum a_n q^n$ with coefficients in $\mathcal{O}$ whose eigenvalues λ_n lift the $\varphi(T_n)$. There is then a newform g of level dividing $p^\nu N$ whose n^{th} coefficient coincides with λ_n for n prime to pN. The level of g is in fact divisible by N. Indeed, let W be the $\mathfrak{p}$-adic representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ associated to f. According to results of Deligne, Langlands and Carayol (see [7]), the level of g is the conductor of W. Further, this conductor is divisible by the conductor $N = N(\rho)$ which Serre associates to V ([8], §1.1 or [19]).

Thus the conductors of V and W coincide locally at each prime $r \neq p$. Concretely, this equality means that the $\overline{\mathbf{F}}_p$-dimension of V^{I_r} agrees with the $\overline{\mathbf{Q}}_p$-dimension of the space W^{I_r} ([8], *loc. cit.*). By viewing V as the mod $\mathfrak{p}$ reduction of a lattice in W, we then obtain the congruence

$$\mathrm{trace}(\sigma_r \mid V^{I_r}) \equiv \mathrm{trace}(\sigma_r \mid W^{I_r}) \bmod \mathfrak{p}.$$

However, by the results of Deligne, Langlands and Carayol mentioned above, we have the equality

$$\mathrm{trace}(\sigma_r \mid W^{I_r}) = \lambda_r.$$

Since λ_r reduces to $\varphi(T_r)$ mod $\mathfrak{p}$, we find the desired congruence (1). □

Analogously, we find:

Proposition 3 *There is at most one p-ordinary homomorphism φ associated to ρ.*

Proof. In view of the proof we have given for Proposition 2, the proposition will follow after we show that there is at most one possibility for $\varphi(T_p)$, given that $\varphi(T_p)$ is non-zero and that φ is associated to ρ.

PROPOSITION **4 ([23])** *Let φ be associated to ρ and suppose that $\varphi(T_p) \neq 0$. Then V, viewed as a representation of a decomposition group for p, D_p, in* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, *has a 1-dimensional unramified quotient on which σ_p acts by multiplication by $\varphi(T_p)$.*

This proposition follows from Theorem 9 of [23] (which, incidentally, requires the hypothesis $p > 3$ which we imposed above). It clearly implies that there is at most one non-zero possibility for $\varphi(T_p)$, since V cannot have two distinct unramified quotients. Indeed, the full representation V cannot be unramified at p, since the determinant of V is given by the character $\epsilon\chi$, which is *ramified* at p. (Note that $p \neq 2$ by assumption.) □

2 Admissible models and admissible morphisms

Let p be a prime number. Let K be a finite field extension of $\mathbf{Q}_p$, $\mathcal{O} \subset K$ its ring of integers, and k its residue field. Let $\mathcal{O}^{\mathsf{h}}$ be the completion of a strict henselization of $\mathcal{O}$, and denote by $\overline{k}$ the (algebraically closed) residue field of $\mathcal{O}^{\mathsf{h}}$. The *normalized valuation* on $\mathcal{O}^{\mathsf{h}}$ is the one which gives a uniformizer of $\mathcal{O}$ the value 1.

Let n be a positive integer. A complete local $\mathcal{O}^{\mathsf{h}}$-algebra R will be said to be of *type n* if there is an element $\zeta \in \mathcal{O}^{\mathsf{h}}$ of normalized valuation n, such that R is isomorphic (as complete local $\mathcal{O}^{\mathsf{h}}$-algebra) to $\mathcal{O}^{\mathsf{h}}[[X,Y]]/(XY-\zeta)$, where $\mathcal{O}^{\mathsf{h}}[[X,Y]]$ is the power series ring in the two variables X and Y over $\mathcal{O}^{\mathsf{h}}$. If R is of type n, then R is a rational singularity, and, in fact, an isolated normal singularity of type A_n in the sense of [1] (see also: [16] and [10] Chap. VI 6.9). If R is of type 1, then R is regular, and the images of X and Y provide a *regular sequence* for R. If R is of type $n > 1$, then R is not regular. Nevertheless, the scheme $\mathrm{Spec}\, R$ has a canonical (minimal) desingularization obtained by a series of blow-ups; the inverse image of the closed point of $\mathrm{Spec}\, R$ in this canonical desingularization is a chain of $n-1$ curves of genus zero. For a readable and graphic account of this blow-up procedure, at least in the analogous situation of complex surfaces, see Pinkham's survey article [26].

Say that a local $\mathcal{O}^{\mathsf{h}}$-algebra R is *admissible* if it is of type n for some positive integer n.

Let $\mathcal{X}$ be a proper flat $\mathcal{O}$-scheme. Then we will call $\mathcal{X}$ *admissible* if the closed fiber is reduced, every irreducible component of the closed fiber is a smooth curve, and the completions of the strict henselizations of the local rings of the scheme $\mathcal{X}$ at all closed points x at which the structure morphism $\mathcal{X} \to \operatorname{Spec} \mathcal{O}$ is non-smooth are admissible local $\mathcal{O}^{\mathsf{h}}$-algebras. A proper flat admissible $\mathcal{O}$-scheme has the property that its closed fiber is reduced, and is a union of smooth curves which possesses only ordinary double points as singularities. In particular, such a scheme $\mathcal{X}$ has only a finite number of non-regular points, and possesses a canonical minimal desingularization $\tilde{\mathcal{X}}$ obtained by punctual blow-ups.

Let $X_{/K}$ be a smooth, proper (not necessarily irreducible) curve. An *admissible model* for $X_{/K}$ over $\mathcal{O}$ is a proper flat model $X_{/\mathcal{O}}$ for $X_{/K}$ over $\operatorname{Spec} \mathcal{O}$ such that the scheme $X_{/\mathcal{O}}$ is admissible. If $X_{/\mathcal{O}}$ is admissible, then the canonical desingularization $\tilde{X}_{/\mathcal{O}}$ is also admissible.

Example 1 Let N be an integer relatively prime to p, and let $X_o(Np)_{/\mathbf{Q}_p}$ be Shimura's canonical model of the modular curve $X_o(Np)$ over $\mathbf{Q}_p$. Then the canonical model $X_o(Np)_{/\mathbf{Z}_p}$ as described in [10, 14] is *admissible* in the above sense. The special fiber of $X_o(Np)_{/\mathbf{Z}_p}$ is isomorphic to two copies of $X_o(N)_{/\mathbf{F}_p}$ intersecting transversally at each of the supersingular points, these supersingular points being of type A_n for some $n \geq 1$.

For a proof of this assertion, the reader can consult [10], Chapter VI, Theorem 6.9, where in fact a more general result (which will also be useful to us) is proved. Namely, let N be an integer prime to p, let H be a subgroup of $\mathbf{GL}(2, \mathbf{Z}/N\mathbf{Z})$, and let $H^{\tilde{}}$ be the inverse image of H in $\mathbf{GL}(2, \hat{\mathbf{Z}})$. In [10], the coarse moduli scheme $M_{H^{\tilde{}} \cap \Gamma_o(p)}$ over $\mathbf{Z}[\frac{1}{N}]$ is studied. Let $\mathcal{O} = \mathbf{Z}_p$ and let $X_o(p; H^{\tilde{}})_{/\mathbf{Z}_p}$ be the pullback of $M_{H^{\tilde{}} \cap \Gamma_o(p)}$ to $\mathbf{Z}_p$. (It should perhaps be noted that the scheme $X_o(p; H^{\tilde{}})_{/\mathbf{Z}_p}$ is not necessarily irreducible, but this is not much of a bother.) The indicated theorem of [10] guarantees that $X_o(p; H^{\tilde{}})_{/\mathbf{Z}_p}$ is admissible.

Consider a finite morphism

$$f : X_{1/\mathcal{O}} \to X_{2/\mathcal{O}}$$

between admissible $\mathcal{O}$-schemes which is surjective on generic fibers. It follows that f is finite and faithfully flat on generic fibers. The restriction of f to fibers over $\overline{k}$ has the property that it is again finite and surjective (but not necessarily flat).

If s_2 is any singular point of the fiber of X_2 over $\overline{k}$, denote by A_2 and B_2 the two irreducible components of $X_{2/\overline{k}}$ containing s_2. Let s_1 be a point of $X_{1/\overline{k}}$ in $f^{-1}(s_2)$.

Definition 3 The mapping f is said to be *equi-ramified* at s_1 if:

(a) *The point s_1 is singular in $X_{1/\overline{k}}$.* The two components of $X_{1/\overline{k}}$ containing s_1 then have the property that one of them (say, A_1) is mapped by f onto A_2 and the other (call it B_1) is mapped onto B_2.

(b) *The ramification indices at s_1 of the two mappings*

$$A_1 \to A_2 \qquad B_1 \to B_2$$

induced by f are equal.

If f, as above, is equi-ramified at s_1, we let the *ramification index $e_f(s_1)$* of f at s_1 be the common ramification index of the two mappings $A_1 \to A_2$ and $B_1 \to B_2$.

Definition 4 The mapping f is said to be *admissible* if it is a finite morphism of admissible models, as above, which is equi-ramified at every point s_1 of $X_{1/\overline{k}}$ such that $f(s_1)$ is a singular point in $X_{2/\overline{k}}$.

We thank Bas Edixhoven for providing us with a proof of the following Proposition.

PROPOSITION **5** *Let*

$$f : X_{1/\mathcal{O}} \to X_{2/\mathcal{O}}$$

be a finite morphism between admissible models. Then f is an admissible morphism. If the schemes $X_{1/\mathcal{O}}$ and $X_{2/\mathcal{O}}$ are regular, then f is finite and flat; moreover, for s_1 any closed point of $X_{1/\overline{k}}$ such that $s_2 = f(s_1)$ is a singular point of $X_{2/\overline{k}}$, the ramification index $e_f(s_1)$ is 1 (i.e., f is unramified at s_1).

Proof. Without loss of generality, we may assume that $\overline{k} = k$. Let s_1 be a closed point of $X_{1/k}$ such that $s_2 = f(s_1)$ is a double point. For $i = 1, 2$, let R_i denote the completed local rings of the schemes $X_{i/\mathcal{O}}$ at s_i. Then the rings R_i are of the form

$$R_1 = A[[x, y]](xy - z^a), \qquad R_2 = A[[u, v]]/(uv - z^b),$$

where A is a complete discrete valuation ring, z is a uniformizer of A, and a, b are positive integers. The morphism f induces a morphism $\varphi\colon R_2 \to R_1$ of A-algebras which makes R_1 a finite R_2-algebra. Let Z_x, Z_y denote the irreducible components of $\operatorname{Spec} R_1/zR_1$ defined as the reduced subschemes with support $x = 0$ and $y = 0$, respectively. Interchanging x and y, if necessary, we may suppose that f maps Z_x and Z_y to the branches of $\operatorname{Spec} R_2/zR_2$ cut out by $u = 0$ and $v = 0$, respectively. In particular, $\varphi(u)$ is a unit at the generic point of Z_y and $\varphi(v)$ is a unit at the generic point of Z_x.

