Clothbound editions of Princeton University Press books are printed on acid-free paper, and binding materials are chosen for strength and durability. Paperbacks, while satisfactory for personal collections, are not usually suitable for library rebinding

ISBN 0-691-08349-5 (cloth)
ISBN 0-691-08352-5 (paper)

Printed in the United States of America
by Princeton University Press, 41 William Street
Princeton, New Jersey

☆

Library of Congress Cataloging in Publication data will be found on the last printed page of this book

TABLE OF CONTENTS

INTRODUCTION

This book is devoted to giving an account of the arithmetic theory of the moduli spaces of elliptic curves. The main emphasis is on understanding the behavior of these moduli spaces at primes dividing the "level" of the moduli problem being considered. Until recently, this seemed a very difficult problem, because one had no a priori construction of these spaces at the "bad" primes. One defined them as schemes over, say, $\mathbf{Z}[1/N]$ as the solution to some well-posed moduli problem which *only made sense* for elliptic curves over rings in which N was *invertible*, and then one used a process of *normalization* to extend them to schemes over $\mathbf{Z}$, e.g., one took the "proj" of the graded subring of the ring of all modular forms of the type in question consisting of those with *integral* Fourier ("q-expansion") coefficients at the cusps. This procedure produced a scheme over $\mathbf{Z}$, but one had no idea of what moduli interpretation this scheme had, nor a fortiori did one have any idea of the modular interpretation of its reduction modulo p, for p a prime dividing the level.

Historically, the only case where this question was in any way satisfactorily understood was the case of $\Gamma_0(p)$, which made universal sense as the moduli problem "p-isogenies", or "finite flat subgroup-schemes of rank p." This modular interpretation was implicitly known to Kronecker, for whom it appears as the statement that the "modular equation of degree p, reduced mod p, is the curve in the (j_1,j_2)-plane

$$(j_1-(j_2)^p)((j_1)^p-j_2) = 0\ .''$$

One knows the crucial role that the reinterpretation of this Kronecker congruence by Eichler-Shimura as the "congruence relation"

$$T_p = F + V \mod p$$

played in the reduction of the Ramanujan conjecture to Weil's "Riemann Hypothesis for varieties over finite fields."

Eichler-Shimura made use of this relation to prove that for all but finitely many p the Ramanujan conjecture held for any given cusp form of weight two and level N which is a simultaneous eigenfunction of all T_p with p not dividing N. The method was intrinsically incapable of *specifying* the exceptional p, which were *believed* to consist only of primes dividing N.

Partly in order to settle definitively this question of exceptional p for weight two forms, Igusa, in a brilliant series of papers ([Ig 2, 3, 4, 5]), gave a complete and definitive account of the level N moduli scheme over $Z[1/N]$. Except for a difference of mathematical language, and the modular interpretation of the cusps by Deligne-Rapoport, there have been no "improvements" to Igusa's account of what happens over $Z[1/N]$. Although Igusa's papers contain many stimulating speculations about the situation mod p for "bad" p (e.g., the footnote ([Ig 2], p. 472) where he points out that the genus of $\Gamma_0(p)$ is closely related to the number of [super] singular points in characteristic p), there was to be no significant progress in understanding the situation at "bad" p for another decade.

In 1968, Deligne completed the general reduction of Ramanujan's conjecture, for forms of arbitrary weight, and in particular for Δ, to Weil's Riemann Hypothesis for varieties over finite fields. In his article [De 1], he mentions that in fact the $\Gamma_0(p)$ moduli scheme, (with suitable auxiliary prime-to-p rigidification) is actually a *regular* scheme, and in a letter of July 10, 1970 to Parshin he proves this regularity by checking what happens at the supersingular points in characteristic p.

Simultaneously, another theme was developing. Shimura conjectured and Casselman [Cmn 1] proved that for $p = 29, 53, 61, 73, 89, 97$, the Jacobian of (the modular curve for) $\Gamma_1(p)$, modulo the Jacobian of $\Gamma_0(p)$, acquired good reduction over the field $Q(\zeta_p)$. Casselman [Cmn 2]

explained that such theorems of good reduction could be predicted by the "Langlands philosophy", which related, conjecturally, such questions to questions in representation theory which were already well-understood.

The paper of Deligne-Rapoport [De-Ra] in 1972 provided an exhaustive account of what was then known about arithmetic moduli of elliptic curves. It gave a complete account of level N moduli problems over $Z[1/N]$, including a modular interpretation of the compactified moduli scheme (i.e., including the cusps) as the moduli space of "generalized elliptic curves with auxiliary structure." It also gave a modular interpretation over Z to the $\Gamma_1(p)$ moduli problem, and with it a proof that the good reduction phenomenon of Shimura-Casselman held for any p. Another innovation was the systematic use of algebraic stacks, as developed by Mumford [Mum 1] and Deligne-Mumford [De-Mu].

The next significant progress came in 1974, with Drinfeld's introduction (in the context of his theory of "elliptic modules") of the notion of a "full level N-structure" on an elliptic curve over an arbitrary scheme, where N need not be invertible, as a pair of points P,Q of order N such that the group-scheme $E[N]$ of points of order N is equal to the sum

$$\sum_{a,b \bmod N} [aP + bQ]$$

as a Cartier divisor inside E. Drinfeld showed that with this definition, the corresponding full level N moduli problem for his "elliptic modules" was regular. It was clear to the experts, although never published, that with Drinfeld's definition applied to usual elliptic curves, one obtained a moduli problem over Z which was regular, and which, over $Z[1/N]$, coincided with the usual "full level N" moduli problem. In particular, one now had a *modular* interpretation of its reduction modulo any p, as the moduli space of elliptic curves, together with Drinfeld level N structures, over F_p-algebras. With this modular interpretation, it became a pleasant *exercise* to calculate explicitly the reduction modulo any prime p.

In a letter to Drinfeld of January 21, 1975, Deligne explained how the Drinfeld idea of using Cartier divisors allowed one to define universally the $\Gamma_1(N)$ problem as well as a "balanced" version of it by saying that a point P in an elliptic curve has "exact order N" if it is killed by N and if the Cartier divisor inside E defined by

$$\sum_{a \bmod N} [aP]$$

is actually a sub*group*-scheme of E. Deligne also explained that the resulting moduli problem was regular.

In June 1979, the present authors rediscovered Deligne's $\Gamma_1(N)$ idea, and they formulated a Drinfeldian version of $\Gamma_0(N)$ by defining a finite locally free subgroup-scheme G of rank N inside an elliptic curve to be cyclic if locally f.p.p.f. on the base one could find a point P in it which generated it, in the sense that

$$G = \sum_{a \bmod N} [aP]$$

as Cartier divisors inside E. Using this definition of $\Gamma_0(N)$ as the moduli problem of "elliptic curves together with cyclic subgroup-schemes which are finite locally free of rank N," they proved that the $\Gamma_0(N)$ problem was regular and worked out explicitly the reductions mod p of all the "standard" moduli problems.

These calculations of special fibers, together with some intricate (due to wild ramification) calculations of the topological invariants of the special fibers, led to a direct geometric verification of a rather general theorem of good reduction which includes the Shimura-Casselman-Deligne-Rapoport theorem as a special case. For the most part, this good reduction theorem is also a consequence of the above-mentioned Langlands philosophy, which reduces it to a known question in representation theory (cf. [La] and [M W], proof of Prop. 2, §2, Chapter 3).

In writing this book, we have tried simultaneously to be self-contained and to be as general as possible.

In the first chapter, we develop the Drinfeldian notions of level structure through the notion of equality of Cartier divisors in the ambient elliptic curve. With an eye to future applications to the moduli of higher-dimensional abelian varieties, in which the points of order N cease to be a Cartier divisor, we give a reformulation of all the Drinfeldian notions in the context of finite locally free commutative group-schemes, *without* reference to any ambient space. This reformulation, and the questions it raises, may prove to be of some independent interest.

This chapter is followed by a short "Review of Elliptic Curves", in which we recall all the basic facts we will use about elliptic curves. We give either complete proofs or precise references for all of these facts.

In Chapter 3, we apply the general notions developed in the first chapter to the special case of elliptic curves, and we formulate in terms of them the basic moduli problems for elliptic curves.

In Chapter 4, we develop a rudimentary formalism for speaking about these moduli problems, which amounts to working systematically with stacks without ever saying so. We speak rather of "relatively representable moduli problems", a notion which seems admirably suited to our purposes, and which is a throw-back to Mumford's original exposition [Mum 1].

After these preliminary chapters, we turn to the detailed study of the basic moduli problems *as* "open arithmetic surfaces." The basic results on their structure and inter-relations (e.g., which are regular, which are finite flat over which others, which are quotients by finite groups of which others,...) are given in Chapters 5, 6 and 7.

The remaining 7 chapters are devoted to the detailed study of these same moduli problems *as* "curves over $\mathrm{Spec}(\mathbf{Z})$."

In Chapter 8, we compactify our moduli problems, relative to $\mathrm{Spec}(\mathbf{Z})$, by adding the cusps. In Chapter 9, we explain how to deal systematically with these moduli problems which are "really" defined over cyclotomic integer rings rather than over $\mathbf{Z}$. In Chapter 10 we give the basic results on the structure of our compactified moduli problems *as* relative curves.

After a brief digression concerning "exotic" isomorphisms of moduli problems in Chapter 11, the remaining three chapters are devoted to the detailed study of the degeneration at bad primes of our moduli problems as relative curves. Chapter 12 gives the theory of the Igusa curves, which are the "basic" p-power level moduli problems in characteristic p. In Chapter 13, we give the detailed structure of the reduction mod p of each of our basic moduli problems as a "disjoint union, with crossings at the supersingular points", of suitable Igusa curves.

In Chapter 14, we apply the specific calculations of the previous chapter to prove a general theorem of good reduction for suitable "pieces" of Jacobians of modular curves.

We would like to thank the IHES for providing the congenial atmosphere in which this book was written. We warmly thank Ofer Gabber, whose innumerable comments and corrections were invaluable to us in preparing the final version of this work. Lauri Hein and Perry Di Verita of Princeton University, and Helen Mann of Princeton University Press prepared the original and final manuscripts respectively. To them and to our editor, Barbara Stump of Princeton University Press, we extend our thanks for their patience in the face of our numerous and unexpected revisions.

NICHOLAS M. KATZ
BARRY MAZUR

Arithmetic Moduli of Elliptic Curves

Chapter 1

GENERALITIES ON "A-STRUCTURES" AND "A-GENERATORS"

(1.1) *Review of relative Cartier divisors* (Compare [Mum 2], pp. 61-73.)

(1.1.1) Let S be an arbitrary scheme, and let X be an S-scheme. By an effective Cartier divisor D in X/S we mean a closed subscheme $D \subset X$ such that

$$\begin{cases} D \text{ is flat over } S \\ \text{the ideal sheaf } I(D) \subset \mathcal{O}_X \text{ is an invertible } \mathcal{O}_X\text{-module, i.e.,} \\ \text{it is a locally free } \mathcal{O}_X\text{-module of rank one.} \end{cases}$$

This notion is local on S. When S is affine, say $S = \mathrm{Spec}\,(R)$, it means that we can cover X by affine opens $U_i = \mathrm{Spec}\,(A_i)$, A_i an R-algebra, such that $D \cap U_i$ is defined in U_i by one equation $f_i = 0$, where $f_i \in A_i$ is an element such that

$$\begin{cases} A_i/f_iA_i \text{ is flat over } R \\ f_i \text{ is not a zero-divisor in } A_i\,. \end{cases}$$

The tautological exact sequence on X,

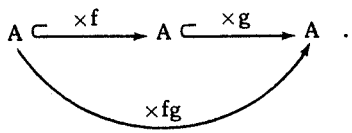
$$0 \to I(D) \to \mathcal{O}_X \to \mathcal{O}_D \to 0\,,$$

becomes on $U_i = \mathrm{Spec}\,(A_i)$ the exact sequence

$$0 \longrightarrow A_i \xrightarrow{\times f_i} A_i \longrightarrow A_i/f_iA_i \longrightarrow 0\,.$$

(1.1.2) Given two effective Cartier divisors D and D' in X/S, their sum $D+D'$ is the effective Cartier divisor in X/S defined locally by the

product of the defining equations of D and D′. Explicitly, if $S=\mathrm{Spec}(R)$ and if on an affine open $\mathrm{Spec}(A)$ of X, D and D′ are defined respectively by equations $f=0$ and $g=0$, then $D+D'$ is defined there by $fg=0$. To check that fg is not a zero-divisor in A, one notes the commutative diagram



To check that A/fgA is flat over R, one notes the short exact sequence

$$0 \longrightarrow A/gA \xrightarrow{\times f} A/fgA \longrightarrow A/fA \longrightarrow 0\,,$$

which exhibits A/fgA as an extension of flat R-modules.

(1.1.3) Given an effective Cartier divisor D in X/S, we may speak of the inverse (as invertible $\mathcal{O}_X$-module) $I^{-1}(D)$ of its ideal sheaf. We have a tautological exact sequence

$$0 \to \mathcal{O}_X \to I^{-1}(D) \to \mathcal{O}_D \underset{\mathcal{O}_X}{\otimes} I^{-1}(D) \to 0\,.$$

The inclusion of $\mathcal{O}_X$ in $I^{-1}(D)$ allows us to view the constant function "1" as a global section of $I^{-1}(D)$, and we may recover D as the scheme of zeroes of this global section of $I^{-1}(D)$.

Conversely, suppose we are given a pair $(\mathcal{L},\ell)$ consisting of an invertible $\mathcal{O}_X$-module $\mathcal{L}$ on X together with a global section $\ell \in H^0(X,\mathcal{L})$ which sits in a short exact sequence of $\mathcal{O}_X$-modules

$$0 \longrightarrow \mathcal{O}_X \xrightarrow{\times \ell} \mathcal{L} \longrightarrow \mathcal{L}/\mathcal{O}_X \longrightarrow 0$$

with $\mathcal{L}/\mathcal{O}_X$ *flat* over S. Then the scheme of zeroes of the section ℓ of $\mathcal{L}$ is easily seen to be an effective Cartier divisor D in X/S, and there is a unique isomorphism of $(\mathcal{L},\ell)$ with $(I^{-1}(D),\text{"1"})$.

This construction allows us to interpret effective Cartier divisors in X/S as isomorphism classes of pairs $(\mathcal{L},\ell)$ as above. From this point of view, the operation "sum of effective Cartier divisors in X/R" is none other than the operation of tensor product:

$$(\mathcal{L},\ell)+(\mathcal{L}',\ell') = (\mathcal{L}\otimes\mathcal{L}',\ell\otimes\ell')\,.$$

The zero element for this addition is the pair $(\mathcal{O}_X,1)$, corresponding to the *empty* Cartier divisor.

(1.1.4) There are two natural situations in which one can define the inverse image of a relative Cartier divisor. First let

$$T \to S$$

be an arbitrary morphism of schemes. Then for any effective Cartier divisor D in X/S, say represented by a pair $(\mathcal{L},\ell)$, the closed subscheme $D_T \underset{\text{dfn}}{=\!=} D \underset{S}{\times} T$ of $X_T = X \underset{S}{\times} T$ is an effective Cartier divisor in X_T/T, represented by the pair $(\mathcal{L}_T,\ell_T)$ on X_T. To see this, it suffices to treat the case when $S=\mathrm{Spec}(R)$ and $T=\mathrm{Spec}(R')$ are both affine; then the sequence on $X_T = X\otimes R'$

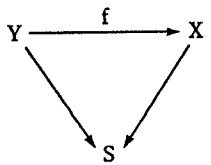
$$\mathcal{O}_X \underset{R}{\otimes} R' \xrightarrow{\ell\otimes 1} \mathcal{L}\otimes R' \longrightarrow \mathcal{L}\otimes R'/\mathcal{O}_X \underset{R}{\otimes} R'$$

is obtained from the short exact sequence on X

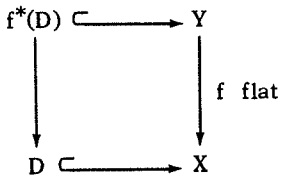
$$0 \longrightarrow \mathcal{O}_X \xrightarrow{\ell} \mathcal{L} \longrightarrow \mathcal{L}/\mathcal{O}_X \longrightarrow 0$$

by applying the functor $\underset{R}{\otimes} R'$. Because $\mathcal{L}/\mathcal{O}_X$ is assumed flat over R, this sequence stays short exact after $\underset{R}{\otimes} R'$, and its last term is R′-flat. Therefore $(\mathcal{L} \underset{R}{\otimes} R', \ell\otimes 1)$ defines an effective Cartier divisor in $X \underset{R}{\otimes} R'/R'$, as required.

Second, let



be a flat morphism of S-schemes. Then any effective Cartier divisor D in X/S gives rise to an effective Cartier divisor $f^*(D)$ in Y/S. Indeed, the cartesian diagram



shows that $f^*(D)$ is flat over D, and hence, D being S-flat, that $f^*(D)$ is flat over S. To see that the ideal sheaf $I(f^*(D))$ is an invertible $\mathcal{O}_Y$-module, we remark that this ideal sheaf is none other than $f^*(I(D))$, as follows from the fact that the short exact sequence on X

$$0 \to I(D) \to \mathcal{O}_X \to \mathcal{O}_D \to 0$$

remains short exact after application of the functor f^*, thanks to the flatness of f.

(1.1.5) We now turn to the question of recognizing which closed subschemes of X are in fact effective Cartier divisors in X/S.

PROPOSITION 1.1.5.1. *Suppose that S is locally noetherian, and that X is an S-scheme of finite type which is flat over S. Let $\mathcal{F}$ be a coherent sheaf on X which is flat over S. Then the necessary and sufficient condition that $\mathcal{F}$ be flat over $\mathcal{O}_X$ is that for every geometric point of S, i.e., every morphism Spec(k) → S with k an algebraically closed field, the induced coherent sheaf $\mathcal{F}_{\otimes_R k}$ on the fibre $X_{\otimes_R k}$ be flat over $\mathcal{O}_{X_{\otimes_R k}}$.*

Proof. This is just the fibre-by-fibre criterion of flatness [A-K 1, V, 3.6]. Q.E.D.

COROLLARY 1.1.5.2. *Let S be locally noetherian, X a flat S-scheme of finite type, and D ⊂ X a closed subscheme which is flat over S. Then D is an effective Cartier divisor in X/S if and only if for all geometric points Spec(k) → S of S, the closed subscheme $D_{\otimes_R k}$ of $X_{\otimes_R k}$ is an effective Cartier divisor in $X_{\otimes_R k}/k$.*

Proof. The necessity is a special case of the preservation of effective Cartier divisors in X/S under arbitrary change of base T → S. For the sufficiency, we apply the proposition to $\mathcal{F} = I(D)$, which is S-flat because it sits in the short exact sequence

$$0 \to I(D) \to \mathcal{O}_X \to \mathcal{O}_D \to 0\ ,$$

in which both $\mathcal{O}_X$ and $\mathcal{O}_D$ are S-flat by hypothesis. Tensoring over $\mathcal{O}_S$ with k (for any geometric point Spec(k) → S), this sequence stays exact (S-flatness of $\mathcal{O}_D$), so comparing first terms yields

$$I(D)_{\otimes_R k} \xrightarrow{\sim} I(D_{\otimes_R k})\ .$$

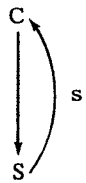
By hypothesis, $I(D_{\otimes k})$ is an invertible $\mathcal{O}_{X_{\otimes k}}$-module, so in particular it is $\mathcal{O}_{X_{\otimes k}}$-flat. Therefore I(D) is $\mathcal{O}_X$-flat by the proposition. Because I(D) is also coherent, it is a locally free $\mathcal{O}_X$-module. That it is locally free of rank one may then be seen by restricting it to the fibres $X_{\otimes k}$ of X/S, on each of which it is locally free of rank one. Q.E.D.

(1.2) *Relative Cartier divisors in curves*

(1.2.1) Let S be an arbitrary scheme. By a smooth curve C/S, we will

always mean a smooth morphism $C \to S$ of relative dimension one which is separated and of finite presentation.

LEMMA 1.2.2. *If* C/S *is a smooth curve, then any section* $s \in C(S)$



defines an effective Cartier divisor, noted $[s]$, *in* C/S.

Proof. Because C/S is of finite presentation, we are immediately reduced to the case when $S = \mathrm{Spec}(R)$ with R noetherian, (EGA IV, 8.9.1) then by Corollary 1.1.5.2 to the case when R is an algebraically closed field k, and in this case the assertion is obvious. Q.E.D.

LEMMA 1.2.3. *Let* C/S *be a smooth curve as above. Let* $D \subset C$ *be a closed sub-scheme which is finite and flat over* S, *and of finite presentation over* S. *Then* D *is an effective Cartier divisor in* C/S, *which is proper over* S. *Conversely every effective Cartier divisor in* C/S *which is proper over* S *is of this form.*

Proof. To prove the first statement, we are immediately reduced (by EGA IV, 8.9.1 and 11.2.6.1) to the case when $S = \mathrm{Spec}(R)$ with R noetherian, then by Corollary 1.1.5.2 to the case when R is an algebraically closed field k, in which case it is obvious that D is an effective Cartier divisor. That D is proper over S follows from its being assumed finite over S.

Conversely, any effective Cartier divisor D in C/S is certainly of finite presentation, so we are reduced to the case when $S = \mathrm{Spec}(R)$ with R noetherian (EGA IV, 8.9.1 and 11.2.6.1). We must prove that D is finite over R. But D is proper over R, so it suffices to prove that D/R has finite fibres. Thus we are reduced to the case when R is an

algebraically closed field k, i.e., to the assertion that an effective Cartier divisor in a smooth curve over k is a finite k-scheme, which is obvious. Q.E.D.

REMARK 1.2.4. If C/S is a *proper* smooth curve, then *every* effective Cartier divisor in C/S is automatically proper over S.

DEFINITION 1.2.5. Let C/S be a smooth curve, D an effective Cartier divisor in C/S which is proper over S. Then locally on S, say $S = \mathrm{Spec}(R)$, the affine ring of D is a locally free R-module of finite rank. This rank, which is constant Zariski locally on S, is called the *degree* of D, noted $\deg(D)$. In terms of an $(\mathcal{L}, \ell)$ presentation of D, the exact sequence on C

$$0 \longrightarrow \mathcal{O}_C \xrightarrow{\ell} \mathcal{L} \longrightarrow \mathcal{L}/\mathcal{O} \longrightarrow 0$$

has

$$\mathcal{L}/\mathcal{O} \simeq I^{-1}(D)/\mathcal{O} \simeq I^{-1}(D) \underset{\mathcal{O}_C}{\otimes} \mathcal{O}_D \simeq \mathcal{L} \underset{\mathcal{O}_C}{\otimes} \mathcal{O}_D = \text{an invertible } \mathcal{O}_D\text{-module.}$$

Therefore D is proper over S if and only if the sheaf $\mathcal{L}/\mathcal{O}$ on C has its support proper over S. If this is the case, then locally on S, say $S = \mathrm{Spec}(R)$, the R-module

$$H^0(C, \mathcal{L}/\mathcal{O}) = H^0(C, I^{-1}(D)/\mathcal{O})$$

is a locally free R-module of rank $= \mathrm{degree}(D)$.

LEMMA 1.2.6. *Let* C/S *be a smooth curve,* D_1 *and* D_2 *two effective Cartier divisors in* C/S *which are both proper over* S. *Then* $D_1 + D_2$ *is proper over* S, *and we have the equality*

$$\deg(D_1 + D_2) = \deg(D_1) + \deg(D_2).$$

Proof. In terms of representatives $(\mathcal{L}_1, \ell_1)$ and $(\mathcal{L}_2, \ell_2)$ of D_1 and D_2 respectively, we have a short exact sequence of sheaves on C

$$0 \to \mathcal{L}_2/\mathcal{O} \to \mathcal{L}_1 \otimes \mathcal{L}_2/\mathcal{O} \to \mathcal{L}_1 \otimes \mathcal{L}_2/\mathcal{L}_2 \to 0$$

obtained by applying the snake lemma to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O} & \xrightarrow{\times 1} & \mathcal{O} & \longrightarrow & 0 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \times \ell_2} & & \downarrow{\scriptstyle \times \ell_1 \otimes \ell_2} & & \downarrow{\scriptstyle 0} & & \\ 0 & \longrightarrow & \mathcal{L}_2 & \xrightarrow{\times \ell_1} & \mathcal{L}_1 \otimes \mathcal{L}_2 & \longrightarrow & \mathcal{L}_1 \otimes \mathcal{L}_2/\mathcal{L}_2 & \longrightarrow & 0 \end{array}$$

when bottom row is obtained by applying $\otimes_{\mathcal{O}} \mathcal{L}_2$ to

$$0 \longrightarrow \mathcal{O} \xrightarrow{\times \ell_1} \mathcal{L}_1 \longrightarrow \mathcal{L}_1/\mathcal{O} \longrightarrow 0 .$$

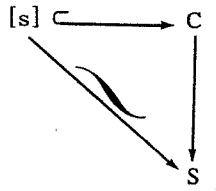
In any case, the above exact sequence, when rewritten

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{L}_2 \otimes_{\mathcal{O}} \mathcal{O}_{D_2} & \longrightarrow & (\mathcal{L}_1 \otimes \mathcal{L}_2) \otimes_{\mathcal{O}} \mathcal{O}_{D_1+D_2} & \longrightarrow & (\mathcal{L}_1 \otimes \mathcal{L}_2) \otimes_{\mathcal{O}} \mathcal{O}_{D_1} & \longrightarrow & 0 \\ & & \| & & \| & & \| & & \\ & & (\mathcal{L}_2)|D_2 & & (\mathcal{L}_1 \otimes \mathcal{L}_2)|D_1+D_2 & & (\mathcal{L}_1 \otimes \mathcal{L}_2)|D_1 & & \end{array}$$

shows that D_1+D_2 is proper over S and shows, taking Euler characteristics, that the degrees add as asserted. Q.E.D.

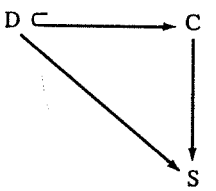
LEMMA 1.2.7. *Let* C/S *be a smooth curve. Then for any section* $s \in C(S)$, *the associated effective Cartier divisor* $[s]$ *in* C/S *is proper over* S, *and has degree one. Conversely, any effective Cartier divisor* D *in* C/S *which is proper over* S *and has degree one is of the form* $[s]$ *for a unique section* $s \in C(S)$.

Proof. If $s \in C(S)$, then the Cartier divisor $[s]$ sits in a diagram



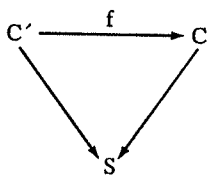
which shows that $[s]$ is proper over S, of degree one.

Conversely, if D is an effective Cartier divisor in C/S, proper over S of degree one, then we have a diagram



in which the diagonal arrow is an isomorphism (because locally on S, say $S = \mathrm{Spec}(R)$, it turns the affine ring of D into an R-algebra which is an *invertible* R-module, i.e., into R itself). Q.E.D.

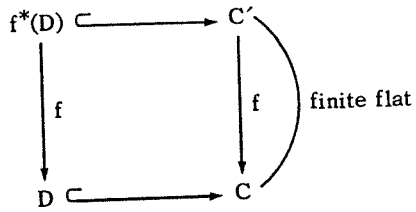
LEMMA 1.2.8. *Let* C', C *be two smooth curves over* S, *and*



a morphism which is finite and flat of degree noted $\deg(f)$. *If* D *is an effective Cartier divisor in* C/S, *proper over* S, *then its inverse image* $f^*(D)$ *in* C' *is an effective Cartier divisor in* C'/S, *proper over* S, *and its degree is given by*

$$\deg(f^*(D)) = \deg(f)\deg(D) .$$

Proof. That $f^*(D)$ is an effective Cartier divisor in C'/S we have already seen results from the flatness of f. The cartesian diagram of schemes

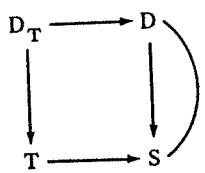


shows that $f^*(D)$ is finite flat over D of degree $= \deg(f)$, and the result follows. Q.E.D.

LEMMA 1.2.9. *Let C/S be a smooth curve, D an effective Cartier divisor in C/S which is proper over S, and $T \to S$ an arbitrary morphism of schemes. Then D_T is an effective Cartier divisor in C_T, proper over T, whose degree is unchanged:*

$$\deg(D_T) = \deg(D) .$$

Proof. That D_T is an effective Cartier divisor in C_T we have already seen. The assertion of properness of D_T over T, as well as the fact that D_T is finite locally free over T of rank $= \deg(D)$, result from the cartesian diagram



finite locally free of $\deg(D)$. Q.E.D.

(1.3) *Existence of Incidence schemes*

(1.3.1) Given two effective Cartier divisors D, D' in X/S, we say that $D' \leq D$ if $D' \subset D$ (inclusion of closed subschemes of X), i.e., if

$I(D) \subset I(D')$ (inclusion of ideal sheaves inside $\mathcal{O}_X$), or equivalently if there exists an effective Cartier divisor D'' in X/S such that

$$D = D' + D'' .$$

In terms of local equations $f = 0$ for D and $g = 0$ for D', the condition $D' \leq D$ means precisely that g *divides* f, i.e., that locally we have $f = gh$ for some function h. This function h is unique (because g is not a zero-divisor), and h itself is not a zero divisor (because $gh = f$ is not a zero divisor). The locally defined subschemes $h = 0$ of X patch together to define a subscheme D'' of X, whose ideal sheaf $I(D'')$, locally $h\mathcal{O}_X$, is invertible. To see that D'' is flat over S, we may assume $S = \mathrm{Spec}(R)$, $X = \mathrm{Spec}(A)$, D is defined by $f = 0$, D' by $g = 0$, and D'' by $h = 0$, with $f = gh$. The exact sequence

$$0 \longrightarrow A/hA \xrightarrow{\times g} A/fA \longrightarrow A/gA \longrightarrow 0$$

then shows that A/hA is R-flat (because A/fA and A/gA are R-flat), as required.

Globally, in terms of representatives $(\mathcal{L}, \ell)$ for D and $(\mathcal{L}', \ell')$ for D', the condition $D' \leq D$ is precisely that the global section ℓ of $\mathcal{L}$ vanish identically in $\mathcal{L}|D' = \mathcal{L} \underset{\mathcal{O}_X}{\otimes} \mathcal{O}_{D'}$. Then D'' is represented by $(\mathcal{L}'', \ell')$ with $\mathcal{L}'' = \mathcal{L} \otimes (\mathcal{L}')^{-1}$ and $\ell'' = \ell/\ell'$. The global version of the above short exact sequence is

$$0 \to \mathcal{L}'' \underset{\mathcal{O}_X}{\otimes} \mathcal{O}_{D''} \to \mathcal{L} \underset{\mathcal{O}_X}{\otimes} \mathcal{O}_D \to \mathcal{L} \underset{\mathcal{O}_X}{\otimes} \mathcal{O}_{D'} \to 0 . \tag{1.3.1.1}$$

(1.3.2) We now turn from a general X/S to a smooth curve C/S (cf. 1.2.1).

LEMMA 1.3.3. *Let C/S be a smooth curve, D and D' effective Cartier divisors in C/S which are both proper over S. If $D' \leq D$, then the effective Cartier divisor $D'' = D - D'$ is proper over S, and*

$$\deg(D'') = \deg(D) - \deg(D') .$$

Proof. The properness is obvious from the short exact sequence (1.3.1.1). The degree assertion then results from (1.2.6). Q.E.D.

KEY LEMMA 1.3.4. *Let* C/S *be a smooth curve,* D *and* D' *effective Cartier divisors in* C/S, *with* D' *proper over* S. *Then*

(1) *there exists a unique closed subscheme* $Z \subset S$ *which is universal for the relation* $D' \leq D$ *in the following sense: given any morphism of schemes* $T \to S$, *the inverse images* D'_T *and* D_T *in* C_T *satisfy* $D'_T \leq D_T$ *if and only if the morphism* $T \to S$ *factors through* Z;

(2) *the subscheme* $Z \subset S$ *is defined locally on* S *by* $\deg(D')$ *equations;*

(3) *formation of the closed subscheme* $Z \subset S$ *commutes with arbitrary change of base* $S' \to S$, *in the sense that the closed subscheme* Z' *of* S' *"universal for the relation* $D'_{S'} \leq D_{S'}$*" is none other than* $Z \underset{S}{\times} S'$.

Proof. The question is clearly local on S, which we may assume affine, say $S = \mathrm{Spec}(R)$. In terms of a representative $(\mathfrak{L}, \ell)$ for D, the condition $D' \leq D$ is that the global section ℓ of $\mathfrak{L}$ vanish identically in $\mathfrak{L} \underset{\mathcal{O}_C}{\otimes} \mathcal{O}_{D'} = \mathfrak{L}|D'$. Because D' is finite locally-free over S, and $\mathfrak{L}|D'$ is an invertible $\mathcal{O}_{D'}$-module, the module $H^0(D', \mathfrak{L}|D')$ is a locally free R-module of rank $= \deg(D')$. Locally on R, we may choose an R-basis $e_1, \cdots, e_{d'}$ of this R-module. The element ℓ has a unique expression

$$\ell = \sum_{i=1}^{\deg(D')} r_i e_i, \quad \text{coefficients } r_i \in R.$$

The condition "$\ell = 0$" is then represented by the closed subscheme of $\mathrm{Spec}(R)$ defined by the simultaneous vanishing of $r_1, \cdots, r_{d'}$. Q.E.D.

COROLLARY 1.3.5. *Let* C/S *be a smooth curve,* D *and* D' *effective Cartier divisors in* C/S *which are both proper over* S *of the same degree. Then there exists a unique closed subscheme* $Z \subset S$ *which is universal*

for the relation $D = D'$, *in the sense that for any* $T \to S$, *we have* $D_T = D'_T$ *in* C_T *if and only if* $T \to S$ *factors through* Z. *The subscheme* $Z \subset S$ *is defined locally in* S *by* $\deg(D)$ *equations, and its formation commutes with arbitrary change of base* $S' \to S$.

Proof. The condition $D = D'$ is equivalent to the condition $D' \leq D$, because D and D' both have the same degree. Q.E.D.

(1.3.6) Let C/S be a smooth curve which is a group-scheme over S. Let D be an effective Cartier divisor in C/S which is proper over S. We say that D is a subgroup of C/S if for every S-scheme T the subset $D(T)$ of the group $C(T)$ is in fact a sub-group. This amounts to the existence of a (necessarily unique) structure of finite flat S-group-scheme on D such that $D \hookrightarrow C$ is an S-group-scheme homomorphism.

COROLLARY 1.3.7. *Let* C/S *be a smooth curve which is a group-scheme over* S. *Let* D *be an effective Cartier divisor in* C/S, *proper over* S. *Then there exists a unique closed subscheme* $Z \subset S$ *which is universal for the relation "*D *is a subgroup," in the sense that for any* $T \to S$, D_T *in* C_T/T *is a subgroup if and only if* $T \to S$ *factors through* Z. *The subscheme* $Z \subset S$ *is defined locally in* S *by* $1 + \deg(D) + (\deg(D))^2$ *equations, and its formation commutes with arbitrary change of base* $S' \to S$.

Proof. Let us denote by $e \in C(S)$ the identity section for the group structure, by

$$\mathrm{inv} : C \to C$$

the S-automorphism of C expressing inversion, and by

$$m : C \underset{S}{\times} C \to C$$

the S-morphism "multiplication."

In order that D be a subgroup, it is necessary and sufficient that the following three conditions be satisfied:

(1) Denoting by $[e]$ the effective Cartier divisor in C/S attached to the identity section $e \in C(S)$, we have the inequality of Cartier divisors

in C/S

$$[e] \leq D .$$

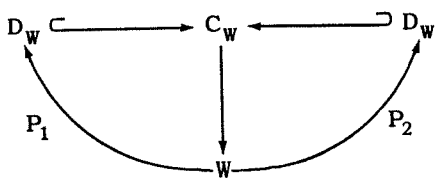
(This is the condition that the subset $D(T) \subset C(T)$ always contain the identity.)

(2) We have the equality of effective Cartier divisors in C/S

$$D = \mathrm{inv}^*(D) .$$

(This is the condition that the subset $D(T) \subset C(T)$ be stable by inversion.)

(3) Let W denote the S-scheme $D \underset{S}{\times} D$, which represents the functor "ordered pairs of points of D." Let (P_1, P_2) be the universal pair of points of D, so that we have a tautological diagram



Then we must have the inequality of effective Cartier divisors in C_W

$$[m(P_1, P_2)] \leq D_W .$$

(This is the condition that the subset $D(T) \subset C(T)$ always be stable by multiplication.)

Now condition (1) is represented locally on S by one equation. Condition (2) is represented locally on S by $\deg(D)$ equations. Condition (3) is represented locally on W by one equation, but because W is finite locally free over S of rank $(\deg(D))^2$, the vanishing on W of a single function is equivalent to the vanishing on S of its $(\deg(D))^2$ "coordinates." Q.E.D.

(1.4) *Points of "exact order N" and cyclic subgroups*

(1.4.1) Let C/S be a smooth curve (cf. 1.2.1), given with a structure of commutative S-group-scheme. We will refer to such a C/S as a "smooth commutative S-group-scheme of relative dimension one"; in view of 1.2.1, C/S is automatically separated and of finite presentation over S. Let $N \geq 1$ be an integer. We say that a point $P \in C(S)$ has "exact order N" if the effective Cartier divisor D in C/S of degree N defined by

$$D \overset{\mathrm{dfn}}{=\!=} [P] + [2P] + \cdots + [NP] \tag{1.4.1.1}$$

is a *subgroup* of C/S. We call this subgroup the cyclic subgroup of rank N "*generated*" by P. We say that a closed subgroup-scheme $G \subset C$ which is finite locally-free of rank N over S is *cyclic* if, locally f.p.p.f. (SGA III, Exp. IV, 6.3) on S, G admits a generator, i.e., if there exists some f.p.l.p.f. (faithfully flat, locally of finite presentation) morphism $T \to S$ and a point $P \in C(T) = C_T(T)$ of "exact order N" on C_T/T which generates the subgroup G_T of C_T, i.e., such that we have an equality of Cartier divisors in C_T:

$$G_T = \sum_{a=1}^{N} [aP] . \tag{1.4.1.2}$$

Clearly if a point $P \in C(S)$ has "exact order N" in C/S, and generates a subgroup G of rank N, then for any change of base $T \to S$ the induced point $P_T \in C(T) = C_T(T)$ has "exact order N" in C_T/T, and it generated the subgroup G_T of C_T/T.

LEMMA 1.4.2. *If $P \in C(S)$ has "exact order N," then $NP = 0$.*

Proof. Any finite locally free commutative group-scheme of rank N is known to be killed by N (cf. [Oort-Tate]). Therefore every section, in particular P, of the effective Cartier divisor $\sum_{1}^{N} [aP]$ is killed by N. Q.E.D.

CAUTION 1.4.3. If S is an $\mathbf{F}_p$-scheme, then for every integer $n \geq 1$ the zero-section $0 \in C(S)$ has "exact order p^n"; indeed it "generates" the

subgroup $\mathrm{Ker}(F^n : C \to C^{(p^n)})$ of rank p^n. This example shows that a given point can have many different "exact orders."

LEMMA 1.4.4. *Suppose that* N *is invertible on* S. *Let* $P \in C(S)$ *be a point killed by* N. *Then the following conditions are equivalent.*

(1) P *has "exact order* N*" in* C/S.

(2) *For every geometric point* $\mathrm{Spec}(k) \to S$ *of* S, *the induced point* $P_k \in C(k) = C_k(k)$ *has "exact order* N*" in* C_k/k.

(3) *For every geometric point* $\mathrm{Spec}(k) \to S$ *of* S, *the induced point* $P_k \in C(k)$ *has exact order* N *in the usual sense that* N *is the least positive integer which kills* P_k, *i.e., the* N *points* $\{aP_k\}$, $a = 1, \cdots, N$ *are all distinct in* $C(k)$.

(4) *The effective Cartier divisor in* C/S

$$\sum_{a=1}^{N} [aP]$$

in C/S *is finite etale over* S.

(5) *The unique* S*-group homomorphism* $\mathbf{Z}/N\mathbf{Z} \to C$ *which maps "1"* $\in \mathbf{Z}/N\mathbf{Z}$ *to* $P \in C(S)$ *defines a closed* S*-immersion*

$$\mathbf{Z}/N\mathbf{Z} \hookrightarrow C$$

which identifies the constant S*-scheme* $\mathbf{Z}/N\mathbf{Z}$ *with the Cartier divisor* $\Sigma\,[aP]$:

$$\mathbf{Z}/N\mathbf{Z} \xrightarrow{\sim} \sum_{a=1}^{N} [aP].$$

Proof. (1) $\Rightarrow$ (2), because the property of having "exact order N" is preserved under arbitrary changes of base $T \to S$.

(2) $\Rightarrow$ (3). Let G be the rank N subgroup-scheme of C_k "generated" by P_k. Then G is finite flat of rank N over k. Because N is *invertible* in S, it is invertible in k, and therefore G is automatically finite

etale over k of rank N. Therefore as a Cartier divisor in C_k, G consists of a uniquely determined set of N distinct points. The equality of Cartier divisors in C_k

$$G = \sum_{a=1}^{N} [aP_k]$$

shows that the N points $\{aP_k\}$, $a = 1, \cdots, N$, are all distinct in C_k, as required.

(3) $\Longleftrightarrow$ (4). Let us denote by D the effective Cartier divisor

$$D = \sum_{a=1}^{N} [aP]$$

in C/S. As a scheme over S, D is finite and locally free of rank N over S. It is finite etale over S if and only if its discriminant (determinant of the matrix $\mathrm{tr}(e_i e_j) \cdots$) is invertible on S. This holds if and only if for all geometric points $\mathrm{Spec}(k) \to S$, the Cartier divisor in C_k

$$D_k = \sum_{a=1}^{N} [aP_k]$$

is finite etale over k, i.e., if and only if (3) holds.

(3) $\Longleftrightarrow$ (5). The morphism of S-groups $\mathbf{Z}/N\mathbf{Z} \to C$ mapping 1 to P certainly factors through the effective Cartier divisor

$$D = \sum_{a=1}^{N} [aP],$$

thus defining an S-morphism

$$(\mathbf{Z}/N\mathbf{Z})_S \to D.$$

Both source and target of this morphism are finite locally-free over S of the same rank N, so locally on S, say S = Spec(R), the map on coordinate rings is given by an N×N matrix over R. Our map is an isomorphism if and only if this matrix has determinant a *unit* in R. Therefore our map is an isomorphism if and only if for all geometric points Spec(k) → S of S, the k-morphism

$$\mathbf{Z}/N\mathbf{Z} \xrightarrow{1 \mapsto P_k} D_k = \sum_{a=1}^{N} [aP_k]$$

is an isomorphism, i.e., if and only if the N points $\{aP_k\}$, $a = 1, \cdots, N$, are all distinct.

(5) ⇒ (1). Indeed if (5) holds, then $\sum_{a=1}^{N} [aP]$ is endowed with the structure of subgroup of C/S. Q.E.D.

REMARK 1.4.5. If we do *not* assume N invertible on S, we still have the implications

$$(3) \Longleftrightarrow (4) \Longleftrightarrow (5) \Longrightarrow (1) \Longrightarrow (2).$$

A point $P \in C(S)$ which is killed by N and which satisfies any of the equivalent conditions (3), (4), (5), might be called an "etale point of exact order N."

(1.5) *A mild generalization*: A-*structures and* A-*generators*

(1.5.1) As before, C/S is a smooth commutative group-scheme over S of relative dimension one (cf. 1.4.1). Let A be an "abstract" finite abelian group. A homomorphism of abstract groups

(1.5.1.1) $$\phi : A \to C(S)$$

is said to be an A-structure on C/S if the effective Cartier divisor D in C/S of degree = #(A) defined by

(1.5.1.2) $$D = \sum_{a \in A} [\phi(a)]$$

is a subgroup G of C/S. We call this subgroup G the A-subgroup of C/S generated by ϕ, and we call ϕ an A-generator of G. We say that a closed subgroup-scheme $G \subset C$ which is finite locally free over S of rank = #(A) is an A-subgroup if, locally f.p.p.f. on S, it admits as A-generator, i.e., if there exists an f.p.l.p.f. T → S and an A-structure

(1.5.1.3) $$\phi : A \to C(T) = C_T(T)$$

on C_T which generates G_T.

Clearly if $\phi : A \to C(S)$ is an A-structure, generating G, then for any change of base T → S, the composite

$$\phi_T : A \to C(S) \to C(T) = C_T(T)$$

is an A-structure on C_T/T, and it generates G_T.

(1.5.2) When we take A to be Z/NZ, we recover the notion of a point of "exact order N"; for a homomorphism

$$\phi : \mathbf{Z}/N\mathbf{Z} \to C(S)$$

is a Z/NZ-structure on C/S if and only if the point $P = \phi(1) \in C(S)$ is a point of "exact order N" in C(S). Similarly, a finite locally free of rank N subgroup-scheme of C/S is a Z/NZ-subgroup if and only if it is a cyclic subgroup.

The analogue of Lemma (1.4.4) is the following, whose proof, entirely similar, is left to the reader.

LEMMA 1.5.3. *Let* C/S *be as above,* A *a finite abelian "abstract" group, and* $\phi : A \to C(S)$ *a group homomorphism. Consider the following conditions*:

(1) ϕ *is an* A-*structure on* C/S.

(2) *For every geometric point* $\mathrm{Spec}(k) \to S$ *of* S, *the induced homomorphism* $\phi_k : A \to C(k) = C_k(k)$ *is an* A*-structure on* C_k/k.

(3) *For every geometric point* $\mathrm{Spec}(k) \to S$ *of* S, *the induced homomorphism* $\phi_k : A \to C(k)$ *is injective.*

(4) *The effective Cartier divisor in* C/S

$$\sum_{a \in A} [\phi(a)]$$

is finite etale over S.

(5) ϕ *defines a closed* S*-immersion*

$$A \hookrightarrow C$$

which identifies the constant S*-scheme* A *with the Cartier divisor* $\Sigma[\phi(a)]$:

$$A \xrightarrow{\sim} \sum_{a \in A} [\phi(a)] .$$

We always have the implications

$$(3) \Longleftrightarrow (4) \Longleftrightarrow (5) \Longrightarrow (1) \Longrightarrow (2) ,$$

and, if $\#(A)$ *is invertible on* S, *then all of* (1), (2), (3), (4), (5) *are equivalent.*

(1.6) *General representability theorems for* A*-structures and* A*-generators*

(1.6.1) As before, C/S is a smooth commutative group-scheme over S of relative dimension one (cf. 1.4.1), and A is a fixed "abstract" finite abelian group. For every integer $N \geq 1$, we denote by $C[N]$ the S-subgroup-scheme of C/S of points of order N : for any S-scheme $T \to S$, we have

$$C[N](T) = \mathrm{Ker} \text{ of } N : C(T) \to C(T) .$$

Let us fix an isomorphism of abelian groups

(1.6.1.1) $$A \simeq \mathbf{Z}/N_1\mathbf{Z} \times \cdots \times \mathbf{Z}/N_r\mathbf{Z} .$$

Then the functor on S-schemes $Hom_{S\text{-gp}}(A,C)$ defined by

(1.6.1.2) $$T \mapsto \mathrm{Hom}_{gp}(A, C(T)) ,$$

is represented by the S-scheme of finite presentation

(1.6.1.3) $$C[N_1] \underset{S}{\times} C[N_2] \underset{S}{\times} \cdots \underset{S}{\times} C[N_r] .$$

PROPOSITION 1.6.2. *Hypotheses and notations as above, the functor* $A\text{-}Str(C/S)$ *on* S*-schemes*

$$T \mapsto \textit{the set of } A\textit{-structures on } C_T/T$$

is represented by a closed subscheme of $Hom_{S\text{-gp}}(A,C) \simeq C[N_1] \underset{S}{\times} \cdots \underset{S}{\times} C[N_r]$ *definable locally by* $1 + \#(A) + (\#(A))^2$ *equations.*

Proof. By definition, the functor $A\text{-}Str(C/S)$ is a sub-functor of the representable functor $Hom_{S\text{-gp}}(A,C)$. It is represented by the closed subscheme of $Hom_{S\text{-gp}}(A,C)$ over which the effective Cartier divisor of degree $\#(A)$ in $C \underset{S}{\times} Hom_{S\text{-gp}}(A,C)/Hom_{S\text{-gp}}(A,C)$

$$\sum_{a \in A} [\phi_{\mathrm{univ}}(a)] ,$$

attached to the universal homomorphism $\phi_{\mathrm{univ}} : A \to C$, is a subgroup. The asserted result now follows from (1.3.7). Q.E.D.

COROLLARY 1.6.3. *Let* N *be the exponent of the group* A. *If the* S*-morphism*

$$[N] : C \to C$$

is finite, then $A\text{-}Str(C/S)$ *is represented by a finite* S*-scheme of finite presentation.*

Proof. Then $C[N_1] \underset{S}{\times} \cdots \underset{S}{\times} C[N_r]$ is itself a closed sub-scheme of finite presentation of the finite S-scheme $C[N] \underset{S}{\times} \cdots \underset{S}{\times} C[N]$. Q.E.D.

PROPOSITION 1.6.4. *Hypotheses and notations as above, suppose that the exponent* N *of the group* A *is invertible on* S, [*and that the* S*-group* C[N] *is finite over* S]. *Then the* S*-scheme* A-*Str*(C/S) *is* [*finite*] *etale over* S (*possibly empty*!).

Proof. Because N is invertible on S, and C/S is smooth, the homomorphism

$$[N]: C \to C$$

is etale. Therefore C[N] is etale over S, [hence finite etale over S]. The functor A-*Str*(C/S) is known to be [finite over S] of finite presentation, so it suffices to check that it is formally etale. Thus let T be an S-scheme, $T_0 \subset T$ a closed subscheme defined by a nilpotent ideal, and

$$\phi_0: A \to C(T_0)$$

an A-structure on C_{T_0}/T_0. We must show that ϕ_0 extends *uniquely* to a homomorphism

$$\phi: A \to C(T)$$

which defines an A-structure on C_T/T. To see this, we argue as follows. Because A has exponent N, ϕ_0 automatically factors through C[N]:

$$\phi_0: A \to C[N](T_0) .$$

Because C[N] is etale over S, ϕ_0 extends uniquely to a homomorphism

$$\phi: A \to C[N](T) .$$

To see that this ϕ defines an A-structure on C_T/T, it suffices, N being invertible, to test after pulling back to each geometric point of T. But T and T_0 have precisely the same geometric points, and at each of

them $(\phi)_k$ is none other than $(\phi_0)_k$, which by hypothesis is an A-structure on C_k/k. Q.E.D.

PROPOSITION 1.6.5. *Hypotheses and notations as above, let* $G \subset C$ *be a closed* S*-subgroup-scheme of* C *which is finite locally-free over* S *of* rank = #(A). *The functor* A-*Gen*(G/S) *on* S*-schemes defined by*

$$T \mapsto \textit{the set of A-generators of the subgroup } G_T \textit{ in } C_T/T$$

is represented by a finite S*-scheme of finite presentation, which is a closed subscheme of the finite* S*-scheme of finite presentation* $Hom_{S\text{-gp}}(A,G)$, *defined locally by* #(A) *equations.*

Proof. A group homomorphism $\phi: A \to C(S)$ is an A-generator of G if and only if the following two conditions are satisfied:

(1) ϕ maps A to the subgroup G(S) of C(S).

(2) We have an equality of Cartier divisors $G = \sum_{a \in A} [\phi(a)]$. Therefore

A-Gen(G/S) is represented by the closed subscheme of $Hom_{S\text{-gp}}(A,G)$ over which the effective Cartier divisor D_{univ} in $C \underset{S}{\times} Hom_{S\text{-gp}}(A,G)$ over $Hom_{S\text{-gp}}(A,G)$ associated to $\phi_{univ}: A \to G$

$$D_{univ} = \sum_{a \in A} [\phi_{univ}(a)]$$

satisfies

$$D_{univ} = G .$$

The S-scheme $Hom_{S\text{-gp}}(A,G)$ is itself a finite S-scheme of finite presentation, being none other than $G[N_1] \underset{S}{\times} \cdots \underset{S}{\times} G[N_r]$. The result now follows from 1.3.5. Q.E.D.

REMARK 1.6.6. The notation "A-*Gen*(G/S)" makes no reference to the ambient C/S, although the definition of an A-generator for G very much involves the ambient space, as the space in which the equality

$$G = \sum_{a \in A} [\phi(a)]$$

of Cartier divisors takes place. We will see later (sections 1.9 ff.) that there is in fact an *intrinsic* notion of an A-generator for a finite locally-free commutative group-scheme G/S which coincides with above notion whenever G is embeddable as a subgroup of a smooth one-parameter group C/S.

PROPOSITION 1.6.7. *Hypotheses and notations as in the preceding proposition, if* G *is finite etale over* S *(e.g., if its rank is invertible on* S*), then the functor* A-Gen(G/S) *is represented by a finite etale* S*-scheme.*

Proof. Just as in the proof of (1.6.4), it suffices to show that the functor A-Gen(G/S) is formally etale over S. But for G etale over S, this is none other than the functor $Isom_{S\text{-gp}}(A,G)$, which for any two etale S-groups is itself formally etale over S. Q.E.D.

(1.7) *Factorization into prime powers of* A*-structures and* A*-generators*

(1.7.1) Let A_1 and A_2 be finite abelian groups, of orders N_1 and N_2 respectively. Let $A = A_1 \times A_2$, and denote its order by $N = N_1 N_2$. Given any abelian group B, and any group homomorphism

(1.7.1.1) $$\phi : A \to B$$

there are unique group homomorphisms

(1.7.1.2) $$\phi_i : A_i \to B, \quad i = 1,2,$$

such that

(1.7.1.3) $$\phi(a_1, a_2) = \phi_1(a_1) + \phi_2(a_2).$$

PROPOSITION 1.7.2. *Suppose that* N_1 *and* N_2 *are relatively prime. Let* C/S *be a smooth commutative* S*-group of relative dimension one*

(cf. 1.4.1). Then a homomorphism

$$\phi : A \to C(S)$$

is an A*-structure on* C/S *if and only if the two homomorphisms*

$$\phi_i : A_i \to C(S), \quad i = 1,2,$$

are each A_i*-structures,* $i = 1,2$, *on* C/S. *If this is the case, then the groups* G, G_1, G_2 *generated by* ϕ, ϕ_1, ϕ_2 *respectively are related by* $G = G_1 \underset{S}{\times} G_2$.

Proof. Suppose first that ϕ an A-structure on C/S. Let $G \subset C$ be the A-subgroup generated by ϕ. Then G is finite locally-free over S of rank $N = N_1 N_2$. Because G is killed by N, and $N = N_1 N_2$ with N_1 and N_2 relatively prime, we have a canonical product decomposition (as abelian group valued functors on S-schemes)

$$G \xleftarrow{\sim} G[N_1] \underset{S}{\times} G[N_2].$$

Then $G[N_1]$ and $G[N_2]$ are finite locally-free over S of ranks N_1 and N_2 respectively. To see this, notice first that $G[N_1]$ is representable by a closed subscheme of G which is of finite presentation over S, simply because $G[N_1]$ is the kernel of an S-homomorphism $([N_1] : G \to G)$ between S-group-schemes of finite presentation. Because G is finite over S, $G[N_1]$ is a finite S-scheme of finite presentation. Because $N = N_1 N_2$ with N_1 and N_2 relatively prime, $G[N_1]$ is a direct factor of G, corresponding to the S-projector on G

$$P_1 + P_2 \mapsto P_1 .$$

Therefore the sheaf of S-algebras defining $G[N_1]$ is an S-direct factor of that defining G, so flat over S. Therefore $G[N_1]$ is finite flat over S of finite presentation. By (EGA IV, 8.9.1 and 11.2.6.1) we may reduce to the case S noetherian to conclude that $G[N_1]$ is finite locally free over

S. Similarly $G[N_2]$ is finite locally free over S. To show that $G[N_1]$ and $G[N_2]$ are locally free of the asserted ranks N_1 and N_2, respectively, it suffices to treat the case when S is Spec(k) with k an algebraically closed field. The product decomposition

$$G[N_1] \underset{S}{\times} G[N_2] \xrightarrow{\sim} G$$

shows that

$$\text{rank}(G[N_1]) \cdot \text{rank}(G[N_2]) = \text{rank}(G) = N_1 N_2 .$$

Because $G[N_i]$ is killed by N_i, the rank of $G[N_i]$ divides a power of N_i (cf. [De-Ga IV, §3, 5.3-9]). Therefore the above product-formula for ranks forces $\text{rank}(G[N_i]) = N_i$, as required.

Because N_1 and N_2 are relatively prime, we may, localizing on S assume one of them, say N_1, is invertible on S. Then $G[N_1]$ is finite etale over S, of rank N_1.

We first show that $\phi_1 = \phi|A_1$ is an A_1-structure on C/S, and that it A_1-generates $G[N_1]$. To show that ϕ_1 is an A_1-structure, it suffices by (1.5.3) to show that for every geometric point Spec(k) $\to$ S of S, the N_1 points $\{\phi(a_1)_k\}$, $a_1 \in A_1$, are all distinct in G(k). To see this, notice that because N_1 is invertible in k we have

$$\begin{aligned} G(k) &= G[N_1](k) \times G[N_2](k) \\ &= (\text{a group of order } N_1) \times (\text{a group killed by } N_2). \end{aligned}$$

Therefore G(k) contains precisely N_1 distinct points killed by N_1. But the expression of G as a Cartier divisor

$$G = \sum_{a_1, a_2} [\phi(a_1) + \phi(a_2)]$$

shows that the group G(k) is exhausted by the points

$$\{\phi(a_1)_k + \phi(a_2)_k\}, \quad a_1 \in A_1, \quad a_2 \in A_2 .$$

But of these points, only those for which $\phi(a_2)_k = 0$ are killed by N_1. Therefore the N_1 points

$$\{\phi(a_1)_k\}, \quad a_1 \in A_1$$

must exhaust the point killed by N_1 in G(k). Therefore these N_1 points are all distinct. This shows that ϕ_1 is an A_1-structure on C/S. The map $\phi_1 : A_1 \to G$ clearly factors through $G[N_1]$, inducing

$$\phi_1 : A_1 \to G[N_1] .$$

It remains to show that this last map is an isomorphism. As its source and target are finite flat of the same rank N_1 over S, it suffices to check that for every geometric point Spec(k) $\to$ S of S, the induced map on k-valued points is bijective. But it is precisely this bijectivity

$$\phi_1 : A_1 \xrightarrow{\sim} G(k)[N_1]$$

which was established above.

We next must show that $\phi_2 = \phi|A_2$ is an A_2-structure on C/S, and that it A_2-generates $G[N_2]$. We have already proved that ϕ_1 defines an isomorphism

$$\phi_1 : A_1 \xrightarrow{\sim} \sum_{a_1 \in A_1} [\phi_1(a_1)] = G[N_1] .$$

Let us denote by D_2 the effective Cartier divisor in C/S defined by

$$D_2 = \sum_{a_2 \in A_2} [\phi(a_2)] .$$

Then the decomposition

$$G = \sum [\phi(a_1) + \phi(a_2)]$$

may be rewritten

$$G = \sum_{a_1 \epsilon A_1} \mathrm{Trans}(\phi(a_1))^*(D_2) ,$$

a decomposition in which the N_1 translates of D_2 which occur are everywhere disjoint (say as sub-functors of C/S on S-schemes). Therefore as an S-scheme, G is isomorphic to the disjoint union,

$$G \simeq \coprod_{a_1 \epsilon A_1} \mathrm{Trans}(\phi(a_1))^*(D_2) .$$

We must show that $G[N_2] = D_2$. Because both sides have the same degree, it suffices to show that $G[N_2] \leq D_2$. For this, it suffices to show that for any point $P \epsilon G[N_2](T)$, with T any connected S-scheme, we have $P \epsilon D_2(T)$. Certainly $P \epsilon G(T)$, and, because T is connected, the disjoint union expression of G shows that

$$G(T) = \coprod_{a_1 \epsilon A_1} \mathrm{Trans}(\phi(a_1))^*(D_2(T)) .$$

In other words, there is an element $a_1 \epsilon A_1$ such that

$$P - \phi(a_1) = \text{an element of } D_2(T) .$$

We must show that $\phi(a_1) = 0$. For this, it suffices to make the change of base to any geometric point $\mathrm{Spec}(k) \to T$ of T. Then we find

$$P_k - \phi(a_1)_k = \text{an element of } D_2(k) = \phi(a_2)_k \text{ for some } a_2 \epsilon A_2 .$$

As both P_k and $\phi(a_2)_k$ are killed by N_2, while $\phi(a_1)$ is killed by N_1, this is impossible unless $\phi(a_1) = 0$.

We now prove the converse. We are given

$$\phi : A \to C(S)$$

such that $\phi_i = \phi | A_i$ is an A_i-structure, $i = 1, 2$, on C/S. We must show

that ϕ is an A-structure. Because $N = N_1 N_2$ with N_1 and N_2 relatively prime, we may, by localizing on S, suppose that one of N_1 and N_2, say N_1, is invertible on S. Let $G_i \subset C$ be the A_i-subgroup generated by ϕ_i, for $i = 1, 2$. Because N_1 is invertible on S, we know that ϕ_1 defines an S-group isomorphism

$$\phi_1 : A_1 \xrightarrow{\sim} G_1 .$$

Because G_1 and G_2 have relatively prime ranks, the sum map defines a closed immersion

$$G_1 \underset{S}{\times} G_2 \hookrightarrow C ;$$

whose image G is the disjoint union of the N_1 translates of G_2 by the given sections of G_1 :

$$G_1 \underset{S}{\times} G_2 \xrightarrow{\sim} G = \coprod_{a_1 \epsilon A_1} \mathrm{Trans}(\phi(a_1))^*(G_2) .$$

Because these translates are everywhere disjoint in C/S, their union in C is just their *sum* as Cartier divisors, so that

$$G_1 \underset{S}{\times} G_2 \xrightarrow{\sim} G = \sum_{a_1 \epsilon A_1} \mathrm{Trans}(\phi(a_1))^*(G_2) .$$

By hypothesis on ϕ_2 we have an equality of Cartier divisors in C/S,

$$G_2 = \sum_{a_2 \epsilon A_2} [\phi(a_2)] ,$$

so that we find

$$G_1 \underset{S}{\times} G_2 \xrightarrow{\sim} G = \sum_{a_1 \epsilon A_1, a_2 \epsilon A_2} [\phi(a_1) + \phi(a_2)]$$

$$= \sum_{a \epsilon A} [\phi(a)] ,$$

as required. Q.E.D.

COROLLARY 1.7.3. *Let* A *be a finite abelian group,* N *its order,*

$$N = \prod_{i=1}^{r} p_i^{n_i}$$

the factorization of N *as a product of powers of distinct primes, and*

$$A = A_1 \times \cdots \times A_r$$

the corresponding decomposition of A *into the product of its* p_i*-primary subgroups* A_i. *Let* C/S *be a smooth commutative group-scheme of relative dimension one (cf. 1.4.1). Then the decomposition* $A = \prod A_i$ *defines a canonical isomorphism of* S*-schemes*

$$A\text{-}Str(C/S) \xrightarrow{\sim} A_1\text{-}Str(C/S) \underset{S}{\times} \cdots \underset{S}{\times} A_r\text{-}Str(C/S) .$$

For any closed S*-subgroup-scheme* $G \subset C/S$ *which is finite and flat over* S *of finite presentation and rank* N, *let*

$$G = G_1 \underset{S}{\times} \cdots \underset{S}{\times} G_r, \quad G_i \overset{dfn}{=\!=} G[p_i^{n_i}]$$

be the canonical factorization of G *into its* p*-primary components. Then we have a canonical isomorphism of* S*-schemes*

$$A\text{-}Gen(G/S) \xrightarrow{\sim} A_1\text{-}Gen(G_1/S) \underset{S}{\times} \cdots \underset{S}{\times} A_r\text{-}Gen(G_r/S) .$$

(1.8) *Full sets of sections*

(1.8.1) Let S be a scheme, and Z/S a finite flat S-scheme of finite presentation and rank $N \geq 1$. The standard reduction to the noetherian case (by EGA IV, 8.9.1 and 11.2.6.1) shows that, equivalently, Z/S is finite locally free over S of rank $N \geq 1$. This means that for every affine S-scheme $\mathrm{Spec}(R) \to S$, the R-scheme Z_R/R obtained from Z/S by change of base is of the form $\mathrm{Spec}(B)$, where B is an R-algebra which

as an R-module is locally free of rank N. Any element $f \in B$ acts by multiplication to define an R-linear endomorphism of B. Because B is a locally free R-module of rank N, we can speak of the characteristic polynomial of this endomorphism,

(1.8.1.1) $\det(T-f) = T^N - \mathrm{trace}(f)T^{N-1} + \cdots + (-1)^N \mathrm{Norm}(f)$,

which is a monic polynomial in R[T] of degree N.

(1.8.2) We say that a set of N not-necessarily-distinct points $P_1, \cdots, P_N$ in Z(S) is a "full set of sections of Z/S" if either of the two following equivalent conditions is fulfilled:

(1) For every affine S-scheme $\mathrm{Spec}(R)$, and for every function f on Z_R, i.e., for every $f \in B = H^0(Z_R, \mathcal{O})$, we have the equality of characteristic polynomials in R[T]

$$\det(T-f) = \prod_{i=1}^{N} (T - f(P_i)) .$$

(2) For every affine S-scheme $\mathrm{Spec}(R)$, and for every function f on Z_R, we have the equality in R

$$\mathrm{Norm}(f) = \prod_{i=1}^{N} f(P_i) .$$

To see that (1) and (2) are equivalent, we argue as follows. We have the implication

(1) for $(R, f) \Rightarrow$ (2) for (R, f)

simply by putting $T = 0$ in (1), and we have the implication

(1) for $(R, f) \Leftarrow$ (2) for $(R[T], T-f)$

simply because the characteristic polynomial of $f \in B$ is just the norm of $T-f$ relative to $B \underset{R}{\otimes} R[T]/R[T]$.

LEMMA 1.8.3. *Let* Z/S *be a finite etale* S*-scheme of rank* N, *and* $P_1, \cdots, P_N \in Z(S)$. *Then the following conditions are equivalent.*

(1) *The* S*-morphism*

$$\underbrace{S \amalg S \amalg \cdots \amalg S}_{N\text{-fold disjoint union}} \to Z$$

defined by the N*-sections* $P_1, \cdots, P_N$ *is an isomorphism of* S*-schemes. If* S *is connected, this is equivalent to saying that the set* Z(S) *consists of* N *elements, and that these elements are* $P_1, \cdots, P_N$.

(2) $P_1, \cdots, P_N$ *form a full set of sections of* Z/S.

(3) *For every geometric point of* S, Spec(k) → S, *the* N *points* $(P_i)_k \in Z(k)$ *are all distinct.*

Proof. Trivially (3) ⟺ (1) ⟹ (2). To prove (2) ⟹ (3), we may reduce to the case when S is the spectrum of an algebraically closed field k. Then Z is just N distinct reduced points over k, say $Q_1, \cdots, Q_N$. We must show that $P_1, \cdots, P_N$ exhaust these N points, i.e., that $P_1, \cdots, P_N$ are all distinct. Let f be any function on Z which takes N distinct values on $Q_1, \cdots, Q_N$; by hypothesis, its characteristic polynomial is given by

$$\prod (T - f(Q_i)) \overset{\text{dfn}}{=\!=} \det(T - f) = \prod (T - f(P_i)) .$$

Therefore the N values $f(P_i)$ are all distinct, and therefore the P_i are all distinct. Q.E.D.

LEMMA 1.8.4. *Let* Z_1 *and* Z_2 *be two finite flat* S*-schemes of finite presentation, and ranks* N_1 *and* N_2 *respectively. Let*

$$\begin{cases} P_1^{(1)}, \cdots, P_{N_2}^{(1)} \in Z_1(S) \\ P_1^{(2)}, \cdots, P_{N_2}^{(2)} \in Z_2(S) \end{cases}$$

be given sequences of N_i *points in* $Z_i(S)$, *for* i = 1,2. *The following conditions are equivalent*

(1) *For* i = 1,2, *the* N_i S*-valued points* $P_1^{(i)}, \cdots, P_{N_i}^{(i)}$ *form a full set of sections of* Z_i/S.

(2) *The* N_1+N_2 S*-valued points* $\{P_1^{(1)}, \cdots, P_{N_1}^{(1)}, P_1^{(2)}, \cdots, P_{N_2}^{(2)}\}$ *of the disjoint union* $Z_1 \amalg Z_2$ *form a full set of sections of* $(Z_1 \amalg Z_2)/S$.

Proof. Locally on S, we have S = Spec(R), and Z_i = Spec(B_i) whose B_i is an R-algebra which as R-module is free of rank N_i for i = 1,2. Then $Z_1 \amalg Z_2$ is Spec($B_1 \oplus B_2$). For any element

$$f = f_1 \oplus f_2 \quad \text{in} \quad B_1 \oplus B_2 ,$$

we have

$$\text{Norm}(f) = \text{Norm}(f_1)\,\text{Norm}(f_2) .$$

For any of the N_1+N_2 points $P_j^{(i)}$, we have

$$f(P_j^{(i)}) = f_i(P_j^{(i)}) .$$

To show (1) ⇒ (2), write $f = f_1 \oplus f_2$ to compute Norm(f). To show (2) ⇒ (1), say for Z_1, notice that for $f_1 \in B_1$, we have

$$\text{Norm}(f_1) = \text{Norm}(f_1 \oplus 1) ,$$

and then use (2) to compute Norm($f_1 \oplus 1$). Q.E.D.

LEMMA 1.8.5. *Let* Z_1/S *and* Z_2/S *be two** *finite flat* S*-schemes of finite presentation, and ranks* N_1 *and* N_2 *respectively. Let*

$$P_1^{(1)}, \cdots, P_{N_1}^{(1)} \in Z_1(S)$$

$$P_1^{(2)}, \cdots, P_{N_2}^{(2)} \in Z_2(S)$$

be given sequences of N_i *points in* $Z_i(S)$, *for* i = 1,2. *Suppose that* Z_1/S *is finite etale. Then the following conditions are equivalent:*

* non-empty.

(1) *For* $i = 1,2$, *the* N_i *points* $P_1^{(i)}, \cdots, P_{N_i}^{(i)}$ *in* $Z_i(S)$ *form a full set of sections of* Z_i/S.

(2) *The* $N_1 \times N_2$ *S-valued points* $P_j^{(1)} \times P_k^{(2)}$ *of* $Z_1 \times_S Z_2$ *form a full set of sections of* $Z_1 \times_S Z_2$.

Proof. To see that (1) ⇒ (2), notice that (1) for Z_1 insures that the $P_j^{(1)}$'s define an S-isomorphism

$$S \amalg \cdots \amalg S \xrightarrow{\sim} Z_1 ,$$

whence an S-isomorphism

$$Z_2 \amalg \cdots \amalg Z_2 \xrightarrow{\sim} Z_1 \times_S Z_2 .$$

The result now follows from (1.8.4).

It remains to prove (2) ⇒ (1). We first show that (1) holds for Z_1/S. For this, it suffices to treat the case when $S = \operatorname{Spec}(k)$ with k algebraically closed. Consider the function $f_1 \otimes 1$ on $Z_1 \times_S Z_2$. Its characteristic polynomial is given by

$$\det(T - f_1 \otimes 1) = (\det(T-f_1))^{N_2} ,$$
$$\| $$
$$\left(\prod_{j=1}^{N_1} (T - f_1(P_j^{(1)})) \right)^{N_2} ,$$

the vertical equality in virtue of (2). Therefore we may infer

$$\det(T-f_1) = \prod_{j=1}^{N_1} (T - f_1(P_j^{(1)})) ,$$

since both sides are monic polynomials in $k[T]$. As this holds for any function f_1 on Z_1, it follows that the $P_j^{(1)}$'s are a full set of sections for Z_1/k (compare the proof of (1.8.3)).

Once we know that the $P_j^{(1)}$'s are a full set of sections Z_1/S, we have as before an S-isomorphism

$$S \amalg \cdots \amalg S \xrightarrow{\sim} Z_1 ,$$

whence

$$Z_2 \amalg \cdots \amalg Z_2 \xrightarrow{\sim} Z_1 \times_S Z_2 ,$$

defined by the sections $P_j^{(1)}$ of Z_1/S. It now follows from (1.8.4) that for *each* $1 \le j \le N_1$, the N_2 points $P_j^{(1)} \times P_k^{(2)}$, $k = 1, \cdots, N_2$, are a full set of sections of $S \times_S Z_2 \xrightarrow{\sim} Z_2$, i.e., the points $P_k^{(2)}$, $k = 1, \cdots, N_2$ are a full set of sections of Z_2/S. Q.E.D.

When we drop the hypothesis that Z_1 be etale over S, we have only (1) ⇒ (2). More precisely, we have:

LEMMA 1.8.6. *Let* Z_1/S *and* Z_2/S *be two finite flat S-schemes of finite presentation, and ranks* N_1 *and* N_2 *respectively. Suppose that for* $i = 1,2$, *we are given sequences of* N_i *S-valued points of* Z_i:

$$P_1^{(i)}, \cdots, P_{N_i}^{(i)} \in Z_i(S) \quad \textit{for} \quad i = 1,2 ,$$

which are full sets of sections of Z_i/S *for* $i = 1,2$. *Then the* $N_1 \times N_2$ *S-valued points* $P_j^{(1)} \times P_k^{(2)}$ *of* $Z_1 \times_S Z_2$ *form a full set of sections of* $Z_1 \times_S Z_2/S$.

Proof. The points $P_j^{(1)}$ being a full set of sections of Z_1/S, they remain a full set of sections after any change of base $T \to S$ of the resultant situation $Z_1 \times_S T/T$. Taking for $T \to S$ the scheme $Z_2 \to S$, we see that the $P_j^{(1)}$'s give a full set of sections of $Z_1 \times_S Z_2/Z_2$. The assertion now results from the transitivity of the norm in the tower

$$\begin{array}{c} Z_1 \underset{S}{\times} Z_2 \\ \downarrow \\ Z_2 \\ \downarrow \\ S\ . \end{array}$$

Q.E.D.

(1.9) *Intrinsic A-structures and A-generators*

PROPOSITION 1.9.1. *Let Z/S be a finite flat S-scheme of finite presentation and rank $N \geq 1$. Let $P_1, \cdots, P_N \in Z(S)$ be a set of N not-necessarily-distinct S-valued points of Z. There exists a unique closed subscheme W of S which is universal for the relation "$P_1, \cdots, P_N$ are a full set of sections of Z/S" in the sense that for any S-scheme $T \to S$, the induced points $P_{1,T}, \cdots, P_{N,T} \in Z(T)$ are a full set of sections of Z_T/T if and only if the morphism $T \to S$ factors through W. Locally on S, W is defined by finitely many equations.*

Proof. The question is Zariski local on S, which we may therefore suppose affine, $S = \mathrm{Spec}(R)$. Further localizing on S, we may suppose that $Z = \mathrm{Spec}(B)$ where B is an R-algebra which as an R-module is free of rank N. Let $b_1, \cdots, b_N$ be an R-basis of B. Then the "universal" element $f \in B$ is the element

$$f = \sum T_i b_i \in B \underset{R}{\otimes} R[T_1, \cdots, T_N]\ .$$

The points $P_1, \cdots, P_N$ form a full set of sections of $\mathrm{Spec}(B)/R$ if and only if this universal f satisfies

$$\mathrm{Norm}(f) = \prod f(P_i) \quad \text{in} \quad R[T_1, \cdots, T_N]\ ,$$

i.e., if and only if we have

$$\mathrm{Norm}\left(\sum T_i b_i\right) = \prod_{j=1}^{N} \left(\sum T_i b_i(P_j)\right)\ ,$$

equality inside $R[T_1, \cdots, T_N]$. Both sides of this identity are homogeneous forms of degree N in the variables $T_1, \cdots, T_N$. The required closed subscheme $W \subset \mathrm{Spec}(R)$ is the one defined by the ideal in R generated by the $\binom{2N-1}{N}$ coefficients of the *difference* of these two homogeneous forms. Q.E.D.

COROLLARY 1.9.2. *Hypotheses and notations as above, suppose that S is reduced. Then in order that $P_1, \cdots, P_N$ form a full set of sections of Z/S, it is necessary and sufficient that for every geometric point $\mathrm{Spec}(k) \to S$ of S, the following condition be satisfied:*

> *For every function f in the affine algebra $B \otimes k$ of Z_k/k, we have the equality in k*
>
> $$\mathrm{Norm}(f) = \prod_{i=1}^{N} f((P_i)_k)\ .$$

Proof. The condition is clearly necessary. To see that it is sufficient, we may suppose $S = \mathrm{Spec}(R)$ with R reduced, and $Z = \mathrm{Spec}(B)$ with B an R-algebra which is a free R-module of rank N, say with basis $b_1, \cdots, b_N$. We must show that

$$\mathrm{Norm}\left(\sum T_i b_i\right) = \prod_{j=1}^{N} \left(\sum T_i b_i(P_j)\right)\ .$$

in the ring $R[T_1, \cdots, T_N]$, which by hypothesis is reduced. To show this, it suffices to check equality of values at all geometric points of $\mathrm{Spec}(R[T_1, \cdots, T_N])$, i.e., to check that for any homomorphism $R \to k$ and any N-tuple $(a_1, \cdots, a_N) \in k^N$, the function $f = \Sigma\, a_i (b_i \underset{R}{\otimes} 1)$ satisfies the identity

$$\mathrm{Norm}(f) = \prod_{i=1}^{N} f((P_i)_k)\ .$$

Q.E.D.

(1.10) *Relation to Cartier divisors*

THEOREM 1.10.1. *Let* S *be a scheme,* C/S *a smooth curve (cf. 1.2.1) and* $Z \hookrightarrow C$ *a closed subscheme which is finite flat over* S *of finite presentation, and of rank* $N \geq 1$. *Let* $P_1,\cdots,P_N$ *be a set of* N *not-necessarily distinct points of* C(S). *Then the following conditions are equivalent*:

(1) *We have an equality of effective Cartier divisors in* C/S

$$Z = \sum_{i=1}^{N} [P_i] .$$

(2) *The points* $P_1,\cdots,P_N$ *all lie in the subset* Z(S) *of* C(S), *and they are a "full set of sections" of* Z/S.