Form the complete regular local ring $R = A[[s,t]]/(st - z)$. Map the ring R_1 to R by sending x to s^a and y to t^a and send R_2 to R by composing φ with this homomorphism $R_1 \to R$. The homomorphisms of R_i to R are injections. The ring R is a unique factorization domain, and the factorization of z is given by $z = st$ (s and t being irreducible elements). Since $uv = z^b$ ($= s^b \cdot t^b$ in R), and since $\varphi(u)$ is a unit at the generic point of Z_y, the unique factorization of the image $\tilde{u}$ of u in R is given by $\tilde{u} = \tilde{\alpha} \cdot s^c$ where $\tilde{\alpha}$ is a unit of R, and c is a positive integer. For the same reason, the unique factorization of the image $\tilde{v}$ of v in R is given by $\tilde{v} = \tilde{\beta} \cdot t^d$ for $\tilde{\beta}$ a unit of R and d a positive integer. It follows that $\tilde{\alpha}\tilde{\beta} = 1$ and $c = d = b$. Now let $\mathcal{O}_s$, $\mathcal{O}_t$ denote the discrete valuation rings which are the localizations at the generic points of the irreducible components $s = 0$ and $t = 0$, respectively, in $\operatorname{Spec} R$. Let $\mathcal{O}_x$, $\mathcal{O}_y$, $\mathcal{O}_u$, $\mathcal{O}_v$ be the analogously defined discrete valuation rings for x, y, u and v. Their residue fields are respectively $k((t))$, $k((s))$ and $k((y))$, $k((x))$, $k((v))$, $k((u))$, where k is A/zA, the residue field of A. All six of these discrete valuation rings have $z \in A$ as uniformizer. Therefore, the extensions

$$\mathcal{O}_u \subset \mathcal{O}_x \subset \mathcal{O}_s, \qquad \mathcal{O}_v \subset \mathcal{O}_y \subset \mathcal{O}_t$$

have degrees equal to the degrees of the corresponding residue field extensions

$$k((u)) \subset k((x)) \subset k((s)), \qquad k((v)) \subset k((y)) \subset k((t)).$$

In view of the two equalities

$$[k((s)) : k((u))] = [k((s)) : k((x))] \cdot [k((x)) : k((u))],$$
$$[k((t)) : k((v))] = [k((t)) : k((y))] \cdot [k((y)) : k((v))],$$

we have $b = a \cdot n$, where n is the (common) degree

$$n = [k((x)) : k((u))] = [k((y)) : k((v))].$$

Hence $\tilde{\alpha} \cdot \tilde{x}^n = \tilde{u}$ and $\tilde{\alpha}^{-1} \cdot \tilde{y}^n = \tilde{v}$, giving that

$$\varphi(u) = \alpha \cdot x^n \text{ and } \varphi(v) = \alpha^{-1} y^n,$$

for α a suitable unit in R_1. In particular, f is admissible, the ramification index $e_f(s_1)$ is equal to n, and we have established the first assertion of the Proposition.

Suppose now that the schemes $X_{i/\mathcal{O}}$ are regular. Then $a = b = 1$, and so $n = e_f(s_1)$ is also equal to 1. Since f is a finite morphism between regular (equidimensional) schemes of the same dimension, it follows that f is finite and flat; for a proof of this, see [14], *Notes added in proof*, pp. 507–508. □

PROPOSITION **6** *Let M and N be positive integers such that M divides N and N is relatively prime to p. Then the natural mapping*

$$X_o(Np)_{/\mathbf{Z}_p} \to X_o(Mp)_{/\mathbf{Z}_p},$$

composed, before and after, with any automorphisms of the domain and range $\mathbf{Z}_p$-schemes, is an admissible morphism of admissible schemes.

Proof. We will prove (and make use of) a more general assertion. Let H_1 and H_2 be subgroups of $\mathbf{GL}(2, \mathbf{Z}/N\mathbf{Z})$ with $H_1 \subseteq H_2$, and let $\tilde{H_1}$ and $\tilde{H_2}$ be their inverse images in $\mathbf{GL}(2, \hat{\mathbf{Z}})$. Let $X_o(p; \tilde{H_1})_{/\mathbf{Z}_p}$ and $X_o(p; \tilde{H_2})_{/\mathbf{Z}_p}$ be the corresponding modular curves, as in Example 1 above. Consider the natural projection

$$X_o(p; \tilde{H_1})_{/\mathbf{Z}_p} \to X_o(p; \tilde{H_2})_{/\mathbf{Z}_p},$$

and let h be a composition of this map with automorphisms of the source and target $\mathbf{Z}_p$-schemes. Then we have

PROPOSITION **7** *The mapping h is admissible.*

Proof. By the discussion in Example 1 above, the domain and range of h are admissible schemes over $\mathbf{Z}_p$. The morphism h being finite, Proposition 5 implies the statement of our Proposition. □

3 The graph S

Let $X_{/\mathcal{O}}$ be admissible, and denote by $Z_{/k} \to X_{/k}$ the normalization of the special fiber. Thus $Z_{/k}$ is a disjoint union of smooth projective curves over k. By the *graph of our model*, we mean the usual graph S (or $S(\overline{k})$ to emphasize its dependence on the choice of an algebraic closure, $\overline{k}$) of its special fiber. In other words, the set of *vertices of* $S(\overline{k})$ is the set of irreducible components of $X_{/\overline{k}}$ (or equivalently, of $Z_{/\overline{k}}$) and the set of *edges* of $S(\overline{k})$ is $\mathrm{Sing}(X_{/\overline{k}})$, the set of singular points of $X_{/\overline{k}}$. The incidence relations are the evident ones, i.e., inverse-inclusion, and the graph $S(\overline{k})$ is endowed with a natural action of $\mathrm{Gal}(\overline{k}/k)$.

By $H_1(S, W)$ we mean the singular (first) homology group of the graph S, with coefficients in an abelian group W. We may view $H_1(S, W)$ explicitly as follows (cf. [13], IX 12.3.5). The *oriented edges* of the graph $S(\overline{k})$ are in 1-1 correspondence with points $\mathbf{s}$ on $Z_{/\overline{k}}$ which lie over singular points $s \in \mathrm{Sing}(X_{/\overline{k}})$. Since each s is an ordinary double point, there are two oriented edges lying over each singular point s. A 1-chain with values in W is a formal sum $\sum w_{\mathbf{s}} \cdot \mathbf{s}$ where the summation is taken over oriented edges, the coefficients are drawn from W, and we have $w_{\mathbf{s}} = -w_{\mathbf{s}'}$ whenever $\mathbf{s}$ and $\mathbf{s}'$ are the two oriented edges lying over a given $s \in \mathrm{Sing}(X_{/\overline{k}})$. For each $\mathbf{s}$, let $A(\mathbf{s})$ be the irreducible component of $Z_{/\overline{k}}$ containing $\mathbf{s}$, and set

$$\partial(\sum w_{\mathbf{s}} \cdot \mathbf{s}) := \sum w_{\mathbf{s}} \cdot A(\mathbf{s}),$$

where the right-hand sum is considered as formal sum, with coefficients in W, on the set of components of $Z_{/\overline{k}}$. The group $H_1(S, W)$ is then the subgroup of the group of 1-chains consisting of those 1-chains $\sum w_{\mathbf{s}} \cdot \mathbf{s}$ which are annihilated by ∂. This condition means that for each irreducible component A we have $\sum w_{\mathbf{s}} = 0$, where the summation is taken over all oriented edges $\mathbf{s}$ which correspond to points lying on A.

We shall view $H_1(S, \overline{k}) = H_1(S(\overline{k}), \mathbf{F}_p) \otimes \overline{k}$ as a $\mathrm{Gal}(\overline{k}/k)$-module via the *diagonal* action.

Let $f \colon X_{1/\mathcal{O}} \to X_{2/\mathcal{O}}$ be an admissible mapping. Let $Z_{i/k} \to X_{i/k}$ be the normalizations of the special fibers of the domain and range of f and let $S_i(\overline{k})$ denote the associated graphs ($i = 1$ and 2). The mapping f induces a map on special fibers $Z_1 \to Z_2$ over k and a $\mathrm{Gal}(\overline{k}/k)$-equivariant mapping of graphs $S_1 \to S_2$. This latter mapping is surjective on vertices and edges; it collapses an edge of S_1 if and only if the corresponding singular point x_1 of $X_{1/\overline{k}}$ maps to a smooth point of $X_{2/\overline{k}}$. For each abelian group W, we define

$$f_* : H_1(S_1, W) \to H_1(S_2, W)$$

to be the map on homology which is induced by this equivariant mapping. Further, we define

$$f^* : H_1(S_2, W) \to H_1(S_1, W)$$

by defining f^* on oriented edges as follows: $f^*(\mathbf{s}_2) = \sum e_f(s_1) \cdot \mathbf{s}_1$, where the summation is taken over all oriented edges $\mathbf{s}_1$ of the special fiber of X_1 which map, via f, to the oriented edge $\mathbf{s}_2$ of the special fiber of X_2. Here, $e_f(s_1)$ is the ramification index of the unoriented edge s_1 (i.e., the unoriented edge "underlying" $\mathbf{s}_1$). It is straightforward to check that f^* so defined brings 1-cycles to 1-cycles, i.e., induces a mapping $f^*\colon H_1(S_2, W) \to H_1(S_1, W)$, and that $f^* f_*$ is given by multiplication by $\deg(f)$.

In what follows, we will concentrate on the $\mathrm{Gal}(\overline{k}/k)$-equivariant mappings $f_*\colon H_1(S_1, \overline{k}) \to H_1(S_2, \overline{k})$ and $f^*\colon H_1(S_2, \overline{k}) \to H_1(S_1, \overline{k})$ on homology.

PROPOSITION **8** *The homotopy type of the graph S is functorially dependent only upon $X_{/K}$ and not upon the choice of admissible model $X_{/\mathcal{O}}$.*

Proof. The essential fact used in the demonstration of this proposition is that any two (admissible) models $X_{/\mathcal{O}}$ and $X'_{/\mathcal{O}}$ of the same curve $X_{/K}$ are commensurable via blow-ups at points on the special fiber [15, 39]. This being the case, one must show that the homotopy type of S is independent of such blow-ups, which is straightforward. □

4 $\mathrm{Pic}^o(X_{/\mathcal{O}})$

Let $X_{/\mathcal{O}}$ be admissible, and let $\tilde{X}_{/\mathcal{O}} \to X_{/\mathcal{O}}$ be its canonical desingularization. Let Pic^o be the functor which is studied by Raynaud in [27]. Since X has rational singularities, the induced morphism of functors

$$\mathrm{Pic}^o(X_{/\mathcal{O}}) \to \mathrm{Pic}^o(\tilde{X}_{/\mathcal{O}})$$

is an isomorphism. Indeed, this can be seen by a computation of the mapping on tangent spaces induced by the above morphism using the Leray spectral sequence for the mapping $\varphi : \tilde{X} \to X$, and relative coherent cohomology over $\mathcal{O}$. More precisely, since φ is the "blowing down" morphism of a rational singularity, one calculates:

LEMMA **1** *We have*

$$R^q\varphi_*\mathcal{O}_{\tilde{X}} = \begin{cases} 0 & \text{for } q > 0, \\ \mathcal{O}_X & \text{for } q = 0. \end{cases} \qquad \square$$

Since the functor $\mathrm{Pic}^o(\tilde{X}_{/\mathcal{O}})$ is representable by a smooth group scheme over $\mathcal{O}$, so is $\mathrm{Pic}^o(X_{/\mathcal{O}})$. We refer to the group scheme representing $\mathrm{Pic}^o(X_{/\mathcal{O}})$ simply as $\mathrm{Pic}^o(X_{/\mathcal{O}})$.

Let $A_{/\mathcal{O}}$ denote the Néron model over the base $\mathcal{O}$ of the abelian variety $A = \mathrm{Pic}^o(X_{/K})$. (The recent publication [5] may be consulted as a source book on Néron models. It contains, in particular, a detailed discussion of Néron models of Jacobians of curves.) By Raynaud's theorem (for statements, compare: [24] Chap. 2 Prop. 1, [9] Theorem 2.5, [13] IX 12.1 and [27]), which applies to $\tilde{X}_{/\mathcal{O}}$ since $\tilde{X}_{/\mathcal{O}}$ is a regular surface with reduced special fiber, the natural homomorphism of group schemes over $\mathcal{O}$, $\mathrm{Pic}^o(X_{/\mathcal{O}}) \to A_{/\mathcal{O}}$ identifies $\mathrm{Pic}^o(X_{/\mathcal{O}})$ with the open subgroup scheme $A^o_{/\mathcal{O}}$ (the connected component containing the identity) of $A_{/\mathcal{O}}$. We have natural morphisms

$$\begin{aligned} f_* &: \mathrm{Pic}^o(X_{1/K}) \to \mathrm{Pic}^o(X_{2/K}) \\ f^* &: \mathrm{Pic}^o(X_{2/K}) \to \mathrm{Pic}^o(X_{1/K}) \end{aligned} \tag{2}$$

since f is finite and flat on generic fibers. From (2), and functoriality of the Néron model we obtain direct and inverse image mappings

$$\begin{aligned} f_* &: A_{1/\mathcal{O}} \to A_{2/\mathcal{O}} \\ f^* &: A_{2/\mathcal{O}} \to A_{1/\mathcal{O}} \end{aligned} \tag{3}$$

which by restriction to connected components and the identification described above yield:

$$\begin{aligned} f_* &: \mathrm{Pic}^o(X_{1/\mathcal{O}}) \to \mathrm{Pic}^o(X_{2/\mathcal{O}}) \\ f^* &: \mathrm{Pic}^o(X_{2/\mathcal{O}}) \to \mathrm{Pic}^o(X_{1/\mathcal{O}}). \end{aligned} \tag{4}$$

By restriction to the closed fiber, we have morphisms

$$\begin{aligned} f_* &: \mathrm{Pic}^o(X_{1/k}) \to \mathrm{Pic}^o(X_{2/k}) \\ f^* &: \mathrm{Pic}^o(X_{2/k}) \to \mathrm{Pic}^o(X_{1/k}), \end{aligned} \tag{5}$$

In (2)–(5), the composition f^*f_* of direct and inverse image mappings is given by multiplication by $\deg(f)$. Moreover, the inverse image mapping in (5) is the natural pullback morphism.

5 Semi-stable filtrations

Let $X_{/\mathcal{O}}$ be admissible. We shall recall and compare the standard filtrations on (a) the special fiber $A_{/k}$ and (b) the p-divisible group associated to the generic fiber $A_{/K}$.

(a) As for the special fiber $A_{/k}$, we have the three-stage filtration:

$$0 \subset (A_{/k})^{\mathrm{t}} \subset (A_{/k})^{o} \subset A_{/k}, \tag{6}$$

where the superscripts ^{o} and $^{\mathrm{t}}$ refer to "connected component containing the identity" and "toric part," respectively.

Denote by $T_{/k}$ the toric part $(A_{/k})^{\mathrm{t}}$ and let $J_{/k}$ be the abelian variety $(A_{/k})^{o}/T_{/k}$. We have already remarked in §4 above that $\mathrm{Pic}^{o}(X_{/k})$ is isomorphic to $(A_{/k})^{o}$ by Raynaud's theorem. The natural normalization mapping $Z_{/k} \to X_{/k}$ induces a mapping φ: $\mathrm{Pic}^{o}(X_{/k}) \to \mathrm{Pic}^{o}(Z_{/k})$, which is a surjective mapping of group schemes over k. The kernel of φ can be identified with the subfunctor of $\mathrm{Pic}^{o}(X_{/k})$ whose $\overline{k}$-valued points are given by isomorphism classes of line bundles on $X_{/\overline{k}}$ which are trivial on each irreducible component of $X_{/\overline{k}}$. Since $\mathrm{Pic}^{o}(Z_{/k})$ is an abelian variety and since, from the above description, $\ker\varphi$ is seen to be a torus whose character group may be naturally identified with $H_1(S(\overline{k}), \mathbf{Z})$ (cf. [13], IX, 12.3.7), we have:

PROPOSITION 9 *The abelian variety* $\mathrm{Pic}^{o}(Z_{/k})$ *may be identified (via* φ*) with* $J_{/k}$*, the* abelian variety part *of* $\mathrm{Pic}^{o}(X_{/k})$ *while* $T_{/k}$*, the* toric part *of* $\mathrm{Pic}^{o}(X_{/k})$*, may be identified with* $\ker\varphi$*, whose character group is canonically isomorphic to* $H_1(S(\overline{k}), \mathbf{Z})$*.* □

It follows from this that the Néron model $A_{/\mathcal{O}}$ is semi-stable.

(b) As for the semi-stable filtration on p-divisible groups over K, let $A_{p/K}$ denote the p-divisible group (over K) attached to the abelian variety $A_{/K}$. We have the filtration of p-divisible groups over K:

$$0 \subset A_p^{\mathrm{t}} \subset A_p^{\mathrm{f}} \subset A_p \tag{7}$$

in which A_p^{t} denotes the maximal p-divisible subgroup of A_p over K which extends to the p-divisible group associated to a torus over $\mathcal{O}$, and where A_p^{f} is the maximal p-divisible subgroup of $A_{p/K}$ which extends to a p-divisible group over $\mathcal{O}$ (cf. [13] IX §5 and especially Raynaud's result quoted there (Thm. 5.8)). By a result of Tate [42], if there is an extension of a p-divisible group over K to $\mathcal{O}$, then that extension is unique (up to canonical isomorphism). Let, then, $A^{\mathrm{f}}_{p/\mathcal{O}}$ and $A^{\mathrm{t}}_{p/\mathcal{O}}$ denote the unique extensions of A_p^{f} and A_p^{t}, respectively, to $\mathcal{O}$.

By ([13] IX 5.2) the filtration (7) is self-dual in the sense that in the natural (Cartier) self-duality on the $\mathrm{Gal}(\overline{K}/K)$-module $\mathsf{Ta}(A_p(\overline{K}))$, the submodules $\mathsf{Ta}(A_p^{\mathrm{t}}(\overline{K}))$ and $\mathsf{Ta}(A_p^{\mathrm{f}}(\overline{K}))$ are the annihilator subspaces of each other, where Ta denotes "Tate module."

Proposition **10** *There are canonical morphisms*

(i) $A^{\mathrm{f}}_{p/\mathcal{O}} \to A_{/\mathcal{O}}$

(ii) $A^{\mathrm{t}}_{p/\mathcal{O}} \to A^{\mathrm{f}}_{p/\mathcal{O}}$,

where (i) is a morphism in the evident sense (i.e., a direct limit of compatible morphisms on the kernels of multiplication by p^n *in the* p*-divisible group over* $\mathcal{O}$*, as* n *goes to infinity) extending the natural morphisms on the generic fiber, and where (ii) is an embedding of* p*-divisible groups over* $\mathcal{O}$ *extending the natural embedding on the generic fiber.*

Proof. The existence of the morphism (i) is a direct consequence of Raynaud ([13] IX 5.8). To see that (ii) is an embedding, note that the dual of $A^{\mathrm{t}}_{p/\mathcal{O}}$ is etale, and is consequently a (faithfully flat) quotient of the "etale quotient group" of $A^{\mathrm{f}}_{p/\mathcal{O}}$. The result then follows easily by dualizing. □

Starting with the morphism (i) of Proposition 10, we first pass to the special fiber, and then note that the resulting morphism factors through $(A_{/k})^o$ and hence through its associated p-divisible group. We obtain therefore a morphism

(iii) $$A^{\mathrm{f}}_{p/k} \to (A_{/k})^o_p.$$

of p-divisible groups over k.

Proposition **11** *The above morphism is an isomorphism, and it identifies the* p*-divisible subgroup* $A^{\mathrm{t}}_{p/k}$ *of* $A^{\mathrm{f}}_{p/k}$ *with* $(A_{/k})^{\mathrm{t}}_p \subset (A_{/k})^o_p$.

Proof. This is the content of the isomorphisms (7.3.1)–(7.3.4) of [13]. □

Returning to the filtration (7) of p-divisible group schemes over K, and letting the "suffix" $[p^n]$ denote kernel of multiplication by p^n, we have the filtration

$$0 \subset A^{\mathrm{t}}_p[p^n] \subset A^{\mathrm{f}}_p[p^n] \subset A_p[p^n] \tag{8}$$

of finite (etale) group schemes over K. The Weil pairing [,] defines a perfect (alternating) self-duality

$$A_p[p^n] \times A_p[p^n] \to \mu_{p^n}$$

with values in the scheme-theoretic kernel μ_{p^n} of multiplication by p^n in the multiplicative group $\mathbf{G}_{\mathsf{m}}$. The filtration (8) is auto-dual with respect to this pairing, in the sense that $A^{\mathrm{t}}_p[p^n]$ and $A^{\mathrm{f}}_p[p^n]$ are each other's annihilators. This follows from a simple argument using ([13] IX 5.2.2 or Prop. 5.6).

Corollary *Let W denote the module defined by the exact sequence*

$$0 \to A_p^{\mathrm{f}}[p](\overline{K}) \to A_p[p](\overline{K}) \to W \to 0.$$

Choose an algebraic closure $\overline{K}/K$ compatible with the choice of algebraic closure $\overline{k}/k$ of the residue field, giving a surjection

$$\iota : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(\overline{k}/k).$$

Use ι to endow the $\mathbf{F}_p[\mathrm{Gal}(\overline{k}/k)]$-module $H_1(S(\overline{k}), \mathbf{F}_p)$ with an action of the Galois group $\mathrm{Gal}(\overline{K}/K)$. Once $\overline{K}$ and ι are fixed, there is a canonical isomorphism of $\mathbf{F}_p[\mathrm{Gal}(\overline{K}/K)]$-modules,

$$W \approx H_1(S(\overline{k}), \mathbf{F}_p).$$

In particular, the action of $\mathrm{Gal}(\overline{K}/K)$ on W is unramified.

Proof. This is a straightforward calculation using the duality statement above combined with Proposition 9. (Cf. [13], IX, §11.6.) □

6 Rosenlicht differentials

Let $X_{/\mathcal{O}}$ be admissible, and let $Z_{/k} \to X_{/k}$ be the normalization mapping of its special fiber. If $s \in X(\overline{k})$ is a singular point, denote by $s_1, s_2 \in Z(\overline{k})$ the two points in its pre-image. If k' is a subfield of $\overline{k}$, a *Rosenlicht differential* on an open subscheme U of $X_{/k'}$ is a rational differential 1-form ω on V, the pre-image of U in $Z_{/k'}$, such that ω is regular on the complement in V of the pre-image of the singular locus of U and such that ω has, at worst, simple poles on the pre-image points $s_1, s_2 \in V(\overline{k})$ of each singular point s in $U(\overline{k}) \subset X(\overline{k})$ and such that ω has residues of opposite sign at these pre-image points:

$$\mathrm{res}_{s_1} \omega = -\,\mathrm{res}_{s_2} \omega. \tag{9}$$

The assignment

$$U \mapsto \text{ Rosenlicht differentials on } U$$

defines a coherent sheaf on X/k, which we denote simply Ω or $\Omega_{X_{/k}}$.

Remark. The reader might compare the above definition with ([33] bottom of page 177 and Theorem 8) and also ([35] Chapter IV, §3, n°9), where the notion of *regular differential* is defined on singular curves. Specifically, if

X is a complete singular (reduced) algebraic curve, a *regular differential* on X is defined to be a regular differential ω (in the ordinary sense) on the normalization X' of X, which has the property that

$$\sum_{s' \to s} \operatorname{res}_{s'}(g \cdot \omega) = 0.$$

Here, s is any $\overline{k}$-valued point of X, s' ranges over all points of X' lying over s, and g is an arbitrary rational function on X' which is regular at all points lying over s.

A global Rosenlicht differential ω on $X_{/\overline{k}}$ defines a simplicial 1-cycle with coefficients in $\overline{k}$ on the graph $S(\overline{k})$ in an evident manner. Indeed, let

$$c_\omega := \sum \operatorname{res}_{\mathbf{s}} \omega \cdot \mathbf{s},$$

where the sum runs over all points on $Z_{/\overline{k}}$ lying over some singular point of $X_{/\overline{k}}$. In view of (9), the sum c_ω is a 1-chain in the sense of §3. Moreover, this 1-chain is visibly a 1-cycle (i.e., satisfies $\partial(c_\omega) = 0$) because the sum of the residues of ω over all points in any irreducible component vanishes. Passing to the homology class of the cycle c_ω, we obtain a map

$$h : H^0(X_{/\overline{k}}, \Omega) \to H_1(S(\overline{k}), \overline{k}).$$

This map is $\operatorname{Gal}(\overline{k}/k)$-equivariant because of the formula

$$\sigma(\operatorname{res}_{\mathbf{s}} \omega) = \operatorname{res}_{\sigma\mathbf{s}}(\sigma\omega), \tag{10}$$

valid for $\sigma \in \operatorname{Gal}(\overline{k}/k)$, $\omega \in H^0(X_{/\overline{k}}, \Omega)$, and $\mathbf{s}$ a $\overline{k}$-valued point on Z.