Proof. A standard reduction reduces us to treating the case when $S = \mathrm{Spec}(R)$ with R an artin local ring with algebraically closed residue field k. Let $z_1,\cdots,z_r$ denote the distinct points of Z(k). Then we have a canonical decomposition of Z into a disjoint union

$$Z = \coprod_{j=1,\cdots,r} Z_j$$

where Z_j is the completion of Z along z_j. Because Spec(R) is connected, we have a disjoint union decomposition

$$Z(R) = \coprod_{j=1,\cdots,r} Z_j(R) .$$

Under either of the conditions (1), (2) to be proven equivalent, the points $P_1,\cdots,P_N$ all lie in Z(R). Therefore we may partition them according to which subset $Z_j(R)$ of Z(R) they lie in, say

$$P_1^{(j)},\cdots,P_{n(j)}^{(j)} \quad \text{lie in} \quad Z_j, \quad j = 1,\cdots,r .$$

One verifies easily that in this situation of disjointness, each of the conditions (1), (2) holds for Z and $P_1,\cdots,P_N$ if and only if it holds for the r situations (Z_j and $P_1^{(j)},\cdots,P_{n(j)}^{(j)}$), $j = 1,\cdots,r$.

Therefore it suffices to treat the case where Z is itself local, concentrated at $z = z_1 \in Z(k) \subset C(k)$. Let $\hat{\mathcal{O}}_{C,z}$ denote the complete local ring of C at z. In terms of a choice of uniformizing parameter X at z, we obtain a noncanonical isomorphism

$$\hat{\mathcal{O}}_{C,z} \xrightarrow{\sim} R[[X]] .$$

By Weierstrass preparation the effective Cartier divisor Z of degree N is defined inside Spec(R[[X]]) by a unique monic equation F(X) of degree N, all of whose lower coefficients lie in the maximal ideal of R

$$\begin{aligned} Z &\simeq \mathrm{Spec}(R[[X]]/(F(X))) \\ &\simeq \mathrm{Spec}(R[X]/(F(X))) \\ F(X) &= X^N + (\text{lower terms with coefficients in } \max(R)) . \end{aligned}$$

The effective Cartier divisor in C/R

$$\sum [P_i]$$

is also concentrated at z; it is defined inside Spec(R[[X]]) by the monic polynomial G(X) of degree N defined by

$$G(X) = \prod_{i=1}^{N} (X - X(P_i)) .$$

All of the lower coefficients of G lie in max(R), because each $X(P_i) \in R$ is a root of F and so must lie in max(R).

Because the effective Cartier divisors Z and $\Sigma[P_i]$ are both supported at $z \in C$, they are equal in C/R if and only if they are equal inside Spec(R[[X]]). Thus (1) is equivalent to the equality of monic polynomials

$$F(X) = \prod_{i=1}^{N} (X - X(P_i)) .$$

Because Z is the finite free R-scheme

$$Z = \mathrm{Spec}(R[X]/(F(X))) ,$$

we are reduced to treating the case $S = \mathrm{Spec}(R)$, $C = \mathrm{Spec}(R[X])$, and Z is defined by a monic polynomial $F(X)$ of degree N. Let $a_i = X(P_i)$ for $i = 1, \cdots, N$. The assertion amounts to the following.

LEMMA 1.10.2. *Let R be a ring, $F(X) \in R[X]$ a monic polynomial of degree $N \geq 1$, and $a_1, \cdots, a_N$ elements of R. Let B denote the R-algebra $R[X]/(F(X))$. Then the following two conditions are equivalent:*

(1) *We have the factorization*

$$F(X) = \prod_{i=1}^{N} (X - a_i) .$$

(2) *For every $f \in B$, we have the factorization*

$$\det(T - f) = \prod_{i=1}^{N} (T - f(a_i)) .$$

Proof. To see that (2) $\Rightarrow$ (1), notice that for $R[X]/(F(X))$ we have the identity

$$\det(T - X) = F(T) .$$

Therefore if (2) holds for $f = X$, we obtain

$$\prod_{i=1}^{N} (T - a_i) = F(T) ,$$

as required. To prove (1) $\Rightarrow$ (2), we may reduce to the universal case

$$R = Z[A_1, \cdots, A_N, B_0, \cdots, B_{N-1}]$$

$$(a_1, \cdots, a_N) = (A_1, \cdots, A_N)$$

$$F(X) = \prod_{i=1}^{N} (X - A_i)$$

$$f = \sum_{i=0}^{N-1} B_i X^i ,$$

in which the A's, B's are independent variables. As it is enough to verify that (2) holds after any injective extension of scalars $R \hookrightarrow R'$, we may pass to the fraction field of R and thus reduce to the case in which R is a field and $a_1, \cdots, a_N$ are all distinct. Then we have an algebra isomorphism

$$R[X]/\left(\prod (X - a_i)\right) \xrightarrow{\sim} \prod_{i=1}^{N} R[X]/(X - a_i) ,$$

which makes (1) $\Rightarrow$ (2) obvious.

COROLLARY 1.10.3. *Let S be a scheme, Z/S a finite flat S-scheme of finite presentation, and $P_1, \cdots, P_r \in Z(S)$. Suppose that Z/S is embeddable as a closed subscheme of a smooth curve C/S (cf. 1.2.1). Then there is at most one closed subscheme $W \hookrightarrow Z$ such that both of the following conditions hold:*

(a) *W/S is locally free over S of rank r.*

(b) *$P_1, \cdots, P_r \in W(S)$, and they form a "full set of sections" of W/S.*

This W exists if and only if, locally f.p.p.f. on S, $P_1, \cdots, P_r$ can be completed to a full set of sections $P_1, \cdots, P_r, P_{r+1}, \cdots, P_n$ of Z/S. Furthermore, there is a closed subscheme of S, defined locally by finitely many equations, which is universal for the existence of this W.

Proof. Inside C/S, form $W' = \Sigma [P_i]$. Then if W exists, it is none other than W', and the closed subscheme of S over which W exists is pre-

cisely the locus $W' \leq Z$. The condition $W' \leq Z$ inside C is equivalent to the possibility, locally f.p.p.f. on S, of extending $P_1, \cdots, P_r$ to a full set $P_1, \cdots, P_r, P_{r+1}, \cdots, P_n$ of sections of Z/S. Q.E.D.

REMARK 1.10.4. This "uniqueness of W" is false without the "embeddable in a curve" hypothesis. For example, take Z to be $\alpha_p \times \alpha_p$. Then the p points $0, \cdots, 0$, form a full set of sections of any of the p^1 of α_p's sitting inside $\alpha_p \times \alpha_p$.

(1.10.5) Now let G/S be a finite flat S-group-scheme of finite presentation, and rank $N \geq 1$. Let A be a finite abelian "abstract" group of order N. We say that a group homomorphism

$$\phi : A \to G(S) \tag{1.10.5.1}$$

is an A-generator of G/S if the N points $\{\phi(a)\}$, $a \in A$ are a "full set of sections" of G/S.

It results immediately from the preceding corollary that this notion of A-generator is compatible with the previous one. Explicitly, we have

PROPOSITION 1.10.6. *Let C/S be a smooth commutative group-scheme over S of relative dimension one (cf. 1.4.1). Let $G \subset C$ be a closed S-subgroup-scheme which is finite flat over S of rank N, and of finite presentation. Let A be a finite "abstract" abelian group of order N, and let*

$$\phi : A \to C(S)$$

be a group homomorphism. Then the following conditions are equivalent:

(1) ϕ is an A-structure on C/S, and it A-generates G/S in the sense of (1.5.1).

(2) ϕ maps A to the subgroup $G(S) \subset C[N](S)$, and the homomorphism $\phi : A \to G(S)$ is an A-generator of G/S in the sense of (1.10.5).

As an immediate corollary, we obtain

COROLLARY 1.10.7. *Let C/S be a smooth commutative group-scheme over S of relative dimension one, and of finite presentation. Let $N \geq 1$ be an integer, and let A be a finite abelian "abstract" group of order N. Then there is a natural functorial bijection,*

$$\{\text{A-structures on } C/S\}$$
$$\updownarrow$$
$$\{\text{A-structures on } C[N]/S\},$$

which we define to mean pairs (G, ϕ) consisting of

(1) a closed S-subgroup-scheme $G \subset C[N]$ which is finite flat over S of finite presentation and of rank $= N$

(2) an A-generator ϕ of G/S in the sense of (1.10.5).

In particular, the notion of A-structure on C/S may be described entirely in terms of the S-group-scheme $C[N]$.

COROLLARY 1.10.8. *Suppose that C/S and C'/S are two smooth commutative group-schemes over S of relative dimension one (cf. 1.4.1). Suppose that for some integer $N \geq 1$, we have an isomorphism of S-groups*

$$C[N] \xrightarrow{\sim} C'[N].$$

Then via (1.10.7) above we have an induced isomorphism of S-schemes

$$A\text{-}Str(C/S) \xrightarrow{\sim} A\text{-}Str(C'/S)$$

for any finite abelian "abstract" group A of order N.

Proof. This results immediately from the description of A-structures in terms of data involving only the N-division points. Q.E.D.

COROLLARY 1.10.9. *With the hypotheses and notations of (1.10.7) above, suppose in addition that the group-scheme $C[N]$ is finite and flat over S. Let*

$$\phi : A \to C[N](S)$$

be a group homomorphism. Then

(1) If there exists a closed S-subgroup-scheme $G \subset C[N]$ such that (G, ϕ) is an A-structure on $C[N]/S$, then G is unique.

(2) *There exists a closed subscheme of* S, *defined locally by finitely many equations, which is universal for the existence of this* G.

Proof. Inside C/S, consider the Cartier divisor $W = \Sigma\,[\phi(a)]$, the sum over the N elements $a \in A$. Then as Cartier divisors in C/S, we must have $G = W$. This gives uniqueness of G, and G exists if and only if we first have $W \leq C[N]$ and if, secondly, this W inside C[N] is a subgroup-scheme. As these conditions are successively defined, locally on S, by finitely many equations, we get the second assertion as well. Q.E.D.

REMARK 1.10.10. Analogously, given an abstract finite abelian group A of order N and a finite flat commutative group-scheme of finite presentation G over an arbitrary S, we can define an A-structure on G/S to be a pair (K, ϕ) consisting of

a finite flat S-subgroup-scheme $K \subset G$ which is locally free of rank $N = \#A$.

a homomorphism $\phi : A \to G(S)$ which lands in K(S) and which is an "A-generator" of K.

The analogous result (with the same proof) is:

LEMMA 1.10.11. *If* G/S *is embeddable as a closed subscheme of a smooth curve* C/S *(cf. 1.2.1), then given a homomorphism*

$$\phi : A \to G(S),$$

there is at most one K *such that* (K, ϕ) *is an* A*-structure on* G/S, *and there is a closed subscheme of* S, *defined locally by finitely many equations, which is universal for the existence of this* K. *In particular, the functor* A-Str(G/S) *is represented by a closed subscheme of the finite* S*-scheme* Hom(A, G).

PROPOSITION 1.10.12. *Let* G/S *be a finite flat commutative group-scheme of finite presentation, and rank* N. *Let* A *be a finite abelian group of order* N, *and*

$$\phi : A \to G(S)$$

a group homomorphism. Then the following conditions are equivalent.

(1) ϕ *defines an isomorphism of* S*-group-schemes*

$$A \xrightarrow{\sim} G.$$

(2) G/S *is etale, and* ϕ *is an* A*-generator of* G/S.

If S *is connected, then (1) and (2) are each equivalent to*

(3) G/S *is a constant group-scheme, and* $\phi : A \to G(S)$ *is an isomorphism of abstract groups.*

Proof. This is immediate from its set theoretic analogue (1.8.3). Q.E.D.

PROPOSITION 1.10.13. *Let* G/S *be a finite flat commutative group-scheme of finite presentation, and rank* N. *Let* A *be a finite abelian group of order* N.

(1) *Then the functor* A-Gen(G/S) *on* S*-schemes defined by*

$$T \mapsto \begin{cases} \text{the set of group homomorphisms } \phi : A \to G(T) \text{ such that the} \\ \text{elements } \{\phi(a)\},\ a \in A \text{ are a full set of sections of } G_T/T \end{cases}$$

is representable by a finite S*-scheme of finite presentation, namely by the closed subscheme of* $Hom_{S\text{-}gp}(A, G)$ *over which the image sections* $\{\phi_{univ}(a)\}$, $a \in A$ *of the universal homomorphism* $A \to G$ *form a "full set of sections."*

(2) *If* G/S *if finite etale over* S *of rank* N, *then by 1.10.12, we have*

$$A\text{-Gen}(G/S) \simeq Isom_{S\text{-}gp}(A, G),$$

so that over each connected component of S, A-Gen(G/S) *is either empty or is a finite etale* Aut(A)*-torsor.*

PROPOSITION 1.10.14. *Let* G/S *be a finite flat commutative group-scheme of finite presentation, and rank* N. *Let* A *be a finite abelian*

group of order N, *and*

$$\phi : A \to G(S)$$

a group-homomorphism. Let

$$N = p_1^{n_1} \cdots p_r^{n_r}$$

be the factorization of N *into distinct prime powers, and let*

$$A = \prod A_i \qquad A_i \overset{\text{dfn}}{=\!=} A[p_i^{n_i}]$$

$$G = G_1 \underset{S}{\times} \cdots \underset{S}{\times} G_r \qquad G_i \overset{\text{dfn}}{=\!=} G[p_i^{n_i}]$$

be the corresponding decompositions of A *and* G *into* p*-primary components. Then the following conditions are equivalent*:

(1) ϕ *is an* A*-generator of* G/S;

(2) *for each* $i = 1, \cdots, r$, *the induced homomorphism is an* A_i*-generator of* G_i/S.

Proof. If the number r of distinct primes dividing N is one, there is nothing to prove. If $r \geq 2$, then locally on S all save at most one p_i, say p_r, is invertible. Then the groups $G_1, \cdots, G_{r-1}$ are all finite etale, and the result follows from its set-theoretic analogue (1.8.5) applied successively to $G_1 \times (G_2 \times \cdots \times G_r)$, $G_2 \times \cdots \times G_r, \cdots, G_{r-1} \times G_r$. Q.E.D.

COROLLARY 1.10.15. *Hypotheses and notations as above, we have a canonical isomorphism of* S*-schemes*

$$A\text{-}Gen(G/S) \xrightarrow{\sim} A_1\text{-}Gen(G_1/S) \underset{S}{\times} \cdots \underset{S}{\times} A_r\text{-}Gen(G_r/S) .$$

(1.11) *Extensions of an etale group*

(1.11.1) Let S be a connected scheme, and suppose given a short exact sequence (as f.p.p.f abelian sheaves on the category of S-schemes, (cf. SGA III, Exp. IV))

(1.11.1.1) $$0 \to H \to G \to E \to 0$$

of finite flat commutative S-group-schemes of finite presentation, with E/S finite etale. Let A be a finite abelian group whose order is the rank G/S, and let

(1.11.1.2) $$\phi : A \to G(S)$$

be a group homomorphism. We will analyze exactly what it means, in terms of the given structure of extension on G/S, for ϕ to be a generator of G/S.

Consider first the composite homomorphism

(1.11.1.3) $$A \to G(S) \to E(S) ,$$

which we may view as a morphism between finite etale S-group-schemes

(1.11.1.4) $$(A)_S \to E .$$

Such a morphism has as kernel a finite etale S-group, which is in fact constant (because it is a subgroup of the constant group $(A)_S/S$, and S is connected), thus corresponding to an "abstract" subgroup

(1.11.1.5) $$K \subset A .$$

For any non-empty S-scheme $T \to S$, we have

(1.11.1.6) $$K = \text{Ker of } A \to E(T) .$$

Thus we have a short exact sequence of abelian groups

(1.11.1.7) $$0 \to K \to A \to A/K \to 0 ,$$

and a commutative diagram with exact rows

(1.11.1.8)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & A & \longrightarrow & A/K & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi|K} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi|(A/K)} & & \\ 0 & \longrightarrow & H(S) & \longrightarrow & G(S) & \longrightarrow & E(S) & & \end{array}$$

In terms of this commutative diagram, we have the following criterion.

PROPOSITION 1.11.2. *Hypotheses and notations as above, ϕ is an A-generator of G/S if and only if both of the following conditions are satisfied:*

(1) *The order of K is equal to the rank of H/S, and the induced homomorphism $\phi|K$ is a K-generator of H/S.*

(2) *The order of A/K is equal to the rank of E/S, and the induced homomorphism $\phi|(A/K)$ is an A/K-generator of E/S.*

Proof. Suppose first that ϕ is an A-generator of G/S. Then for every geometric point $\mathrm{Spec}(k) \to S$ of S, ϕ_k is an A-generator of G_k/k. Therefore for every such geometric point the homomorphism on k-valued points

$$\phi_k : A \to G(k)$$

must be surjective. Over an algebraically closed field, the extension structure on G provides a short exact sequence of groups of k-valued points

$$0 \to H(k) \to G(k) \to E(k) \to 0 ,$$

which sits in the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & A & \longrightarrow & A/K & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H(k) & \longrightarrow & G(k) & \longrightarrow & E(k) & \longrightarrow & 0 . \end{array}$$

By the snake lemma, the right-most vertical arrow is an isomorphism

$$A/K \xrightarrow{\sim} E(k) .$$

This shows that A/K has order equal to the rank of E/S, and that $\phi|(A/K)$ defines an A/K-structure on E/S. Therefore (2) is proven.

If (2) holds, then any choice of *set-theoretic* section

$$\begin{array}{ccccccccc} & & & & \overset{s}{\frown} & & & & \\ 0 & \longrightarrow & K & \longrightarrow & A & \longrightarrow & A/K & \longrightarrow & 0 \end{array}$$

defines a *scheme-theoretic* isomorphism of S-schemes

$$H \underset{S}{\times} E \xrightarrow{\sim} G .$$

It now results immediately from (1.8.5) that, given (2), then (1) holds if and only if ϕ is an A-structure on G/S. Q.E.D.

If we consider arbitrary extensions, we have only the following weaker result.

PROPOSITION 1.11.3. *Over an arbitrary scheme S, suppose given a short exact sequence (as f.p.p.f. abelian sheaves)*

(1.11.3.1) $$0 \to G_1 \to G \to G_2 \to 0$$

of finite flat commutative S-group-schemes of finite presentation, and ranks N_1, N, and N_2 respectively.

Let A_1, A, and A_2 be finite abelian groups of orders N_1, N, and N_2 respectively, and suppose given a short exact sequence

(1.11.3.2) $$0 \to A_1 \to A \to A_2 \to 0 ,$$

and a commutative diagram of homomorphisms ϕ_1, ϕ, ϕ_2:

(1.11.3.3)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \longrightarrow & A & \longrightarrow & A_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi_2} & & \\ 0 & \longrightarrow & G_1(S) & \longrightarrow & G(S) & \longrightarrow & G_2(S) & & \end{array}$$

If for $i = 1,2$ *the homomorphisms* ϕ_i *are* A_i*-generators of* G_i/S, *then* ϕ *is an* A*-generator of* G/S.

Proof. This is an immediate consequence of the transitivity of the norm for the finite locally free morphisms $G \to G_2$ and $G_2 \to S$, together with the observation that the fiber of $G \to G_2$ over any S-valued point $\phi_2(a_2)$ of G_2 is $G_1 \to S$. Therefore for f any function on G, we have

$$N_{G/S}(f) = N_{G_2/S}(N_{G/G_2}(f))$$

$$= \prod_{a_2 \in A_2} \{(N_{G/G_2}(f))(\phi_2(a_2))\}$$

$$= \prod_{a_2 \in A_2} \Big\{ \prod_{\substack{a \in A \\ a \to a_2}} f(\phi(a)) \Big\} . \qquad \text{Q.E.D.}$$

REMARK 1.11.4. Here is an example to show that the *converse* of the preceding proposition is false. Let $S = \mathrm{Spec}(R)$ with R an F_p-algebra. For any p'th root of unity $\zeta \in \mu_p(R)$, we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbf{Z}/p\mathbf{Z} & \longrightarrow & \mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}/p\mathbf{Z} & \longrightarrow & \mathbf{Z}/p\mathbf{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi_2} & & \\ 0 & \longrightarrow & \mu_p(R) & \longrightarrow & \mu_{p^2}(R) & \xrightarrow{\times p} & \mu_p(R) & & \end{array}$$

with

$$\phi_1(a) = \zeta^a , \quad \phi(a,b) = \zeta^a , \quad \phi_2(b) = 1 .$$

Then ϕ is a $(\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z})$-generator of μ_{p^2}/R, because we have the polynomial identity

$$\prod_{a,b \in \mathbf{Z}/p\mathbf{Z}} (T - \phi(a,b)) = \prod_a (T - \zeta^a)^p$$

$$= \prod_a (T^p - 1)$$

$$= T^{p^2} - 1 .$$

However, in order for ϕ_1 to be a $\mathbf{Z}/p\mathbf{Z}$-structure on μ_p/R, we must have the polynomial identity

$$T^p - 1 = \prod_a (T - \zeta^a) ;$$

in particular, ζ must be a root of the polynomial

$$\Phi_p(X) = 1 + X + \cdots + X^{p-1}$$

as one sees by comparing coefficients of T^{p-1}. Thus if we take

$$R = F_p[X]/(X^p - 1), \quad \zeta = X ,$$

then Φ_1 is *not* a $\mathbf{Z}/p\mathbf{Z}$-generator of μ_p.

A second example is provided by the product situation

$$A = \mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}/p\mathbf{Z} \xrightarrow{\phi} \alpha_p \times \alpha_p$$

$$\phi(a,b) = (0, bY)$$

over an F_p-algebra R, with $Y \in R$ satisfying $Y^p = 0$, $Y^{p-1} \neq 0$. Then ϕ and ϕ_1 are generators, but not ϕ_2.

(1.11.5) Here is a final example in which ϕ is a generator, but neither ϕ_1 nor ϕ_2 is a generator. One takes the product situation

$$A = \mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}/p\mathbf{Z} \xrightarrow{\phi = 0} \mu_p \times \mu_p ,$$

over the ring $\mathbf{Z}/p^2\mathbf{Z}$. In this situation, both ϕ_1 and ϕ_2 are the zero-map $\mathbf{Z}/p\mathbf{Z} \to \mu_p$, and this map is *not* a generator of μ_p over $\mathbf{Z}/p^2\mathbf{Z}$, simply because we do not have the required equality of Cartier divisors in G_m over $\mathbf{Z}/p^2\mathbf{Z}$:

$$(X-1)^p \neq (X^p-1) \quad \text{in} \quad (\mathbf{Z}/p^2\mathbf{Z})[X] .$$

To see that ϕ *is* a generator of $\mu_p \times \mu_p$ over $\mathbf{Z}/p^2\mathbf{Z}$, we will verify the norm criterion: for any algebra R, and for any

$$f(X,Y) \in R[X,Y]/(X^p-1, Y^p-1) ,$$

we must show that

$$\mathrm{Norm}(f) \equiv f(1,1)^{p^2} \mod p^2R .$$

For this, we view the norm as the composite of the norm maps in the X and Y variables separately:

$$\begin{array}{c} R[X,Y]/(X^p-1, Y^p-1) \\ \downarrow N_X \\ R[Y]/(Y^p-1) \\ \downarrow N_Y \\ R . \end{array}$$

Because the zero map $\mathbf{Z}/p\mathbf{Z} \to \mu_p$ is a generator over any $\mathbf{F}_p$-algebra, e.g., over $(R/pR)[Y]/(Y^p-1)$, we have the congruence

$$N_X(f(X,Y)) = f(1,Y)^p + pg(Y)$$

with some $g(Y) \in R[Y]/(Y^p-1)$. For any two elements A, B in $R[Y]/(Y^p-1)$ and an indeterminate T, the norm with respect to Y of $A+TB$

$$\begin{array}{ccc} A+TB & \in & R[T][Y]/(Y^p-1) \\ \downarrow & & \downarrow N_Y \\ N_Y(A+TB) & \in & R[T] , \end{array}$$

is a polynomial in T of degree p, of the form

$$N_Y(A+TB) = N_Y(A) + \sum_{i=1}^{p-1} T^i \Lambda_i(A,B) + T^p N_Y(B) .$$

But mod p we have

$$N_Y(A+TB) \equiv (A(1)+TB(1))^p \equiv A(1)^p + T^p B(1)^p \mod p .$$

Therefore equating coefficients yields

$$\Lambda_i(A,B) \equiv 0 \,(p) \quad \text{for} \quad i = 1, \cdots, p-1 ,$$

and therefore

$$N_Y(A+TB) \equiv N_Y(A) \mod (pT, T^p) .$$

Applying this with $T = p$, we find

$$N_Y(A+pB) \equiv N_Y(A) \,(p^2) .$$

Therefore

$$\begin{aligned} \mathrm{Norm}(f(X,Y)) &= N_Y(N_X(f)) \\ &= N_Y(f(1,Y)^p + pg(Y)) \\ &\equiv N_Y((f(1,Y))^p) \qquad (p^2) \\ &\equiv (N_Y(f(1,Y))^p) \qquad (p^2) \\ &\equiv (f(1,1)^p + pk)^p \qquad (p^2) \\ &\equiv f(1,1)^{p^2} \qquad (p^2) . \end{aligned}$$

Q.E.D.

(1.12) *Roots of unity*

(1.12.1) In this section, we will work out the general theory in the case of the multiplicative group $G_m/\mathbf{Z}$, and $A = \mathbf{Z}/N\mathbf{Z}$. We denote by $\mu_N/\mathbf{Z}$ the group-scheme "N'th roots of unity", i.e., $\mu_N = G_m[N]$.

LEMMA 1.12.2. *Over any scheme* S, $(\mu_N)_S$ *is the unique closed* S*-subgroup-scheme of* $(G_m)_S$ *which is finite flat over* S *of finite presentation and of rank* N.

Proof. Visibly $(\mu_N)_S$ is such a closed S-subgroup-scheme of $(G_m)_S$. If G/S is any other, then G is killed by N (because it is of rank N). Therefore $G \subset G_m[N] = \mu_N$, whence we have $G \leq \mu_N$ as effective Cartier divisors in $(G_m)_S/S$. Because both G and μ_N have the same degree N, we may infer that $G = \mu_N$, as required. Q.E.D.

COROLLARY 1.12.3. *If* A *is any finite abelian "abstract" group of order* N, *we have a natural equality of functors*

$$A\text{-}Str(G_m/Z) = A\text{-}Gen(\mu_N/Z),$$

in particular

$$Z/NZ\text{-}Str(G_m/Z) = Z/NZ\text{-}Gen(\mu_N/Z).$$

Proof. If ϕ is an A-structure on G_m, then the A-subgroup it generates can be none other than μ_N. Q.E.D.

(1.12.4) Henceforth we will consider only $A = Z/NZ$ (the natural choice since over any base scheme on which N is invertible, μ_N is a twisted form of the constant group Z/NZ). We denote by $(\mu_N)^\times$ the closed subscheme of μ_N consisting of roots of unity of "exact order N", i.e.,

$$(\mu_N)^\times = Z/NZ\text{-}Str(G_m/Z) = Z/NZ\text{-}Gen(\mu_N/Z).$$

Thus for any ring R, we have

(1.12.5) $(\mu_N)^\times(R)$ = the set of elements $\zeta \in R$ such that in the polynomial ring $R[T]$ we have the identity

$$T^N - 1 = \prod_{a=1}^{N} (T - \zeta^a).$$

(1.12.6) We will use interchangeably the expressions "root of unity of "exact order N" in R" and "primitive N'th root of unity in R" for elements of $(\mu_N)^\times(R)$.

THEOREM 1.12.7. *The scheme* $(\mu_N)^\times$ *of "primitive* N*'th roots of unity" is a regular one-dimensional scheme, which is finite and flat over* Z *of rank* $\phi(N)$. *Over* $Z[1/N]$, *it is finite etale.*

Proof. Suppose $N = N_1N_2$ with N_1 and N_2 relatively prime. By (1.10.5), we have a canonical isomorphism

$$(\mu_N)^\times \simeq (\mu_{N_1})^\times \underset{Z}{\times} (\mu_{N_2})^\times.$$

Therefore if the theorem is true for N_1 and N_2, then it is true for N.

This reduces us to treating the case when N is a prime power > 1, say $N = p^n$. Over $Z[1/p]$, we have a canonical isomorphism of $Z[1/p]$-schemes

$$(\mu_{p^n})^\times \xrightarrow{\sim} \underline{\mathrm{Isom}}(Z/p^nZ, \mu_{p^n}),$$

which shows that, over $Z[1/p]$, the scheme $(\mu_{p^n})^\times$ is indeed finite etale of rank $\phi(p^n)$.

The structural morphism

$$\begin{array}{c} (\mu_{p^n})^\times \\ \downarrow \\ \mathrm{Spec}(Z) \end{array}$$

is surjective (because it is a finite morphism whose image, necessarily a closed subset of $\mathrm{Spec}(Z)$, contains $\mathrm{Spec}(Z[1/p])$). Because $\mathrm{Spec}(Z)$ is one-dimensional, this surjectivity implies that there exists at least one closed point of $(\mu_{p^n})^\times$ lying over p whose local ring has dimension ≥ 1. In fact, there is at most one closed point of $(\mu_{p^n})^\times$ with characteristic p

(simply because for any field k of characteristic p, $(\mu_{p^n})^\times(k) \subset \mu_{p^n}(k) = \{1\}$). Therefore $(\mu_{p^n})^\times$ has a unique closed point of characteristic p, namely the F_p-valued point $\zeta = 1$. To show that $(\mu_{p^n})^\times$ is a regular one-dimensional scheme, it remains only to show that the local ring of $(\mu_{p^n})^\times$ at $\zeta = 1$ is regular and one-dimensional. As this local ring has dimension ≥ 1, it suffices to show that its maximal ideal is generated by a single function. We claim that $\zeta - 1$ is such a function. Indeed, the global coordinate ring of $(\mu_{p^n})^\times$ is

$$\mathbf{Z}[\zeta] \Big/ \left(\begin{array}{c} \text{the relations obtained by equating coefficients in the} \\ \text{identity } T^{p^n} - 1 = \prod_{a=1}^{p^n} (T - \zeta^a) . \end{array} \right)$$

We claim that if we divide this ring by the ideal $(\zeta - 1)$, the residue ring will be F_p itself. The residue ring is visibly

$$\mathbf{Z} \Big/ \left(\text{the relations obtained by equating coefficients in } T^{p^n} - 1 = (T-1)^{p^n} \right) .$$

Comparing coefficients of T, we see that our ring is a quotient of $\mathbf{Z}/p^n\mathbf{Z}$. Comparing coefficients of $T^{p^{n-1}}$, and remembering that

$$\mathrm{ord}_p \binom{p^n}{p^{n-1}} = 1 ,$$

we see that our ring is a quotient of F_p itself. But our ring visibly maps onto F_p, and hence it is F_p. This concludes the proof that $(\mu_{p^n})^\times$ is a regular one-dimensional scheme.

To prove that $(\mu_{p^n})^\times$ is finite flat over $\mathbf{Z}$ of the asserted degree, it suffices to prove that it is finite and flat over $\mathbf{Z}$, for we know that over $\mathbf{Z}[1/p]$ it has the required degree. But $(\mu_{p^n})^\times$ is certainly finite over $\mathrm{Spec}(\mathbf{Z})$, being a closed subscheme of μ_{p^n}, and its flatness over $\mathrm{Spec}(\mathbf{Z})$ results from the general fact that any finite morphism between regular schemes of the same dimension is automatically flat [A-K 1, V, 3.6]. Q.E.D.

(1.12.8) Let $\Phi_N(X) \in \mathbf{Z}[X]$ denote the N'th cyclotomic polynomial, i.e., the monic polynomial of degree $\phi(N)$ whose complex roots are the $\exp(2\pi i a/N)$, with $1 \leq a \leq N-1$ and $(a,N) = 1$. As is well-known, the ring

$$\mathcal{O}_N \overset{\text{dfn}}{=\!=} \mathbf{Z}[X]/(\Phi_N(X))$$

is precisely the ring of all algebraic integers in the field $\mathbf{Q}(\zeta_N)$ of N'th roots of unity.

THEOREM 1.12.9. *Over any ring R, an element $\zeta \in R$ is a root of the polynomial Φ_N if and only if ζ is a "primitive N'th root of unity." Equivalently, we have an isomorphism of schemes*

$$\mathrm{Spec}(\mathcal{O}_N) \xrightarrow{\sim} (\mu_N)^\times .$$

Proof. We have a natural morphism

$$\mathrm{Spec}(\mathcal{O}_N) \to (\mu_N)^\times ,$$

namely the $\mathcal{O}_N$-valued point of $(\mu_N)^\times$ which is the element

$$X \in \mathcal{O}_N = \mathbf{Z}[X]/(\Phi_N(X)) .$$

(To see that this element X actually lies in $(\mu_N)^\times(\mathcal{O}_N)$, i.e., that it satisfies the identity

$$T^N - 1 = \prod_{a=1}^{N} (T - X^a) ,$$

it suffices to do so after any injective extension of scalars $\mathcal{O}_N \to K$. We use the embedding $\mathcal{O}_K \to C$ given by $X \mapsto \exp(2\pi i/N)$, which makes this identity obvious.)

This morphism is certainly an isomorphism over $Z[1/N]$, (because both source and target are finite etale of the same rank $\phi(N)$ over $Z[1/N]$, it suffices to check that for any algebraically closed field k in which N is invertible, the map induces an isomorphism on k-valued points. By (1.4.4, (3)) this amounts to the statement that the roots of Φ_N in such a field k are precisely those N'th roots of unity in k which are not M'th roots of unity for any $1 \leq M < N$, which is standard).

We next define a morphism

$$(\mu_N)^\times \to \mathrm{Spec}(\mathcal{O}_N),$$

which carries the universal primitive N'th root of unity ζ to the universal solution X of $\Phi_N(X) = 0$. To do this, we must show that the element ζ in the coordinate ring B of $(\mu_N)^\times$

$$\zeta \in B = Z[\zeta] \Big/ \left(\text{the relations obtained by equating coefficients in } T^N - 1 = \prod_{a=1}^{N} (T - \zeta^a) \right)$$

is a root of Φ_N in that same ring, i.e., that

$$\Phi_N(\zeta) = 0 \quad \text{in} \quad B.$$

But B is flat over Z, so in particular $B \subset B \otimes_Z Z[1/N]$. Therefore it suffices to verify that

$$\Phi_N(\zeta) = 0 \quad \text{in} \quad B[1/N].$$

But *this* vanishing amounts precisely to the just-proven statement that the natural morphism

$$\mathrm{Spec}(\mathcal{O}_N) \to (\mu_N)^\times$$

is an isomorphism over $Z[1/N]$.

To verify that each of the two composite maps

$$\mathrm{Spec}(\mathcal{O}_N) \to (\mu_N)^\times \to \mathrm{Spec}(\mathcal{O}_N)$$

$$(\mu_N)^\times \to \mathrm{Spec}(\mathcal{O}_N) \to (\mu_N)^\times$$

is the identity, it again suffices to check over $Z[1/N]$ (since both $\mathcal{O}_N$ and $(\mu_N)^\times$ are flat over Z), where this is obvious. Q.E.D.

REMARK 1.12.10. The arguments given in this section are in many ways typical of the arguments which will be used later in discussing moduli of elliptic curves. This perhaps justifies giving them in such detail.

(1.13) *Some open problems*

In this section we would like to mention explicitly some open problems related to the ideas developed in this chapter.

1. Let S be an arbitrary scheme, Z/S a finite locally free S-scheme of rank $N \geq 2$. Is it true that locally f.p.p.f. on S, Z/S always admits a full set of sections? (It is of course true if Z/S is embeddable in a smooth curve C/S.)

2. Let S be an arbitrary scheme, Z_1/S and Z_2/S two finite locally free S-schemes of the same rank $N \geq 1$. Let

$$\phi : Z_1 \to Z_2$$

be an S-morphism. We say that ϕ is a $\times$-morphism if for every affine S-scheme $\mathrm{Spec}(R)$, and for every function f on $(Z_2)_R = \mathrm{Spec}(B_2)$ we have an equality of characteristic polynomials in $R[T]$

$$\det(T - f) = \det(T - \phi^*(f)).$$

Clearly the composition of two $\times$-morphisms is another. When Z_1 is the

disjoint union of N copies of S, such a $\times$-morphism is exactly what we have called a full set of sections of Z_2/S.

Now suppose that G_1 and G_2 are finite locally free commutative group-schemes over S, of the same rank N. We say that a homomorphism of S-group-schemes

$$\phi : G_1 \to G_2$$

is a $\times$-homomorphism if it is a $\times$-morphism of the underlying S-schemes. Clearly the composition of two $\times$-homomorphisms is another one. So for given $N \geq 1$, we can form a category by taking as objects the finite locally free commutative S-group-schemes of rank N, and as morphisms the set

$$\mathrm{Hom}^{\times}_{S-gp}(G_1, G_2)$$

of all $\times$-homomorphisms. If G_1 is a constant abelian group A of order N, then we have

$$\mathrm{Hom}^{\times}_{S}(A_S, G_2) = \text{the set of A-generators of } G_2/S.$$

Given G_1, G_2, let us say that G_2 is a "degeneration" of G_1 if, after some f.p.l.p.f. base-change, $T \to S$, the set

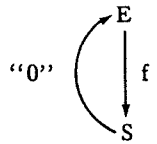
$$\mathrm{Hom}^{\times}_{T}(G_1, G_2),$$

which we might call the " G_1-generators of G_2 ", is non-empty. Is there an interesting theory of "degeneration"? Are there cases "in nature" where one wants to consider moduli problems based on the notion of a " G_1-generator" when G_1 is *not constant*?

Chapter 2
REVIEW OF ELLIPTIC CURVES

(2.1) *The group structure* (Compare [De 2].)

(2.1.1) Let S be an arbitrary scheme. An elliptic curve E/S is a proper smooth curve



with geometrically connected fibers all of genus one, given with a section "0". For any section $P \in E(S)$, we denote by $I(P)$ the ideal sheaf of P viewed as an effective Cartier divisor of degree one in E, and by $I^{-1}(P)$ the inverse ideal sheaf.

THEOREM 2.1.2 (Abel). *There exists a unique structure of commutative group-scheme on E/S such that for any S-scheme T, and any three points P, Q, R in $E(T) = E_T(T)$, we have*

$$P + Q = R$$

if and only if there exists an invertible sheaf $\mathcal{L}_0$ on T and an isomorphism of invertible sheaves on E_T

$$I^{-1}(P) \otimes I^{-1}(Q) \otimes I(0) \simeq I^{-1}(R) \otimes f_T^*(\mathcal{L}_0).$$

Proof. What must be shown is that the map

$$E(T) \to \mathrm{Pic}^{(1)}(E_T/T) \overset{\text{dfn}}{=\!=} \text{the set of isomorphism classes of invertible sheaves } \mathcal{L} \text{ on } E_T \text{ which are fiber-by-fiber of degree one, modulo the equivalence relation } \mathcal{L} \sim \mathcal{L} \otimes f_T^*(\mathcal{L}_0) \text{ for any invertible sheaf } \mathcal{L}_0 \text{ on } T$$

defined by

$$P \mapsto \text{the class of } I^{-1}(P)$$

is *bijective*. For if this is the case, then given $P, Q \in E(T)$, the invertible sheaf on E_T,

$$I^{-1}(P) \otimes I^{-1}(Q) \otimes I(0) ,$$

which is fiber-by-fiber of degree one, is isomorphic to one of the form

$$I^{-1}(R) \otimes f^*(\mathcal{L}_0)$$

for some unique $R \in E(T)$. Therefore the group-law is unique. To see that it *exists*, we compose the above bijection with the bijection

$$\mathrm{Pic}^{(1)}(E_T/T) \to \mathrm{Pic}^{(0)}(E_T/T)$$

$$\mathcal{L} \mapsto \mathcal{L} \otimes I(0)$$

to obtain a *bijection of sets*

$$E(T) \xrightarrow{\sim} \mathrm{Pic}^{(0)}(E_T/T) = \text{the } \textit{abelian group} \text{ of isomorphism classes of invertible sheaves on } E_T \text{ which are fiber-by-fiber of degree zero, modulo the } \textit{subgroup} \text{ of those of the form } f_T^*(\mathcal{L}_0)$$

$$P \mapsto \text{the class of } I^{-1}(P) \otimes I(0) \text{ in } \mathrm{Pic}^{(0)}(E_T/T)$$

between the set $E(T)$ and the abelian group $\mathrm{Pic}^{(0)}(E_T/T)$. Transporting

the group structure to $E(T)$ by this bijection, we obtain an abelian group law on $E(T)$, functorially in T, which by its construction does satisfy Abel's theorem.

It remains to verify that the map

$$E(T) = E_T(T) \to \mathrm{Pic}^{(1)}(E_T/T)$$

is bijective. Replacing E/S by E_T/T, it suffices to treat the case $T = S$. We next claim that the question is Zariski local on S, i.e., if we are given $\mathcal{L}$ and $\mathcal{L}'$ on E, an affine open covering $\{U_i\}$ of S, invertible sheaves $\mathcal{L}_{0,i}$ on U_i, and isomorphisms

$$\phi_i : \mathcal{L} \xrightarrow{\sim} \mathcal{L}' \otimes f^*(\mathcal{L}_{0,i}) \quad \text{on} \quad f^{-1}(U_i) ,$$

then there exists an $\mathcal{L}_0$ on S and an isomorphism

$$\phi : \mathcal{L} \xrightarrow{\sim} \mathcal{L}' \otimes f^*(\mathcal{L}_0) .$$

Because E/S is proper and smooth with geometrically connected fibers, we have

$$f_*(\mathcal{O}_E) = \mathcal{O}_S ,$$

whence

$$f_* f^*(\mathcal{L}_{0,i}) = \mathcal{L}_{0,i} \quad \text{on} \quad U_i .$$

Therefore the existence of the isomorphism ϕ_i shows that both

$$f_*(\mathcal{L}^{-1} \otimes \mathcal{L}'), \quad f_*(\mathcal{L} \otimes (\mathcal{L}')^{-1})$$

are invertible sheaves on $\mathcal{O}_S$, inverse to each other. If we call the second one $\mathcal{L}_0$, and write

$$\mathcal{L}'' = \mathcal{L}' \otimes f^*(\mathcal{L}_0) ,$$

we find canonical isomorphisms

$$f_*(\mathcal{L}^{-1}\otimes\mathcal{L}'') = \mathcal{O}_S = f_*(\mathcal{L}\otimes(\mathcal{L}'')^{-1}),$$

under which the unit section $1 \in \Gamma(S,\mathcal{O}_S)$ *is* the required isomorphism

$$\mathcal{L} \xrightarrow{\sim} \mathcal{L}''.$$

This reduces us to the case when S is affine. Because E/S is of finite presentation, we reduce easily to the case when S is affine and noetherian (even a finitely generated $\mathbb{Z}$-algebra if we like). We will construct the inverse map.

Let $\mathcal{L}$ be an invertible sheaf on E, fiber-by-fiber of degree one. Then we claim that

$f_*\mathcal{L}$ is an invertible sheaf on S, of formation compatible with arbitrary change of base.

$R^1f_*\mathcal{L} = 0$.

It suffices to prove that $R^1f_*\mathcal{L} = 0$, for then [Mum 4, p. 53] $f_*\mathcal{L}$ is automatically locally free and of formation compatible with arbitrary change of base, so necessarily of rank one because this is obviously so over an algebraically closed field. Now $R^1f_*\mathcal{L} = 0$ because it is of formation compatible with arbitrary change of base (being an R^1f_* for f proper and flat of relative dimension one) and because over an algebraically closed field, $H^1(E,\mathcal{L}) = 0$ for degree $(\mathcal{L}) > 2g-2 = 0$. As $R^1f_*\mathcal{L}$ is a coherent sheaf on S with all fibers zero, it vanishes by Nakayama's lemma.

Because $f_*\mathcal{L}$ is invertible on S, Zariski locally on S we may pick an $\mathcal{O}_S$-basis ℓ of $f_*\mathcal{L}$. We claim that, locally over S, the pair $(\mathcal{L},\ell)$ on E defines an effective Cartier divisor in E. We must show that we have an exact sequence

$$0 \longrightarrow \mathcal{O} \xrightarrow{\ell} \mathcal{L} \longrightarrow \mathcal{L}/\mathcal{O} \longrightarrow 0$$

with $\mathcal{L}/\mathcal{O}$ flat over S. This amounts to the statement that the map of invertible sheaves

$$\mathcal{O} \xrightarrow{\ell} \mathcal{L}$$

on E is injective, and remains so after any base change $T \to S$ on S.

For this we are reduced to the case $S = \mathrm{Spec}(k)$ with k a field, and $\ell \in H^0(E,\ell)$ a k-basis, so non-zero, in which case the assertion is obvious.

Therefore $(\mathcal{L},\ell)$ defines an effective Cartier divisor in E/S. Looking fiber-by-fiber, we see that it is of degree one. By (1.2.7), any effective Cartier divisor of degree one is a section $P \in E(S)$. One verifies easily that the two maps

$$E(S) \rightleftarrows \mathrm{Pic}^{(1)}(E/S)$$

$$P \longmapsto \Gamma^{-1}(P)$$

$$\begin{array}{l}\text{the scheme of zeroes}\\ \text{of a local-on-S}\\ \mathcal{O}_S\text{-basis of } f_*\mathcal{L}\end{array} \longmapsto \mathcal{L}$$

are inverse isomorphisms. Q.E.D.

(2.2) *Generalized Weierstrass equations, and some elementary universal families*

(2.2.1) Given an elliptic curve E/S, the invertible sheaf $\Omega^1_{E/S}$ is fibre-by-fiber of degree zero, and Serre-Grothendieck duality defines a canonical isomorphism

(2.2.1.1) $$R^1f_*\Omega^1_{E/S} \xrightarrow{\sim} \mathcal{O}_S$$

of formation compatible with arbitrary change of base. Therefore

(2.2.1.2) $$\underline{\omega}_{E/S} \overset{\mathrm{dfn}}{=\!=} f_*\Omega^1_{E/S}$$

is necessarily an invertible sheaf on S, of formation compatible with arbitrary change of base.

(2.2.2) Zariski locally on S, we may choose an $\mathcal{O}_S$-basis ω of $\underline{\omega}_{E/S}$; such an ω is nothing other than a nowhere-vanishing one-form on E/S, i.e., an isomorphism $\mathcal{O} \xrightarrow{\sim} \Omega^1_{E/S}$. This ω is necessarily translation-invariant, because the effect of translation on ω defines a homomorphism of S-group-schemes

$$\phi : E \to G_m ,$$

which is necessarily constant (because ϕ viewed as a function on E, is an element of $H^0(E, \mathcal{O}_E) = H^0(S, f_*\mathcal{O}_E) = H^0(S, \mathcal{O}_S)$), so trivial (because a homomorphism).

(2.2.3) Zariski locally on S, the formal completion $\hat{E}$ of E along its zero-section "0" is of the form

$$\hat{E} \simeq \mathrm{Spf}(A[[T]]), \quad S = \mathrm{Spec}(A) .$$

Such an isomorphism is called a formal parameter(ization) at zero, and noted simply "T".

(2.2.4) Once we have chosen a formal parameter T at zero, there is a *unique* $\mathcal{O}_S$-basis ω of $\underline{\omega}_{E/S}$ "adapted to T", i.e., whose formal expansion along the zero-section is

$$\omega = (1 + \text{higher terms}) \cdot dT .$$

Conversely, if we are given an $\mathcal{O}_S$-basis ω of $\underline{\omega}_{E/S}$ on S, then locally on S there exists a formal parameter T to which ω is "adapted" as above, and this T is unique up to $T \mapsto T +$ higher terms.

(2.2.5) For each integer $n \geq 1$, the invertible sheaf $I(0)$ has

$$f_*(I^{-n}(0)) = \text{locally free of rank } n \text{ on } S .$$

Once we have chosen an $\mathcal{O}_S$-basis ω of $\underline{\omega}_{E/S}$ over an affine $S = \mathrm{Spec}(A)$, we have

$$f_*(I^{-2}(0)) \text{ is free on } 1, x$$

with x uniquely determined up to $x \mapsto x + a$ by the normalization

$$x \sim \frac{1}{T^2}(1 + \text{higher terms}) ,$$

(for *any* formal parameter T to which ω is adapted, it doesn't matter which) and

$$f_*(I^{-3}(0)) \text{ is free on } 1, x, y$$

with y uniquely determined up to $y \mapsto y + ax + b$ by the normalization

$$y \sim \frac{1}{T^3}(1 + \text{higher terms}) .$$

We say that such x, y are "adapted to ω".

Then we easily see that

$$f_*(I^{-4}(0)) \text{ is free on } 1, x, y, x^2$$
$$f_*(I^{-5}(0)) \text{ is free on } 1, x, y, x^2, xy$$
$$f_*(I^{-6}(0)) \text{ is free on } 1, x, y, x^2, xy, x^3$$
$$\text{or free on } 1, x, y, x^2, xy, y^2 ,$$

and that

$$y^2 - x^3 \in f_*I^{-5}(0), \text{ which is free on } 1, x, y, x^2, xy .$$

Therefore we obtain a generalized Weierstrass equation

(2.2.5.1) $$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 ,$$

and indeed the affine ring

$$H^0(E - \{0\}; \mathcal{O}) = \varinjlim_n H^0(E, I^{-n}(E))$$

is none other than

$$A[x, y]/(\text{this Weierstrass equation}) .$$

When 2 is invertible in A, there is a *unique* choice of y adapted to ω such that $a_1 = a_3 = 0$. When 3 is invertible in A, there is a unique choice of x adapted to ω such that $a_2 = 0$.

(2.2.6) *Case I.* (Weierstrass) 6 invertible: once we locally on S pick a basis ω of $\underline{\omega}_{E/S}$, we get unique adapted x, y such that (E, ω) is

$$(2y)^2 = 4x^3 - g_2 x - g_3 ; \quad \omega = \frac{-dx}{2y} ,$$

and (g_2, g_3) are arbitrary in $\Gamma(S, \mathcal{O}_S)$ such that the cubic is smooth, i.e.,

$$\Delta \overset{\text{dfn}}{=\!=} (g_2)^3 - 27(g_3)^2$$

is invertible on S. The corresponding Weierstrass family over

$$\text{Spec}\,(\mathbf{Z}[1/6, g_2, g_3][1/\Delta])$$

is the universal (E, ω) over a scheme where 6 is invertible.

(2.2.7) (Weierstrass with $\Delta = 1$) The same Weierstrass family, over the closed subscheme of equation

$$(g_2)^3 - 27(g_3)^2 = 1$$

is the universal (E, ω) with $\Delta(E, \omega) = 1$, over a $\mathbf{Z}[1/6]$-algebra.

(2.2.8) *Case II.* (Legendre) 2 invertible: once we locally on S pick a basis ω of $\underline{\omega}_{E/S}$, x is free up to $x \mapsto x+a$, but y is specified if we insist $a_1 = a_3 = 0$. The equation is

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6 , \quad \omega = \frac{-dx}{2y} .$$

The cubic equation

$$x^3 + a_2 x^2 + a_4 x + a_6$$

must define a finite etale covering of S of degree three if our equation is

to be smooth over S. The automorphism $P \mapsto -P$ of E is given by $(x, y) \mapsto (x, -y)$ (because the function $x - a$ always has two zeroes, and a double pole at infinity). So the points of order two are the origin and the three points with $y = 0$. Let us *specify* two of these, say P_2, Q_2;

$$x(P_2) = e_1 , \quad x(Q_2) = e_2 .$$

The third is the *sum* of the first two (the function y has the correct divisor to realize this). So we may eliminate the $x \mapsto x+a$ indeterminacy if we insist that

$$x(P_2) = 0 .$$

We may normalize ω up to $\pm$ if we require that this x, already normalized by $x(P_2) = 0$, satisfy

$$x(Q_2) = 1 .$$

(2.2.9) Then the Legendre family

$$y^2 = x(x-1)(x-\lambda) , \quad \omega = \frac{-dx}{y}$$

over $\mathbf{Z}[1/2, \lambda][1/\lambda(\lambda-1)]$ is the universal $(E, \omega, P_2, Q_2$ everywhere finite points of order two such that $x(P_2) = 0$, $x(Q_2) = 1$) over schemes where 2 is invertible.

(2.2.10) *Case III.* (Naive level three) 3 invertible: again we pick a local on S basis ω of $\underline{\omega}_{E/S}$. Now x is unique, y free up to $y \mapsto y + ax + b$, and the equation is

$$y^2 + a_1 xy + a_3 y = x^3 + a_4 x + a_6 .$$

By Abel's theorem the points of order three are the nine flex points of this cubic. Suppose given a nowhere-trivial point of order 3, say P_3. Then locally over S there exists a function with a triple zero at P_3, and a triple pole at zero, so a linear combination of $1, x, y$. So there is a

unique such function of the form $y+ax+b$. Taking this to be y, we get an equation of the form

$$y^2 + a_1xy + a_3y = x^3 .$$

This cubic is smooth if and only if

$$(a_1^3-27a_3)a_3$$

is invertible.

Now suppose given a second nowhere-trivial point Q_3 of order three, which is disjoint from both $P_3 = (0,0)$ and $-P_3 = (0,-a_3)$. By Abel, Q_3 is the triple zero of a unique function of the form

$$y - Ax - B .$$

We claim that A is invertible. For this, it suffices to treat the case when S is a field of characteristic $\neq 3$. Suppose $A = 0$. Then $y-B$ has a triple zero at Q_3. This means that when we substitute $y = B$ in the equation for our curve, we get a polynomial in x with a triple zero at $x(Q_3)$:

$$x^3 - (B^2+a_1xB+a_3B) = (x-x(Q_3))^3 .$$

Comparing coefficients of x^2, we see that $x(Q_3) = 0$, whence $Q_3 = \pm P_3$, contradiction.

Because A is invertible, there is a *unique* choice of ω for which $A = 1$. The condition that $y = x+B$ meet our curve triply is that when we substitute $y = x+B$ into its equation, we get a polynomial in x with a triple zero at $x(Q_3) = C$;

$$(*) \qquad x^3 - ((x+B)^2 + (a_1x+a_3)(x+B)) = (x-C)^3 .$$

Equating coefficients of like powers of x, we find

$$\begin{cases} 3C &= 1 + a_1 \\ -3C^2 &= 2B + a_1B + a_3 \\ C^3 &= B^2 + a_3B . \end{cases}$$

The first two of these formulas define a_1, a_3 as polynomials in B, C. Subtracting from the third equation the product of the second with B, we get

$$C^3 + 3BC^2 + B^2(1+a_1) = 0 ,$$

and substituting $1 + a_1 = 3C$ by the first equation we find

$$(C+B)^3 = B^3 .$$

(2.2.11) Thus

$$\begin{cases} a_1 = 3C - 1 \\ a_3 = -3C^2 - B - 3BC , \end{cases}$$

and the curve

$$y^2 + a_1xy + a_3y = x^3$$

with marked points

$$P_3 = (0,0), \quad Q_3 = (C, B+C)$$

over the ring

$$Z[1/3, B, C][1/(a_1^3-27a_3)a_3C] \Big/ \left(B^3 = (B+C)^3\right)$$

is the universal (E, non-trivial P_3, non-trivial $Q_3 \neq \pm P_3$) over a $Z[1/3]$-algebra.

(2.3) *The structure of* $[N]$

THEOREM 2.3.1. *Let* S *be an arbitrary scheme,* E/S *an elliptic curve,* $N \geq 1$ *an integer. Then the* S*-homomorphism "multiplication by* N*"*

$$[N]: E \to E$$

is finite locally free of rank N^2. *If* N *is invertible on* S, *its kernel* $E[N]$ *is finite etale over* S, *locally for the etale topology on* S *isomorphic to* $Z/NZ \times Z/NZ$.

Proof. When $S = \mathrm{Spec}(\mathbf{C})$, the transcendental theory of elliptic functions shows that the complex manifold E^{an} underlying E is a one-dimensional complex torus, non-canonically of the form $\mathbf{C}/L$ for some lattice $L \subset \mathbf{C}$, say $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ with $\mathrm{Im}(\omega_2/\omega_1) > 0$. Then $E[N]$ is visibly the group $\frac{1}{N}L/L$, which is a free $\mathbf{Z}/N\mathbf{Z}$ module of rank two, with basis ω_1/N, ω_2/N. We will ultimately reduce to this case.

Zariski locally on S, E is given by a smooth Weierstrass cubic in $\mathbf{P}^2_S$, with origin $(0,0,1)$, and any smooth Weierstrass cubic in $\mathbf{P}^2_S$ is an elliptic curve over S with origin $(0,0,1)$. So by reduction to the universal case, we may suppose that S is the open set in

$$\mathrm{Spec}(\mathbf{Z}[a_1, a_2, a_3, a_4, a_6])$$

over which the cubic

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

is smooth.

In this case, S is a regular scheme, and therefore the total space E, being smooth over S, is itself regular. We will exploit the fact that any *finite* morphism between regular schemes of the same dimension is automatically flat [A-K 1, V, 3.6].

We first show that $[N]: E \to E$ is finite and flat. It suffices to show that it is finite. Because E is proper over S, any S-endomorphism of E is proper, so it suffices to show that $[N]: E \to E$ has finite fibers. This in turn may be checked geometric fiber by geometric fiber over S. So we are reduced to showing that $[N]: E \to E$ is finite when E is an elliptic curve over an algebraically closed field. Any morphism between proper smooth connected curves over an algebraically closed field is either finite flat or it is constant. If $\mathrm{char}(k)$ does not divide N, then $[N]$ is etale (its tangent map at the origin being multiplication by N), hence non-constant, hence finite and flat. Therefore $[N]: E \to E$ is finite etale over any algebraically closed field of characteristic prime to $[N]$. Over $S[1/N]$, then, $[N]$ is finite flat and fiber-by-fiber etale, so finite etale. Because $S[1/N]$ is normal and connected, to check that $E[N]$ is a twisted $(\mathbf{Z}/N\mathbf{Z})^2$ over $S[1/N]$, it suffices to do so at a single geometric point of $S[1/N]$. Take a C-valued point!

We now return to the general case. To show that $[N]$ is always finite flat, we must show that on an elliptic curve E/k with k algebraically closed, $[N]$ is not the zero map. Take an integer M, prime to both N and to $\mathrm{char}(k)$. Then $E(k)$ has M^2 points of order M. Because $(N, M) = 1$, $[N]$ induces an automorphism of these points. Therefore $[N]$ is not the zero map. Therefore $[N]$ is always finite flat. Because S is noetherian, "finite flat" is the same as a "finite locally free." Because S is connected the degree of $[N]$ is constant on S, so may be computed at any geometric point. Take a C-valued point! Q.E.D.

COROLLARY 2.3.2. *Let S be an arbitrary scheme, E/S an elliptic curve, and $N \geq 1$ an integer. If $E[N]$ is finite etale over S (e.g., if $E[N]$ is S-isomorphic to $(\mathbf{Z}/N\mathbf{Z})^2$), then N is invertible on S.*

Proof. By 2.3.1, the map $[N]: E \to E$ is an f.p.p.f $E[N]$-torsor. Therefore if $E[N]$ is finite etale over S, the map $[N]: E \to E$ is finite etale. Therefore $[N]$ induces an isomorphism on Lie algebras

$$Lie([N]): Lie(E/S) \xrightarrow{\sim} Lie(E/S).$$

But $Lie([N])$ is simply N-fold usual addition, i.e., $Lie([N]) = N$. Thus $Lie(E/S)$ is an invertible $\mathcal{O}_S$-module on which multiplication by N is an automorphism. Q.E.D.

(2.4) *Rigidity* (Compare [Mum 3])

THEOREM 2.4.1. *Let R be a ring, I an ideal of R, p a prime number. Suppose that the ideal (I, p) is nilpotent. Let*

$$f: E_1 \to E_2$$

be a homomorphism of elliptic curves over R. If $f = 0 \bmod I$, then $f = 0$.

Proof (Drinfeld). Consider the sequence of ideals in R

$$I^{(0)} = I, \quad I^{(1)} = (pI, I^2), \cdots, I^{(n+1)} = (pI^{(n)}, (I^{(n)})^2) .$$

Clearly, we have $I^{(n)} = 0$ for $n >> 0$. Working our way from R/I to R through the intermediary $R/I^{(\nu)}$'s, we may assume that

$$I^2 = pI = 0 \quad \text{in} \quad R .$$

Because $[p]: E_1 \to E_1$ is f.p.p.f. surjective, it suffices to show that $pf = 0$, if f is 0 mod I.

Locally on R, we may choose a parameter, X, for the formal group of E_2. In terms of this parameter, we have

$$[p](X) = pX + \text{higher terms} \in (pX, X^2) .$$

Now if B is any R-algebra, and $P \in E_1(B)$ is any point, then by hypothesis $f(P) \in E_2(B)$ *dies* in $E_2(B/IB)$. Therefore $f(P)$ lies in the formal group of E_2, and its X-coordinate lies in IB. Because $pI = I^2 = 0$, the shape of $[p](X)$ shows that $p \cdot f(P) = 0$. Q.E.D.

THEOREM 2.4.2 (Rigidity). *Let S be an arbitrary scheme, E_1 and E_2 two elliptic curves over S, and $f: E_1 \to E_2$ an S-homomorphism. Then Zariski locally on S, either $f = 0$ or f is an isogeny, i.e., f is finite locally free.*

Proof. The question is Zariski local S, so we may assume S affine, say $S = \mathrm{Spec}(A)$, and E_1 and E_2 are Weierstrass cubics in $\mathbf{P}^2_S$. The data (E_1, E_2, f) is of finite presentation over A, so we may reduce to the case when A is of finite type over $\mathbf{Z}$.

The general theory of the Hilbert Scheme [Mum 3, p. 22] and [A-K 2, 2.8] shows that for *any* two projective A-schemes X, Y, the functor $\underline{\mathrm{Hom}}_A(X,Y)$ of all scheme-morphisms from X to Y is represented by a separated A-scheme (which is a countable disjoint union of projective A-schemes). Therefore for any two morphisms $f, g: X \to Y$, the locus "$f = g$" is a

closed subscheme of $\mathrm{Spec}(A)$. In our situation, then "$f = 0$" defines a closed subscheme Z of $\mathrm{Spec}(A)$. We now show that Z is open. For this we must show that Z is stable by generization of $\mathrm{Spec}(A)$. Because Z is *closed*, it suffices to show that if x is a closed point of $\mathrm{Spec}(A)$ which lies in Z, then every generization of x lies in Z. This amounts to showing that if $\hat{\mathcal{O}}$ is the complete local ring of $\mathrm{Spec}(A)$ at a closed point, and if f is zero modulo its maximal ideal m, then f is zero over $\hat{\mathcal{O}}$. By passage to the limit, it suffices to show f is zero over the artinian quotients of $\hat{\mathcal{O}}$. Because A was of finite type over $\mathbf{Z}$, these artinian quotients are finite, so of finite residue characteristic, and so we may apply the previous theorem.

Therefore the condition "$f = 0$" defines an open and closed subscheme of $\mathrm{Spec}(A)$, i.e., a union of components. It remains to examine the other components. Over any of these, f is fiber-by-fiber non-zero, hence fiber-by-fiber finite and flat. By the fiber-by-fiber criterion for flatness, it follows that f is flat. Being proper with finite fibers, f is also finite. So f is finite and flat, and, being over a noetherian base, f is finite locally free. Q.E.D.

(2.5) *Manifestations of autoduality*

THEOREM 2.5.1. *Let E/S be an elliptic curve. The above structure of S-group-scheme on E/S is the unique structure of S-group-scheme on E/S for which "0" is the origin. If E and E' are two elliptic curves over S, any S-morphism $f: E \to E'$ with $f(0) = 0$ is a homomorphism.*

Proof. Let $K: E \underset{S}{\times} E \to E$ be a structure of S-group-scheme on E/S, for which "0" $\in E(S)$ is the identity. We claim

$$K(P, Q) = P + Q$$

for any $P, Q \in E(T)$, T any S-scheme. By the base-change $T \to S$, it suffices to treat the case $T = S$. Fix $P \in E(S)$, and consider the S-morphism

$$f_P : E \to E$$

$$f_P(Q) = K(P,Q) - P .$$

We must show that f_P is the identity map.

Visibly f_P is an S-automorphism of E. Let g_P denote the inverse automorphism. For any $Q \in E(S)$, we have

$$g_P^*(I(Q)) = I(f_P(Q)) .$$

Taking $Q = 0$, we have

$$g_P^*(I(0)) = I(f_P(0)) = I(0) .$$

Therefore we have a commutative diagram

$$\begin{array}{ccccc} Q & & E(S) & \xrightarrow{f_P} & E(S) & & Q \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ I^{-1}(Q)\otimes I(0) & & \mathrm{Pic}^{(0)}(E/S) & \xrightarrow{g_P^*} & \mathrm{Pic}^{(0)}(E/S) & & I^{-1}(Q)\otimes I(0) , \end{array}$$

in which the vertical arrows are group isomorphisms, and in which g_P^* is a group automorphism. This shows that f_P is an automorphism of E for its "Abel's theorem" group structure.

Viewing P as a variable, i.e., making the f.p.p.f. base change $E \to S$, we may apply rigidity to the homomorphism

$$f_P - \mathrm{id} : E_E \to E_E$$

of elliptic curves over the base E. This homomorphism is *zero* for $P = 0$, i.e., over the zero-section of the base E. As the zero section meets every connected component of E, this implies $f_P = \mathrm{id}$ over all of E, in particular for any $P \in E(S)$. Therefore $K(P,Q) = P+Q$ as required.

Suppose we are given an S-morphism between elliptic curves over S,

$$f : E \to E', \quad f(0) = 0 .$$

We must show

$$f(P+Q) = f(P) + f(Q)$$

for all $P,Q \in E(T)$, T any S-scheme. Making the base-change $T \to S$, we may suppose $T = S$. The question is local on S, which we may suppose affine. Because E, E' are of finite presentation over S, we may further assume $S = \mathrm{Spec}(A)$ with A a finitely generated $\mathbf{Z}$-algebra. We may replace A by the product of its complete local rings at all closed points (faithful flatness), to reduce to the case A complete noetherian local with finite residue field. By passage to the limit, it suffices to treat the case when A is artin local with finite residue field k, of characteristic $p > 0$. Denote by $f_0 : E\otimes k \to E'\otimes k$ the morphism of special fibers, a map of smooth connected curves over a field. So either $f_0 = 0$, or f_0 is finite and flat.

If $f_0 = 0$, we claim $f = 0$. Certainly for any A-algebra R, $f(E(R))$ lies in $\mathrm{Ker}(E'(R) \to E'(R\otimes_A k))$, and this kernel is killed by a fixed power p^n of p independently of R, as in Drinfeld's rigidity argument (cf. (2.4.7)). Therefore $p^n f = 0$, i.e., f lands in the finite flat group-scheme $E'[p^n]$ of rank p^{2n} over A. Taking an A-basis of the coordinate ring of $E'[p^{2n}]$, f is given by p^{2n} coordinate functions $f_i \in H^0(E, \mathcal{O}_E) \xrightarrow{\sim} A$. Therefore f is a constant map. As $f(0) = 0$, we have $f = 0$.

If $f_0 \neq 0$, then f_0 is finite and flat. By the local criterion of flatness, f is flat, and f is finite because it is proper with finite fibers. So f is finite and flat, say locally free of degree N. The map

$$\begin{aligned} f^t = \mathrm{Pic}(f) = f^* : Pic^{(0)}_{E'/S} &\to Pic^{(0)}_{E/S} \\ \mathfrak{L} &\mapsto f^*(\mathfrak{L}) \end{aligned}$$

is certainly a homomorphism of S-group-schemes, so via Abel's isomorphism it corresponds to an S-homomorphism $f^t : E' \to E$. We claim that the composite

$$E \xrightarrow{f} E' \xrightarrow{f^t} E$$

is multiplication by N. This amounts to the statement

$$(I^{-1}(P)\otimes I(0))^{\otimes N} \xrightarrow{\sim} f^*(I^{-1}(f(P))\otimes I(0)) .$$

But

$$f^*(I(f(P))) = \mathrm{trans}^*_{-P}(I(f^{-1}(0))) = I(P+f^{-1}(0))$$
$$f^*(I(0)) = I(f^{-1}(0)) ,$$

so we need

$$I^{-N}(P)\otimes I^N(0) \xrightarrow{\sim} I^{-1}(P+f^{-1}(0))\otimes I(f^{-1}(0)) .$$

This is an equality to be checked in $\mathrm{Pic}^{(0)}(E/S) \simeq E(S)$, so we may f.p.p.f. localize on S. Because $f^{-1}(0)$ is a subscheme of E finite locally free of rank N over S, it is an effective Cartier divisor in E, so f.p.p.f. locally on the base it may be written as

$$f^{-1}(0) = [Q_1] + \cdots + [Q_N] .$$

So we have

$$I(P+f^{-1}(0)) = \bigotimes_i I(P+Q_i)$$

$$I(f^{-1}(0)) = \bigotimes_i I(Q_i) ,$$

and we are reduced to showing

$$(I^{-1}(P)\otimes I(0))^{\otimes N} \simeq \bigotimes_{i=1}^{N} (I^{-1}(P+Q_i)\otimes I(Q_i)) .$$

In fact, we have, for any point Q,

$$I^{-1}(P)\otimes I(0) \simeq I^{-1}(P+Q)\otimes I(Q) ,$$

in $\mathrm{Pic}^{(0)}(E/S)$, precisely by Abel's theorem!

Thus we have proven the identity

$$f^t \circ f = \text{multiplication by } N \text{ on } E .$$

Therefore f^t is f.p.p.f. surjective, so by 2.4.2 it is an isogeny. Now consider, for fixed P, the morphism $f_P : E \to E'$ defined by

$$f_P(Q) = f(P+Q) - f(P) - f(Q) .$$

Composing with the *homomorphism* f^t, we find

$$f^t(f_P(Q)) = N(P+Q) - NP - NQ = 0 ,$$

i.e., f_P takes values in $\mathrm{Ker}(f^t)$. But $\mathrm{Ker}(f^t)$ is itself finite and flat, so just as above we see that f_P is a constant map to $\mathrm{Ker}(f^t)$. As $f_P(0) = f(P) - f(P) - f(0) = 0$, we have $f_P = 0$, whence f itself is a homomorphism. Q.E.D.

(2.6) *Hasse's theory* (cf. [H])

THEOREM 2.6.1. *Let $f : E \to E'$ be a homomorphism of elliptic curves over a connected base S. Let $f^t : E' \to E$ be the dual homomorphism*

$$\begin{array}{ccc} f^t = \mathrm{Pic}(f) : Pic^0_{E'/S} & \longrightarrow & Pic^{(0)}_{E/S} \\ \wr| & & \wr| \\ E' & & E . \end{array}$$

Then the composite $f^t \circ f$ is given by

$$f^t f = \deg(f) \overset{\text{dfn}}{=\!=} \begin{cases} N & \text{if } f \text{ is an isogeny of degree } N \\ 0 & \text{if } f = 0 . \end{cases}$$

Proof. We proved this (in the course of proving the preceding theorem) over an artin local S, which by rigidity, applied to $f^t f - N$, is sufficient. Q.E.D.

COROLLARY 2.6.1.1. *If* f *is an isogeny of degree* N, *so is* f^t *and* $f^{tt} = f$.

Proof. If f is an isogeny of degree N, the formula

$$f^t \circ f = N$$

shows that f^t is f.p.p.f. surjective, so non-zero, so itself an isogeny, so finite locally free of some degree. But

$$\text{degree}(f^t \circ f) = \deg(f^t)\deg(f) = N \deg(f^t)$$

$$\deg([N]) = N^2 ,$$

so $\deg(f^t) = N$. Now consider the composite $ff^t : E' \to E'$. We have

$$ff^t(f(P)) = f(NP) = Nf(P) ,$$

so that $ff^t - N$ kills the image of f. But f is f.p.p.f. surjective, so we conclude

$$ff^t = N .$$

But as f^t is an isogeny of degree N, we have

$$f^{tt}f^t = N ,$$

whence $f - f^{tt}$ kills the image of f^t. As f^t is f.p.p.f. surjective, we conclude $f = f^{tt}$. Q.E.D.

THEOREM 2.6.2. *Let* $f,g : E \to E'$ *be homomorphisms of elliptic curves over* S. *Then* $(f+g)^t = f^t + g^t$.

Proof. View f, g, and $f+g$ as E-valued points of E' (Hasse's trick!). Making the base change $E \to S$, we are reduced to showing that if E'/S is an elliptic curve, and if $P, Q \in E(S)$, then for line bundle $\mathcal{L}$ on E' which is fiber-by-fiber of degree zero, we have an isomorphism of line bundles

$$P^*(\mathcal{L}) \otimes Q^*(\mathcal{L}) \simeq (P+Q)^*(\mathcal{L}) \otimes 0^*(\mathcal{L})$$

on S. Clearly the statement is invariant if we replace $\mathcal{L}$ by $\mathcal{L} \otimes (\pi^*(\mathcal{L}_0))$ for $\pi : E' \to S$ the structural map, and $\mathcal{L}_0$ a line bundle on S. So we may assume

$$\mathcal{L} = I^{-1}(R) \otimes I(0) \text{ for some } R \in E(S) .$$

Let $\text{trans}_P : E' \to E'$ be the automorphism $X \mapsto X + P$. Then as morphisms $S \to E$, we have $P = \text{trans}_P \circ 0$, so

$$P^*(\mathcal{L}) = 0^*(\text{trans}_P^*(\mathcal{L})) .$$

Therefore we may rewrite the hoped-for isomorphism on S

$$P^*(\mathcal{L}) \otimes Q^*(\mathcal{L}) \simeq (P+Q)^*(\mathcal{L}) \otimes 0^*(\mathcal{L})$$

as an isomorphism

$$\mathcal{O}_S \simeq 0^*(\text{trans}_P^*(\mathcal{L}) \otimes \text{trans}_Q^*(\mathcal{L}) \otimes \text{trans}_{P+Q}^*(\mathcal{L}^{-1}) \otimes \mathcal{L}^{-1}) .$$

But $\mathcal{L} \simeq I^{-1}(R) \otimes I(0)$, so the line bundle on E being pulled back is

$$I^{-1}(R-P) \otimes I(-P) \otimes I^{-1}(R-Q) \otimes I(-Q) \otimes I(R-P-Q) \otimes$$

$$\otimes I^{-1}(-P-Q) \otimes I(R) \otimes I^{-1}(0)$$

$$= (I^{-1}(R-P) \otimes I^{-1}(R-Q) \otimes I(R-P-Q) \otimes I(R)) \otimes$$

$$\otimes (I(-P) \otimes I(-Q) \otimes I^{-1}(-P-Q) \otimes I^{-1}(0)) .$$

By Abel's theorem, the first clump of terms is of the form $\pi^*(\mathcal{L}_0)$, while the second clump is $\text{trans}_R^*(\text{the first clump})^{-1}$, so all in all the expression being pulled back is of the form

$$\pi^*(\mathcal{L}_0) \otimes \text{trans}_R^*(\pi^*(\mathcal{L}_0))^{-1} = \pi^*(\mathcal{L}_0) \otimes \pi^*(\mathcal{L}_0)^{-1} = \mathcal{O}_E . \text{ Q.E.D.}$$

COROLLARY 2.6.2.1. *For any integer* $N \in \mathbf{Z}$, *the transpose of the endomorphism* $[N] : E \to E$ *is* $[N]$ *itself.*

Proof. For $N = 0$, this is obvious. For $N \neq 0$, $[N]$ is an isogeny of degree N^2, so $N^t \cdot N = N^2$, whence $(N^t - N)$ kills the image of $[N]$, so $N^t = N$. Q.E.D.

COROLLARY 2.6.2.2. *If* $f : E \to E$ *is an* S*-endomorphism of an elliptic curve over a connected base* S, *there exists an integer, called* trace(f), *such that* $f + f^t = \text{trace}(f)$.

Proof. $\deg(1+f) = (1+f)^t(1+f) = (1+f^t)(1+f) = 1 + \deg(f) + (f+f^t)$. Q.E.D.

THEOREM 2.6.3. *If* $f : E \to E$ *is an* S*-endomorphism of an elliptic curve over a connected base* S, *then*:

(1) *Inside* End(E), f *is a root of the* Z*-polynomial*

$$X^2 - \text{trace}(f)X + \deg(f) = 0 .$$

(2) *We have the inequality*

$$(\text{trace}(f))^2 \leq 4 \deg(f) .$$

Proof. For (1), we write

$$f^2 - (f^t + f)f + f^t f = 0 .$$

For (2), the inequality is equivalent to the assertion that the polynomial

$$X^2 - \text{tr}(f)X + \deg(f)$$

takes only values ≥ 0 for $X \in \mathbf{R}$, or equivalently for $X \in \mathbf{Q}$, or equivalently that for all integers $n, m \in \mathbf{Z}$, we have

$$n^2 - \text{tr}(f) \cdot nm + \deg(f)m^2 \geq 0 .$$

But this last inequality is none other than

$$\deg(n - mf) \geq 0 .$$ Q.E.D.

COROLLARY 2.6.4. *If* E *is an elliptic curve over a finite field* $\mathbf{F}_q$,

$$|\#E(\mathbf{F}_q) - (q+1)| \leq 2\sqrt{q} .$$

Proof. Denote by F the Frobenius relative to $\mathbf{F}_q$. Then $1 - F$ is etale, and its kernel is exactly the constant group $E(\mathbf{F}_q)$. Therefore

$$\#E(\mathbf{F}_q) = \deg(1-F) = (1-F^t)(1-F) = 1 - \text{tr}(F) + \deg(F)$$
$$= 1 + q - \text{tr}(F) ,$$

and by the above inequality

$$(\text{tr}(F))^2 \leq 4 \deg(F) = 4q .$$ Q.E.D.

(2.7) *Applications to rigidity*

COROLLARY 2.7.1. *Let* $\varepsilon : E \to E$ *be an automorphism of an elliptic curve over a connected base* S. *Then* ε *satisfies an equation*

$$X^2 - \text{tr}(\varepsilon)X + 1 = 0$$

with $\text{tr}(\varepsilon)$ *one of the integers* $0, \pm 1, \pm 2$.

Proof. For an automorphism, ε, we have $\deg(\varepsilon) = 1$, whence $(\text{tr}(\varepsilon))^2 \leq 4$ by (2.6.3). Q.E.D.

COROLLARY 2.7.2 (Rigidity of level N structures). *Let* $\varepsilon : E \to E$ *be an automorphism of an elliptic curve over a connected base* S. *Let* $N \geq 2$ *be an integer,* E[N] *the scheme-theoretic kernel of* N. *Suppose that* ε *induces the identity automorphism of* E[N].

(1) *If* $N \geq 3$, *then* $\varepsilon = \text{id}$.

(2) *If* $N = 2$, *then* $\varepsilon = \pm \text{id}$.

Proof. By hypothesis, $\varepsilon - 1$ kills E[N], so it factors as

$$\varepsilon - 1 = g \cdot N$$

for some $g \in \text{End}(E)$. Then

$$\varepsilon = 1 + gN ,$$

so

$$\begin{cases} \text{trace}(\varepsilon) &= 2 + N\ \text{trace}(g) \\ \deg(\varepsilon) &= 1 + N\ \text{trace}(g) + N^2 \deg(g)\ . \end{cases}$$

But $\deg(\varepsilon) = 1$, and $|\text{trace}(\varepsilon)| \leq 2$. So

$$|N\ \text{trace}(g)| \leq 4\ ,$$
$$N\ \text{trace}(g) = -N^2 \deg(g),\ \text{i.e.,}$$
$$|N^2 \deg(g)| \leq 4\ .$$

If $N \geq 3$, this last inequality gives $|\deg(g)| < 1$, whence, $\deg(g) = 0$, i.e., $g = 0$, so $\varepsilon = 1$, as required. If $N = 2$, we find either $g = 0$, and $\varepsilon = 1$, or $\deg(g) = 1$, $\text{trace}(g) = -2$, whence $\text{trace}(\varepsilon) = 2 + N\ \text{trace}(g) = -2$, and we find

$$(\varepsilon+1)^2 = 0\ .$$

But either $\varepsilon+1 = 0$, in which case we win, or $\varepsilon + 1$ is an isogeny of some non-zero degree, in which case $(\varepsilon+1)^2$ is also an isogeny, so non-zero. Q.E.D.

COROLLARY 2.7.3 (Rigidity of $\Gamma_1(N)$-structures). *Let $\varepsilon : E \to E$ be an automorphism of an elliptic curve E over a connected base S. Let $N \geq 4$ be an integer and $G \subset E$ a closed subgroup-scheme which is finite locally free over S of rank N. If ε induces the identity automorphism of G, then $\varepsilon = \text{id}$, or: $N = 4$, $G = E[2]$, and $\varepsilon = -1$.*

Proof. As above, $\varepsilon - 1$ kills G. So if $\varepsilon \neq 1$, then $\varepsilon - 1$ is an isogeny, whose kernel contains G. Therefore its degree is divisible by N:

$$\deg(\varepsilon - 1) \equiv 0(N)\ ,$$

i.e.,

$$(\varepsilon^t - 1)(\varepsilon - 1) = 1 - \text{tr}(\varepsilon) + 1 \equiv 0(N)\ ,$$

i.e.,

$$\text{tr}(\varepsilon) \equiv 2(N)\ .$$

If $N \geq 5$, this congruence, together with $|\text{tr}(\varepsilon)| \leq 2$, shows that $\text{tr}(\varepsilon) = 2$, whence ε satisfies $(\varepsilon-1)^2 = 0$, and just as above this forces $\varepsilon = 1$.

If $N = 4$, we have also to consider the possibility that $\text{tr}(\varepsilon) = -2$, in which case $(\varepsilon+1)^2 = 0$, and $\varepsilon = -1$. But then $\varepsilon - 1 = -2$ kills G, so $G \subset E[2]$, whence $G = E[2]$.

COROLLARY 2.7.4. *Let $\varepsilon : E \to E$ be an automorphism of an elliptic curve over a connected base S. Let $N \geq 4$ be an integer, and $G = \mathbf{Z}/N\mathbf{Z} \to E$ (resp. $G = \mu_N \hookrightarrow E$) a closed subgroup of E. If ε induces the identity on G, then $\varepsilon = \text{id}$.*

Proof. The only case not covered above is $N = 4$. But neither $\mathbf{Z}/4\mathbf{Z}$ nor μ_4 is killed by [2], so we must have $\varepsilon = \text{id}$ in this case as well. Q.E.D.

(2.8) *Pairings* (cf. [Oda])

(2.8.1) For any N-isogeny π (always understood to mean: finite locally free of rank N) between elliptic curves over an arbitrary base S, with dual N-isogeny π^t

$$E \underset{\pi^t}{\overset{\pi}{\rightleftarrows}} E'\ ,$$

there is a canonical bilinear pairing of finite locally-free commutative S-group-schemes

(2.8.1.2) $$\text{Ker}\ \pi \times \text{Ker}\ \pi^t \to \mu_N \subset G_m$$

denoted

(2.8.1.3) $$(P, P') \mapsto \langle P, P' \rangle_\pi$$

or more simply

$$(P, P') \mapsto \langle P, P' \rangle$$

if there is no ambiguity about which isogeny π is in question. Its definition, the opposite of [Oda, pp. 66-67], is as follows on T-valued points, T any S-scheme.

By base-change $T \to S$, it suffices to define $<P, P'>$ when P, P' are S-valued points of $\mathrm{Ker}(\pi)$ and of $\mathrm{Ker}(\pi^t)$ respectively. Let $K_E^\times \subset \mathcal{O}_E^\times$ denote the subsheaf of invertible functions on E which take the value "1" along the zero-section of E/S. As explained in [K5, §5, esp. 5.2, pp. 186-187], we have a natural isomorphism

$$\mathrm{Pic}(E/S) \simeq H^1(E, K^\times), \tag{2.8.1.5}$$

while

$$H^0(E, K^\times) = \{1\}. \tag{2.8.1.6}$$

By Abel's theorem (cf. 2.1), we may interpret a point $P' \in (\mathrm{Ker}\ \pi^t)(S)$ as an element $\mathfrak{L}$ of $\mathrm{Pic}^{(0)}(E'/S)$ which lies in the kernel of π^*:

$$(\mathrm{Ker}\ \pi^t)(S) = \mathrm{Ker}(\pi^*: \mathrm{Pic}(E'/S) \to \mathrm{Pic}(E/S)). \tag{2.8.1.7}$$

In terms of a normalized cocycle (i.e., one with values in $K^\times$) for $\mathfrak{L}$ with respect to some open covering U_i of E',

$$f_{i,j} \in \Gamma(U_i \cap U_j, K_{E'}^\times),$$

the triviality of $\pi^*(\mathfrak{L})$ in $\mathrm{Pic}(E/S)$ means that the normalized cocycle representing $\pi^*(\mathfrak{L})$ with respect to the open covering $\pi^{-1}(U_i)$ of E,

$$f_{i,j} \circ \pi \in \Gamma(\pi^{-1}(U_i \cap U_j), K_E^\times),$$

may be written uniquely in the form

$$f_{i,j} \circ \pi = h_i / h_j,$$

with functions

$$h_i \in \Gamma(\pi^{-1}(U_i), K_E^\times).$$

Now view $P \in (\mathrm{Ker}\ \pi)(S) \subset E(S)$ as an S-morphism

$$S \xrightarrow{P} E.$$

Over the open covering of S given by the open sets

$$P^{-1}(\pi^{-1}U_i),$$

we have the invertible functions

$$h_i \circ P,$$

which, in view of the relations

$$f_{i,j} \in K^\times, \quad h_i/h_j = f_{i,j} \circ \pi, \quad \pi P = 0,$$

patch together to define a global section

$$\text{"h(P)"} \in \Gamma(S, \mathcal{O}_S^\times) = G_m(S).$$

One then defines (the *opposite* of [K 5, §5]),

$$<P, P'>_\pi = \text{"h(P)"}.$$

One verifies easily that this construction defines a bilinear pairing

$$(\mathrm{Ker}\ \pi)(S) \times (\mathrm{Ker}\ \pi^t)(S) \to G_m(S).$$

Because $(\mathrm{Ker}\ \pi)(S)$ is killed by N, the pairing lands in $\mu_N(S)$.

(2.8.2) According to the fundamental Cartier-Nishi duality theory (cf. [Oda]), this pairing defines an isomorphism of S-group-schemes

$$\mathrm{Ker}(\pi^t) \xrightarrow{\sim} \mathit{Hom}_{S\text{-gp}}(\mathrm{Ker}(\pi), G_m) \tag{2.8.2.1}$$

of $\mathrm{Ker}(\pi^t)$ with the Cartier dual of $\mathrm{Ker}(\pi)$.

(2.8.3) One also knows (cf. [Oda]) that this pairing is alternating, in the sense that

$$(<P, P'>_\pi)(<P', P>_{\pi^t}) = 1.$$

(2.8.4) Let π_1 and π_2 be composable isogenies of elliptic curves over a base-scheme S:

$$E_0 \underset{\pi_1^t}{\overset{\pi_1}{\rightleftarrows}} E_1 \underset{\pi_2^t}{\overset{\pi_2}{\rightleftarrows}} E_2 .$$

For any S-valued points

$$P_0 \in \mathrm{Ker}(\pi_1), \quad P_2 \in \mathrm{Ker}(\pi_1^t \circ \pi_2^t) ,$$

we have the formula

(2.8.4.1) $$\langle P_0, P_2 \rangle_{\pi_2 \circ \pi_1} = \langle P_0, \pi_2^t P_2 \rangle_{\pi_1} ,$$

as follows immediately from the above definition of $\langle\ ,\ \rangle$, via the interpretation of P_2 as a suitable line bundle on E_2.

(2.8.5) If we apply the discussion 2.8.1.2 to the N^2-isogeny "multiplication by N", which is self-dual (2.6.2.1), we obtain the "e_N-pairing"

(2.8.5.1) $$E[N] \times E[N] \to \mu_N$$

$$(P, Q) \mapsto \langle P, Q \rangle_N = e_N(P, Q) ,$$

which (by 2.8.3) is an alternating* autoduality of $E[N]$.

(2.8.5.2) To eliminate any possibility of sign ambiguity, let us state explicitly that on a complex torus C/L, for any two N-division points ℓ_1/N, ℓ_2/N, we have the formula

(2.8.5.3) $$e_N(\ell_1/N, \ell_2/N) = \exp\left(\frac{2\pi i}{N} \cdot \frac{\mathrm{Im}(\bar{\ell}_1 \ell_2)}{A(L)}\right) ,$$

where $A(L)$ is the area of a fundamental parallelogram for the lattice L.

(2.8.6) Let us return to an arbitrary N-isogeny

$$E \underset{\pi^t}{\overset{\pi}{\rightleftarrows}} E' .$$

We will apply (2.8.4.1) to the composable isogenies π and π^t. Because

*In fact, $e_N(P,P) = 1$, cf. Notes Added in Proof.

$\pi^t \pi = N$ (cf. the proof of 2.5.1) and $(\pi^t)^t = \pi$ by 2.6.2.1, the identity (2.8.4.1) becomes

(2.8.6.1) Let $\pi : E \to E'$ be an N-isogeny of elliptic curves over S. For $P \in (\mathrm{Ker}\ \pi)(S)$ and $Q \in E[N](S)$, we have

$$e_N(P, Q) = \langle P, \pi Q \rangle_\pi .$$

(2.8.7) As a consequence of (2.8.6.1), we see that the restriction of the e_N-pairing to $\mathrm{Ker}(\pi) \times \mathrm{Ker}(\pi)$ is trivial:

(2.8.7.1) any finite locally free subgroup-scheme of $E[N]$ of rank N is *isotropic* for the e_N-pairing.

(2.9) *Deformation theory* (cf. [Se-Ta 1], [Dr 2], [K-5])

THEOREM 2.9.1 (Serre-Tate). *Let R be a ring, I an ideal of R, p a prime number. Suppose that the ideal (I, p) is nilpotent. Let $N \geq 1$ be an integer divisible by p, and denote by R_0 the ring R/I. Consider the following three categories $\mathfrak{A}, \mathfrak{B}_N, \mathfrak{C}_N$:*

$\mathfrak{A}$: *objects are elliptic curves E/R, maps are R-homomorphisms*

$\mathfrak{B}_N$: *objects are quadruples $(E_0/R_0, G, (\ ,\ ), i)$ where E_0/R_0 is an elliptic curve, $G = \bigcup G[N^\nu]$ is an "N-divisible group" over R, $(\ ,\ )$ is a compatible family of alternating autodualities $(\ ,\ )_{N^\nu}$ on the $G[N^\nu]$'s,*

$$(NP, NQ)_{N^{\nu-1}} = ((P, Q)_{N^\nu})^N$$

for P, Q sections of $G[N^\nu]$, and i is an isomorphism of N-divisible groups over K_0 between $E_0[N^\infty]$ and $G \otimes_R R_0$ which carries the e_{N^ν}-pairings on the $E_0[N^\nu]$'s to the given

pairings $(\ ,\ )_{N^\nu}$ *on the* $G[N]\underset{R}{\otimes}R_0$*'s. Morphisms are pairs* (f_0, f) *with* f_0 *an* R_0*-homomorphism of elliptic curves,* f *an* R*-homomorphism of* N*-divisible groups, such that* f_0 *and* $f\underset{R}{\otimes}R_0$ *agree (via* i*) on the* N*-divisible groups over* R_0.

$\mathcal{C}_N$: *objects are triples* $(E_0/R_0, G, i)$ *where* E_0/R_0 *is an elliptic curve,* G/R *is an* N*-divisible group, and* i *is an* R_0*-isomorphism* $E_0[N^\nu] \xrightarrow{\sim} G\underset{R}{\otimes}R_0$ *of* N*-divisible groups, morphisms are pairs* (f_0, f) *as in* $\mathcal{B}_N$ *above.*

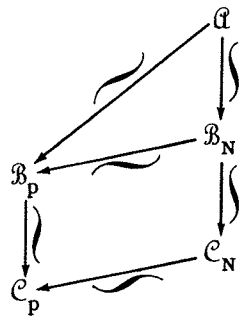
There are obvious functors $\mathcal{A} \to \mathcal{B}_N \to \mathcal{C}_N$, *defined by*

$$(E/R) \mapsto (E_0/R_0, E[N^\infty], \{e_{N^\nu}\}, \mathrm{id}), \quad (E_0/R_0, G, (\ ,\ ), i) \to (E_0/R_0, G, i).$$

These functors are equivalences of categories.

Proof. That the composite $\mathcal{A} \to \mathcal{C}_N$ is an equivalence of categories is the special case "dimension one" of the Serre-Tate theorem for abelian schemes (cf. [Mes] or [K-5] for a proof). Therefore $\mathcal{B}_N \to \mathcal{C}_N$ is essentially surjective. But $\mathcal{B}_N \to \mathcal{C}_N$ is visibly fully faithful – morphisms in $\mathcal{B}_N$ "don't know about $(\ ,\ )$" – hence $\mathcal{B}_N \to \mathcal{C}_N$ is an equivalence also. Therefore $\mathcal{A} \to \mathcal{B}_N$ is also an equivalence. Q.E.D.

REMARK 2.9.2. In the literature, the Serre-Tate theorem is usually stated only for $N = p$. This is the essential case, because the prime-to-p part of the N-divisible group is ind-etale over any ring R in which p is nilpotent, so contributes nothing to the categories $\mathcal{B}_N$, $\mathcal{C}_N$; in other words, we have a commutative diagram of equivalences for any N divisible by p:



THEOREM 2.9.3. *Let* k *be an algebraically closed field of characteristic* $p > 0$, E/k *an elliptic curve. Then the* p*-divisible group of* E *is, up to* k*-isomorphism, one of the following two* p*-divisible groups:*

1) $\mu_{p^\infty} \times Q_p/Z_p$ (*"ordinary"*)

2) *the unique* 1*-parameter formal Lie group over* k *of height two* (*"supersingular"*).

Proof. Any p-divisible group over an algebraically closed field is the product of a p-divisible commutative formal Lie group and a finite number of copies of Q_p/Z_p. So necessarily

$$E[p^\infty] = \hat{E} \times (Q_p/Z_p)^a$$

for some integer $a \geq 0$. Because $p: E \to E$ is finite flat of degree p^2 (2.3.1), we have

$$\mathrm{height}(\hat{E}) + a = 2.$$

If E has height *one*, then we have $\hat{E} \simeq \hat{G}_m = \mu_{p^\infty}$, because k is algebraically closed of characteristic $p > 0$, and this is case 1). The only other possibility is $\mathrm{height}(\hat{E}) = 2$, $a = 0$. Again one knows that over an algebraically closed k of characteristic $p > 0$, there is up to k-isomorphism a unique one-parameter formal Lie group of height two (or indeed of any height).

THEOREM 2.9.4. *In every characteristic* $p > 0$, *the second case occurs, and it occurs only a finite number of times.*

Proof. Let k be an algebraically closed field of characteristic $p > 0$, and E/k an elliptic curve. The Frobenius morphism

$$F : E \to E^{(p)}$$

visibly has degree p, so by (2.6.1) we have

$$F^t F = p .$$

As customary, we denote $F^t : E^{(p)} \to E$ by V:

$$E \xrightarrow{F} E^{(p)} \xrightarrow{V} E , \qquad E \xrightarrow{p} E .$$

By (2.6.1.1), V also has degree p. Therefore $\mathrm{Ker}(V)$ in $E^{(p)}$ is either *etale*, or it is *connected*, in which case it is equal to $\mathrm{Ker}(F^{(p)})$ in $E^{(p)}$, the unique connected subgroup-scheme of E/k which has rank p.

By (2.9.3), the curve E is supersingular if and only if $E[p]$ is connected. The short exact sequence of k-group-schemes

$$0 \longrightarrow \mathrm{Ker}\, F \longrightarrow E[p] \xrightarrow{F} \mathrm{Ker}\, V \longrightarrow 0$$

shows that $E[p]$ is connected if and only if $\mathrm{Ker}(V)$ is connected. Therefore E is supersingular if and only if $\mathrm{Ker}(V) = \mathrm{Ker}(F^{(p)})$.

To prove that there are only finitely many k-isomorphism classes of supersingular E, we notice that if E is supersingular, then the two isogenies

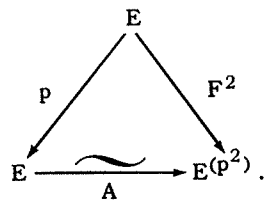
$$E^{(p)} \xrightarrow{V} E$$

$$E^{(p)} \xrightarrow{F^{(p)}} E^{(p^2)}$$

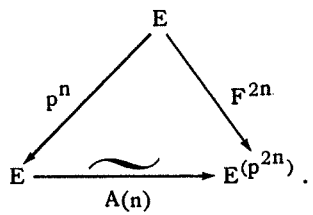
have the *same* kernels. Therefore we obtain a k-isomorphism

$$E \xrightarrow{A}_{\sim} E^{(p^2)}$$

sitting in a commutative diagram



Iterating this construction, we obtain for every integer $n \geq 1$ a commutative diagram



Choose an integer $N \geq 3$ prime to p, and an integer $n \geq 1$ such that $p^n \equiv 1 \mod N$ (for example, if $p \neq 2$, take $N = p-1$ and $n = 1$, and if $p = 2$ take $N = 3$, $n = 2$). The k-group-scheme $E[N]$ is k-isomorphic to $(\mathbf{Z}/N\mathbf{Z})^2$ (by (2.3.1), k being algebraically closed). Let us fix a k-isomorphism

$$\phi : (\mathbf{Z}/N\mathbf{Z})^2 \xrightarrow{\sim} E[N] .$$

Then $\phi^{(p^{2n})} = F^{2n} \circ \phi$ is such an isomorphism for $E^{(p^{2n})}$. Because $p^n \equiv 1 \mod N$, the commutative diagram above shows that

$$\phi^{(p^{2n})} = F^{2n} \circ \phi = A(n) \circ p^n \circ \phi = A(n) \circ \phi .$$

Therefore $A(n)$ defines a k-isomorphism

$$(E, \phi) \xrightarrow[A(n)]{\sim} (E^{(p^{2n})}, \phi^{(p^{2n})}) .$$

By rigidity of level $N \geq 3$ structures (2.7.2), and galois descent, this implies that (E, ϕ) is defined over $F_{p^{2n}}$. In particular, E is definable over $F_{p^{2n}}$, by a generalized Weierstrass equation (2.2.5.1) with coefficients in $F_{p^{2n}}$. Thus there are only finitely many supersingular E's in characteristic $p > 0$.

It remains to show that there *exist* supersingular elliptic curves in every characteristic. In characteristic 2, the curve $X^3+Y^3+Z^3 = 0$ is supersingular. In characteristic $p \geq 3$, a Legendre curve

$$y^2 = x(x-1)(x-\lambda)$$

is supersingular precisely when the Hasse invariant (i.e., the tangent map of $V: E^{(p)} \to E$) vanishes.

A standard calculation [Mum 4, p. 216] shows that for the Legendre family, the Hasse invariant is a polynomial in λ of degree $(p-1)/2$. We refer to [Ig 1] for Igusa's elegant proof that this polynomial has $(p-1)/2$ distinct roots, all of which are different from $0, 1, \infty$. Thus there are $(p-1)/2$ values of λ in characteristic $p \geq 3$ for which the corresponding elliptic curve is supersingular. Q.E.D.

REMARK 2.9.5. An alternate approach to showing the existence of supersingular elliptic curves in characteristic p is to construct them explicitly by means of the theory of complex multiplication [Deu]. Let K be a quadratic imaginary field, $\mathcal{O}_K$ its ring of integers, and $K \hookrightarrow \mathbf{C}$ a complex embedding. Then $\mathcal{O}_K$ is a lattice in $\mathbf{C}$, and the quotient $\mathbf{C}$ modulo $\mathcal{O}_K$ is an elliptic curve E over $\mathbf{C}$ with complex multiplication by $\mathcal{O}_K$. One knows that E is definable over a subfield of $\mathbf{C}$ which is a finite extension of $\mathbf{Q}$, and that over a sufficiently large such finite extension, say L, this elliptic curve has "everywhere good reduction", i.e., there exists an elliptic curve E over $\mathcal{O}_L$, the ring of all algebraic integers in L, whose complex fiber is the original E.

This being the case, for any maximal ideal $\mathfrak{p}$ of $\mathcal{O}_L$, with residue field $F_\mathfrak{p}$, we may speak of the reduction modulo $\mathfrak{p}$ of E, i.e., of the elliptic curve

$$E \otimes_{\mathcal{O}_L} F_\mathfrak{p}$$

over the finite field $F_\mathfrak{p}$. Denoting by p the characteristic of $F_\mathfrak{p}$, one knows that $E \otimes F_\mathfrak{p}$ is ordinary if and only if the rational prime p *splits* in the quadratic extension $K/\mathbf{Q}$. Equivalently, $E \otimes F_\mathfrak{p}$ is supersingular if and only if the rational prime p either ramifies or stays prime in K.

To obtain a supersingular elliptic curve in a given characteristic $p > 0$, simply take for K the field $\mathbf{Q}(\sqrt{-p})$, a quadratic imaginary field in which p is visibly ramified.

Chapter 3

THE FOUR BASIC MODULI PROBLEMS FOR ELLIPTIC CURVES: SORITES

Let S be a scheme, E/S an elliptic curve over S, and $N \geq 1$ an integer. We will make use of the Drinfeldian ideas of the first chapter to define four sorts of "level structure" on E/S, which correspond to the classical notions of $\Gamma(N)$, $\Gamma_1(N)$, "balanced"-$\Gamma_1(N)$, and $\Gamma_0(N)$ structures (and which coincide with these notions when N is invertible on S).

(3.1) $\Gamma(N)$-*structures*

A $\Gamma(N)$-structure on E/S (also called a "full level N structure", or a "Drinfeld basis of $E[N]$") is a group homomorphism

$$\phi : (\mathbf{Z}/N\mathbf{Z})^2 \to E[N](S) \tag{3.1.1}$$

which is a "generator" of $E[N]$ in the sense of Chapter 1, 1.5. Explicitly, this means that we have an equality of effective Cartier divisors in E:

$$E[N] = \sum_{a,b \bmod N} [\phi(a,b)] \tag{3.1.2}$$

or equivalently that the N^2 sections $\phi(a,b)$ of $E[N](S)$ form a "full set of sections." The points

$$P = \phi(1,0), \qquad Q = \phi(0,1)$$

in $E[N](S)$ are the corresponding "Drinfeld basis" of $E[N]$.

(3.2) $\Gamma_1(N)$-*structures*

A $\Gamma_1(N)$-structure on E/S, also called a point of "exact order N" in $E(S)$, is a homomorphism

$$\phi : \mathbf{Z}/N\mathbf{Z} \to E[N](S) \tag{3.2.1}$$

which is a "$\mathbf{Z}/N\mathbf{Z}$-structure on $E[N]/S$" in the sense of 1.5.1. Explicitly, this means that the effective Cartier divisor in E

$$\sum_{a \bmod N} [\phi(a)] \tag{3.2.2}$$

is a subgroup-scheme of E. The point

$$P = \phi(1)$$

in $E[N](S)$ is the corresponding point of "exact order N."

Equivalently, a $\Gamma_1(N)$-structure on E/S is an N-isogeny of elliptic curves over S

$$E \xrightarrow{\pi} E' \tag{3.2.3}$$

(by definition, a homomorphism which is finite locally free of degree N) together with a *generator* of $\operatorname{Ker} \pi$, i.e., a point

$$P \in (\operatorname{Ker} \pi)(S) \subset E[N](S) \tag{3.2.4}$$

such that the corresponding homomorphism

$$\begin{aligned} \phi : \mathbf{Z}/N\mathbf{Z} &\longrightarrow \operatorname{Ker} \pi \\ a &\longmapsto aP \end{aligned}$$

is a "generator" of $\operatorname{Ker} \pi$ in the sense of the 1.4.1, i.e., such that we have an equality of effective Cartier divisors in E

$$\operatorname{Ker} \pi = \sum_{a \bmod N} [aP]. \tag{3.2.5}$$

(3.3) *Balanced* $\Gamma_1(N)$*-structures*

A *balanced* $\Gamma_1(N)$-structure on E/S is a diagram

$$P;\ E \underset{\pi^t}{\overset{\pi}{\rightleftarrows}} E';\ P' \tag{3.3.1}$$

in which E' is an elliptic curve over S, π is an N-isogeny, π^t is the dual N-isogeny ($\pi^t\pi = N_E$, $\pi\pi^t = N_{E'}$), $P \in (\mathrm{Ker}\,\pi)(S)$ is a generator of $\mathrm{Ker}\,\pi$, and $P' \in (\mathrm{Ker}\,\pi^t)(S)$ is a generator of $\mathrm{Ker}\,\pi^t$.

Less symmetrically, we can (by SGA III, Exp. V, 4.1) describe a balanced $\Gamma_1(N)$-structure on E/S purely "on E" as consisting of an f.p.p.f. short exact sequence of group-schemes on S

$$0 \to K \to E[N] \to K' \to 0\,, \tag{3.3.2}$$

with K and K' both locally free of rank N, together with points

$$P \in K(S), \qquad P' \in K'(S) \tag{3.3.3}$$

which are generators of K and K' respectively.

(3.4) $\Gamma_0(N)$*-structures*

A $\Gamma_0(N)$-structure on E/S is an N-isogeny

$$E \xrightarrow{\pi} E' \tag{3.4.1}$$

which is *cyclic* in the sense that locally f.p.p.f. on S, the kernel $\mathrm{Ker}(\pi)$ admits a generator. Equivalently, a $\Gamma_0(N)$-structure on E/S is a finite flat subgroup-scheme

$$K \subset E[N]\,, \tag{3.4.2}$$

locally free of rank N, which is *cyclic* in the sense that locally f.p.p.f. on S, it admits a generator.

(3.5) *Factorization into prime powers*

LEMMA (3.5.1). *Suppose that* $N = AB$ *with* A *and* B *relatively prime. Then for any elliptic curve* E/S, *we have functorial isomorphisms*

$$\Gamma(N)\text{-Str}(E/S) \xrightarrow{\sim} \Gamma(A)\text{-Str}(E/S) \times \Gamma(B)\text{-Str}(E/S)$$

$$\Gamma_1(N)\text{-Str}(E/S) \xrightarrow{\sim} \Gamma_1(A)\text{-Str}(E/S) \times \Gamma_1(B)\text{-Str}(E/S)$$

$$\mathrm{Bal}\,\Gamma_1(N)\text{-Str}(E/S) \xrightarrow{\sim} \mathrm{Bal}\,\Gamma_1(A)\text{-Str}(E/S) \times \mathrm{Bal}\,\Gamma_1(B)\text{-Str}(E/S)$$

$$\Gamma_0(N)\text{-Str}(E/S) \xrightarrow{\sim} \Gamma_0(A)\text{-Str}(E/S) \times \Gamma_0(B)\text{-Str}(E/S)\,.$$

Proof-construction. For any abelian group G killed by N, we have two distinct canonical isomorphisms

$$G \longrightarrow G[A] \times G[B] \tag{3.5.1.1}$$

of G with the products of its A-torsion and B-torsion subgroups. The first is the inverse of the "sum" map

$$G[A] \times G[B] \overset{\text{sum}}{\xrightarrow{\sim}} G\,, \tag{3.5.1.2}$$

the second is

$$\begin{aligned} G &\xrightarrow{\sim} G[A] \times G[B] \\ g &\longmapsto (Bg, Ag)\,. \end{aligned} \tag{3.5.1.3}$$

[The second is (A+B) times the first.] Applying *either* of these decompositions to our structures defines isomorphisms of the kind desired as follows easily from the general theorems of factorization into prime powers of "A-structures" and "A-generators", cf., (1.7.3). For definiteness, let us choose the *second*. Then explicitly the isomorphisms are given by

$$\begin{cases} \text{for } \Gamma(N): & \text{Drinfeld basis } (P,Q) \mapsto \text{Drinfeld bases } (BP, BQ), \text{ and } (AP, AQ) \\ \text{for } \Gamma_1(N): & \text{point } \underline{P} \text{ of exact order } N \mapsto \text{points } BP,\ AP \text{ of exact orders } A, B \\ \text{for } \Gamma_0(N): & \text{cyclic subgroup-scheme } K \text{ of order } N \mapsto \text{cyclic subgroups } K[A],\ K[B] \text{ of orders } A, B. \end{cases}$$

To make explicit the isomorphism for balanced $\Gamma_1(N)$-structures, we view such a structure "asymmetrically", as an f.p.p.f. short exact sequence together with generators of end terms

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & E[N] & \longrightarrow & K' & \longrightarrow & 0\,. \\ & & \cup & & & & \cup & & \\ & & P & & & & P' & & \end{array}$$

The associated balanced $\Gamma_1(A)$-structure is then

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K[A] & \longrightarrow & E[A] & \longrightarrow & K'[A] & \longrightarrow & 0 \\ & & \cup & & & & \cup & & \\ & & BP & & & & BP' & & \end{array}$$

and similarly for the $\Gamma_1(B)$-structure (just interchange A and B). Q.E.D.

(3.6) *Relative representability*

RELATIVE REPRESENTABILITY THEOREM (3.6.0). *Fix an elliptic curve* E/S, *and an integer* $N \geq 1$. *Consider the three functors on* (Sch/S) *defined by*

$$T \mapsto \begin{cases} \Gamma(N)\text{-structures on } E_T/T \\ \Gamma_1(N)\text{-structures on } E_T/T \\ \text{balanced } \Gamma_1(N)\text{-structures on } E_T/T\,. \end{cases}$$

Each of these functors is represented by a finite S*-scheme.*

Proof. For the first two functors, this is a special case of the representability results of the previous chapter, in whose notations the first two functors are respectively

$$(\mathbf{Z}/N\mathbf{Z})^2\text{-}Gen(E[N]/S) \quad \text{and} \quad \mathbf{Z}/N\mathbf{Z}\text{-}Str(E/S)\,.$$

The third functor is represented by a scheme finite over $\mathbf{Z}/N\mathbf{Z}\text{-}Str(E/S)$, namely the scheme

$$\mathbf{Z}/N\mathbf{Z}\text{-}Gen\Big(K' \Big/ \Big(\mathbf{Z}/N\mathbf{Z}\text{-}Str(E/S)\Big)\Big)\,,$$

where K' is the tautological *quotient* of $E[N]$ by the subgroup K specified by a $\mathbf{Z}/N\mathbf{Z}$-structure on $E[N]$. Q.E.D.

REMARK (3.6.1). We will see later that the functor of $\Gamma_0(N)$-structures on E/S is also representable by a finite S-scheme, but this fact lies much deeper.

If we apply the factorization lemma (1.7.3) to the finite schemes representing these functors, we obtain

COROLLARY (3.6.2). *If* $N = AB$ *with* $(A, B) = 1$, *then the constructions (3.5.1.3) define canonical isomorphisms of finite* S*-schemes*

$$\Gamma(N)\text{-}Str(E/S) \xrightarrow{\sim} \Gamma(A)\text{-}Str(E/S) \underset{S}{\times} \Gamma(B)\text{-}Str(E/S)$$

and similarly for Γ_1 *and for balanced* Γ_1.

REMARK (3.6.2.1). Similarly, the functor $\Gamma_0(N)\text{-}Str(E/S)$ on (Sch/S) defined by

$$T \mapsto \Gamma_0(N)\text{-structures on } E_T/T$$

admits a canonical product decomposition, as functor on (Sch/S),

$$\Gamma_0(N)\text{-}Str(E/S) \xrightarrow{\sim} \Gamma_0(A)\text{-}Str(E/S) \underset{S}{\times} \Gamma_0(B)\text{-}Str(E/S)\ .$$

This decomposition reduces the problem of proving representability for $\Gamma_0(N)$ to the case when N is a power of a prime.

PROPOSITION (3.6.3). *Let* E *and* E' *be elliptic curves over a base scheme* S. *Suppose that we are given an isomorphism of* S*-group-schemes*

$$E[N] \xrightarrow{\sim} E'[N]\ .$$

Then we have induced isomorphisms of functors on (Sch/S)

$$\Gamma(N)\text{-}Str(E'/S) \xrightarrow{\sim} \Gamma(N)\text{-}Str(E/S)$$

and similarly for $\Gamma_1(N)$, *balanced* $\Gamma_1(N)$, *and* $\Gamma_0(N)$.

Proof. Indeed all of these sorts of structures depend only on the underlying S-group-scheme $E[N]$. Q.E.D.

(3.7) *The situation when* N *is invertible*

THEOREM 3.7.1. *Let* $N \geq 1$ *be an integer,* S *a scheme on which* N *is invertible* (*i.e.,* S *is a* $\mathbf{Z}[1/N]$*-scheme*), *and* E/S *an elliptic curve. Consider the four functors on* (Sch/S) *given by*

$$T \mapsto \begin{cases} \Gamma(N)\text{-structures on } E_T/T \\ \Gamma_1(N)\text{-structures on } E_T/T \\ \text{balanced } \Gamma_1(N)\text{-structures on } E_T/T \\ \Gamma_0(N)\text{-structures on } E_T/T\ . \end{cases}$$

Each is represented by a finite etale S*-scheme.*

Proof. Because N is invertible on S, the group-scheme $E[N]$ is finite etale over S, locally (etale) isomorphic to $(\mathbf{Z}/N\mathbf{Z})^2$ (cf. 2.3.1). The

assertion for $\Gamma(N)$ (resp. for $\Gamma_1(N)$) therefore results immediately from 1.6.7 applied to $E[N]/S$ (resp. from 1.6.4 applied to $A = \mathbf{Z}/N\mathbf{Z}$, $C = E$). The assertion for balanced $\Gamma_1(N)$ results by combining 1.6.4 for $A = \mathbf{Z}/N$, $C = E$ over S with 1.6.7 applied to the base scheme $A\text{-}Str(E/S)$, the group $A = \mathbf{Z}/N\mathbf{Z}$, and the quotient group-scheme $G = E[N] \bmod K_{univ}$ inside the curve $E \bmod K_{univ}$, where K_{univ} is the tautological subgroup of $E[N]$ specified by the universal $\mathbf{Z}/N\mathbf{Z}$-structure.

For the $\Gamma_0(N)$-problem, we argue as follows. The functor in question is an etale sheaf (etale descent (SGA I, 7.9) for finite locally free subgroup-schemes of $E[N]$, and the fact that the notion of cyclicity is by definition local for the f.p.p.f. topology, so a fortiori for the etale topology). Therefore by etale descent it suffices to show that after a surjective etale base change $S' \to S$, the $\Gamma_0(N)$ problem *becomes* representable by a finite etale S'-scheme. By 2.3.1, we may make such a base change and reduce to the case when $E[N]$ is the constant group-scheme $(\mathbf{Z}/N\mathbf{Z})^2$. In this case, we claim that the $\Gamma_0(N)$ functor is represented by the constant S-scheme

$$S \times \{\text{the set of cyclic subgroups of order } N \text{ in } (\mathbf{Z}/N\mathbf{Z})^2\}\ .$$

To show this, it suffices to check that over any connected scheme T, any finite locally-free closed subgroup-scheme K of rank N of a constant (e.g., $(\mathbf{Z}/N\mathbf{Z})^2$) finite locally-free group-scheme G over T is itself constant. For once we know this, it follows from 1.10.12 (3) that our constant group-scheme K is cyclic in the sense of f.p.p.f.-locally admitting a generator if and only if the abstract group $K(T)$ is a cyclic group of order N.

To prove that K is constant, we may reduce easily to the case where T is connected and noetherian (EGA IV, 8.9.1, 11.2.6.1). Then K is finite etale over T, because it is both "net" [De-Ga I, 4,3.1-2], being a closed subscheme of an etale (because constant) T-scheme, and finite flat over T.

Finally, over any connected, locally noetherian scheme T, any finite etale T-subscheme K of a constant finite etale T-scheme G is itself constant. To see this, pick a geometric point t of T. In view of the standard theory of the fundamental group (SGA I, Exp V, §7), a finite etale T-scheme K is constant if and only if the action of $\pi_1(T,t)$ on the fiber $K(t)$ is trivial, and by assumption, $K(t)$ is a $\pi_1(T,t)$-stable subset of the finite $\pi_1(T,t)$-set $G(t)$, which has *trivial* action of π_1. Q.E.D.

COROLLARY 3.7.2. *Let $N \geq 1$ be an integer, S a scheme on which N is invertible, and E/S an elliptic curve. Suppose that $E[N]$ is S-isomorphic to the constant group-scheme $(\mathbf{Z}/N\mathbf{Z})^2$ (a condition which by 3.7.1 is always fulfilled after a finite etale surjective base-change $S' \to S$). Then the four functors on (Sch/S) defined by*

$$T \mapsto \left\{ \begin{array}{l} \Gamma(N)\text{-structures} \\ \Gamma_1(N)\text{-structures} \\ \text{balanced } \Gamma_1(N)\text{-structures} \\ \Gamma_0(N)\text{-structures} \end{array} \right\} \text{ on } E_T/T$$

are represented by the constant S-schemes

$S \times \{$*the set of* $\mathbf{Z}/N\mathbf{Z}$*-bases of* $(\mathbf{Z}/N\mathbf{Z})^2\}$

$S \times \{$*the set of elements* P *of* $(\mathbf{Z}/N\mathbf{Z})^2$ *having exact order* $N\}$

$S \times \{$*the set of triples* (K, P, P') *consisting of a cyclic subgroup* K *of* $(\mathbf{Z}/N\mathbf{Z})^2$ *of order* N, *a generator* P *of* K, *and a generator* P' *of the quotient* $(\mathbf{Z}/N\mathbf{Z})^2$ *modulo* $K\}$

$S \times \{$*the set of cyclic subgroups of* $(\mathbf{Z}/N\mathbf{Z})^2$ *of order* $N\}$.

Proof. For $\Gamma(N)$, this is obvious from 1.10.12 (3). For $\Gamma_0(N)$, this was proven in the course of proving 3.7.1. From the result for $\Gamma_0(N)$, the results for $\Gamma_1(N)$ (resp. for balanced $\Gamma_1(N)$) follow immediately from 1.10.12 (3) applied to $A = \mathbf{Z}/N\mathbf{Z}$ and to $G = K$ (resp. to $G = K$ and to $G = (\mathbf{Z}/N\mathbf{Z})^2$ modulo K). Q.E.D.

Chapter 4
THE FORMALISM OF MODULI PROBLEMS

(4.1) *The category* (Ell)

Consider the category (Ell) whose objects are elliptic curves

(4.1.1)
$$\begin{array}{c} E \\ \downarrow \pi \\ S \end{array}$$

over variable base-schemes, and whose morphisms are cartesian squares of elliptic curves

(4.1.2)
$$\begin{array}{ccc} E_1 & \xrightarrow{a} & E \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi} \\ S_1 & \xrightarrow{f} & S \end{array}$$

i.e., commutative squares such that the induced morphism of S_1-schemes

(4.1.3)
$$E_1 \xrightarrow{(a, \pi_1)} E \underset{S}{\times} S_1$$

is an isomorphism of elliptic curves over S_1. This category (Ell) is the "modular stack" of Deligne-Rapoport (cf. [De-Ra]).

(4.2) *Moduli problems*

A contravariant functor $\mathcal{P}$ from (Ell) to (Sets) is called a moduli problem for elliptic curves. Given an elliptic curve E/S, an element of

the set $\mathcal{P}(E/S)$ is called a "level $\mathcal{P}$ structure" on E/S. The moduli problem $\mathcal{P}$ is said to be relatively representable over (Ell) if for every elliptic curve E/S, the functor on (Sch/S) defined by

$$T \mapsto \mathcal{P}(E_T/T)$$

is representable by an S-scheme denoted $\mathcal{P}_{E/S}$.

(4.3) *Representable moduli problems*

The moduli problem $\mathcal{P}$ is said to be representable if it is representable as a functor on (Ell), i.e., if there exists an elliptic curve over a scheme

$$\begin{array}{c} E \\ \downarrow \\ \mathfrak{M}(\mathcal{P}) \end{array}$$

together with a functorial isomorphism

$$\mathcal{P}(E/S) \simeq \mathrm{Hom}_{(Ell)}(E/S, E/\mathfrak{M}(\mathcal{P})) .$$

If the moduli problem $\mathcal{P}$ is representable, the scheme $\mathfrak{M}(\mathcal{P})$ is easily seen to represent the functor on (Sch)

$$\begin{array}{ll} & S \mapsto \text{isomorphism classes of pairs } (E/S, \alpha) \\ (4.3.1) & \qquad \text{with } E \text{ an elliptic curve over } S \text{ and} \\ & \qquad \alpha \in \mathcal{P}(E/S) \text{ a "level } \mathcal{P} \text{ structure" on } E/S . \end{array}$$

Conversely, if this moduli problem on (Sch) is representable by a scheme $\mathfrak{M}(\mathcal{P})$ with universal object $(E/\mathfrak{M}(\mathcal{P}), \alpha)$ and if $\mathcal{P}$ is rigid (4.4), then $\mathcal{P}$ is easily seen to be represented by the object $E/\mathfrak{M}(\mathcal{P})$ of (Ell).

(4.3.2) Any representable moduli problem $\mathcal{P}$ is relatively representable over (Ell); indeed for any E/S we have a natural isomorphism of S-schemes

$$(4.3.3) \qquad \mathcal{P}_{E/S} \simeq Isom_{S\times\mathfrak{M}(\mathcal{P})}(\mathrm{pr}_1^*(E), \mathrm{pr}_2^*(E)) .$$

(4.3.4) If $\mathcal{P}$ is representable, and $\mathcal{P}'$ is relatively representable, then the product, or "simultaneous", moduli problem

$$E/S \mapsto \mathcal{P}(E/S) \times \mathcal{P}'(E/S)$$

is representable; indeed if $E/\mathfrak{M}(\mathcal{P})$ represents $\mathcal{P}$, then we have

$$\mathfrak{M}(\mathcal{P}, \mathcal{P}') = \mathcal{P}'_{E/\mathfrak{M}(\mathcal{P})} .$$

(4.3.5) Any particular elliptic curve E/S tautologically defines a representable moduli problem, namely

$$\mathrm{Hom}_{(Ell)}(\quad, E/S) ,$$

the moduli problem of " E/S-structures" on variable elliptic curves E_1/S_1:

$$\begin{array}{l} E_1/S_1 \mapsto \text{pairs } (f, \alpha) \text{ where } f : S_1 \to S \\ \qquad\qquad \text{is a morphism and where} \\ \qquad\qquad \alpha : E_1 \xrightarrow{\sim} f^*(E) \text{ is an isomorphism} \\ \qquad\qquad \text{of elliptic curves over } S_1 . \end{array}$$

(4.4) *Rigid moduli problems*

A moduli problem $\mathcal{P}$ is said to be rigid if for any elliptic curve E/S and any level $\mathcal{P}$ structure $\alpha \in \mathcal{P}(E/S)$ on E/S, the pair $(E/S, \alpha)$ has no non-trivial automorphism (i.e., the group $\mathrm{Aut}(E/S)$ acts freely on the set $\mathcal{P}(E/S)$, for every E/S). Any representable moduli problem is rigid (as is visible from the explicit description above of representable problems)!

(4.5) *Geometric properties of moduli problems*

Let P be a property of morphisms of schemes. A moduli problem $\mathcal{P}$ is said to be "of type P" over (Ell) if it is relatively representable over (Ell) and if for every E/S, the morphism of schemes

$$\begin{array}{c} \mathcal{P}_{E/S} \\ \downarrow \\ S \end{array}$$

has property P. For example, to say that $\mathcal{P}$ is etale over (Ell) means that it is relatively representable, locally of finite presentation, and that for every elliptic curve E/S and every closed subscheme $S_0 \subset S$ defined by a nilpotent ideal, the natural map

$$\mathcal{P}(E/S) \to \mathcal{P}(E \underset{S}{\times} S_0/S_0)$$

is bijective (i.e., "level $\mathcal{P}$ structures don't see nilpotents").

The representable moduli problems

$$\begin{cases} \text{Weierstrass with } \Delta = 1 \quad (2.2.7) \\ \text{Legendre} \quad (2.2.9) \\ \text{naive level three} \quad (2.2.11) \end{cases}$$

are each etale over (Ell), and the disjoint union of the last two is etale and surjective over (Ell).

(4.6) *Some examples*

The basic example of a moduli problem $\mathcal{P}$ etale over (Ell) is provided by the "naive" level N moduli problem ($N \geq 1$ arbitrary)

$$E/S \mapsto \text{the set of S-group-scheme isomorphisms}$$

$$(\mathbf{Z}/N\mathbf{Z})^2 \xrightarrow{\sim} E[N].$$

The corresponding S-scheme $\mathcal{P}_{E/S}$ is concentrated over $S[1/N]$, over which it is a finite etale $GL(2, \mathbf{Z}/N\mathbf{Z})$-torsor.

(4.6.1) We have already seen explicitly (2.2.11) that for $N = 3$ the naive level N moduli problem is representable, and its representing scheme is a smooth affine connected curve over $\mathbf{Z}[1/3]$.

(4.6.2) Another example of a moduli problem $\mathcal{P}$ which is etale over (Ell) is the Legendre moduli problem 2.2.9

$$\begin{aligned} E/S \mapsto \text{pairs } (\phi_2, w) \text{ consisting of an S-group-scheme} \\ \text{isomorphism } \phi_2 : (\mathbf{Z}/2\mathbf{Z})^2 \xrightarrow{\sim} E[2] \text{ together} \\ \text{with an S-basis } \omega \text{ of } \omega_{E/S} \text{ for which the} \\ \text{adapted } x \text{ satisfies } x(P_2) = 0, \ x(Q_2) = 1. \end{aligned}$$

The corresponding S-scheme $\mathcal{P}_{E/S}$ is concentrated over $S[1/2]$, over which it is a finite etale $GL(2, \mathbf{Z}/2\mathbf{Z}) \times \{\pm 1\}$ torsor.

(4.7) *A basic result: representability and rigidity*

SCHOLIE (4.7.0) *Let $\mathcal{P}$ be relatively representable and affine over (Ell); then a necessary and sufficient condition that $\mathcal{P}$ be representable is that $\mathcal{P}$ be rigid.*

Proof. As already pointed out above (4.4), any representable problem is automatically rigid. Conversely, suppose $\mathcal{P}$ is rigid, relatively representable and affine. We must show it is represented, by an

$$\begin{array}{c} E, a_{univ} \in \mathcal{P}(E/\mathcal{M}(\mathcal{P})) \\ \downarrow \\ \mathcal{M}(\mathcal{P}) \end{array}$$

where $\mathcal{M}(\mathcal{P})$ is an affine Z-scheme. For this, it suffices to show that $\mathcal{P}$ is separately representable over both $\mathbf{Z}[1/2]$ and over $\mathbf{Z}[1/3]$, (the rigidity of $\mathcal{P}$ will then provide a unique isomorphism between the restrictions to $\mathbf{Z}[1/6]$ of the representing objects, giving a representing object over Z by "recollement").

To show the representability separately over $\mathbf{Z}[1/2]$ and $\mathbf{Z}[1/3]$, we will make use of the Legendre and of the naive level three moduli problems discussed in 4.6 above. To clarify the argument, we will axiomatize it.

Let $N \geq 1$ be an integer, G a finite group, and $\mathcal{S}$ a relatively representable and affine moduli problem on (Ell) which satisfies the following axioms:

1) $\mathcal{S}$ is representable, by an affine $\mathbf{Z}[1/N]$-scheme
2) G operates upon $\mathcal{S}$, in such a way that for every elliptic curve E/S with S a $\mathbf{Z}[1/N]$-scheme, the S-scheme $\mathcal{S}_{E/S}$ is a finite etale G-torsor.

We claim that over $\mathbf{Z}[1/N]$, $\mathcal{P}$ is represented by the affine $\mathbf{Z}[1/N]$-scheme

$$\mathcal{M}(\mathcal{P}, \mathcal{S})/G .$$

Once we have verified this claim, we simply apply it successively with ($N = 2$, $\mathcal{S}$ = Legendre problem, $G = GL(2, \mathbf{Z}/2\mathbf{Z}) \times \{\pm 1\}$) and with ($N = 3$, $\mathcal{S}$ = naive level three problem, $G = GL(2, \mathbf{F}_3)$).

To prove the claim, we argue as follows. Because $\mathcal{S}$ is representable, and $\mathcal{P}$ is relatively representable, the simultaneous problem $(\mathcal{P}, \mathcal{S})$ is representable, by

$$\mathcal{M}(\mathcal{P}, \mathcal{S}) = \mathcal{P}_{E/\mathcal{M}(\mathcal{S})} .$$

Because $\mathcal{M}(\mathcal{S})$ is affine, and $\mathcal{P}$ is affine over (Ell), the scheme $\mathcal{M}(\mathcal{P}, \mathcal{S})$ is affine over $\mathcal{M}(\mathcal{S})$, hence absolutely affine. Let G operate upon $\mathcal{M}(\mathcal{P}, \mathcal{S})$ through its action on $\mathcal{S}$.

Consider the universal curve

$$\begin{array}{c} E;\ (\alpha_{univ}, \beta_{univ}) \in (\mathcal{P} \times \mathcal{S})(E/\mathcal{M}(\mathcal{P}, \mathcal{S})) \\ \Big\downarrow \\ \mathcal{M}(\mathcal{P}, \mathcal{S}) . \end{array}$$

We will descend (E, α_{univ}) to $\mathcal{M}(\mathcal{P}, \mathcal{S})/G$. To do this, we argue as follows.

The action of $g \in G$ on $\mathcal{M}(\mathcal{P}, \mathcal{S})$ is defined as follows; the curve

$$\begin{array}{c} E, \text{ with } (\alpha_{univ}, g\beta_{univ}) \\ \Big\downarrow \\ \mathcal{M}(\mathcal{P}, \mathcal{S}) \end{array}$$

is an elliptic curve with $(\mathcal{P}, \mathcal{S})$-structure over $\mathcal{M}(\mathcal{P}, \mathcal{S})$, so it is "classified" by a unique morphism

$$g : \mathcal{M}(\mathcal{P}, \mathcal{S}) \to \mathcal{M}(\mathcal{P}, \mathcal{S}) ,$$

for which we have an isomorphism

$$g^*(E, \alpha_{univ}, \beta_{univ}) \xrightarrow{\theta(g)}{\sim} (E, \alpha_{univ}, g\beta_{univ})$$

over $\mathcal{M}(\mathcal{P}, \mathcal{S})$. *Forgetting* β_{univ}, $\theta(g)$ defines an $\mathcal{M}(\mathcal{P}, \mathcal{S})$-isomorphism

$$\theta(g) : g^*(E, \alpha_{univ}) \xrightarrow{\sim} (E, \alpha_{univ}) .$$

Because the moduli problem $\mathcal{P}$ is *rigid*, the object (E, α_{univ}) has no non-trivial automorphisms. Therefore $\theta(g)$ is the unique $\mathcal{M}(\mathcal{P}, \mathcal{S})$-isomorphism between $g^*(E, \alpha_{univ})$ and (E, α_{univ}). By *uniqueness*, $\theta(g)$ must be compatible with composition of elements of G, (i.e., $g \mapsto \theta(g)$ is a one-cocycle).

By axiom 2) and the rigidity of $\mathcal{P}$, G operates freely on $\mathcal{M}(\mathcal{P}, \mathcal{S})$. Because $\mathcal{M}(\mathcal{P}, \mathcal{S})$ is affine, the quotient $\mathcal{M}(\mathcal{P}, \mathcal{S})/G$ exists, and the projection

$$\begin{array}{c} \mathcal{M}(\mathcal{P}, \mathcal{S}) \\ \Big\downarrow \pi_{univ} \\ \mathcal{M}(\mathcal{P}, \mathcal{S})/G \end{array}$$

is a finite etale G-torsor [De-Ga III, 2,6.1] (SGA III, Exp V, 4.1). Because $g \mapsto \theta(g)$ is compatible with composition, θ is descent data for

(E, α_{univ}) relative to this projection. Because E is projective, via $I^{-1}(0)$, it descends, and because $\mathcal{P}$ is relatively affine, α_{univ} descends (SGA I, Exp VIII, 7.8, 1.2 and 1.7). Thus we obtain an object

$$\begin{array}{c} E_0, \alpha_{univ,0} \in \mathcal{P}(E_0/(\mathcal{M}(\mathcal{P},\mathcal{S})/G)) \\ \downarrow \\ \mathcal{M}(\mathcal{P},\mathcal{S})/G\ , \end{array}$$

whose pull-back to $\mathcal{M}(\mathcal{P},\mathcal{S})$ is the original (E, α_{univ}).

It remains to show that $(E_0, \alpha_{univ,0})$ over $\mathcal{M}(\mathcal{P},\mathcal{S})/G$ does in fact represent $\mathcal{P}$ over $\mathbf{Z}[1/N]$. Let S be a $\mathbf{Z}[1/N]$-scheme, and $(E/S, \alpha \in \mathcal{P}(E/S))$ an elliptic curve over S with level $\mathcal{P}$-structure. We must show that it is induced from $(E_0, \alpha_{univ,0})$ by a unique map $S \to \mathcal{M}(\mathcal{P},\mathcal{S})/G$. For this, consider the finite etale G-torsor over S

$$\begin{array}{c} \mathcal{S}_{E/S} \\ \downarrow \pi \\ S\ , \end{array}$$

over which E acquires its universal level $\mathcal{S}$-structure β_{univ}. The classifying map for $(E \underset{S}{\times} \mathcal{S}_{E/S}, \alpha, \beta_{univ})$ is a map

$$\mathcal{S}_{E/S} \xrightarrow{f} \mathcal{M}(\mathcal{P},\mathcal{S})$$

which is (tautologically) G-equivariant. Passing to quotients by G yields a map f_0 which sits in a commutative diagram

$$\begin{array}{ccc} \mathcal{S}_{E/S} & \xrightarrow{f} & \mathcal{M}(\mathcal{P},\mathcal{S}) \\ \downarrow \pi & & \downarrow \pi_{univ} \\ S & \xrightarrow{f_0} & \mathcal{M}(\mathcal{P},\mathcal{S})/G\ . \end{array}$$

Because the vertical arrows are finite etale G-torsors, the G-equivariance of f guarantees that this diagram is cartesian.

We must show that a), $f_0^*(E_0, \alpha_{univ,0})$ is isomorphic to (E, α), and that b), f_0 is the unique map of S to $\mathcal{M}(\mathcal{P},\mathcal{S})/G$ for which this is true. To establish a), we note that because $\mathcal{P}$ is *rigid*, and π is etale and surjective, it suffices to show that on $\mathcal{S}_{E/S}$, $\pi^* f_0^*(E_0, \alpha_{univ,0})$ is isomorphic to $\pi^*(E, \alpha)$. But this is clear from the commutativity of the above diagram, and the definition of f.

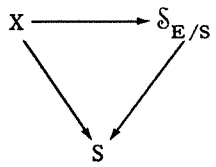
To show the uniqueness of f_0 we argue as follows. Let

$$h_0 : S \to \mathcal{M}(\mathcal{P},\mathcal{S})/G$$

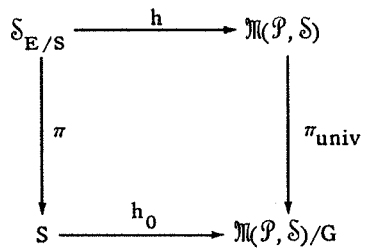
be any morphism for which $h_0^*(E_{univ,0}, \alpha_{univ,0}) \xrightarrow{\sim} (E/S, \alpha)$, and denote by X the fiber-product

$$\begin{array}{ccc} X & \xrightarrow{h} & \mathcal{M}(\mathcal{P},\mathcal{S}) \\ \downarrow & & \downarrow \pi_{univ} \\ S & \xrightarrow{h_0} & \mathcal{M}(\mathcal{P},\mathcal{S})/G\ . \end{array}$$

Then X/S is a G-torsor, and the pull-back to X of $(E/S, \alpha)$ acquires an $\mathcal{S}$-structure β. The resulting G-equivariant S-morphism which classifies this $\mathcal{S}$-structure



is necessarily an isomorphism (being a G-map between G-torsors). Therefore we have a cartesian diagram of G-torsors



and an isomorphism $h^*(E_{univ}, \alpha_{univ}, \beta_{univ}) \simeq (E, \alpha, \beta_{univ})$ over $\mathcal{S}_{E/S}$. Therefore $h = f$, since both classify $(E, \alpha, \beta_{univ})$ over $\mathcal{S}_{E/S}$. From the equality $h = f$, we deduce $h_0\pi = f_0\pi$, whence $h_0 = f_0$ because π is etale and surjective. Q.E.D.

COROLLARY 4.7.1. *Any relatively representable moduli problem $\mathcal{P}$ which is affine and etale over* (Ell), *and rigid, is representable by a smooth affine curve over* $\mathbf{Z}$.

Proof. By 4.7.0, $\mathcal{P}$ is representable by an affine, and we have

$$\mathcal{M}(\mathcal{P}) \otimes \mathbf{Z}[1/2] = \mathcal{M}(\mathcal{P}, \text{Legendre}) \Big/ \begin{matrix}\text{a finite group} \\ \text{acting freely}\end{matrix}$$

$$\mathcal{M}(\mathcal{P}) \otimes \mathbf{Z}[1/3] = \mathcal{M}(\mathcal{P}, \text{naive level 3}) \Big/ \begin{matrix}\text{a finite group} \\ \text{acting freely.}\end{matrix}$$

Therefore it suffices to prove that $\mathcal{M}(\mathcal{P}, \text{Legendre})$ is a smooth curve over $\mathbf{Z}[1/2]$, and that $\mathcal{M}(\mathcal{P}, \text{naive level 3})$ is a smooth curve over $\mathbf{Z}[1/3]$. By hypothesis, $\mathcal{P}$ is etale over (Ell), so that the morphisms

$$\mathcal{M}(\mathcal{P}, \text{Legendre}) \qquad , \qquad \mathcal{M}(\mathcal{P}, \text{naive level 3})$$
$$\downarrow \qquad\qquad\qquad\qquad \downarrow$$
$$\mathcal{M}(\text{Legendre}) \qquad\qquad \mathcal{M}(\text{naive level 3})$$

are *etale*. This reduces us to checking that $\mathcal{M}$(Legendre) and $\mathcal{M}$(naive level three) are both smooth curves over $\mathbf{Z}$, a fact which is obvious by inspection of their explicit defining equations (2.2.9, 2.2.11). Q.E.D.

COROLLARY 4.7.2. *For $N \geq 3$, the naive level N moduli problems of 4.6 is representable, by a smooth affine curve $Y(N)$ over $\mathbf{Z}[1/N]$.*

Proof. This results from 4.7.1 above, thanks to the rigidity 2.7.2 and the relative representability 3.7.1 of naive level N structures. Q.E.D.

(4.8) *Another example*

Another example of a moduli problem which is affine and etale over (Ell) is the problem, for any $N \geq 1$,

$$E/S \mapsto \text{the set of } S\text{-group-scheme homomorphisms}$$
$$\mu_N \to E[N],$$

which is relatively represented by the affine S-scheme

$$Hom_{S\text{-gp}}(\mu_N, E[N]).$$

To see that this S-scheme is etale, simply apply Cartier duality to view it as

$$Hom_{S\text{-gp}}(E[N], \mathbf{Z}/N\mathbf{Z}),$$

which is etale over S simply because $\mathbf{Z}/N\mathbf{Z}$ is etale over S.

(4.9) *Yet another example*

Yet another example of a moduli problem which is affine and etale over (Ell) is the subfunctor of the above problem defined by

$E/S \mapsto$ the set $\mathrm{Incl}_{S\text{-gp}}(\mu_N, E[N])$

of S-group-scheme inclusions $\mu_N \hookrightarrow E[N]$,

i.e., homomorphisms which are f.p.p.f. injective.

By Cartier duality, we may view this as the subfunctor

$$Hom\ Surj_{S\text{-gp}}(E[N], Z/NZ)$$

of $Hom_{S\text{-gp}}(E[N], Z/NZ)$ consisting of the (f.p.p.f)-surjective homomorphisms from $E[N]$ to Z/NZ. To show that this subfunctor is affine and etale over S, it suffices to show that it is represented by an open and closed subscheme of $Hom_{S\text{-gp}}(E[N], Z/NZ)$. This results from (1) and (2) of the following lemma, applied to the universal homomorphism $E[N] \to Z/NZ$ over the scheme $Hom_{S\text{-gp}}(E[N], Z/NZ)$.

(4.10) *Lemmas on group-schemes*

LEMMA (4.10.0). *Let* T *be a scheme,* G *and* H *two finite locally free commutative* T*-group-schemes, and* $f: G \to H$ *a* T*-homomorphism. Then*

(1) *The conditions "* f *is a closed immersion" and "* f *is f.p.p.f. surjective" are each represented by open subschemes of* T.

(2) *If* H *is etale, the condition "* f *is f.p.p.f. surjective" is represented by a closed subscheme of* T.

(3) *If* H *is etale, the condition "* $f = 0$ *" is represented by an open and closed subscheme of* T.

Proof. In (1), it suffices to prove the first statement, because the two conditions are interchanged by Cartier duality. Everything being of finite presentation over T, we reduce easily to the case when T is noetherian. Let $\mathcal{G}$ and $\mathcal{H}$ be the locally free coherent sheaves of $\mathcal{O}_T$-algebras corresponding to G and H respectively. Then f corresponds to an $\mathcal{O}_T$-linear map of sheaves

$$\mathcal{H} \to \mathcal{G}$$

whose cokernel we denote $\mathcal{K}$:

$$\mathcal{H} \to \mathcal{G} \to \mathcal{K} \to 0.$$

Then $\mathcal{K}$ is a coherent sheaf (given with a presentation by locally free ones), and its formation commutes with arbitrary change of base $T' \to T$. The condition "f is a closed immersion" is represented by the open subscheme of T where the coherent sheaf $\mathcal{K}$ *vanishes.*

To prove (2), we may again reduce to the case when T is noetherian. By (1), we know the problem in question is represented by an open subscheme U of T. To show that U closed, it suffices to show that it is *stable under specialization.* This reduces us to the case $T = \mathrm{Spec}(A)$ with A complete noetherian local. Because A is a complete noetherian local ring, G has a canonical structure of extension

$$0 \to G^0 \to G \to G^{et} \to 0$$

of finite flat A-groups with G^0 connected, and G^{et} etale. The morphism $f: G \to H$ must factor through G^{et}. This reduces us to the induced map $\tilde{f}: G^{et} \to H$, i.e., to the case when G and H are *both* etale, in which case the assertion is obvious.

To prove (3), notice first that for any two morphisms between finite locally free T-schemes, the locus where they coincide is represented by the closed subscheme of T where their matrices agree entry by entry. In particular, "$f = 0$" is represented by a closed subscheme Z of T, defined locally on T by finitely many equations. Again reducing easily to the case T noetherian, it suffices to show that Z is stable by generization. This reduces us to the case of T the spectrum of a complete noetherian local ring A, then just as above in case (2) to the case where both G and H are etale, and once again the assertion is obvious in this case. Q.E.D.

COROLLARY (4.10.1). *Let* T *be a scheme,* G *and* H *two finite locally free commutative* T*-groups,* $f: G \to H$ *a* T*-homomorphism. If* H *is etale,*

then there exists a unique finite etale locally free T-group-scheme $H' \subset H$ *such that* f *factors through* H' *and such that the induced map* $f : G \to H'$ *is f.p.p.f. surjective.*

Proof. One reduces easily to the case when T is noetherian (everything given or to be constructed being of finite presentation over T). By etale descent, it suffices to prove the existence and uniqueness of H' locally (etale) on T, so we may further suppose H constant, and T connected. Pick any geometric point $\mathrm{Spec}(\overline{k}) \to T$ of T, and let $H' \subset H$ be the constant subgroup-scheme with fiber $H'(\overline{k}) = \text{image } f : G(\overline{k}) \to H(\overline{k})$. This H' is the *unique* candidate which "works" at the given geometric point. Applying (3) to the composite $G \to H \to H/H'$, we see this composite $G \to H/H'$ vanishes everywhere on T, i.e., G factors through H'. Apply (1), (2) to $G \to H'$, we see that $G \to H'$ is f.p.p.f. surjective. Q.E.D.

Returning to the moduli problem

$$E/S \mapsto \mathrm{Incl}_{S\text{-gp}}(\mu_N, E[N]) .$$

which we now know to be affine and etale over (Ell), we remark that for $N \geq 4$ this problem is also *rigid* (by 2.7.4), hence (4.7.1) *representable* by an elliptic curve

$$\begin{array}{c} E \\ \downarrow \\ Y(\mu_N) \end{array}$$

over a $Y(\mu_N)$ which is a smooth curve over Z.

(4.11) *Modular families*

A family of elliptic curves $E/\mathfrak{M}$ is called a modular family if the moduli problem $\mathcal{P}$ it represents is etale over (Ell). A collection of modular families $E_i/\mathfrak{M}_i$ is said to cover (Ell) if their corresponding

moduli problems $\mathcal{P}^{(i)}$ satisfy the condition that for any elliptic curve E/S, the morphism of schemes

$$\begin{array}{c} \coprod \mathcal{P}^{(i)}_{E/S} \\ \downarrow \\ S \end{array}$$

is etale and surjective.

For example, if N and M are relatively prime integers both ≥ 3, the two modular families carried by Y(N) and by Y(M) cover (Ell). Similarly, for any $N \geq 4$ the single modular family carried by $Y(\mu_N)$ covers the "open set" of (Ell) consisting of those E/S whose fibers at all geometric points of S of characteristic dividing N are ordinary elliptic curves.

(4.12) *More geometric properties of moduli problems*

Let Q be any property of schemes which is local for the etale topology (e.g., being regular of given dimension,* being smooth over Z, being normal, ...). We say that a relatively representable moduli problem $\mathcal{P}$ has property Q if, for every modular family $E/\mathfrak{M}$, the scheme

$$\mathcal{P}_{E/\mathfrak{M}}$$

has property Q. Clearly it is sufficient to check for $E/\mathfrak{M}$ running over a collection of modular families which cover (Ell). If $\mathcal{P}$ is representable, then $\mathcal{P}$ has property Q if and only if the scheme $\mathfrak{M}(\mathcal{P})$ has property Q.

For example, if $E/\mathfrak{M}$ is any modular family, then $\mathfrak{M}$ is a smooth curve over Z (because this is true by inspection for the problems 2.2.9 and 2.2.11).

Similarly, if P is a property of morphisms of schemes which is local on the base for the etale topology, and stable by arbitrary change of base, then a relatively representable moduli problem $\mathcal{P}$ is "of type P" over (Ell) if and only if for some collection of modular families $E_i/\mathfrak{M}_i$ which

*See Notes Added in Proof.

cover (Ell), the morphisms of schemes

$$\mathcal{P}_{E_i/\mathcal{M}_i} \downarrow \mathcal{M}_i$$

are all of type P.

LEMMA (4.12.1) *Let $\mathcal{P}$ be a relatively representable moduli problem on* (Ell). *If $\mathcal{P}$ is finite and flat over* (Ell), *then there exists an integer $d \geq 0$ such that $\mathcal{P}$ is finite and locally free of degree d.*

Proof. The representable problems 2.2.7, 2.2.9 and 2.2.11 are each visibly represented by *connected* schemes. Applying $\mathcal{P}$ to these universal families yields "candidate" degrees d_6, d_2, d_3 such that for any E/S, and $n = 6,2,3$ $\mathcal{P}_{E/S}$ becomes finite locally free of rank d_n over $S[1/n]$ when we invert $n = 6,2,3$ respectively. Taking for E/S the universal family of smooth Weierstrass cubics, whose S is faithfully flat over Z, we may infer that $d_6 = d_2 = d_3$, and this common value is the desired "d." Q.E.D.

(4.13) *The category* (Ell/R)

For any ring R, we denote by (Ell/R) the category of elliptic curves over variable R-schemes, with morphisms the cartesian squares whose bottom arrow is R-linear. A contravariant functor from (Ell/R) to (Sets) is called a moduli problem "over R", or an "R-moduli problem", or a moduli problem "for elliptic curves over R-schemes."

All the preceding notions concerning relatively representable and representable moduli problems carry over mutatis mutandis to the case of R-moduli problems.

There is a natural "forget R"-functor

$$(Ell/R) \to (Ell),$$

by means of which any moduli problem $\mathcal{P}$ on (Ell) gives rise to a moduli problem $\mathcal{P}\otimes R$ on (Ell/R). If $\mathcal{P}$ is relatively representable, by morphisms, one for each E/S,

$$\mathcal{P}_{E/S} \downarrow S,$$

then $\mathcal{P}\otimes R$ is relatively representable (by the same morphisms, for each E/S/R). If $\mathcal{P}$ is representable, by

$$E \downarrow \mathcal{M}(\mathcal{P}),$$

then $\mathcal{P}\otimes R$ is representable, by

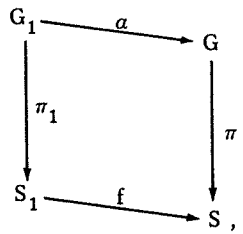
$$E\otimes R \downarrow \mathcal{M}(\mathcal{P})\otimes R,$$

i.e., for representable problems $\mathcal{P}$ we have

$$\mathcal{M}(\mathcal{P}\otimes R) = \mathcal{M}(\mathcal{P})\otimes R.$$

(4.14) *Moduli problems of finite level*

(4.14.1) Let us denote by (FLFG) the category whose objects are finite locally free commutative group-schemes G over variable base-schemes S and whose morphisms are cartesian squares of group-schemes



i.e., commutative squares such that the induced map

$$G_1 \xrightarrow{(a,\pi_1)} G \underset{S}{\times} S_1$$

is an isomorphism of S_1-group-schemes.

Just as with (Ell), we have the notion of a moduli problem $\mathcal{F}$ on (FLFG), namely a contravariant functor

$$\mathcal{F} : (\text{FLFG}) \to (\text{Sets}) .$$

We say that $\mathcal{F}$ is relatively representable if for every G/S, the functor on (Sch/S)

$$T \mapsto \mathcal{F}(G \underset{S}{\times} T/T)$$

is representable by an S-scheme, noted $\mathcal{F}_{G/S}$.

(4.14.2) For any integer $N \geq 1$, there is an obvious functor "kernel of N"

$$(\text{Ell}) \to (\text{FLFG})$$

$$E/S \mapsto E[N]/S .$$

By composition, any moduli problem $\mathcal{F}$ on (FLFG) gives rise to a moduli problem $\mathcal{P} = \mathcal{F} \circ [N]$ on (Ell), defined by

$$\mathcal{P}(E/S) = \mathcal{F}(E[N]/S) .$$

Clearly, if $\mathcal{F}$ is relatively representable, then $\mathcal{P} = \mathcal{F} \circ [N]$ is relatively representable, by

$$\mathcal{P}_{E/S} = \mathcal{F}_{E[N]/S} .$$

(4.14.3) We say that a relatively representable $\mathcal{P}$ on (Ell) is of level (dividing) N if there exist a relatively representable problem $\mathcal{F}$ on (FLFG) such that $\mathcal{P} = \mathcal{F} \circ [N]$. We say that $\mathcal{P}$ is of finite level if it is of level N for some $N \geq 1$. For example, the basic problems $[\Gamma(N)]$, $[\text{bal } \Gamma_1(N)]$, $[\Gamma_1(N)]$, $[\Gamma_0(N)]$, are all of level N in this sense.

APPENDIX

(A.4) *More on rigidity and representability*

(A.4.1) Let R be a ring, $\mathcal{P}$ a moduli problem on (Ell/R), and $\widetilde{\mathcal{P}}$ the contravariant functor on (Sch/R) defined by (cf. 4.3.1)

(A.4.1.1) $S/R \mapsto$ isomorphism classes of pairs $(E/S, \alpha)$ with E an elliptic curve over S and $\alpha \in \mathcal{P}(E/S)$ a "level $\mathcal{P}$ structure" on E/S.

It is a tautology that

$$\text{(A.4.1.2)} \qquad \mathcal{P} \text{ is representable} \iff \begin{cases} \widetilde{\mathcal{P}} \text{ is representable} \\ \textit{and } \mathcal{P} \text{ is rigid.} \end{cases}$$

However, it is *not* in general true that

$$\widetilde{\mathcal{P}} \text{ representable} \implies \mathcal{P} \text{ rigid} .$$

Here is a simple counterexample, due to Ofer Gabber. At the expense of Zariski-localizing on Spec(R), we may suppose that there exists an elliptic curve over R. Fix one, say E/R, and define a moduli problem $\mathcal{P}$ on (Ell/R) by defining

$$\text{(A.4.1.3)} \qquad \mathcal{P}(E/S) = \begin{cases} \text{the set with one element, if } E/S \text{ is} \\ S\text{-isomorphic to } E_S/S, \text{ the empty set,} \\ \text{if not.} \end{cases}$$

This $\mathcal{P}$ is not rigid (because the automorphism -1 acts trivially), but the associated functor $\widetilde{\mathcal{P}}$ is visibly representable (by Spec(R) itself!).

In the positive direction, we have the following result, which is well known to the specialists but for which we know no reference.

PROPOSITION (A.4.2). *Let* R *be a ring, and* $\mathcal{P}$ *a moduli problem on* (Ell/R). *Suppose that for every* R*-scheme* S *and for every elliptic curve* E/S, *the contravariant functor on* (Sch/S) *defined by (cf. 4.2)*

$$T \mapsto \mathcal{P}(E_T/T)$$

is an etale sheaf on (Sch/S). (*N.B. This condition is automatically satisfied if* $\mathcal{P}$ *is relatively representable.*) *Then the following conditions are equivalent.*

(1) $\widetilde{\mathcal{P}}$ *is representable.*

(2) $\widetilde{\mathcal{P}}$ *is representable, and* $\mathcal{P}$ *is rigid.*

(3) $\mathcal{P}$ *is representable.*

Proof. That (2) $\Longleftrightarrow$ (3) is just "mise pour memoire." We must prove that (1) $\Longrightarrow$ (2). We argue by contradiction. Suppose that $\mathcal{P}$ is not rigid. Then there exists an E/S/R, an element $\alpha \in \mathcal{P}(E/S)$, and an automorphism $g \neq id$ of E/S such that $g^*(\alpha) = \alpha$. Because $g \neq id$, there exists, (by rigidity (2.4.2)), a geometric point s of S, say $s : \mathrm{Spec}(k) \to S$ such that on the elliptic curve E_s/k, the induced automorphism g_s is not the identity. Because $g^*(\alpha) = \alpha$ in $\mathcal{P}(E/S)$, it follows by functoriality that $g_s^*(\alpha_s) = \alpha_s$ in $\mathcal{P}(E_s/k)$.

By (2.7.2), the non-trivial automorphism g_s is of finite order, say of order $d \geq 2$. Let K be an extension field of k, and L/K a galois extension with galois group $\mathbf{Z}/d\mathbf{Z}$. (For example, take $L = k(X_1, \cdots, X_d)$, with $\mathbf{Z}/d\mathbf{Z}$ acting by cyclic permutation of the variables, and K the field of invariants.) Fix a generator τ of the galois group $\mathbf{Z}/d\mathbf{Z}$.

Let us denote by E_1/K the elliptic curve over K obtained from E_s/k by the extension of scalars $k \to K$, by $g_1 \in \mathrm{Aut}(E_1/K)$ the automorphism of exact order d deduced from g_s by extension of scalars, and by $\alpha_1 \in \mathcal{P}(E_1/K)$ the element deduced from $\alpha_s \in \mathcal{P}(E_s/k)$ by extension of scalars. Thus $g_1^*(\alpha_1) = \alpha_1$.

Now consider the "twist" of E_1/K by the cyclic extension L/K, via the automorphism g_1. This "twist" is the K-elliptic curve E_2/K deduced from the L-elliptic curve $E_1 \underset{\mathrm{Spec}(K)}{\times} \mathrm{Spec}(L)$ by descent, via the semi-linear action of $\mathrm{Gal}(L/K)$ under which the chosen generator τ acts by $(g_1, \mathrm{Spec}(\tau))$.

The two curves E_1/K and E_2/K become isomorphic over L, by an L-isomorphism

$$E_1 \underset{\mathrm{Spec}(K)}{\times} \mathrm{Spec}(L) \simeq E_2 \underset{\mathrm{Spec}(K)}{\times} \mathrm{Spec}(L),$$

under which $(g_1, \mathrm{Spec}(\tau)) \simeq (\mathrm{id}, \mathrm{Spec}(\tau))$.

Consider the element $\alpha_1 \otimes_K L \in \mathcal{P}(E_1 \otimes_K L/L)$, deduced from $\alpha_1 \in \mathcal{P}(E_1/K)$ by the extension of scalars $K \hookrightarrow L$. Because it is "defined over K," this element is invariant under $(\mathrm{id}, \mathrm{Spec}(\tau))$, and by hypothesis it is invariant under (g_1, id). Therefore this element $\alpha_1 \otimes_K L$ is invariant under $(g_1, \mathrm{Spec}(\tau))$. By means of the above L-isomorphism of $E_1 \otimes_K L$ with $E_2 \otimes_K L$, this element $\alpha_1 \otimes L$ gives rise to an element, say β, in $\mathcal{P}(E_2 \otimes_K L/L)$, which is *invariant* under $(\mathrm{id}, \mathrm{Spec}(\tau))$. Because the functor on (Sch/K) defined by

$$T \mapsto \mathcal{P}((E_2)_T/T)$$

is assumed to be an etale sheaf, we have

$$\left(\mathcal{P}(E_2 \otimes_K L/L)\right)^{\mathrm{Gal}(L/K)} \xleftarrow{\sim} \mathcal{P}(E_2/K).$$

Therefore our element β comes from a unique element, say α_2, of $\mathcal{P}(E_2/K)$.