PROPOSITION **12** *The map $h\colon \omega \mapsto c_\omega$ is a surjection*

$$H^0(X_{/\overline{k}}, \Omega) \to H_1(S(\overline{k}), \overline{k})$$

whose kernel may be identified with $H^0(Z_{/\overline{k}}, \Omega^1)$. We have, in other words, a $\operatorname{Gal}(\overline{k}/k)$-equivariant exact sequence:

$$0 \to H^0(Z_{/\overline{k}}, \Omega^1) \to H^0(X_{/\overline{k}}, \Omega) \xrightarrow{h} H_1(S(\overline{k}), \overline{k}) \to 0.$$

Proof. Left-exactness of the sequence in the statement of the Proposition is immediate. The surjectivity of h follows from a general fact: given any finite set $\mathcal{S}$ of points on a smooth projective curve over $\overline{k}$, and any mapping $r\colon \mathcal{S} \to \overline{k}$ such that the sum $\sum_{s \in \mathcal{S}} r(s)$ vanishes, there is a 1-differential ω on the curve with at worst simple poles on $\mathcal{S}$ as singularities and such that for each $s \in \mathcal{S}$ we have $\operatorname{res}_s(\omega) = r(s)$. □

Corollary *Let k' be an extension of k in $\overline{k}$, and let $G' = \mathrm{Gal}(\overline{k}/k')$. Then we have an exact sequence*

$$0 \to H^0(Z_{/k'}, \Omega^1) \to H^0(X_{/k'}, \Omega) \to H_1(S(\overline{k}), \overline{k})^{G'} \to 0. \tag{11}$$

Proof. Taking G'-invariants in the exact sequence of Proposition 12, we obtain (11). Indeed, it is well known that the 1-dimensional cohomology of G' with values in the $\overline{k}$-vector space $H^0(Z_{/\overline{k}}, \Omega^1)$ vanishes (Hilbert's Theorem 90). □

Now let $f\colon X_{1/\mathcal{O}} \to X_{2/\mathcal{O}}$ be an admissible mapping. Then we have a series of induced "direct" and "inverse" image mappings f_*, f^* which fit into a diagram

$$\begin{array}{ccccccccc} 0 & \to & H^0(Z_{1/\overline{k}}, \Omega^1) & \to & H^0(X_{1/\overline{k}}, \Omega) & \to & H_1(S_1(\overline{k}), \overline{k}) & \to & 0 \\ & & f^* \uparrow\downarrow f_* & & f^* \uparrow\downarrow f_* & & f^* \uparrow\downarrow f_* & & \\ 0 & \to & H^0(Z_{2/\overline{k}}, \Omega^1) & \to & H^0(X_{2/\overline{k}}, \Omega) & \to & H_1(S_2(\overline{k}), \overline{k}) & \to & 0. \end{array} \tag{12}$$

The definition of f^* and f_* on regular differentials on $Z_{1/\overline{k}}$ and $Z_{2/\overline{k}}$ is given in the standard local manner, the definition of f_* being the usual trace construction on differentials using flatness of the morphism $Z_{1/\overline{k}} \to Z_{2/\overline{k}}$. To check that the trace mapping (which is defined *a priori* on rational differential 1-forms) extends to regular and to Rosenlicht differentials, we may use the characterization of Rosenlicht differentials which is given in the above Remark, together with the local calculation

$$\sum_{s' \mapsto s} \mathrm{res}_{s'}(\omega) = \mathrm{res}_s(\mathrm{Trace}_{Z_1/Z_2}(\omega))$$

for ω any rational differential 1-form on $Z_{1/\overline{k}}$ and for s' ranging through all points of $Z_{1/\overline{k}}$ lying over a point s of $Z_{2/\overline{k}}$. (Compare: [35], Chapter II, n°12, Lemma 4; or [2] Chapter VIII (3.7) and (4.4).)

The definition of f^* and f_* on the homology of the graphs is as given in §3.

Proposition **13** *The above diagram (12) is commutative.*

Proof. Commutativity of the square(s) on the left is immediate. As for those on the right, it is a direct calculation, where in the case of commutativity involving f_* one uses the fact that $\mathrm{res}_s(f_*\omega) = f_*(\sum \mathrm{res}_{s'} \omega)$, where the summation is over all s' in Z_1 mapping to s in Z_2. □

7 Regular differentials on $X_{/\mathcal{O}}$

Let $X_{/\mathcal{O}}$ be admissible, and let $\tilde{X}_{/\mathcal{O}}$ be its canonical desingularization. The smooth loci $Y_{/\mathcal{O}}$ and $\tilde{Y}_{/\mathcal{O}}$ of the $\mathcal{O}$-schemes $X_{/\mathcal{O}}$ and $\tilde{X}_{/\mathcal{O}}$ are open subschemes consisting in the complements of the closed (finite) subschemes of ordinary double points in the special fibers of $X_{/\mathcal{O}}$ and $\tilde{X}_{/\mathcal{O}}$, respectively. Let $\Omega^1_{\tilde{Y}_{/\mathcal{O}}}$ denote the coherent sheaf of (relative) Kähler differentials on the smooth $\mathcal{O}$-scheme $\tilde{Y}_{/\mathcal{O}}$. Since $\tilde{X}$ is regular, the complement of $\tilde{Y}$ in $\tilde{X}$ consists in closed points of depth 2, and therefore the coherent sheaf $\Omega^1_{\tilde{Y}_{/\mathcal{O}}}$ has a unique extension (the direct image) to an invertible coherent sheaf on $\tilde{X}$, which we shall call $\Omega_{\tilde{X}_{/\mathcal{O}}}$.

Definition 5 Let $X_{/\mathcal{O}}$ be admissible. Let $\varphi\colon \tilde{X}_{/\mathcal{O}} \to X_{/\mathcal{O}}$ be the canonical desingularization. By the sheaf $\Omega_{X_{/\mathcal{O}}}$ we mean the direct image $\varphi_*\Omega_{\tilde{X}_{/\mathcal{O}}}$.

The sheaf $\Omega_{\tilde{X}_{/\mathcal{O}}}$ may be seen to be the relative dualizing sheaf of the $\mathcal{O}$-scheme $\tilde{X}$, and, as a consequence of this, together with the fact that $\varphi\colon \tilde{X} \to X$ consists in blowing up rational isolated singularities, one sees that $\Omega_{X_{/\mathcal{O}}}$ is an invertible $\mathcal{O}_X$-module, and is the relative dualizing sheaf of the $\mathcal{O}$-scheme X. Further, we have:

Lemma **2** *The natural mappings*

$$i : \Omega_{\tilde{X}_{/\mathcal{O}}} \to \varphi^*\Omega_{X_{/\mathcal{O}}}, \qquad j : \varphi_*\Omega_{\tilde{X}_{/\mathcal{O}}} \to \Omega_{X_{/\mathcal{O}}}$$

are isomorphisms. □

Remark. It would be good to have a concise and complete reference for Duality Theory tailored to admissible models and, in particular, to modular curves over rings of integers in number fields. Lacking such a reference, we suggest [10] and [20] II 3 for a discussion of these issues, and especially [15] Chapter IV §4 for a more complete discussion, with some proofs.

Next, if $f\colon X_{1/\mathcal{O}} \to X_{2/\mathcal{O}}$ is an admissible mapping, we have "direct" and "inverse" image mappings f_*, f^* connecting $\Omega^1_{\tilde{Y}_{1/\mathcal{O}}}$ and $\Omega^1_{\tilde{Y}_{2/\mathcal{O}}}$. These extend uniquely to $\Omega^1_{\tilde{X}_{1/\mathcal{O}}}$ and $\Omega^1_{\tilde{X}_{2/\mathcal{O}}}$, since the schemes $\tilde{X}_{i/\mathcal{O}}$ are regular and the subschemes $\tilde{Y}_{i/\mathcal{O}}$ are the complements in $\tilde{X}_{i/\mathcal{O}}$ of points of codimension 2. Using Lemma 2, one constructs "direct" and "inverse" image mappings f_* and f^* connecting $\Omega_{X_{1/\mathcal{O}}}$ and $\Omega_{X_{2/\mathcal{O}}}$.

Proposition **14** *(i) Let $X_{/\mathcal{O}}$ be admissible. There is a natural isomorphism of coherent sheaves over $X_{/k}$:*

$$\Omega_{X_{/\mathcal{O}}} \otimes k \approx \Omega_{X_{/k}}.$$

(ii) If $f\colon X_{1/\mathcal{O}} \to X_{2/\mathcal{O}}$ is an admissible mapping, then the direct and inverse image mappings f_*, f^* are compatible, in an evident sense, with the isomorphisms of (i) above for X_1 and X_2.

Proof. Part (i) is seen by local calculations where we distinguish the case of a neighborhood of a smooth point for the morphism f and that of a neighborhood of an ordinary double point of the fiber of f. Once (i) is established, (ii) follows easily. □

Now suppose that $X_{/\mathcal{O}}$ is admissible, and let $\mathrm{Cot}(A_{/\mathcal{O}})$ denote the cotangent space at the zero-section of the Néron model $A_{/\mathcal{O}}$. If $f\colon X_{1/\mathcal{O}} \to X_{2/\mathcal{O}}$ is an admissible mapping, let

$$f_*\colon\ \mathrm{Cot}(A_{1/\mathcal{O}}) \to \mathrm{Cot}(A_{2/\mathcal{O}})$$

be the mapping induced by $f^*\colon A_{2/\mathcal{O}} \to A_{1/\mathcal{O}}$, and define f^* on $\mathrm{Cot}(A_{2/\mathcal{O}})$ similarly.

Proposition **15** *There is a natural identification*

$$H^0(X, \Omega_{X_{/\mathcal{O}}}) \approx \mathrm{Cot}(A_{/\mathcal{O}})$$

which is compatible with f^* and f_* whenever $f\colon X_{1/\mathcal{O}} \to X_{2/\mathcal{O}}$ is an admissible mapping.

Proof. This is standard. See the discussion in [21] §2 (e). □

8 Admissible correspondences

Let $X_{i/\mathcal{O}}$ $(i = 0, 1, 2)$ be admissible, and let $X_1 \swarrow X_0 \searrow X_2$ be a diagram of admissible mappings $f_i\colon X_0 \to X_i$ $(i = 1, 2)$. Referring to such an *ordered* pair of admissible morphisms (f_1, f_2) by the single letter f, we call f an *admissible correspondence*. We think of f as a generalized admissible mapping

$X_1 \rightsquigarrow X_2$. Set $f_* := f_{2*}{f_1}^*$ and $f^* := f_{1*}{f_2}^*$, so that we have direct and inverse image mappings defined for the same panoply of instances that they have been defined, in the case of admissible mappings. If f is an admissible correspondence corresponding to the ordered pair (f_1, f_2), its *adjoint* is the admissible correspondence f' obtained by reversing the order, i.e., by using (f_2, f_1) in place of (f_1, f_2). Clearly, $f'_* = f^*$ and $f'^* = f_*$.

Let $X_{/\mathcal{O}}$ be admissible. A *commutative* subring

$$R \subset \mathrm{End}(A_{/K})$$

will be called *admissible* if it is generated by the direct and inverse image mappings f_* and g^* coming from admissible correspondences $\begin{array}{ccc} & X_0 & \\ \swarrow & & \searrow \\ X & & X \end{array}$ (with no *a priori* restriction on the admissible models $X_{0/\mathcal{O}}$ which may appear). By replacing correspondences by their adjoints, we may require in the definition that R be generated exclusively by inverse image or direct image mappings.

PROPOSITION **16** *For each $T \in R$, there are associated endomorphisms T_* and T^* on each of the following: $A_{/K}$, $A_{/\mathcal{O}}$, $A_{/k}$, $H^0(X, \Omega)$, $H^0(Z, \Omega^1)$, and $H_1(S, \overline{k})$. For fixed $T \in R$, the families of maps (T_*) and (T^*) are each compatible with the morphisms listed in Propositions 13–15.*

Proof. This is immediate from the statements of those Propositions. □

In the discussion which follows, we will be concerned principally with the maps (T_*). We use the phrase "covariant action" to suggest that T acts as T_* on a given object.