By construction, the two pairs

$$(E_1/K, \alpha_1), \quad (E_2/K, \alpha_2)$$

become isomorphic after the extension of scalars $K \hookrightarrow L$. We claim that they are not K-isomorphic. Granting this, they provide two distinct elements of $\widetilde{\mathcal{P}}(K)$ which become equal in $\widetilde{\mathcal{P}}(L)$. Therefore $\widetilde{\mathcal{P}}$ cannot be representable as a contravariant functor on (Sch/R), since for any scheme X, and any field extension $K \hookrightarrow L$, the map $X(K) \to X(L)$ is always injective.

It remains to explain why $(E_1/K, \alpha_1)$ and $(E_2/K, \alpha_2)$ are not K-isomorphic. Indeed, we will see that E_1/K and E_2/K are not K-isomorphic as elliptic curves. By general descent theory, given E_1/K, the K-isomorphism classes of L/K forms of E_1/K are in bijective correspondence with the galois cohomology set

$$H^1(\mathrm{Gal}(L/K), \mathrm{Aut}(E_1 \otimes_K L/L)) .$$

Because $E_1 \otimes_K L = E_s \otimes_k L$ is obtained by field extension from a curve over an algebraically closed field, it follows easily from rigidity (2.4.2) that every L-automorphism (or L-endomorphism, for that matter) is obtained from a k-automorphism (or k-endomorphism) of E_s/k. Therefore we have $\mathrm{Aut}(E_s/k) \xrightarrow{\sim} \mathrm{Aut}(E_1 \otimes_K L/L)$, and consequently $\mathrm{Gal}(L/K)$ operates trivially on $\mathrm{Aut}(E_1 \otimes_K L/L)$. Thus we may rewrite the H^1 as the set of conjugacy classes of homomorphisms from $\mathrm{Gal}(L/K)$ to $\mathrm{Aut}(E_s/k)$, with the trivial homomorphism corresponding to E_1/K itself. The curve E_2/K is represented by the conjugacy class of the homomorphism sending the chosen generator τ of $\mathrm{Gal}(L/K) \simeq Z/dZ$ to the element $g_s \in \mathrm{Aut}(E_s/k)$ of exact order d. Because $d \geq 2$, the element g_s is not conjugate in $\mathrm{Aut}(E_s/k)$ to the identity, whence E_2 is not K-isomorphic to E_1. Q.E.D.

Chapter 5
REGULARITY THEOREMS

(5.1) *First Main Theorem*

In this chapter, we study the regularity properties of the first three of the four basic moduli problems discussed in Chapter III (i.e., $\Gamma(N)$-structures, $\Gamma_1(N)$-structures, balanced $\Gamma_1(N)$-structures and $\Gamma_0(N)$-structures on variable elliptic curves E/S). For brevity, we will denote these moduli problems on (Ell) by the symbols

$$[\Gamma(N)],\ [\Gamma_1(N)],\ [\mathrm{bal}.\Gamma_1(N)],\ [\Gamma_0(N)] .$$

FIRST MAIN THEOREM 5.1.1. *Each of the four moduli problems* $[\Gamma(N)]$, $[\Gamma_1(N)]$, $[\mathrm{bal}.\Gamma_1(N)]$, *and* $[\Gamma_0(N)]$ *is relatively representable over* (Ell). *Each is finite and flat over* (Ell) *of constant rank* ≥ 1, *and regular (necessarily of dimension two). Each tensored with* $Z[1/N]$ *is finite etale over* $(Ell/Z[1/N])$.

(5.2) *Axiomatics*

By 3.7.1, the theorem is true over $Z[1/N]$. In view of the "factorization into prime powers" (3.5.1) of all the moduli problems involved, it suffices to treat the case when N is a power of a single prime p.

To clarify the ideas which enter into the proof, we will explain the general mechanism (Deligne's "homogeneity principle") which underlies it (cf. [De-Ra], Introduction). Thus we consider any moduli problem $\mathcal{P}$ which satisfies the following axioms with respect to a fixed prime number p.

Reg. 1. $\mathcal{P}$ is relatively representable and finite over (Ell).

Reg. 2. $\mathcal{P} \otimes Z[1/p]$ is finite etale over $(Ell/Z[1/p])$.

Reg. 3. $\mathcal{P}$ depends only on the underlying p-divisible group, in the sense that for any two elliptic curves over a common base, say E/S and E'/S, and any isomorphism of their p-divisible groups over S

$$E[p^\infty] \xrightarrow{\sim} E'[p^\infty] ,$$

there exists an isomorphism of S-schemes

$$\mathcal{P}_{E'/S} \xrightarrow{\sim} \mathcal{P}_{E/S} .$$

(e.g., any $\mathcal{P}$ of p-power level in the sense of (4.14) satisfies Reg. 3).

Reg. 4. Let k be an algebraically closed field of characteristic p, E_0/k a supersingular elliptic curve, and $E/W(k)[[T]]$ its universal formal deformation. Then

(4A) $\mathcal{P}(E_0/k)$ consists of a single element, and

(4B) the (consequently local) finite $W[[T]]$-scheme

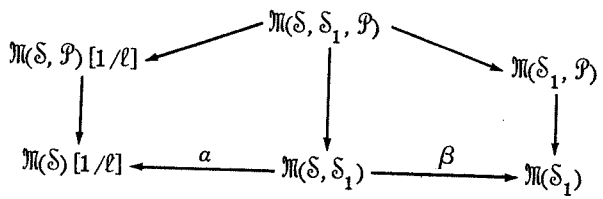
$$\mathcal{P}_{E/W[[T]]}$$

is the spectrum of a regular two-dimensional local ring.

AXIOMATIC REGULARITY THEOREM 5.2.1. *Any moduli problem $\mathcal{P}$ satisfying the axioms Reg. 1 through Reg. 4 is finite and flat over* (Ell) *of constant rank ≥ 1, and regular (necessarily of dimension two).*

Proof. Let $\mathcal{S}$ be any representable moduli problem which is etale over (Ell). We must show that $\mathcal{M}(\mathcal{S}, \mathcal{P})$ is a regular two-dimensional scheme, and that it is finite and flat over $\mathcal{M}(\mathcal{S})$. Because $\mathcal{M}(\mathcal{S})$ is (by 4.7.1) a smooth curve over $\mathbf{Z}$, it is itself a regular two-dimensional scheme. By Reg. 2, $\mathcal{M}(\mathcal{S}, \mathcal{P})$ becomes finite etale over $\mathcal{M}(\mathcal{S})$ as soon as we invert p. In particular, then, $\mathcal{M}(\mathcal{S}, \mathcal{P}) \otimes \mathbf{Z}[1/p]$ is itself a regular two-dimensional scheme, finite and flat over $\mathcal{M}(\mathcal{S}) \otimes \mathbf{Z}[1/p]$.

Therefore it suffices to show that for some odd prime $\ell \neq p$, the scheme $\mathcal{M}(\mathcal{S}, \mathcal{P}) \otimes \mathbf{Z}[1/\ell]$ is two-dimensional regular, and is finite and flat over $\mathcal{M}(\mathcal{S}) \otimes \mathbf{Z}[1/\ell]$. For this, we may replace $\mathcal{S}$ by any representable moduli problem $\mathcal{S}_1$ which is etale and surjective over $(Ell/\mathbf{Z}[1/\ell])$ (e.g., by $\mathcal{S}_1$ the "naive" full level ℓ moduli problem, carried by $Y(\ell)$) simply because we have cartesian diagrams



in which α is etale and surjective, and in which β is etale.

Now consider the finite morphism

We must show that

$$\begin{cases} \mathcal{M}(\mathcal{S}_1, \mathcal{P}) \text{ is a regular scheme} \\ \mathcal{M}(\mathcal{S}_1, \mathcal{P}) \text{ is (finite and) flat over } \mathcal{M}(\mathcal{S}_1) . \end{cases}$$

(Recall that by Reg. 1, $\mathcal{M}(\mathcal{S}_1, \mathcal{P})$ is finite over $\mathcal{M}(\mathcal{S}_1)$.) Once these points are established, $\mathcal{M}(\mathcal{S}_1, \mathcal{P})$ will necessarily be a two-dimensional regular scheme, because $\mathcal{M}(\mathcal{S}_1)$ is itself regular two-dimensional, being a smooth curve over $\mathbf{Z}$.

Consider the open set $\mathcal{U} \subset \mathcal{M}(\mathcal{S}_1)$ defined by

$\mathcal{U}$ = those points y of $\mathcal{M}(\mathcal{S}_1)$ such that for all points x of $\mathcal{M}(\mathcal{S}_1, \mathcal{P})$ with $\pi(x) = y$, the local ring $\mathcal{O}_{\mathcal{M}(\mathcal{S}_1, \mathcal{P}), x}$ is regular, and is flat over the local ring $\mathcal{O}_{\mathcal{M}(\mathcal{S}_1), y}$.

This is indeed an open set, for its complement is the union of the two closed sets in $\mathcal{M}(\mathcal{S}_1)$ which are the images by the finite (and hence proper) map π of the closed subsets of $\mathcal{M}(\mathcal{S}_1,\mathcal{P})$ at which $\mathcal{M}(\mathcal{S}_1,\mathcal{P})$ is not regular, respectively is not flat over $\mathcal{M}(\mathcal{S}_1)$. We must show that $\mathcal{U} = \mathcal{M}(\mathcal{S}_1)$. Because $\mathcal{M}(\mathcal{S}_1)$ is of finite type over $\mathbf{Z}$, it suffices to show that $\mathcal{U}$ contains every closed point of $\mathcal{M}(\mathcal{S}_1)$. By Reg. 2, we know that $\mathcal{U}$ contains all of $\mathcal{M}(\mathcal{S}_1)\otimes\mathbf{Z}[1/p]$, so it suffices to show that $\mathcal{U}$ contains every closed point of $\mathcal{M}(\mathcal{S}_1)$ of residue characteristic p, i.e., every closed point of $\mathcal{M}(\mathcal{S}_1)\otimes\mathbf{F}_p$.

Recall that a closed point of $\mathcal{M}(\mathcal{S}_1)\otimes\mathbf{F}_p$ is said to be ordinary (respectively supersingular) if the corresponding elliptic curve with $\mathcal{S}_1$-structure over the residue field is an ordinary (respectively supersingular) elliptic curve. The set of supersingular points of $\mathcal{M}(\mathcal{S}_1)\otimes\mathbf{F}_p$ is finite and non-empty, and every open neighborhood of a supersingular point contains ordinary points (2.9.4, 4.7.2).

We will show that the open set $\mathcal{U}$ has the following "homogeneity properties."

(H1) if $\mathcal{U}$ contains one supersingular point of $\mathcal{M}(\mathcal{S}_1)\otimes\mathbf{F}_p$, it contains all supersingular points of $\mathcal{M}(\mathcal{S}_1)\otimes\mathbf{F}_p$.

(H2) if $\mathcal{U}$ contains one ordinary point of $\mathcal{M}(\mathcal{S}_1)\otimes\mathbf{F}_p$, it contains all ordinary points of $\mathcal{M}(\mathcal{S}_1)\otimes\mathbf{F}_p$.

If we grant that $\mathcal{U}$ satisfies (H1) and (H2), then we are reduced to showing that $\mathcal{U}$ contains some supersingular point of $\mathcal{M}(\mathcal{S}_1)\otimes\mathbf{F}_p$ [by (H1), $\mathcal{U}$ will contain all the supersingular points; being open, it also contains *some* ordinary point, so by (H2) it contains all ordinary points].

We now explain why (H1) and (H2) are true. By definition, a closed point y of $\mathcal{M}(\mathcal{S}_1)$ lies in $\mathcal{U}$ if and only if for each of the finitely many closed points x of $\mathcal{M}(\mathcal{S}_1,\mathcal{P})$ lying over it, we have:

the local ring $\mathcal{O}_{\mathcal{M}(\mathcal{S}_1,\mathcal{P}),x}$ is regular, and it is flat over $\mathcal{O}_{\mathcal{M}(\mathcal{S}_1),y}$.

We first reduce to the case of an algebraically closed residue field, by passing to the completion of the strict henselization. Let k be an algebraic closure of $\mathbf{F}_p$, and $W = W(k)$ its ring of Witt vectors. For any scheme X of finite type over $\mathbf{Z}$, there are natural bijections

$$\{\text{closed points } x \text{ of } X\otimes W \text{ with residue field } k\} \leftrightarrow$$
$$\{k\text{-valued points } x \text{ of } X\} \leftrightarrow$$
$$\left\{\begin{array}{l}\text{pairs } (x_0,i) \text{ where } x_0 \text{ is a closed point of } X \text{ with residue}\\ \text{characteristic } p \text{ and } i \text{ is an inclusion of the finite residue}\\ \text{field } \mathbf{F}_p(x_0) \text{ into } k\end{array}\right\}.$$

Under this bijection the complete local rings are related by

$$\hat{\mathcal{O}}_{X\otimes W,x} = \hat{\mathcal{O}}^{h.s.}_{X,x_0}.$$

Recall that for any noetherian local ring A, both its strict henselization $A^{h.s.}$ and its completion $\hat{A}$ are noetherian local rings which are faithfully flat over A, and which are regular if and only if A is regular (for $\hat{A}$ this is standard, for $A^{h.s.}$ it's EGA IV, 18.8.8, 18.8.13). Applying this to the local rings at closed points of both $\mathcal{M}(\mathcal{S}_1)$ and $\mathcal{M}(\mathcal{S}_1,\mathcal{P})$, it follows that a closed point y_0 of $\mathcal{M}(\mathcal{S}_1)$ of residue characteristic p lies in $\mathcal{U}$ if and only if for any k-valued point y of $\mathcal{M}(\mathcal{S}_1)\otimes W$ lying over it, we have the following condition:

for all k-valued points x of $\mathcal{M}(\mathcal{S}_1,\mathcal{P})\otimes W$ lying over y, the complete local ring

$\hat{\mathcal{O}}_{\mathcal{M}(\mathcal{S}_1,\mathcal{P})\otimes W,x}$ is regular, and it is flat over $\hat{\mathcal{O}}_{\mathcal{M}(\mathcal{S}_1)\otimes W,y}$.

Because $\mathcal{M}(\mathcal{S}_1,\mathcal{P})$ is finite over $\mathcal{M}(\mathcal{S}_1)$, the spectrum of the direct sum (over all $x \to y$) of these complete local rings is just the scheme

$$(*)\qquad (\mathcal{M}(\mathcal{S}_1,\mathcal{P})\otimes W) \underset{\mathcal{M}(\mathcal{S}_1)\otimes W}{\times} \mathrm{Spec}(\hat{\mathcal{O}}_{\mathcal{M}(\mathcal{S}_1)\otimes W,y}).$$

Consider the elliptic curve E_0/k underlying y viewed as a k-valued point of $\mathcal{M}(\mathcal{S}_1)$, and let $E/W[[T]]$ be its universal formal deformation.

Because $\mathcal{M}(\delta_1)$ is etale over (Ell), we have an isomorphism of complete local rings

$$W[[T]] \xrightarrow{\sim} \hat{\mathcal{O}}_{\mathcal{M}(\delta_1)\otimes W, y},$$

with $E/W[[T]]$ identified with the inverse image of the universal curve over $\mathcal{M}(\delta_1)$. Therefore the scheme (*) in question is none other than

$$\mathcal{P}_{E/W[[T]]}.$$

The condition that y lie in $\mathcal{U}$ is thus a condition on the $W[[T]]$-scheme $\mathcal{P}_{E/W[[T]]}$, (that it be a regular scheme, flat over $W[[T]]$).

By the Serre-Tate theorem, the p-divisible group of $E/W[[T]]$ is the universal formal deformation of the p-divisible group of E_0/k. By Reg. 3, the $W[[T]]$-scheme $\mathcal{P}_{E/W[[T]]}$ depends only on the p-divisible group of $E/W[[T]]$. Therefore by Serre-Tate the $W[[T]]$-scheme $\mathcal{P}_{E/W[[T]]}$ depends only on the p-divisible group of E_0/k. Because k is algebraically closed, the p-divisible group of E_0/k is necessarily k-isomorphic to either $\mu_{p^\infty} \times \mathbf{Q}_p/\mathbf{Z}_p$, corresponding to E_0/k ordinary, or to the unique one-parameter formal Lie group over k of height two, corresponding to E_0/k supersingular.

Therefore up to $W[[T]]$-isomorphism, there are only two distinct schemes $\mathcal{P}_{E/W[[T]]}$, one corresponding to E_0/k ordinary, the other to E_0/k supersingular.

Therefore the open set $\mathcal{U}$ contains either all ordinary (respectively all supersingular) points in characteristic p, or it contains none; the conditions (H1) and (H2) are satisfied.

To complete the proof, it remains to establish that $\mathcal{U}$ contains some supersingular point of characteristic p. But by Reg. 4, the open set $\mathcal{U}$ contains all supersingular points of characteristic p.

Finally, we recall (4.12.1) that once we know $\mathcal{P}$ is finite and flat over (Ell), its rank is necessarily constant.

This concludes the proof of the Axiomatic Regularity Theorem. Q.E.D.

In practice, it is convenient to replace axiom Reg. 4B by a more computationally accessible condition Reg. 4B bis:

PROPOSITION 5.2.2. *Let $\mathcal{P}$ be a moduli problem satisfying Reg. 1 through Reg. 3 and Reg. 4A. Then $\mathcal{P}$ satisfies Reg. 4B if and only if it satisfies*

Reg. 4B bis $\mathcal{P}_{E/W[[T]]}$ *is the spectrum of a local ring whose maximal ideal is generated by two elements.*

Proof. Clearly 4B implies 4B bis. We must establish the converse. Write $\mathcal{P}_{E/W[[T]]} = \mathrm{Spec}(A)$. Then A is local by 4A, and is finite over $W[[T]]$ by Reg. 1. By Reg. 2, $A \otimes \mathbf{Z}[1/p]$ is finite etale over $(W[[T]]) \otimes \mathbf{Z}[1/p]$. Therefore the finite morphism

$$\mathrm{Spec}(A) \to \mathrm{Spec}(W[[T]])$$

is surjective, because its image is closed (the map being finite, hence proper) and its image contains the open dense set $\mathrm{Spec}((W[[T]]) \otimes \mathbf{Z}[1/p])$. Therefore the local ring A must have dimension *at least* two. So if its maximal ideal is generated by two elements, A must be a regular local ring of dimension two. It is then automatically flat over $W[[T]]$, because any finite morphism between regular schemes of the same dimension is automatically flat [A-K 1, V, 3.6]. Q.E.D.

(5.3) *End of the proof*

In this section, we will complete the proof of the First Main Theorem for the three moduli problems

$$[\Gamma(N)],\ [\Gamma_1(N)],\ \text{and}\ [\mathrm{bal}.\Gamma_1(N)].$$

As already noted, it suffices to treat the case N = a power of a prime p, say $N = p^n$ with $n \geq 1$.

Each of these problems, with $N = p^n$, satisfies Reg. 1 through Reg. 3 (3.6, 3.7.1, 4.14.3). We must show that each also satisfies Reg. 4A and Reg. 4B bis. We begin with 4A.

LEMMA 5.3.1. *Each of the problems*

$$\mathcal{P} = [\Gamma(p^n)],\ [\Gamma_1(p^n)],\ [\text{bal.}\,\Gamma_1(p^n)]$$

has $\mathcal{P}(E_0/k)$ = *a single element for any supersingular elliptic curve* E_0 *over any field* k *of characteristic* p.

Proof. Because E_0 is supersingular, the group-scheme $E_0[p^n]$ over k is local for every n, and the unique closed subgroup-scheme of E_0 of any given rank p^r is the kernel of the r-fold Frobenius morphism

$$F^r : E_0 \to E_0^{(p^r)}.$$

In particular, we have

$$\text{Ker}\,(F^{2n}) = \text{Ker}\,(p^n)$$

by uniqueness.

Consider first $\mathcal{P} = [\Gamma(p^n)]$. Then $\mathcal{P}(E_0/k)$ is the set of pairs P, Q of k-points of $E_0[p^n]$ which form a Drinfeld basis. Because $E_0[p^n]$ is local, and k is a field, we have $P = Q = 0$. This is in fact a Drinfeld basis of $E_0[p^n] = \text{Ker}\,(p^n) = \text{Ker}\,(F^{2n})$, simply because for $P = Q = 0$ we have the equality of Cartier divisors

$$\sum_{a,b \bmod p^n} [aP + bQ] = p^{2n}[0] = \text{Ker}\,(F^{2n}).$$

Consider next $\mathcal{P} = [\Gamma_1(N)]$. Then $\mathcal{P}(E_0/k)$ is the set of k-valued points P of $E_0[p^n]$ of "exact order p^n." Again the only possibility is $P = 0$, which does in fact have "exact order p^n", because it generates $\text{Ker}\,(F^n)$.

Finally for $\mathcal{P} = [\text{bal.}\,\Gamma_1(p^n)]$, the set $\mathcal{P}(E_0/k)$ is the set of triples (K, P, P') with K a finite flat k-subgroup-scheme of $E_0[p^n]$ of rank p^n, $P \in K(k)$ a generator of K, and P' a k-valued generator of the quotient group $K' = E_0[p^n] \bmod K$. Then K and K' are local, so $P = 0$ and $Q = 0$, and K must be $\text{Ker}\,(F^n)$. Q.E.D.

We now turn to the condition 4B bis.

THEOREM 5.3.2. *Let* k *be an algebraically closed field of characteristic* p. E_0/k *a supersingular elliptic curve,* $E/W[[T]]$ *its universal formal deformation. Then for each of the three moduli problems*

$$\mathcal{P} = [\Gamma(p^n)],\ [\Gamma_1(p^n)],\ [\text{bal.}\,\Gamma_1(p^n)],$$

we have $\mathcal{P}_{E/W[[T]]} = \text{Spec}\,(A)$ *with* A *a local ring whose maximal ideal is generated by two elements.*

Proof. By 4A, we know that A is a local ring, finite over $W[[T]]$, hence complete. Consider the elliptic curve $\mathcal{E}/A$ obtained from $E/W[[T]]$ by the extension of scalars $W[[T]] \to A$. Let $\alpha \in \mathcal{P}(\mathcal{E}/A)$ be the tautological level $\mathcal{P}$ structure on $\mathcal{E}/A$. Then $(\mathcal{E}/A, \alpha)$ pro-represents the functor on artin local $W(k)$-algebras with residue field k

$R \mapsto$ triples $(E/R, \alpha, i)$ where E/R is an elliptic curve, $\alpha \in \mathcal{P}(E/R)$ is a level $\mathcal{P}$ structure, and i is an isomorphism of elliptic curves over k,

$$E \underset{R}{\otimes} (R/\max(R)) \xrightarrow{\sim} E_0,$$

which (necessarily) carries α to the unique element of $\mathcal{P}(E_0/k)$.

Suppose we are given two functions f, g in $\max(A)$. Then in order that f and g generate $\max(A)$, it is necessary and sufficient that the following moduli-theoretic rigidity condition hold:

If R is an artin local $W(k)$-algebra,* and if $\phi : A \to R$ is a homomorphism with $\phi(f) = \phi(g) = 0$, then the induced triple $(E/R, \alpha, i)$ is *constant* in the sense that R is a k-algebra and this triple comes from the constant triple $(E_0/k, \alpha_0, \text{id})$ by extension of scalars $k \to R$.

*With residue field k.

We remark that in this condition, it is sufficient that $(E/R, \alpha)$ be constant, for by rigidity the only hom's between constant abelian schemes are themselves constant.

Case I. $\mathcal{P} = [\Gamma(p^n)]$. Choose a parameter X for the formal group of $\mathcal{E}/A$. The universal $\mathcal{P}$-structure on $\mathcal{E}/A$ is a pair of points P, Q in $\mathcal{E}(A)$ which form a Drinfeld p^n-basis. Because A is complete local, and E_0/k is supersingular, the points P, Q both lie in the formal group. Therefore we may speak of the X-coordinates of these points,

$$X(P),\ X(Q) \in \max(A)\ .$$

We claim that the two functions $f = X(P)$, $g = X(Q)$, *generate* $\max(A)$. This amounts to the following rigidity assertion:

(5.3.2.1) (Rigid I). Let k be an algebraically closed field of characteristic p. If R is an artin local $W(k)$-algebra,* and if E/R admits $(0,0)$ as a Drinfeld p^n-basis, then R is a k-algebra and E/R is constant.

Case II. $\mathcal{P} = [\Gamma_1(p^n)]$. Again choose a parameter X for the formal group of $\mathcal{E}/A$. The universal k-structure on $\mathcal{E}/A$ is a point P in $\mathcal{E}(A)$ of "exact order p^n", and just as above P lies in the formal group, so we may speak of its X-coordinate

$$X(P) \in \max(A)\ .$$

We also have "the" parameter T of $W[[T]]$ (strictly speaking, any element of $W[[T]]$ which, together with p, generates the maximal ideal of $W[[T]]$). By means of $W[[T]] \to A$, we may speak of T as lying in $\max(A)$. We claim that the two functions

$$X(P),\ T \in \max(A)$$

generate $\max(A)$. This amounts to the following rigidity assertion:

(5.3.2.2) (Rigid II). Let k be an algebraically closed field of characteristic p. If R is an artin local $W(k)$-algebra,* and if E/R admits 0 as

*With residue field k.

a point of "exact order p^n", then R is a k-algebra, i.e., $p = 0$ in R.

For if we grant that $p = 0$ in R, then the vanishing of the T-invariant of E/R means precisely that E/R is constant.

Case III. $\mathcal{P} = [\text{bal.}\,\Gamma_1(p^n)]$. This time we choose a parameter X for the formal group of $\mathcal{E}/A$, and we choose a parameter X' for the formal group of $\mathcal{E}'/A$, where $\mathcal{E}'$ is the quotient of $\mathcal{E}$ by the cyclic subgroup-scheme K of rank p^n of $\mathcal{E}$ which is part of the data of the $\mathcal{P}$-structure. All in all, we have

$$P \in \mathcal{E}(A) \qquad \mathcal{E} \underset{\pi^t}{\overset{\pi}{\rightleftarrows}} \mathcal{E}' \qquad P' \in \mathcal{E}'(A)\ ,$$

where P has "exact order p^n" on $\mathcal{E}/A$ and generates $\operatorname{Ker}\pi$, and where P' has "exact order p^n" on $\mathcal{E}'/A$ and generates $\operatorname{Ker}(\pi^t)$. As in Cases I and II, the points P and P' lie in the formal groups of $\mathcal{E}$ and $\mathcal{E}'$ respectively, so we can speak of their X and X'-coordinates:

$$X(P),\ X'(P') \in \max(A)\ .$$

We claim that these two functions generate $\max(A)$. This amounts to the following rigidity assertion:

(5.3.2.3) (Rigidity III). Let k be an algebraically closed field of characteristic p. If R is an artin local $W(k)$-algebra* and if E and E' are elliptic curves over R joined by dual p^n-isogenies

$$E \underset{\pi^t}{\overset{\pi}{\rightleftarrows}} E'$$

whose kernels are both cyclic and generated by their zero-sections, then R is a k-algebra, E/R is constant, and $\operatorname{Ker}(\pi) = \operatorname{Ker}(F^n)$.

We now turn to proving the rigidity assertions I, II, III. For ease of later reference, we will give an analysis of a slightly more general situation, which is useful in other contexts as well (compare our discussion of roots of unity (1.12)).

*With residue field k.

PROPOSITION 5.3.3. *Let* R *be an arbitrary ring,* C/R *a smooth commutative one-dimensional group-scheme over* R (*cf. 1.4.1*), p *a prime number,* $n \geq 1$ *an integer. Suppose that the zero section* $0 \in C(R)$ *is a point of "exact order* p^n *" in* C/R, *i.e., that the effective Cartier divisor* $p^n[0]$ *in* C/R *is a subgroup-scheme. Then* $p = 0$ *in* R, *and the subgroup-scheme* $p^n[0]$ *is none other than* $\mathrm{Ker}(F^n)$.

Proof. The zero-section and the Cartier divisor $p^n[0]$ both lie in the formal group of C/R. Zariski locally on R, we may choose a parameter X for the formal group. Once this is done, our proposition results from the following one.

PROPOSITION 5.3.4. *Let* R *be an arbitrary ring, and*

$$G(X,Y) = X + Y + \cdots$$

a one-parameter commutative formal group law over R. *Suppose that for some prime power* p^n, *the equation*

$$X^{p^n} = 0$$

defines a subgroup-scheme of G. *Then* $p = 0$ *in* R, *and this subgroup-scheme is equal to* $\mathrm{Ker}(F^n)$.

Proof. Once we prove $p = 0$ in R, the Frobenius morphism is defined, and we visibly have that $\mathrm{Ker}(F^n)$ is defined by $X^{p^n} = 0$. To prove that $p = 0$ in R, we argue as follows. The hypothesis means that for any R-algebra B, and any elements $x,y \in B$, we have the implication

$$x^{p^n} = y^{p^n} = 0 \text{ in } B \Rightarrow (G(x,y))^{p^n} = 0 \text{ in } B .$$

Considering the universal situation

$$B = R[[X,Y]]/(X^{p^n}, Y^{p^n}) ,$$

we see that inside $R[[X,Y]]$, we have

$$(G(X,Y))^{p^n} \in (X^{p^n}, Y^{p^n}) ,$$

say

$$G(X,Y)^{p^n} = X^{p^n} \cdot A(X,Y) + Y^{p^n} \cdot B(X,Y) .$$

Comparing terms of total degree p^n, we obtain

$$(X+Y)^{p^n} = X^{p^n} \cdot A(0,0) + Y^{p^n} \cdot B(0,0) .$$

Comparing coefficients of X^{p^n} and Y^{p^n}, we see that $A(0,0) = B(0,0) = 1$, whence

$$(X+Y)^{p^n} = X^{p^n} + Y^{p^n} \text{ in } R[[X,Y]] .$$

Explicitly, this means that all the intermediate binomial coefficients vanish in R:

$$\binom{p^n}{i} = 0 \text{ in } R \text{ for } i = 1, \cdots, p^n - 1 .$$

Taking $i = 1$, we see that $p^n = 0$ in R. In particular, R is a Z_p-algebra. Taking $i = p^{n-1}$, and using the standard fact that

$$\binom{p^n}{p^{n-1}} = p \times (\text{an integer prime to } p),$$

We see that $p = 0$ in R. Q.E.D.

(5.3.5) It is now a simple matter to deduce the rigidity assertions I, II, III, (i.e., 5.3.2.1-2-3). Assertion II is just the proposition itself, applied to E/R. In Assertion III, the proposition applied directly to E/R shows that $p = 0$ in R and that $\mathrm{Ker}(\pi) = \mathrm{Ker}(F^n)$. To finish the proof of III, we must show that E/R is constant. This itself results from Assertion I, for it follows from (1.11.3), applied to the commutative diagram

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & K & \longrightarrow & E[p^n] & \longrightarrow & K' & \longrightarrow & 0 \\
 & & \uparrow 0 & & \uparrow 0 & & \uparrow 0 & & \\
0 & \longrightarrow & Z/p^nZ & \longrightarrow & (Z/p^nZ)^2 & \longrightarrow & (Z/p^nZ) & \longrightarrow & 0\,,
\end{array}
\qquad (5.3.5.1)
$$

that $(0,0)$ is a Drinfeld p^n-basis of E/R.

(5.3.6) To prove Assertion I, we argue as follows. If $(0,0)$ is a Drinfeld p^n-basis of E/R, then we have an equality of Cartier divisors

$$p^{2n}[0] = \mathrm{Ker}(p^n)\,.$$

In particular, $p^{2n}[0]$ is a subgroup, so Proposition 5.3.3 (with $E/R, p^{2n}$) shows that $p = 0$ in R, and that

$$\mathrm{Ker}(p^n) = \mathrm{Ker}(F^{2n})\,.$$

To show that E/R is constant, we argue as follows. We have exact sequences of R-group-schemes

$$
\begin{cases}
0 \longrightarrow \mathrm{Ker}(p^n) \longrightarrow E \xrightarrow{p^n} E \longrightarrow 0 \\
0 \longrightarrow \mathrm{Ker}(F^{2n}) \longrightarrow E \xrightarrow{F^{2n}} E^{(p^{2n})} \longrightarrow 0\,.
\end{cases}
$$

Because the kernels are equal, we have an R-isomorphism

$$E \xleftarrow{\sim} E^{(p^{2n})}\,.$$

Taking the Frobenius pull-backs of these isomorphism, we obtain isomorphisms

$$E \xleftarrow{\sim} E^{(p^{2n})} \xleftarrow{\sim} E^{(p^{4n})} \xleftarrow{\sim} E^{(p^{6n})} \cdots\,.$$

But for all sufficiently large r, the elliptic curve

$$E^{(p^r)}$$

is *constant*, simply because R is an artin local k-algebra,* so that for all $r >> 0$ the p^r-th power map on R factors

$$R \xrightarrow{F^r} k \longrightarrow R\,,$$

(i.e., we recover k as the subring of p^r-th powers for all $r >> 0$).

This concludes the proof of the rigidity assertions I, II, III, and with them the proof of the First Main Theorem 5.1.1 for

$$[\Gamma(N)],\ [\Gamma_1(N)],\ [\mathrm{bal.}\,\Gamma_1(N)]\,.\quad \text{Q.E.D.}$$

The proof of the First Main Theorem 5.1.1 for $\Gamma_0(N)$ will be given in Chapter 6.

(5.4) *Summary of parameters at supersingular points*

E_0/k is a supersingular elliptic curve over a perfect field k of characteristic p, $E/W(k)[[T]]$ is its universal formal deformation, X is a parameter for its formal group, A is the complete local ring such that $\mathcal{P}_{E/W[[T]]} = \mathrm{Spec}(A)$. If $\mathcal{P}$ is bal-Γ_1 or Γ_1, then E'/A is the quotient of $E \otimes A$ by the universal cyclic subgroup it carries, and X' is a parameter for the formal group of E' over A.

Moduli problem	basic data	parameters for A
$[\Gamma(p^n)]$	Drinfeld p^n-basis (P,Q)	$X(P)$, $X(Q)$
$[\mathrm{bal.}\,\Gamma_1(p^n)]$	$P\,;\ E \underset{\pi^t}{\overset{\pi}{\rightleftarrows}} E'\,;\ P'$ P generates $\mathrm{Ker}\,\pi$, P' generates $\mathrm{Ker}\,\pi^t$	$X(P)$, $X'(P')$
$[\Gamma_1(p^n)]$	point P of exact order p^n	T, $X(P)$.

(5.5) *First applications*

In this section, we will deduce some immediate consequences of the First Main Theorem for Γ, Γ_1, and balanced Γ_1.

*With residue field k.

THEOREM 5.5.1. *Let* $N > 1$ *be an integer, and let* $\mathcal{S}$ *be a representable moduli problem which is etale over* (Ell). *Then for*

$$\mathcal{P} = [\Gamma(N)],\ [\Gamma_1(N)],\ [\text{bal.}\,\Gamma_1(N)],$$

we have

(1) $\mathcal{M}(\mathcal{S}, \mathcal{P})$ *is a regular two-dimensional scheme, finite and flat over* $\mathcal{M}(\mathcal{S})$.

(2) $\mathcal{M}(\mathcal{S}, \mathcal{P}) \otimes \mathbf{Z}[1/N]$ *is finite etale over* $\mathcal{M}(\mathcal{S}) \otimes \mathbf{Z}[1/N]$.

(3) $\mathcal{M}(\mathcal{S}, \mathcal{P})$ *is flat over* $\mathbf{Z}$.

(4) $\mathcal{M}(\mathcal{S}, \mathcal{P})$ *is the normalization of* $\mathcal{M}(\mathcal{S})$ *in* $\mathcal{M}(\mathcal{S}, \mathcal{P}) \otimes \mathbf{Z}[1/N]$.

Proof. Assertions (1) and (2) are simply "mise pour memoire." Assertion (3) results from (1) because $\mathcal{M}(\mathcal{S})$ is itself flat over $\mathbf{Z}$, being a smooth curve over $\mathbf{Z}$. Assertion (4) results from (1) and (2), because the normalization in question is the unique normal scheme finite over $\mathcal{M}(\mathcal{S})$ which agrees with $\mathcal{M}(\mathcal{S}, \mathcal{P})$ outside of N.* Q.E.D.

THEOREM 5.5.2. *Let* E/S *be an elliptic curve,* $N > 1$ *an integer, and* $P, Q \in E[N](S)$ *a Drinfeld* N*-basis of* E/S. *Then*

(1) *the point* P *has "exact order* N*" on* E/S, *i.e.,* P *is a* $\Gamma_1(N)$*-structure on* E/S.

(2) *Let* $K \subset E[N]$ *denote the cyclic subgroup-scheme of rank* N *generated by* P. *The image* Q' *of* Q *in the quotient elliptic curve* E' *of* E *modulo* K *has "exact order* N*" on* E', *and* Q' *generates* K', *the quotient of* $E[N]$ *by* K. *In other words, the data* (P, K, Q') *is a balanced* $\Gamma_1(N)$*-structure on* E/S.

Proof. The theorem is obvious if N is invertible on S, (cf. 3.7.2). We will reduce to that case.

The question is f.p.p.f. local on S, so we may assume that some odd prime ℓ is invertible on S and that E/S admits a naive full level ℓ structure, which we abbreviate "$\mathcal{S}$-structure." By reduction to the universal case, we may assume that $S = \mathcal{M}(\mathcal{S}, \Gamma(N))$ and that E/S is the

*i.e., over the open set where N is invertible.

corresponding universal curve, (P,Q) its universal $\Gamma(N)$-structure. In particular, we may assume that the base S is flat over $\mathbf{Z}$, and affine, say $S = \text{Spec}(A)$.

Let us prove (1). We know that the $\Gamma_1(N)$-moduli problem $\mathcal{P}$ is relatively representable by a closed subscheme $\mathcal{P}_{E/A}$ of the affine A-scheme $Hom(\mathbf{Z}/N\mathbf{Z}, E) = E[N]$:

$$\mathcal{P}_{E/A} \hookrightarrow E[N].$$

Pick a collection of functions f_i in the affine ring of $E[N]$ which define the closed subscheme $\mathcal{P}_{E/A}$. We must show that, for all i,

$$f_i(P) = 0 \quad \text{in} \quad A.$$

But the theorem is true as soon as we invert N, i.e., we know that

$$f_i(P) = 0 \quad \text{in} \quad A[1/N].$$

Because A is flat over $\mathbf{Z}$, we have $A \subset A[1/N]$, whence $f_i(P) = 0$ in A, as required.

Let us now prove (2). Let K denote the cyclic subgroup-scheme of $E[N]$ "generated" by P, let K' denote the quotient of $E[N]$ by K, and let $Q' \in K'(A)$ denote the image of the point Q. We must show that Q' "generates" K'. But the scheme of generators of K' is a closed subscheme of the affine A-scheme $Hom(\mathbf{Z}/N\mathbf{Z}, K') = K'$:

$$\mathbf{Z}/N\mathbf{Z}\text{-}Gen(K'/A) \hookrightarrow K'.$$

Again, choosing a collection of functions f_i in the affine ring of K' which defines the closed subscheme of generators, we must show that

$$f_i(Q') = 0 \quad \text{in} \quad A.$$

Because the theorem is true as soon as we invert N, we know that

$$f_i(Q') = 0 \quad \text{in} \quad A[1/N],$$

so again by the flatness of A over $\mathbf{Z}$, we conclude that $f_i(Q') = 0$ in A. Q.E.D.

COROLLARY 5.5.3. *The constructions of the preceding theorem define natural morphisms of moduli problems*

$$[\Gamma(N)] \xrightarrow{\text{degree } N} [\text{bal. } \Gamma_1(N)] \xrightarrow{\text{degree } \phi(N)} [\Gamma_1(N)]$$

which are finite and flat of the indicated degrees. Concretely, for any representable moduli problem $\mathcal{S}$, *we have a natural diagram of morphisms, each of which is finite flat of the indicated degree*

$$\text{degree} = \#GL(2, \mathbb{Z}/N\mathbb{Z}) \left\{ \begin{array}{c} \mathcal{M}(\mathcal{S}, \Gamma(N)) \\ \downarrow \text{ degree } N \\ \mathcal{M}(\mathcal{S}, \text{bal. } \Gamma_1(N)) \\ \downarrow \text{ degree } \phi(N) \\ \mathcal{M}(\mathcal{S}, \Gamma_1(N)) \\ \downarrow \text{ degree } N^2 \cdot \prod_{p|N} \left(1 - \frac{1}{p^2}\right) \\ \mathcal{M}(\mathcal{S}) \end{array} \right.$$

Proof. That these morphisms are defined is the content of the preceding theorem. To see that they are finite and flat of the asserted degrees, we may reduce to the case when $\mathcal{S}$ is etale over (Ell), and $\mathcal{M}(\mathcal{S})$ is connected. In this case all the schemes involved are regular two-dimensional schemes, finite over $\mathcal{M}(\mathcal{S})$. Therefore all morphisms between them are necessarily finite; and consequently flat as well. To compute degrees, we may invert N (because $\mathcal{M}(\mathcal{S})$ is flat over $\mathbb{Z}$), and then the result is physically obvious (3.7.2). Q.E.D.

COROLLARY 5.5.4. *Let* E/S *be an elliptic curve,* $N > 1$ *an integer. Then*

(1) *locally f.p.p.f. on* S, *any* $\Gamma_1(N)$*-structure can be completed to a balanced* $\Gamma_1(N)$*-structure, and any balanced* $\Gamma_1(N)$*-structure on* E/S *can be completed to a* $\Gamma(N)$*-structure.*

(2) *locally f.p.p.f. on* S, E/S *admits* $\Gamma_1(N)$, balanced $\Gamma_1(N)$, *and* $\Gamma(N)$*-structures.*

(3) *If* K *is a finite locally free* S*-subgroup-scheme of rank* N *in* E[N], *and if* K *is "cyclic" (i.e., locally f.p.p.f. admits a "generator"), then the quotient* K′ *of* E[N] *by* K *is also cyclic.*

(4) *a point* $P \in E(S)$ *has "exact order* N*" on* E/S *if and only if locally f.p.p.f. on* S *we can complete* P *to a* $\Gamma(N)$*-structure* (P,Q) *on* E/S.

Proof. Indeed (1) and (2) hold if we only allow finite locally free base-changes $S' \to S$; this is precisely the meaning of the previous corollary. To prove (3), we may f.p.p.f. localize on S and suppose that K is the subgroup-scheme "generated" by some point $P \in E(S)$ of "exact order N." By (1), we may complete P to balanced $\Gamma_1(N)$-structure (P,K,Q′), after a further finite locally free $S' \to S$. Having done so, we have produced a generator for K′, namely Q′. The final assertion (4) is just the concatenation of assertion (1) above and of assertion (1) of Theorem 5.5.2. Q.E.D.

COROLLARY 5.5.5. *Let* E/S *be an elliptic curve,* $N > 1$ *an integer,* $P \in E[N](S)$ *a point of "exact order* N*" on* E/S, $Q \in E[N](S)$ *a point killed by* N. *Denote by* $K \subset E[N]$ *the cyclic subgroup-scheme of rank* N *generated by* P, *by* E′ *the quotient of* E mod K, *by* $K' \subset E'$ *the quotient of* E[N] mod K, *and by* $Q' \in K'(S)$ *the image of* Q. *Then the following conditions are equivalent.*

(1) (P,Q) *is a* $\Gamma(N)$*-structure on* E/S

(2) (P,K,Q′) *is a balanced* $\Gamma_1(N)$*-structure on* E/S.

Proof. By (5.5.2), (1) implies (2). The converse is a special case of (1.11.3), applied to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/N\mathbb{Z} & \longrightarrow & \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z} & \longrightarrow & \mathbb{Z}/N\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow P & & \downarrow (P,Q) & & \downarrow Q' & & \\ 0 & \longrightarrow & K & \longrightarrow & E[N] & \longrightarrow & K' & \longrightarrow & 0. \end{array}$$

Q.E.D.

CAUTION 5.5.6. In the above corollary, consider the condition

(3) Q' has "exact order N" in E'/S.

Trivially (2) $\Rightarrow$ (3), but they are *not* equivalent. Indeed, if N is a prime power p^n, and if S is an F_p-scheme, then the origin $Q' = 0$ has "exact order p^n" in E'/S, and $P = 0$ has "exact order p^n" on E/S. So if (3) were equivalent to (2), and so to (1), we would find that on *any* E/S with S/F_p, $(0,0)$ is a Drinfeld p^n-basis!

THEOREM 5.5.7. *Let E/S be an elliptic curve, $N > 1$ an integer, and $P,Q \in E[N](S)$ a pair of points of order N. Then*

(1) *If (P,Q) is a Drinfeld N-basis of E/S, then for any divisor d of N, the points (dP, dQ) are a Drinfeld N/d-basis of E/S.*

(2) *If P has "exact order N" on E/S, then for every divisor d of N, the point dP has "exact order N/d" on E/S.*

(3) *Suppose that $N = p^n$ with p a prime, and $n \geq 2$. Then (P,Q) is a Drinfeld p^n-basis of E/S if and only if (pP,pQ) is a Drinfeld p^{n-1}-basis on E/S.*

(4) *If $N = p^n$ with $n \geq 2$ as in (3) above, then P has "exact order p^n" on E/S if and only if pP has "exact order p^{n-1}" on E/S.*

Proof. The problem is local f.p.p.f. on S. By (4) of Corollary (5.5.4), the assertions (2) and (4) are consequences of the assertions (1) and (3). The proof of (1) is entirely analogous to the proof of part (1) of Theorem 5.5.2; it uses only the fact that $[\Gamma(N)]$ is flat over $\mathbf{Z}$, that $[\Gamma(N/d)]$ is relatively representable by a closed subscheme of the relatively affine moduli problem

$$E/S \mapsto E[N/d](S) \times E[N/d](S),$$

and that the assertion is (by 3.7.2) obviously true once we invert N.

To prove the "if" direction of (3), we must show that if (pP,pQ) is a Drinfeld p^{n-1}-basis of E/S, then (P,Q) is a Drinfeld p^n-basis of E/S. Let us temporarily denote by $\mathcal{P}$ the moduli problem

$\mathcal{P}(E/S)$ = pairs of points P,Q in $E[p^n](S)$ such that (pP,pQ) is a Drinfeld p^{n-1}-basis of E/S.

This is a relatively representable moduli problem; indeed for any E/S, we have a cartesian diagram of S-schemes

$$\begin{array}{ccc} (P,Q) & \mathcal{P}_{E/S} \subset & E[p^n] \times E[p^n] \\ \downarrow & \downarrow & \downarrow (p,p) \text{ finite flat of degree } p^4 \\ (pP,pQ) & [\Gamma(p^{n-1})]_{E/S} \subset & E[p^{n-1}] \times E[p^{n-1}] \end{array}.$$

Therefore $\mathcal{P}$ is finite flat over $[\Gamma(p^{n-1})]$ of degree p^4, and hence it is finite and flat over (Ell), so in particular flat over $\mathbf{Z}$. By reduction to the universal case, it suffices to show that if E/A is an elliptic curve over a ring A which is flat over $\mathbf{Z}$, and if P,Q in $E[p^n](A)$ are a $\mathcal{P}$-structure on E/A, then they are a $\Gamma(p^n)$-structure. The moduli problem $[\Gamma(p^n)]$ is relatively representable by a closed subscheme of the affine A-scheme $E[p^n] \times E[p^n]$:

$$[\Gamma(p^n)]_{E/A} \hookrightarrow E[p^n] \times E[p^n].$$

It is physically obvious (from 3.7.2) that the pair (P,Q) defines a $\Gamma(p^n)$-structure as soon as we pass to $A[1/p]$; therefore if $f_i = 0$ are the equations defining $[\Gamma(p^n)]$ inside $E[p^n] \times E[p^n]$, we have $f_i(P,Q) = 0$ in $A[1/p]$ whence $f_i(P,Q) = 0$ in A because A is flat over $\mathbf{Z}$. Q.E.D.

COROLLARY 5.5.8. *Let E/S be an elliptic curve, $N \geq 1$ and integer, d a divisor of N such that N and N/d have exactly the same prime divisors. Let P,Q be a pair of points in $E[N](S)$. Then*

(1) *The pair (P,Q) is a Drinfeld N-basis on E/S if and only if the pair (dP,dQ) is a Drinfeld N/d-basis on E/S.*

(2) *The point* P *has "exact order* N *" on* E/S *if and only if the point* dP *has "exact order* N/d *" on* E/S.

Proof. This is just the concatenation of (3) and (4) of Theorem (5.5.7), with the elementary "factorization into prime powers" (3.5.1) for $\Gamma(N)$ and $\Gamma_1(N)$-structures. Q.E.D.

(5.6) *Pairings*

(5.6.1) In this section, we analyze the behavior of our moduli problems with respect to the e_N pairing and the $<\ ,\ >_\pi$ pairing (cf. 2.8).

(5.6.2) Recall (1.12) that an N'th root of unity $\zeta \in \mu_N(S)$ is said to be a "primitive N'th of unity" if it is a root of the N'th cyclotomic polynomial in the ring $\Gamma(S, \mathcal{O}_S^\times)$, or equivalently, if viewed as a point of $G_m(S)$ it has "exact order N " in G_m/S, or equivalently if it "generates" μ_N/S.

THEOREM 5.6.3. *Let* E/S *be an elliptic curve,* $N \geq 1$ *an integer. Then*

(1) *If* (P,Q) *is a Drinfeld* N*-basis of* E/S, *then* $e_N(P,Q)$ *is a "primitive* N'th *root of unity" in* $\mu_N(S)$.

(2) *If the data*

$$P \in (\mathrm{Ker}\ \pi)(S);\quad E \underset{\pi^t}{\overset{\pi}{\rightleftarrows}} E';\quad P' \in (\mathrm{Ker}\ \pi^t)(S)$$

is a balanced $\Gamma_1(N)$*-structure on* E/S, *then* $<P, P'>_\pi$ *is a "primitive* N'th *root of unity" in* $\mu_N(S)$.

Proof. The question is f.p.p.f. local on S, so to prove (2) we may, by (5.5.4), part (1), assume there is a Drinfeld N-basis on E/S, (P,Q), with $P' = \pi Q$. Then $<P, P'>_\pi = e_N(P,Q)$, so it suffices to prove (1). Now (1) is physically obvious if N is invertible. We will reduce to that case. By reduction to the universal case, we may assume that S is affine, say $S = \mathrm{Spec}(A)$, with A flat over $\mathbf{Z}$. We must show that

$$\Phi_N(e_N(P,Q)) = 0 \quad \text{in} \quad A,$$

where Φ_N denotes the N'th cyclotomic polynomial. But we know that $\Phi_N(e_N(P,Q)) = 0$ in $A[1/N]$, and A is flat over $\mathbf{Z}$. Q.E.D.

REMARK 5.6.4. Given an elliptic curve E/S with N invertible on S, a pair of points (P,Q) in E[N](S) is a $\Gamma(N)$-structure if and only if $e_N(P,Q)$ is a primitive N'th root of unity in $\mu_N(S)$. This equivalence breaks down over a general S. Indeed if N is a prime power p^n, then for any $\mathbf{F}_p$-scheme S, and any power p^k of p, the trivial root of unity $1 \in \mu_{p^k}(S)$ is a "primitive p^k'th root of unity." But in general (0,0) is not a $\Gamma(p^k)$-structure on an elliptic curve over an $\mathbf{F}_p$-scheme, although $e_{p^k}(0,0) = 1$ is a "primitive p^k'th root of unity."

COROLLARY 5.6.5. *The moduli problems* $[\Gamma(N)]$ *and* $[\mathrm{bal.}\,\Gamma_1(N)]$ *are relatively representable over* (Ell) *by* $\mathbf{Z}[\zeta_N]$*-schemes, where* $\mathbf{Z}[\zeta_N]$ *denotes the ring* $\mathbf{Z}[X]/(\Phi_N(X))$. *Concretely, for any representable moduli problem* $\mathcal{S}$, *the schemes*

$$\mathcal{M}(\mathcal{S}, \Gamma(N)),\quad \mathcal{M}(\mathcal{S}, \mathrm{bal.}\,\Gamma_1(N))$$

have natural structures of schemes over $\mathcal{M}(\mathcal{S}) \underset{\mathbf{Z}}{\otimes} \mathbf{Z}[\zeta_N]$, *defined by the functions* $e_N(P,Q)$, $<P, P'>_\pi$ *on these schemes.*

TERMINOLOGY 5.6.6. We will refer to the primitive N'th root of unity $e_N(P,Q)$ (resp. $<P, P'>_\pi$) as the *determinant* of the corresponding $\Gamma(N)$ (resp. balanced $\Gamma_1(N)$)-structure.

Chapter 6
CYCLICITY

In this chapter, we develop the theory of "cyclic" subgroups of elliptic curves, and prove the First Main Theorem 5.1.1 for $[\Gamma_0(N)]$.

(6.1) *The Main Theorem*

Let S be an arbitrary scheme, and G/S a finite locally free commutative group-scheme of rank N. We say that G is cyclic if, locally f.p.p.f. on S, G admits a generator, (a "$\mathbf{Z}/N\mathbf{Z}$-generator" in the notations of (1.10.5)) i.e., a section $P \in G(S)$ such that its N multiples $\{aP\}$, $a = 0, 1, \cdots, N-1$ form a "full set of sections" of G/S. The functor on (Sch/S)

$$T \mapsto \text{generators of } G_T/T$$

is representable by a closed subscheme $G^\times$ of G, defined, locally on S, by finitely many equations ($G^\times$ is the scheme denoted "$\mathbf{Z}/N\mathbf{Z}$-*Gen*(G/S)" in (1.10.13)),

$$\begin{array}{ccc} G^\times & \subset & G \\ & \searrow \quad \swarrow & \\ & S & \end{array}$$

We refer to $G^\times$ as the "scheme of generators" of G. It is a finite S-scheme of finite presentation, whose formation commutes with arbitrary change of base $S' \to S$.

MAIN THEOREM ON CYCLIC GROUPS (6.1.1). *Let E/S be an elliptic curve over an arbitrary base S, $N \geq 1$ an integer, and $G \subset E[N]$ a finite locally free commutative S-subgroup-scheme of E/S, of rank N over S. Then*

(1) *G is cyclic if and only if its scheme of generators $G^\times$ is finite locally free over S, of rank $\phi(N)$.*

(2) *Suppose that G/S is cyclic, and that $P \in G(S)$ is a generator. Then the Cartier divisor D in E defined by*

$$D = \sum_{\substack{(a,N)=1 \\ a \bmod N}} [aP]$$

lies in G, and we have an equality of closed subschemes of G

$$D = G^\times .$$

Proof. If $G^\times$ is finite locally free over S, of rank $\phi(N)$, then G is certainly cyclic, for it acquires a generator after the f.p.p.f. base change $G^\times \to S$. The problem is to prove the converse, that if G is cyclic then necessarily $G^\times$ is finite locally free over S of the asserted rank $\phi(N)$. The question is f.p.p.f. local on S, so we may assume that G admits a generator $P \in G(S)$. In this case, (1) follows from (2), for the Cartier divisor D is visibly finite locally free over S, of degree $\phi(N)$. Thus it suffices to prove (2). By the "factorization into prime powers" lemma (1.7.3, 1.10.15), we may reduce to the case when N is a prime power > 1, say $N = p^n$. We also remark that (by 3.7.2), (2) is physically obvious if N is invertible on S.

We will first show that D lies inside $G^\times$. It is obvious that D lies inside G, for G as a Cartier divisor in E is given by

$$G = \sum_{a \bmod N} [aP] .$$

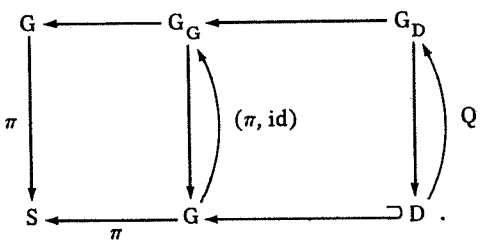
Because G is embedded in E/S, it follows from (1.10.11) that D is the

unique closed subscheme of G which is finite locally free over S of degree $\phi(N)$ and for which the $\phi(N)$ sections $\{aP\}$ with a mod N, $(a,N)=1$ form a full set of sections.

To show that $D \subset G^\times$, it suffices, by reduction to the universal case, to treat the case when S is affine, $S = \mathrm{Spec}(A)$, and flat over $\mathbf{Z}$ (simply because $[\Gamma_1(N)]$ is flat over $\mathbf{Z}$). Let

$$Q \in G(D) = G_D(D)$$

be the tautological section which G acquires when pulled back to D:



We must show that Q is a generator of G_D. Let $\{f_i\}$ be a collection of functions in the affine coordinate ring of G which define the closed subscheme $G^\times$. We must show that

$$f_i(Q) = 0 \quad \text{in} \quad \Gamma(D, \mathcal{O}_D).$$

But D is flat over $\mathbf{Z}$, being finite flat over A, and we know that the assertion is true if we invert N:

$$f_i(Q) = 0 \quad \text{in} \quad \Gamma(D, \mathcal{O}_D) \otimes \mathbf{Z}[1/N].$$

Therefore we must have $f_i(Q) = 0$ in $\Gamma(D, \mathcal{O}_D)$. This concludes the proof that $D \subset G^\times$.

Because both D and $G^\times$ are finite over S the inclusion $D \subset G^\times$ is necessarily a closed immersion. We wish to show that this closed immersion is an isomorphism. To do this, we reduce to the universal case.

Consider the following two moduli problems, $\mathcal{P}_1$ and $\mathcal{P}_2$, with respect to the fixed prime power $N = p^n$:

$\mathcal{P}_1(E/S)$ = triples (P, G, Q) where $P \in E[N](S)$ is a generator of a cyclic S-subgroup-scheme $G \subset E[N]$ finite locally free over S of rank N, and $Q \in D(S)$, where $D \subset G$ is the unique finite locally free S-subscheme of rank $\phi(N)$ of which the sections $\{aP\}$, a mod N, $(a,N)=1$, are a full set of sections.

$\mathcal{P}_2(E/S)$ = triples (P, G, Q) where P, G are as above, and $Q \in G^\times(S)$ is another generator of G.

Because $D \subset G^\times$, any $\mathcal{P}_1$-structure is a $\mathcal{P}_2$-structure, so we have a morphism of moduli problems

$$\mathcal{P}_1 \to \mathcal{P}_2.$$

To prove that $D = G^\times$ is to prove that this morphism is an isomorphism.

We will prove this by a variant of the homogeneity argument of (5.2).

(6.2) *Axiomatics*

AXIOMATIC ISOMORPHISM THEOREM (6.2.1). *Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be moduli problems on* (Ell), *and*

$$\mathcal{P}_1 \to \mathcal{P}_2$$

a morphism between them. Suppose that

(1) *Both $\mathcal{P}_1$ and $\mathcal{P}_2$ satisfy axioms Reg. 1, Reg. 3, and Reg. 4A of (5.2).*

(2) *After inverting p, the induced morphism of moduli problems on* (Ell/$\mathbf{Z}[1/p]$) *is an isomorphism*

$$\mathcal{P}_1 \otimes \mathbf{Z}[1/p] \xrightarrow{\sim} \mathcal{P}_2 \otimes \mathbf{Z}[1/p].$$

(3) *For any algebraically closed field* k *of characteristic* p, *and any supersingular elliptic curve* E_0/k *with universal formal deformation* $E/W(k)[[T]]$, *the morphism of finite* $W[[T]]$*-schemes*

$$\mathcal{P}_{1,E/W[[T]]} \to \mathcal{P}_{2,E/W[[T]]}$$

is an isomorphism.

Then the given morphism is an isomorphism $\mathcal{P}_1 \xrightarrow{\sim} \mathcal{P}_2$.

Proof. The proof is entirely analogous to that of the Axiomatic Regularity Theorem 5.2.1, with the open set $\mathcal{U} \subset M(\mathcal{S})$ of that proof replaced by "the" open set V over which the morphism of finite $M(\mathcal{S})$-schemes

$$M(\mathcal{S}, \mathcal{P}_1) \to M(\mathcal{S}, \mathcal{P}_2)$$

is an isomorphism. To see that "the" open set V makes sense, interpret the finite $M(\mathcal{S})$-schemes in question as coherent sheaves of algebras $\mathcal{F}_1$ and $\mathcal{F}_2$ on $M(\mathcal{S})$. The given morphism corresponds to an $\mathcal{O}_{M(\mathcal{S})}$-linear map

$$\mathcal{F}_2 \to \mathcal{F}_1$$

of coherent sheaves on $M(\mathcal{S})$, which happens to be an algebra homomorphism. Forget the algebra structure, and consider the kernel and cokernel as coherent sheaves on $M(\mathcal{S})$, say

$$0 \to \text{Ker} \to \mathcal{F}_2 \to \mathcal{F}_1 \to \text{Coker} \to 0 .$$

Then V is precisely the open set of the noetherian scheme $M(\mathcal{S})$ over which the coherent sheaf Ker $\oplus$ Coker vanishes. Q.E.D.

(6.3) *End of the proof*

(6.3.1) We will now apply this Axiomatic Isomorphism Theorem 6.2.1 to the moduli problems $\mathcal{P}_1$ and $\mathcal{P}_2$ defined in 6.1 above. They are both relatively representable and finite over (Ell) (the axiom Reg. 1) simply because they are both relatively representable and finite over $[\Gamma_1(p^n)]$, by

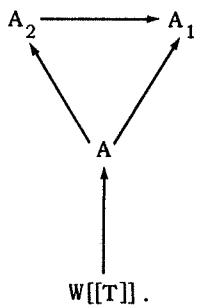
D and by $G^\times$ respectively, and because $[\Gamma_1(p^n)]$ is itself finite and flat (5.1.1) over (Ell). That they both satisfy Reg. 3, i.e., depend only on the underlying p-divisible groups, is clear from the somewhat convoluted definitions we have given of them. That they both satisfy Reg. 4A is clear from the fact that on a supersingular E_0/k, the unique possible G is $\text{Ker}(F^n)$, the unique possible P, Q's are zero, because $G(k) = \{0\}$, and the zero-section is in fact a generator of $\text{Ker}(F^n)$.

This shows that condition (1) of 6.2.1 is satisfied. We have already remarked that condition (2) holds. The work comes in checking condition (3).

(6.3.2) We must show that the morphism

$$\mathcal{P}_{1,E/W[[T]]} \to \mathcal{P}_{2,E/W[[T]]}$$

is an isomorphism. This is a morphism of schemes finite over $\mathcal{P}_{E/W[[T]]}$, where $\mathcal{P}$ is the moduli problem $[\Gamma_1(p^n)]$, and $\mathcal{P}_{E/W[[T]]}$ is itself finite over $W[[T]]$. These schemes are spectra of complete local rings, which sit in a diagram



Let us recall the explicit description of these rings.

Fix a parameter X for the formal group of $E/W[[T]]$. For any integer a, denote by

$$[a](X) \in W[[T]][[X]]$$

the expression of the endomorphism "multiplication by a" on this formal group. Then A is easily described as a $W[[T]]$-algebra:

$A = W[[T, P]]/I$

where I is the ideal generated by the equations which express that the finite free subscheme of $\hat{E}$ of rank p^n defined over $W[[T, P]]$ by the equation

$$\prod_{1 \le a \le p^n} (X - [a](P)) = 0$$

is in fact a subgroup-scheme.

We know that A is a regular two-dimensional local ring with parameters (T, P), and that A is finite flat over $W[[T]]$ (5.1.1 and 5.4).

Over A, A_1 is easily described:

$A_1 = A[[Q]]/J$

where J is the principal ideal generated by

$$\prod_{\substack{(b,p)=1 \\ b \bmod p^n}} (Q - [b](P)) .$$

Over A, A_2 is also easily described:

$A_2 = A[[Q]]/K$

where K is the ideal in $A[[Q]]$ which expresses that in $A[[Q]][[X]]$, we have an equality of monic polynomials in X

$$\prod_{1 \le a \le p^n} (X - [a](Q)) = \prod_{a \bmod p^n} (X - [a](P)) .$$

We know that $D \hookrightarrow G^\times$ is a closed immersion, i.e., that the homomorphism of rings

$$A_2 \to A_1$$

is *surjective*. Both A_2 and A_1 are finite A-modules (i.e., both D and $G^\times$ lie inside G, so are finite over S), and A_1 is free of rank $\phi(p^n)$

over A. Consider the kernel

$$0 \to \mathrm{Ker} \to A_2 \to A_1 \to 0 ;$$

it is a finite A-module. We must show that $\mathrm{Ker} = 0$.

Both A_1 and A_2 are presented as quotients of the ring $A[[Q]]$. Therefore Ker is itself a (finitely generated) $A[[Q]]$-module, being the kernel of a homomorphism of (finitely generated) $A[[Q]]$-modules. By Nakayama's lemma, we have

$$\mathrm{Ker} = 0 \iff \mathrm{Ker}/Q\mathrm{Ker} = 0 .$$

(6.3.3) We will show that $\mathrm{Ker}/Q\mathrm{Ker} = 0$. For this, consider the serpent lemma, applied to the exact sequence

$$0 \to \mathrm{Ker} \to A_2 \to A_1 \to 0$$

and to the endomorphism "multiplication by Q."

LEMMA 6.3.4. *The endomorphism "multiplication by Q" on A_1 is injective.*

Proof. By Weierstrass preparation, we may view A_1 as the quotient of the polynomial ring $A[Q]$ by the monic polynomial in Q

$$\prod_{\substack{b \bmod p^n \\ (b,p)=1}} (Q - [b](P)) = 0 .$$

Therefore A_1 is A-free with basis $1, Q, Q^2, \cdots, Q^{\phi(p^n)-1}$. Because A is a regular local ring, it is an integral domain, so an endomorphism of a free A-module of finite rank is injective if and only if its *determinant* is non-zero in A. The determinant of "multiplication by Q" on A_1 is $\pm$ the *constant term* of the monic polynomial

$$\prod_{\substack{b \bmod p^n \\ (b,p)=1}} (Q - [b](P)) ,$$

i.e., we have

$$\det_A(Q|A_1) = \prod_{\substack{b \bmod p^n \\ (b,p)=1}} [b](P) .$$

To see that this determinant is non-zero, we argue as follows. There is an obvious action of the group $(\mathbf{Z}/p^n\mathbf{Z})^\times$ on the moduli problem $[\Gamma_1(p^n)]$, given modularly by $P \mapsto bP$. The induced action of $(\mathbf{Z}/p^n\mathbf{Z})^\times$ on A is given precisely by $P \mapsto [b](P)$. Therefore the determinant is the product of P and all its transforms by a group of automorphisms of A. As P is *non-zero* in A, being part of a regular system of parameters for A, (cf. 5.4) all its $(\mathbf{Z}/p^n\mathbf{Z})^\times$-transforms are also non-zero, and hence, A being a domain, their product is non-zero in A. Q.E.D.

Therefore the serpent lemma yields a short exact sequence

$$0 \to \mathrm{Ker}/Q\mathrm{Ker} \to A_2/QA_2 \to A_1/QA_1 \to 0 .$$

LEMMA 6.3.5. *The natural map* $A_2/QA_2 \to A_1/QA_1$ *is an isomorphism.*

Proof. From the explicit descriptions of A_1 and A_2 as A-algebras, we have

$$A_2/QA_2 = A/\underline{K}$$

where $\underline{K}$ is the ideal of A generated by the coefficients of the polynomial

$$X^{p^n} - \prod_{a \bmod p^n} (X - [a](P))$$

$$A_1/QA_1 = A/\underline{\mathfrak{h}}$$

where $\underline{\mathfrak{h}}$ is the principal ideal of A generated by

$$\prod_{\substack{b \bmod p^n \\ (b,p)=1}} [b](P) .$$

We must show that $\underline{K} = \underline{\mathfrak{h}}$. From the fact that the map $A_2/QA_2 \to A_1/QA_1$ *exists* (i.e., from the inclusion $D \subset G^\times$) we see that

$$\underline{K} \subset \underline{\mathfrak{h}} .$$

To reverse the inclusion, we must show that the element of A

$$\prod_{\substack{b \bmod p^n \\ (b,p^n)=1}} [b](P)$$

actually lies in the ideal $\underline{K}$.

For this, consider the term of degree $p^n - \phi(p^n)$ in the polynomial

$$X^{p^n} - \prod_{a \bmod p^n} (X - [a](P)) .$$

Its coefficient lies in $\underline{K}$. We will show that, up to a *unit* in A, this coefficient is equal to

$$\prod_{\substack{b \bmod p^n \\ (b,p)=1}} [b](P) .$$

Indeed, this coefficient is equal to the sum of *all* $\phi(p^n)$-fold products of distinct elements of the set of p^n quantities

$$[a](P), \quad a \bmod p^n .$$

LEMMA 6.3.6. *Let* a *be an integer. In the ring* A *we have*

$$[a](P) = \begin{cases} P \times (\textit{unit of } A) & \textit{if} \quad (a,p) = 1 \\ P \times (\textit{elt. of } \max(A)) & \textit{if} \quad p \textit{ divides } a . \end{cases}$$

Proof. Consider the series $[a](X)$ expressing "multiplication by a" on our formal group $\hat{E}$ over A:

$$[a](X) \equiv aX \bmod (X^2)A[[X]] ;$$

therefore

$$[a](X) = X \times (a + \text{elt. in } XA[[X]]) .$$

Substituting $P \in \max(A)$ gives the assertion. Q.E.D.

It is now immediate that both quantities

$$\begin{cases} \prod_{\substack{b \bmod p^n \\ (b,p)=1}} [b](P) \\ \\ \text{the coefficient of } X^{p^n - \phi(p^n)} \text{ in } \prod_{a \bmod p^n} (X - [a](P)) \end{cases}$$

are of the form

$$(\text{a unit in } A) \times P^{\phi(p^n)} .$$

This concludes the proof of the Main Theorem (6.1.1) on Cyclic groups. Q.E.D.

(6.4) *Cyclicity as a closed condition*

THEOREM 6.4.1. *Let* E/S *be an elliptic curve,* $N \geq 1$ *an integer, and* $G \subset E[N]$ *a finite locally free commutative* S*-subgroup-scheme of* E/S, *of rank* N *over* S. *Then there exists a closed subscheme* $W \subset S$, *defined locally on* S *by finitely many equations, which is universal for the condition "* G *is cyclic", in the sense that for any morphism* $T \to S$, *the inverse image* G_T/T *is cyclic if and only if the map* $T \to S$ *factors through the closed subscheme* W.

Proof. The question is Zariski local on S, which we may suppose affine. Because E and G are of finite presentation over S, we may further reduce to the case when S is noetherian. Consider the finite S-scheme $G^\times$ of generators of G, which we view as the *Spec* of a coherent sheaf $\mathcal{F}$ of algebras on S:

$$G^\times = Spec(\mathcal{F}) .$$

By the Main Theorem on Cyclic Groups (6.1), the condition on an S-scheme $T \to S$ that G_T be cyclic is that its scheme of generators $(G_T)^\times \xleftarrow{\simeq} (G^\times) \times_S T$ be a finite locally free scheme over T of rank $\phi(N)$. In terms of the coherent sheaf $\mathcal{F}$ on S, the condition is that the inverse image coherent sheaf $\mathcal{F}_T$ on T be locally free on T of rank $\phi(N)$.

LEMMA 6.4.2. *For any field-valued point* $\mathrm{Spec}(k) \to S$ *of* S, *the fiber* $\mathcal{F} \otimes k$ *is a* k*-vector space, whose dimension is given by*

$$\dim_k(\mathcal{F} \otimes k) = \begin{cases} \phi(N) & \text{if } G_k/k \text{ is cyclic} \\ \\ 0 & \text{if not.} \end{cases}$$

Proof. The k-vector space $\mathcal{F} \otimes k$ is the affine ring of $(G^\times) \otimes k \simeq (G_k)^\times$. If G_k/k is cyclic, then $(G_k)^\times$ is a finite k-scheme of rank $\phi(N)$, by the Main Theorem on Cyclic Groups (6.1). If G_j/k is *not* cyclic, then, k being a field, G_k never becomes cyclic after any field extension. Therefore the k-scheme $(G_k)^\times$ has no field-valued points, hence it is the empty scheme, i.e., its affine ring is the zero-ring. Q.E.D.

In view of this lemma, Theorem 6.4.1 is a special case of

PROPOSITION (6.4.3). *Given a noetherian scheme* S, *a coherent sheaf* $\mathcal{F}$ *on* S, *and an integer* n *such that*

$$\text{for all } s \in S, \quad \dim_{k(s)}(\mathcal{F} \otimes k(s)) \leq n ,$$

the condition on S*-schemes* $T \to S$ *that* $\mathcal{F}_T$ *be locally free of rank* n *on* T *is represented by a closed subscheme* W *of* S.

Proof. This is Mumford's "flattening stratification", cf. [Mum 2]. For the reader's convenience, we briefly recall the construction of the closed subscheme W. Let $s \in S$ be a point of S. By hypothesis, we can find n sections $e_1, \cdots, e_n$ of $\mathcal{F}$ over some open neighborhood U of s in S which span $\mathcal{F} \otimes k(s)$, hence which span $\mathcal{F} \otimes \mathcal{O}_{S,s}$ (by Nakayama), hence

which span $\mathcal{F}$ in some open neighborhood, which we may, by shrinking the original U, take to be U itself.

Thus we have a surjection

$$(\mathcal{O}_U)^n \xrightarrow{\pi} \mathcal{F}|U \longrightarrow 0\,,$$

which, U being noetherian, we may extend (again shrinking U) to a presentation

$$(\mathcal{O}_U)^m \xrightarrow{\alpha} (\mathcal{O}_U)^n \xrightarrow{\pi} \mathcal{F}|U \longrightarrow 0\,.$$

We claim that $W \cap U$ is defined inside U by the vanishing of the nm matrix coefficients of the map α. It is clear that over the locus $\alpha = 0$, $\mathcal{F}$ will be locally free of rank n.

To prove the converse, pull back to any U-scheme. The presentation pulls back to a presentation (right-exactness of $\otimes$), so we are reduced to checking that over a no-longer-necessarily noetherian U, if $\mathcal{F}|U$ is locally free of rank n then $\alpha = 0$. Zariski-localizing on U, we may assume $\mathcal{F}$ free of rank n on U, and that we have a splitting β ($\pi\beta = \mathrm{id}_{\mathcal{F}}$) of the projection $(\mathcal{O}_U)^n \twoheadrightarrow \mathcal{F}$:

$$\begin{array}{ccccccc} (\mathcal{O}_U)^m & \xrightarrow{\alpha} & (\mathcal{O}_U)^n & \xrightarrow{\pi} & \mathcal{F} & \longrightarrow & 0 \\ & & \| & & & & \\ & & (\mathcal{O}_U)^n & \xleftarrow{\beta} & & & \end{array}$$

The " $\alpha = 0$ " is equivalent to " β is surjective." By Cramer's rule, " β surjective" is implied by " $\det(\beta)$ invertible", and this invertibility follows from " $\pi \circ \beta = \mathrm{id}_{\mathcal{F}}$ " upon taking determinants. Q.E.D.

(6.5) *The moduli problem* [N-Isog]

For any elliptic curve E/S, we define

[N-Isog](E/S) = the set of finite locally free commutative S-subgroup-schemes $G \subset E[N]$ which are of rank N over S.

PROPOSITION 6.5.1. *The moduli problem* [N-Isog] *is relatively representable and finite over* (Ell).

Proof. Given E/S, view E[N]/S as the *Spec* of a coherent sheaf $\mathcal{F}$ of bi-algebras on S which is locally free of rank N^2. A subgroup $G \subset E[N]$ of the type being sought is nothing other than a locally free rank-N quotient $\mathfrak{h}$ of $\mathcal{F}$, such that the locally free rank N^2-N kernel $\mathcal{K} \subset \mathcal{F}$ is a bi-ideal in $\mathcal{F}$. Therefore [N-Isog] is relatively represented by a closed subscheme of the Grassmannian of all rank N quotients of $\mathcal{F}$, i.e., [N-Isog] is relatively representable and projective over (Ell). To see that it is finite over (Ell), we must show it has finite fibers, i.e., we must show that

$$[N\text{-Isog}](E/k) = \{\text{a finite set}\}$$

when k is an algebraically closed field. Factoring N into a product of prime powers, say $N = \prod p_i^{n_i}$, we have

$$[N\text{-Isog}] = \prod [p_i^{n_i}\text{-Isog}]\,,$$

so we are reduced to the case when N is a prime power, say $N = p^n$. If $\mathrm{char}(k) \neq p$, the assertion is physically obvious ($(\mathbf{Z}/p^n\mathbf{Z})^2$ has only finitely many subgroups). If $\mathrm{char}(k) = p$, and E/k is supersingular, the *unique* subgroup of E/k of rank p^n is $\mathrm{Ker}(F^n)$. If $\mathrm{char}(k) = p$ and E/k is ordinary, the $E[p^n]$ is isomorphic to $\mu_{p^n} \times \mathbf{Z}/p^n\mathbf{Z}$. Any G/k is canonically a product (k being perfect)

$$G \xrightarrow{\sim} G^{\mathrm{conn}} \times G^{\mathrm{et}}$$

and therefore the only possible G's of rank p^n are the $n+1$ subgroups

$$\mu_{p^a} \times (p^{n-b}\mathbf{Z}/p^n\mathbf{Z}), \qquad a+b=n,$$

of $\mu_{p^n} \times \mathbf{Z}/p^n\mathbf{Z}$. Q.E.D.

(6.6) *The moduli problem* $[\Gamma_0(N)]$; *proof of the First Main Theorem 5.1.1*

THEOREM 6.6.1. *The moduli problem* $[\Gamma_0(N)]$ *is relatively representable over* (Ell). *It is finite and flat over* (Ell) *of degree*

$$\frac{N^2}{\phi(N)} \prod_{p|N} \left(1 - \frac{1}{p^2}\right).$$

The natural map

$$[\Gamma_1(N)] \to [\Gamma_0(N)]$$

is finite and flat of rank $\phi(N)$. *The moduli problem* $[\Gamma_0(N)]$ *is regular and two-dimensional.*

Proof. For any E/S, $[\Gamma_0(N)]$ is relatively represented by the closed subscheme of the finite S-scheme

$$[\text{N-Isog}]_{E/S}$$

over which the universal N-isogeny is cyclic. Therefore by (6.5.1), $[\Gamma_0(N)]$ is itself relatively representable and finite over (Ell).