9 Local admissible data

For simplicity, we now suppose that $k = \mathbf{F}_p$. Let $X_{/\mathcal{O}}$ be an admissible model of its generic fiber X. We preserve much of the previous notation. Thus, for example, we let $Z_{/k}$ be the normalization of the special fiber $X_{/k}$ of $X_{/\mathcal{O}}$. In addition, we shall let Φ be the group of components of $A_{/k}$. We view Φ as a finite abelian group furnished with an action of $\mathrm{Gal}(\overline{k}/k)$ ([13], IX, §11).

Let R be a commutative subring of $\mathrm{End}(A_{/K})$ generated by admissible correspondences. Then R operates by functoriality on $A_{/k}$ and thereby (covariantly) on the component group Φ and the abelian variety $\mathrm{Pic}^o Z$. We let

$\overline{R}$ be the image of R in $\mathrm{End}(\mathrm{Pic}^o Z)$. We consider the *covariant* action of R on $H^0(X_{/k}, \Omega)$.

Suppose that $\mathfrak{p} \subset R$ is a maximal ideal of residual characteristic p. Let $F = R/\mathfrak{p}$ be the residue field of R. We say that the triple $\{X_{/\mathcal{O}}, R, \mathfrak{p}\}$ is *local admissible data* if the following axioms are satisfied:

I. The image of $\mathfrak{p}$ in $\overline{R}$ is the unit ideal of $\overline{R}$.

II. The F-vector space $H^0(X_{/k}, \Omega)[\mathfrak{p}]$ has dimension ≤ 1.

III. If $p = 2$, then $\mathfrak{p}$ does not belong to the support of the R-module Φ.

Remark. To anticipate the application of our theory, it might help if we dropped these hints: We will be working in the context where $K = \mathbf{Q}_p$, and X is a classical modular curve. Axiom I will follow since $\mathfrak{p}$ will correspond to a p-newform, and since Z "involves" only forms of lower p-level, $\mathfrak{p}$ can have no support in $H^0(Z, \Omega^1)$. Axiom II will follow from a version of the "q-expansion principle." Axiom III results from the fact that the component group Φ is known to be "Eisenstein" in the situation we encounter [31]. Hence a prime $\mathfrak{p}$ of R can belong to the support of Φ only if the associated Galois representation is reducible.

Proposition **17** *Let* $\{X_{/\mathcal{O}}, R, \mathfrak{p}\}$ *be local admissible data. Let* W *be the module introduced in the Corollary to Proposition 11. Then*

$$\dim_F W[\mathfrak{p}] \leq 1.$$

Proof. By the Corollary to Proposition 11, it is equivalent to prove that

$$\dim_F H_1(S(\overline{k}), \mathbf{F}_p)[\mathfrak{p}] \leq 1.$$

By the Corollary to Proposition 12, and by Axiom I, we have for each k' an isomorphism

$$H^0(X_{/k'}, \Omega)[\mathfrak{p}] \approx H_1(S(\overline{k}), \overline{k})^{\mathrm{Gal}(\overline{k}/k')}[\mathfrak{p}].$$

Consider this isomorphism in the case where $k' = k = \mathbf{F}_p$, and let $G = \mathrm{Gal}(\overline{k}/\mathbf{F}_p)$. The proposition follows from the following lemma, in which we have put $Y := H_1(S(\overline{k}), \mathbf{F}_p)$.

Lemma **3** *We have* $\dim_F Y[\mathfrak{p}] = \dim_F (Y \otimes_{\mathbf{F}_p} \overline{k})^G[\mathfrak{p}]$.

Proof. One first shows that the natural inclusion

$$Y[\mathfrak{p}] \otimes_{\mathbf{F}_p} \overline{k} \subset (Y \otimes_{\mathbf{F}_p} \overline{k})[\mathfrak{p}]$$

is an isomorphism (e.g., by proving this with $\overline{k}$ replaced by any finite subfield k', via a dimension count over $\mathbf{F}_p$, and then passing to $\overline{k}$ by direct limit). Since passage to the submodule of G-invariants commutes with passage to the kernel of $\mathfrak{p}$, we get that the natural inclusion

$$(Y[\mathfrak{p}] \otimes_{\mathbf{F}_p} \overline{k})^G \subset (Y \otimes_{\mathbf{F}_p} \overline{k})^G[\mathfrak{p}]$$

is also an isomorphism. This reduces us to the case where $Y = Y[\mathfrak{p}]$. In this case, the equality to be proved,

$$\dim_{\mathbf{F}_p} Y = \dim_{\mathbf{F}_p} (Y \otimes_{\mathbf{F}_p} \overline{k})^G,$$

is evident. □

10 Global admissible data

We now let $X_{/\mathbf{Q}}$ be a smooth projective curve over $\mathbf{Q}$, and denote by $A_{/\mathbf{Z}}$ the Néron model of its Jacobian over the base $\mathbf{Z}$. Let R be a subring of endomorphisms of $A_{/\mathbf{Q}}$ defined over $\mathbf{Q}$ (equivalently, a subring of $\mathrm{End}(A_{/\mathbf{Z}})$). Let $\mathfrak{p} \subset R$ be a maximal ideal of residual characteristic p. Let F be the residue field of $\mathfrak{p}$, as in §8. Let $X_{/\mathbf{Q}_p}$ denote the base extension of $X_{/\mathbf{Q}}$ to $\mathbf{Q}_p$. Let $\mathcal{O} = \mathbf{Z}_p$ and let $X_{/\mathcal{O}}$ be an admissible model of $X_{/\mathbf{Q}_p}$ over the base $\mathbf{Z}_p$. We shall say that $\{X_{/\mathbf{Q}}, X_{/\mathcal{O}}, R, \mathfrak{p}\}$ is *globally admissible data* if:

(a) It is *locally admissible*; i.e., $\{X_{/\mathcal{O}}, R, \mathfrak{p}\}$ is locally admissible in the sense of §9, and,

(b) The $F[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module $A_{/\mathbf{Q}}[\mathfrak{p}](\overline{\mathbf{Q}})$ has a Jordan-Hölder filtration all of whose successive quotients are isomorphic to one absolutely irreducible $F[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module V for which $\dim_F V = 2$.

Proposition **18 ("dimension two")** *Assume that*

$$\{X_{/\mathbf{Q}}, X_{/\mathcal{O}}, R, \mathfrak{p}\}$$

is globally admissible. Then $A_{/\mathbf{Q}}[\mathfrak{p}](\overline{\mathbf{Q}})$ is an F-vector space of dimension two.

Proof. Let U denote the $F[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module $A_{/\mathbf{Q}}[\mathfrak{p}](\overline{\mathbf{Q}})$. Then U is non-zero because R acts faithfully on A. By property (b) above, all minimal $F[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-submodules of U are isomorphic to V. Choose one such submodule, and identify it with V; this gives us an inclusion $V \subset U$.

Let $\dim_F U = 2N$, so that U possesses an $F[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-stable Jordan-Hölder filtration of N stages, each of whose "successive quotients" is isomorphic, as $F[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module, to V. We must prove that $N = 1$.

Fix an embedding $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$; use it to identify $U = A_{/\mathbf{Q}}[\mathfrak{p}](\overline{\mathbf{Q}})$ with $A_{/\mathbf{Q}_p}[\mathfrak{p}](\overline{\mathbf{Q}}_p)$. Via this identification, U and its submodule V inherit filtrations (as $F[\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)]$-modules) from the filtration (8), made with $n = 1$:

$$\begin{array}{ccccccc} 0 & \subset & U^{\mathrm{t}} & \subset & U^{\mathrm{f}} & \subset & U, \\ 0 & \subset & V^{\mathrm{t}} & \subset & V^{\mathrm{f}} & \subset & V. \end{array}$$

Axiom I of §9 (coupled with Propositions 9 and 11) proves that $U^{\mathrm{t}} = U^{\mathrm{f}}$ and therefore that $V^{\mathrm{t}} = V^{\mathrm{f}}$. Further, since $U/U^{\mathrm{t}} = U/U^{\mathrm{f}}$ embeds in the module $W[\mathfrak{p}]$ of the previous §, and since, by Proposition 17, $W[\mathfrak{p}]$ is of F-dimension ≤ 1, the codimension c of U^{t} in U is at most 1.

The inertia subgroup I of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ acts trivially on U/U^{t} and as the mod p cyclotomic character χ on U^{t}. Hence the semisimplification of U as an I-module is the sum of c copies of the trivial representation and $2N - c$ copies of the 1-dimensional representation corresponding to χ. Meanwhile, this semisimplification is the sum of N copies of the semisimplification of V.

Assume now that p is an odd prime. Then χ is non-trivial, and we see that either $N = 1$ or else $U = U^{\mathrm{t}}$. We will eliminate the latter possibility, using the assumption that p is odd.

For this, we note first that the entire p-divisible group $A_p(\overline{\mathbf{Q}}) \otimes_R R_{\mathfrak{p}} = \bigcup A[\mathfrak{p}^i](\overline{\mathbf{Q}}_p)$ lies in the toric part A_p^{t} of the p-divisible group of A. Indeed, suppose that $A[\mathfrak{p}^i]$ lies in $A_p[p^n]$. Then, by Axiom I, to say that $A[\mathfrak{p}^i]$ is contained in $A_p^{\mathrm{t}}[p^n]$ is to say that it is contained in $A_p^{\mathrm{f}}[p^n]$. If not, then $A[\mathfrak{p}^i]$ maps non-trivially to $A_p[p^n]/A_p^{\mathrm{f}}[p^n]$, which is unramified, whereas the assumption $U = U^{\mathrm{t}}$ implies easily that $A[\mathfrak{p}^i]$ has no unramified quotient. (One uses the standard fact that $A[\mathfrak{p}^i]/A[\mathfrak{p}^{i-1}]$ maps injectively to a direct sum of copies of U, cf. [20], II, §14.)

We then conclude by using an argument due to Serre (compare [24], Chap. III §7). Let Γ be the $\mathbf{Q}_p$-adic Tate module associated to $A_p(\overline{\mathbf{Q}}) \otimes_R R_{\mathfrak{p}}$, and let Λ denote its h^{th} exterior power where h is the dimension of Γ. Let $\Lambda(-h)$ be the twist of Λ by the $-h$th power of the p-adic cyclotomic character of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Then $\Lambda(-h)$ is unramified at p, so that $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on $\Lambda(-h)$ via a character of finite order. Hence the eigenvalues of Frobenius elements φ_ℓ on Λ (where $\ell \neq p$ is any prime of good reduction for A) are of the form $\ell^h\zeta$, where ζ is a root of unity. These eigenvalues thus have archimedean absolute values ℓ^h. However, the eigenvalues of φ_ℓ on Γ all have absolute values $\ell^{1/2}$, which is a contradiction.

We now consider the case $p = 2$. Then, by Axiom III, the maximal ideal $\mathfrak{p}$ does not belong to the support of Φ. Using this information, but making no further use of the assumption $p = 2$, we shall establish that U^{t} has dimension ≤ 1. Since its codimension is also bounded from above by 1, we get that U has dimension at most 2, so that $N = 1$ as desired.