The moduli problem $[\Gamma_1(N)]$ is relatively representable over $[\Gamma_0(N)]$ by the scheme of generators $G^\times$ of the universal cyclic N-group over $[\Gamma_0(N)]$. Therefore $[\Gamma_1(N)]$ is finite and flat over $[\Gamma_0(N)]$ of rank $\phi(N)$. We have already proven (5.1.1) that $[\Gamma_1(N)]$ is regular and two-dimensional, therefore $[\Gamma_0(N)]$ is also regular and two-dimensional, being finite flat "under" $[\Gamma_1(N)]$ (cf. [A-K 1, VII, 4.8]). Once $[\Gamma_0(N)]$ is regular and two-dimensional, and is finite over (Ell), it is necessarily finite and flat over (Ell) [A-K 1, V, 3.8].* We may compute its degree after inverting N

*Alternately, $[\Gamma_0(N)]$ is flat over (Ell) because $[\Gamma_1(N)]$ is flat over (Ell) and faithfully flat over $[\Gamma_0(N)]$.

(cf. 4.12.1), where we find the asserted degree, namely the number of cyclic subgroups of order N inside $(\mathbf{Z}/N\mathbf{Z})^2$ (cf. 3.7.2). Q.E.D.

THEOREM 6.6.2. *Let* $N \geq 1$ *be an integer, and* $\mathcal{S}$ *a representable moduli problem which is etale over* (Ell). *Then:*

(1) $M(\mathcal{S}, \Gamma_0(N))$ *is a regular two-dimensional scheme, finite and flat over* $M(\mathcal{S})$.
(2) $M(\mathcal{S}, \Gamma_0(N)) \otimes \mathbf{Z}[1/N]$ *is finite etale over* $M(\mathcal{S}) \otimes \mathbf{Z}[1/N]$.
(3) $M(\mathcal{S}, \Gamma_0(N))$ *is flat over* $\mathbf{Z}$.
(4) $M(\mathcal{S}, \Gamma_0(N))$ *is the normalization of* $M(\mathcal{S})$ *in* $M(\mathcal{S}, \Gamma_0(N)) \otimes \mathbf{Z}[1/N]$.

Proof. Entirely analogous to the proof of (5.5.1). Q.E.D.

(6.7) *Detailed theory of cyclic isogenies and cyclic subgroups; standard factorizations*

(6.7.1) We will use the expression "cyclic group (over S) of order N" or simply "cyclic group" if S and its order N are understood, as shorthand for "finite locally free commutative S-group-scheme, of rank N, and cyclic", and the expression "cyclic N-isogeny" to mean an isogeny whose kernel is a cyclic group of order N.

THEOREM 6.7.2. *Let* E/S *be an elliptic curve,* $G \subset E/S$ *a cyclic subgroup over* S *of order* N. *For every divisor* d *of* N, *there is a "standard" cyclic subgroup* $G_d \subset G$ *of order* d, *which may be described, f.p.p.f. locally on* S, *in terms of any generator* P *of* G, *as the cyclic subgroup of order* d *generated by* $(N/d)P$.

Proof. It suffices to construct G_d f.p.p.f. locally on S. Let P and P′ be two generators of G. By (5.5.7) we know that the points $(N/d)P$ and $(N/d)P'$ both have "exact order d", so they generate subgroups G_d and G'_d respectively. We must show that $G'_d = G_d \subset G$. That they both lie in G is clear from their descriptions as Cartier divisors inside E:

$$G = \sum_{a \bmod N} [aP]$$

$$G_d = \sum_{b \bmod d} [b(N/d)P]$$

and similarly for G'_d, with P replaced by P'.

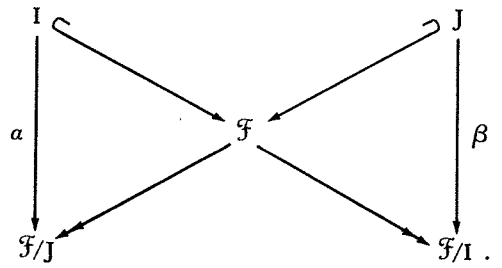
To show that $G_d = G'_d$, we may reduce to the case where S is flat over $\mathbf{Z}$, and noetherian (because the universal case of a cyclic G with two generators is the moduli problem

$$[\Gamma_1(N)] \times [\Gamma_1(N)]$$
$$[\Gamma_0(N)]$$

which by (6.6.1) is finite flat over $[\Gamma_0(N)]$ of degree $(\phi(N))^2$, hence is flat over $\mathbf{Z}$). It is physically obvious that $G_d = G'_d$ whenever N is invertible on S. Because S is flat over $\mathbf{Z}$, the open set $S \otimes \mathbf{Z}[1/N]$ of S is dense in S. So it suffices to see that the condition "$G_d = G'_d$" defines a *closed* subscheme of S.

USEFUL LEMMA 6.7.3. *Let S be a noetherian scheme, W a finite flat S-scheme, and Z_1, Z_2 two closed subschemes of W, each of which is finite flat over S. Then the locus "$Z_1 = Z_2$" is a closed subscheme of S.*

Proof. Let $\mathcal{F}$ denote the locally free sheaf of algebras on S such that $W = Spec(\mathcal{F})$, I and J the locally free sheaves of ideals in $\mathcal{F}$ whose locally free quotients $\mathcal{F}/I$ and $\mathcal{F}/J$ correspond to Z_1 and Z_2 respectively. The locus "$Z_1 = Z_2$" is the closed subscheme of S over which both of the maps α, β between locally free sheaves on S vanish.



Q.E.D.

THEOREM 6.7.4. *Let E/S be an elliptic curve, $G \subset E[N]$ a cyclic subgroup of order N, d a divisor of N, and $G_d \subset G$ the standard cyclic subgroup of G of order d. Then the quotient group $G' = G \bmod G_d$ in the quotient elliptic curve $E' = E \bmod G_d$ is cyclic of order N/d. If P is a generator of G, then its image P' in G' generates G'. If $d|d'|N$, then $G_d \subset G_{d'}$ is the standard cyclic subgroup of $G_{d'}$ of order d, and the quotient $G_{d'}/G_d$ in G/G_d is its standard cyclic subgroup of order (d'/d).*

Proof. The question is f.p.p.f. local on S, so we may assume G has a generator P. By reduction to the universal case ($[\Gamma_1(N)]$ being flat over $\mathbf{Z}$), it suffices to treat the case when S is flat over $\mathbf{Z}$. The locus over which G' is cyclic is a closed subscheme of S, which contains the dense open $S \otimes \mathbf{Z}[1/N]$. Similarly, the locus over which P' generates G' is closed in S, and contains the dense open $S \otimes \mathbf{Z}[1/N]$. The third assertion is that $G_d = (G_{d'})_d$ inside G, and that $G_{d'}/G_d = (G/G_d)_{d'/d}$ inside G'. This is physically obvious when N is invertible, and its locus of truth is a closed subscheme of S, this time by the Useful Lemma (6.7.3). Q.E.D.

COROLLARY 6.7.5. *Let E/S be an elliptic curve, $G \subset E/S$ a cyclic subgroup over S of order N. For each divisor d of N, denote by $G_d \subset G$ the standard cyclic subgroup of order d, and by $(G_d)^\times \subset G_d$ its scheme of generators. Then we have an equality of Cartier divisors inside E*

$$G = \sum_{d|N} (G_d)^{\times}.$$

Proof. The equality of two Cartier divisors inside E/S may be checked f.p.p.f. locally on S. This reduces us to the case when G admits a generator P, in which case the assertion is obvious; for we have

$$G = \sum_{a \bmod N} [aP]; \qquad G_d^{\times} = \sum_{b \bmod d} [b(N/d)P]. \qquad \text{Q.E.D.}$$

(6.7.6) In the situation of Theorem 6.7.4, we will refer to $G' = G \bmod G_d$ as the standard cyclic N/d-quotient of the cyclic group G. Given a cyclic N-isogeny, π, with kernel G,

$$E \xrightarrow[\ker = G]{\pi} E''$$

and a divisor d of N, we will refer to the factorization

$$E \xrightarrow[\ker = G_d]{\pi_d} E' \xrightarrow[\ker = G']{\pi'} E''$$

as the *standard factorization* of the cyclic N-isogeny π into a cyclic d-isogeny followed by a cyclic N/d-isogeny, or simply as the standard factorization, if d and N/d are given.

(6.7.7) Suppose we are given a pair of composable isogenies

$$E \xrightarrow{\pi_1} E' \xrightarrow{\pi_2} E''$$

with π_1 and π_2 of degrees d_1 and d_2 respectively. We say that the pair (π_1, π_2) is cyclic in standard order if both of the following conditions hold:

(1) The composite $\pi_2 \circ \pi_1$ is cyclic.

(2) The given factorization is standard, i.e., $\mathrm{Ker}(\pi_1)$ is the standard cyclic subgroup of $\mathrm{Ker}(\pi_2\pi_1)$ of order d_1.

PROPOSITION 6.7.8. *Let π_1 and π_2 be a pair of composable isogenies*

$$E \xrightarrow{\pi_1} E' \xrightarrow{\pi_2} E''$$

over a base S, of constant ranks d_1 and d_2. Suppose that π_2 is etale (a condition which is automatic if d_2 is invertible on S). Then the following are equivalent.

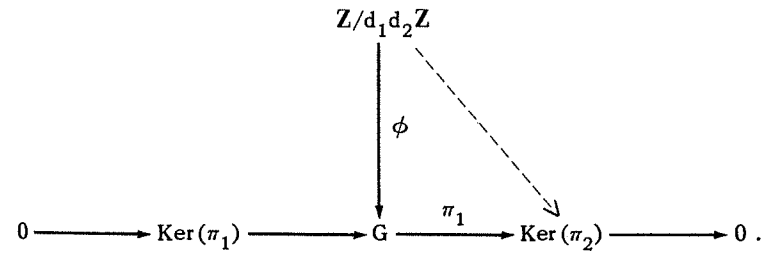
(1) *The composite $\pi = \pi_2\pi_1$ is cyclic.*

(2) *π_1, π_2 and $\pi = \pi_2\pi_1$ are all cyclic.*

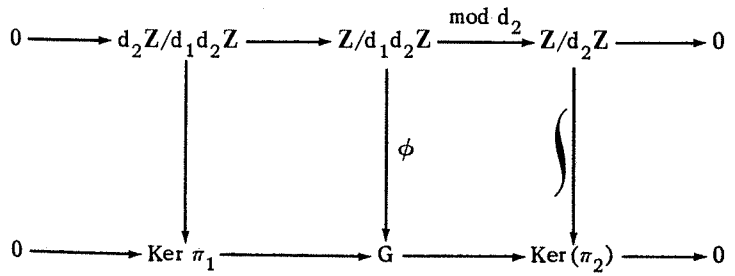
(3) *π, π_1, π_2 are all cyclic, and (π_1, π_2) is the standard factorization of π.*

Proof. Trivially (3) $\Rightarrow$ (2) $\Rightarrow$ (1). We must show (1) $\Rightarrow$ (2), (3).

The question is f.p.p.f. local on S, so we may assume that $G = \mathrm{Ker}(\pi)$ admits a generator $\phi : \mathbf{Z}/d_1d_2\mathbf{Z} \to G(S)$. Consider the exact sequence



Applying the key result (1.11.2), we see that the oblique arrow must be surjective, whence we have a commutative diagram



all of whose vertical arrows are generators. Thus (1) $\Rightarrow$ (2). Therefore G is generated by $P = \phi(1)$, and Ker π_1 is generated by $d_2 P$, so that Ker π_1 is the standard subgroup of G of rank d_1. Thus (1) $\Rightarrow$ (3). Q.E.D.

THEOREM 6.7.9. *Let π_1 and π_2 be composable cyclic isogenies of elliptic curves over a base S*

$$E \xrightarrow{\pi_1} E' \xrightarrow{\pi_2} E'',$$

with π_i cyclic of degree d_i. Consider the diagram of dual isogenies

$$E \xleftarrow{\pi_1^t} E' \xleftarrow{\pi_2^t} E''.$$

(By (5.5.4, (3)), these duals are also cyclic.) Then (π_1, π_2) is cyclic in standard order if and only if (π_2^t, π_1^t) is cyclic in standard order.

Proof. By symmetry, it suffices to prove the implication one way. Thus let $\pi = \pi_2 \pi_1$, a cyclic isogeny of degree $d_1 d_2$. The statement is that for any cyclic isogeny π of degree $d_1 d_2$, the standard subgroup of $\mathrm{Ker}(\pi^t)$ of order d_2 is *equal* to the subgroup $\mathrm{Ker}(\pi_2^t)$ of $\mathrm{Ker}(\pi^t)$. Because $[\Gamma_0(d_1 d_2)]$ is flat over $\mathbf{Z}$, we may reduce to the case when S is flat over $\mathbf{Z}$, and noetherian. The assertion is visibly true over the dense open set $S \otimes \mathbf{Z}[1/N]$, $N = d_1 d_2$, and by the Useful Lemma 6.7.3 its locus of truth is closed in S. Q.E.D.

PROPOSITION 6.7.10. *Let π_1 and π_2 be composable isogenies of elliptic curves over a base S,*

$$\begin{array}{ccccc} E & \xrightarrow{\pi_1} & E' & \xrightarrow{\pi_2} & E'', \\ & \searrow^{\pi} & & & \end{array}$$

whose degrees d_1 and d_2 are relatively prime: $(d_1, d_2) = 1$. Then the following conditions are equivalent.

(1) *π_1 and π_2 are each cyclic.*

(2) *π is cyclic.*

(3) *π, π_1 and π_2 are each cyclic, and (π_1, π_2) is the standard factorization of π.*

Proof. Let $G = \mathrm{Ker}(\pi)$. Then G has rank $d = d_1 d_2$ with $(d_1, d_2) = 1$. Therefore G has a unique product structure $G = G_1 \times G_2$ where for $i = 1, 2$, $G_i = G[d_i]$ is the subgroup-scheme of G of elements killed by d_i, and where G_i is itself finite locally free of rank d_i. Then G is cyclic if and only if both G_1 and G_2 are cyclic, and a point $P = (P_1, P_2)$ is a generator of G if and only if P_i generates G_i for $i = 1, 2$. Therefore (1) $\Longleftrightarrow$ (2), and we have (2) $\Longleftrightarrow$ (3) because $\mathrm{Ker}(\pi_1)$, having rank d_1, must lie in $G[d_1] = G_1$, whence $\mathrm{Ker}\ \pi_1 = G_1$, and similarly if G is cyclic, its standard subgroup of rank d_1 must also coincide with G_1. Q.E.D.

BACKING-UP THEOREM 6.7.11. *Let E/S be an elliptic curve, $N \geq 1$ an integer, d a divisor of N, and*

$$\begin{array}{ccccc} E & \xrightarrow{\pi_d} & E' & \xrightarrow{\pi'} & E'' \\ & \searrow & & \nearrow & \\ & & \pi & & \end{array}$$

the standard factorization of a cyclic N-isogeny into a cyclic d-isogeny followed by a cyclic N/d-isogeny.

Let $P \in (\mathrm{Ker}\ \pi)(S)$. Then

(1) *If P generates Ker π, then $\pi_d P$ generates Ker π', and $(N/d)P$ generates $\mathrm{Ker}(\pi_d)$.*

(2) *If N and N/d have the same prime factors, then P generates Ker π if and only if $\pi_d P$ generates Ker π'. (In particular, 0 generates Ker π if and only if 0 generates Ker π'.)*

Let us first prove (1). That $(N/d)P$ generates $\mathrm{Ker}(\pi_d)$ is clear from the definition of the standard factorization. To prove that $\pi_d P$ generates Ker π', we argue as follows.

The data of a cyclic N-isogeny together with a generator P of $\mathrm{Ker}(\pi)$ is precisely a $\Gamma_1(N)$-structure on E. As $[\Gamma_1(N)]$ is flat over $\mathbf{Z}$, we may, by reduction to the universal case, reduce to the case when S is flat over $\mathbf{Z}$. The statement (1) is obviously true over $S \otimes \mathbf{Z}[1/N]$, and the locus in S over which a given point $(\pi_d P)$ generates a given group $(\mathrm{Ker}\ \pi')$ is closed in S.

To prove (2), we argue as follows. By (1), the map π_d defines a morphism of schemes of generators

$$\begin{array}{ccc} (\mathrm{Ker}\ \pi)^\times & \xrightarrow{\pi_d} & (\mathrm{Ker}\ \pi')^\times \\ \downarrow & & \downarrow \\ \mathrm{Ker}\ \pi & \xrightarrow{\pi_d} & \mathrm{Ker}\ \pi' \ . \end{array}$$

The assertion of (2) is that when N and N/d have the same prime factors, this diagram of finite S-schemes is cartesian, whenever π is a cyclic N-isogeny. Because $[\Gamma_0(N)]$ is flat over $\mathbf{Z}$, the usual reduction to the universal case reduces us to the case when S is flat over $\mathbf{Z}$, and noetherian.

It is physically obvious that (2) holds over $S \otimes \mathbf{Z}[1/N]$. So it suffices to check that the locus in S where (2) holds is a closed subscheme of S. For this, we simply apply the Useful Lemma 6.7.3 to the finite flat S-scheme $\mathrm{Ker}\ \pi$, its finite, flat over S subscheme $(\mathrm{Ker}\ \pi)^\times$, and the fiber-product of the diagram

$$\begin{array}{ccc} & & (\mathrm{Ker}\ \pi')^\times \\ & & \downarrow \\ (\mathrm{Ker}\ \pi) & \xrightarrow{\pi_d} & \mathrm{Ker}\ \pi' \ . \end{array}$$

This fiber product is finite flat over S because π_d is a finite flat map, and $(\mathrm{Ker}\ \pi')^\times$ is finite flat over S. Q.E.D.

THEOREM 6.7.12. *Let π_1, π_2 be a pair of composable isogenies of elliptic curves over a base S,*

$$E \xrightarrow{\pi_1} E' \xrightarrow{\pi_2} E''$$

which are both cyclic, of degrees d_1 and d_2 respectively. Suppose that d_1 and d_2 have exactly the same prime divisors.

Let $P \in \mathrm{Ker}(\pi_2\pi_1)(S)$. Then the following conditions are equivalent:

(1) *The cyclic isogenies (π_1, π_2) are cyclic in standard order, and P generates $\mathrm{Ker}(\pi_2\pi_1)$.*

(2) *The point d_2P generates $\mathrm{Ker}\ \pi_1$, and the point $\pi_1 P$ generates $\mathrm{Ker}\ \pi_2$.*

Proof. That (1) implies (2) is part (1) of the preceding theorem. To prove that (2) implies (1), we argue as follows. Consider the point $P \in E(S)$.

Because d_2P generates $\mathrm{Ker}\ \pi_1$, d_2P has "exact order d_1", and hence P has "exact order d_1d_2" (by 5.5.8, (2)). Consider the cyclic subgroup $G \subset E$ of order d_1d_2 generated by P. Its standard cyclic subgroup of order d_1 is precisely $\mathrm{Ker}\ \pi_1$. Therefore its standard cyclic quotient G′ of order d_2 is the cyclic subgroup of E′ generated by $\pi_1 P$. As $\pi_1 P$ generates $\mathrm{Ker}\ \pi_2$, we have $G' = \mathrm{Ker}(\pi_2)$. This shows that (π_1, π_2) is the standard factorization of the cyclic d_1d_2 isogeny whose kernel is generated by P. Q.E.D.

STANDARD ORDER CRITERION 6.7.13. *Let π_1, π_2 be a composable pair of cyclic isogenies*

$$E \xrightarrow{\pi_1} E' \xrightarrow{\pi_2} E''$$

where π_i is cyclic of degree d_i, $i = 1, 2$, and where d_1 and d_2 have the same prime divisors. In order that (π_1, π_2) be cyclic in standard order, it is necessary and sufficient that, locally f.p.p.f. on S, we have one of the following equivalent conditions:

a) *For every generator* $P' \in E'(S)$ *of* $\mathrm{Ker}\ \pi_2$, *and every* $P \in E(S')$ *with* $S' \to S$ *f.p.p.f. and* $\pi_1 P = P'$, *the point* $d_2 P$ *generates* $\mathrm{Ker}\ \pi_1$ *over* S'.

b) *For some generator* $P' \in E'(S)$ *of* $\mathrm{Ker}\ \pi_2$, *and for some* $P \in E(S')$ *with* $S' \to S$ *f.p.p.f. and* $\pi_1 P = P'$, *the point* $d_2 P$ *generates* $\mathrm{Ker}\ \pi_1$ *over* S'.

Proof. Clearly a) implies b). If b) holds, then the point P satisfies condition (2) of the preceding theorem, and hence (π_1, π_2) is cyclic in standard order, with $\mathrm{Ker}(\pi_2 \pi_1)$ generated by P. If (π_1, π_2) is cyclic in standard order, we claim a) holds.

By the Backing-up Theorem 6.7.11, if P' generates $\mathrm{Ker}\ \pi_2$, any P with $\pi_1 P = P'$ generates $\mathrm{Ker}(\pi_2 \pi_1)$, and therefore by the preceding theorem we have $d_2 P$ generates $\mathrm{Ker}(\pi_1)$. Q.E.D.

(6.7.14). Suppose we are given a sequence of $n \geq 2$ composable isogenies of elliptic curves over some base S

$$E_0 \xrightarrow{\pi_1} E_1 \xrightarrow{\pi_2} E_2 \longrightarrow \cdots \xrightarrow{\pi_n} E_n ,$$

with each π_i cyclic of degree d_i.

We say that $(\pi_1, \cdots, \pi_n)$ are cyclic in standard order if the composite $\pi_n \circ \cdots \circ \pi_1$ is cyclic, and if the given factorization corresponds to the filtration of its kernel $G = \mathrm{Ker}(\pi_n \cdots \pi_1)$ by the successive standard cyclic subgroups $G_{d_1}, G_{d_1 d_2}, \cdots, G_{d_1 d_2 \cdots d_n}$ of G, i.e., if for every i the i-fold composite $\pi_i \cdots \pi_1$ has kernel $G_{d_1 \cdots d_i}$. If this is the case, then for $j > i$ the map $\pi_j \cdots \pi_{i+1}$ has kernel the standard cyclic subgroup of $G/G_{d_1 \cdots d_i}$ of order $d_{i+1} \cdots d_j$.

THEOREM 6.7.15. *Consider a sequence of* $n \geq 2$ *composable cyclic isogenies*

$$E_0 \xrightarrow{\pi_1} E_1 \xrightarrow{\pi_2} \cdots \xrightarrow{\pi_n} E_n ,$$

whose degrees $d_1, \cdots, d_n$ *all have the same prime divisors. Then in order that* $(\pi_1, \cdots, \pi_n)$ *be cyclic in standard order, it is necessary and sufficient that every two-step chain* (π_i, π_{i+1}) *be cyclic in standard order.*

Proof. As already noted, the necessity is clear. For sufficiency, we proceed by induction on n, the case $n = 2$ being vacuously true. By induction, we know all chains of length $\leq n-1$ are cyclic in standard order. In particular, for $1 \leq i \leq n-1$ the isogeny $\pi_i \cdots \pi_1$ is cyclic, and its kernel is the standard cyclic subgroup of order $d_1 \cdots d_i$ in $\mathrm{Ker}(\pi_{n-1} \cdots \pi_1)$. Because standard subgroups of standard subgroups are standard, we are left with proving that $\pi_n \cdots \pi_1$ is cyclic, and that $\mathrm{Ker}(\pi_{n-1} \cdots \pi_1)$ is its standard cyclic subgroup of order $d_1 \cdots d_{n-1}$. In other words, we must prove that the pair $(\pi_{n-1} \cdots \pi_1, \pi_n)$ is cyclic in standard order. Locally f.p.p.f. on S, we may choose $P_{n-1} \in E_{n-1}(S)$ which generates $\mathrm{Ker}(\pi_n)$, and a sequence of points $P_i \in E_i(S)$ for $i = 0, \cdots, n-2$ such that

$$P_{n-1} = \pi_{n-1} P_{n-2}, P_{n-2} = \pi_{n-2} P_{n-3}, \cdots, P_1 = \pi_1 P_0 .$$

By the standard order criterion, it suffices to show that

$$d_n P_0 \text{ generates } \mathrm{Ker}(\pi_{n-1} \circ \cdots \circ \pi_1) .$$

To see this, we argue as follows. The pair (π_{n-1}, π_n) is cyclic in standard order. Therefore $d_n P_{n-2}$ generates $\mathrm{Ker}(\pi_{n-1})$, by the standard order criterion. The pair $(\pi_{n-2} \cdots \pi_1, \pi_{n-1})$ is cyclic in standard order by induction, and $(\pi_{n-2} \cdots \pi_1)(d_n P_0) = d_n P_{n-2}$. Therefore by the Backing-up Theorem, $d_n P_0$ generates $\mathrm{Ker}(\pi_{n-1} \circ \cdots \circ \pi_1)$, as required. Q.E.D.

REMARK 6.7.16. The reason we have developed the notion of the standard factorization of a cyclic isogeny, and criteria for recognizing it, is that an isogeny which isn't etale may have non-standard factorizations. The most striking example is this. Let S be any F_p-scheme, E/S an elliptic curve, and $E^{(p)}/S$ its absolute Frobenius transform. We will see later

that over F_p-schemes, the morphism "multiplication by p" is cyclic, and that its standard factorization is

$$E \xrightarrow{F} E^{(p)} \xrightarrow{V} E .$$

If we replace E by $E^{(p)}$, we get the decidedly *non-standard* factorization

$$E^{(p)} \xrightarrow{V} E \xrightarrow{F} E^{(p)} .$$

We *do not know* a good criterion to decide when a composition of two cyclic isogenies is again a cyclic isogenies if the two are *not* in standard order.

(6.8) *More on* [N-Isog]

THEOREM 6.8.1. *For any integer* $N \geq 1$, *the moduli problem* [N-Isog] *is finite and flat over* (Ell). *In particular, it is flat over* $\mathbf{Z}$. *After tensoring with* $\mathbf{Z}[1/N]$, *it becomes finite etale over* $(Ell/\mathbf{Z}[1/N])$.

Proof. We will first reduce to the case when N is a prime power. If $N = N_1N_2$ with $(N_1, N_2) = 1$ then we have, for any representable moduli problem $\mathcal{S}$, a canonical $\mathcal{M}(\mathcal{S})$-isomorphism

$$\mathcal{M}(\mathcal{S}, [N\text{-Isog}]) \xrightarrow{\sim} \mathcal{M}(\mathcal{S}, [N_1\text{-Isog}]) \underset{\mathcal{M}(\mathcal{S})}{\times} \mathcal{M}(\mathcal{S}, [N_2\text{-Isog}]) .$$

We also remark that it is physically obvious that $[N\text{-Isog}] \otimes \mathbf{Z}[1/N]$ is finite etale over $(Ell/\mathbf{Z}[1/N])$.

To prove the theorem with N a prime power, say $N = p^n$, we will use a variant of the Axiomatic Regularity Theorem.

AXIOMATIC FINITE FLATNESS THEOREM 6.8.2.. *Let* $\mathcal{P}$ *be a moduli problem which satisfies the axioms Reg. 1, Reg. 2, Reg. 3, and Reg. 4A, with respect to a prime number* p. *Then* $\mathcal{P}$ *is finite flat over* (Ell) *if and only if the following condition holds*:

(FF) *Let* k *be any algebraically closed field of characteristic* p, E_0/k *any supersingular elliptic curve,* $E/W(k)[[T]]$ *its universal formal deformation. Then the scheme* $\mathcal{P}_{E/W[[T]]}$, *which is the spectrum of a local ring finite over* $W[[T]]$, *is flat over* $W[[T]]$.

Proof. The proof is entirely analogous to the proof of the Axiomatic Regularity Theorem, with the open set U in $\mathcal{M}(\mathcal{S}_1)$ the open set of all points $x \in \mathcal{M}(\mathcal{S}_1)$ such that for every $y \in \mathcal{M}(\mathcal{S}_1, \mathcal{P})$ with $y \to x$, the local ring upstairs at y is flat over the local ring downstairs at x. Q.E.D.

(6.8.3). We now apply this theorem to $\mathcal{P} = [p^n\text{-Isog}]$. We have already checked axioms Reg. 1 and Reg. 2, and Reg. 3 obviously holds. Reg. 4A holds because in a supersingular E_0/k with k a field, $\mathrm{Ker}(F^n)$ is the unique subgroup-scheme of E_0/k of rank p^n. It remains to prove that $[p^n\text{-Isog}]$ verifies the condition (FF).

Let A denote the complete local ring such that

$$[p^n\text{-Isog}]_{E/W[[T]]} = \mathrm{Spec}(A) .$$

Let

$$G \subset E \underset{W[[T]]}{\otimes} A$$

be the universal finite flat subgroup of rank p^n, let E' be the elliptic curve over A which is the quotient of $E \otimes A$ mod G, and let

$$E \otimes A \xrightarrow{\pi} E'$$

be the corresponding p^n-isogeny with kernel G.

Let E_1/k denote the special fiber of E'/A. We fix an isomorphism $E_1 \xleftarrow{\sim} E_0^{(p^n)}$ which carries π to F^n.

The ring A pro-represents the functor Φ on artin local $W(k)$-algebras with residue field k defined by

$$\Phi(R) = \begin{cases} p^n\text{-isogenies } E \xrightarrow{\pi} E' \text{ of elliptic curves} \\ \text{over } R \text{ together with an isomorphism of} \\ \text{the special fiber with the } p^n\text{-isogeny} \\ \\ E_0 \xrightarrow{F^n} E_0^{(p^n)} \xrightarrow{\sim} E_1 \,. \end{cases}$$

Fix a universal formal deformation of E_1/k, say $E_1/W[[T_1]]$. The constructions "source of π", "target of π", define a morphism of functors

$$\Phi(R) \to \begin{pmatrix}\text{formal deformations}\\ \text{of } E_0/k \text{ to } R\end{pmatrix} \times \begin{pmatrix}\text{formal deformations}\\ \text{of } E_1/k \text{ to } R\end{pmatrix}.$$

By rigidity, this map is *injective* on R-valued points, for any artin local W(k)-algebra R. Furthermore, it is a closed immersion, as follows immediately from Drinfeld's approach to the Serre-Tate theorem. For the reader's convenience, we state the result explicitly.

THEOREM 6.8.4 (Drinfeld). *Let* R *be a ring in which a prime number* p *is nilpotent,* I *a nilpotent ideal of* R, R_0 *the ring* R/I, *and* X, Y *two abelian schemes over* R. *Suppose that we are given a homomorphism of abelian schemes over* R_0

$$X \underset{R}{\otimes} R_0 \xrightarrow{f_0} Y \underset{R}{\otimes} R_0 .$$

Then

(1) *For any* n *large enough that the sequence of ideals of* R *given by* $I^{(0)} = I, \cdots, I^{(k+1)} = (pI^{(k)}, (I^{(k)})^2)$, *has* $I^{(n)} = 0$, *the homomorphism* $p^n f_0$ *lifts to a homomorphism of abelian schemes over* R

$$X \xrightarrow{\text{"}p^n f\text{"}} Y .$$

(2) *The homomorphism* f_0 *lifts to a homomorphism of abelian schemes over* R

$$X \xrightarrow{f} Y$$

if and only if for n *as above, the homomorphism "*$p^n f$*" induces the zero-map*

$$X[p^n] \xrightarrow{\text{"}p^n f\text{"}} Y[p^n] .$$

(3) *If* f_0 *lifts to an* f, *the lifting* f *is unique. If* f *exists, then* f *is an isogeny (i.e., finite flat) if and only if* f_0 *is.*

Proof. See [Dr 2] or [K-5]. Q.E.D.

COROLLARY 6.8.5. *The "locus of existence" of a lifting* f *is the closed subscheme of* R *over which a specific map, "*$p^n f_0$*", between specific finite flat locally free* R*-group-schemes, namely* $X[p^n]$ *and* $Y[p^n]$, *is the zero-map.*

Applying these results to our functor Φ, we see that Φ is pro-represented by the formal closed subscheme of $\mathrm{Spec}(W[[T, T_1]])$ over which the map of elliptic curves over k

$$E_0 \xrightarrow{F^n} E_0^{(p^n)} \xrightarrow{\sim} E_1$$

lifts to a homomorphism of elliptic curves

$$E \xrightarrow{\pi} E_1 .$$

Concretely, this means that the ring A is a quotient of the ring $W[[T, T_1]]$, by some ideal J. It suffices to prove that the ideal J is principal, say $J = (f)$. For if this is so, then f is $\neq 0$ (because A is finite over $W[[T]]$, and $f \neq 1$ (because $\Phi(k)$ is non-empty). Therefore, f is a non-unit non-zero-divisor in a regular local ring $W[[T, T_1]]$ of dimension three, and hence $A = W[[T, T_1]]/(f)$ is itself Cohen-Macaulay of dimension two. We already know that A is finite over the two-dimensional regular local ring $W[[T]]$, and therefore it is automatically finite and flat over $W[[T]]$ (cf. [A-K 1, V, 3.5]).

To prove that the ideal J is generated by a single element, we argue as follows (compare the proof of Proposition 1.5 in [De-Il]). The ideal J is a proper ideal of $W[[T,T_1]]$ (because A is finite over $W[[T]]$), and hence lies in the maximal ideal. Therefore $W[[T,T_1]]$ is J-adically complete and separated. So an obvious recursion argument shows that any element $f \in J$ such that $J = (J^2, f)$ is automatically a generator of J. To see that such an element exists, we argue as follows. Over the ring $R_0 = W[[T,T_1]]/J$, we have the universal lifting π of the isogeny F^n. Suppose we try to lift further to the ring $R = W[[T,T_1]]/J^2$, a "square-zero thickening" of R_0. We must show that the "locus of liftability of π" in $\mathrm{Spec}(R)$ is defined by a single equation $f = 0$ with $f \in R$. (For by construction this locus of liftability is the subscheme defined by the ideal J/J^2 in R, hence any lifting of $f \in J/J^2$ to an element of J will satisfy $J = (J^2, f)$, as required.) Q.E.D.

Thus we are reduced to the following proposition (which applies "globally" on our R, because it is a local ring).

PROPOSITION 6.8.6. *Let R be a ring, $I \subset R$ an idea of square zero, E and E_1 elliptic curves over R, and ϕ_0 a homomorphism between their reductions* mod I

$$E\otimes(R/I) \xrightarrow{\phi_0} E_1\otimes(R/I)\,.$$

Then the closed subscheme of $\mathrm{Spec}(R)$ *over which ϕ_0 lifts is defined, locally on R, by a single equation $f = 0$.*

Proof. By autoduality of elliptic curves, the homomorphism ϕ_0 is induced by an invertible sheaf $\mathcal{L}_0$ on $(E\underset{R}{\times}E_1)\otimes(R/I)$, by the formalism of divisorial correspondences (cf. [De-Gi-Ray, Exp. VII, §2], [SGA 7, VIII 3.2.4 and VII 2.9.5]). The invertible sheaf $\mathcal{L}_0$ is unique up to tensoring with an arbitrary invertible sheaf of the form $\mathrm{pr}_1^*(\mathcal{F}_0)\otimes\mathrm{pr}_2^*(\mathcal{G}_0)$, where $\mathcal{F}_0$ and $\mathcal{G}_0$ are arbitrary invertible sheaves on $E\otimes(R/I)$ and on $E_1\otimes(R/I)$ respectively. Because E and E_1 are curves, there is no obstruction to

lifting any such $\mathcal{F}_0$, $\mathcal{G}_0$ to invertible sheaves on E and on E_1 respectively. Therefore the homomorphism lifts if and only if the invertible sheaf $\mathcal{L}_0$ lifts to an invertible sheaf $\mathcal{L}$ on $E\underset{R}{\times}E_1$. The obstruction to the existence of such a lifting is an element in the cohomology group

$$H^2(E\underset{R}{\times}E_1, \mathcal{O})\otimes I\,.$$

Locally on R, the group $H^2(E\times E_1, \mathcal{O})$ is a free R-module of rank one, and so locally on R the vanishing of the obstruction is expressed by a single equation. Q.E.D.

COROLLARY 6.8.7. *If $N \geq 1$ is a square-free integer, then every N-isogeny is cyclic, i.e., the closed immersion of moduli problems over* (Ell)

$$[\Gamma_0(N)] \hookrightarrow [N\text{-Isog}]$$

is an isomorphism.

Proof. We must show that if N is square-free, then for any elliptic curve E/S and any S-subgroup $G \subset E[N]$ which is finite locally free of rank N over S, G is cyclic. Because $[N\text{-Isog}]$ is flat over $\mathbf{Z}$, the usual "reduction to the universal case" reduces us to treating the case when S is flat over $\mathbf{Z}$. The locus "G is cyclic" is a closed subscheme of S, so it suffices to show that G is cyclic over $S\otimes\mathbf{Z}[1/N]$, where it is physically obvious: an abelian group of square-free order is cyclic. Q.E.D.

THEOREM 6.8.8. *If N is not a square-free integer, then the moduli problem* [N-Isog] *is not normal.*

Proof. Write $N = p^n N_1$ with $n \geq 2$ and N_1 prime to p. We will show that already over $\mathbf{Z}[1/N_1]$, the moduli problem [N-Isog] is not normal. The moduli problem $[N_1\text{-Isog}]$ is finite etale over $(\mathrm{Ell}/\mathbf{Z}[1/N_1])$, so it is equivalent to show that $[p^n\text{-Isog}]$ is not normal.

To see this, first look at $[p^n\text{-Isog}]\otimes\mathbf{Z}[1/p]$. Any subgroup of $(\mathbf{Z}/p^n\mathbf{Z})^2$ of order p^n contains a maximal subgroup of the form $(\mathbf{Z}/p^a\mathbf{Z})^2$,

modulo which it is cyclic. Therefore over any connected $\mathbf{Z}[1/p]$-scheme S, any p^n isogeny of elliptic curves over S has a unique factorization

$$E \xrightarrow{p^a} E \xrightarrow{\pi} E'$$

where $n = 2a+b$ and where π is a cyclic p^b-isogeny. Modularly, this means that over $\mathbf{Z}[1/p]$, we have a decomposition of moduli problems

$$[p^n\text{-Isog}] \otimes \mathbf{Z}[1/p] \xrightarrow{\sim} \coprod_{2a+b=n} [\Gamma_0(p^b)] \otimes \mathbf{Z}[1/p].$$

If $[p^n\text{-Isog}]$ were normal, it would be the normalization of (Ell) in $[p^n\text{-Isog}] \otimes \mathbf{Z}[1/p]$, i.e., for any representable etale moduli problem $\mathcal{S}$, the scheme $\mathcal{M}(\mathcal{S}, [p^n\text{-Isog}])$ would be the normalization of $\mathcal{M}(\mathcal{S})$ in $\mathcal{M}(\mathcal{S}, [p^n\text{-Isog}]) \otimes \mathbf{Z}[1/p]$, because it would be the unique normal scheme finite over $\mathcal{M}(\mathcal{S})$ which outside of p coincides with $\mathcal{M}(\mathcal{S}, [p^n\text{-Isog}])$.

So if $[p^n\text{-Isog}]$ were normal, we could deduce from our decomposition over $\mathbf{Z}[1/p]$ a decomposition

$$[p^n\text{-Isog}] \xrightarrow{\sim} \coprod_{2a+b=n} [\Gamma_0(p^b)].$$

That such a decomposition does not exist is obvious from the fact that for E_0/k a supersingular elliptic curve over a field, we have

$$[p^n\text{-Isog}](E_0/k) = \text{a single element } (\text{Ker } F^n)$$

while for each $b = n, n-2, \cdots$ we also have

$$[\Gamma_0(p^b)](E_0/k) = \text{a single element } (\text{Ker } F^b)\ !$$ Q.E.D.

REMARK 6.8.9. Indeed, the above proof shows that the *normalization* of $[p^n\text{-Isog}]$ *is* the disjoint union

$$\coprod_{2a+b=n} [\Gamma_0(p^b)],$$

and hence that $[p^n\text{-Isog}]$ is not geometrically unibranch at any supersingular point in characteristic p, as soon as $n \geq 2$.

Chapter 7

QUOTIENTS BY FINITE GROUPS

(7.1) *The general situation*

(7.1.1) Let R be a ring, G a finite group, and $\mathcal{P}$ a moduli problem on (Ell/R). We say that G operates on $\mathcal{P}$ if for every R-scheme S, and every elliptic curve E/S, the group G operates on the set $\mathcal{P}(E/S)$ in such a way that for every morphism in (Ell/R), viewed as a Cartesian diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\alpha} & E \\ \downarrow & & \downarrow \\ S_1 & \xrightarrow{f} & S \end{array},$$

the obvious diagram of actions below commutes:

7.1.1.1
$$\begin{array}{ccc} G \times \mathcal{P}(E/S) & \xrightarrow{\text{action}} & \mathcal{P}(E/S) \\ \downarrow{\scriptstyle \mathrm{id} \times (\alpha, f)^*} & & \downarrow{\scriptstyle (\alpha, f)^*} \\ G \times \mathcal{P}(E_1/S_1) & \xrightarrow{\text{action}} & \mathcal{P}(E_1/S_1). \end{array}$$

If $\mathcal{P}$ is relatively representable, then for every E/S, the group G acts on the S-scheme $\mathcal{P}_{E/S}$.

(7.1.2) Let $\mathcal{P}$ and $\mathcal{P}'$ be two relatively representable moduli problems on which G operates, and let

$$\mathcal{P} \to \mathcal{P}'$$

be a G-equivariant morphism of moduli problems on (Ell/R); for every $E/S/R$, we are given a G-equivariant map of G-sets

$$\mathcal{P}(E/S) \to \mathcal{P}'(E/S)$$

compatible with morphisms in (Ell/R). We say that $\mathcal{P}'$ is "the" quotient of $\mathcal{P}$ by G, and write $\mathcal{P}' = \mathcal{P}/G$, if the following two conditions hold:

(Q1): G operates trivially on $\mathcal{P}'$.

(Q2): For every representable moduli problem $\mathcal{S}$ on (Ell/R) which is etale over (Ell/R), the quotient scheme $\mathcal{M}(\mathcal{S}, \mathcal{P})/G$ exists, and it maps isomorphically to $\mathcal{M}(\mathcal{S}, \mathcal{P}')$. [Equivalently: for every modular family of elliptic curves $E/S/R$, the quotient scheme $(\mathcal{P}_{E/S})/G$ exists, and maps isomorphically to $(\mathcal{P}')_{E/S}$.]

THEOREM 7.1.3. *Let $\mathcal{P}$ be relatively representable and affine over* (Ell/R), *and* G *a finite group acting on* $\mathcal{P}$. *Then*

(1) *The quotient $\mathcal{P}/G$ exists as a relatively representable moduli problem, affine over* (Ell/R). *For any relatively representable $\mathcal{P}'$, with trivial* G*-action, any* G*-equivariant map $\mathcal{P} \to \mathcal{P}'$ factors uniquely through the projection $\mathcal{P} \to \mathcal{P}/G$, so that $\mathcal{P}/G$ represents the covariant functor on the category of all relatively representable moduli problems with trivial* G*-action defined by*

$$\mathcal{P}' \mapsto \mathrm{Hom}_{G\text{-equiv}}(\mathcal{P}, \mathcal{P}').$$

(2) *If* G *operates freely on* $\mathcal{P}$, *in the sense that for every* $E/S/R$, G *operates freely on the set* $\mathcal{P}(E/S)$, *then* $\mathcal{P}$ *is an etale* G*-torsor over* $\mathcal{P}/G$; *for every* $E/S/R$, G *operates freely on the* S*-scheme* $\mathcal{P}_{E/S}$, $\mathcal{P}_{E/S}$ *is an etale* G*-torsor over* $(\mathcal{P}/G)_{E/S}$, *and* $(\mathcal{P}_{E/S})/G \xrightarrow{\sim} (\mathcal{P}/G)_{E/S}$.

(3) *For any* $E/S/R$, *the quotient scheme* $\mathcal{P}_{E/S}/G$ *exists, and there is a natural* S*-morphism*

$$(\mathcal{P}_{E/S})/G \to (\mathcal{P}/G)_{E/S},$$

which is bijective on geometric points. It is an isomorphism if any of the following conditions hold:

a) E/S *is (as representable moduli problem) flat over* (Ell/R);

b) *the order of* G *is invertible on* S;

c) G *operates freely on* $\mathcal{P}$.

(4) *The morphism* $\mathcal{P} \to \mathcal{P}/G$ *is finite.*

(5) *If* $\mathcal{P}$ *is normal, so is* $\mathcal{P}/G$.

(6) *If* $\mathcal{P}$ *is finite over* (Ell/R), *and* R *is noetherian, then* $\mathcal{P}/G$ *is finite over* (Ell/R).

Construction-proof. Let us denote by (Sch/R-Sch) the category whose objects are R-morphisms of R-schemes

$$\begin{array}{c} X \\ \downarrow \\ S \end{array} \qquad S \text{ an R-scheme}$$

and whose morphisms are cartesian squares of R-schemes

$$\begin{array}{ccc} X_1 & \xrightarrow{a} & X \\ \downarrow & & \downarrow \\ S_1 & \xrightarrow{f} & S \end{array}.$$

We denote by

$$\text{Base} : (\text{Sch/R-Sch}) \to (\text{R-Sch})$$

the functor

$$\begin{array}{c} X \\ \downarrow \\ S \end{array} \longmapsto S.$$

When no confusion is possible, we also denote by

$$\text{Base} : (\text{Ell/R}) \to (\text{R-Sch}),$$

the analogous functor

$$\begin{array}{c} E \\ \downarrow \\ S \end{array} \longmapsto S.$$

A covariant functor

$$\mathcal{F} : (\text{Ell/R}) \to (\text{Sch/R-Sch})$$

is called base-preserving if the diagram

$$\begin{array}{ccc} (\text{Ell/R}) & \xrightarrow{\mathcal{F}} & (\text{Sch/R-Sch}) \\ & {\scriptstyle \text{Base}} \searrow \quad \swarrow {\scriptstyle \text{Base}} & \\ & (\text{R-Sch}) & \end{array}$$

is commutative.

Given a relatively representable moduli problem $\mathcal{P}$ on (Ell/R), we denote by $\mathcal{P}^{\text{Sch}}$ the base-preserving functor

$$\mathcal{P}^{\text{Sch}} : (\text{Ell/R}) \to (\text{Sch/R-Sch})$$

defined by

$$\begin{array}{ccc} E & & \mathcal{P}_{E/S} \\ \downarrow & \longmapsto & \downarrow \\ S & & S\ . \end{array}$$

The construction

$$\mathcal{P} \mapsto \mathcal{P}^{Sch}$$

defines an equivalence of categories

$$\begin{pmatrix} \text{relatively repre-} \\ \text{sentable problems} \\ \text{on (Ell/R)} \end{pmatrix} \xrightarrow{\sim} \begin{pmatrix} \text{base-preserving} \\ \text{functors from} \\ \text{(Ell/R) to (Sch/R-Sch)} \end{pmatrix}.$$

The inverse construction associates to a base-preserving functor $\mathcal{F}$ the relatively representable moduli problem $\mathcal{P}$ defined by

$$\mathcal{P}(E/S) = \mathrm{Hom}_{S\text{-Sch}}(S, \mathcal{F}_{E/S}),$$

so that

$$\mathcal{P}_{E/S} = \mathcal{F}_{E/S}.$$

We will make use of this equivalence to discuss the case of a finite group G acting freely on a relatively representable moduli problem $\mathcal{P}$ which is affine over (Ell/R). In this case, G operates freely and S-linearly on the affine S-scheme $\mathcal{P}_{E/S}$, for every $E/S/R$. By [De-Ga III, §2,6.1], we know that if a finite group G operates freely and S-linearly on an affine S-scheme X, then the quotient X/G exists, X is a finite etale G-torsor over X/G, and the formation of X/G commutes with arbitrary base-change $S' \to S$. Therefore the construction

$$\begin{array}{ccc} E & & (\mathcal{P}_{E/S})/G \\ \downarrow & \longmapsto & \downarrow \\ S & & S \end{array}$$

defines a base-preserving functor

$$\mathcal{P}^{Sch}/G : (Ell/R) \to (Sch/R\text{-}Sch),$$

whose associated relatively representable moduli problem we define to be $\mathcal{P}/G$, so that

$$(\mathcal{P}/G)^{Sch} = \mathcal{P}^{Sch}/G.$$

It is clear that this $\mathcal{P}/G$ does indeed have the universal property required in (1) of the theorem, and that (2) of the theorem holds.

We now consider the general case, when G is no longer assumed to act freely on $\mathcal{P}$. The problem of constructing $\mathcal{P}/G$ satisfying (1) is clearly Zariski local on R, so we may assume that an odd prime ℓ is invertible in R. Consider the simultaneous problem $([\Gamma(\ell)], \mathcal{P})$. It is representable because it maps to the representable problem $[\Gamma(\ell)]$, the product group $GL(2, \mathbf{F}_\ell) \times G$ operates on it, and the first factor $GL(2, \mathbf{F}_\ell)$ operates freely on it (because $GL(2, \mathbf{F}_\ell)$ operates freely on $[\Gamma(\ell)]$ over any ring R in which ℓ invertible, cf. (3.7.2)).

By the above discussion of the quotient by a free action, we may recover $\mathcal{P}$ from the simultaneous problem $([\Gamma(\ell)], \mathcal{P})$ with its action of $GL(2, \mathbf{F}_\ell)$ by the rule

$$([\Gamma(\ell)], \mathcal{P})/GL(2, \mathbf{F}_\ell) \times 1 \xrightarrow{\sim} \mathcal{P}.$$

Therefore the construction

$$\mathcal{P} \mapsto ([\Gamma(\ell)], \mathcal{P}) \text{ with action of } GL(2, \mathbf{F}_\ell)$$

defines an equivalence of categories

$$\begin{array}{ccc} \text{relatively representable} \\ \text{moduli problems } \mathcal{P} \text{ on} \\ \text{(Ell/R)} \end{array} \xrightarrow{\sim} \begin{array}{l} \text{representable moduli} \\ \text{problems } \mathcal{S} \text{ on (Ell/R)} \\ \text{given with an action of} \\ GL(2, \mathbf{F}_\ell) \text{ and with a} \\ GL(2, \mathbf{F}_\ell)\text{-equivariant map} \\ \text{to } [\Gamma(\ell)] \otimes R. \end{array}$$

Passing to modular schemes defines an equivalence

representable moduli problems $\mathcal{S}$ on (Ell/R) given with an action of $GL(2, F_\ell)$ and with a $GL(2, F_\ell)$-equivariant-map to $[\Gamma(\ell)]\otimes R$.	$\xrightarrow{\sim}$	$\mathcal{M}(\Gamma(\ell))\otimes R$-schemes given with an action of $GL(2, F_\ell)$ covering its standard action on $\mathcal{M}(\Gamma(\ell))\otimes R$.

$$\mathcal{S} \mapsto \mathcal{M}(\mathcal{S}) .$$

By means of this last equivalence an action of a finite group G on a relatively representable $\mathcal{P}$ which is affine over (Ell/R) corresponds to an $\mathcal{M}(\Gamma(\ell))\otimes R$-linear action of G on an affine $\mathcal{M}(\Gamma(\ell))\otimes R$-scheme $\mathcal{M}(\mathcal{S})$ which commutes with the given action of $GL(2, F_\ell)$ on $\mathcal{M}(\mathcal{S})$. Viewed in this way, it is clear that the quotient of $\mathcal{P}$ by G exists and satisfies the required universal property; it corresponds under this equivalence to the quotient $\mathcal{M}(\mathcal{S})/G$ with its induced action of $GL(2, F_\ell)$ and its $GL(2, F_\ell)$-equivariant map to $\mathcal{M}(\Gamma(\ell))\otimes R$:

$$\begin{array}{c} \mathcal{M}(\mathcal{S}) \\ \downarrow \\ \mathcal{M}(\mathcal{S})/G \\ \downarrow \\ \mathcal{M}(\Gamma(\ell))\otimes R . \end{array}$$

This concludes the proof of parts (1) and (2) of the theorem.

"Concretely", for any representable problem $\mathcal{S}$ on (Ell/R), the $\mathcal{M}(\mathcal{S})$-scheme $\mathcal{M}(\mathcal{S}, \mathcal{P}/G)$ is constructed in three steps:

(a) $\mathcal{M}(\mathcal{S}, \mathcal{P}/G) = \mathcal{M}(\mathcal{S}, \Gamma(\ell), \mathcal{P}/G)\big/GL(2, F_\ell)$

(b) $\mathcal{M}(\mathcal{S}, \Gamma(\ell), \mathcal{P}/G) = \mathcal{M}(\mathcal{S}, \Gamma(\ell)) \underset{\mathcal{M}(\Gamma(\ell))}{\times} \mathcal{M}(\Gamma(\ell), \mathcal{P}/G)$

(c) $\mathcal{M}(\Gamma(\ell), \mathcal{P}/G) = \mathcal{M}(\Gamma(\ell), \mathcal{P})\big/G .$

Thus all in all we have

$$\mathcal{M}(\mathcal{S}, \mathcal{P}/G) = \Big(\mathcal{M}(\mathcal{S}, \Gamma(\ell)) \underset{\mathcal{M}(\Gamma(\ell))}{\times} (\mathcal{M}(\Gamma(\ell), \mathcal{P})/G)\Big)\Big/GL(2, F_\ell) ,$$

while computing $\mathcal{M}(\mathcal{S}, \mathcal{P})$ this way leads to

$$\mathcal{M}(\mathcal{S}, \mathcal{P}) = \Big(\mathcal{M}(\mathcal{S}, \Gamma(\ell)) \underset{\mathcal{M}(\Gamma(\ell))}{\times} \mathcal{M}(\Gamma(\ell), \mathcal{P}))\Big)\Big/GL(2, F_\ell) ,$$

and so

$$\begin{aligned} \mathcal{M}(\mathcal{S}, \mathcal{P})/G &= \Big(\mathcal{M}(\mathcal{S}, \Gamma(\ell)) \underset{\mathcal{M}(\Gamma(\ell))}{\times} \mathcal{M}(\Gamma(\ell), \mathcal{P})\Big)\Big/GL(2, F_\ell)\times G \\ &= \Big(\Big(\mathcal{M}(\mathcal{S}, \Gamma(\ell)) \underset{\mathcal{M}(\Gamma(\ell))}{\times} \mathcal{M}(\Gamma(\ell), \mathcal{P})\Big)\Big/G\Big)\Big/GL(2, F_\ell) . \end{aligned}$$

The canonical morphism from $\mathcal{M}(\mathcal{S}, \mathcal{P})/G$ to $\mathcal{M}(\mathcal{S}, \mathcal{P}/G)$ is just the one deduced from passage to $GL(2, F_\ell)$-invariants from the morphism

$$\Big(\mathcal{M}(\mathcal{S}, \Gamma(\ell)) \underset{\mathcal{M}(\Gamma(\ell))}{\times} \mathcal{M}(\Gamma(\ell), \mathcal{P})\Big)\Big/G \to \mathcal{M}(\mathcal{S}, \Gamma(\ell)) \underset{\mathcal{M}(\Gamma(\ell))}{\times} (\mathcal{M}(\Gamma(\ell), \mathcal{P})/G) .$$

The question of when this morphism is an isomorphism, or a bijection on geometric points, is the question of the extent to which formation of rings of invariants commutes with extension of scalars.

The results of (3) follow immediately from the standard facts about this question, which are given in (A.7). In the same vein, (4), (5), and (6) are simply translations of the following facts:

for (4): take any modular E/S with S affine, $S = \mathrm{Spec}(B)$; then $\mathcal{P}_{E/S}$ is $\mathrm{Spec}(A)$ for some B-algebra A of finite presentation, upon which G acts B-linearly. Therefore A is finitely generated as an A^G-algebra. Visibly every element a of A is integral over A^G, being a root of the A^G-polynomial

$$\prod_g (T - g(a)) .$$

Therefore A is finite as an A^G-module.

for (5): This says A^G is normal if A is.

for (6): If A is a finite B-module, and if B is noetherian, then $A^G \subset A$ is a sub-B-module, so also finite over B. Q.E.D.

REMARK 7.1.4. If $R \to R'$ is a ring homomorphism, then for $\mathcal{P}$ and G as in the theorem there is a natural morphism

$$(\mathcal{P} \underset{R}{\otimes} R')/G \to (\mathcal{P}/G) \underset{R}{\otimes} R'$$

of moduli problems on (Ell/R'), which is an isomorphism if $R \to R'$ is flat, or if the order of G is invertible in R', or if G acts freely on $\mathcal{P}$. It is always surjective and radicial.

COROLLARY 7.1.5. *Suppose that* R *is noetherian. Let* $\mathfrak{p}$ *be a prime ideal of* R, k_0 *its residue field,* k *a separable closure of* k_0, *and* $\hat{R}$ *the completion of the strict henselization of the local ring at* $\mathfrak{p}$. *For any elliptic curve* E/k, *let* $E/\hat{R}[[T]]$ *be its universal formal deformation (to artin local* $\hat{R}$*-algebras with residue field* k*). If* $\mathcal{P}$ *is relatively representable and affine over* (Ell/R), *and if* G *is a finite group acting on* $\mathcal{P}$, *then we have a canonical isomorphism of* $\hat{R}[[T]]$*-schemes*

$$(\mathcal{P}_{E/\hat{R}[[T]]})/G \xrightarrow{\sim} (\mathcal{P}/G)_{E/\hat{R}[[T]]}.$$

Proof. Choose an odd prime $\ell \neq \mathrm{char}(k)$, which we may assume invertible on R. Then the moduli problem $\mathcal{S} = [\Gamma(\ell)] \underset{\mathbf{Z}}{\otimes} R$ is finite etale over (Ell/R). Fix a $\Gamma(\ell)$-structure on E/k. It extends uniquely to a $\Gamma(\ell)$-structure on $E/\hat{R}[[T]]$, and with it we may view $\hat{R}[[T]]$ as the completion of the strict henselization of $\mathcal{M}(\mathcal{S})$ at the image of the point (E/k, its $\Gamma(\ell)$-structure). Consider the diagram of schemes over $\mathcal{M}(\mathcal{S})$

$$\begin{array}{ccc} \mathcal{M}(\mathcal{S}, \mathcal{P}) & \longrightarrow & \mathcal{M}(\mathcal{S}, \mathcal{P}/G) = \mathcal{M}(\mathcal{S}, \mathcal{P})/G \\ & \searrow \quad \swarrow & \\ & \mathcal{M}(\mathcal{S}) . & \end{array}$$

Because $\hat{R}[[T]]$ is flat over $\mathcal{M}(\mathcal{S})$, we have

$$(\mathcal{M}(\mathcal{S}, \mathcal{P}) \underset{\mathcal{M}(\mathcal{S})}{\times} \hat{R}[[T]])/G \xrightarrow{\sim} (\mathcal{M}(\mathcal{S}, \mathcal{P})/G) \underset{\mathcal{M}(\mathcal{S})}{\times} \hat{R}[[T]],$$

which is none other than the desired isomorphism

$$(\mathcal{P}_{E/\hat{R}[[T]]})/G \xrightarrow{\sim} (\mathcal{P}/G)_{E/\hat{R}[[T]]}. \qquad \text{Q.E.D.}$$

(7.2) *A descent situation*

(7.2.1) Let $\mathcal{P}$ and $\mathcal{P}'$ be relatively representable and affine over (Ell/R). Suppose that a finite group G acts on both $\mathcal{P}$ and $\mathcal{P}'$, and that we are given a G-equivariant morphism

$$\mathcal{P} \to \mathcal{P}'.$$

PROPOSITION 7.2.2. *If* G *operates freely on* $\mathcal{P}'$, *then the natural map*

$$\mathcal{P}/G \to \mathcal{P}'/G$$

sits in a cartesian diagram

$$\begin{array}{ccc} \mathcal{P} & \longrightarrow & \mathcal{P}/G \\ \downarrow & & \downarrow \\ \mathcal{P}' & \longrightarrow & \mathcal{P}'/G , \end{array}$$

i.e., for every E/S *the diagram of* S*-schemes*

$$\begin{array}{ccc} \mathcal{P}_{E/S} & \longrightarrow & (\mathcal{P}/G)_{E/S} \\ \downarrow & & \downarrow \\ \mathcal{P}'_{E/S} & \longrightarrow & (\mathcal{P}'/G)_{E/S} \end{array}$$

is cartesian.

Proof. Because G operates freely on $\mathcal{P}'$, we know that for every E/S, $\mathcal{P}'_{E/S}$ is an etale G-torsor over $(\mathcal{P}'/G)_{E/S} = (\mathcal{P}'_{E/S})/G$. By etale descent, it is the same to give a $(\mathcal{P}'/G)_{E/S}$-scheme Z_2 as it is to give a $\mathcal{P}'_{E/S}$-scheme Z_1 together with a lifting of the action of G, the two related by

$$Z_2 = Z_1/G, \quad Z_1 = \left(Z_2 \underset{(\mathcal{P}'/G)_{E/S}}{\times} (\mathcal{P}')_{E/S}\right).$$

Take for Z_1 the scheme $\mathcal{P}_{E/S}$. The associated Z_2 which fits into the cartesian diagram is $Z_1/G = (\mathcal{P}_{E/S})/G$. But because G acts freely on $\mathcal{P}'$ it acts all the more freely on $\mathcal{P}$, so we do indeed have $Z_2 = (\mathcal{P}/G)_{E/S}$. by (7.1.3, 3(c)). Q.E.D.

(7.3) *Quotients of product problems*

PROPOSITION 7.3.1. *Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be two relatively representable moduli problems affine over* (Ell/R). *Suppose that finite groups G_1 and G_2 operate on $\mathcal{P}_1$ and $\mathcal{P}_2$ respectively, that $\mathcal{P}_1$ is flat over* (Ell/R), *and that $\mathcal{P}_2/G_2$ is flat over* (Ell/R).

Then we have a canonical isomorphism

$$(\mathcal{P}_1, \mathcal{P}_2)/(G_1 \times G_2) \xrightarrow{\sim} (\mathcal{P}_1/G_1, \mathcal{P}_2/G_2).$$

Proof. Let $\mathcal{S}$ be a representable problem, etale over (Ell/R). By definition of quotients we have

$$\begin{aligned}\mathcal{M}(\mathcal{S}, (\mathcal{P}_1, \mathcal{P}_2)/G_1 \times G_2) &= \mathcal{M}(\mathcal{S}, \mathcal{P}_1, \mathcal{P}_2)/G_1 \times G_2 \\ &= (\mathcal{M}(\mathcal{S}, \mathcal{P}_1) \underset{\mathcal{M}(\mathcal{S})}{\times} \mathcal{M}(\mathcal{S}, \mathcal{P}_2))/G_1 \times G_2,\end{aligned}$$

while

$$\begin{aligned}\mathcal{M}(\mathcal{S}, \mathcal{P}_1/G_1, \mathcal{P}_2/G_2) &= \mathcal{M}(\mathcal{S}, \mathcal{P}_1/G_1) \underset{\mathcal{M}(\mathcal{S})}{\times} \mathcal{M}(\mathcal{S}, \mathcal{P}_2/G_2) \\ &= (\mathcal{M}(\mathcal{S}, \mathcal{P}_1)/G_1) \underset{\mathcal{M}(\mathcal{S})}{\times} (\mathcal{M}(\mathcal{S}, \mathcal{P}_2)/G_2).\end{aligned}$$

If Spec(B) is an affine open of $\mathcal{M}(\mathcal{S})$, and if Spec(A_1) and Spec(A_2) are its inverse images in $\mathcal{M}(\mathcal{S}, \mathcal{P}_1)$ and $\mathcal{M}(\mathcal{S}, \mathcal{P}_2)$ respectively, then the natural map $(\mathcal{P}_1, \mathcal{P}_2)/G_1 \times G_2 \to (\mathcal{P}_1/G_1, \mathcal{P}_2/G_2)$ is given on affine rings by

$$(A_1)^{G_1} \otimes_B (A_2)^{G_2} \to (A_1 \otimes_B A_2)^{G_1 \times G_2}.$$

By hypothesis, A_1 and $(A_2)^{G_2}$ are both flat over B. Therefore

$$\begin{aligned}(A_1 \underset{B}{\otimes} A_2)^{G_1 \times G_2} &= ((A_1 \underset{B}{\otimes} A_2)^{G_2})^{G_1} \\ &= (A_1 \underset{B}{\otimes} (A_2)^{G_2})^{G_1} \\ &= (A_1)^{G_1} \underset{B}{\otimes} (A_2)^{G_2}. \quad \text{Q.E.D.}\end{aligned}$$

(7.4) *Applications to the four basic moduli problems*

(7.4.1) Let $N \geq 1$ be an integer. The group $GL(2, \mathbf{Z}/N\mathbf{Z})$ operates on the moduli problem $[\Gamma(N)]$, through its right action on Drinfeld bases: $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbf{Z}/N\mathbf{Z})$ acts by

$$(P, Q) \mapsto (P, Q)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (aP + cQ, bP + dQ).$$

This action is well defined, for it leaves unchanged the Cartier divisor

$$\sum_{n,m \bmod N} [nP + mQ].$$

The group $(\mathbf{Z}/N\mathbf{Z})^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$ operates on the moduli problem [bal. $\Gamma_1(N)$], through its action on the generators: an element (a, b) of this group acts as

$$(P; E \underset{\pi^t}{\overset{\pi}{\rightleftarrows}} E'; P') \mapsto (aP; E \underset{\pi^t}{\overset{\pi}{\rightleftarrows}} E'; bP').$$

The group $(\mathbf{Z}/N\mathbf{Z})^\times$ operates on the moduli problem $[\Gamma_1(N)]$ through its action on the given generator; an element a acts as

$$(E, P) \mapsto (E, aP) .$$

THEOREM 7.4.2. *Let $N \geq 1$ be an integer. Then*

(1) *For any divisor d of N, the natural map*

$$[\Gamma(N)] \to [\Gamma(d)]$$
$$(P, Q) \mapsto ((N/d)P, (N/d)Q)$$

identifies $[\Gamma(d)]$ with the quotient of $[\Gamma(N)]$ by the principal congruence subgroup of $GL(2, \mathbf{Z}/N\mathbf{Z})$ consisting of those elements $\equiv$ id mod d.

(2) *The natural map*

$$[\Gamma(N)] \longrightarrow [\text{bal. } \Gamma_1(N)]$$
$$(P, Q) \longmapsto (P, Q \bmod P)$$

identifies [bal. $\Gamma_1(N)$] with the quotient of $[\Gamma(N)]$ by the unipotent subgroup $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ of $GL(2, \mathbf{Z}/N\mathbf{Z})$.

(3) *The natural map*

$$[\Gamma(N)] \longrightarrow [\Gamma_1(N)]$$
$$(P, Q) \longmapsto P$$

identifies $[\Gamma_1(N)]$ with the quotient of $[\Gamma(N)]$ by the "semi-Borel" subgroup $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$ of $GL(2, \mathbf{Z}/N\mathbf{Z})$.

(4) *The natural map*

$$[\Gamma(N)] \longrightarrow [\Gamma_0(N)]$$
$$(P, Q) \longmapsto \text{subgroup "generated" by } P$$

identifies $[\Gamma_0(N)]$ with the quotient of $[\Gamma(N)]$ by the Borel subgroup $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ of $GL(2, \mathbf{Z}/N\mathbf{Z})$.

(5) *The natural map*

$$[\text{bal. } \Gamma_1(N)] \longrightarrow [\Gamma_1(N)]$$
$$\left(P ; E \underset{\pi^t}{\overset{\pi}{\rightleftarrows}} E' ; P'\right) \longmapsto (E, P)$$

identifies $[\Gamma_1(N)]$ as the quotient of [bal. $\Gamma_1(N)$] by the subgroup $1 \times (\mathbf{Z}/N\mathbf{Z})^\times$ of $(\mathbf{Z}/N\mathbf{Z})^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$.

(6) *The natural map*

$$[\text{bal. } \Gamma_1(N)] \longrightarrow [\Gamma_0(N)]$$
$$\left(P ; E \underset{\pi^t}{\overset{\pi}{\rightleftarrows}} E' ; P'\right) \longmapsto (E, \operatorname{Ker}(\pi))$$

identifies $[\Gamma_0(N)]$ with the quotient of [bal. $\Gamma_1(N)$] by $(\mathbf{Z}/N\mathbf{Z})^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$.

(7) *The natural map*

$$[\Gamma_1(N)] \to [\Gamma_0(N)]$$
$$(E, P) \mapsto (E, \text{subgroup generated by } P)$$

identifies $[\Gamma_0(N)]$ with the quotient of $[\Gamma_1(N)]$ by $(\mathbf{Z}/N\mathbf{Z})^\times$.

Proof. We will prove (1). The other proofs are entirely analogous, and are left to the reader. Let G denote the mod d congruence subgroup of $GL(2, \mathbf{Z}/N\mathbf{Z})$. The given morphism

$$[\Gamma(N)] \to [\Gamma(d)]$$

is G-equivariant, with G acting trivially on $[\Gamma(d)]$. We must show that for any representable moduli problem $\mathcal{S}$ which is etale over (Ell), the induced map of $\mathcal{M}(\mathcal{S})$-schemes

$$\mathcal{M}(\mathcal{S}, \Gamma(N))/G \to \mathcal{M}(\mathcal{S}, \Gamma(d))$$

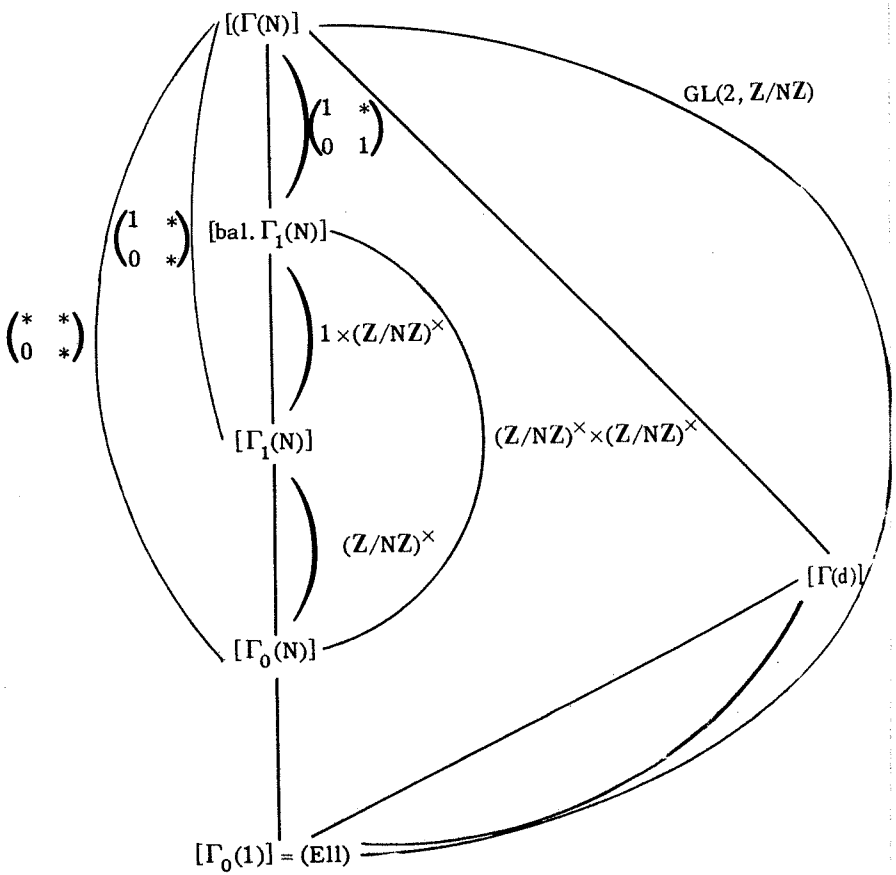
is an isomorphism. This is obviously the case if N is invertible, and both sides are normal schemes finite over $\mathcal{M}(\mathcal{S})$. Therefore they and the

map between them are obtained from the isomorphism of finite etale $\mathfrak{M}(\mathcal{S}) \otimes \mathbf{Z}[1/N]$-schemes

$$\begin{array}{ccc} (\mathfrak{M}(\mathcal{S}, \Gamma(N)) \otimes \mathbf{Z}[1/N])/G & \xrightarrow{\sim} & \mathfrak{M}(\mathcal{S}, \Gamma(d)) \otimes \mathbf{Z}[1/N] \\ & \searrow \quad \swarrow & \\ & \mathfrak{M}(\mathcal{S}) \otimes \mathbf{Z}[1/N] & \end{array}$$

by normalizing $\mathfrak{M}(\mathcal{S})$. Q.E.D.

(7.4.3) *Summarizing diagram*



(7.5) *Axiomatics*

AXIOMATIC REGULARITY OF QUOTIENTS THEOREM 7.5.1. *Let $\mathcal{P}$ be a relatively representable moduli problem on* (Ell), *which satisfies axioms Reg. 1, Reg. 2, Reg. 3, Reg. 4A, Reg. 4B of 5.1.1 with respect to some prime* p. *Let* G *be a finite group which operates on $\mathcal{P}$. Suppose that this* G*-action satisfies the following three axioms*:

(G-1) G *acts freely on* $\mathcal{P} \otimes \mathbf{Z}[1/p]$.

(G-2) *The action of* G *on* $\mathcal{P}$ *depends only upon the underlying* p*-divisible group, in the sense that for any two elliptic curves over a common base, say* E/S *and* E′/S, *and any* S*-isomorphism of their* p*-divisible groups*

$$E[p^\infty] \xrightarrow{\sim} E'[p^\infty],$$

there exists an isomorphism (cf. Reg. 3) of S*-schemes*

$$\mathcal{P}_{E'/S} \xrightarrow{\sim} \mathcal{P}_{E/S}$$

which is G*-equivariant.*

(G-3) *Let* k *be any algebraically closed field of characteristic* p, E_0/k *any supersingular elliptic curve,* E/W[[T]] *its universal formal deformation, and* A *the complete local (Reg. 4A) ring such that* $\mathcal{P}_{E/W[[T]]} = \mathrm{Spec}(A)$. *Then* A *is a finite module over* A^G, *generated by* #G *elements.*

Then

(1) *The quotient* $\mathcal{P}/G$ *is finite and flat over* (Ell) *of constant rank* ≥ 1, *and regular (necessarily of dimension two).*

(2) *The morphism of moduli problems over* (Ell)

$$\mathcal{P} \to \mathcal{P}/G$$

is finite and flat of degree #G. *Outside of* p, *this morphism makes* $\mathcal{P}$ *into an etale* G*-torsor.*

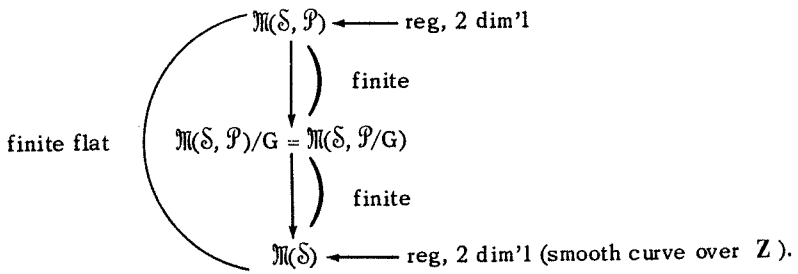
(3) *The "complete local ring of* $\mathcal{P}/G$ *at a supersingular* E_0/k *" is given by* A^G, *i.e., we have* $\mathrm{Spec}(A^G) = (\mathcal{P}/G)_{E/W[[T]]}$ *for* $E/W[[T]]$ *as in axiom* G-3.

(4) *For any elliptic curve* E/k *with* k *the algebraic closure of a finite field, and universal formal deformation* $E/W[[T]]$, *we have an isomorphism of* $W[[T]]$*-schemes*

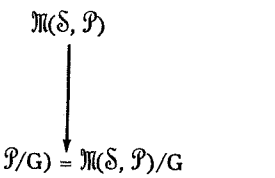
$$(\mathcal{P}_{E/W[[T]]})/G \xrightarrow{\sim} (\mathcal{P}/G)_{E/W[[T]]}.$$

Proof. We first explain why it suffices to prove (1). Given (1), it follows from (5.2.1) that both $\mathcal{P}$ and $\mathcal{P}/G$ are regular two-dimensional, finite and flat over (Ell). Then (2) results from [A-K 1, V, 3.8], combined with 7.1.3, (2) applied to $\mathcal{P} \otimes_{\mathbf{Z}} \mathbf{Z}[1/p]$ over the ring $R = \mathbf{Z}[1/p]$. Conclusion (3) is a special case of conclusion (4), itself a special case of (7.1.5).

We now turn to the proof of (1). Pick any odd prime $\ell \neq p$, and denote by $\mathcal{S}$ the naive full level ℓ moduli problem. We must show that $\mathcal{M}(\mathcal{S}, \mathcal{P}/G)$ is a regular two-dimensional scheme, which is finite and flat over $\mathcal{M}(\mathcal{S})$. By definition of $\mathcal{P}/G$, we have $\mathcal{M}(\mathcal{S}, \mathcal{P}/G) = \mathcal{M}(\mathcal{S}, \mathcal{P})/G$. Consider the diagram



It suffices to show that $\mathcal{M}(\mathcal{S}, \mathcal{P})/G$ is regular two-dimensional, for then being finite over $\mathcal{M}(\mathcal{S})$ it will automatically be finite flat over $\mathcal{M}(\mathcal{S})$ —once again, a finite map between regular schemes of the same dimension is necessarily flat. Because $\mathcal{M}(\mathcal{S}, \mathcal{P})$ is itself regular two-dimensional, it suffices to show that the finite morphism



is finite and flat (by [A-K 1, VII, 4.8]).

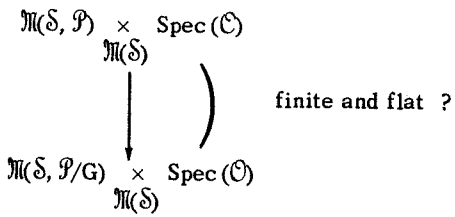
Consider the set $\mathcal{U} \subset \mathcal{M}(\mathcal{S})$ of points x such that for any $y \in \mathcal{M}(\mathcal{S}, \mathcal{P}/G)$ with $y \to x$, and any $z \in \mathcal{M}(\mathcal{S}, \mathcal{P})$ with $z \to y$, $\mathcal{M}(\mathcal{S}, \mathcal{P})$ is flat over $\mathcal{M}(\mathcal{S}, \mathcal{P}/G)$ at z. This set $\mathcal{U}$ is *open* in $\mathcal{M}(\mathcal{S})$, because its complement is the image by the finite map $\mathcal{M}(\mathcal{S}, \mathcal{P}) \to \mathcal{M}(\mathcal{S})$ of the set of points in $\mathcal{M}(\mathcal{S}, \mathcal{P})$ where $\mathcal{M}(\mathcal{S}, \mathcal{P}) \to \mathcal{M}(\mathcal{S}, \mathcal{P}/G)$ is not flat, and this is a closed set ([A-K, V, 5.5]). We know that $\mathcal{U}$ contains all of $\mathcal{M}(\mathcal{S}) \otimes \mathbf{Z}[1/p]$. So it suffices to show that $\mathcal{U}$ contains all closed points of $\mathcal{M}(\mathcal{S})$ in characteristic p.