Let $\mathcal{X}$ denote temporarily the character group $\mathrm{Hom}_{\overline{\mathbf{F}}_p}(A^{\mathrm{t}}_{/k}, \mathbf{G}_{\mathsf{m}})$ of the maximal torus in the reduction of A. Then $U^{\mathrm{t}} = \mathrm{Hom}(\mathcal{X}/\mathfrak{p}\mathcal{X}, \mu_p(\overline{\mathbf{Q}}_p))$. Hence the F-dimension of U^{t} is that of $\mathcal{X}/\mathfrak{p}\mathcal{X}$. If $\mathcal{Y}$ is the analogue of $\mathcal{X}$ for the reduction of the dual of A (so that $\mathcal{Y}$ and $\mathcal{X}$ are in fact isomorphic), then the monodromy pairing of SGA7I furnishes an exact sequence

$$0 \to \mathcal{Y} \to \mathrm{Hom}(\mathcal{X}, \mathbf{Z}) \to \Phi \to 0.$$

By considering the maps "multiplication by p" on the groups in this sequence, and by using the Snake Lemma, we find a 4-term exact sequence

$$0 \to \Phi[p] \to W \to \mathrm{Hom}(\mathcal{X}/p\mathcal{X}, \mathbf{F}_p) \to \Phi/p\Phi \to 0,$$

since W is canonically $\mathcal{Y}/p\mathcal{Y}$. If we localize at $\mathfrak{p}$, the two terms involving Φ disappear, because of Axiom III. Hence, localizing and then performing the operation "$[\mathfrak{p}]$" gives an isomorphism

$$W[\mathfrak{p}] \approx \mathrm{Hom}(\mathcal{X}/\mathfrak{p}\mathcal{X}, \mathbf{F}_p).$$

In view of Proposition 17, the dimension of the right-hand side is ≤ 1, as claimed. $\square$

11 Modular curves and Hecke operators

Let N be an integer prime to p, and let $M = pN$. Let X be the complete modular curve $X_o(M)_{/\mathbf{Q}}$, which is associated with the subgroup $\Gamma_o(M)$ of $\mathbf{PSL}(2, \mathbf{Z})$. We will be working with this curve and its canonical model over $\mathbf{Z}[1/N]$. As we intimated in the Introduction, however, one could work equally well with the curve $X(N, p)$ attached to the subgroup $\Gamma_1(N) \cap \Gamma_o(p)$ of $\Gamma_o(pN)$. This subgroup is defined by matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ which satisfy the additional congruence $a \equiv d \equiv 1 \pmod{N}$. These two cases could be treated simultaneously by the introduction of a curve which lies between $X(N,p)$ and X in the natural covering $X(N,p) \to X$.

As we recalled in our introductory comments, the curve X is furnished with a standard Hecke correspondence T_n for each integer $n \geq 1$; the correspondence T_ℓ is frequently called U_ℓ when ℓ is a prime number dividing pN. The correspondences T_n induce endomorphisms of the Jacobian $J_o(pN) = \mathrm{Pic}^o(X)$ of X, which are again denoted T_n. (We use the convention which was explained in §3 of [30]. Thus, the endomorphism T_n is the transpose of the endomorphism ξ_n which is defined in Chapter 7 of [41].) Let $w = w_p$ be the Atkin-Lehner involution of X relative to the prime p, and write again w for the involution of $J_o(pN)$ induced by this operator.

Also, recall [21] that there are two *degeneracy maps*

$$\alpha = \delta_1, \beta = \delta_p : X \rightrightarrows X_o(N).$$

These correspond respectively to the modular operations

$$(E, C_N, C_p) \mapsto (E, C_N), \quad (E, C_N, C_p) \mapsto (E/C_p, (C_N + C_p)/C_p),$$

where C_N and C_p denote cyclic subgroups of orders N and p on an elliptic curve E. These degeneracy maps induce maps $\alpha_*, \beta_* : J_o(pN) \rightrightarrows J_o(N)$ and $\alpha^*, \beta^* : J_o(N) \rightrightarrows J_o(pN)$. The maps α^* and β^* each identify $J_o(N)$ with an abelian subvariety of $J_o(pN)$.

Consider now the following three closely related commutative subrings of $\mathrm{End}(J_o(pN))$:

- $S =$ the subring generated by the T_n with n prime to p,
- $\mathbf{T} = \mathbf{T}_{pN} =$ the subring generated by the T_n for all n,
- $R =$ the ring generated by S and w.

We have $\mathbf{T} = S[T_p] = S[U_p]$ and $R = S[w]$. All three rings are finitely generated as $\mathbf{Z}$-modules, since $\mathrm{End}(J_o(pN))$ is of finite rank over $\mathbf{Z}$.

We say that maximal ideals $\mathfrak{p} \subset R$ and $\mathfrak{m} \subset \mathbf{T}$ are *compatible* if their intersections with S coincide. By the "going-up" theorem of Cohen-Seidenberg, there is always at least one maximal ideal $\mathfrak{m}$ or $\mathfrak{p}$ compatible with a given $\mathfrak{p}$ or $\mathfrak{m}$.

Next, let $\overline{S}$ be the "p-old quotient" of S, defined (for instance) as the quotient of S cut out by $J_o(N)$, viewed as an abelian subvariety of $J_o(pN)$.

In other words, we identify $J_o(N)$ with its image in $J_o(pN)$ under α^*, and observe that this image is stable under T_n for all n prime to p. The subring of $\mathrm{End}(J_o(N))$ generated by these T_n is then the quotient $\overline{S}$ of S. (Alternatively, $\overline{S}$ may be defined as the image of S in $\overline{R}$, where $\overline{R}$ is defined as in §9, cf. [30], 3.11.) Note that $\overline{S}$ is a subring of the Hecke algebra $\mathbf{T}_N$, which is the subring of $\mathrm{End}(J_o(N))$ generated by *all* the Hecke operators T_n at level N. Thus $\mathbf{T}_N$ is the ring generated by $\overline{S}$ and the Hecke operator T_p at level N.

We call a maximal ideal $\mathfrak{m}_o$ of S *strongly p-new*, or simply *strongly new*, if it is not the inverse image in S of a maximal ideal of $\overline{S}$. Thus, "strongly p-new" means "not p-old." A maximal ideal $\mathfrak{m} \subset \mathbf{T}$ or $\mathfrak{p} \subset R$ is defined to be strongly (p-)new if its intersection with S is strongly new.

PROPOSITION **19** *Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}_{pN}$. Assume that $\rho_\mathfrak{m}$ is an irreducible representation which is not modular of level N. Then $\mathfrak{m}$ is strongly p-new.*

Proof. Let $\mathfrak{m}_o = \mathfrak{m} \cap S$. Assume that $\mathfrak{m}$ is not strongly p-new, so that $\mathfrak{m}_o$ is the inverse image of a maximal ideal I of $\overline{S}$. The residue field of I is then the quotient $S/\mathfrak{m}_o$, which is a subfield of $\mathbf{T}_{pN}/\mathfrak{m}$. Let J be a maximal ideal of $\mathbf{T}_N$ lying over I, and consider the representation ρ_J. For almost all prime numbers r, we have

$$\begin{aligned} \mathrm{trace}(\rho_m(\sigma_r)) &= T_r \bmod \mathfrak{m}_o = \mathrm{trace}(\rho_J(\sigma_r)), \\ \det(\rho_\mathfrak{m}(\sigma_r)) &= r \bmod \mathfrak{m} = \det(\rho_J(\sigma_r)), \end{aligned}$$

the equalities holding in the common subfield $S/\mathfrak{m}_o$ of $\mathbf{T}_{pN}/\mathfrak{m}$ and $\mathbf{T}_N/J$. (Here, σ_r is a Frobenius element for r in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.) By the Cebotarev density theorem, the representations $\rho_\mathfrak{m}$ and ρ_J are isomorphic in the sense that they both arise by base change from the same two-dimensional representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $S/\mathfrak{m}_o$. This contradicts the assumption that $\rho_\mathfrak{m}$ is not modular of level N. □

PROPOSITION **20** *Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}$ which is strongly p-new. Then R acts on $J_o(pN)[\mathfrak{m}](\overline{\mathbf{Q}})$ via a surjective homomorphism $R \to \mathbf{T}/\mathfrak{m}$.*

Proof. The endomorphism T_p+w of $J_o(pN)$ maps $J_o(pN)$ into the subvariety $\alpha^*(J_o(N))$ of $J_o(pN)$ (cf. [30], proof of Proposition 3.7). In particular, T_p+w maps $J_o(pN)[\mathfrak{m}]$ into $J_o(N) \cap J_o(pN)[\mathfrak{m}_o]$, where $\mathfrak{m}_o$ is the intersection $S \cap \mathfrak{m}$. The group $J_o(N) \cap J_o(pN)[\mathfrak{m}_o]$ is killed by the image of $\mathfrak{m}_o$ in $\overline{S}$, which is the unit ideal of $\overline{S}$ by hypothesis. Hence $J_o(N) \cap J_o(pN)[\mathfrak{m}_o] = 0$, so that $T_p = -w$ on $J_o(pN)[\mathfrak{m}]$. All generators of R now act on $J_o(pN)[\mathfrak{m}]$ as elements of $\mathbf{T}$, since $T_\ell \in R$ acts as $T_\ell \in \mathbf{T}$, for $\ell \neq p$. The result now follows; in particular, the action of R on $J_o(pN)[\mathfrak{m}](\overline{\mathbf{Q}})$ is given by a *surjective* homomorphism because each generator of $\mathbf{T}/\mathfrak{m}$ is, up to sign, the image of a generator of R. □

Corollary *Assume that* $\mathfrak{m}$ *is strongly* p*-new. Then we have*

$$J_o(pN)[\mathfrak{m}](\overline{\mathbf{Q}}) \subseteq J_o(pN)[\mathfrak{p}](\overline{\mathbf{Q}}),$$

for some maximal ideal $\mathfrak{p}$ *of* R *which is compatible with* $\mathfrak{m}$ *and whose residue field is isomorphic to that of* $\mathfrak{m}$. □

12 Admissible data coming from modular curves

We continue the discussion of §11, retaining the notation. In addition, we let $X_{/\mathbf{Z}[1/N]}$ denote the canonical model of the modular curve $X = X_{/\mathbf{Q}}$, as in [10], [14], or [24]. Let $\mathcal{O} = \mathbf{Z}_p$, and let $X_{/\mathcal{O}}$ denote the base change of $X_{/\mathbf{Z}[1/N]}$ to $\mathcal{O}$.

Proposition **21** *The model* $X_{/\mathcal{O}}$ *is admissible, and the ring* R *is an admissible subring of* $\mathrm{End}(J_o(pN))$.

Proof. That $X_{/\mathcal{O}}$ is an admissible model follows from the discussion of Example 1 of § 2. The scheme-theoretic definitions given in ([24], Chapter 2, §5) of the correspondences defining the T_ℓ (for ℓ not dividing pN) and the U_ℓ (for ℓ dividing N) show that these correspondences are determined by diagrams

$$\begin{array}{ccc} & X'_{/\mathcal{O}} & \\ \swarrow & & \searrow \\ X_{/\mathcal{O}} & & X_{/\mathcal{O}} \end{array}$$

where the oblique arrows are morphisms of the type given in Proposition 6. It follows from that Proposition that the correspondences T_ℓ (for ℓ not dividing pN) and U_ℓ (for ℓ dividing N) are admissible. The map w_p, in the other hand, extends to an automorphism of $X_{/\mathcal{O}}$, so its admissibility again follows from Proposition 6. □

The scheme-theoretic definition of the correspondence U_p (as in [24], Chapter 2, §5) does not exhibit U_p as an admissible correspondence. However, U_p behaves as the negative of w on the representation spaces which interest us, cf. Proposition 20 and its corollary. Thus, U_p is "morally" an element of the ring R.

Now let $\mathfrak{p} \subset R$ be a maximal ideal whose residue field F is of characteristic p. As we recalled in the Introduction (in discussing maximal ideals of $\mathbf{T}$), one can attach to $\mathfrak{p}$ a two-dimensional semi-simple Galois representation

$$\rho_{\mathfrak{p}} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, F).$$

This representation is unramified at primes not dividing pN and enjoys the following property: Let ℓ be a prime number not dividing pN, and let $\varphi_\ell \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ be a Frobenius element for the prime ℓ. Then the characteristic polynomial of $\rho_{\mathfrak{p}}(\varphi_\ell)$ is $X^2 - a_\ell X + \ell$, where a_ℓ is the image in $F = R/\mathfrak{p}$ of the Hecke operator $T_\ell \in R$. This representation visibly depends only on the intersection $\mathfrak{p} \cap S$; it coincides with $\rho_{\mathfrak{m}}$ for any $\mathfrak{m} \subset \mathbf{T}$ which is compatible with $\mathfrak{p}$.

We say that $\mathfrak{p}$ is *of absolutely irreducible type* if the associated representation $\rho_{\mathfrak{p}}$ is absolutely irreducible. By working with a complex conjugation in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, one sees when $p > 2$ that $\rho_{\mathfrak{p}}$ is absolutely irreducible if and only if it is irreducible over F.

PROPOSITION **22** *Let p be a prime number and N an integer not divisible by p. Let $X_{/\mathbf{Q}}$, $X_{/\mathcal{O}}$, and R be as above. Let $\mathfrak{p}$ be a maximal ideal in R of residual characteristic p, which is strongly p-new of absolutely irreducible type. Then $\{X_{/\mathbf{Q}}, X_{/\mathcal{O}}, R, \mathfrak{p}\}$ is globally admissible.*

Proof. Since $\mathfrak{p}$ is strongly p-new one sees immediately that Axiom I (in the definition of "local admissible data," §9) holds for $\{X_{/\mathcal{O}}, R, \mathfrak{p}\}$. Indeed, R acts on $H^0(Z, \Omega^1)$ through its quotient $\overline{R}$.

To establish Axiom II, we shall make use of "q-expansion principle" techniques, very similar to those used in ([24], Chap. 2 §10). The work of Deligne-Rapoport [10] implies that $X_{/k}$ is as depicted on page 177 of [20]. In particular, two components of $X_{/\overline{k}}$ are copies of the modular curve $X_o(N)$; we shall refer to these below as the "good components." The remaining components, if any, are projective lines arising from supersingular points of $X_o(N)_{/\overline{k}}$ (which are represented by elliptic curves plus subgroups of order N) with "extra automorphisms." We refer to these components as the "possible $\mathbf{P}^1$'s."

To prove Axiom II, we must bound the dimension of the F-vector space $H^0(X_{/k}, \Omega)[\mathfrak{p}]$. Let k' be a subfield of $\overline{k}$. A Rosenlicht differential ω in the $k' \otimes_k F$-module $H^0(X_{/k'}, \Omega)[\mathfrak{p}]$ is uniquely determined by its restriction to the good component containing the cusp ∞. Indeed, the restriction of ω to the good component containing ∞ determines it on the other good component as well (the action of w_p permutes the two good components and takes ω to ω times the image of w_p in F). Further, its restriction to the "possible $\mathbf{P}^1$'s" is also determined since we know its residues by virtue of the fact that ω is a Rosenlicht differential. Thus ω is entirely determined by its q-expansion at the cusp ∞, since it is standard that this q-expansion determines ω on the good component containing ∞.

Let F' be a finite field extension of F, and suppose that we are given a Rosenlicht differential ω on $X_{/k}$ with the property that when viewed as Rosenlicht differential over F', it is an eigenvector for the operators in R. Say that λ_n is the eigenvalue of T_n acting on ω (for each integer n prime to p) and that $-\lambda_p = \pm 1$ is the eigenvalue of w_p acting on ω. We need to show that ω is determined by its eigenvalues up to multiplication by a scalar in F'. (Cf. Propositions 9.2 and 9.3 of [20], Chapter II.)

Consider the q-expansion $f = a_1 q^1 + a_2 q^2 + \ldots$ of ω. We will show that all a_n are determined by a_1 and the λ's. A familiar argument (cf. [24] Chap. 2 §10) proves that the coefficients a_n for n prime to p are determined by a_1. Indeed, since the coefficient of q in the expansion of $\omega | T_n$ is a_n, we have $a_n = \lambda_n a_1$ for each n prime to p. To control the coefficients a_n with n divisible by p, we shall establish the complementary formula $a_{np} = \lambda_p a_n$ for $n \geq 1$.

Consider the Cartier operator $\mathcal{C}$ ([34], §10) on the space $H^0(X_o(N)_{/\overline{k}}, \Omega^1)$. (Compare the discussion in [24] Chap. 2 §10.) Think of $X_o(N)$ as the good component containing ∞, and write simply ω for the restriction of ω to this component. Let σ denote the Frobenius automorphism of $\overline{k}$. The differential $\sigma(\mathcal{C}\omega)$ has q-expansion $\sum_n a_{np} q^n$, and it will suffice to show that $\sigma(\mathcal{C}\omega)$ is the negative of the restriction to $X_o(N)$ of $w_p \omega$.

At each supersingular point $\mathbf{s}$ of $X_o(N)_{/\overline{k}}$, the residue of $w_p \omega$ is $-\operatorname{res}_{\mathbf{s}^{(p)}} \omega$, since w_p permutes the two good components and induces the Frobenius map ${}^{(p)}$ (an involution) on the set of singular points of $X_{/\overline{k}}$. On the other hand, we have the formula

$$\sigma(\operatorname{res}_{\mathbf{s}}(\mathcal{C}\omega)) = \operatorname{res}_{\mathbf{s}^{(p)}} \sigma(\mathcal{C}\omega),$$

cf. (10). The left-hand side of this equation, however, represents the residue at $\mathbf{s}$ of ω, in view of equation (33) of [34]. [The exponent ${}^{(p)}$ was incorrectly placed on the left-hand side of this latter equation in the initial printing of [34]. The equation was reprinted correctly, with the exponent on the right-hand side, in Serre's *Œuvres*.] Hence $w_p \omega + \sigma(\mathcal{C}\omega)$ is a differential of the first kind on $X_o(N)_{/\overline{k}}$. However, it is clear that this differential is annihilated by the intersection $\mathfrak{m}_o$ of $\mathfrak{m}$ and the subring S of R. By the definition of "strongly p-new," we see that $w_p\omega + \sigma(\mathcal{C}\omega) = 0$.

We now come to Axiom III. This follows from Theorem 2 of [31], which proves that the component group Φ is "Eisenstein." Indeed, if the mod p Galois representation associated with a prime $\mathfrak{p}$ is irreducible, $\mathfrak{p}$ cannot intervene in the support of a module which is Eisenstein (cf. [30], Th. 5.2c). (It is perhaps worth pointing out that no information about the residue characteristic of $\mathfrak{p}$ is used.)

We have therefore established that $\{X_{/\mathcal{O}}, R, \mathfrak{p}\}$ is locally admissible. To see that $\{X_{/\mathbf{Q}}, X_{/\mathcal{O}}, R, \mathfrak{p}\}$ constitutes global admissible data we need only check condition (b) of §10. This follows from the argument in the proof of Proposition 14.2 of [20]. To give the bearest hint: the Eichler-Shimura relations, and the Cebotarev Density Theorem guarantee that the characteristic polynomials of the action of elements of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on the F-vector space $J_o(pN)_{/\mathbf{Q}}[\mathfrak{p}]$ are the same as on a direct sum of a number of copies of V. The Brauer-Nesbitt theorem then provides the existence of an $F[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-Jordan-Hölder filtration whose successive quotients are isomorphic to V. [Alternatively, we could now apply the main theorem of [6], which guarantees that $J_o(pN)_{/\mathbf{Q}}[\mathfrak{p}]$ is a *direct sum* of copies of V.] □

We now can prove the Main Theorem which appears in the Introduction. We repeat it here as

THEOREM **1** *Let p be a prime number and N an integer not divisible by p. Let $\mathfrak{m}$ be a maximal ideal in $\mathbf{T}_{pN}$ of residue characteristic p, which is of absolutely irreducible type and such that $\rho_\mathfrak{m}$ is not modular of level N. Then $J_o(pN)(\overline{\mathbf{Q}})[\mathfrak{m}]$ is a vector space of dimension two over $\mathbf{T}_{pN}/\mathfrak{m}$, and the representation $\rho_\mathfrak{m}$ is equivalent to the natural representation of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *on $J_o(pN)(\overline{\mathbf{Q}})[\mathfrak{m}]$.*

Proof. Let $\mathfrak{p}$ be chosen as in the Corollary to Proposition 20. By that Corollary, it suffices to prove that $J_o(pN)(\overline{\mathbf{Q}})[\mathfrak{p}]$ is of dimension two. This result follows from Proposition 18, in view of Propositions 21, 19, and 22. □

13 Higher multiplicities

In this §, we construct kernels $J_o(M)[\mathfrak{m}]$ with multiplicities $\mu_\mathfrak{m} > 1$. In our examples, M is divisible by p^3, and the representation $\rho_\mathfrak{m}$ is modular of level M/p^2.

Let p be a prime number, and let N be a positive integer prime to p. For each ν, let $\alpha_\nu : X_o(p^{\nu+1}N) \to X_o(p^\nu N)$ be the degeneracy covering with the modular interpretation $(E, C) \mapsto (E, C[p^\nu N])$, where C denotes a cyclic subgroup of order $p^{\nu+1}N$ in an elliptic curve E. Let β_ν be the "other" degeneracy covering $X_o(p^{\nu+1}N) \to X_o(p^\nu N)$; it has the modular interpretation $(E, C) \mapsto (E/C[p], C/C[p])$. The degeneracy coverings α_ν, β_ν have degree p if $\nu \geq 1$, and degree $p+1$ when $\nu = 0$. (In §11, we introduced the degeneracy coverings $\alpha = \alpha_0$ and $\beta = \beta_0$.) They induce maps

$$\alpha_{\nu *}, \beta_{\nu *} : J_o(p^{\nu+1}N) \rightrightarrows J_o(p^\nu N), \qquad \alpha_\nu^*, \beta_\nu^* : J_o(p^\nu N) \rightrightarrows J_o(p^{\nu+1}N)$$

via the two functorialities of the Jacobian. Since neither covering α_ν, β_ν factors through a non-trivial unramified abelian covering $Z \to X_o(p^\nu N)$, the maps α_ν^* and β_ν^* are injective. Correspondingly, their duals $\alpha_{\nu *}$ and $\beta_{\nu *}$ are surjective, with connected kernels.

Let α_ν' and β_ν' denote the transposes of α_ν and β_ν, viewed as correspondences. (We regard α_ν' and β_ν' as generalized maps $X_o(p^\nu N) \rightsquigarrow X_o(p^{\nu+1}N)$.) We have the formulas $\alpha_{\nu *}' = \alpha_\nu^*$, and $\beta_{\nu *}' = \beta_\nu^*$. The Hecke correspondence T_p on $X_o(p^\nu N)$ is defined as the composition $\alpha_\nu \circ \beta_\nu'$. Accordingly, we have the formula $T_p' = \beta_\nu \circ \alpha_\nu'$ for the transpose of T_p. One may check that this Hecke correspondence has the familiar modular description

$$(E, C) \mapsto \sum_D (E/D, (C \oplus D)/D),$$

in which the sum runs over subgroups of E having order p whose intersection with C is trivial. From this description, we obtain for $\nu \geq 1$ the formulas

$$\alpha_\nu \circ T_p = T_p \circ \alpha_\nu, \qquad \beta_\nu \circ T_p = p \cdot \alpha_\nu.$$

The Hecke operator T_p on the left-hand side of each equation is a self correspondence of $X_o(p^{\nu+1}N)$, whereas the T_p on the right-hand side of the first equation is a self-correspondence of $X_o(p^\nu N)$. Finally, consider the Hecke operator T_p and the Atkin-Lehner involution w_p on the modular curve $X_o(pN)$. As we recalled above in our proof of Proposition 20, the sum $T_p + w_p$ is the correspondence $\beta_0' \circ \alpha_0$ of degree $p+1$ (cf. [30], Prop. 3.7).

Fix $\nu \geq 1$. For each $n \geq 1$, write, as usual, T_n for the n^{th} Hecke operator on $J_o(p^\nu N)$, i.e., the pullback to $J_o(p^\nu N) = \mathrm{Pic}^o(X_o(p^\nu N))$ of the Hecke correspondence T_n on $X_o(p^\nu N)$. Similarly, write w_p for the involution of $J_o(p^\nu N)$ induced by the Atkin-Lehner involution of $X_o(p^\nu N)$. Also, write $T_n^\vee$ for the "dual" of T_n, i.e., the pullback of T_n' to $J_o(p^\nu N)$.