Let x be a closed point of $\mathcal{M}(\mathcal{S})$ in characteristic p, corresponding to an elliptic curve E_0 over a finite field k_0, together with a level $\mathcal{S}$-structure.

Let us denote by $\mathcal{O}$ the *completion* of the strict henselization of the local ring of $\mathcal{M}(\mathcal{S})$ at x, with respect to some choice $k_0 \hookrightarrow k$ of algebraic closure of k_0.

Let E/k be $E_0 \otimes_{k_0} k$, and denote by $E/W(k)[[T]]$ the universal formal deformation of E/k. Then $\mathcal{O} \simeq W(k)[[T]]$, with $E/W(k)[[T]]$ induced from the universal curve over $\mathcal{M}(\mathcal{S})$ by the base change $\mathrm{Spec}(\mathcal{O}) \to \mathcal{M}(\mathcal{S})$.

We must show that after the base-change $\mathrm{Spec}(\mathcal{O}) \to \mathcal{M}(\mathcal{S})$, we have a finite flat map:



The source is by definition the scheme $\mathcal{P}_{E/W[[T]]}$, and the target is (using the flatness of $\mathrm{Spec}(\mathcal{O}) \to \mathcal{M}(\mathcal{S})$)

$$\mathcal{M}(\mathcal{S}, \mathcal{P}/G) \underset{\mathcal{M}(\mathcal{S})}{\times} \mathrm{Spec}(\mathcal{O}) = (\mathcal{M}(\mathcal{S}, \mathcal{P})/G) \underset{\mathcal{M}(\mathcal{S})}{\times} \mathrm{Spec}(\mathcal{O})$$

$$= (\mathcal{M}(\mathcal{S}, \mathcal{P}) \underset{\mathcal{M}(\mathcal{S})}{\times} \mathrm{Spec}(\mathcal{O}))\Big/G$$

$$= \left(\mathcal{P}_{E/W[[T]]}\right)\Big/G .$$

Thus we must show that

$$\mathcal{P}_{E/W[[T]]}$$

$$\downarrow$$

$$(\mathcal{P}_{E/W[[T]]})/G$$

is finite flat.

Because $\mathcal{P}$ satisfies Reg. 3, and the action of G on $\mathcal{P}$ satisfies G-2, it follows by Serre-Tate theory that this morphism of $W[[T]]$-schemes is, up to isomorphism, of only two possible types, depending on whether E/k is ordinary or supersingular. In particular, the question of whether it is finite flat depends only on whether E/k is ordinary or not.

Because $\mathcal{U}$ is open, and contains $\mathcal{M}(\mathcal{S}) \otimes Z[1/p]$, it suffices to show $\mathcal{U}$ contains all supersingular points in characteristic p. (Then it contains all nearby points, so some ordinary points, then all ordinary points.)

We now study the case of a supersingular E/k. In the notations of G-3, we must show that A is a *free* module over A^G. For this, we argue as follows.

The map $G \to \mathrm{Aut}(A)$ is injective, because A is flat over Z (being finite flat over $W[[T]]$) and, by G-1, G acts freely on $\mathrm{Spec}(A \otimes Z[1/p])$. Let K denote the fraction field of A. Then K^G is the fraction field of A^G (replace denominators by their norms). By galois theory, K is a $\#G$-dimensional vector space over K^G. Therefore if A is spanned over

A^G by $\#G$ elements, these elements must be linearly independent over K^G, whence A is a free module over A^G of rank $\#G$. Q.E.D.

In order to apply (7.5.1), we will need the following result (with $n=2$).

PROPOSITION 7.5.2. *Let A be a complete noetherian local ring which is regular of dimension n and whose residue field is perfect. Let G be a finite subgroup of $\mathrm{Aut}(A)$, such that every $g \in G$ acts trivially on the residue field of A. Suppose that A admits a regular system of parameters $(x_1, \cdots, x_{n-1}, y)$ such that for each $g \in G$ we have*

$$g(x_i) = x_i \quad \text{for} \quad i = 1, \cdots, n-1$$

$$g(y) \equiv y \times (\text{unit}) \qquad \mathrm{mod}\,(x_1, \cdots, x_{n-1}) .$$

Then

(1) *A is free over A^G, with basis $1, y, y^2, \cdots, (y)^{\#G-1}$.*

(2) *A^G is a regular local ring of dimension n.*

(3) *A set of parameters for A^G is $(x_1, \cdots, x_{n-1}, N(y))$ where $N(y)$ is the norm $\prod_g g(y)$.*

Proof. Clearly the element $N(y)$ satisfies the congruence

$$N(y) \equiv (y^{\#G})(\text{unit of } A) \ \mathrm{mod}\,(x_1, \cdots, x_{n-1}) ,$$

and clearly the elements $(x_1, \cdots, x_{n-1}, N(y))$ all lie in A^G.

We first claim that A is spanned over A^G by the $\#G$ elements

$$1, y, \cdots, y^{\#G-1} .$$

To prove this, it suffices by Nakayama to show that $A/\mathrm{max}(A^G) \cdot A$ is spanned over A^G by these elements. We have an obvious inclusion

$$\mathrm{max}(A^G) \supset (x_1, \cdots, x_{n-1}, N(y)) ,$$

and by our congruence on $N(y)$ we have

$$(x_1, \cdots, x_{n-1}, N(y))\,A = (x_1, \cdots, x_{n-1}, y^{\#G}) \cdot A\ .$$

Therefore it suffices to show that

$$A/(x_1, \cdots, x_{n-1}, y^{\#G})\,A$$

is spanned over A^G by the lower powers of y. Because A and A^G have the same residue field k, the Cohen ring $C(k)$ maps to A through A^G. Therefore it suffices if

$$A/(x_1, \cdots, x_{n-1}, y^{\#G})\,A$$

is spanned over $C(k)$ by the lower powers of y, and this is visibly the case, just because $\max(A) = (x_1, \cdots, x_{n-1}, y)$.

By considering the extension of fraction fields, we conclude that A is free over A^G on these elements, thus proving (1) and its consequence (2) (again by [A-K 1, VII, 4.8]). Now let $I \subset \max(A^G)$ be any ideal of A^G. Then A/IA is free of rank $\#G$ over A^G/I. Therefore $I = \max(A^G)$ if and only if A/IA has *length* $\leq \#G$. Applying this criterion to $I = (x_1, \cdots, x_{n-1}, N(y))$, we get (3). Q.E.D.

VARIANT 7.5.3. *Let A be a complete noetherian regular local ring of dimension n with perfect residue field, G a finite subgroup of $\mathrm{Aut}(A)$ of the form $G_1 \times \cdots \times G_n$. Suppose that every $g \in G$ acts trivially on the residue field of A, and that there exists a regular system of parameters $(x_1, \cdots, x_n)$ for A such that for each i, any element $g_i \in G_i$ satisfies*

$$\begin{cases} g_i(x_j) = x_j & \text{if} \quad j \neq i \\ g_i(x_i) = x_i \times (\text{unit})\ . \end{cases}$$

Then A^G is regular of dimension n, a set of parameters of A^G is $(N_{G_1}(x_1), \cdots, N_{G_n}(x_n))$, and A is free over A^G on the $\#G$ monomials $\prod x_i^{w_i}$ with $0 \leq w_i \leq \#G_i - 1$.

Proof. Straightforward adaptation of the proof of the preceding proposition. Q.E.D.

(7.6) *Applications to regularity*

We now list some cases to which the Axiomatic Regularity of Quotients Theorem 7.5.1 applies *via* this proposition.

THEOREM 7.6.1.

(1) *For any prime power p^n with $n \geq 1$, and any subgroup G of the "semi-Borel"*

$$G \subset \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \subset GL(2, \mathbf{Z}/p^n\mathbf{Z})$$

or any product subgroup $G = \begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$ of the Cartan $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \subset GL(2, \mathbf{Z}/p^n\mathbf{Z})$ the quotient $[\Gamma(p^n)]/G$ is regular two-dimensional, finite and flat over (Ell) *and under $[\Gamma(p^n)]$.*

(2) *For any prime power p^n with $n \geq 1$, and any two subgroups $G, H \subset (\mathbf{Z}/p^n\mathbf{Z})^\times$, the quotients*

$$[\text{bal. } \Gamma_1(p^n)]\Big/(G \times H)$$

$$[\Gamma_1(p^n)]/G$$

are regular two-dimensional, finite and flat over (Ell) *and under* $[\text{bal. } \Gamma_1(p^n)]$ (*resp.* $[\Gamma_1(p^n)]$).

Proof. Simply apply the proposition (7.5.1) to G, and its variation (7.5.3) to $G_1 \times G_2$ and to $G \times H$. Q.E.D.

(7.7) *Summary of parameters at supersingular points (notations as in (5.4))*

moduli problem	basic data	Parameters for A
$[\Gamma(p^n)]$	(P, Q)	$X(P), X(Q)$
$[\Gamma(p^n)]/G$ with $G \subset \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$	?	$X(P), N_G(X(Q))$
$[\Gamma(p^n)]/\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$	?	$N_{G_1}(X(P)), N_{G_2}(X(Q))$
$[\text{bal. } \Gamma_1(p^n)]$	$P \in E \rightleftarrows E' \ni P'$	$X(P), X'(P')$
$[\text{bal. } \Gamma_1(p^n)]/G \times H$	?	$N_G(X(P)), N_H(X'(P'))$
$[\Gamma_0(p^n)]$ viewed as $[\text{bal. } \Gamma_1(p^n)]/(\mathbf{Z}/p^n\mathbf{Z})^\times \times (\mathbf{Z}/p^n\mathbf{Z})^\times$	$E \underset{\pi^t}{\overset{\pi}{\rightleftarrows}} E'$	$N_G(X(P)), N_H(X'(P'))$
$[\Gamma_1(p^n)]$ viewed as $[\text{bal. } \Gamma_1(p^n)]/1 \times (\mathbf{Z}/p^n\mathbf{Z})^\times$	$P \in E \underset{\pi^t}{\overset{\pi}{\rightleftarrows}} E'$ (forget P')	$X(P), N(X'(P'))$
$[\Gamma_1(p^n)]$	$P \in E$	$T, X(P)$
$[\Gamma_0(p^n)]$ viewed as $[\Gamma_1(p^n)]/(\mathbf{Z}/p^n\mathbf{Z})^\times$	(forget P) $E \xrightarrow{\pi} E'$	$T, N(X(P))$

REMARK 7.7.1. Depending upon how we view $\Gamma_0(p^n)$ and $\Gamma_1(p^n)$, we get *different* sets of parameters at the supersingular points, depending on whether we think of the objects being classified as extra data on a single E, or as extra data on a diagram $E \rightleftarrows E'$. We give below still another set of parameters for $\Gamma_0(p^n)$ at the supersingular points, namely the "T-invariants" of the source and target.

(7.8) *More parameters for* $[\Gamma_0(p^n)]$, $n \geq 1$, *at supersingular points*

(7.8.1) Fix a supersingular elliptic curve E_0/k, k a perfect field of characteristic p, $E/W[[T]]$ its universal formal deformation, and $E_1/W[[T_1]]$ the universal formal deformation of $E_1 = E_0^{(p^n)}$. We know that $[\Gamma_0(p^n)]_{E/W[[T]]}$ is a closed subscheme of $[p^n\text{-Isog}]_{E/W[[T]]}$, and that this latter is a closed subscheme of $\text{Spec}(W[[T, T_1]])$, by the constructions

$$(\text{cyclic } p^n\text{-isogeny}) \mapsto (\text{source, target}).$$

We denote by A the complete two-dimensional regular local ring such that

$$\text{Spec}(A) = [\Gamma_0(p^n)]_{E/W[[T]]}.$$

Then A is a quotient of $W[[T, T_1]]$, and we have already seen (7.7) that A admits a regular sequence of parameters of the form (T, Y) for some Y (e.g., $Y = N(X(P))$, viewing $[\Gamma_0(p^n)]$ as $[\Gamma_1(p^n)]/(\mathbf{Z}/p^n\mathbf{Z})^\times$).

PROPOSITION 7.8.2. *The elements* (T, T_1) *are a regular sequence of parameters for* A.

Proof. This is true for any quotient of $W[[T, T_1]]$ which is regular of dimension two, which is finite and flat over $W[[T]]$ of degree ≥ 2, and admits (T, Y) as parameters for some Y. For A is necessarily of the form $W[[T, T_1]]/(f)$ where f is part of a regular system of parameters of $W[[T, T_1]]$. So modulo m^2, f is a k-linear combination of p, T, T_1. Our assertion is that the coefficient of p is non-zero (then (f, T, T_1) is a system of parameters for $W[[T, T_1]]$). If not, then

$$f = aT + bT_1 \mod m^2.$$

If $b \neq 0$, then (f, T, p) is a system of parameters for $W[[T, T_1]]$, whence (T, p) would be a system of parameters for A. This is impossible if A is to be finite flat over $W[[T]]$ of degree ≥ 2. If $b = 0$, then $a \neq 0$ (otherwise A won't be regular), so we can take $a = 1$, and then mod f we find $T \in (\max(A))^2$, contradicting the fact that T is part of a regular system of parameters for A. Q.E.D.

(7.9) *Detailed study of the congruence quotients* $[\Gamma_0(p^n);a,b]$ *of* $[\mathrm{bal.}\,\Gamma_1(p^n)]$

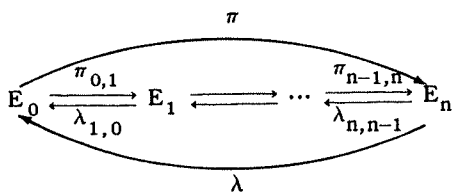
(7.9.1) In this section, we will give the modular interpretation of the quotient of $[\mathrm{bal.}\,\Gamma_1(p^n)]$ by any subgroup of $(\mathbf{Z}/p^n\mathbf{Z})^\times \times (\mathbf{Z}/p^n\mathbf{Z})^\times$ of the form $\Gamma \times \Gamma'$, where Γ and Γ' are *both* standard congruence subgroups of $(\mathbf{Z}/p^n\mathbf{Z})^\times$.

Recall (6.7.6, 6.7.9) that if

$$E_0 \underset{\lambda=\pi^t}{\overset{\pi}{\rightleftarrows}} E_n \tag{7.9.1.1}$$

is a dual pair of cyclic p^n-isogenies between elliptic curves over any base S, then both π and λ admit "standard" factorization into (necessarily) cyclic p-isogenies, and these standard factorizations are dual to each other: we have a diagram

(7.9.1.2)



where $(\pi_{0,1},\cdots,\pi_{n-1,n})$ is the standard factorization of π, $(\lambda_{n,n-1},\cdots,\lambda_{1,0})$ is the standard factorization of λ, and where for $1 \le a \le n$, we have

$$\lambda_{a,a-1} = (\pi_{a-1,a})^t . \tag{7.9.1.4}$$

For brevity, we denote, for $0 \le i < j \le n$, the partial composites

$$E_i \underset{\lambda_{j,i}}{\overset{\pi_{i,j}}{\rightleftarrows}} E_j \tag{7.9.1.5}$$

i.e.,

$$\pi_{i,j} = \pi_{j-1,j} \circ \pi_{j-2,j-1} \circ \cdots \pi_{i,i+1}$$

$$\lambda_{j,i} = \lambda_{i+1,i} \circ \lambda_{i+2,i+1} \cdots \circ \lambda_{j,j-1} .$$

PROPOSITION 7.9.2. *Let* $P \in (\mathrm{Ker}\,\pi)(S)$ *be a generator of* $\mathrm{Ker}\,\pi$, *and let* $Q \in (\mathrm{Ker}\,\lambda)(S)$ *be a generator of* $\mathrm{Ker}(\lambda)$. *Then*

(1) *for every* (a,b) *with* $0 \le a,b \le n-1$ *and* $0 \le a+b \le n-1$, $p^b\pi_{0,a}(P)$ *generates* $\mathrm{Ker}(\pi_{a,n-b})$, *and* $p^a\lambda_{n,n-b}(Q)$ *generates* $\mathrm{Ker}(\lambda_{n-b,a})$.

(2) *The canonical pairings* $<\ ,\ >$ *of these points are related by*

$$<p^b\pi_{0,a}(P),\ p^a\lambda_{n,n-b}(Q)>_{\pi_{a,n-b}} = (<P,Q>_\pi)^{p^{a+b}} ,$$

and $<P,Q>_\pi$ *is a "primitive"* p^n*'th root of unity.*

Proof. Assertion (1) is a special case of the Backing-Up Theorem (6.7.11). Assertion (2) is physically obvious if p is invertible, and as $[\mathrm{bal.}\,\Gamma_1(p^n)]$ is flat over $\mathbf{Z}$ it follows in general. Q.E.D.

PROPOSITION 7.9.3. *Let* $0 \le a,b \le n$ *be two integers. Let* $P_a \in \mathrm{Ker}(\pi_{a,n})(S)$ *be a generator of* $\mathrm{Ker}(\pi_{a,n})$, *and let* $Q_{n-b} \in \mathrm{Ker}(\lambda_{n-b,0})$ *be a generator of* $\mathrm{Ker}(\lambda_{n-b,0})$.

$$E_0 \underset{\lambda_{n-b,0}}{\overset{\pi_{0,a}}{\rightleftarrows}} \begin{matrix} P_a \\ \overset{\frown}{E_a} \\ E_{n-b} \\ \underset{\smile}{Q_{n-b}} \end{matrix} \underset{\lambda_{n,n-b}}{\overset{\pi_{a,n}}{\rightleftarrows}} E_n .$$

Then

(1) *for* $0 \le c \le a$, $\lambda_{a,c}(P_a)$ *generates* $\mathrm{Ker}(\pi_{c,n+c-a})$.

(2) *for* $0 \le d \le b$, $\pi_{n-b,n-b+d}(Q_{n-b})$ *generates* $\mathrm{Ker}(\lambda_{n-b+d,d})$.

(3) *If* $a \le b$, *then for* $0 \le c \le a$ *the canonical pairing*

$$<p^{b-a}\lambda_{a,c}(P_a),\ \pi_{n-b,n-b+c}(Q_{n-b})>$$

is a "primitive" p^{n-b}*'th root of unity, independent of the choice of* c.

(3 bis) *If* $a \geq b$, *then for* $0 \leq d \leq b$ *the canonical pairing*

$$<\lambda_{a,a-d}(P_a),\ p^{a-b}\pi_{n-b,n-d}(Q_{n-b})>$$

is a "primitive" p^{n-a}*'th root of unity, independent of the choice of* d.

Proof. The assertion is f.p.p.f. local on S. So we may assume we are given a point $P_0 \in (\mathrm{Ker}\ \pi)(S)$ such that $\pi_{0,a}(P_0) = P_a$, and a point $Q_n \in (\mathrm{Ker}\ \lambda)(S)$ such that $\lambda_{n,n-b}(Q_n) = Q_{n-b}$. By the Backing-Up Theorem (6.7.11), P_0 generates $\mathrm{Ker}\ \pi$, and Q_n generates $\mathrm{Ker}\ \lambda$. The result now follows from the previous proposition applied to P_0, Q_n. Q.E.D.

DEFINITION 7.9.4. For integers $0 \leq a,b \leq n$, we define a $[\Gamma_0(p^n); a,b]$ structure on an elliptic curve E/S to be a cyclic p^n-isogeny $\pi : E_0 \to E_n$ with dual $\lambda = \pi^t$ together with points $P_{n-a} \in (\mathrm{Ker}\ \pi_{n-a,n})(S)$ and $Q_b \in (\mathrm{Ker}\ \lambda_{b,0})(S)$ which *generate* these kernels

$$E_0 \underset{\lambda_{b,0}}{\overset{\pi_{0,n-a}}{\rightleftarrows}} E_{n-a} \underset{\lambda_{n,b}}{\overset{\pi_{n-a,n}}{\rightleftarrows}} E_n \ .$$

We denote by

(7.9.4.1) $$[\Gamma_0(p^n); a,b]$$

the corresponding moduli problem. It is naturally a moduli problem over $\mathbf{Z}[\zeta_{p^{\min(a,b)}}]$, by the $<\ ,\ >$ pairing (cf. (3), (3 bis) of 7.9.3).

There are natural morphisms of moduli problems

(7.9.4.2)
$$\begin{array}{c} [\mathrm{bal}.\,\Gamma_1(p^n)] = [\Gamma_0(p^n); n,n] \\ \downarrow \\ [\Gamma_0(p^n); a,b] \\ \downarrow \\ [\Gamma_0(p^n)] \end{array}$$

defined by

(7.9.4.3)
$$\begin{array}{c} (E_0 \underset{\lambda}{\overset{\pi}{\rightleftarrows}} E_n;\ P_0, Q_n) \\ \downarrow \\ (E_0 \underset{\lambda}{\overset{\pi}{\rightleftarrows}} E_n;\ P_{n-a} = \pi_{0,n-a}P_0;\ Q_b = \lambda_{n,b}Q_n) \\ \downarrow \\ (E_0 \underset{\lambda}{\overset{\pi}{\rightleftarrows}} E_n)\ . \end{array}$$

Let us temporarily denote by

(7.9.4.4) $$\Gamma(a) \subset (\mathbf{Z}/p^n\mathbf{Z})^\times$$

the subgroup of elements $\equiv 1 \bmod p^a$, so that we have a tautological exact sequence

$$1 \to \Gamma(a) \to (\mathbf{Z}/p^n\mathbf{Z})^\times \to (\mathbf{Z}/p^a\mathbf{Z})^\times \to 1\ .$$

LEMMA 7.9.5. *The map*

$$[\mathrm{bal}.\,\Gamma_1(p^n)] \to [\Gamma_0(p^n); a,b]$$

is equivariant for the natural action of $\Gamma(a) \times \Gamma(b)$ *on* $[\mathrm{bal}.\,\Gamma_1(p^n)]$, *and its trivial action on* $[\Gamma_0(p^n); a,b]$.

Proof. We must show that if $\alpha \equiv 1 \bmod p^a$, then $\pi_{0,n-a}(P_0) = \pi_{0,n-a}(\alpha P_0)$ (and similarly for b and Q_0). Writing $\alpha = 1 + p^a\gamma$, this amounts to

$$\pi_{0,n-a}(p^a P_0) = 0\ .$$

But $p^a P_0$ is in fact a generator of $\mathrm{Ker}(\pi_{0,n-a})$. Q.E.D.

There is also an obvious action of the group $(\mathbf{Z}/p^a\mathbf{Z})^\times \times (\mathbf{Z}/p^b\mathbf{Z})^\times$ on $[\Gamma_0(p^n); a,b]$, defined by having (α, β) move $(E_0 \rightleftarrows E_n; P_{n-a}, Q_b)$ to $(E_0 \rightleftarrows E_n; \alpha P_{n-a}, \beta Q_b)$.

THEOREM 7.9.6. *For any* $0 \le a,b \le n$, *the moduli problem* $[\Gamma_0(p^n); a,b]$ *is regular two-dimensional, finite and flat over* $[\Gamma_0(p^n)]$, *finite and flat under* $[\text{bal.}\,\Gamma_1(p^n)]$. *The natural maps*

$$\begin{array}{ccc} & [\text{bal.}\,\Gamma_1(p^n)] & \\ & \big\downarrow \;\Gamma(a)\times\Gamma(b) & \\ (\mathbf{Z}/p^n\mathbf{Z})^\times \times (\mathbf{Z}/p^n\mathbf{Z})^\times & [\Gamma_0(p^n); a,b] & \\ & \big\downarrow \;(\mathbf{Z}/p^a\mathbf{Z})^\times \times (\mathbf{Z}/p^b\mathbf{Z})^\times & \\ & [\Gamma_0(p^n)] & \end{array}$$

define isomorphisms

$$[\text{bal.}\,\Gamma_1(p^n)]/\Gamma(a)\times\Gamma(b) \xrightarrow{\sim} [\Gamma_0(p^n); a,b]$$

$$[\Gamma_0(p^n); a,b]/(\mathbf{Z}/p^a\mathbf{Z})^\times \times (\mathbf{Z}/p^b\mathbf{Z})^\times \xrightarrow{\sim} [\Gamma_0(p^n)]\,.$$

Proof. It suffices to establish that $[\Gamma_0(p^n); a,b]$ is regular two-dimensional and finite over (Ell). Then the finite flatness is automatic. The statements about quotients result from the physically obvious fact that they are true outside of p (compare the proof of (7.4.2)). We prove the regularity by a straightforward application of the Axiomatic Regularity Theorem (5.2.1). Axioms Reg. 1, Reg. 2, Reg. 3, and Reg. 4A are easily checked. Suppose both $a,b \ge 1$. Then we verify Reg. 4B bis by observing that the (formal-group coordinates of the) points P_{n-a}, Q_b provide parameters. For consider, over an artin local ring R with perfect residue field k of characteristic p, a cyclic p^n-isogeny

$$E_0 \underset{\lambda_{1,0}}{\overset{\pi_{0,1}}{\rightleftarrows}} E_1 \rightleftarrows \cdots \underset{\lambda_{n,n-1}}{\overset{\pi_{n-1,n}}{\rightleftarrows}} E_n$$

such that 0 generates $\text{Ker}(\pi_{n-a,n})$, and such that 0 generates $\text{Ker}(\lambda_{b,0})$. By the Backing-up Theorem (6.7.11), 0 generates $\text{Ker}(\pi)$

and it generates $\text{Ker}(\lambda)$. Therefore R is a k-algebra, and both $\text{Ker}(\pi) = \text{Ker}(F^n)$, $\text{Ker}(\lambda) = \text{Ker}(F^n)$; whence

$$E_0 \simeq (E_n)^{(p^n)} \quad \text{via } \lambda$$

$$E_n \simeq (E_0)^{(p^n)} \quad \text{via } \pi$$

so that $E_0 \simeq E_0^{(p^{2n})}$, whence E_0/R is constant, E_n/R is constant, and the isogenies $\pi_{i,i+1}, \lambda_{i+1,i}$ are all F.

If $a = b = 0$, then $[\Gamma_0(p^n); 0,0]$ is just $[\Gamma_0(p^n)]$, and the theorem is already proven. If one but not both of (a,b) vanishes, say $a > 0$, $b = 0$, then "T_0" and "$X(P_{n-a})$" give parameters. For if $P_{n-a} = 0$, then 0 generates $\text{Ker}(\pi)$, whence $p = 0$, R is a k-algebra and $\text{Ker}(\lambda) = \text{Ker}(F^n)$. Because "$T_0$" $= 0$, we also have E_0 constant over R.

If $a = 0$ and $b > 0$, then "T_n" and "$X(Q_b)$" give parameters, by the symmetric argument. Q.E.D.

(A7) *Appendix: Base-change for rings of invariants*

(A7.1) *Sufficient conditions*

Let R be a ring, A an R-algebra, and G a finite group which acts on A by R-linear ring automorphisms. We denote by $A^G \subset A$ the the R-subalgebra of all G-invariants. For any R-algebra R′, the group G acts R′-linearly on $A \underset{R}{\otimes} R'$ [by $g(a\otimes r') = g(a)\otimes r'$], and we have a natural R′-homomorphism

$$A^G \underset{R}{\otimes} R' \to (A \underset{R}{\otimes} R')^G\,.$$

Let us denote by

$$*(A, G, R, R')$$

the statement that the above map is an *isomorphism*, and by

$$*(A, G, R)$$

the statement that the above map is an isomorphism for every R-algebra R'.

THEOREM A7.1.1. *Let* R *be a ring,* A *an* R*-algebra, and* G *a finite group operating on* A *by* R*-algebra automorphisms. Suppose that* G *acts freely on* A *in the sense that for any non-zero* R*-algebra* R'*, and any element* $g \neq \mathrm{id}$ *of* G, g *operates without fixed points on the set* $\mathrm{Hom}_{R\text{-alg}}(A, R')$. *Then* A *is a finite etale* G*-torsor over* A^G*, and the natural map*

$$A \underset{A^G}{\otimes} A \to \prod_{g \in G} A$$

$$x \otimes y \mapsto (\cdots, x \otimes g(y), \cdots)$$

is an isomorphism of left A*-algebras.*

Proof. In the absence of noetherian hypotheses, this is rather delicate. See ([SGA III], Expose V, Thm. 4.1), or [De-Ga, III, §2, 6.1] for the proof.

COROLLARY A7.1.2. *Hypotheses as in A7.1.1 above,* $*(A, G, R)$ *holds.*

Proof. By the above theorem, A is a finite etale G-torsor over A^G. For any R-algebra R', if we make the extension of scalars $A^G \to A^G \underset{R}{\otimes} R'$, we obtain a finite etale G-torsor over $A^G \underset{R}{\otimes} R'$, namely $A \underset{R}{\otimes} R'$. But if $A \otimes R'$ is a finite etale G-torsor over $A^G \underset{R}{\otimes} R'$, then we certainly have

$$(A \underset{R}{\otimes} R')^G = A^G \underset{R}{\otimes} R' ,$$

i.e., $*(A, G, R, R')$ holds for any R'. Q.E.D.

PROPOSITION A7.1.3.

(0) *For any* R*-algebra* R', $*(A, G, R) \Rightarrow *(A \underset{R}{\otimes} R', G, R')$.

(1) *If* R' *is flat over* R, *then* $*(A, G, R, R')$ *holds.*

(2) *If* R' *is faithfully flat over* R, *then* $*(A, G, R) \Longleftrightarrow *(A \underset{R}{\otimes} R', G, R')$.

(3) *If* #G *is invertible in* R', *then* $*(A, G, R, R')$ *holds.*

(4) *If* #G *is invertible in* R, *then* $*(A, G, R)$ *holds.*

Proof. Assertion (0) is essentially a tautology. For if $*(A, G, R)$ holds, then for any homomorphisms $R \to R' \to R''$, we have a commutative diagram

$$\begin{array}{ccc} (A \underset{R}{\otimes} R')^G \underset{R'}{\otimes} R'' & \longrightarrow & ((A \underset{R}{\otimes} R') \underset{R'}{\otimes} R'')^G \\ \uparrow & & \uparrow \\ (A^G \underset{R}{\otimes} R') \underset{R'}{\otimes} R'' & \xrightarrow{\sim} A^G \underset{R}{\otimes} R'' \xrightarrow{\sim} & (A \underset{R}{\otimes} R'')^G . \end{array}$$

Assertion (1) holds simply because A^G is a kernel:

$$0 \longrightarrow A^G \longrightarrow A \xrightarrow{\oplus(1-g)} \underset{g}{\oplus} A$$

is an exact sequence of R-modules. For (2), let $R \to R''$ be an R-algebra. Then $R''' = R' \underset{R}{\otimes} R''$ is faithfully flat over R''. Consider the exact sequence of R''-modules

$$0 \to \mathrm{Ker} \to A^G \underset{R}{\otimes} R'' \to (A \underset{R}{\otimes} R'')^G \to \mathrm{Coker} \to 0 .$$

Because R''' is flat over R'', we may infer using (1) an exact sequence

$$0 \to \mathrm{Ker} \underset{R''}{\otimes} R''' \to A^G \underset{R}{\otimes} R''' \to (A \underset{R}{\otimes} R''')^G \to \mathrm{Coker} \underset{R''}{\otimes} R''' \to 0 .$$

Because R''' is faithfully flat over R'', the two end terms vanish after $\otimes R'''$ if and only if they vanished before.

To prove (3) and (4), we argue as follows. It suffices to prove (4), for if #G is invertible in R', then $R \to R'$ factors as

$$R \to R[1/\#G] \to R' .$$

The first arrow is a localization, so flat, and (4) covers the second. To prove (4), simply use the divided trace

$$T = \frac{1}{\#G} \sum_g g \quad \in R[G]$$

as a projection to exhibit A^G as a direct factor of A as R-module:

$$A = A^G \oplus (1-T)(A) .$$

Therefore the map

$$A^G \otimes R' \to (A \otimes R')^G \subset A \otimes R'$$

is injective. It is also surjective, because given an element

$$\sum a_i \otimes r_i' \in (A \otimes R')^G ,$$

it is the image of the element

$$\sum T(a_i) \otimes r_i' \in A^G \otimes R' . \qquad \text{Q.E.D.}$$

PROPOSITION A7.1.4. *Let* R *be a discrete valuation ring, with uniformizing parameter* π. *Consider the conditions* :

(1) $*(A, G, R)$ *holds.*

(2) $*(A, G, R, R/\pi^n R)$ *holds for all* $n \geq 1$.

(3) $*(A/\pi^n A, G, R/\pi^n R)$ *holds for all* $n \geq 1$.

Then we always have the implications

$$(1) \Longleftrightarrow (2) \Longrightarrow (3) .$$

If the fraction field of R *has characteristic zero, and if* A *is* R*-flat, then*

$$(1) \Longleftrightarrow (2) \Longleftrightarrow (3) .$$

Proof. Trivially, (1) $\Rightarrow$ (2), and (1) $\Rightarrow$ (3) by part (0) of the preceding proposition. Let us prove (2) $\Rightarrow$ (1). To prove (1), it obviously suffices to prove that for any R-module M, the natural map of R-modules

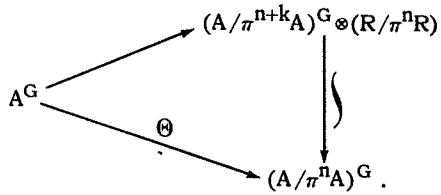
$$A^G \underset{R}{\otimes} M \to (A \underset{R}{\otimes} M)^G$$

is an isomorphism. Expressing M as the direct limit of its finitely generated submodules, and noting that both source and target commute with direct limits, we are reduced to checking when M is a finitely generated R-module. Because R is a discrete valuation ring, such an M is a direct sum of R's and of $R/\pi^n R$'s for various $n \geq 1$.

Let us now prove that (3) $\Rightarrow$ (2). Let us denote by k the π-adic valuation of $\#G$:

$$\#G = \pi^k \times (\text{unit in } R).$$

We will show that (3)(n+k) $\Rightarrow$ (2)(n). Consider the commutative diagram



We first show that Θ is surjective. Given an element

$$a_n \in (A/\pi^n A)^G ,$$

lift it to an element

$$a_{n+k} \in (A/\pi^{n+k}A)^G , \qquad a_{n+k} \bmod \pi^n = a_n ,$$

then choose

$$a \in A , \quad a \bmod \pi^{n+k} = a_{n+k} .$$

Because a_{n+k} is G-invariant, we have the congruence

$$(\#G)(a) \equiv \text{trace}_G(a) \bmod \pi^{n+k} A .$$

Because A is R-flat, this shows that the divided trace of a lies in A, and satisfies the congruence

$$a \equiv T(a) \bmod \pi^n A .$$

It remains to show that the kernel of Θ is $\pi^n(A^G)$. Because $(A/\pi^n A)^G$ is a subring of $A/\pi^n A$, the kernel of Θ is $A^G \cap \pi^n A$. Let $a \in \mathrm{Ker}$. Then $a = \pi^n b$, with $a \in A^G$ and $b \in A$. Then $\pi^n(g(b)-b) = 0$ for $g \in G$, whence A being R-flat, $b \in A^G$. Q.E.D.

(A7.2) *Radiciality*

PROPOSITION A7.2.1 (O. Gabber). *In the situation of A7.1, let* p *be a prime number,* p^n *the highest power of* p *which divides* $\#G$. *If* R' *is a* $Z_{(p)}$*-algebra (*$Z_{(p)}$ = *the localization of* Z *at* $(p) = \mathbf{Q} \cap Z_p$*), then the canonical homomorphism*

$$A^G \underset{R}{\otimes} R' \to (A \underset{R}{\otimes} R')^G$$

satisfies

(1) *every element of the target ring has* p^n*'th power in the image.*

(2) *every element of the kernel has* p^n*'th power equal to zero.*

Proof. We first reduce to the case when R is itself a $Z_{(p)}$-algebra. For this, factor $R \to R'$ as

$$R \to R \underset{Z}{\otimes} Z_{(p)} \to R' .$$

Because the first map is flat, we may, by A7.1.3 (1), replace R by $R \underset{Z}{\otimes} Z_{(p)}$.

We next reduce to the case when $R' = R/I$ for some ideal I of R. For this, write R' as the quotient of a polynomial ring $R'' = R[X_1, X_2, \cdots]$ over R, possibly in infinitely many variables, by an ideal I. Then factor $R \to R'$ as

$$R \to R'' \to R''/I .$$

Again the first map is flat (indeed R'' is a free R-module), so we may, by A7.1.3 (1), replace R by R''.

Thus we may assume that R is a $Z_{(p)}$-algebra, and that $R' = R/I$. We first prove (1), that the image of

$$A^G/IA^G \to (A/IA)^G$$

contains all p^n'th powers. Let

$$\tilde{a} \in (A/IA)^G ,$$

and choose an element

$$a \in A , \quad a \equiv \tilde{a} \bmod IA .$$

We will show that a^{p^n} lies in A^G. For this, we argue as follows. Because $\tilde{a}$ is G-invariant, we have a congruence of polynomials

$$\prod_{g \in G} (1 + g(a)X) \equiv (1 + aX)^{\#G} \bmod IA[X] .$$

The left-hand polynomial visibly has coefficients in A^G. Equating coefficients of X^{p^n}, we obtain

$$(\text{an element of } A^G) \equiv \binom{\#G}{p^n} a^{p^n} \bmod IA .$$

By hypothesis, $\#G = p^n N$ with $(N,p) = 1$, whence

$$\binom{\#G}{p^n} \equiv N \bmod pZ ,$$

so that

$$\binom{\#G}{p^n} = \text{a unit in } Z_{(p)} .$$

We next show that every element in the kernel of

$$A^G/IA^G \to (A/IA)^G$$

has p^n'th power equal to zero. Thus let

$$a \in A^G \cap (IA) ,$$

say

$$a = \sum f_i a_i \quad \text{with} \quad f_i \in I,\ a_i \in A .$$

Because a is G-invariant, we have an equality of polynomials

$$\prod_{g \in G} (1 + g(a)X) = (1 + aX)^{\#G} .$$

Writing $a = \Sigma f_i a_i$, and momentarily viewing the f_i as indeterminates, we see that in the polynomial

$$\prod_{g \in G} (1 + g(a)X) = \prod_{g \in G} \left(1 + \left(\sum f_i g(a_i)\right) X\right) ,$$

the coefficient of X^j is a sum, with A^G-coefficients, of monomials of degree j in the f_i's. In particular, for $j > 0$, the coefficient of X^j lies in IA^G. Again equating coefficients of X^{p^n}, we find

$$\binom{\#G}{p^n} a^{p^n} \in IA^G ,$$

as required. Q.E.D.

COROLLARY A7.2.2. *For any* $R \to R'$, *the map*

$$A^G \underset{R}{\otimes} R' \to (A \underset{R}{\otimes} R')^G$$

is bijective on geometric points.

Proof. We reduce immediately to the case where R' is itself an algebraically closed field K. If K has characteristic zero, the map $A^G \underset{R}{\otimes} K \to (A \underset{R}{\otimes} K)^G$ is an isomorphism (because #G is invertible in K),

while if K has characteristic $p > 0$, this map is surjective and radicial (by A7.2.1). Q.E.D.

Chapter 8

COARSE MODULI SCHEMES, CUSPS, AND COMPACTIFICATION

(8.1) *Coarse moduli schemes*

(8.1.1) Let R be a ring, $\mathcal{P}$ a relatively representable moduli problem on (Ell/R) which is affine over (Ell/R). We will recall the definition of the "coarse moduli scheme" $M(\mathcal{P})$. This is an R-scheme which agrees with $\mathcal{M}(\mathcal{P})$ for representable $\mathcal{P}$, and which is a "best replacement" if $\mathcal{P}$ is not representable.

To define $M(\mathcal{P})$ as an R-scheme, it suffices to do so locally on R. So we may assume that some integer $N \geq 3$ is invertible in R. Let $\mathcal{S}$ be any representable moduli problem which is finite etale galois over (Ell/R), with galois group G (e.g., $\mathcal{S} = [\Gamma(N)]$, $G = GL(2, Z/NZ)$). We define $M(\mathcal{P})$ as the quotient scheme

$$M(\mathcal{P}) = \mathcal{M}(\mathcal{P}, \mathcal{S})/G .$$

The resulting R-scheme is clearly independent of the auxiliary choice of $\mathcal{S}$ (and so patches together). It "exists" because $\mathcal{M}(\mathcal{P}, \mathcal{S})$ is itself affine.

LEMMA 8.1.2. *If $\mathcal{P}$ is normal, then $M(\mathcal{P})$ is normal.*

Proof. If $\mathcal{P}$ is normal, then $\mathcal{M}(\mathcal{P}, \mathcal{S})$ is normal, hence also its quotient by a finite group. Q.E.D.

(8.1.3) Let S be an R-scheme, E/S an elliptic curve, and $\alpha \in \mathcal{P}(E/S)$ a level $\mathcal{P}$-structure on E/S. Then there is a canonical "classifying map" of R-schemes

$$S \to M(\mathcal{P})$$

defined as follows. Locally on S, we may assume some integer $N \geq 3$ is invertible on S. Let S_N denote the finite etale galois S-scheme

$$S_N = [\Gamma(N)]_{E/S} ,$$

G the galois group $GL(2, Z/NZ)$ of S_N over S. Then $E \times_S S_N/S_N$ carries both a level $\mathcal{P}$-structure and a $[\Gamma(N)]$-structure, so we have an honest G-equivariant classifying map

$$\begin{array}{ccc} G\left(\right. & S_N & \longrightarrow \mathcal{M}(\mathcal{P}, \Gamma(N)) \\ & \downarrow & \downarrow \\ & S & \dashrightarrow M(\mathcal{P}) \end{array} ,$$

which therefore induces a map between the quotients by the G-action. Again, one verifies easily that the map $S \to M(\mathcal{P})$ constructed this way is independent of the auxiliary choice of N. Of course if $\mathcal{P}$ is representable, this map $S \to M(\mathcal{P}) = \mathcal{M}(\mathcal{P})$ is the classifying map for the isomorphism class of the data $(E/S/R, \alpha)$.

LEMMA 8.1.3.1. *When k is an algebraically closed field, then*

$$M(\mathcal{P})(k) = \textit{the set of } k\textit{-isomorphism classes of "elliptic curves } E/k \textit{ with given level } \mathcal{P}\textit{-structure."}$$

Proof. By (A7.2.2), on k-valued points we have a bijection

$$\mathcal{M}(\mathcal{P}, [\Gamma(N)])(k)/G \xrightarrow{\sim} M(\mathcal{P})(k) . \qquad \text{Q.E.D.}$$

(8.1.4) If $\mathcal{P}$ and $\mathcal{P}'$ are two relatively representable moduli problems on (Ell/R), any morphism

$$\mathcal{P} \to \mathcal{P}'$$

over (Ell/R) induces a morphism of R-schemes

$$M(\mathcal{P}) \to M(\mathcal{P}') ,$$

which, for any representable $\mathcal{S}$ which is finite etale galois over (Ell/R) with galois group G, sits in a commutative diagram

$$\begin{array}{ccc} \mathfrak{M}(\mathcal{P},\mathcal{S}) & \longrightarrow & \mathfrak{M}(\mathcal{P}',\mathcal{S}) \\ \Big\downarrow & & \Big\downarrow \\ M(\mathcal{P}) & \dashrightarrow & M(\mathcal{P}') \end{array}$$

(divide by G on the left; divide by G on the right).

LEMMA 8.1.5. *Suppose that a finite group* G *acts on* $\mathcal{P}$. *Then*

$$M(\mathcal{P})/G \xrightarrow{\sim} M(\mathcal{P}/G) .$$

Proof. The action of G on $\mathcal{P}$ induces an action of G on $M(\mathcal{P})$. The morphism $\mathcal{P} \to \mathcal{P}/G$ induces a G-equivariant map

$$M(\mathcal{P}) \to M(\mathcal{P}/G) ,$$

whence a map

$$M(\mathcal{P})/G \to M(\mathcal{P}/G) .$$

This is the map we must show to be an isomorphism. The question is local on R, so we may assume some odd prime ℓ invertible in R. Then by definition we have

$$\begin{aligned} M(\mathcal{P}/G) &= \mathfrak{M}(\mathcal{P}/G, [\Gamma(\ell)])/GL(2,\mathbf{F}_\ell) \\ &= (\mathfrak{M}(\mathcal{P}, [\Gamma(\ell)])/G)/GL(2,\mathbf{F}_\ell) \\ &= \mathfrak{M}(\mathcal{P}, [\Gamma(\ell)])/G \times GL(2,\mathbf{F}_\ell) \\ &= (\mathfrak{M}(\mathcal{P}, [\Gamma(\ell)])/GL(2,\mathbf{F}_\ell))/G \\ &= M(\mathcal{P})/G . \end{aligned}$$

Q.E.D.

PROPOSITION 8.1.6. *For any extension of scalars* $R \to R'$, *we have a canonical morphism of* R′*-schemes*

$$M(\mathcal{P}\otimes_R R') \to M(\mathcal{P})\otimes_R R' .$$

This morphism is an isomorphism if any of the following conditions holds

(1) $\mathcal{P}$ *is representable.*

(2) $R \to R'$ *is flat.*

(3) *the integer* $6 = 2\times 3$ *is invertible in* R.

(4) $\mathcal{P}$ *is the quotient of a representable problem* $\mathcal{P}'$ *by a finite group* G *whose order is invertible in* R′.

Proof. If $\mathcal{P}$ is representable, then $M(\mathcal{P}) = \mathfrak{M}(\mathcal{P})$ and the assertion is tautologous. If (4) holds, simply apply (A7.1.3, (3)) to the action of G on the coordinate ring of $\mathfrak{M}(\mathcal{P}')$. If 6 is invertible, we can take for $\mathcal{P}'$ the simultaneous problem $(\mathcal{P}, [\Gamma(3)])$, with $G = GL(2,\mathbf{F}_3)$, a group of order 48. If $R \to R'$ is flat, then Zariski locally on R we may apply (A7.1.3, (1)), by inverting an odd prime ℓ and viewing $\mathcal{P}$ as the quotient of $(\mathcal{P}, [\Gamma(\ell)])$ by the group $GL(2,\mathbf{F}_\ell)$. Q.E.D.

REMARK 8.1.7. Formation of the coarse moduli scheme does *not* always commute with base change.

(8.1.7.1) The simplest example is provided by the moduli problem $[\omega]$ on (Ell/Z) defined by

$[\omega](E/S)$ = the set of nowhere vanishing invariant one-forms on E/S.

This $[\omega]$ is a $\mathbf{G}_m$-torsor on (Ell/Z). For any ring R, the coarse moduli scheme $M([\omega]\otimes R)$ is the graded ring MF(R) of all level one modular forms (with no condition at infinity) over R. It is known that (cf. [De 2])

$$MF(\mathbf{Z}) = \mathbf{Z}[c_4, c_6, \Delta, \Delta^{-1}]/(c_4^3 - c_6^2 = 1728\,\Delta)$$

$$MF(\mathbf{F}_3) = \mathbf{F}_3[a_2, \Delta, \Delta^{-1}] \quad ; \quad a_2 = \text{Hasse invar.}$$

$$MF(\mathbf{F}_2) = \mathbf{F}_2[a_1, \Delta, \Delta^{-1}] \quad ; \quad a_1 = \text{Hasse invar.} ,$$

with interrelations

$$\begin{cases} c_4 \to a_2^2\,, \quad c_6 \to a_2^3 & \text{mod } 3 \\ c_4 \to a_1^4\,, \quad c_6 \to a_1^6 & \text{mod } 2\,. \end{cases}$$

Thus the maps

$$\begin{cases} MF(\mathbf{Z}) \otimes \mathbf{F}_3 \to MF(\mathbf{F}_3) \\ MF(\mathbf{Z}) \otimes \mathbf{F}_2 \to MF(\mathbf{F}_2) \end{cases}$$

both fail to be isomorphisms.

(8.1.7.2) For an example which is finite flat over $(\mathrm{Ell}/\mathbf{Z})$, consider the sub-problem $[\Delta = 1]$ defined by

$$[\Delta=1](E/S) = \text{the set of nowhere vanishing translation-invariant } \omega\text{'s such that } \Delta(E,\omega) = 1\,.$$

This $[\Delta=1]$ is a μ_{12}-torsor over $(\mathrm{Ell}/\mathbf{Z})$. Over any ring R, it is easy to see that

$$M([\Delta=1]\otimes R) = \mathrm{Spec}\,(MF(R)/(\Delta-1))\,,$$

and so

$$M([\Delta=1]) = \mathrm{Spec}\,(\mathbf{Z}[c_4, c_6]/(c_4^3 - c_6^2 = 1728))$$

$$M([\Delta=1]\otimes \mathbf{F}_3) = \mathrm{Spec}\,(\mathbf{F}_3[a_2])$$

$$M([\Delta=1]\otimes \mathbf{F}_2) = \mathrm{Spec}\,(\mathbf{F}_3[a_1])\,.$$

Once again, base change fails at the primes two and three.

(8.2) *The j-line as a coarse moduli scheme*

(8.2.1) It is well known (cf. [Ig 3, §2]) that over any ring R, the coarse moduli scheme attached to the moduli problem $[\Gamma(1)]$ is the j-line over R:

$$M([\Gamma(1)]) = \mathrm{Spec}\,(R[j])\,,$$

with the j-invariant normalized à la Tate (cf. [De 2]); $j = 0$ has complex multiplication by $\mathbf{Z}[\zeta_3]$, $j = 1728$ by $\mathbf{Z}[i]$.

For any relatively representable $\mathcal{P}$, affine over (Ell/R), the unique map of moduli problems on (Ell/R)

$$\mathcal{P} \to [\Gamma(1)]$$

defines a morphism of R-schemes

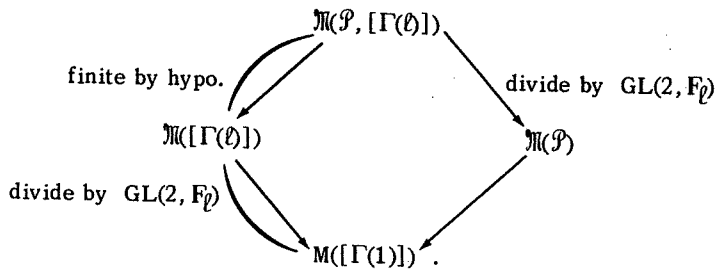
$$M(\mathcal{P}) \to \mathrm{Spec}\,(R[j])\,.$$

PROPOSITION 8.2.2. *If R is noetherian, and if $\mathcal{P}$ is finite over (Ell/R), then*

$$M(\mathcal{P}) \to \mathrm{Spec}\,(R[j])$$

is finite.

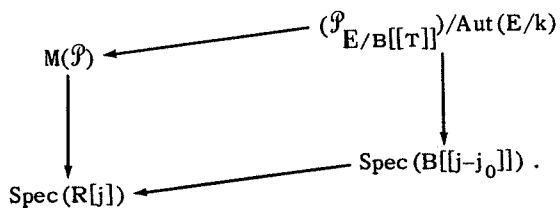
Proof. The question is local on R, so we may assume some odd prime ℓ is invertible in R. We have a commutative diagram of R-schemes



Because $\mathcal{M}([\Gamma(\ell)])$ is an affine R-scheme of finite type, it is finite over its quotient $M([\Gamma(1)])$ by the finite group $GL(2, \mathbf{F}_\ell)$. Therefore $\mathcal{M}(\mathcal{P}, [\Gamma(\ell)])$ is finite over $M([\Gamma(1)])$. Because R is noetherian, $M([\Gamma(1)])$ is the Spec of a noetherian ring, and therefore the coordinate ring of $M(\mathcal{P})$, being contained in a finite $R[j]$-module, is itself finite over $R[j]$. Q.E.D.

PROPOSITION 8.2.3. *Let $\mathcal{P}$ be relatively representable and finite over (Ell/R). Let B be a complete local noetherian R-algebra which is flat*

over R, *and whose residue field* k *is algebraically closed. Let* E/k *be an elliptic curve, and denote by* E/B[[T]] *its universal formal deformation (to artin local* B*-algebras). Let* $j_{00} \in k$ *be the* j*-invariant* j(E/k), *and* $j_0 \in B$ *some lifting of it to* B. *Then we have a cartesian diagram*



Proof. Because B is R-flat, $M(\mathcal{P}\underset{R}{\otimes}B) \simeq M(\mathcal{P})\underset{R}{\otimes}B$, and we are reduced to the case R = B. The action of Aut(E/k) on the finite B[[T]]-scheme $\mathcal{P}_{E/B[[T]]}$ is by viewing it as the formal B-scheme which pro-represents the functor on artin local B-algebras with residue field k

$$A \mapsto \text{triples } (\tilde{E}/A, \alpha, i) \text{ where } \tilde{E}/A \text{ is an elliptic curve,}$$
$$\alpha \in \mathcal{P}(\tilde{E}/A), \text{ and } i \text{ is a k-isomorphism } \tilde{E}\underset{R}{\otimes}k \simeq E.$$

The group Aut(E/k) acts on this functor by moving the isomorphism i.

Choose an odd prime $\ell \neq \mathrm{char}(k)$. Then ℓ is invertible in B, so that $\mathcal{S} = [\Gamma(\ell)]\underset{Z}{\otimes}B$ is a finite etale $GL(2, F_\ell)$-torsor over (Ell/B). By definition, we have

$$M(\mathcal{P}) \simeq \mathfrak{M}(\mathcal{P}, \mathcal{S})/GL(2, F_\ell),$$

as B[j]-schemes. By flatness of $B[[j-j_0]]$ over B[j], we infer

$$M(\mathcal{P}) \underset{B[j]}{\otimes} B[[j-j_0]] \simeq \left(\mathfrak{M}(\mathcal{P}, \mathcal{S}) \underset{B[j]}{\otimes} B[[j-j_0]]\right)\Big/GL(2, F_\ell).$$

If we knew the proposition for $(\mathcal{P}, \mathcal{S})$, we could rewrite this

$$= ((\mathcal{P}, \mathcal{S})_{E/B[[T]]})/\mathrm{Aut}(E/k) \times GL(2, F_\ell)$$
$$= ((\mathcal{P}, \mathcal{S})_{E/B[[T]]})/GL(2, F_\ell)/\mathrm{Aut}(E/k)$$
$$= (\mathcal{P}_{E/B[[T]]})/\mathrm{Aut}(E/k),$$

the last equality because $(\mathcal{P}, \mathcal{S})$ is a finite etale $GL(2, F_\ell)$-torsor over $\mathcal{P}$, so we can pass to the quotient "object by object."

Thus we are reduced to the case when $\mathcal{P}$ is *representable* and finite over (Ell/B). Then $\mathfrak{M}(\mathcal{P})$ is finite over B[j], so we have a canonical decomposition, B being complete,

$$\mathfrak{M}(\mathcal{P}) \underset{B[j]}{\times} B[[j-j_0]] = \coprod_{j(x)=j_0} \mathrm{Spec}(\hat{\mathcal{O}}_{\mathfrak{M}(\mathcal{P}),x})$$

over the k-valued (= closed) points of $\mathfrak{M}(\mathcal{P})$ with j-invariant j_0. Each such point x is of the form (E/k, some $\alpha_x \in \mathcal{P}(E/k)$), and the α_x run over a set of representatives of $\mathcal{P}(E/k)$ modulo Aut(E/k). By definition of $\mathfrak{M}(\mathcal{P})$, the corresponding complete local ring $\hat{\mathcal{O}}_{\mathfrak{M}(\mathcal{P}),x}$ pro-represents the functor on artin local B-algebras with residue field k

$$A \mapsto \begin{cases} \text{pairs } (\tilde{E}/A, \alpha \in \mathcal{P}(\tilde{E}/A)) \text{ such that} \\ (\tilde{E}/A, \alpha)\otimes k \text{ admits an isomorphism} \\ \text{with } (E/k, \alpha_x). \end{cases}$$

Because $\mathcal{P}$ is representable, it is rigid, so Aut(E/k) acts freely on $\mathcal{P}(E/k)$; therefore if $(\tilde{E}/A, \alpha)\underset{A}{\otimes}k$ admits an isomorphism with $(E/k, \alpha_x)$, this isomorphism is unique.

Therefore the finite B[[T]]-scheme

$$\mathfrak{M}(\mathcal{P}) \underset{B[j]}{\times} B[[j-j_0]]$$

pro-represents the functor

$$A \mapsto \begin{cases} \text{an element } a_x \in \mathcal{P}(E/k) \text{ among our chosen} \\ \text{set of representatives, together with a triple} \\ (\tilde{E}/A,\ a \in \mathcal{P}(\tilde{E}/A),\ i) \text{ with } i \text{ an isomorphism} \\ (\tilde{E}/A, a) \underset{A}{\otimes} k \xrightarrow{\sim} (E/k, a_x)\ . \end{cases}$$

On the other hand, $\mathcal{P}_{E/B[[T]]}$ pro-represents the functor

$$A \mapsto \begin{cases} \text{an element } a_0 \in \mathcal{P}(E/k) \text{ and a triple} \\ (\tilde{E}/A,\ a \in \mathcal{P}(\tilde{E}/A),\ i) \text{ where } i \text{ is an} \\ \text{isomorphism} \\ (\tilde{E}/A, a) \underset{A}{\otimes} k \xrightarrow{\sim} (E/k, a_0)\ . \end{cases}$$

By the rigidity of $\mathcal{P}$, the isomorphism i is *unique*. As $\mathrm{Aut}(E/k)$ operates freely on the indexing set $\mathcal{P}(E/k)$ of a_0's we may identify the quotient of $\mathcal{P}_{E/B[[T]]}$ by $\mathrm{Aut}(E/k)$ to the subfunctor of $\mathcal{P}_{E/B[[T]]}$ defined by requiring a_0 to lie in a fixed set of representatives, say the a_x's, of $\mathcal{P}(E/k)$ modulo $\mathrm{Aut}(E/k)$. Q.E.D.

(8.3) *Localization of moduli problems over the* j*-line*

(8.3.1) Let U be an open set in the affine j-line $\mathrm{Spec}(R[j])$. We denote by $(\mathrm{Ell}/U/R)$ the full subcategory of (Ell/R) consisting of those elliptic curves $E/S/R$ whose j-invariant "lies in U", in the sense that the morphism "j" factors through U:

(8.3.1.1)
$$\begin{array}{ccc} S & \dashrightarrow & U\ . \\ \downarrow{\scriptstyle j} & & \\ \mathrm{Spec}(R[j]) & & \end{array}$$

We denote by $[U]$ the moduli problem on (Ell/R) which is the "characteristic function of U"; for any $E/S/R$, we define

$$(8.3.1.2) \qquad [U](E/S) = \begin{cases} \text{the set with one element if} \\ E/S/R \text{ lies in } (\mathrm{Ell}/U/R), \\ \text{the empty set if not.} \end{cases}$$

This moduli problem is relatively representable and etale (indeed an open immersion) over (Ell/R); for any $E/S/R$, we have

$$(8.3.1.3) \qquad [U]_{E/S} = S \underset{\mathrm{Spec}(R[j])}{\times} U\ .$$

(8.3.2) For any moduli problem $\mathcal{P}$ on (Ell/R), we define $\mathcal{P}|U$ to be the open sub-problem defined by

$$(8.3.2.1) \qquad (\mathcal{P}|U)(E/S) = \mathcal{P}(E/S) \times [U](E/S)$$

$$= \begin{cases} \mathcal{P}(E/S) \text{ if } E/S \text{ lies in } (\mathrm{Ell}/U/R) \\ \text{the empty set if not.} \end{cases}$$

If $\mathcal{P}$ is relatively representable over (Ell/R), then so is $\mathcal{P}|U$, and we have

$$(8.3.2.2) \qquad (\mathcal{P}|U)_{E/S} = \mathcal{P}_{E/S} \underset{\mathrm{Spec}(R[j])}{\times} U \underline{\text{ notation }} \mathcal{P}_{E/S}|U\ .$$

In particular, if $\mathcal{P}$ is representable, then $\mathcal{P}|U$ is representable and we have

$$(8.3.2.3) \qquad \mathfrak{M}(\mathcal{P}|U) = \mathfrak{M}(\mathcal{P}) \underset{\mathrm{Spec}(R[j])}{\times} U = \mathfrak{M}(\mathcal{P})|U\ .$$

If U is affine over R, then for any relatively representable $\mathcal{P}$ which is affine over (Ell/R), $\mathcal{P}|U$ is affine over (Ell/R), and the coarse moduli schemes of $\mathcal{P}$ and of $\mathcal{P}|U$ are related by

$$(8.3.2.4) \qquad M(\mathcal{P}|U) = M(\mathcal{P}) \underset{\mathrm{Spec}(R[j])}{\times} U = M(\mathcal{P})|U\ .$$

In particular, taking $\mathcal{P} = [\Gamma(1)]$, we find

$$(8.3.2.5) \qquad M([U]) = U\ .$$

(8.4) *The j-invariant as a fine modulus, coarse moduli schemes as fine moduli schemes* (!)

(8.4.1) Recall from [De 2] that the ring of modular forms over $\mathbf{Z}$ is generated by the forms c_4, c_6, Δ, and Δ^{-1}, with the single relation

$$(c_4)^3 - (c_6)^2 = 1728\Delta$$

and that j is given by the formulas

$$j = (c_4)^3/\Delta$$

$$j - 1728 = (c_6)^2/\Delta .$$

(8.4.2) Recall also that for an elliptic curve E/S, the following conditions are equivalent

(1) For any connected S-scheme T, the elliptic curve E_T/T has $\mathrm{Aut}(E_T/T) = \pm 1$.

(2) $j(E/S)(j(E/S)-1728)$ is invertible in $\Gamma(S, \mathcal{O}_S)$.

(3) For any S-scheme T, and any nowhere vanishing invariant differential ω on E_T/T, the elements $c_4(E_T, \omega)$, $c_6(E_T, \omega)$ are both invertible in $\Gamma(T, \mathcal{O}_T)$.

(4) E/S lies in $(\mathrm{Ell}/U/\mathbf{Z})$ for U the open set $\mathrm{Spec}(\mathbf{Z}[j][1/j(j-1728)])$ of $\mathrm{Spec}(\mathbf{Z}[j])$.

One also has the following more precise result, which we quote from [De 2].

PROPOSITION 8.4.3. *Let S be an arbitrary scheme, E_1/S and E_2/S two elliptic curves over S. Suppose that $j(E_1/S) = j(E_2/S)$, and that $j(E_1/S)\cdot(j(E_1/S)-1728)$ is invertible in $\Gamma(S, \mathcal{O}_S)$. Then the functor on* (Sch/S)

$$T \mapsto \textit{isomorphisms of elliptic curves over } T \textit{ from } E_1 \times_S T \textit{ to } E_2 \times_S T ,$$

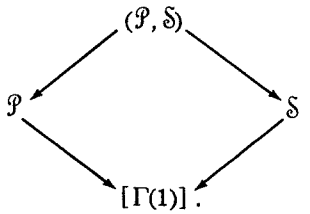
is represented by an S-scheme $\mathrm{Isom}_S(E_1, E_2)$ which is a finite etale galois covering of S with group ± 1.

COROLLARY 8.4.4. *Let R be an arbitrary ring, $\mathcal{P}$ and $\mathcal{S}$ two representable moduli problems on* (Ell/R).

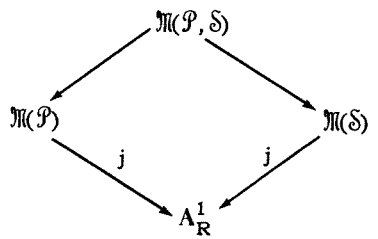
Let $(\mathcal{P}, \mathcal{S})$ denote the simultaneous moduli problem

$$E/S \mapsto \mathcal{P}(E/S) \times \mathcal{S}(E/S) ,$$

which sits in a commutative diagram of moduli problems on (Ell/R)



The induced morphisms of coarse moduli schemes



define a morphism of $\mathbf{A}^1_R$-schemes

$$\mathfrak{M}(\mathcal{P}, \mathcal{S}) \longrightarrow \mathfrak{M}(\mathcal{P}) \times_{\mathbf{A}^1_R} \mathfrak{M}(\mathcal{S}) .$$

This morphism, over the open set U in $\mathbf{A}^1_R$ where $j(j-1728)$ in invertible, makes $\mathfrak{M}(\mathcal{P}, \mathcal{S})|U$ into a finite etale galois covering of $\mathfrak{M}(\mathcal{P}|U) \times_U \mathfrak{M}(\mathcal{S}|U)$, with group ± 1, and so it induces an isomorphism of U-schemes

$$(\mathfrak{M}(\mathcal{P}, \mathcal{S})|U)/\pm 1 \xrightarrow{\sim} \mathfrak{M}(\mathcal{P}|U) \times_U \mathfrak{M}(\mathcal{S}|U) .$$

Proof. Consider the functor Z on (Sch/R) represented by $\mathfrak{M}(\mathcal{P}|U) \times_U \mathfrak{M}(\mathcal{S}|U)$. For any R-scheme S, we have

$Z(S)$ = S-isomorphism classes of data $(E_1/S,\alpha, E_2/S,\beta)$ with E_1/S, E_2/S elliptic curves over S with $j(E_1/S) = j(E_2/S)$, $j(E_1/S)(j(E_1/S)-1728)$ invertible in $\Gamma(S,\mathcal{O}_S)$, $\alpha \in \mathcal{P}(E_1/S)$, $\beta \in \mathcal{S}(E_2/S)$.

Now consider the functor W on (Sch/R) represented by $\mathcal{M}(\mathcal{P},\mathcal{S})|U$. For any R-scheme S, we have

$W(S)$ = S-isomorphism classes of data $(E/S,\alpha,\beta)$ with E/S an elliptic curve over S with $j(E/S)(j(E/S)-1728)$ invertible in S, $\alpha \in \mathcal{P}(E/S)$, $\beta \in \mathcal{S}(E/S)$.

The morphism of U-schemes

$$\mathcal{M}(\mathcal{P},\mathcal{S})|U \to \mathcal{M}(\mathcal{P}|U) \underset{U}{\times} \mathcal{M}(\mathcal{S}|U)$$

corresponds to the map on functors

$$W \to Z$$

defined on S-valued points by

$$(E/S,\alpha,\beta) \mapsto (E/S,\alpha,E/S,\beta) .$$

Therefore if we are given any R-morphism $S \to \mathcal{M}(\mathcal{P}|U) \underset{U}{\times} \mathcal{M}(\mathcal{S}|U)$, corresponding to data $(E_1/S,\alpha,E_2/S,\beta)$, then the fiber product

$$\begin{array}{ccc} \square & \longrightarrow & S \\ \downarrow & & \downarrow \\ \mathcal{M}(\mathcal{P},\mathcal{S})|U & \longrightarrow & \mathcal{M}(\mathcal{P}|U) \underset{U}{\times} \mathcal{M}(\mathcal{S}|U) , \end{array}$$

is none other than the scheme

$$Isom_S(E_1,E_2) ,$$

which is finite etale galois over S with group ± 1. Q.E.D.

COROLLARY 8.4.5. *Let* R *be a regular noetherian ring,* $\mathcal{P}$ *a representable moduli problem on* (Ell/R). *Let* U *be an affine open set in* Spec(R[j]). *Suppose that* j(j–1728) *is invertible on* U, *and suppose that* $\mathcal{P}|U$ *is finite etale over* [U]. *Then the morphism* "j"

$$\mathcal{M}(\mathcal{P}) \to \text{Spec}(R[j])$$

is finite etale over U, *i.e., the map*

$$\mathcal{M}(\mathcal{P}|U) \to U$$

is finite etale.

Proof. Because R is regular, and $\mathcal{P}|U$ is finite etale over [U], the moduli scheme $\mathcal{M}(\mathcal{P}|U)$ is regular, as is U itself. The morphism $\mathcal{M}(\mathcal{P}|U) \to U$ is certainly finite, so it is automatically flat, because source and target are regular schemes of the same dimension. Because $\mathcal{M}(\mathcal{P}|U) \to U$ is finite and flat, we may base-change by it to test whether some other map $X \to U$ is finite etale. Thus it suffices to see that

$$\mathcal{M}(\mathcal{P}|U) \underset{U}{\times} \mathcal{M}(\mathcal{P}|U) \xrightarrow{pr_1} \mathcal{M}(\mathcal{P}|U)$$

is finite etale. This map sits under

$$\mathcal{M}(\mathcal{P}|U,\mathcal{P}|U) \longrightarrow \mathcal{M}(\mathcal{P}|U) \underset{U}{\times} \mathcal{M}(\mathcal{P}|U) \xrightarrow{pr_1} \mathcal{M}(\mathcal{P}|U) .$$

The first map is a finite etale ± 1 torsor, [± 1 acting on pairs of level $\mathcal{P}$ structures by $(\alpha_1,\alpha_2) \mapsto (\alpha_1,\pm\alpha_2)$], and the composite

$$\mathcal{M}(\mathcal{P}|U,\mathcal{P}|U) \to \mathcal{M}(\mathcal{P}|U)$$

is finite etale by hypothesis. Therefore our map is also finite etale. Q.E.D.

PROPOSITION 8.4.6. *Let* R *be any ring,* U *any affine open set of* Spec(R[j]) *on which* j(j–1728) *is invertible,* $\mathcal{P}$ *a relatively representable moduli problem which is affine over* (Ell/R). *Suppose that for*

any E/S/R *which lies in* (Ell/U/R), *the automorphism* $[-1]_E$ *operates on the set* $\mathcal{P}(E/S)$ *without fixed points. Then* $\mathcal{P}|U$ *is representable, and*

$$\mathfrak{M}(\mathcal{P}|U) = M(\mathcal{P}|U) = M(\mathcal{P})|U .$$

Proof. The hypothesis assures that $\mathcal{P}|U$ is rigid. Q.E.D.

COROLLARY 8.4.7. *Let* $N \geq 1$ *be any integer. Let* U_N *be an affine open set in* Spec(Z[j]) *such that*

$$\begin{cases} j(j-1728) \text{ is invertible on } U_N \\ \text{for all } p|N,\ U_N(\bar{F}_p) \text{ contains no j's of} \\ \text{supersingular curves in characteristic } p. \end{cases}$$

Then

(1) *If* $N \geq 3$, *then* $[\Gamma(N)]|U_N$ *is representable on* (Ell/Z).

(2) *If* $N = 1,2,4$, *then* [bal. $\Gamma_1(N)$]$|U_N$ *is representable on* (Ell/Z).

Proof. Of course if N is divisible by two relatively prime integers both ≥ 3, (resp. both ≥ 4), then $[\Gamma(N)]$ (resp. [bal. $\Gamma_1(N)$]) itself is representable.

To prove (1), it suffices to show that if E/S is an elliptic curve with a $\Gamma(N)$-structure (P,Q) with $2P = 2Q = 0$, then there is a geometric point s of S of characteristic p|N at which E_s is supersingular. If N is odd, $2P = 2Q = 0$ implies $P = Q = 0$, whence for any prime p|N, $((N/p)P, (N/p)Q) = (0,0)$ is a Drinfeld p-basis for E/S (5.5.7). Therefore S is an F_p-scheme, and E_s is supersingular at *every* geometric point of S (5.3.2.1, 5.3.6). In particular, N is a power of p. If N is even, then $(2P, 2Q) = (0,0)$ is a Drinfeld N/2-structure in E/S, and we repeat the same argument with N/2, which by hypothesis is still ≥ 2.

To prove (2), it suffices to show that if $(E \rightleftarrows E', P, P')$ is a balanced $\Gamma_1(N)$ structure over some S, with $2P = 2P' = 0$, then there is a geometric point s of S of characteristic p|N at which E_s is supersingular. If N is odd, $2P = 2P' = 0$ implies $P = P' = 0$. Therefore (5.5.5) (0,0) is a $\Gamma(N)$-structure on E/S, and we conclude as before.

If N is even, we argue as follows. First suppose $N = 2^k M$ with M odd ≥ 3. Consider the standard factorization of our given cyclic $E \to E'$ into a cyclic M-isogeny followed by a cyclic 2^k-isogeny:

$$P\ ;\ E \underset{\pi^t_{odd}}{\overset{\pi_{odd}}{\rightleftarrows}} E'' \underset{\pi^t_{even}}{\overset{\pi_{even}}{\rightleftarrows}} E'\ ;\ P'.$$

By the Backing-up Theorem (6.7.11), $2^k P$ generates $\mathrm{Ker}(\pi_{odd})$ and $\pi^t_{even}(P')$ generates $\mathrm{Ker}(\pi^t_{odd})$. As $2P = 2P' = 0$, the previous case " N odd " applies to

$$2^k P\ ;\ E \underset{\pi^t_{odd}}{\overset{\pi_{odd}}{\rightleftarrows}} E''\ ;\ \pi^t_{even}(P') .$$

If $N = 2^n$, we consider the standard factorization into a sequence of 2-isogenies

$$P = P_0\ ;\ E = E_0 \underset{}{\overset{\pi_{0,1}}{\rightleftarrows}} E_1 ::: E_{n-1} \underset{\lambda_{n,n-1}}{\overset{}{\rightleftarrows}} E_n = E'\ ;\ P' = Q_n .$$

Then $2\pi_{0,1}(P_0)$ generates $\mathrm{Ker}(\pi_{1,n-1})$, and $2\lambda_{n,n-1}(Q_n)$ generates $\mathrm{Ker}(\lambda_{n-1,1})$. As n is ≥ 3, these are dual 2^{n-2}-isogenies, both generated by zero, so by (5.3.2.3) S is an F_2-scheme and E_1/S is supersingular at every geometric point of S. Since E_0 is isogenous to E_1, it too is supersingular at every geometric point of S. Q.E.D.

REMARK 8.4.8. The moduli problems $[\Gamma(1)]$, $[\Gamma(2)]$, [bal. $\Gamma_1(2)$] are *not* representable, over *any* non-void open set of the j-line, because they are *not rigid*; the automorphism [-1] visibly acts trivially. As for [bal. $\Gamma_1(4)$], it is of course representable over Z[1/2], but it is *not* representable over *any* non-void open set of the j-line which contains *any* point of characteristic two. For such an open meets the j-line over F_2 in a non-void open set, hence contains ordinary points in characteristic two. If E/k is an ordinary curve over an algebraically closed field k of

characteristic 2, then there exists an isomorphism

$$E[4] \simeq \mu_4 \times Z/4Z .$$

The points

$$P = (1,2)$$
$$Q = (1,1)$$

form a $\Gamma(4)$-structure (because $P - 2Q$ generates the μ_4, and Q generates the $Z/4Z$). Visibly $2Q = P$, so the associated balanced $\Gamma_1(4)$-structure $(P, Q \bmod P)$ is fixed by the automorphism $[-1]$.

THEOREM 8.4.9. *Let* R *be a ring in which* 2 *is invertible, and let* $a \in R^\times$ *be a unit of* R. *Let* $U \subset \mathrm{Spec}(R[j])$ *be the open set* $U = \mathrm{Spec}(R[j][1/j(j-1728)])$ *where* $j(j-1728)$ *is invertible. Denote by* $[U,a]$ *the moduli problem on* (Ell/R) *defined by*

$[U,a](E/S)$ = *the set of nowhere vanishing invariant differentials* ω *on* E/S *such that* $c_4(E,\omega)$ *and* $c_6(E,\omega)$ *are both invertible on* S, *and such that*

$$c_6(E,\omega)/c_4(E,\omega) = a .$$

Then we have

(1) *The natural morphism "forget* ω*" of moduli problems on* (Ell/R)

$$[U,a] \mapsto [U]$$

is finite etale and galois with galois group ± 1.

(2) *The moduli problem* $[U,a]$ *is representable, and is affine and etale over* (Ell/R).

(3) *The map of coarse moduli schemes induced by (1),*

$$\mathfrak{M}([U,a]) \to M([U]) = U$$

is an isomorphism of R*-schemes.*

Proof. It is clear from the formulas expressing j via c_4, c_6 and Δ, that the natural map $[U,a] \to [\Gamma(1)]$ factors through $[U]$. To show that (1) holds, consider an $E/S/R$ such that its $j(j-1728)$ is invertible on S. Zariski localizing on S, we may suppose there exists a nowhere-vanishing invariant differential ω_0 on E/S. Then both $c_4(E,\omega_0)$ and $c_6(E,\omega_0)$ are invertible on S. Then a nowhere-vanishing ω on E/S may be written in the form $\lambda^{-1}\omega_0$ for some unit $\lambda \in \Gamma(S,\mathcal{O}_S)^\times$, and such an ω lies in $[U,a](E/S)$ if and only if

$$\lambda^2 = a \cdot \frac{c_4(E,\omega_0)}{c_6(E,\omega_0)} .$$

Because 2 is invertible, this equation defines $[U,a]_{E/S}$ as a finite etale galois covering of S with group ± 1. Thus (1) holds, and, $[U]$ being affine and etale over (Ell/R), we see that its finite etale covering $[U,a]$ is itself relatively representable, affine and etale over (Ell/R). Because $[U,a]$ is a *rigid* moduli problem, it is consequently representable, necessarily by a smooth affine curve $\mathfrak{M}([U,a])$ over R.

Because $[U]$ is the quotient of $[U,a]$ by the group ± 1, we have

$$\mathfrak{M}([U,a])/\pm 1 \xrightarrow{\sim} M([U]) = U .$$

But the group ± 1 acts *trivially* on the scheme $\mathfrak{M}([U,a])$, because as an R-scheme $\mathfrak{M}([U,a])$ represents the functor on R-schemes

$$S \mapsto \text{S-isomorphism classes of pairs } (E/S,\omega)$$
$$\text{where } \omega \text{ is a } [U,a]\text{-structure on } E/S ,$$

and the data $(E/S,\omega)$ is S-isomorphic (by $[-1]_E$) to the data $(E/S,-\omega)$.

Q.E.D.

COROLLARY 8.4.10. *Let* R *be a ring in which* 2 *is invertible,* $a \in R^\times$ *a unit,* $\mathcal{P}$ *a relatively representable moduli problem which is affine over* (Ell/R). *Let* U *denote the open set of* $\mathrm{Spec}(R[j])$ *where* $j(j-1728)$ *is invertible. Then*

(1) *The simultaneous moduli problem* $(\mathcal{P}, [U,a])$ *is representable, and it is finite etale galois over* $\mathcal{P}|U$ *with galois group* ± 1.

(2) *We have a natural isomorphism of* R*-schemes*

$$\mathcal{M}(\mathcal{P}, [U,a])/\pm 1 \xrightarrow{\sim} M(\mathcal{P}|U) = M(\mathcal{P})|U .$$

(3) *If, for every elliptic curve* E/S/R, *the automorphism* $[-1]_E$ *acts trivially on the set* $\mathcal{P}(E/S)$, *then the isomorphism in (2) above is an isomorphism of* R*-schemes*

$$\mathcal{M}(\mathcal{P}, [U,a]) \xrightarrow{\sim} M(\mathcal{P}|U) = M(\mathcal{P})|U .$$

Proof. Assertion (1) holds because $[U,a]$ is representable, and finite etale galois over $[U]$ with group ± 1. By (8.1.5), this implies (2). Under the hypothesis of (3), the group ± 1 acts trivially on $\mathcal{M}(\mathcal{P}, [U,a])$. Q.E.D.

THEOREM 8.4.11. *Let* R *be a ring in which* 2 *is nilpotent,* U *the open set of* Spec(R[j]) *where* j(j–1728) *is invertible. Denote by* $[\mu_4]$ *the moduli problem on* (Ell/R) *defined by*

$$[\mu_4](E/S) = \text{the set of } S\text{-group injections } \mu_4 \xrightarrow{\alpha} E .$$

Then

(1) *The natural morphism "forget* α*" of moduli problems on* (Ell/R) $[\mu_4] \to [\Gamma(1)]$ *factors through* $[U]$, *and the induced map*

$$[\mu_4] \to [U]$$

is finite etale and galois with galois group ± 1.

(2) *The moduli problem* $[\mu_4]$ *is representable, and it is affine and etale over* (Ell/R).

(3) *The map of coarse moduli schemes induced by (1)*

$$\mathcal{M}([\mu_4]) \to M([U]) = U$$

is an isomorphism of R*-schemes.*

Proof. Because 2 is nilpotent, an E/S/R has j(j–1728) invertible if and only if its j is invertible if and only if E/S is fiber-by-fiber *ordinary*.

Now when 2 is nilpotent, E/S is fiber-by-fiber ordinary if and only if locally f.p.p.f. on S, the kernel of 4 in the formal group $\hat{E}[4]$ is isomorphic to μ_4, if and only if locally f.p.p.f. on S there exists an S-group inclusion $\mu_4 \hookrightarrow E$. Therefore $[\mu_4]$ does indeed lie over $[U]$, and over $[U]$ it is the finite etale galois covering with galois group $\pm 1 = (\mathbf{Z}/4\mathbf{Z})^\times$ defined by

$$[\mu_4]_{E/S} = \mathit{Isom}_S(\mu_4, \hat{E}[4])$$

for any fiber-by-fiber ordinary E/S/R. Assertion (2) is in fact true over $\mathbf{Z}$, as has already been noted, because $[\mu_4]$ is a rigid problem. Assertion (3) holds because $[U] = [\mu_4]/\pm 1$, while ± 1 acts trivially on the scheme $\mathcal{M}([\mu_4])$. Q.E.D.

COROLLARY 8.4.12. *Let* R *be a ring in which* 2 *is nilpotent,* U *the open set of* Spec(R[j]) *where* j(j–1728) *is invertible,* $\mathcal{P}$ *a relatively representable moduli problem affine over* (Ell/R). *Then conclusions (1), (2), (3) of (8.4.10) hold, with* $[U,a]$ *replaced by* $[\mu_4]$.

(8.5) *Base change for coarse moduli schemes*

(8.5.1) Let R be a ring, $\mathcal{P}$ a relatively representable moduli problem which is affine over (Ell/R), and U an affine open set of Spec(R[j]) on which j(j–1728) is invertible. For any extension of scalars $R \to R'$, we have natural morphisms of $R'[j]$-schemes

(8.5.1.1) $$M(\mathcal{P}) \underset{R}{\otimes} R' \to M(\mathcal{P} \underset{R}{\otimes} R') ,$$

(8.5.1.2) $$M(\mathcal{P}|U) \underset{R}{\otimes} R' \to M((\mathcal{P}|U) \underset{R}{\otimes} R') ,$$

the second of which is simply the restriction of the first to the open set U.

(8.5.2) If the first of these maps is an isomorphism for any $R \to R'$, we say that $\mathcal{P}$ satisfies coarse base change. If the second is always an isomorphism, we say that $\mathcal{P}|U$ satisfies coarse base change.

THEOREM 8.5.3.

(I) *$\mathcal{P}$ satisfies coarse base change if any of the following conditions holds:*

(1) *$\mathcal{P}$ is representable.*

(2) *The integer $6 = 2 \times 3$ is invertible in R.*

(3) *$\mathcal{P}$ is the quotient of a representable $\mathcal{P}'$ by a finite group G whose order is invertible in R.*

(II) *$\mathcal{P}|U$ satisfies coarse base change if any of the following conditions holds:*

(0) *$\mathcal{P}$ satisfies coarse base change*

(1) *The integer 2 is invertible in R.*

(2) *For any $E/S/R$ which lies in $(Ell/U/R)$, the automorphism $[-1]_E$ acts without fixed points on the set $\mathcal{P}(E/S)$.*

(3) *R is a Dedekind domain with fraction field of characteristic zero, for every $E/S/R$, the automorphism $[-1]_E$ acts trivially on the set $\mathcal{P}(E/S)$, and $\mathcal{P}$ is flat over R.*

Proof. Part I has already been proven (8.1.6). Let us prove II. If 2 is invertible, then $\mathcal{P}|U$ is the quotient of a representable problem, namely $(\mathcal{P}, [U, a])$, by ± 1, and the result follows by I(3). Under the hypothesis II(2), $\mathcal{P}|U$ is representable (because rigid). To prove II(3), it suffices to do so after the faithfully flat base change

$$R \to R[1/2] \oplus \Big(\bigoplus_{v|2} R_v \Big)$$

where the sum is over the places v of R of residue characteristic 2, and R_v denotes the v-adic completion. Over $R[1/2]$, II(1) applies. So we are reduced to considering an R_v. By (A7.1.4), it suffices to show that for every $n \geq 1$,

$$\mathcal{P} \otimes_R (R_v/\pi_v^n R_v)|U$$

satisfies coarse base change over the ring $R_v/\pi_v^n R_v$. But 2 is nilpotent in this ring, so that by (8.4.12), the coarse moduli scheme in question is a fine moduli scheme, to which I(1) applies

$$\begin{array}{c} \mathcal{M}(\mathcal{P} \otimes_R (R_v/\pi_v^n R_v), [\mu_4]) \\ \big\downarrow \\ M(\mathcal{P} \otimes_R (R_v/\pi_v^n R_v))|U. \end{array}$$

Q.E.D.

(8.5.4) Summarizing Table

In the table below, $N \geq 1$ is an integer, and $U = U_N$ is any affine open set of the j-line over $\mathbf{Z}$ such that

$$\begin{cases} j(j-1728) \text{ is invertible on } U_N. \\ \text{For any prime } p \text{ dividing } N, \text{ and any} \\ \text{supersingular } E/k \text{ with } k \text{ a field of} \\ \text{characteristic } p, \text{ the j-invariant } j(E/k) \\ \text{does } \textit{not} \text{ lie in } U_N(k). \end{cases}$$

Problem $\mathcal{P}$	Coarse base change $\mathcal{P}\|U$ over $\mathbf{Z}$	Justification over $\mathbf{Z}_2$
$[\Gamma(N)]$	YES	if $N=1,2$; II(3) if $4\|N$; II(2) if odd $p\|N$; II(2)
[bal. $\Gamma_1(N)$]	YES if $N \neq 4$? if $N = 4$	if $N=1,2$; II(3) if $8\|N$; II(2) if odd $p\|N$; II(2)
$[\Gamma_1(N)]$	YES if $N \neq 4,8,16\cdots$? if $N = 4,8,16\cdots$	if $N=1,2$; II(3) if odd $p\|N$; II(2)
$[\Gamma_0(N)]$	YES	II(3)
$[\Gamma_0(p^n);a,b]$ with $a\geq 1, b\geq 1$	YES if p odd YES if $p=2, n\geq 3, a\geq 2, b\geq 2$ YES if $p=2$, $a=b=1$? in other cases	II(2) II(2) II(3)

(8.6) *Cusps by normalization near infinity; compactified coarse moduli schemes*

(8.6.1) In this section, we will assume that R is a noetherian ring which is regular and *excellent* (e.g., R is excellent if it is of finite type over $\mathbf{Z}$, over a field, over a mixed-characteristic discrete valuation ring ... cf. [EGA IV, 7.8]).

(8.6.2) Let $\mathcal{P}$ be a moduli problem on (Ell/R) which satisfies the following two axioms:

C1. $\mathcal{P}$ is relatively representable and finite over (Ell/R)

C2. $M(\mathcal{P})$ is normal near infinity, in the sense that there exists a monic polynomial $f(j) \in R[j]$ such that over the open set $U \subset \mathbf{A}^1_R$ where f is invertible, $M(\mathcal{P})|U$ is normal.

Then $M(\mathcal{P})$ is finite over $\mathbf{A}^1_R = \mathrm{Spec}\,(R[j])$, and the open set $M(\mathcal{P})|U$ is normal. Notice that if $\mathcal{P}$ itself is normal near infinity, i.e., if $\mathcal{P}|U$ is normal, then $M(\mathcal{P})$ is normal near infinity.

(8.6.3) We now extend the $\mathbf{A}^1_R$-scheme $M(\mathcal{P})$ to a $\mathbf{P}^1_R$-scheme $\bar{M}(\mathcal{P})$ by "normalizing near infinity." To be precise, let us temporarily denote by D the divisor $f = 0$ in $\mathbf{A}^1_R$. Because f is monic, the open set

$$\bar{U} \overset{\text{dfn}}{=\!=} \mathbf{P}^1_R - D$$

is a neighborhood of the ∞-section in $\mathbf{P}^1_R$. We define

$$\begin{array}{c} \bar{M}(\mathcal{P}) \\ \downarrow \\ \mathbf{P}^1_R \end{array}$$

as follows. Over $\mathbf{A}^1_R$, it coincides with $M(\mathcal{P})$. Over $\bar{U}$, it is the *normalization* of $\bar{U}$ in $M(\mathcal{P})|U$:

(8.6.3.1)
$$\begin{array}{ccccc} M(\mathcal{P}) & \longleftarrow\!\supset & M(\mathcal{P})|U & \subset\!\longrightarrow & M(\mathcal{P})|\bar{U} \\ \downarrow & & \downarrow & & \downarrow \\ \mathbf{A}^1_R & \longleftarrow\!\supset & U & \subset\!\longrightarrow & \bar{U}\,. \end{array}$$

These two pieces agree over $\bar{U} \cap \mathbf{A}^1_R = U$, precisely because $M(\mathcal{P})|U$ is already normal, and finite over U.

Thus $\bar{M}(\mathcal{P})$ is the unique scheme finite over $\mathbf{P}^1_R$, which agrees with $M(\mathcal{P})$ over $\mathbf{A}^1_R$ and which over some open neighborhood $\bar{U}$ of the ∞-section in $\mathbf{P}^1_R$ is normal (cf. [Nag, 36.6], [EGA IV, 7.8.3, (vi)]).

The scheme of cusps of $\mathcal{P}$ is by definition the reduced finite R-scheme

(8.6.3.2) $$\mathrm{Cusps}\,(\mathcal{P}) \overset{\text{dfn}}{=\!=} (\bar{M}(\mathcal{P}) - M(\mathcal{P}))^{\mathrm{red}} = (j^{-1}(\infty))^{\mathrm{red}}\,.$$

The formal completion of $\bar{M}(\mathcal{P})$ along its cusps, or equivalently along the divisor defined by the equation " $1/j = 0$ ", is denoted $\widehat{\mathrm{Cusps}}\,(\mathcal{P})$. We have a cartesian diagram

(8.6.3.3)
$$\begin{array}{ccccc} \widehat{\mathrm{Cusps}}\,(\mathcal{P}) & & \subset\!\longrightarrow & & \bar{M}(\mathcal{P}) \\ \downarrow & & & & \downarrow \\ \mathrm{Spec}\,(R[[1/j]]) & & \subset\!\longrightarrow & \mathrm{Spec}\,(R[1/j]) & \subset\!\longrightarrow\ \mathbf{P}^1_R\,. \end{array}$$

PROPOSITION 8.6.4. *Let R be an excellent noetherian regular ring, $\mathcal{P}$ a moduli problem on (Ell/R) satisfying C1 and C2, and G a finite group operating on $\mathcal{P}$. Then $\mathcal{P}/G$ satisfies C1 and C2 (by 7.1.3, (5), (6)), and*

(1) *G acts on $\bar{M}(\mathcal{P})$, covering its trivial action on $\mathbf{P}^1_R = \bar{M}([\Gamma(1)])$.*

(2) *We have an isomorphism $\bar{M}(\mathcal{P})/G \xrightarrow{\sim} \bar{M}(\mathcal{P}/G)$ of $\mathbf{P}^1_R$-schemes.*

(3) *We have an isomorphism*

$$\widehat{\mathrm{Cusps}}\,(\mathcal{P})/G \xrightarrow{\sim} \widehat{\mathrm{Cusps}}\,(\mathcal{P}/G)$$

of $R[[1/j]]$-schemes.

Proof. (1) The action of G on $M(\mathcal{P})/M([\Gamma(1)])$ extends by normalization. (2) The isomorphism $M(\mathcal{P})/G \xrightarrow{\sim} M(\mathcal{P}/G)$ of $M([\Gamma(1)])$-schemes extends by normalization (the scheme $(M(\mathcal{P})/G)|\bar{U}$ is normal, finite over $\bar{U}$, and agrees with $\bar{M}(\mathcal{P}/G)$ over U). (3) follows from (2) and the above cartesian diagram, which shows that $\widehat{\text{Cusps}}(\mathcal{P})/R[[1/j]]$ is obtained from $\bar{M}(\mathcal{P})/\mathbf{P}^1_R$ by a flat base extension. Because formation of quotients by finite groups commutes with flat base extension, we get (3). Q.E.D.

DEFINITION 8.6.5. We say that a moduli problem $\mathcal{P}$ on (Ell/R) which satisfies C1 and C2 is smooth near infinity if it satisfies *both* of the following conditions:

S–∞–1. There exists an open neighborhood V of the cusps in $\bar{M}(\mathcal{P})$,

$$\text{Cusps}(\mathcal{P}) \subset V \subset \bar{M}(\mathcal{P})$$

which is smooth over R (necessarily of relative dimension one).

S–∞–2. The scheme of cusps $\text{Cusps}(\mathcal{P})$ is finite etale over R.

In practice, it is convenient to replace S–∞–1 by the equivalent

S–∞–1 bis. The formal completion $\widehat{\text{Cusps}}(\mathcal{P})$ of $\bar{M}(\mathcal{P})$ along its cusps is formally smooth over R.

PROPOSITION 8.6.6. *Let* R *be an excellent noetherian regular ring, and* $\mathcal{P}$ *a moduli problem on* (Ell/R) *which is relatively representable. Suppose that:*

(1) $\mathcal{P}$ *is finite over* (Ell/R), *and* $M(\mathcal{P})$ *is normal near infinity.*

(2) $\mathcal{P}$ *satisfies coarse base change near infinity, in the sense that there exists a monic polynomial* $f(j) \in R[j]$, *such that for* U *the open set where* $j(j-1728)f(j)$ *is invertible,* $\mathcal{P}|U$ *satisfies coarse base change.* <*Recall that this is automatic if* $\mathcal{P}$ *is representable, or if* 2 *is invertible, or ... (cf. 8.5.3)*>.

(3) $\mathcal{P}$ *is smooth near infinity.*

Then for any extension of scalars $R \to R'$ *with* R' *an excellent noetherian regular ring,* $\mathcal{P} \underset{R}{\otimes} R'$ *also satisfies (1), (2), (3), and we have*

(a) *for some open neighborhood* $\bar{U}$ *of the* ∞*-section of* $\mathbf{P}^1_R$,

$$\bar{M}(\mathcal{P}) \underset{R}{\otimes} R'|\bar{U} \xrightarrow{\sim} \bar{M}(\mathcal{P} \underset{R}{\otimes} R')|\bar{U}.$$

(b) $\widehat{\text{Cusps}}(\mathcal{P}) \underset{R}{\hat{\otimes}} R' \xrightarrow{\sim} \widehat{\text{Cusps}}(\mathcal{P} \underset{R}{\otimes} R')$.

(c) $\text{Cusps}(\mathcal{P}) \underset{R}{\otimes} R' \xrightarrow{\sim} \text{Cusps}(\mathcal{P} \underset{R}{\otimes} R')$.

Proof. Enlarging the monic polynomial f, we may assume that the open neighborhood V of the cusps in $\bar{M}(\mathcal{P})$ is the inverse image of $\bar{U} = \mathbf{P}^1_R$ - (the divisor $j(j-1728)f(j)$). Then $V \cap M(\mathcal{P})$ is $M(\mathcal{P})|U$, which by hypothesis is smooth over R. Therefore $(M(\mathcal{P})|U) \underset{R}{\otimes} R'$ is smooth over R'. Because $\mathcal{P}|U$ satisfies coarse base change, this says that $M(\mathcal{P} \underset{R}{\otimes} R')|U$ is smooth over R', hence normal. This already shows that $\mathcal{P} \underset{R}{\otimes} R'$ satisfies (1) and (2). The scheme $\bar{M}(\mathcal{P}) \otimes R'|\bar{U}$ is smooth over R', hence normal. As it is finite over $\bar{U} \underset{R}{\otimes} R'$, and coincides over $U \otimes R'$ with $M(\mathcal{P}) \otimes R'|U = M(\mathcal{P} \underset{R}{\otimes} R')|U$, it must be $\bar{M}(\mathcal{P} \underset{R}{\otimes} R')|\bar{U}$. This proves that $\mathcal{P} \otimes R'$ is smooth near infinity, and that (a) holds. If the cusps of $\mathcal{P}$ are finite etale over R, they are a Cartier divisor Z in the smooth R-curve $\bar{M}(\mathcal{P})|\bar{U}$. Then $Z \underset{R}{\otimes} R'$ is finite etale over R', it is reduced, and so it is the cusps of $\mathcal{P} \underset{R}{\otimes} R'$ inside the smooth R'-curve $(\bar{M}(\mathcal{P})|\bar{U}) \otimes R' = \bar{M}(\mathcal{P}) \otimes R'|\bar{U}$. Therefore (b) and (c) hold. Q.E.D.

PROPOSITION 8.6.7. *Let* R *be an excellent noetherian regular ring, and let* R' *be an excellent noetherian regular* R*-algebra which is flat over* R, *and such that the fibers of* $\text{Spec}(R') \to \text{Spec}(R)$ *are all geometrically regular (e.g.,* R' *etale over* R, *or smooth over* R, *or a completion of* R *at a closed point of* Spec(R), ...). *Let* $\mathcal{P}$ *be a moduli problem on* (Ell/R) *satisfying* C1 *and* C2, *i.e.,* $\mathcal{P}$ *is relatively representable and finite over* (Ell/R), *and* $M(\mathcal{P})$ *is normal near infinity. Then*

(1) *The moduli problem* $\mathcal{P} \underset{R}{\otimes} R'$ *on* (Ell/R′) *satisfies C1 and C2.*

(2) *The natural extension of scalars map of coarse moduli schemes defines an isomorphism of* R′*-schemes*

$$M(\mathcal{P} \underset{R}{\otimes} R') \xrightarrow{\sim} M(\mathcal{P}) \underset{R}{\otimes} R'.$$

(3) *The above isomorphism extends to define an isomorphism of compactified coarse moduli schemes*

$$\bar{M}(\mathcal{P} \underset{R}{\otimes} R') \xrightarrow{\sim} \bar{M}(\mathcal{P}) \underset{R}{\otimes} R'.$$

Proof. The map in (2) is an isomorphism because $R \to R'$ is flat. Because of the "regular fibers" hypothesis, $M(\mathcal{P}) \underset{R}{\otimes} R'$ is still normal near infinity, so $\mathcal{P} \underset{R}{\otimes} R'$ satisfies C1 and C2. The isomorphism (3) is the fact that both sides are R′-schemes finite over the projective j-line, normal near infinity, and which agree over the affine j-line. Q.E.D.

THEOREM 8.6.8. *Let* R *be an excellent noetherian regular domain, whose fraction field has characteristic zero. Let* $\mathcal{P}$ *be a representable moduli problem on* (Ell/R) *which is finite over* (Ell/R). *Suppose that for some open set* $U \subset \mathrm{Spec}(R[j])$ *defined by inverting a monic polynomial in* j, $\mathcal{P}|U$ *is finite etale over* [U]. *Then*

(1) *over the open set* $U' = U[1/j(j-1728)]$; *the map*

$$\mathcal{M}(\mathcal{P}|U') \xrightarrow{j} U'$$

is finite etale, and tamely ramified along the infinity section of the projective j*-line.*

(2) *The compactified moduli scheme* $\bar{\mathcal{M}}(\mathcal{P})$ *is smooth over* R *of relative dimension one in a neighborhood of the cusps, the scheme of cusps is finite etale over* R, *and in a neighborhood of the cusps, the invertible sheaf*

$$\Omega^1_{\bar{\mathcal{M}}(\mathcal{P})/R}(\log \text{ cusps})$$

of one-forms with at worst simple poles along the cusps is free on the one-form $d\log(1/j)$.

(3) *For any excellent noetherian regular* R*-algebra* R′, *statements (1) and (2) remain true for* $\mathcal{P} \underset{R}{\otimes} R'$, *and we have isomorphisms of* $P^1_{R'}$*-schemes*

$$\bar{\mathcal{M}}(\mathcal{P}) \underset{R}{\otimes} R' \xrightarrow{\sim} \bar{\mathcal{M}}(\mathcal{P} \underset{R}{\otimes} R').$$

Proof. That $\mathcal{M}(\mathcal{P}|U') \to U'$ is finite etale has already been proven (8.4.5). That it is tamely ramified along the infinity section results from the fact that R has generic characteristic zero. Once we know $\mathcal{M}(\mathcal{P}|U') \to U'$ is finite etale and tame along infinity, (2) and (3) result by Abhyankar's lemma (cf. [SGA I], Exp. XIII, 5.5). Q.E.D.

(8.7) *Interlude: The groups* T[N] *and* T

(8.7.1) Over the ring $Z[q,q^{-1}]$ of Laurent polynomials over Z in one variable, we will define for every integer $N \geq 1$ a finite flat commutative group-scheme T[N] of rank N^2 which is killed by N. As a *scheme*, T[N] is the disjoint union of N schemes $T_0[N], \cdots, T_{N-1}[N]$, where

$$(8.7.1.1) \qquad T_i[N] = \mathrm{Spec}(Z[q,q^{-1}][X]/(X^N - q^i)).$$

For any $Z[q,q^{-1}]$-algebra R with connected spectrum, we have

(8.7.1.2) T[N](R) = pairs (X, i/N) with $0 \leq i \leq N-1$ and with $X \in R$ satisfying $X^N = q^i$.

The group structure is given by defining

$$(8.7.1.3) \qquad (X, i/N) \cdot (Y, j/N) = \begin{cases} (XY, (i+j)/N) & \text{if } i+j \leq N-1 \\ (XY/q, (i+j-N)/N) & \text{if } i+j \geq N. \end{cases}$$

The elements of the form $(X,0)$ form a subgroup $\mu_N(R)$, and we have a short exact sequence

$$(8.7.1.4)\qquad 0 \longrightarrow \mu_N \xrightarrow{a_N} T[N] \xrightarrow{b_N} Z/NZ \longrightarrow 0$$
$$\zeta \longmapsto (\zeta,0)$$
$$(X, i/N) \longmapsto i \bmod N .$$

This exact sequence splits over any R containing an N'th root of q, say $q^{1/N}$, for then we may write

$$(8.7.1.5)\qquad (X, i/N) = (Xq^{-i/N},0) \times (q^{i/N}, i/N) .$$

Thus over $Z[q,q^{-1}][q^{1/N}]$, we have

$$(8.7.1.6)\qquad T[N] \simeq \mu_N \times Z/NZ .$$

There is a unique alternating* pairing of $Z[q,q^{-1}]$-group-schemes

$$(8.7.1.7)\qquad e_N : T[N] \times T[N] \to \mu_N ,$$

which is *compatible* with the above extension structure in the following sense: for every $Z[q,q^{-1}]$-algebra R, every $\zeta \in \mu_N(R)$ and every $P \in T[N](R)$, we have

$$(8.7.1.8)\qquad e_N(a_N(\zeta), P) = \zeta^{b_N(P)} .$$

(It is unique because these formulas and the requirement it be alternating uniquely determine it after the f.p.p.f. base extension to $Z[q,q^{-1}][q^{1/N}]$.) The pairing is given explicitly by the formula

$$(8.7.1.9)\qquad e_N((X, i/N), (Y, j/N)) = X^j/Y^i .$$

We will refer to the exact sequence

$$(8.7.1.10)\qquad 0 \longrightarrow \mu_N \xrightarrow{a_N} T[N] \xrightarrow{b_N} Z/N \longrightarrow 0$$

*i.e., for any $Z[q,q^{-1}]$-algebra R, and any $P \in T[N](R)$, we have $e_n(P,P) = 1$.

as the canonical extension-structure on $T[N]$, and to the alternating pairing

$$e_N : T[N] \times T[N] \to \mu_N$$

as the e_N-pairing.

(8.7.2) We will now define a smooth one-dimensional commutative group-scheme T over $Z[q,q^{-1}]$, locally of finite type, which sits in an f.p.p.f. short exact sequence of group-schemes over $Z[q,q^{-1}]$

$$(8.7.2.1)\qquad 0 \to G_m \to T \to Q/Z \to 0$$

in such a way that $T[N]$ is the kernel of N in T, for every integer $N \geq 1$. As a scheme, T is the disjoint union of schemes T_α, indexed by α's running over all *rational* numbers in the interval $[0,1)$, where each T_α is just the scheme G_m. Thus over any $Z[q,q^{-1}]$-algebra R with connected spectrum, we have

$$(8.7.2.2)\qquad T(R) = \text{pairs } (X,\alpha) \text{ with } X \in R^\times \text{ and } \alpha \in Q \cap [0,1) .$$

The group-structure is defined by

$$(8.7.2.3)\qquad (X,\alpha)\cdot(Y,\beta) = \begin{cases} (XY, \alpha+\beta) & \text{if } \alpha+\beta < 1 \\ \left(\frac{XY}{q}, \alpha+\beta-1\right) & \text{if } \alpha+\beta \geq 1 . \end{cases}$$

Let us temporarily denote by $[\alpha]$ the integral part of the rational number α, and by $<\alpha>$ its fractional part:

$$(8.7.2.4)\qquad \begin{cases} \alpha = [\alpha] + <\alpha> \text{ with} \\ [\alpha] \in Z, \ 0 \leq <\alpha> < 1 . \end{cases}$$

For any $Z[q,q^{-1}]$-algebra R with connected spectrum, we have a fundamental short exact sequence of groups

$$(8.7.2.5)(*)\qquad 0 \longrightarrow Z \xrightarrow{a} G_m(R) \times Q \xrightarrow{\pi} T(R) \longrightarrow 0$$

defined by

$$a(n) = (q^n, n)$$

$$\pi(X, \alpha) = (X/q^{[\alpha]}, <\alpha>) . \tag{8.7.2.6}$$

Thus (8.7.2.1) is the "pushout" of the short exact sequence

$$0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0 \tag{8.7.2.7}$$

of constant group-schemes over $\mathbf{Z}[q,q^{-1}]$ by the tautological homomorphism of group-schemes over $\mathbf{Z}[q,q^{-1}]$

$$\mathbf{Z} \to \mathbf{G}_m ;$$

$$n \mapsto q^{-n} \in \mathbf{G}_m(\mathbf{Z}[q,q^{-1}]) .$$

The short exact sequence (*) allows for easy computation. Thus given a point $(X, \alpha) \in T(R)$, i.e., $X \in R^\times$, $\alpha \in \mathbf{Q} \cap [0,1)$, we have, for every integer N, the formula

$$N \cdot (X, \alpha) = (X^N/q^{[N\alpha]}, <N\alpha>) . \tag{8.7.2.8}$$

(8.7.3) In particular, (X, α) is killed by N if and only if $\alpha = i/N$ for some $0 \le i \le N-1$ and $X^N = q^i$. Thus as promised we find $T[N] = T[N]$ compatibly with the canonical extension structures on T and on $T[N]$.

(8.7.4) Over any $\mathbf{Z}[q,q^{-1}]$-algebra R containing a compatible system of N'th roots $q^{1/N}$ of q for every N, (i.e., for every integer $N \ge 1$, we are given $Y_N \in R^\times$ such that $Y_1 = q$ and $(Y_{NM})^M = Y_N$ for every $M,N \ge 1$), the inverse image T_R of T on $\mathrm{Spec}(R)$ has a product decomposition as R-group-scheme

$$T_R \xrightarrow{\sim} \mathbf{G}_m \times \mathbf{Q}/\mathbf{Z} . \tag{8.7.4.1}$$

defined on R'-valued points, for any R-algebra R' with connected spectrum, by

$$\begin{array}{ccc} (X, \alpha) & \longmapsto & (X/q^\alpha, \alpha) \\ \in & & \in \\ T(R') & & \mathbf{G}_m(R') \times \mathbf{Q}/\mathbf{Z} \end{array} \tag{8.7.4.1}$$

where " q^α " means that we write $\alpha = i/N$ with $0 \le i \le N-1$ and then define q^α to be $(q^{1/N})^i$. Because the $q^{1/N}$'s are compatible, this q^α is well defined independently of the representation of α as a fraction.

THEOREM 8.7.5. *There exists a faithfully flat $\mathbf{Z}[q,q^{-1}]$-algebra R, an elliptic curve E/R, and an isomorphism of ind-group-schemes over R*

$$T_{\text{torsion}} \otimes_{\mathbf{Z}[q,q^{-1}]} R \xrightarrow{\sim} E_{\text{tors}} ,$$

such that for every $N \ge 1$, the isomorphism on N-division points

$$T[N] \otimes R \xrightarrow{\sim} E[N]$$

is compatible with e_N-pairings.

Proof. Over the faithfully flat $\mathbf{Z}[q,q^{-1}]$-algebra

$$\varinjlim_{N \ge 1} \mathbf{Z}[q,q^{-1}][X_N]/((X_N)^{N!} - q)$$

with transition maps $X_N \mapsto (X_{N+1})^{N+1}$, we have a compatible system of N'th roots of q, so T becomes isomorphic to the product $\mathbf{G}_m \times (\mathbf{Q}/\mathbf{Z})$, and T_{tors} therefore becomes isomorphic to the product

$$\mu_\infty \times \mathbf{Q}/\mathbf{Z} .$$

As this group with all its e_N-pairings begins life over $\mathbf{Z}$, we are reduced to showing

LEMMA 8.7.6. *There exists a faithfully flat $\mathbf{Z}$-algebra R, an elliptic curve E/R, and an isomorphism of ind-group-schemes over R*

$$\phi_\infty : \mu_\infty \times \mathbf{Q}/\mathbf{Z} \xrightarrow{\sim} E_{\text{tors}}$$

which is compatible with all e_N*-pairings.*

Proof. Suppose we have constructed an E/R and an isomorphism ϕ_∞. Then we can always modify ϕ_∞ by an automorphism of $\mu_\infty \times \mathbf{Q}/\mathbf{Z}$ of the form (auto. of μ_∞) $\times$ (id) to render it compatible with the e_N-pairings. For let e'_N be the pairings on the $\mu_N \times \mathbf{Z}/N\mathbf{Z}$'s obtained via ϕ_∞ from the e_N-pairings on the $E[N]$'s. Because they are alternating, we necessarily have

$$e'_N((\zeta, i), (\eta, j))$$
$$= e'_N((\zeta^j/\eta^i, 0), (1,1)) .$$

[Because R is flat over $\mathbf{Z}$, it suffices to verify this over $R[1/N]$, where it is physically obvious that the "other terms" $e'_N((\zeta,0),(\eta,0))$ and $e'_N((1,i),(1,j))$ are both equal to 1, because e'_N is alternating in the strong sense $e'_N(x,x) = 1$.] Because e'_N must define an auto-duality on $\mu_N \times \mathbf{Z}/N\mathbf{Z}$ (this being true for e_N on $E[N]$), the map

$$\mu_N \longrightarrow \mu_N$$
$$\zeta \longmapsto e'_N((\zeta,0),(1,1))$$

must be an automorphism a_N of μ_N. For variable N, the compatibilities satisfied by the e_N-pairings on the $E[N]$ give compatibilities on the e'_N-pairings which force these automorphisms a_N to fit together and provide a single automorphism a_∞ of μ_∞. Then if we compose ϕ_∞ with (a_∞^{-1} on μ_∞) $\times$ (id), we get a "new" ϕ_∞ which is compatible with e_N-pairings.

We now turn to the construction of $(E/R, \phi_\infty)$ with R faithfully flat over $\mathbf{Z}$. For each prime number p, choose an algebraically closed field $k(p)$ of characteristic p. Denote by $W(k(p))$ its ring of Witt vectors.

Then the product ring

$$\prod_p W(k(p))$$

is faithfully flat over $\mathbf{Z}$ (since it's torsion free, and non-zero mod p for every p). Thus it suffices to construct, separately for each p, an elliptic curve $E/W(k(p))$ together with a ϕ_∞.

Choose an ordinary elliptic curve E_0 over $k(p)$. Because $k(p)$ is algebraically closed, and E_0 is ordinary, there exists an isomorphism of p-divisible groups over $k(p)$

$$\phi_{0,p} : E_0[p^\infty] \simeq \mu_{p^\infty} \times \mathbf{Q}_p/\mathbf{Z}_p .$$

The prime-to-p torsion subgroup is etale, so again because $k(p)$ is algebraically closed, there exists an isomorphism over $k(p)$

$$\phi_{0,\text{ not } p} : E_0[\text{prime-to-p torsion}] \simeq \mu_{\text{prime to p}} \times \left(\prod_{\ell \neq p} \mathbf{Q}_\ell/\mathbf{Z}_\ell\right).$$

These isomorphisms together form an isomorphism over $k(p)$

$$\phi_{0,\infty} : (E_0)_{\text{torsion}} \xrightarrow{\sim} \mu_\infty \times \mathbf{Q}/\mathbf{Z} .$$

Let $E/W(k(p))$ be the *canonical lifting* à la Serre-Tate of $E_0/k(p)$. Then by its very definition, *any* isomorphism $\phi_{0,p}$ lifts to an isomorphism of p-divisible groups over $W(k(p))$:

$$\phi_p : E[p^\infty] \simeq \mu_{p^\infty} \times \mathbf{Q}_p/\mathbf{Z}_p .$$

The isomorphism $\phi_{0,\text{ not } p}$ also lifts uniquely, and the two together define the inverse of an isomorphism

$$\mu_\infty \times \mathbf{Q}/\mathbf{Z} \xrightarrow{\sim} E_{\text{torsion}} .$$ Q.E.D.

(8.8) *Relation to the Tate curve*

For any ring R, we denote by $R((q))$ the ring of finite-tailed Laurent series over R in one variable q. One knows ([Roq], [De-Ra], [K-2]) that over the ring $\mathbf{Z}((q))$ there is an elliptic curve $\mathrm{Tate}(q)$ together a nowhere vanishing invariant one-form ω_{can}, which satisfies all of the following properties T.1 through T.4.

T.1
$$\begin{cases} j(\mathrm{Tate}(q)) = \frac{1}{q} + 744 + \cdots \\ c_4(\mathrm{Tate}(q), \omega_{can}) = 1 + 240 \sum_{n\geq 1} q^n \sum_{d|n} d^3 \\ c_6(\mathrm{Tate}(q), \omega_{can}) = 1 - 504 \sum_{n\geq 1} q^n \sum_{d|n} d^5 \\ \Delta(\mathrm{Tate}(q), \omega_{can}) = q \cdot \prod_{n\geq 1} (1-q^n)^{24} . \end{cases}$$

T.2 There exists a unique isomorphism ϕ_{can} of formal Lie groups over $\mathbf{Z}((q))$

$$\phi_{can} : \widehat{\mathrm{Tate}(q)} \xrightarrow{\sim} \hat{G}_m = \hat{T}$$

under which the "standard" invariant differential dX/X on $G_m \subset T$ pulls back to ω_{can}

$$\phi_{can}^*(dX/X) = \omega_{can} .$$

T.3 For every $N \geq 1$, there exists a unique short exact sequence (as f.p.p.f. abelian sheaves) of finite flat commutative group-schemes over $\mathbf{Z}((q))$

$$0 \longrightarrow \mu_N \xrightarrow{a_N} \mathrm{Tate}(q)[N] \xrightarrow{b_N} \mathbf{Z}/N\mathbf{Z} \longrightarrow 0 ,$$

with the following properties:

T.3.a_N: for any $\mathbf{Z}((q))$-algebra R in which N is nilpotent, and any $\zeta \in \mu_N(R)$, we have

$$\phi_{can}(a_N(\zeta)) = \zeta .$$

The formula makes sense, because when N is nilpotent, a_N necessarily maps μ_N into the formal group of $\mathrm{Tate}(q)$.

T.3.b_N: for any $\mathbf{Z}((q))$-algebra R, any element $\zeta \in \mu_N(R)$, and any element $X \in \mathrm{Tate}(q)[N](R)$, we have the formula

$$e_N(a_N(\zeta), X) = \zeta^{b_N(X)} .$$

T.4 There exists a unique isomorphism of ind-group-schemes on $\mathbf{Z}((q))$

$$T_{torsion} \underset{\mathbf{Z}[q,q^{-1}]}{\otimes} \mathbf{Z}((q)) \xrightarrow{\sim} \mathrm{Tate}(q)_{torsion}$$

which is compatible with the canonical extension structures:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mu_\infty & \longrightarrow & T_{torsion} & \longrightarrow & \mathbf{Q}/\mathbf{Z} & \longrightarrow & 0 \\ & & \| & & \downarrow & & \| & & \\ 0 & \longrightarrow & \mu_\infty & \longrightarrow & \mathrm{Tate}(q)_{torsion} & \longrightarrow & \mathbf{Q}/\mathbf{Z} & \longrightarrow & 0 . \end{array}$$

[This isomorphism is unique because it is a priori indeterminate up to a $\mathbf{Z}((q))$-homomorphism from $\mathbf{Q}/\mathbf{Z}$ to μ_∞, i.e., up to an element of the one-element group

$$\varprojlim_N \mu_N(\mathbf{Z}((q))) \xleftarrow{\sim} \varprojlim_N \mu_N(\mathbf{Z}) = \{1\} .$$

It is automatically compatible with e_N-pairings, because these pairings are uniquely determined by the fact that they are alternating, and compatible with the extension-structures in the sense of (8.7.1.8).]

(8.9) *Relation with ordinary elliptic curves via the Serre-Tate parameter*

Let k be an algebraically closed field of characteristic $p > 0$, $W = W(k)$ its ring of Witt-vectors, R a complete noetherian local $W(k)$-algebra with residue field k, E/R an elliptic curve, and E_0/k its special fiber.

Because k is algebraically closed, and E_0/k is ordinary, there exists an isomorphism of ind-group-schemes over k

$$\phi_0 : \mu_\infty \times Q/Z \xrightarrow{\sim} (E_0)_{\text{torsion}} ,$$

which is compatible with all the e_N-pairings. Associated to the data $(E/R, \phi_0)$ is the "Serre-Tate parameter"

$$q(E/R, \phi_0) \in 1 + \max(R) \subset R^\times .$$

By means of the Serre-Tate parameter, we may view R as a $Z[q,q^{-1}]$-algebra:

$$q \mapsto q(E/R, \phi_0) .$$

According to the Serre-Tate theorem (cf. [K-5]), there is a *unique* isomorphism of ind-group-schemes over R

$$\phi : T_{\text{tors}} \underset{Z[q,q^{-1}]}{\otimes} R \xrightarrow{\sim} E_{\text{tors}}$$

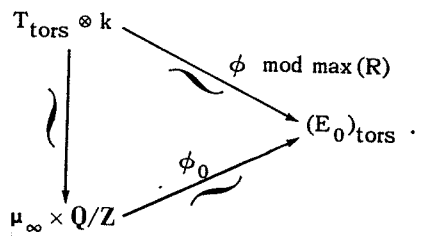
which *lift* the given

$$\phi_0 : \mu_\infty \times Q/Z \xrightarrow{\sim} (E_0)_{\text{tors}}$$

in the following sense: via the isomorphism of k-group-schemes

$$T \underset{Z[q,q^{-1}]}{\otimes} k \xrightarrow{\sim} G_m \times Q/Z$$

defined by using the canonical system $\{Y_N = 1\}$ of N'th roots of the image of q in k, we have a commutative diagram of isomorphisms



Because ϕ_0 is compatible with e_N-pairings, its lifting ϕ is also compatible [by reduction to the universal case $R = W[[q-1]]$ which is flat over Z, one sees as in the proof of (8.7.6) that the possible error appears through a section " det " over R of the constant group $\varprojlim (Z/NZ)^\times$. Since we have " det = 1 " for ϕ_0, and Spec(R) is connected, we have " det = 1 " for ϕ also].

(8.10) *Other universality properties of the groups* $T[N]$

(8.10.1) Let S be an arbitrary scheme, $N \geq 1$ an integer, and G/S a finite locally free commutative group-scheme over S of rank N^2 which is killed by N. A bilinear pairing

$$(\ , \ ) : G \times G \to \mu_N$$

(as S-group-schemes) is said to be *strongly alternating* if the following two conditions hold

S.A.1 for any S-scheme T, and any point $P \in G(T)$, we have

$$(P,P) = 1 \in \mu_N(T) .$$

S.A.2 for any S-scheme T, any finite, locally free of rank N T-subgroup-scheme $K \subset G \times T$, and any pair of points P_1, P_2 both in $K(T)$, we have

$$(P_1,P_2) = 1 \in \mu_N(T) .$$

Recall (2.8.7.1) that the e_N-pairing on $E[N]$, for E/S an elliptic curve, is strongly alternating.

(8.10.2) Clearly if $(\ ,\ )$ is strongly alternating, then for any short exact (as f.p.p.f. sheaves) sequence of S-group-schemes

$$0 \longrightarrow K \longrightarrow G \xrightarrow{\pi} K' \longrightarrow 0$$

with K and K' both locally free of rank N, there is an induced bilinear pairing of S-group-schemes

$$<\ ,\ >: K \times K' \to \mu_N$$

characterized by the following property:

for any S-scheme T, for any points $P \in K(T)$, $Q \in G(T)$, we have

$$(P,Q) = <P, \pi Q> .$$

(8.10.3) If G is given with a structure of extension of S-groups

$$0 \to \mu_N \to G \to Z/NZ \to 0 ,$$

we say that a strongly alternating bilinear form $(\ ,\ )$ on G is compatible with the extension structure if the induced pairing

$$<\ ,\ >: \mu_N \times Z/NZ \to \mu_N$$

is given by

$$<\zeta, a> = \zeta^a .$$

LEMMA 8.10.4. *Let G/S be a finite locally free commutative group-scheme of rank N^2 which is killed by N, given with an extension structure*

$$0 \to \mu_N \to G \to Z/NZ \to 0 .$$

Then there exists a unique strongly alternating $(\ ,\ )$ on G which is compatible with the extension structure.

Proof. Locally f.p.p.f. on S, the extension is splittable; then $G \simeq \mu_N \times Z/NZ$ and in this case the existence and uniqueness of $(\ ,\ )$ are obvious (cf. (8.7.1.9)); by f.p.p.f. descent, this unique $(\ ,\ )$ descends to a unique $(\ ,\ )$ on G itself. Q.E.D.

PROPOSITION 8.10.5. *Let G/S be a finite locally free commutative group-scheme of rank N^2 which is killed by N, given with an extension structure*

$$0 \longrightarrow \mu_N \longrightarrow G \xrightarrow{\pi} Z/NZ \longrightarrow 0 .$$

Let $(\ ,\ )$ denote the unique strongly alternating bilinear form on G compatible with this extension structure. Then Zariski locally on S, there exists a (non-unique) unit $q \in G_m(S) = \mathrm{Hom}_{Sch}(S, \mathrm{Spec}(Z[q,q^{-1}]))$ and a (non-unique) isomorphism of S-groups

$$T[N] \underset{Z[q,q^{-1}]}{\otimes} S \xrightarrow{\sim} G$$

which is compatible with extension structures. Any such isomorphism necessarily carries the e_N-pairing on $T[N]$ to the pairing $(\ ,\ )$ on G.

Proof. Locally f.p.p.f. on S, the exact sequence

$$0 \longrightarrow \mu_N \longrightarrow G \xrightarrow{\pi} Z/NZ \longrightarrow 0$$

splits (because N kills G, a group-theoretic splitting amounts to specifying a section g of G with $\pi(g) = 1$), so our G is an f.p.p.f. *form* of the product group-scheme $\mu_N \times Z/NZ$ with *its* extension structure. The group $T[N]$ with *its* canonical extension structure is *another* form.

The set of S-isomorphism classes of forms of $\mu_N \times Z/NZ$ *with* its extension structure is the cohomology group $H^1_{f.p.p.f.}(S, Aut)$, where *Aut* denotes the S-group-scheme whose T-valued points are

$$Aut(T) = \left\{ \begin{array}{l} \text{automorphisms } \phi \text{ of } \mu_N \times Z/NZ \text{ over } T \text{ which} \\ \text{are of the form } \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \text{ with } * \in \mathrm{Hom}_T(Z/NZ, \mu_N) \end{array} \right\} .$$

The assignment $\phi \mapsto *$ defines an isomorphism of S-group-schemes

$$Aut \xrightarrow{\sim} \mu_N ,$$

whence it is the group $H^1_{f.p.p.f.}(S, \mu_N)$ which classifies the S-forms of $\mu_N \times Z/NZ$ with its extension structure. One verifies easily that given a form G, its class in $H^1(S, \mu_N)$ is none other than the isomorphism class of the μ_N-torsor $\pi^{-1}(1)$

$$0 \longrightarrow \mu_N \longrightarrow G \xrightarrow{\pi} Z/NZ \longrightarrow 0 .$$

The Kummer sequence on S

$$0 \longrightarrow \mu_N \longrightarrow G_m \xrightarrow{N} G_m \longrightarrow 0$$

yields a long exact cohomology sequence, the relevant part of which is

$$\rightarrow G_m(S) \rightarrow H^1(S, \mu_N) \rightarrow \mathrm{Pic}(S) \rightarrow .$$

Now for any element $q \in G_m(S)$, the corresponding μ_N-torsor on S is $[N]^{-1}(q)$, i.e., it is the torsor whose T-valued points are $\{X \in G_m(T) \text{ with } X^N = q\}$. Now this is precisely the description of the inverse image of 1 in

$$0 \rightarrow \mu_N \rightarrow T[N] \rightarrow Z/NZ \rightarrow 0$$

when we view it as an S-group by the extension of scalars $S \rightarrow \mathrm{Spec}(Z[q,q^{-1}])$ which *is* $q \in G_m(S)$. Therefore a *given* G is S-isomorphic to a T[N] for some $q \in G_m(S)$ if and only if the *image* in Pic(S) of $cl(G) \in H^1(S, \mu_N)$ is the zero-element of Pic(S). But any given element of Pic(S) dies Zariski locally on S. Q.E.D.

PROPOSITION 8.10.6. *Let G/S be a finite locally free commutative group-scheme of rank N^2 which is killed by N, given with an extension structure*

$$0 \rightarrow K \rightarrow G \rightarrow E \rightarrow 0$$

where E is an etale S-group, locally for the etale topology on S isomorphic to Z/NZ. The following statements (1), (2), (3) are equivalent, and they imply statement (4):

(1) *The S-group-scheme K is toroidal, and it is S-isomorphic to the Cartier dual of E.*

(2) *There exists a strongly alternating form (,) on G which makes G auto-dual.*

(3) *There exists a strongly alternating form (,) on G whose induced pairing $< , > : K \times E \rightarrow \mu_N$ makes K and E the Cartier duals of each other.*

(4) *Locally for the etale topology on S, there exists a unit $q \in G_m(S)$ and an isomorphism $T[N] \underset{Z[q,q^{-1}]}{\otimes} S \xrightarrow{\sim} G$ respecting the given extension structures.*

Proof. Clearly we have (2) $\Longleftrightarrow$ (3) $\Longrightarrow$ (1), and we have (1) $\Longrightarrow$ (4) by the previous proposition. The implication (1) $\Longrightarrow$ (3) holds because already (4) shows that (,) exists etale locally on S, and it is unique if we require it to induce a given S-isomorphism of K with the Cartier dual of E. Then by etale descent, we get (,) on G/S. Q.E.D.

COROLLARY 8.10.7. *Let G/S be a finite locally free commutative group-scheme of rank N^2 which is killed by N, which is an extension*

$$0 \rightarrow K \rightarrow G \rightarrow E \rightarrow 0$$

where E is an etale S-group, locally (etale) on S isomorphic to Z/NZ, and where K is given with an S-isomorphism to the Cartier dual of E. Then

(1) *there exists a unique strongly alternating form (,) which induces, via < , >, the given isomorphism of K with the dual of E, and this form (,) makes G auto-dual.*

(2) *There exists a faithfully flat* S'/S, *an elliptic curve* E'/S' *and an isomorphism of* S'*-group-schemes*

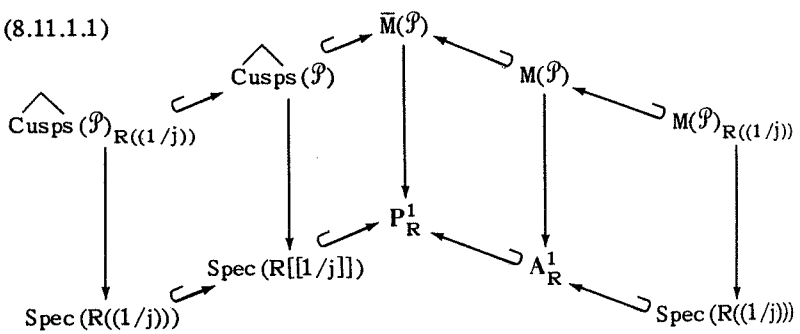
$$E'[N] \simeq G \underset{S}{\times} S'$$

which carries the e_N *pairing on* $E'[N]$ *to the pairing* $(\ ,\ )$ *on* $G \underset{S}{\times} S'$.

(8.11) *Computation of* $\widehat{\text{Cusps}}(\mathcal{P})$ *via the Tate curve*

(8.11.1) We return to the situation of an excellent noetherian regular ring R, and a relatively representable moduli problem $\mathcal{P}$ on (Ell/R) which is finite over (Ell/R), and for which $M(\mathcal{P})$ is normal near infinity. Then $\bar{M}(\mathcal{P})$ is the unique finite $\mathbf{P}^1_R$-scheme which is normal near infinity and which agrees with $M(\mathcal{P})$ over $\mathbf{A}^1_R$. Consider the cartesian diagram

(8.11.1.1)



LEMMA 8.11.2. *For* $\mathcal{P}$ *as in (8.11.1) above,* $\widehat{\text{Cusps}}(\mathcal{P})$ *is the normalization of* $R[[1/j]]$ *in the normal finite* $R((1/j))$*-scheme* $M(\mathcal{P})_{R((1/j))}$.

Proof. Because R is excellent, the morphism

$$\text{Spec}(R[[1/j]]) \to \text{Spec}(R[1/j])$$

has all its fibers geometrically regular (cf. [EGA IV, 7.8.3]). Therefore the morphism

$$\widehat{\text{Cusps}}(\mathcal{P}) \to \bar{M}(\mathcal{P})$$

has all its fibers geometrically regular. As $\bar{M}(\mathcal{P})$ is normal near infinity, it follows ([A-K 1, VII, 4.8]) that $\widehat{\text{Cusps}}(\mathcal{P})$ is normal. As $\widehat{\text{Cusps}}(\mathcal{P})$ also *finite* over $R[[1/j]]$, it is none other than the *normalization* of $R[[1/j]]$ in $M(\mathcal{P})_{R((1/j))}$. Q.E.D.

(8.11.3) For any ring R, there is a unique R-algebra isomorphism

$$R[[q]] \simeq R[[1/j]]$$

which is continuous for the adic topologies and which carries

$$j \mapsto \frac{1}{q} + 744 + \cdots$$

$$= \frac{1}{q}(1 + 744q + \cdots)$$

$$1/j \mapsto q(1 - 744q + \cdots).$$

This isomorphism induces an isomorphism

$$R((q)) \simeq R((1/j)).$$

Expressed in the coordinate q, the previous Lemma 8.11.2 becomes

LEMMA 8.11.4. *For* $\mathcal{P}$ *as in (8.11.1) above, the* $R[[q]]$*-scheme* $\widehat{\text{Cusps}}(\mathcal{P})$ *is the normalization of* $R[[q]]$ *in* $M(\mathcal{P})_{R((q))}$.

(8.11.5) Now view the Tate curve, with its scalars extended to $R((q))$, as an object $\text{Tate}(q)/R((q))$ in (Ell/R), and denote by δ the representable moduli problem on (Ell/R) which it represents. By the fundamental formula

$$j(\text{Tate}(q)) = \frac{1}{q} + 744 + \cdots$$

it is clear that

$$j(\text{Tate}(q))(j(\text{Tate}(q)) - 1728) \in \frac{1}{q^2}(1 + q\,R[[q]])$$

is invertible in $R((q))$.

(8.11.6) Let $\mathcal{P}$ be any representable moduli problem on (Ell/R), and U the open set of A^1_R where $j(j-1728)$ is invertible. We will apply to $\mathcal{P}$ and to $\mathcal{S}$ the result (8.4.4). We have just seen that $\mathcal{S} = \mathcal{S}|U$ already lies over U, so that

$$\mathcal{M}(\mathcal{P},\mathcal{S}) = \mathcal{M}(\mathcal{P},\mathcal{S})|U = \mathcal{P}_{\mathrm{Tate}(q)/R((q))}$$

$$(\mathcal{M}(\mathcal{P}) \underset{A^1_R}{\times} \mathcal{M}(\mathcal{S}))|U = \mathcal{M}(\mathcal{P}) \underset{A^1_R}{\times} \mathrm{Spec}\,(R((q)))\,,$$

and we find

PROPOSITION 8.11.7. *Let* R *be any ring,* $\mathcal{P}$ *any representable moduli problem on* (Ell/R). *Then we have a canonical morphism of* R((q))*-schemes*

$$\mathcal{P}_{\mathrm{Tate}(q)/R((q))} \to \mathcal{M}(\mathcal{P})_{R((q))}$$

which is a finite etale galois covering with group $\mathrm{Aut}\,(\mathrm{Tate}(q)/R((q)))=\pm 1$, *and so defines an isomorphism of* R((q))*-schemes*

$$(\mathcal{P}_{\mathrm{Tate}(q)/R((q))})/\pm 1 \xrightarrow{\sim} \mathcal{M}(\mathcal{P})_{R((q))}\,.$$

THEOREM 8.11.8. *Let* R *be any noetherian ring. Then the elliptic curve* Tate(q)/R((q)) *is flat over* (Ell/R).

Proof. We must show that if $\mathcal{P}$ is any representable moduli problem on (Ell/R) which is etale over (Ell/R), then the morphism

$$\mathcal{P}_{\mathrm{Tate}(q)/R((q))} \to \mathcal{M}(\mathcal{P})$$

is flat. We may factor this map as

$$\mathcal{P}_{\mathrm{Tate}(q)/R((q))} \to \mathcal{M}(\mathcal{P})_{R((q))} \to \mathcal{M}(\mathcal{P})_{R[j,1/j]} \to \mathcal{M}(\mathcal{P})\,.$$

The first map is a finite etale ± 1-torsor, by the preceding proposition. The last two maps are the extension of scalars (by $\mathcal{M}(\mathcal{P}) \to \mathrm{Spec}\,(R[j])$), of the maps

$$\mathrm{Spec}\,(R((q))) = \mathrm{Spec}\,(R((1/j))) \to \mathrm{Spec}\,(R[j,1/j]) \to \mathrm{Spec}\,(R[j])\,.$$

The second of these maps is a localization, the first is the extension of scalars (by $R[1/j] \to R[j,1/j]$) of

$$\mathrm{Spec}\,(R[[1/j]]) \to \mathrm{Spec}\,(R[1/j])\,,$$

which is flat because R is noetherian. Q.E.D.

COROLLARY 8.11.9. *Let* R *be a noetherian ring,* $\mathcal{P}$ *a relatively representable moduli problem on* (Ell/R) *which is affine over* (Ell/R), *and* G *a finite group operating on* $\mathcal{P}$. *The canonical morphism*

$$(\mathcal{P}_{\mathrm{Tate}(q)/R((q))})/G \to (\mathcal{P}/G)_{\mathrm{Tate}(q)/R((q))}$$

is an isomorphism.

Proof. A special case of (7.1.3, (3a)), in virtue of the above theorem. Q.E.D.

THEOREM 8.11.10. *Let* R *be an excellent noetherian regular ring, and* $\mathcal{P}$ *a relatively representable moduli problem on* (Ell/R) *which is finite over* (Ell/R), *and normal near infinity. Suppose either that* $\mathcal{P}$ *is representable near infinity, or that there exists a prime number* ℓ *which is invertible in* R. *Then the finite* R[[q]]*-scheme* $\widehat{\mathrm{Cusps}}\,(\mathcal{P})$ *is the normalization of* R[[q]] *in the finite normal* R((q))*-scheme*

$$(\mathcal{P}_{\mathrm{Tate}(q)/R((q))})/\pm 1\,.$$

Proof. If $\mathcal{P}$ is representable near infinity, apply (8.11.7) to $\mathcal{P}|U$. If a prime ℓ is invertible in R, then the moduli problem $[\Gamma(\ell^2)] \underset{\mathbf{Z}}{\otimes} R$ is representable and finite etale galois over (Ell/R), with galois group $G = GL(2, \mathbf{Z}/\ell^2\mathbf{Z})$. Therefore the moduli problem $\mathcal{P}' = (\mathcal{P}, [\Gamma(\ell^2)] \underset{\mathbf{Z}}{\otimes} R)$ is finite etale galois over $\mathcal{P}$ with the same galois group G. Now by the preceding corollary,

$$(\mathcal{P}'_{\mathrm{Tate}(q)/R((q))})/G \xrightarrow{\sim} \mathcal{P}_{\mathrm{Tate}(q)/R((q))}\,,$$

whence further dividing by $\pm 1 = \mathrm{Aut}(\mathrm{Tate}(q))$, we find

$$((\mathcal{P}'_{\mathrm{Tate}(q)/R((q))})/\pm 1)/G \xrightarrow{\sim} (\mathcal{P}_{\mathrm{Tate}(q)/R((q))})/\pm 1 .$$

Because normalization commutes with passage to quotients by finite groups, we get

$$\widehat{\mathrm{Cusps}}\,(\mathcal{P}')/G \xrightarrow{\sim} \text{normalization of } R[[q]] \text{ in } (\mathcal{P}_{\mathrm{Tate}(q)/R((q))})/\pm 1$$

and the result follows from (8.6.4, (3)). Q.E.D.

Chapter 9

MODULI PROBLEMS VIEWED OVER CYCLOTOMIC INTEGER RINGS

(9.1) *Generalities*

(9.1.1) Let R be a ring, and let

(9.1.1.1) $$\mathcal{F} : (\mathrm{Sch}/R) \mapsto (\mathrm{Sets})$$

be a contravariant functor which is representable by an affine R-scheme $\mathrm{Spec}(A)$. For example, $R = \mathbf{Z}$, and for any integer $N \geq 1$ the functor $\mu_N^{\times}$ "primitive N'th roots of unity" on $(\mathrm{Sch}/\mathbf{Z})$:

$$\mu_N^{\times}(S) = \text{the set of elements } \zeta \in \Gamma(S,\mathcal{O}_S) \text{ such that } \Phi_N(\zeta) = 0$$

where $\Phi_N(X) \in \mathbf{Z}[X]$ is the N'th cyclotomic polynomial. The corresponding A is the ring

$$\mathbf{Z}[\zeta_N] \overset{\mathrm{dfn}}{=\!=} \mathbf{Z}[X]/(\Phi_N(X)) .$$

(9.1.2) Now consider the moduli problem $[\mathcal{F}]$ on (Ell/R) defined by

(9.1.2.1) $$[\mathcal{F}](E/S) \overset{\mathrm{dfn}}{=\!=} \mathcal{F}(S) .$$

It is relatively representable and affine over (Ell/R). Indeed for any $E/S/R$, we have

(9.1.2.2) $$[\mathcal{F}]_{E/S} = S \underset{R}{\otimes} A .$$

Obviously the moduli problem $[\mathcal{F}]$ is *not* representable, simply because it is not rigid: the group $\mathrm{Aut}(E/S)$ operates trivially on the set $[\mathcal{F}](E/S) = \mathcal{F}(S)$.

PROPOSITION 9.1.3. *There is a canonical morphism*

$$M([\mathcal{F}]) \to \mathrm{Spec}(A[j]) ,$$

which is an isomorphism if A *is flat over* R, *or if* $6 = 2\times 3$ *is invertible in* R, *or if* 6 *is invertible in* A.

Proof. The question is local on R, so we may assume some odd prime ℓ invertible in R. Then we have, with $G = GL(2, \mathbb{F}_\ell)$,

$$\begin{aligned} M([\mathcal{F}]) &= \mathcal{M}([\mathcal{F}], [\Gamma(\ell)])/G \\ &= (\mathcal{M}(\Gamma(\ell)) \underset{R}{\otimes} A)/G \end{aligned}$$

and the canonical map

$$(\mathcal{M}(\Gamma(\ell)) \underset{R}{\otimes} A)/G \to (\mathcal{M}(\Gamma(\ell))/G) \underset{R}{\otimes} A = \mathrm{Spec}(R[j] \underset{R}{\otimes} A) .$$

This last map is an isomorphism if A is R-flat, or if the order of G is invertible in R or in A (so if $A \ni 1/6$, take $\ell = 3$, giving $\#G = 48$).

Q.E.D.

(9.1.4) Now consider a relatively representable and affine moduli problem $\mathcal{P}$ on (Ell/R), together with an $[\mathcal{F}]$-structure, i.e., a morphism of moduli problems on (Ell/R)

(9.1.4.1) $$\mathcal{P} \xrightarrow{\pi} [\mathcal{F}] ,$$

i.e., a rule which to every level $\mathcal{P}$-structure on an E/S/R attaches an $\mathcal{F}$-structure on S, compatibly with morphisms in (Ell/R). Because $\mathcal{P}$ is relatively representable, this means that for each E/S/R, we are given a morphism of S-schemes

(9.1.4.2) $$\mathcal{P}_{E/S} \to S \underset{R}{\otimes} A ,$$

i.e., for every representable problem $\mathcal{S}$ on (Ell/R), we have a morphism of R-schemes

(9.1.4.3) $$\mathcal{M}(\mathcal{P}, \mathcal{S}) \to \mathcal{M}(\mathcal{S}) \underset{R}{\otimes} A .$$

Passing to the map on coarse moduli schemes, we get a morphism of R-schemes

(9.1.4.4) $$M(\mathcal{P}) \to M([\mathcal{F}]) ,$$

which for A/R flat or $1/6 \in R$ we may interpret as an R-morphism

(9.1.4.5) $$M(\mathcal{P}) \to \mathrm{Spec}(A[j]) .$$

(9.1.5) Now consider (Ell/A). An object of this category is an E/S/A. The given structure of A-scheme on S provides (indeed "is") a *canonical* $\mathcal{F}$-structure on S (e.g., if $A = \mathbb{Z}[X]/(\Phi_N(X)) = \mathbb{Z}[\zeta_N]$, then the inverse image of $\zeta_N \overset{\mathrm{dfn}}{=\!=} X \bmod \Phi_N$ on any $\mathbb{Z}[\zeta_N]$-scheme S is the canonical primitive N'th root of unity on S we have in mind).

(9.1.6) Out of the given data

$$\mathcal{P} \xrightarrow{\pi} [\mathcal{F}] ,$$

we will now construct a new moduli problem, functorial in the original data, denoted

(9.1.6.1) $$\mathcal{P}^{\mathrm{can}} \text{ on } (\mathrm{Ell}/A) ,$$

as follows:

(9.1.6.2) $\mathcal{P}^{\mathrm{can}}(E/S/A)$ = the set of $\mathcal{P}$-structures on E/S which map by π to the *canonical* $\mathcal{F}$-structure on S.

If we denote by $f_{\mathrm{taut}} \in \mathcal{F}(A)$ the tautological $\mathcal{F}$-structure on A corresponding to the identity map in $\mathrm{Hom}_{R\text{-alg}}(A,A) = \mathcal{F}(A)$, then we can rewrite this as

$$\mathcal{P}^{\mathrm{can}}(E/S/A) = \mathcal{P}(E/S) \underset{\mathcal{F}(S)}{\times} f_{\mathrm{taut}} .$$

For example $[\mathcal{F}]^{\mathrm{can}}$ is the $[\Gamma(1)]$-moduli problem on (Ell/A).

PROPOSITION 9.1.7. *The moduli problem* $\mathcal{P}^{\mathrm{can}}$ *on* (Ell/A) *is relatively representable. It is representable if* $\mathcal{P}$ *is representable. For any representable moduli problem* $\mathcal{S}$ *on* (Ell/R), *we have a canonical isomorphism of schemes over* $\mathcal{M}(\mathcal{S}\underset{R}{\otimes}A) = \mathcal{M}(\mathcal{S})\underset{R}{\otimes}A$

$$\begin{array}{ccc} \mathcal{M}(\mathcal{P}^{\mathrm{can}}, \mathcal{S}\underset{R}{\otimes}A) & \xrightarrow{\sim} & \mathcal{M}(\mathcal{P}, \mathcal{S}) \\ \downarrow{\scriptstyle \mathrm{pr}_2} & & \downarrow{\scriptstyle (\mathrm{pr}_2, \pi)} \\ \mathcal{M}(\mathcal{S}\underset{R}{\otimes}A) & \xrightarrow{\sim} & \mathcal{M}(\mathcal{S})\underset{R}{\otimes}A\ . \end{array}$$

If $\mathcal{P}$ *is affine over* (Ell/R), *then* $\mathcal{P}^{\mathrm{can}}$ *is affine over* (Ell/A) *and we have a canonical isomorphism of coarse moduli schemes as* A[j]*-schemes*

$$\begin{array}{ccc} M(\mathcal{P}^{\mathrm{can}}) & \xrightarrow{\sim} & M(\mathcal{P}) \\ & \searrow \quad \swarrow & \\ & M([\Gamma(1)]\otimes A) \quad M([\mathcal{F}]) & \\ & \searrow \quad \swarrow & \\ & \mathrm{Spec}\,(A[j])\ . & \end{array}$$

Proof. As a moduli problem on (Ell/A), $\mathcal{P}^{\mathrm{can}}$ is a closed sub-problem of $\mathcal{P}\underset{R}{\otimes}A$. Over any E/S/A, $\mathcal{P}^{\mathrm{can}}$ is relatively represented by the fiber-product of the diagram

$$\begin{array}{ccc} \mathcal{P}_{E/S} & & \\ \downarrow & & \\ S\underset{R}{\otimes}A & \xleftarrow{(\mathrm{id},\ \mathrm{given})} & S\ . \end{array}$$

Now let $\mathcal{S}$ be a representable problem on (Ell/R), and Z an $\mathcal{M}(\mathcal{S})\underset{R}{\otimes}A$-scheme. Then Z is provided with a structure of A-scheme, and Z is provided with an elliptic curve E/Z together with an $\mathcal{S}$-structure on E/Z. To map Z as $\mathcal{M}(\mathcal{S})\otimes A$-scheme to $\mathcal{M}(\mathcal{P}, \mathcal{S})$ is to give, independently, a level $\mathcal{P}$-structure on E/Z which via π lies over the tautological $\mathcal{F}$-structure on "Z as A-scheme." But this is exactly what it means to map Z as $\mathcal{M}(\mathcal{S})\otimes A = \mathcal{M}(\mathcal{S}\otimes A)$-scheme to $\mathcal{M}(\mathcal{P}^{\mathrm{can}}, \mathcal{S}\otimes A)$.

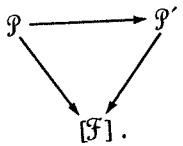
If $\mathcal{P}$ is representable, say by E/T/R, with universal element $a \in \mathcal{P}(E/T)$, then $\pi(a) \in \mathcal{F}(T) = \mathrm{Hom}_{R\text{-sch}}(T, \mathrm{Spec}\,(A))$ provides T with the structure of A-scheme, say $\tilde{T}/A$. Then on $E/\tilde{T}/A$ the "same" element a lies in $\mathcal{P}^{\mathrm{can}}(E/\tilde{T}/A)$, and the object $(E/\tilde{T}/A, a)$ visibly represents $\mathcal{P}^{\mathrm{can}}$.

If $\mathcal{P}$ is affine over (Ell/R), the fiber-product description of $\mathcal{P}^{\mathrm{can}}$ shows that $\mathcal{P}^{\mathrm{can}}$ is affine over (Ell/A). The isomorphism on coarse moduli schemes is constructed locally over R by inverting an odd prime ℓ, taking $\mathcal{S} = [\Gamma(\ell)]$, and then passing to $GL(2, F_\ell)$-invariants in the previous isomorphisms. Q.E.D.

COROLLARY 9.1.8. *Let* Q *be any property of schemes which is local for the etale topology. Then* $\mathcal{P}$ *has property* Q *if and only if* $\mathcal{P}^{\mathrm{can}}$ *has property* Q.

Proof. The problem is local on R, so we may assume an odd prime ℓ is invertible in R. Then $\mathcal{S} = [\Gamma(\ell)]\underset{Z}{\otimes}R$ is etale and surjective over (Ell/A). Therefore $\mathcal{P}$ has property Q if and only if the scheme $\mathcal{M}(\mathcal{P}, \mathcal{S})$ has property Q, while $\mathcal{P}^{\mathrm{can}}$ has property Q if the scheme $\mathcal{M}(\mathcal{P}^{\mathrm{can}}, \mathcal{S}\otimes A)$ has it. Q.E.D.

COROLLARY 9.1.9. *Let* P *be any property of morphisms of schemes which is local for the etale topology on the base. Suppose that we have two relatively representable problems* $\mathcal{P}, \mathcal{P}'$ *on* (Ell/R) *both given with maps to* $[\mathcal{F}]$, *and a morphism of moduli problems on* (Ell/R) *respecting the* $[\mathcal{F}]$*-structures:*



Then the induced map of relatively representable moduli problems on (Ell/A)

$$\mathcal{P}^{can} \to (\mathcal{P}')^{can}$$

has property P *if and only if the original* $\mathcal{P} \to \mathcal{P}'$ *has property* P. *In particular,* $\mathcal{P}^{can}$ *is of type* P *over* (Ell/A) *if and only if the morphism* $\mathcal{P} \to [\mathcal{F}]$ *has property* P.

Proof. Again the question is local on R, so we may assume an odd prime ℓ is invertible in R, and take $\mathcal{S} = [\Gamma(\ell)]$. Then $\mathcal{P} \to \mathcal{P}'$ has property P if and only if the morphism of schemes

$$\mathcal{M}(\mathcal{P}, \mathcal{S}) \to \mathcal{M}(\mathcal{P}', \mathcal{S})$$

has property P, while $\mathcal{P}^{can} \to (\mathcal{P}')^{can}$ has property P if and only if the *same* morphism of the *same* schemes

$$\mathcal{M}(\mathcal{P}^{can}, \mathcal{S} \otimes A) \to \mathcal{M}((\mathcal{P}')^{can}, \mathcal{S} \otimes A)$$

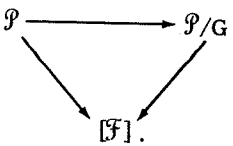
has property P.

In the special case $\mathcal{P}' = [\mathcal{F}]$, we have $[\mathcal{F}]^{can}$ = the moduli problem $[\Gamma(1)]$ on (Ell/A). Q.E.D.

COROLLARY 9.1.10. *Suppose we are given* $\mathcal{P} \xrightarrow{\pi} [\mathcal{F}]$ *as above with* $\mathcal{P}$ *affine over* (Ell/R), *and a finite group* G *acting trivially on* $[\mathcal{F}]$ *and acting on* $\mathcal{P}$ *by automorphisms which commute with* π. *Then* G *acts on* $\mathcal{P}^{can}$ *by functoriality, and we have a natural isomorphism of moduli problems on* (Ell/A)

$$(\mathcal{P}/G)^{can} \simeq \mathcal{P}^{can}/G .$$

Proof. The quotient $\mathcal{P}/G$ maps to $[\mathcal{F}]/G = [\mathcal{F}]$, so we have a G-equivariant commutative diagram



Applying the $\mathcal{P} \mapsto \mathcal{P}^{can}$ construction, we get by functoriality

$$\mathcal{P}^{can} \to (\mathcal{P}/G)^{can} ,$$

which is again G-equivariant, so defines

$$\mathcal{P}^{can}/G \to (\mathcal{P}/G)^{can} .$$

To show that this is an isomorphism, we may localize on R and so assume some odd prime ℓ is invertible in R. Then $\mathcal{S} = [\Gamma(\ell)] \underset{\mathbf{Z}}{\otimes} R$ is etale and surjective over (Ell/R), and $\mathcal{S} \underset{R}{\otimes} A$ is etale and surjective over (Ell/A). It suffices to check that the map in question induces an isomorphism of schemes:

$$\begin{array}{ccc}
\mathcal{M}(\mathcal{P}^{can}/G, \mathcal{S} \underset{R}{\otimes} A) & \longrightarrow & \mathcal{M}((\mathcal{P}/G)^{can}, \mathcal{S} \underset{R}{\otimes} A) \\
\| & & \| \\
\mathcal{M}(\mathcal{P}^{can}, \mathcal{S} \otimes A)/G & & \mathcal{M}(\mathcal{P}/G, \mathcal{S}) \\
\| & & \| \\
\mathcal{M}(\mathcal{P}, \mathcal{S})/G & = & \mathcal{M}(\mathcal{P}, \mathcal{S})/G .
\end{array}$$

Q.E.D.

(9.2) *A descent situation*

(9.2.1) Suppose that a finite group G acts freely on $\mathcal{F}$, the representable functor on (Sch/R) represented by the R-algebra A, so that A is an etale G-torsor over A^G. Then G operates freely on $[\mathcal{F}]$, and the quotient $[\mathcal{F}]/G = [\mathcal{F}/G]$ where $\mathcal{F}/G$ is the representable functor on (Sch/R) represented by A^G.

Now suppose we are given a relatively representable and affine $\mathcal{P}$ on (Ell/R), together with an action of G and a G-equivariant morphism of moduli problems on (Ell/R)

$$\mathcal{P} \xrightarrow{\pi} [\mathcal{F}] .$$

Passing to the quotient by G, we get an induced map

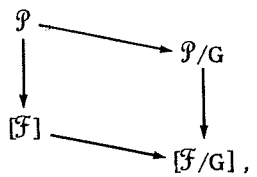
$$\mathcal{P}/G \to [\mathcal{F}/G] .$$

Thus we can speak of $\mathcal{P}^{can}$ on (Ell/A), and of $(\mathcal{P}/G)^{can}$ on (Ell/A^G).

PROPOSITION 9.2.2. *In the above situation, we have a canonical isomorphism of moduli problems on* (Ell/A)

$$(\mathcal{P}/G)^{can} \underset{A^G}{\otimes} A \xrightarrow{\sim} \mathcal{P}^{can} .$$

Proof. Applying (7.2.2), we have a cartesian diagram of moduli problems on (Ell/R)



which renders the assertion tautologous. Q.E.D.

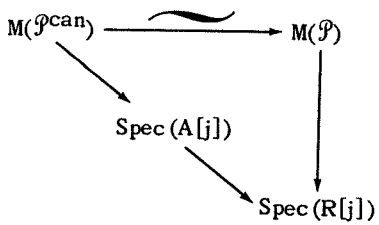
(9.3) *The situation near infinity*

PROPOSITION 9.3.1. *Let* R *be an excellent noetherian regular ring,* A *a finite flat* R*-algebra which is itself regular,* $\mathcal{F}$ *the corresponding functor on* (Sch/R) *represented by* A, *and*

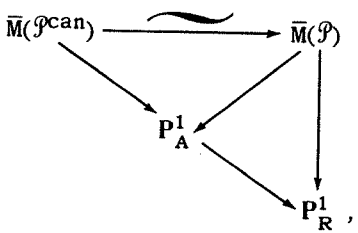
$$\mathcal{P} \xrightarrow{\pi} [\mathcal{F}]$$

a relatively representable $\mathcal{P}$ *on* (Ell/R) *together with an* $[\mathcal{F}]$*-structure. Suppose that* $\mathcal{P}$ *is finite over* (Ell/R), *and normal near infinity. Then*

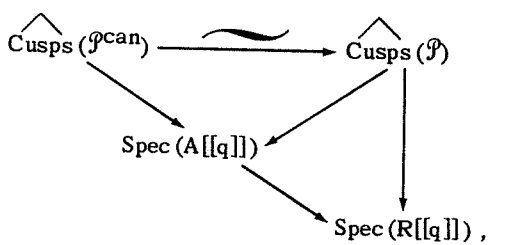
$\mathcal{P}^{can}$ *is finite over* (Ell/R), *and it is normal near infinity. The isomorphism of coarse moduli schemes*



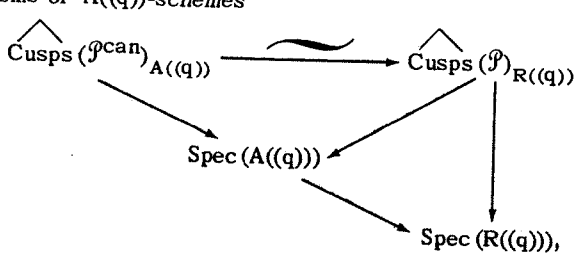
extends to an isomorphism of compactified coarse moduli schemes



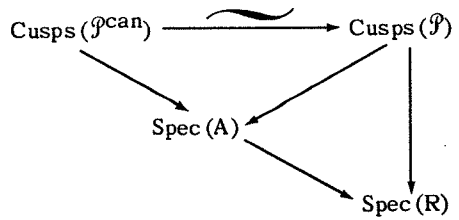
and induces isomorphisms of A[[q]]*-schemes*



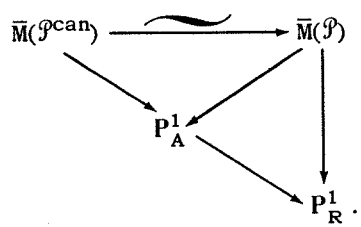
isomorphisms of A((q))*-schemes*



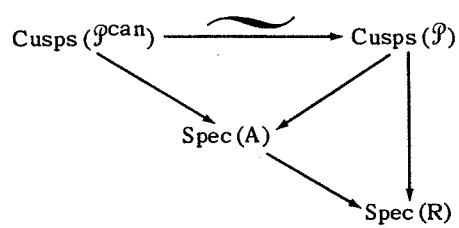
and isomorphisms of A*-schemes*



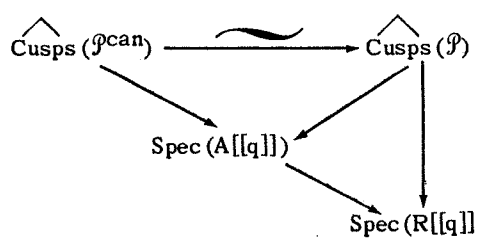
Proof. Because A is finite over R and normal, $\mathbf{P}^1_A$ is normal, and finite over $\mathbf{P}^1_R$. Therefore it is the same to normalize a neighborhood of infinity $\bar{U} \subset \mathbf{P}^1_R$ in the finite A[j]-scheme $M(\mathcal{P})$, or to normalize $\bar{U} \underset{R}{\otimes} A \subset \mathbf{P}^1_A$ in the same scheme. This gives the required isomorphism



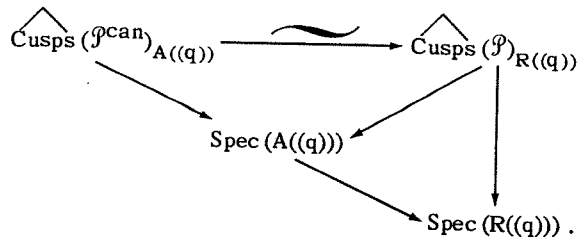
The scheme of cusps is the reduced subscheme " $1/j = 0$ ", which gives



Completing along this subscheme gives



and inverting q then gives



Q.E.D.