Take $\nu = 1$, and let $\mathfrak{m} \subset \mathbf{T}_{pN}$ be a maximal ideal of residue characteristic p for which the associated representation $\rho_{\mathfrak{m}}$ of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is: (1) absolutely irreducible and, (2) not modular of level $N = M/p$. Let $V = J_o(pN)[\mathfrak{m}]$, which is *a priori* a successive extension of some number $\mu_{\mathfrak{m}} \geq 1$ of copies of $\rho_{\mathfrak{m}}$. Our main theorem states that the multiplicity $\mu_{\mathfrak{m}}$ of $\rho_{\mathfrak{m}}$ in V is 1; however, we shall *not* make use of this fact. Since $\rho_{\mathfrak{m}}$ is not modular of level N, we have $\alpha_{0*}(V) = \beta_{0*}(V) = 0$. Because of the formula $T_p + w_p = \alpha_0^* \circ \beta_{0*}$, w_p is the scalar $-T_p$ on V. Similarly, $w_p = -T_p^\vee$ on V. We deduce, first, that $T_p = \pm 1$ on V, and secondly that $T_p^\vee = T_p$ on V. Therefore, $T_p T_p^\vee = T_p^\vee T_p = 1$ on V.

Let $\gamma : J_o(pN)^2 \to J_o(p^2N)$ be the composition of the product $\alpha_1^* \times \beta_1^*$ and the "sum" map on $J_o(p^2N)$. Thus, symbolically,

$$\gamma(x, y) = \alpha_1^*(x) + \beta_1^*(y).$$

Lemma 4 *The map $\beta_2^* \circ \gamma : J_o(pN)^2 \to J_o(p^3N)$ induces an injection*

$$V \times V \hookrightarrow J_o(p^3N).$$

Proof. Let $\delta : J_o(p^2N) \to J_o(pN)^2$ be the map given by the symbolic formula $t \mapsto (\alpha_{1*}(t), \beta_{1*}(t))$. The composition $\delta \circ \gamma$ is the endomorphism of $J_o(pN)^2$ represented by the matrix $\begin{pmatrix} p & T_p \\ T_p^\vee & p \end{pmatrix}$ (or its transpose, depending on conventions). The restriction of this composition to $V \times V$ is thus the automorphism $\begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix}$ of $V \times V$. Accordingly, the restriction of γ to $V \times V$ is injective. The lemma now follows, since $\beta_2^* : J_o(p^2N) \to J_o(p^3N)$ is injective. $\square$

The Hecke ring $\mathbf{T}_{pN}$ acts on V via a tautological character $\mathbf{T}_{pN} \to k$, where k is the residue field of $\mathfrak{m}$. For each $n \geq 1$, let a_n be the image of T_n under this character, i.e., $T_n \bmod \mathfrak{m}$. Let W denote the image of $V \times V$ in $J_o(p^3N)$ under $\beta_2^* \circ \gamma$. For all $n \geq 1$ with $(n, p) = 1$, the Hecke operator $T_n \in \mathbf{T}_{p^3N}$ acts on W by the homothety a_n. In view of the formula $T_p \circ \beta_2^* = p\alpha_2^*$, and the fact that $p = 0$ on W, we see that $T_n = 0$ on W for all n divisible by p. Thus the action of $\mathbf{T}_{p^3N}$ on W is given by the homomorphism $\varphi : \mathbf{T}_{p^3N} \to k$ which is determined by:

$$\varphi(T_n) = \begin{cases} a_n & \text{for } (n, p) = 1, \\ 0 & \text{for } n \text{ divisible by } p. \end{cases}$$

This homomorphism is in fact surjective, since $a_p = \pm 1$.

Let $\mathcal{M}$ be the kernel of φ. Then φ identifies the residue field of $\mathcal{M}$ with the residue field k of $\mathfrak{m}$. Moreover, the k-representations $\rho_{\mathfrak{m}}$ and $\rho_{\mathcal{M}}$ of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ are isomorphic, by the Cebotarev Density Theorem. Now $W \subseteq J_o(p^3N)[\mathcal{M}]$, and the dimension of W over $k = \mathbf{T}_{p^3N}/\mathcal{M}$ is $2\mu_{\mathfrak{m}}$. Hence the multiplicity $\mu_{\mathcal{M}}$ of $\rho_{\mathcal{M}}$ in $J_o(p^3N)[\mathcal{M}]$ satisfies $\mu_{\mathcal{M}} \geq 2\mu_{\mathfrak{m}}$.

Summing up, we get

THEOREM **2** *Let N be a positive integer prime to p, and let $\mathfrak{m} \subseteq \mathbf{T}_{pN}$ be an ideal of residue characteristic p. Assume that the representation $\rho_{\mathfrak{m}}$ is absolutely irreducible and that $\rho_{\mathfrak{m}}$ is not modular of level N. Then there is a homomorphism $\mathbf{T}_{p^3N} \to \mathbf{T}_{pN}/\mathfrak{m}$ taking $T_n \in \mathbf{T}_{p^3N}$ to T_n mod $\mathfrak{m}$ for all n prime to p. If $\mathcal{M}$ is the kernel of this homomorphism, then $\rho_{\mathfrak{m}}$ has multiplicity greater than 1 in the kernel $J_o(p^3N)[\mathcal{M}]$. More precisely, the representations $\rho_{\mathcal{M}}$ and $\rho_{\mathfrak{m}}$ are canonically isomorphic, and $J_o(p^3N)[\mathcal{M}]$ contains a product of two copies of $\rho_{\mathfrak{m}}$.*

To make a concrete example of a maximal ideal $\mathfrak{m}$ as in the Theorem, take $p = 11$ and $N = 1$. The ring $\mathbf{T}_{11}$ is isomorphic to $\mathbf{Z}$, and there is a unique ideal $\mathfrak{m} = (11)$ of residue characteristic p. The associated representation $\rho_{\mathfrak{m}}$ is the two-dimensional representation $J_o(11)[11]$ of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $\mathbf{F}_{11}$. This representation is known to be absolutely irreducible; indeed, the associated map $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(J_o(11)[11])$ is surjective [40].

References

[1] Artin, M.: On isolated singularities of surfaces. Amer. J. Math. **88**, 129–136 (1966)

[2] Altman, A., Kleiman, S.: Introduction to Grothendieck Duality Theory. Lecture Notes in Mathematics **146**. Berlin-Heidelberg-New York: Springer 1970

[3] Atkin, A.O.L., Li, W-C.: Twists of newforms and pseudo-eigenvalues of W-operators. Invent. Math. **48**, 221–243 (1978)

[4] Ash, A., Stevens, G.: Modular forms in characteristic ℓ and special values of their L-functions. Duke Math. J. **53**, 849–868 (1986)

[5] Bosch, S., Lütkebohmert, W., Raynaud, M.: Néron Models. Berlin-Heidelberg-New York: Springer 1990

[6] Boston, N., Lenstra, H.W. Jr., Ribet, K.: Quotients of group rings arising from two-dimensional representations. To appear

[7] Carayol, H.: Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert. Ann. Sci. ENS **19**, 409–468 (1986)

[8] Carayol, H.: Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires. Duke Math. J. **59**, 785–801 (1989)

[9] Deligne, P., Mumford, D.: The irreducibility of the space of curves of given genus. Publ. Math. IHES **36**, 75–109 (1969)

[10] Deligne, P., Rapoport, M.: Schémas de modules de courbes elliptiques. Lecture Notes in Math. **349**, 143–316 (1973)

[11] Deligne, P., Serre, J-P.: Formes modulaires de poids 1. Ann. Sci. Ecole Norm. Sup. **7**, 507–530 (1974)

[12] Gross, B.: A tameness criterion for Galois representations associated to modular forms (mod p). Duke Math. J. **61** (1990). To appear

[13] Grothendieck, A.: Groupes de monodromie en géométrie algébrique (SGA 7 I). Lecture Notes in Mathematics **288**. Berlin-Heidelberg-New York: Springer 1972

[14] Katz, N. M., Mazur, B.: Arithmetic Moduli of Elliptic Curves. Annals of Math. Studies **108**. Princeton: Princeton University Press 1985

[15] Lang, S.: Introduction to Arakelov Theory. Berlin-Heidelberg-New York: Springer 1988

[16] Lipman, J.: Rational singularities, with applications to algebraic surfaces and unique factorization. Publ. Math. IHES **36**, 195–279 (1969)

[17] Ling, S.: Congruence relations between modular forms on $\Gamma_o(p)$ and $\Gamma_o(p^2)$. To appear

[18] Ling, S., Oesterlé, J.: The Shimura subgroup of $J_0(N)$. This volume

[19] Livné, R.: On the conductors of mod ℓ Galois representations coming from modular forms. J. Number Theory **31**, 133–141 (1989)

[20] Mazur, B.: Modular curves and the Eisenstein ideal. Publ. Math. IHES **47**, 33–186 (1977)

[21] Mazur, B.: Rational isogenies of prime degree. Invent. Math. **44**, 129–162 (1978)

[22] Mazur, B. Letter to J-F. Mestre (16 August 1985)

[23] Mazur, B., Tilouine, J.: Représentations galoisiennes, différentielles de Kähler et «conjectures principales». Publ. Math. IHES. **71**, 65–103 (1990)

[24] Mazur, B., Wiles, A.: Class fields of abelian extensions of $\mathbf{Q}$. Invent. Math. **76**, 179–330 (1984)

[25] Mazur, B., Wiles, A.: On p-adic analytic families of Galois representations. Compositio Math. **59**, 231–264 (1986)

[26] Pinkham, H.: Singularités de Klein I, II. Lecture Notes in Math **777**, 1–20 (1980)

[27] Raynaud, M.: Spécialisation du foncteur de Picard. Publ. Math. IHES **38**, 27–76 (1970)

[28] Ribet, K.: Galois representations attached to eigenforms with Nebentypus. Lecture Notes in Math. **601**, 17–52 (1977)

[29] Ribet, K.: Congruence relations between modular forms. Proc. International Congress of Mathematicians 1983, 503–514

[30] Ribet, K.: On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. Invent. Math. **100**, 431–476 (1990)

[31] Ribet, K.: On the Component Groups and the Shimura Subgroup of $J_o(N)$. Sém. Th. Nombres, Université Bordeaux, 1987–88, exposé 6

[32] Ribet, K.: Multiplicities of Galois representations in Jacobians of Shimura curves. Israel Mathematical Conference Proceedings **3**, 221–236 (1990)

[33] Rosenlicht, M.: Equivalence relations on algebraic curves. Ann. of Math. **56**, 169–191 (1952)

[34] Serre, J-P.: Sur la topologie des variétés algébriques en caractéristique p. Symp. Int. de Top. Alg. (Mexico, 1958), 24–53

[35] Serre, J-P.: Groupes Algébriques et Corps de Classes (deuxième édition revue et corrigée). Paris: Hermann 1959

[36] Serre, J-P.: Lettre à J-F. Mestre (13 août 1985). Contemporary Mathematics **67** , 263–268 (1987)

[37] Serre, J-P.: Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbf{Q}}/\mathbf{Q}$). Duke Math. J. **54**, 179–230 (1987)

[38] Serre, J-P.: Lettre à K. Ribet (15 avril 1987)

[39] Shafarevitch, I.: Lectures on Minimal Models. Tata Institute Lecture Notes. Bombay 1966

[40] Shimura, G.: A reciprocity law in non-solvable extensions. Journal für reine und angewandte Mathematik **221**, 209–220 (1966)

[41] Shimura, G.: Introduction to the Arithmetic Theory of Automorphic Functions. Princeton: Princeton University Press 1971

[42] Tate, J.: p-divisible groups. Proceedings of a Conference on Local Fields (Driebergen 1966). Berlin-Heidelberg-New York: Springer 1967

[43] Tilouine, J.: Un sous-groupe p-divisible de la jacobienne de $X_1(Np^r)$ comme module sur l'algèbre de Hecke. Bull. SMF **115**, 329–360 (1987)

B. Mazur
Harvard Mathematics Department
1 Oxford Street
Cambridge, MA 02138
USA K. A. Ribet
Mathematics Department
University of California
Berkeley CA 94720
USA