PROPOSITION 9.3.2. *Let* R *be an arbitrary ring,* A *a finite free* R*-algebra,* $\mathcal{F}$ *the functor on* (Sch/A) *represented by* A*, and*

$$\mathcal{P} \xrightarrow{\pi} [\mathcal{F}]$$

an $[\mathcal{F}]$*-structure on a relatively representable moduli problem* $\mathcal{P}$ *on* (Ell/R)*. Then we have an isomorphism of* A((q))*-schemes*

$$\mathcal{P}^{can}_{Tate(q)/A((q))} \xrightarrow{\sim} \mathcal{P}_{Tate(q)/R((q))} .$$

Proof. This is just (9.1.7) applied to $\mathcal{S}$ = the problem represented by Tate(q)/R((q)). Because A is a free R-module of finite rank, we have

$$R((q)) \underset{R}{\otimes} A \xrightarrow{\sim} A((q)) ,$$

so that $\mathcal{S} \underset{R}{\otimes} A$ is indeed the problem represented by Tate(q)/A((q)). Q.E.D.

(9.4) *Applications to the basic moduli problems*

(9.4.1) Let $N \geq 1$ be an integer. Consider the finite free Z-algebra

$$A = Z[\zeta_N] \overset{dfn}{=\!=} Z[X]/(\Phi_N(X)) ,$$

which represents the functor $\mu_N^{\times}$ of "primitive N'th roots of unity" on (Sch). The e_N-pairing defines a morphism of moduli problems on (Ell)

$$[\Gamma(N)] \to \mu_N^\times$$

$$E/S, (P,Q) \mapsto e_N(P,Q) \in \mu_N^\times(S) .$$

The group $GL(2, \mathbf{Z}/N\mathbf{Z})$ acts on the right on $[\Gamma(N)]$; $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ acts on the Drinfeld N-basis (P,Q) by

$$(P,Q) \mapsto (P,Q)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (P_g, Q_g) .$$

In terms of the corresponding homomorphism

$$\phi : (\mathbf{Z}/N\mathbf{Z})^2 \to E[N](S)$$

$$\phi\begin{pmatrix} x \\ y \end{pmatrix} = xP + yQ = (P,Q)\begin{pmatrix} x \\ y \end{pmatrix} ,$$

the action is

$$\phi \mapsto \phi \circ g .$$

Because e_N is alternating, we have

$$e_N(P_g, Q_g) = e_N(aP+cQ, bP+dQ) = (e_N(P,Q))^{\det(g)} .$$

(9.4.2) Let $G \subset GL(2, \mathbf{Z}/N\mathbf{Z})$ be a subgroup, and $\det(G) \subset (\mathbf{Z}/N\mathbf{Z})^\times$ the image of G under the determinant. Let $(\mathbf{Z}[\zeta_N])^{\det(G)}$ denote the subring of invariants of $\det(G)$ acting on $\mathbf{Z}[\zeta_N]$. The ring inclusion

$$\mathbf{Z}[\zeta_N]^{\det(G)} \hookrightarrow \mathbf{Z}[\zeta_N] ,$$

defines a morphism of $\mathbf{Z}$-schemes

$$\begin{array}{ccc} \mu_N^\times = \mathrm{Spec}\,(\mathbf{Z}[\zeta_N]) & \longrightarrow & \mu_N^\times/\det(G) \\ & & \| \ \mathrm{dfn} \\ & & \mathrm{Spec}\,(\mathbf{Z}[\zeta_N])/\det G \\ & & \| \\ & & \mathrm{Spec}\,((\mathbf{Z}[\zeta_N])^{\det(G)}) \end{array}$$

which by composition with

$$[\Gamma(N)] \to [\mu_N^\times]$$

defines

$$[\Gamma(N)] \to [\mu_N^\times/\det(G)] .$$

This map is *respected* by the action of G, so we obtain

$$[\Gamma(N)]/G \to [\mu_N^\times/\det(G)] .$$

Applying the $\mathcal{P} \mapsto \mathcal{P}^{can}$ construction to this situation, we obtain a relatively representable moduli problem

$$([\Gamma(N)]/G)^{can} \quad \text{on} \quad (Ell/\mathbf{Z}[\zeta_N]^{\det(G)}) .$$

(9.4.3) In all those cases where we know a direct modular description of a quotient $[\Gamma(N)]/G$ of this sort, we can give a modular description of the morphism

$$[\Gamma(N)]/G \to [\mu_N^\times/\det(G)] ,$$

and consequently we can give a directly modular description of the moduli problem $([\Gamma(N)]/G)^{can}$ on $(Ell/\mathbf{Z}[\zeta_N]^{\det(G)})$. Here is a short list of such descriptions:

(9.4.3.1) $N \geq 1$ arbitrary, G trivial. $[\Gamma(N)]^{can}$ is the moduli problem on $(Ell/\mathbf{Z}[\zeta_N])$ defined by

$$E/S/\mathbf{Z}[\zeta_N] \mapsto \text{Drinfeld N-bases } (P,Q) \text{ on } E/S \text{ with } e_N(P,Q) = \zeta_N .$$

(9.4.3.2) $N \geq 1$ arbitrary, $G = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ the upper unipotent subgroup. The quotient $[\Gamma(N)]/G$ is $[\text{bal. } \Gamma_1(N)]$, and $[\text{bal. } \Gamma_1(N)]^{can}$ is the moduli problem on $(Ell/\mathbf{Z}[\zeta_N])$ defined by

$E/S/\mathbf{Z}[\zeta_N] \mapsto$ dual cyclic N-isogenies over S

P; $E \underset{\pi^t}{\overset{\pi}{\rightleftarrows}} E'$; P' together with

generators P of $\operatorname{Ker}\pi$, P' of

$\operatorname{Ker}\pi^t$, whose canonical pairing

is $\langle P, P' \rangle = \zeta_N$.

(9.4.3.3) $N \geq 1$ arbitrary, $G = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$. The quotient $[\Gamma(N)]/G$ is $[\Gamma_1(N)]$, but $\det(G) = (\mathbf{Z}/N\mathbf{Z})^\times$, so $(\mathbf{Z}[\zeta_N])^{\det G} = \mathbf{Z}$, and $[\Gamma_1(N)]^{\mathrm{can}}$ is just $[\Gamma_1(N)]$, on (Ell/Z).

(9.4.3.4) $N \geq 1$ arbitrary, $G = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$. The quotient is $[\Gamma_0(N)]$, but again $\det(G) = (\mathbf{Z}/N\mathbf{Z})^\times$, so $[\Gamma_0(N)]^{\mathrm{can}}$ is just $[\Gamma_0(N)]$, on (Ell/Z).

(9.4.3.5) $N \geq 1$ arbitrary, d a divisor of N, G the subgroup of all matrices congruent mod d to the identity. Then $\det(G)$ is the subgroup $(1+(d)) \cap (\mathbf{Z}/N\mathbf{Z})^\times$, the quotient $[\Gamma(N)]/G$ is $[\Gamma(d)]$, and $[\Gamma(d)]^{\mathrm{can}}$ is the moduli problem on $(\mathrm{Ell}/\mathbf{Z}[\zeta_d])$ described in 1 above, with N replaced by d.

(9.4.3.6) $N = p^n$, a,b two integers in $[0,n]$, $G_{a,b}$ the subgroup of all invertible matrices of the form

$$\begin{pmatrix} 1+(p^a) & * \\ 0 & 1+(p^b) \end{pmatrix}.$$

Then $\det(G)$ is the subgroup $1+(p^{\min(a,b)})$ of $(\mathbf{Z}/p^n\mathbf{Z})^\times$, and $[\Gamma(p^n)]/G_{a,b}$ is $[\Gamma_0(p^n); a,b]$. The problem $[\Gamma_0(p^n); a,b]^{\mathrm{can}}$ on $(\mathrm{Ell}/\mathbf{Z}[\zeta_{p^{\min(a,b)}}])$ is

$E/S/\mathbf{Z}[\zeta_{p^{\min(a,b)}}] \mapsto$ dual cyclic p^n isogenies together with generators of the last a-step (resp. b-step) parts of their standard factorization

$$E = E_0 \underset{\lambda_{1,0}}{\overset{\pi_{0,1}}{\rightleftarrows}} \cdots \underset{\lambda_{n,n-1}}{\overset{\pi_{n-1,n}}{\rightleftarrows}} E_n$$

P_{n-a} : generator of $\operatorname{Ker}(\pi_{n-a,n})$

Q_b : generator of $\operatorname{Ker}(\lambda_{b,0})$,

such that

if $a \leq b$, $\zeta_{p^a} = \langle P_{n-a}, p^{a-b}\pi_{b,n}Q_b \rangle_{\pi_{n-a,n}}$

if $b \leq a$, $\zeta_{p^b} = \langle p^{a-b}\lambda_{n-a,0}P_{n-a}, Q_b \rangle_{\pi_{0,b}}$.

(9.4.3.7) N_1, N_2 two relatively prime integers, $G_1 \subset GL(2, \mathbf{Z}/N_1\mathbf{Z})$ and $G_2 \subset GL(2, \mathbf{Z}/N_2\mathbf{Z})$ subgroups such that the quotients $\mathcal{P}_1 = [\Gamma(N_1)]/G_1$ and $\mathcal{P}_2 = [\Gamma(N_2)]/G_2$ are both flat over (Ell). Then the simultaneous problem $\mathcal{P} = (\mathcal{P}_1, \mathcal{P}_2)$ is the quotient of $[\Gamma(N_1N_2)]$ by the product subgroup $G_1 \times G_2$ of $GL(2, \mathbf{Z}/N_1N_2\mathbf{Z})$, the ring $A = (\mathbf{Z}[\zeta_N])^{\det G}$ is the tensor product over $\mathbf{Z}$ of the rings $A_i = (\mathbf{Z}[\zeta_{N_i}])^{\det(G_i)}$ for $i = 1,2$, and $\mathcal{P}^{\mathrm{can}}$ on (Ell/A) is the simultaneous problem

$$(\mathcal{P}_1^{\mathrm{can}} \underset{A_1}{\otimes} A, \ \mathcal{P}_2^{\mathrm{can}} \underset{A_2}{\otimes} A).$$

Chapter 10

THE CALCULUS OF CUSPS AND COMPONENTS VIA THE GROUPS T[N], AND THE GLOBAL STRUCTURE OF THE BASIC MODULI PROBLEMS

(10.1) *Motivation*

We have already seen that the problem of analyzing the structure near infinity of a relatively representable $\mathcal{P}$ on (Ell/R) is essentially the problem of "computing" the R((q))-scheme

$$\mathcal{P}_{\mathrm{Tate}(q)/R((q))},$$

with its action of the group $\pm 1 = \mathrm{Aut}(\mathrm{Tate}(q)/R((q)))$.

When $\mathcal{P}$ is a problem of level N, i.e., when $\mathcal{P} = \mathcal{F} \circ [N]$ for some relatively representable moduli problem $\mathcal{F}$ on (FLFG/R), (cf. 4.14.2) then we have

$$\mathcal{P}_{\mathrm{Tate}(q)/R((q))} = \mathcal{F}_{\mathrm{Tate}(q)[N]/R((q))}$$

with ± 1 operating on $\mathcal{F}$ as the automorphism ± 1 of $\mathrm{Tate}(q)[N]/R((q))$.

We have already seen that for any integer $N \geq 1$, the group Tate(q)[N] over R((q)) with its e_N-pairing, is isomorphic to the group

$$T[N] \underset{Z[q,q^{-1}]}{\otimes} R((q)), \text{ with its } e_N\text{-pairing}$$

obtained from $T[N]/Z[q,q^{-1}]$ by extension of scalars. Thus we have

$$\mathcal{P}_{\mathrm{Tate}(q)/R((q))} = (\mathcal{F}_{T[N]/R[q,q^{-1}]}) \underset{R[q,q^{-1}]}{\otimes} R((q)).$$

In this chapter we will explicitly calculate

$$\mathcal{F}_{T[N]/R[q,q^{-1}]}$$

for various mixes of the basic moduli problems over Z and their "canonical" incarnations as moduli problems over cyclotomic integer rings. As explained above, these calculations will reveal the structure near infinity of the moduli problems in question (cf. 10.8).

By combining this information with two other ingredients,

(1) the homogeneity principle, (which already played so large a role in Chapter 5),

(2) the *transcendental* description of our moduli spaces as quotients of the upper-half plane, (a description which we have up to now avoided), used in the proof of 10.9.2,

we obtain a good picture of the global structure of our moduli schemes (cf. 10.9 through 10.13).

We will see later, in Chapter 13, that the calculations (10.2 - 10.8) of this chapter also reveal the structure of the reductions mod p of these same moduli problems.

(10.2) *Analysis of* $[\Gamma(N)]$

(10.2.1) Over any base S, consider a finite locally free commutative group-scheme G/S of rank N^2 which is killed by N, and which is *given* as an extension

$$0 \longrightarrow \mu_N \longrightarrow G \xrightarrow{\pi} Z/N \longrightarrow 0.$$

Suppose we are given a $\Gamma(N)$-structure on G/S, which we will view as a homomorphism of S-groups

$$\phi : (Z/NZ)^2 \to G$$

which is a "$(Z/NZ)^2$-generator" of G (cf. 1.10.5). The corresponding Drinfeld N-basis (P,Q) of G/S is related to ϕ by

$$\phi\begin{pmatrix}1\\0\end{pmatrix} = P, \quad \phi\begin{pmatrix}0\\1\end{pmatrix} = Q$$

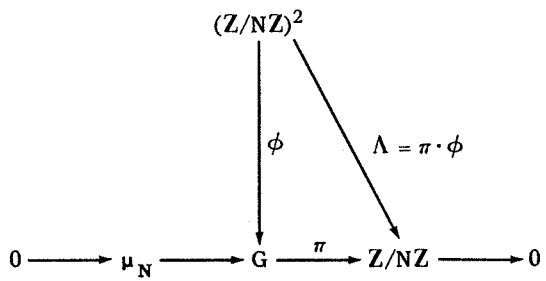
$$\phi\begin{pmatrix}x\\y\end{pmatrix} = xP + yQ = (P,Q)\begin{pmatrix}x\\y\end{pmatrix}.$$

If more than one $\Gamma(N)$-structure is in play, we will write

$$(P_\phi, Q_\phi)$$

for the Drinfeld N-basis corresponding to a particular ϕ.

LEMMA 10.2.2. *The composite homomorphism* $\Lambda = \pi \cdot \phi$



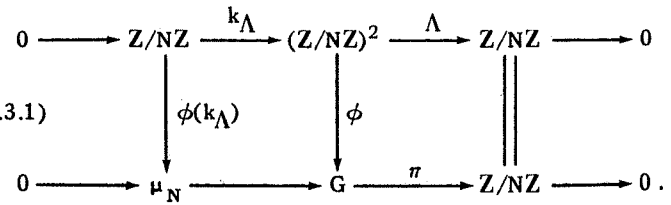
is surjective, and its kernel $\mathrm{Ker}(\Lambda) \subset (\mathbf{Z}/N\mathbf{Z})^2$ *is canonically isomorphic to* $\mathbf{Z}/N\mathbf{Z}$, *with canonical generator* k_Λ.

Proof. That Λ is surjective is a special case of (1.11.2). Its kernel $\mathrm{Ker}(\Lambda)$ is therefore a finite etale subgroup of $(\mathbf{Z}/N\mathbf{Z})^2$, so constant on each connected component of S. The quotient group $(\mathbf{Z}/N\mathbf{Z})^2/\mathrm{Ker}(\Lambda)$ is given as isomorphic to $\mathbf{Z}/N\mathbf{Z}$. Therefore $\mathrm{Ker}(\Lambda)$ must be a cyclic group of order N (elementary divisors), and it has a canonical generator k_Λ determined by the requirement that for any vector $\ell \in (\mathbf{Z}/N\mathbf{Z})^2$,

$$\det(k_\Lambda, \ell) = \Lambda(\ell)\,. \qquad \text{Q.E.D.}$$

(10.2.3) In view of the lemma, we can uniquely complete the above diagram to a commutative diagram

(10.2.3.1)



According to (1.11.2), $\phi(k_\Lambda)$ will necessarily be a *generator* of μ_N.

PROPOSITION 10.2.4. *For each* Λ *in* $\mathrm{Hom\,Surj}((\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}/N\mathbf{Z})$, *let* k_Λ *denote the canonical generator of* $\mathrm{Ker}(\Lambda)$, *defined by the requirement that*

$$\det(k_\Lambda, \ell) = \Lambda(\ell)$$

for all $\ell \in (\mathbf{Z}/N\mathbf{Z})^2$. *Choose a vector*

$$\ell_\Lambda \in (\mathbf{Z}/N\mathbf{Z})^2\,,$$

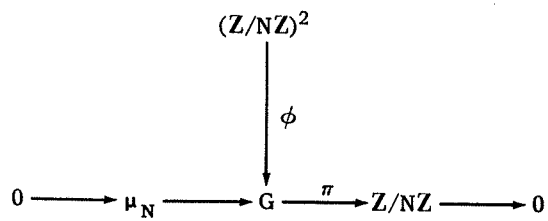
such that

$$\Lambda(\ell_\Lambda) = 1\,.$$

Let G/S *be as above, with* S *connected. Then*

(1) *If* ϕ *is a* $\Gamma(N)$*-structure on* G/S, *then* $\pi \cdot \phi = \Lambda$ *lies in* $\mathrm{Hom\,Surj}((\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}/N\mathbf{Z})$, $\phi(k_\Lambda)$ *is a primitive* N*'th root of unity in* $\mu_N(S)$, *and* $\phi(\ell_\Lambda) \in G(S)$ *has* $\pi\phi(\ell_\Lambda) = 1 \in \mathbf{Z}/N\mathbf{Z}$.

(2) *Given* $\Lambda \in \mathrm{Hom\,Surj}((\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}/N\mathbf{Z})$, *consider the oriented basis* k_Λ, ℓ_Λ *of* $(\mathbf{Z}/N\mathbf{Z})^2$. *A homomorphism* ϕ *of* S*-groups*



is a $\Gamma(N)$*-structure with* $\pi \cdot \phi = \Lambda$ *if and only if both of the following conditions are satisfied:*

$$\begin{cases} \phi(k_\Lambda) \text{ lies in } \mu_N(S), \text{ and is a primitive N'th root of unity.} \\ \phi(\ell_\Lambda) \text{ lies in } G(S), \text{ and } \pi(\phi(\ell_\Lambda)) = 1 \text{ in } \mathbf{Z}/N\mathbf{Z}. \end{cases}$$

Proof. Immediate from (1.11.2). Q.E.D.

COROLLARY 10.2.5. *Let* S *be an arbitrary scheme,* G/S *a finite locally free* S*-group killed by* N *given with an f.p.p.f. exact sequence*

$$0 \longrightarrow \mu_N \longrightarrow G \xrightarrow{\pi} \mathbf{Z}/N\mathbf{Z} \longrightarrow 0 .$$

Let $G_1 \subset G$ *denote the closed subscheme* $\pi^{-1}(1)$, *so that* G_1 *is a* μ_N*-torsor on* S. *Then we have a canonical isomorphism of* S*-schemes*

$$[\Gamma(N)]_{G/S} \xrightarrow{\sim} \coprod_{\Lambda \in \mathrm{Hom\ Surj}((\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}/N\mathbf{Z})} \mathbf{Z}[\zeta_N] \otimes_{\mathbf{Z}} G_1 .$$

whose description in terms of T*-valued points, for any connected* S*-scheme* T, *is given by*

$$\phi \mapsto (\pi \cdot \phi, \phi(k_\Lambda), \phi(\ell_\Lambda)) .$$

The $\Gamma(N)$*-structure*

$$\phi \leftrightarrow (\Lambda, \zeta, X \in G_1(T)) ,$$

with

$$\begin{cases} \phi(k_\Lambda) = \zeta \\ \phi(\ell_\Lambda) = X \end{cases}$$

will sometimes be denoted

$$\phi \leftrightarrow (\Lambda_\phi, \zeta_\phi, X_\phi) .$$

(10.3) *Group action*

We now give the explicit description of the right action of the group $GL(2, \mathbf{Z}/N\mathbf{Z}) = \mathrm{Aut}((\mathbf{Z}/N\mathbf{Z})^2)$ on the scheme $[\Gamma(N)]_{G/S}$. The action is defined by

$$(\phi, g) \mapsto \phi \circ g . \tag{10.3.1}$$

LEMMA 10.3.2. *Under the right action* $\phi \mapsto \phi \circ g$ *of* $GL(2, \mathbf{Z}/N\mathbf{Z})$ *on* $[\Gamma(N)]_{G/S}$, *we have*

(1) $\Lambda_{\phi g} = \Lambda_\phi \circ g$,

(2) $\ell_{\Lambda \cdot g} = g^{-1}(\ell_\Lambda) + n(g, \Lambda)\, g^{-1}(k_\Lambda)$ *for some* $n(g, \Lambda) \in \mathbf{Z}/N\mathbf{Z}$,

(3) $k_{\Lambda \cdot g} = \det(g)\, g^{-1}(k_\Lambda)$, $\mathrm{Ker}(\Lambda g) = g^{-1}(\mathrm{Ker}(\Lambda))$,

(4) $\zeta_{\phi g} = (\zeta_\phi)^{\det(g)}$,

(5) $X_{\phi g} = (\zeta_\phi)^{n(g,\Lambda)} X_\phi$.

Proof. By definition, $\Lambda_\phi = \pi \circ \phi$, whence $\Lambda_{\phi g} = \pi \circ \phi \circ g = \Lambda_\phi \circ g$. By definition, ℓ_Λ is a chosen vector one for each Λ, with $\Lambda(\ell_\Lambda) = 1$. Therefore $g^{-1}(\ell_\Lambda)$ is a candidate for $\ell_{\Lambda \cdot g}$, so their difference must lie in $\mathrm{Ker}(\Lambda g) = g^{-1}\mathrm{Ker}(\Lambda)$. The vector $k_{\Lambda g}$ is characterized by the properties

$$\det(k_{\Lambda g}, \ell_{\Lambda g}) = 1 , \quad k_{\Lambda g} \in \mathrm{Ker}(\Lambda g) .$$

Therefore $k_{\Lambda g}$ is a $(\mathbf{Z}/N\mathbf{Z})^\times$-multiple of the obvious generator $g^{-1}(k_\Lambda)$ of $\mathrm{Ker}(\Lambda g)$, say $k_{\Lambda g} = a\, g^{-1}(k_\Lambda)$. To compute a, we write

$$\begin{aligned} 1 = \det(k_{\Lambda g}, \ell_{\Lambda g}) &= \det(a\, g^{-1}(k_\Lambda), g^{-1}(\ell_\Lambda)) \\ &= a \det(g)^{-1} \det(k_\Lambda, \ell_\Lambda) \\ &= a \det(g)^{-1} . \end{aligned}$$

By definition

$$\begin{aligned} \zeta_{\phi g} = \phi g(k_{\Lambda g}) &= \phi g(\det(g)\, g^{-1}(k_\Lambda)) \\ &= \phi(k_\Lambda)^{\det(g)} \\ &= (\zeta_\phi)^{\det(g)} . \end{aligned}$$

Similarly, we have

$$\begin{aligned} X_{\phi g} = \phi g(\ell_\Lambda) &= \phi g(g^{-1}(\ell_\Lambda) + n(g, \Lambda)\, g^{-1}(k_\Lambda)) \\ &= \phi(\ell_\Lambda + n(g, \Lambda)\, k_\Lambda) \\ &= (\zeta_\phi)^{n(g,\Lambda)} X_\phi . \end{aligned}$$

Q.E.D.

(10.3.3) For each $\Lambda \in \mathrm{Hom\ Surj}((\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}/N\mathbf{Z})$, let $\mathrm{Fix}(\Lambda)$ be the subgroup of $\mathrm{GL}(2, \mathbf{Z}/N\mathbf{Z})$ consisting of all g such that $\Lambda g = \Lambda$. This group acts stably on the Λ-component of $[\Gamma(N)]_{G/S}$,

$$\mathbf{Z}[\zeta_N] \underset{\mathbf{Z}}{\otimes} G_1 ,$$

by

$$(\zeta, X) \mapsto (\zeta^{\det(g)}, \zeta^{n(g,\Lambda)} X) .$$

(10.3.4) The group $\mathrm{Fix}(\Lambda)$ is isomorphic to the subgroup $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$ of $\mathrm{GL}(2, \mathbf{Z}/N\mathbf{Z})$, by the construction

$$g \in \mathrm{Fix}(\Lambda) \mapsto \begin{pmatrix} \det(g) & n(g,\Lambda) \\ 0 & 1 \end{pmatrix} .$$

[Of course, for Λ the homomorphism $\binom{x}{y} \mapsto y = (0,1)\binom{x}{y}$, $\mathrm{Fix}(\Lambda)$ is *already* the subgroup $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$ of $\mathrm{GL}(2, \mathbf{Z}/N\mathbf{Z})$; our $(k_\Lambda, \ell_\Lambda)$-construction is just an explicit incarnation of the fact that $\mathrm{GL}(2, \mathbf{Z}/N\mathbf{Z})$ acts transitively on Hom Surj, so that every $\mathrm{Fix}(\Lambda)$ is conjugate to the "standard" one. From this point of view, the set $\mathrm{Hom\ Surj}((\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}/N\mathbf{Z})$ is the homogeneous space

(10.3.4.1) $$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \backslash \mathrm{GL}(2, \mathbf{Z}/N\mathbf{Z}) \xrightarrow{\sim} \mathrm{Hom\ Surj}((\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}/N\mathbf{Z})$$

if we take $\Lambda = (0,1)$ as base point.]

COROLLARY 10.3.5. *Let Γ be an arbitrary subgroup of $\mathrm{GL}(2, \mathbf{Z}/N\mathbf{Z})$. Let $\{\Lambda_i\}$ be a set of representatives in $\mathrm{Hom\ Surj}((\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}/N\mathbf{Z})$ of the orbit space*

$$\mathrm{Hom\ Surj}/\Gamma$$

for the right action $(\Lambda \mapsto \Lambda \circ g)$ of Γ on $\mathrm{Hom\ Surj}((\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}/N\mathbf{Z})$.

Let S be an arbitrary scheme, G/S a finite locally free S-group killed by N given with an f.p.p.f. exact sequence

$$0 \longrightarrow \mu_N \longrightarrow G \xrightarrow{\pi} \mathbf{Z}/N\mathbf{Z} \longrightarrow 0 .$$

Then the quotient of the S-scheme $[\Gamma(N)]_{G/S}$ by the given subgroup Γ of $\mathrm{GL}(2, \mathbf{Z}/N\mathbf{Z})$ is given by a canonical isomorphism

$$([\Gamma(N)]_{G/S})/\Gamma \simeq \coprod_{\Lambda_i \in \mathrm{Hom\ Surj}/\Gamma} (\mathbf{Z}[\zeta_N] \underset{\mathbf{Z}}{\otimes} G_1)/\Gamma \cap \mathrm{Fix}(\Lambda_i) .$$

(10.4) *Canonical problems*

LEMMA 10.4.1. *Let G/S be a finite locally free commutative group-scheme of rank N^2, killed by N, given with a strongly alternating autoduality*

$$(\ , \ ) : G \times G \to \mu_N ,$$

which after some faithfully flat base change $S' \to S$ becomes isomorphic to $(E'[N], e_N)$ for some elliptic curve E'/S'. Then for any $\Gamma(N)$-structure $\phi = (P, Q)$ on G/S, the pairing-value

$$(P, Q) \in \mu_N(S)$$

is a primitive N'th root of unity on S.

Proof. Because S' is faithfully flat over S, to verify that (P, Q) is a zero of $\Phi_N(X)$ in $\Gamma(S, \mathcal{O}_S)$ it suffices to do so over S', where the result is already known (5.6.3). Q.E.D.

(10.4.2) Let H be a subgroup of $(\mathbf{Z}/N\mathbf{Z})^\times$ and A the corresponding subring of $\mathbf{Z}[\zeta_N]$:

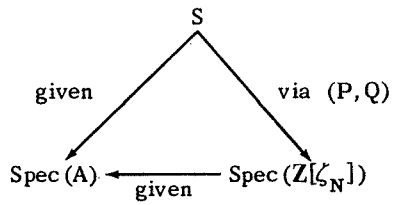
$$A = (\mathbf{Z}[\zeta_N])^H \subset \mathbf{Z}[\zeta_N] .$$

Let S be any A-scheme, $(G/S, (\ , \ ))$ as in the above lemma. We say that a $\Gamma(N)$-structure $\phi = (P, Q)$ on G/S is "A-canonical" if the structure of $\mathbf{Z}[\zeta_N]$-scheme which S acquires from the primitive N'th root of unity

$$(P, Q) \in \mu_N^\times(S)$$

is compatible with its *given* structure of A-scheme, and with the *given* inclusion of A in $\mathbf{Z}[\zeta_N]$; in other words, A-canonicity of (P, Q) means

that the diagram



commutes.

We denote by $[\Gamma(N)]^{A-can}$ the corresponding moduli problem on (Ell/A).

THEOREM 10.4.3. *Let* H *be a subgroup of* $(\mathbf{Z}/N\mathbf{Z})^\times$, A *the subring* $(\mathbf{Z}[\zeta_N])^H$ *of* $\mathbf{Z}[\zeta_N]$. *Let* S *be an arbitrary* A*-scheme, and* G/S *a finite locally free commutative* S*-group of rank* N^2, *killed by* N, *given with an f.p.p.f. short exact sequence*

$$0 \to \mu_N \to G \to \mathbf{Z}/N\mathbf{Z} \to 0 .$$

Recall that G/S *carries a unique strongly alternating autoduality* (,) *whose associated* $< , > : \mu_N \times \mathbf{Z}/N\mathbf{Z} \to \mu_N$ *is the standard pairing* $<\zeta, a> = \zeta^a$ *(cf. 8.10.4), so we can speak of* A*-canonical* $\Gamma(N)$*-structures on* (G/S, (,)).

(1) *We have a canonical isomorphism of* S*-schemes*

$$([\Gamma(N)]^{A-can})_{G/S} = \coprod_{\text{Hom Surj}(\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}/N\mathbf{Z})} \mathbf{Z}[\zeta_N] \otimes_A G_1 .$$

(2) *For any subgroup* $\Gamma \subset GL(2, \mathbf{Z}/N\mathbf{Z})$ *such that*

$$\det(\Gamma) \subset H ,$$

let $\{\Lambda_i\}$ *be a set of representatives for the orbit space*

$$\text{Hom Surj}/\Gamma .$$

Then we have a canonical isomorphism of S*-schemes*

$$(([\Gamma(N)]^{A-can})_{G/S})/\Gamma \simeq \coprod_{\Lambda_i \in \text{Hom Surj}/\Gamma} (\mathbf{Z}[\zeta_N] \otimes_A G_1)/\Gamma \cap \text{Fix}(\Lambda_i) .$$

Proof. Exactly the same as for its Z-analogues (10.2.5) and (10.3.5). Q.E.D.

(10.5) *Explication for* T[N]

THEOREM 10.5.1. *Let* H *be a subgroup of* $(\mathbf{Z}/N\mathbf{Z})^\times$, A *the subring* $\mathbf{Z}[\zeta_N]^H$ *of* $\mathbf{Z}[\zeta_N]$. *For any* $A[q,q^{-1}]$*-algebra* B, *denote by* T[N]/B *the group-scheme*

$$T[N] \otimes_{\mathbf{Z}[q,q^{-1}]} B ,$$

with its canonical extension structure and e_N*-pairing. Then*

(1) *we have a canonical isomorphism of* B*-schemes*

$$([\Gamma(N)]^{A-can})_{T[N]/B} = \coprod_{\text{Hom Surj}(\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}/N)} \text{Spec}(\mathbf{Z}[\zeta_N] \otimes_A (B[X]/(X^N = q))) .$$

(2) *For any subgroup* $\Gamma \subset GL(2, \mathbf{Z}/N\mathbf{Z})$ *with* $\det(\Gamma) \subset H$, *let* $\{\Lambda_i\}$ *be a set of representatives for* Hom Surj/Γ. *Then we have a canonical isomorphism of* B*-schemes*

$$(([\Gamma(N)]^{A-can})_{T[N]/B})/\Gamma =$$

$$\coprod_{\Lambda_i \in \text{Hom Surj}((\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}/N\mathbf{Z})/\Gamma} \text{Spec}((\mathbf{Z}[\zeta_N] \otimes_A (B[X]/(X^N = q)))^{\Gamma \cap \text{Fix}(\Lambda_i)}) .$$

Proof. For $G = T[N]$, the μ_N-torsor G_1, cf. (10.2.5), is just $X^N = q$, and we apply (10.4.3). Q.E.D.

(10.6) *Cusp-labels and component-labels*

Let Γ be a subgroup of $GL(2, \mathbf{Z}/N\mathbf{Z})$. The orbit space

$$\text{Hom Surj}((\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}/N\mathbf{Z})/\Gamma$$

we propose to call the space of cusp-labels for $[\Gamma(N)]/\Gamma$, or, sometimes, for Γ. If we fix the base-point $\Lambda\begin{pmatrix}x\\y\end{pmatrix} = y = (0,1)\begin{pmatrix}x\\y\end{pmatrix}$ for Hom Surj, this space of cusp-labels becomes the double coset space

$$\begin{pmatrix}* & *\\ 0 & 1\end{pmatrix}\backslash GL(2, Z/NZ)/\Gamma .$$

If we view $(Z/NZ)^\times$ as the central subgroup of *scalars* of $GL(2, Z/NZ)$, then we can form the orbit space

$$(Z/NZ)^\times\backslash \text{Hom Surj}((Z/NZ)^2, Z/NZ)/\Gamma .$$

As a double coset space, via base-point $\Lambda = (0,1)$, this space is

$$\begin{pmatrix}* & *\\ 0 & *\end{pmatrix}\backslash GL(2, Z/NZ)/\Gamma .$$

We call this orbit space the space of *component-labels* for Γ, or for $[\Gamma(N)]/\Gamma$. There is a natural projection

$$\begin{array}{c}\text{cusp-labels}\\ \downarrow\\ \text{component-labels},\end{array}$$

whose geometrical significance will become clear later when we reduce mod p, and which will explain the "component-label" terminology.

(10.7) *Some combinatorial lemmas*

LEMMA 10.7.1. *If* $N \geq 3$, *then* -1 *acts without fixed points on* Hom Surj$((Z/NZ)^2, Z/NZ)$.

Proof. If $\Lambda = (a, b)$ is fixed by -1, $2a = 2b = 0$. As (a, b) is primitive, $2 = 0$ in Z/NZ. Q.E.D.

LEMMA 10.7.2. *Let* N *be an odd integer, and* Γ *a subgroup of* $SL(2, Z/NZ)$. *Then either* Γ *contains the scalar* -1, *or* -1 *operates without fixed points on the space* Hom Surj $/\Gamma$ *of cusp-labels for* Γ.

Proof. Suppose that -1 fixes the coset $\Lambda\Gamma$ for some $\Lambda \in$ Hom Surj. This means that

$$-\Lambda = \Lambda \circ \gamma \quad \text{for some} \quad \gamma \in \Gamma .$$

In the basis k_Λ, ℓ_Λ of $(Z/NZ)^2$, the matrix of γ is of the form

$$\begin{pmatrix}* & *\\ 0 & -1\end{pmatrix}.$$

Because $\gamma \in \Gamma \subset SL$, the matrix must be of the form

$$\gamma = \begin{pmatrix}-1 & -x\\ 0 & -1\end{pmatrix}$$

for some $x \in Z/NZ$. Then

$$\gamma^2 = \begin{pmatrix}1 & 2x\\ 0 & 1\end{pmatrix}.$$

Because N is odd, there exists $n \geq 1$ with $2n \equiv 1 \bmod N$, ($n=(N+1)/2$ for example). So

$$\gamma^{2n} = \begin{pmatrix}1 & 2nx\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix} = -\gamma ,$$

and therefore -1 lies in Γ. Q.E.D.

LEMMA 10.7.3. *Let* $N = N_1N_2$ *with* N_1 *and* N_2 *relatively prime integers. Let* Γ *be a subgroup of* $GL(2, Z/NZ)$ *which is of the form* $\Gamma_1 \times \Gamma_2$, *with* Γ_i *a subgroup of* $GL(2, Z/N_iZ)$, $i = 1, 2$, *when we view* $GL(2, Z/NZ)$ *as the product of the* $GL(2, Z/N_iZ)$. *Then*:

(1) *We have a natural bijection*

$$(\textit{cusp-labels for } \Gamma) \xrightarrow{\sim} (\textit{cusp-labels for } \Gamma_1) \times (\textit{cusp-labels for } \Gamma_2)$$

under which any scalar $a \in (\mathbf{Z}/N\mathbf{Z})^\times$ *acts (by right multiplication) as* $(a \bmod N_1, a \bmod N_2)$.

(2) *If* -1 *operates without fixed points on the cusp-labels of* Γ_1, *then it operates without fixed points on the cusp-labels of* Γ.

(3) *If* -1 *operates without fixed points on the cusp-labels of* Γ, *then for some* $i \in \{1,2\}$, *it operates without fixed points on the cusp-labels for* Γ_i.

Proof. (1) is the Chinese Remainder Theorem, (2), (3) the observation that the only fixed points of a product endomorphism of a product space are products of fixed points. Q.E.D.

LEMMA 10.7.4. *If* $N \neq 1,2,4$, *then for any subgroup* Γ *of the standard upper unipotent subgroup*

$$\Gamma \subset \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \subset GL(2, \mathbf{Z}/N\mathbf{Z}),$$

the element -1 *acts without fixed points on the space of cusp-labels of* Γ.

Proof. Visibly $-1 \notin \Gamma$. So for odd N, this is a particular case of (10.7.2).

In the remaining cases, we argue as follows. The existence of a fixed point of -1 acting on Hom Surj/Γ means that there exists some $\Lambda \in$ Hom Surj, and some $\gamma \in \Gamma$, with

$$-\Lambda = \Lambda\gamma .$$

Matricially, this is

$$-(x,y) = (x,y)\begin{pmatrix} 1 & B \\ 0 & 1 \end{pmatrix} = (x, Bx+y)$$

for some primitive vector $(x,y) \in (\mathbf{Z}/N\mathbf{Z})^2$, and some $B \in \mathbf{Z}/N\mathbf{Z}$. Thus we have

$$2x \equiv 0, \quad 2y \equiv -Bx \mod N .$$

If $N = 2M$ with M odd and $M \geq 3$, then we infer

$$x \equiv 0(M), \quad 2y \equiv -Bx \equiv 0(M) .$$

Because M is odd, we may infer $y \equiv 0(M)$ also. Thus (x,y) is not primitive, contradiction.

If $N = 4M$ with $M \geq 2$ arbitrary, we again consider

$$2x \equiv 0(4M), \quad 2y \equiv -Bx(4M) .$$

The first congruence shows $x \equiv 0(2M)$, $4y \equiv -2Bx \equiv 0(4M)$ so $y \equiv 0(M)$. But $x \equiv 0(2M)$ implies x is nilpotent mod $4M$. As (x,y) is primitive mod $4M$, this implies that y is a unit mod $4M$, hence that y mod M is a unit mod M, contradicting $y \equiv 0(M)$. Q.E.D.

(10.8) *Application to structure near infinity*

(10.8.1) Let H be a subgroup of $(\mathbf{Z}/N\mathbf{Z})^\times$, A the subring $\mathbf{Z}[\zeta_N]^H$ of $\mathbf{Z}[\zeta_N]$. We know (5.1.1) that $[\Gamma(N)]$ is a regular moduli problem, finite and flat over (Ell/$\mathbf{Z}$). By (9.1.8, 9.1.9), we know that $[\Gamma(N)]^{A\text{-can}}$ is a regular moduli problem, finite and flat over (Ell/A). For any subgroup $\Gamma \subset GL(2, \mathbf{Z}/N\mathbf{Z})$ with $\det(\Gamma) \subset H$, we know that Γ acts on $[\Gamma(N)]^{A\text{-can}}$ as moduli problem on (Ell/A), and that the quotient $[\Gamma(N)]^{A\text{-can}}/\Gamma$ is itself a normal moduli problem, finite over (Ell/A), and canonically isomorphic to $([\Gamma(N)]/\Gamma)^{A\text{-can}}$.

THEOREM 10.8.2. *Let* H *be a subgroup of* $(\mathbf{Z}/N\mathbf{Z})^\times$, A *the subring* $\mathbf{Z}[\zeta_N]^H$ *of* $\mathbf{Z}[\zeta_N]$, B *a noetherian* A*-algebra. Let* $\Gamma \subset GL(2, \mathbf{Z}/N\mathbf{Z})$ *be a subgroup with* $\det(\Gamma) \subset H$, *and denote by* $\mathcal{P}$ *the moduli problem*

$$\mathcal{P} = ([\Gamma(N)]/\Gamma)^{A\text{-can}} \otimes_A B \quad \text{on} \quad (\text{Ell}/B) .$$

Then we have a canonical isomorphism of $B((q))$*-schemes*

$$\mathcal{P}_{\text{Tate}(q)/B((q))} \simeq$$

$$\coprod_{\substack{\Lambda_i \text{ reps of} \\ \text{Hom Surj}/\Gamma}} \text{Spec}\,(B((q)) \otimes_{A((q))} (\mathbf{Z}[\zeta_N] \otimes A((q))[X]/(X^N - q))^{\Gamma \cap \text{Fix } \Lambda_i}) .$$

If we further suppose that B *is flat over* A, *then this last* $B((q))$*-scheme*

$$\coprod_{\substack{\Lambda_i \text{ reps of} \\ \text{Hom Surj}/\Gamma}} \text{Spec}\left((\mathbf{Z}[\zeta_N]\otimes_A (B((q))[X]/(X^N=q))\right)^{\Gamma \cap \text{Fix } \Lambda_i}).$$

Proof. If B is noetherian and flat over A, then B((q)) is flat over A((q)). Therefore the second assertion results from the first by (A 7.1.3). To prove the first assertion, we note that it suffices to treat the case B = A, for if we denote by $\mathcal{P}_0$ the moduli problem $([\Gamma(N)]/\Gamma)^{A\text{-can}}$ on (Ell/A), then we have $\mathcal{P} = \mathcal{P}_0 \otimes_A B$, whence we have (cf. 4.13) tautological equalities

$$\begin{aligned}\mathcal{P}_{\text{Tate}(q)/B((q))} &= (\mathcal{P}_0)_{\text{Tate}(q)/B((q))} \\ &= ((\mathcal{P}_0)_{\text{Tate}(q)/A((q))}) \otimes_{A((q))} B((q)).\end{aligned}$$

Finally, the case B = A follows immediately from (8.11.9) applied to Γ acting on $[\Gamma(N)]^{A\text{-can}}$, the fact that Tate(q)[N]/A((q)) is $T[N] \otimes_{\mathbf{Z}[q,q^{-1}]} A((q))$, and (10.5.1) applied in the case B = A((q)). Q.E.D.

COROLLARY 10.8.3. *Let* H *be a subgroup of* $(\mathbf{Z}/N\mathbf{Z})^\times$, A *the subring* $\mathbf{Z}[\zeta_N]^H$ *of* $\mathbf{Z}[\zeta_N]$, *and* B *any flat noetherian* A*-algebra.*

Let $\Gamma \subset GL(2, \mathbf{Z}/N\mathbf{Z})$ *be a subgroup such that* $\det(\Gamma) \subset H$, *and denote by* $\mathcal{P}$ *the moduli problem*

$$\mathcal{P} = ([\Gamma(N)]/\Gamma)^{A\text{-can}} \otimes_A B \quad \textit{on} \quad (\text{Ell}/B).$$

Then we have a canonical isomorphism of B((q))*-schemes*

$$(\mathcal{P}_{\text{Tate}(q)/B((q))})/\pm 1 \simeq$$

$$\coprod_{\substack{\Lambda_i \text{ reps of} \\ \text{Hom Surj}/\pm\Gamma}} \text{Spec}\left((\mathbf{Z}[\zeta_N]\otimes_A (B((q))[X]/(X^N=q))\right)^{(\pm\Gamma) \cap \text{Fix } \Lambda_i}).$$

If either Γ *contains* -1, *or if* -1 *acts without fixed points on the set* Hom Surj/Γ *of cusp-labels for* Γ, *then for any* $\Lambda \in \text{Hom Surj}((\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}/N\mathbf{Z})$, *we have*

Proof. Apply the previous theorem to the group $\pm\Gamma$.

If -1 has no fixed points acting on Hom Surj/Γ, then for any element $\gamma \in \Gamma$, we claim $-\gamma$ fixes no $\Lambda \in$ Hom Surj. If this were false, then $\Lambda\gamma = -\Lambda$ for some $\gamma \in \Gamma$, $\Lambda \in$ Hom Surj, and then -1 fixes the coset $\Lambda\Gamma$, contrary to hypothesis. Q.E.D.

(10.9) *Applications to the four basic moduli problems*

THEOREM 10.9.1. *Let* $N \geq 1$ *be an integer,* $\Gamma \subset SL(2, \mathbf{Z}/N\mathbf{Z})$ *a subgroup. Denote by* $\mathcal{P}$ *the moduli problem*

$$([\Gamma(N)]/\Gamma)^{\mathbf{Z}[\zeta_N]\text{-can}} \quad \textit{on} \quad (\text{Ell}/\mathbf{Z}[\zeta_N]),$$

and by $\bar{M}(\mathcal{P})$ *its compactified coarse moduli scheme. Then*

(1) *The cusps of* $\bar{M}(\mathcal{P})$ *are the disjoint union of* $n(\Gamma)$ *sections of* $\bar{M}(\mathcal{P})$ *over* $\mathbf{Z}[\zeta_N]$, *where* $n(\Gamma)$ *is the integer*

$$n(\Gamma) = \#(\text{Hom Surj}((\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}/N\mathbf{Z})/\pm\Gamma).$$

(2) *There exists an open neighborhood* V *of the cusps*

$$\text{cusps}(\mathcal{P}) \subset V \subset \bar{M}(\mathcal{P})$$

which is smooth over $\mathbf{Z}[\zeta_N]$.

(3) *Pick a set of representatives* Λ_i *for the space* Hom Surj/$\pm\Gamma$, *and for each representative let* e_i *be the order of the group* $(\pm\Gamma) \cap (\text{Fix } \Lambda_i)$, $f_i = N/e_i$. *Then the formal completion of* $\bar{M}(\mathcal{P})$ *along its cusps is the* $\mathbf{Z}[\zeta_N]$*-formal scheme*

$$\coprod_{\Lambda_i \in \text{Hom Surj}/\pm\Gamma} \text{Spf}(\mathbf{Z}[\zeta_N][[q^{1/f_i}]]).$$

Proof. The assertions are all Zariski-local on $\mathbf{Z}[\zeta_N]$, so we may choose an auxiliary prime number ℓ, and consider instead $\mathcal{P} \otimes_{\mathbf{Z}[\zeta_N]} \mathbf{Z}[\zeta_N, 1/\ell]$ over the ring $\mathbf{Z}[\zeta_N, 1/\ell]$. By (8.11.10) and (10.8.2), the formal completion of $\bar{M}(\mathcal{P})[1/\ell]$ along its cusps is the normalization of $\mathbf{Z}[\zeta_N, 1/\ell][[q]]$ in

$$\coprod_{\Lambda_i \in \text{Hom Surj}/\pm\Gamma} \text{Spec}\left((\mathbf{Z}[\zeta_N, 1/\ell]((q))[X]/(X^N = q))^{(\pm\Gamma)\cap \text{Fix}(\Lambda_i)}\right).$$

Because $\pm\Gamma$ lies inside SL, the intersection $(\pm\Gamma) \cap \text{Fix}(\Lambda_i)$ is, via the basic k_{Λ_i}, ℓ_{Λ_i} of $(\mathbf{Z}/N\mathbf{Z})^2$ (cf. 10.2.4) isomorphic to a subgroup of the semi-Borel $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$, all of whose elements have determinant *one*. Therefore $(\pm\Gamma) \cap \text{Fix}(\Lambda_i)$ is a subgroup of the upper unipotent group $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, with respect to the basis k_{Λ_i}, ℓ_{Λ_i}. As $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ is cyclic of order N, $(\pm\Gamma) \cap (\text{Fix } \Lambda)$ is the cyclic subgroup generated by the element

$$\begin{pmatrix} 1 & f_i \\ 0 & 1 \end{pmatrix},$$

operating on the ring $\mathbf{Z}[\zeta_N, 1/\ell]((q))[X]/(X^N = q)$ by

$$\begin{cases} \zeta_N \mapsto \zeta_N \\ X \mapsto \zeta_N^{f_i} X. \end{cases}$$

Because $(\zeta_N)^{f_i}$ is a primitive e_i'th root of unity, the subring of invariants is the subring of polynomials in $X^{e_i} = q^{1/f_i}$. Thus the formal completion of $\bar{M}(\mathcal{P}) \underset{\mathbf{Z}[\zeta_N]}{\otimes} \mathbf{Z}[\zeta_N, 1/\ell]$ along the cusps is

$$\coprod_{\Lambda_i \in \text{Hom Surj}/\pm\Gamma} \text{Spec}\left(\mathbf{Z}[\zeta_N, 1/\ell][[q^{1/f_i}]]\right),$$

which is formally smooth over $\mathbf{Z}[\zeta_N]$, and which exhibits the cusps as the asserted number of disjoint sections. Q.E.D.

COROLLARY 10.9.2. *Suppose that* $\Gamma \subset SL(2, \mathbf{Z}/N\mathbf{Z})$, *and that* $K \geq 1$ *is an integer such that the moduli problem* $\mathcal{P} = ([\Gamma(N)]/\Gamma)^{\text{can}}$ *on* $(\text{Ell}/\mathbf{Z}[\zeta_N])$ *becomes representable when we invert* K, *i.e.,* $\mathcal{P}[1/K]$ *is representable on* $(\text{Ell}/\mathbf{Z}[\zeta_N, 1/K])$. *Then*

(1) *The compactified moduli scheme* $\bar{M}(\mathcal{P})[1/K]$ *is smooth over* $\mathbf{Z}[\zeta_N, 1/K]$ *except possibly at supersingular points in characteristic* p *with* p *a divisor of* N, $p \nmid K$.

(2) *The scheme* $\bar{M}(\mathcal{P})[1/NK]$ *is a proper smooth curve over* $\mathbf{Z}[\zeta_N, 1/NK]$ *with geometrically connected fibers.*

Proof. We first prove (2). The moduli problem $[\Gamma(N)] \underset{\mathbf{Z}}{\otimes} \mathbf{Z}[1/N]$ is finite etale galois over $(\text{Ell}/\mathbf{Z}[1/N])$, with galois group $GL(2, \mathbf{Z}/N\mathbf{Z})$, and finite etale galois over $[\mathbf{Z}[\zeta_N, 1/N]]$ with galois group $SL(2, \mathbf{Z}/N\mathbf{Z})$. Therefore $([\Gamma(N)]/\Gamma) \underset{\mathbf{Z}}{\otimes} \mathbf{Z}[1/N]$ is finite etale over $[\mathbf{Z}[\zeta_N, 1/N]]$. By (9.1.9), $\mathcal{P}[1/N]$ is finite etale over $(\text{Ell}/\mathbf{Z}[\zeta_N, 1/N])$, so in particular it is smooth over $\mathbf{Z}[\zeta_N, 1/N]$ of relative dimension one. Because $\mathcal{P}[1/K]$ is representable, this means that $M(\mathcal{P})[1/NK]$ is a smooth curve over $\mathbf{Z}[\zeta_N, 1/NK]$. We already know that $\bar{M}(\mathcal{P})$ is smooth over $\mathbf{Z}[\zeta_N]$ near its cusps. Therefore $\bar{M}(\mathcal{P}) \underset{\mathbf{Z}[\zeta_N]}{\otimes} \mathbf{Z}[\zeta_N, 1/NK]$ is a proper smooth curve over $\mathbf{Z}[\zeta_N, 1/NK]$. By the connectedness theorem, it suffices to show that its geometric generic fiber is connected, i.e., to study the situation after the base change $\mathbf{Z}[\zeta_N] \hookrightarrow \mathbf{C}$ defined by, say $\zeta_N \mapsto \exp(2\pi i/N)$. To show that the smooth C-curve $\bar{\mathcal{M}}(\mathcal{P}) \underset{\mathbf{Z}[\zeta_N]}{\otimes} \mathbf{C}$ is connected, it suffices to show that the complement of the finitely many cusps, $\mathcal{M}(\mathcal{P}) \underset{\mathbf{Z}[\zeta_N]}{\otimes} \mathbf{C}$, is connected. But this is standard, because the underlying complex manifold to $\mathcal{M}(\mathcal{P}) \underset{\mathbf{Z}[\zeta_N]}{\otimes} \mathbf{C}$ is isomorphic to the quotient of the upper half plane by the subgroup $\tilde{\Gamma} \subset SL(2, \mathbf{Z})$ which is the complete inverse image of Γ by reduction mod N.

We now prove (1). Let p be any prime such that $p|N$, $p \nmid K$. Choose an algebraic closure k of $\mathbf{F}_p$, and a homomorphism $\mathbf{Z}[\zeta_N] \to k$.

Let $\mathfrak{p}$ denote the corresponding place of $\mathbf{Z}[\zeta_N]$, and denote by R the completion of the strict henselization of $\mathbf{Z}[\zeta_N]$ at $\mathfrak{p}$, (i.e., R "is"

the p-adic completion of $\mathbf{Z}[\zeta_N]$, with its residue field extended to k). Let E/k be an ordinary elliptic curve, $E/R[[T]]$ its universal formal deformation (for deformations to artin local R-algebras with residue field k).

We are claiming that the finite $R[[T]]$-scheme

$$\mathcal{P}_{E/R[[T]]},$$

viewed as formal scheme over R, is formally smooth over R. We have proven that $\bar{M}(\mathcal{P})$ is smooth over $\mathbf{Z}[\zeta_N]$ near the cusps, hence at *some* ordinary points in every fiber. Therefore there exists an E/k which is ordinary, and such that $\mathcal{P}_{E/R[[T]]}$ is formally smooth over R.

We will now see that the isomorphism class of the formal R-scheme $\mathcal{P}_{E/R[[T]]}$ is independent of the particular choice of ordinary E/k. Because $\mathcal{P}$ is the quotient of $[\Gamma(N)]^{can}$ by Γ, we have (7.1.5)

$$\mathcal{P}_{E/R[[T]]} = ([\Gamma(N)]^{can}_{E/R[[T]]})/\Gamma .$$

By the Serre-Tate theorem, (2.9.1), the deformation theory of any elliptic curve E/k to an artin local ring with residue field k is equal to the deformation theory of its N-divisible group, given with all the e_{N^ν}-pairings, to that same artin local ring, for any integer N divisible by p. Because E/k is ordinary, and k is algebraically closed, there exists an isomorphism

$$E[N^\infty] \simeq \mu_{N^\infty} \times (\mathbf{Q}/\mathbf{Z})_{N^\infty\text{-torsion}},$$

compatible with e_{N^ν}-pairings. Therefore the formal R-scheme

$$[\Gamma(N)]^{can}_{E/R[[T]]}$$

prorepresents the functor on artin local R-algebras with residue field k

$$A \mapsto \begin{cases} \text{deformations } G \text{ to } A \text{ of } \mu_{N^\infty} \times (\mathbf{Q}/\mathbf{Z})_{N^\infty\text{-tors}} \\ \text{with its } e_{N^\nu}\text{-pairings, plus a } (\mathbf{Z}/N\mathbf{Z})^2\text{-generator} \\ (P,Q) \text{ of } G[N] \text{ with } e_N(P,Q) = \zeta_N . \end{cases}$$

The action of Γ is by moving (P,Q). Thus both the formal R-scheme $[\Gamma(N)]^{can}_{E/R[[T]]}$ and the action of Γ upon it, are independent of the choice of ordinary E/k. Therefore the quotient $\mathcal{P}_{E/R[[T]]}$ is, as formal R-scheme, independent of the choice of ordinary E/k. Q.E.D.

(10.9.3) Summarizing Table

APPLICATION TO $[\Gamma(N)]^{can}$, $[\text{bal. }\Gamma_1(N)]^{can}$

	MODULI PBLM OVER $\mathbf{Z}[\zeta_N]$	REPRESENTABLE OVER $\mathbf{Z}[\zeta_N, 1/K]$ for $K = ?$	$\bar{M}(\mathcal{P})$ PROPER SMOOTH OVER $\mathbf{Z}[\zeta_N, 1/K]$ OUTSIDE S/S POINTS IN CHAR $p = ?$
$[\Gamma(N)]^{can}$	$N = 1$ or 2	NEVER	(NOT APPLICABLE)
	$N = p^k \geq 3$	p	NONE LEFT
	$N = 2p^k$, $p \neq 2$	p	2
	N divisible by two rel. prime integers both ≥ 3	1	all $p \mid N$
$[\text{bal. }\Gamma_1(N)]^{can}$	$N = 1, 2, 3$	NEVER	(NOT APPLICABLE)
	$N = p^k \geq 4$	p	NONE LEFT
	$N = 2p^k$, p odd, $p^k \geq 4$	p	2
	$N = 3p^k$, $p \neq 3$, $p^k \geq 4$	p	3
	$N = 6$	6	NONE LEFT
	N divisible by two rel. prime integers both ≥ 4	1	all $p \mid N$

THEOREM 10.9.4. *Let* N_1 *and* N_2 *be integers* ≥ 1 *which are relatively prime:* $(N_1, N_2) = 1$. *Put* $N = N_1 N_2$, *and let* $\Gamma \subset GL(2, Z/NZ)$ *be a subgroup which satisfies*

$$\det(\Gamma) \equiv 1 \bmod N_1 .$$

Let A *denote the subring* $Z[\zeta_N]^{\det(\Gamma)}$ *of* $Z[\zeta_N]$, $\mathcal{P}$ *the moduli problem*

$$([\Gamma(N)]/\Gamma)^{A\text{-can}} \quad \textit{on} \quad (Ell/A) .$$

Denote by Γ_0 *the intersection* $\Gamma \cap SL(2, Z/NZ)$, *and by* $\mathcal{P}_0$ *the moduli problem*

$$([\Gamma(N)]/\Gamma_0)^{Z[\zeta_N]\text{-can}} \quad \textit{on} \quad (Ell/Z[\zeta_N]) .$$

Then

(1) *We have an isomorphism of moduli problems over* $Z[\zeta_N, 1/N_2]$

$$\mathcal{P}[1/N_2] \underset{A[1/N_2]}{\otimes} Z[\zeta_N, 1/N_2] \xrightarrow{\sim} \mathcal{P}_0[1/N_2] ,$$

(2) *This isomorphism induces an isomorphism of compactified moduli schemes*

$$\bar{M}(\mathcal{P}) \underset{A}{\otimes} Z[\zeta_N, 1/N_2] \xrightarrow{\sim} \bar{M}(\mathcal{P}_0)[1/N_2] .$$

(3) *The scheme* $\bar{M}(\mathcal{P})[1/N_2]$ *is smooth over* $A[1/N_2]$ *in a neighborhood of the cusps, and its cusps are a finite etale* $A[1/N_2]$ *scheme of degree* $n(\Gamma_0)$,

$$n(\Gamma_0) = \#(\text{Hom Surj}((Z/NZ)^2, Z/NZ)/\pm\Gamma_0) .$$

Proof. Let $H = \det(\Gamma)$ inside $(Z/NZ)^\times$, and let H_2 be the image of H in $(Z/N_2Z)^\times$. Because $\det H \equiv 1 (N_1)$, we have $H \xrightarrow{\sim} H_2$ operating on

$$Z[\zeta_N] = Z[\zeta_{N_1}] \underset{Z}{\otimes} Z[\zeta_{N_2}]$$

through the second factor. Therefore, we have

$$A = Z[\zeta_N]^{\det(\Gamma)} = Z[\zeta_{N_1}] \otimes (Z[\zeta_{N_2}])^{H_2} .$$

But $Z[\zeta_{N_2}, 1/N_2]$ is finite etale over $Z[1/N_2]$, as is its subring of H_2-invariants. Therefore $Z[\zeta_N, 1/N_2]$ is finite etale over $A[1/N_2]$.

We now apply (9.2.2) to the situation $G = \Gamma/\Gamma_0$ acting on $([\Gamma(N)]/\Gamma_0)[1/N]$, covering its free action on $Z[\zeta_N, 1/N_2]$. This proves (1), and (2) follows from (1) and the fact that $Z[\zeta_N, 1/N_2]$ is etale over $A[1/N_2]$ (cf. 8.6.7, (3)). The assertions of (3) are f.p.p.f. local on the base, and we have already proven, thanks to (2) and (10.9.2), that they become true after the finite etale base change $A[1/N_2] \to Z[\zeta_N, 1/N_2]$. Q.E.D.

COROLLARY 10.9.5. *Hypotheses and notations as in the (10.9.4), suppose further that for some integer* $K \geq 1$ *the moduli problem* $([\Gamma(N)]/\Gamma)[1/K]$ *on* $(Ell/Z[1/K])$ *is representable. Let* $\mathcal{P}$ *denote, as before, the moduli problem* $([\Gamma(N)]/\Gamma)^{A\text{-can}}$ *on* (Ell/A). *Then* $\mathcal{P}[1/N_2K]$ *is representable, by (9.1.7), and we have the following results.*

(1) *The compactified moduli scheme* $\bar{M}(\mathcal{P})[1/N_2K]$ *is smooth over* $A[1/N_2K]$ *except possibly at supersingular points in characteristic* p *with* p *a divisor of* N_1, $p \nmid KN_2$.

(2) *The scheme* $\bar{M}(\mathcal{P})[1/NK]$ *is a proper smooth curve over* $A[1/NK]$ *with geometrically connected fibers, in which the scheme of cusps is finite etale over* $A[1/NK]$.

Proof. The statements are f.p.p.f. local on the base, and we know already they become true after the finite etale base changes $A[1/N_2K] \to Z[\zeta_N, 1/N_2K]$ and $A[1/NK] \to Z[\zeta_N, 1/NK]$ respectively, because the isomorphism (1) of (10.9.4) shows that $\mathcal{P}_0[1/N_2K]$ is representable, so that (10.9.2) applies to it. Q.E.D.

(10.9.6) Summarizing Table

SHORT TABLE OF APPLICATIONS

MODULI PBLM $\mathcal{P}$ OF FORM $([\Gamma(N_1N_2)]/\Gamma)^{A\text{-can}}$ with $(N_1,N_2)=1$, $\det\Gamma \equiv 1 \bmod N_1$	$A = ?$	REP OVER $A[1/K] = ?$	$\bar{M}(\mathcal{P})[1/N_2K]$ PROPER SMOOTH OVER $A[1/N_2K]$ OUTSIDE S/S POINTS IN CHAR $p\|N_1$, $A[1/N_2K] = ?$
$([\Gamma(N_1)]^{Z[\zeta_{N_1}]\text{-can}},[\Gamma_0(N_2)])$ with $N_1 \geq 3$	$Z[\zeta_{N_1}]$	$Z[\zeta_{N_1},1/N_1]$	$Z[\zeta_{N_1},1/N_1N_2]$
$([\text{bal.}\,\Gamma_1(N_1)]^{Z[\zeta_{N_1}]\text{-can}},[\Gamma_0(N_2)])$ with $N_1 \geq 4$	$Z[\zeta_{N_1}]$	$Z[\zeta_{N_1},1/N_1]$	$Z[\zeta_{N_1},1/N_1N_2]$
$([\Gamma_1(N_1)],[\Gamma_0(N_2)])$ with $N_1 \geq 4$	Z	$Z[1/N_1]$	$Z[1/N_1N_2]$
$[\Gamma_1(N_1)]$ with $N_1 \geq 4$	Z	$Z[1/N_1]$	$Z[1/N_1]$
$([\text{bal.}\,\Gamma_1(N_1)]^{Z[\zeta_{N_1}]\text{-can}},[\Gamma_1(N_2)])$ with $N_2 \geq 4$	$Z[\zeta_{N_1}]$	$Z[\zeta_{N_1}][1/N_2]$	$Z[\zeta_{N_1}][1/N_2]$

THEOREM 10.9.7. *Let* $\Gamma \subset GL(2, Z/NZ)$ *be a subgroup,* $A = (Z[\zeta_N])^{\det(\Gamma)}$ *the corresponding subring of* $Z[\zeta_N]$, *and denote by* $\text{discrim}(\Gamma)$ *the product of those prime numbers* p *such that the extension* $Z[\zeta_N]/A$ *is ramified at some* p*-adic place of* A (*so* $\text{discrim}(\Gamma)$ *is always a divisor of* N).

Denote by $\mathcal{P}$ *the moduli problem*

$$([\Gamma(N)]/\Gamma)^{A\text{-can}} \quad \textit{on} \quad (\text{Ell}/A)\,.$$

The compactified coarse moduli scheme $\bar{M}(\mathcal{P})[1/\text{discrim}(\Gamma)]$ *is smooth over* $A[1/\text{discrim}(\Gamma)]$ *except possibly* [*at points of* $M(\mathcal{P})$ *at which either* $j(j-1728)$ *is not invertible, or*]* *at points which are supersingular points in characteristic* p *dividing* N.

*The phrase in brackets can be deleted, see Notes Added in Proof.

Proof. By the descent mechanism already employed (10.9.4) we may replace Γ by $\Gamma \cap SL(2, Z/NZ)$, and A by $Z[\zeta_N]$ itself. Let k be the algebraic closure of a finite field, $j_0 \in k$ a number with $j_0 \neq 0, 1728$, $Z[\zeta_N] \to k$ a homomorphism, $\mathfrak{p}$ the place it defines, and R the completion of the strict henselization of $Z[\zeta_N]$ at $\mathfrak{p}$.

Let E/k be an elliptic curve with $j(E/k) = j_0$ different from $0, 1728$. Let $E/R[[T]]$ be its universal formal deformation. The formal fiber of $M(\mathcal{P}) \to \text{Spec}\,(Z[\zeta_N][j])$ over $E/R[[T]]$ is (8.2.3) the formal R-scheme

$$\mathcal{P}_{E/R[[T]]}/\text{Aut}\,(E/k)\,.$$

We must show that it is formally smooth over R except if E/k is supersingular in characteristic $p|N$. Because $\text{Aut}\,(E/k) = \pm 1$, we may use (7.1.5) to rewrite this

$$([\Gamma(N)]^{\text{can}}_{E/R[[T]]})/\pm\Gamma_0\,.$$

Because we already know smoothness along some neighborhood of the cusps, it suffices to show that for each fixed situation $Z[\zeta_N] \to k$, this formal R-scheme is independent of the particular choice of E/k, provided that E/k is ordinary in case $\text{char}(k)|N$. When $\text{char}(k)|N$, this follows from Serre-Tate theory, exactly as in the proof of (10.9.2). If N is invertible in k, then $E[N]/R[[T]]$ is isomorphic to the extension of scalars of the group over Z

$$\mu_N \times Z/NZ$$

with its canonical e_N ! Q.E.D.

(10.10) *Detailed analysis at a prime* p; *balanced subgroups*

(10.10.1) Definitions. Let p be a prime number, $n \geq 1$ an integer, and

$$\Gamma \subset GL(2, Z/p^nZ)$$

a subgroup. We say that Γ satisfies (*) if

(10.10.1.1) (*) either $p \neq 2$, or $p = 2$ and $n = 1$, or $p = 2$, $n \geq 2$, and $\det(\Gamma) \equiv 1 \bmod 4$.

We say that Γ is *balanced* if for every element

$$\Lambda \in \mathrm{Hom\ Surj}((\mathbf{Z}/p^n\mathbf{Z})^2, \mathbf{Z}/p^n\mathbf{Z}),$$

the subgroup $\Gamma \cap \mathrm{Fix}(\Lambda)$ of Γ has exactly the same group of determinants as Γ itself, i.e., if

(10.10.1.2) $$\det(\Gamma \cap \mathrm{Fix}(\Lambda)) = \det(\Gamma) \quad \text{for all} \quad \Lambda.$$

(10.10.1.3) We say that Γ is "balanced at Λ" if the above equality of determinant groups holds for the particular element $\Lambda \in \mathrm{Hom\ Surj}$.

Clearly for given Γ, the question of whether Γ is balanced at Λ depends only on the image of Λ in the space

$$(\mathbf{Z}/p^n\mathbf{Z})^\times \backslash \mathrm{Hom\ Surj}/\Gamma$$

of component-labels for Γ. We say that Γ is partly balanced if there exists some component-label at which it is balanced, and we say the corresponding component label is Γ-balanced.

(10.10.2) Now let $N \geq 1$ be an integer prime to p, and consider a subgroup

$$\Gamma \subset \mathrm{GL}(2, \mathbf{Z}/Np^n\mathbf{Z})$$

which is a *product* $\Gamma = \Gamma_1 \times \Gamma_2$ of subgroups

$$\Gamma_1 \subset \mathrm{GL}(2, \mathbf{Z}/p^n\mathbf{Z})$$

$$\Gamma_2 \subset \mathrm{GL}(2, \mathbf{Z}/N\mathbf{Z})$$

via the canonical isomorphism

$$\mathrm{GL}(2, \mathbf{Z}/Np^n\mathbf{Z}) \xrightarrow{\sim} \mathrm{GL}(2, \mathbf{Z}/p^n\mathbf{Z}) \times \mathrm{GL}(2, \mathbf{Z}/N\mathbf{Z})$$

of the Chinese Remainder Theorem. Recall (10.7.3) that this isomorphism induces isomorphisms

$$\begin{cases} \mathrm{Hom\ Surj} \xrightarrow{\sim} \mathrm{Hom\ Surj} \times \mathrm{Hom\ Surj} \\ \quad \Lambda \longmapsto (\Lambda_1, \Lambda_2) \\ \text{cusp labels for } \Gamma \xrightarrow{\sim} (\text{cusp labels for } \Gamma_1) \times (\text{cusp labels for } \Gamma_2) \\ \text{compt. labels for } \Gamma \xrightarrow{\sim} (\text{compt. labels for } \Gamma_1) \times (\text{compt. labels for } \Gamma_2). \end{cases}$$

We say that a component label for Γ is Γ_1-*balanced* if its first component via the above isomorphism is a Γ_1-balanced component label for Γ_1. We say that Γ is *balanced at* p if every component label for Γ is Γ_1-balanced, i.e., if Γ_1 is balanced.

THEOREM 10.10.3. *In the above product situation* $\Gamma = \Gamma_1 \times \Gamma_2$, $\Gamma_1 \subset \mathrm{GL}(2, \mathbf{Z}/p^n\mathbf{Z})$, $\Gamma_2 \subset \mathrm{GL}(2, \mathbf{Z}/N\mathbf{Z})$, N *prime to* p, *suppose that*

(a) Γ_1 *satisfies (*) (10.10.1.1)*

(b) *either both* Γ_1 *and* Γ_2 *contain* -1, *or* -1 *operates without fixed points on the space of cusp labels for* Γ.

Let

$$A = (\mathbf{Z}[\zeta_{p^n}])^{\det(\Gamma_1)} \subset \mathbf{Z}[\zeta_{p^n}],$$

$$B = (\mathbf{Z}[\zeta_N])^{\det(\Gamma_2)} \subset \mathbf{Z}[\zeta_N],$$

so that

$$A \underset{\mathbf{Z}}{\otimes} B = (\mathbf{Z}[\zeta_{Np^n}])^{\det(\Gamma)} \subset \mathbf{Z}[\zeta_{Np^n}].$$

Let $\mathcal{P}$ *denote the moduli problem*

$$([\Gamma(Np^n)]/\Gamma)^{A \otimes B\text{-can}} \quad \text{on} \quad (\mathrm{Ell}/A \otimes B).$$

Then

(1) *The compactified coarse moduli scheme* $\bar{M}(\mathcal{P})[1/N]$ *is regular in some neighborhood of the cusps. In fact it is regular except possibly at points at which either* $j(j-1728)$ *fails to be invertible, or at supersingular points in characteristic* p (p = *the given* p).

(2) *If* $\mathcal{P}[1/N]$ *is representable, then* $\bar{M}(\mathcal{P})[1/N]$ *is regular outside of the supersingular points in characteristic* p.

(3) *The completion* $\widehat{\text{Cusps}}(\mathcal{P}[1/N])$ *of* $\bar{M}(\mathcal{P})[1/N]$ *along its cusps is a disjoint union of formal schemes indexed by*

$$\pm 1 \backslash \text{Hom Surj}((\mathbf{Z}/Np^n\mathbf{Z})^2, \mathbf{Z}/Np^n\mathbf{Z}) / \Gamma .$$

For each Λ *in a set of representatives in* Hom Surj *of this indexing set, let* Λ_1 *and* Λ_2 *be the components of* Λ, *and denote by* A_Λ *and* B_Λ *the rings*

$$A \subset A_\Lambda = (\mathbf{Z}[\zeta_{p^n}])^{\det(\Gamma_1 \cap \text{Fix}(\Lambda_1))}$$

$$B \subset B_\Lambda = (\mathbf{Z}[\zeta_N])^{\det(\Gamma_2 \cap \text{Fix}(\Lambda_2))}$$

so that $A_\Lambda \underset{\mathbf{Z}}{\otimes} B_\Lambda$ *is the subring of invariants of* $\det(\Gamma \cap \text{Fix}(\Lambda))$ *in* $\mathbf{Z}[\zeta_{Np^n}]$. *The* Λ*-piece of* $\widehat{\text{Cusps}}(\mathcal{P}[1/N])$ *is naturally a scheme over* $A_\Lambda \underset{\mathbf{Z}}{\otimes} B_\Lambda[1/N]$, *isomorphic to the formal completion of a smooth* $A_\Lambda \underset{\mathbf{Z}}{\otimes} B_\Lambda[1/N]$*-scheme of relative dimension one along a closed subscheme of* $\text{Cusps}(\mathcal{P})[1/N]$ *which is finite etale over* $A_\Lambda \underset{\mathbf{Z}}{\otimes} B_\Lambda[1/N]$.

(4) *If* Λ *is* Γ_1*-balanced, then* $A = A_\Lambda$, *and* $\bar{M}(\mathcal{P})[1/N]$ *is smooth over* $A \otimes B[1/N]$ *in some neighborhood of the* Λ*-cusps. In particular, if* Γ_1 *is partly balanced, the "ouvert de lissité" of* $\bar{M}(\mathcal{P})[1/N]$ *over* $A \otimes B[1/N]$ *meets every fiber.*

(5) *If* Γ_1 *is balanced, then* $\bar{M}(\mathcal{P})[1/N]$ *is smooth over* $A \otimes B[1/N]$ *except possibly [at points at which either* $j(j-1728)$ *is not invertible, or]** *at supersingular points in characteristic* p. *Its scheme of cusps is finite etale over* $A \otimes B[1/N]$.

*The phrase in brackets can be deleted, see Notes Added in Proof.

(6) *If* Γ_1 *is balanced and if* $\mathcal{P}[1/N]$ *is representable, then* $\bar{M}(\mathcal{P})[1/N]$ *is smooth over* $A \otimes B[1/N]$ *outside of the supersingular points in characteristic* p. *Its scheme of cusps is finite etale over* $A \otimes B[1/N]$.

Proof. The basic assertion to prove is (3). Admitting it for a moment, let us explain how the others follow. Each $A_\Lambda \otimes B_\Lambda$ is the full ring of integers in a subfield of $\mathbf{Q}(\zeta_{Np^n})$, so is regular. Therefore the Λ-piece of $\widehat{\text{Cusps}}(\mathcal{P}[1/N])$ is regular, and so $\bar{M}(\mathcal{P})[1/N]$ is regular at its cusps. As it is a scheme of finite type over $\mathbf{Z}$, its set of regular points is open. The usual homogeneity argument then gives (1) and (2). Assertions (4), (5) and (6) follow similarly, for $B_\Lambda[1/N]$ is finite etale over $B[1/N]$, so $A \otimes B_\Lambda[1/N]$ is finite etale over $A \otimes B[1/N]$. Thus whenever $A = A_\Lambda$, we can replace "regular" by "smooth over $A \otimes B[1/N]$" in the above argument.

We now prove (3). By (10.8.3), we know that $\widehat{\text{Cusps}}(\mathcal{P}[1/N])$ is the normalization of $\mathbf{Z}[1/N][[q]]$ in the finite $\mathbf{Z}[1/N]((q))$-scheme

$$\coprod_{\substack{\Lambda \text{ reps of} \\ \text{Hom Surj}/\pm\Gamma}} \text{Spec}((\mathbf{Z}[\zeta_{p^n}, \zeta_N, 1/N]((q))[X]/(X^{Np^n} = q))^{(\pm\Gamma) \cap \text{Fix}(\Lambda)}) .$$

By hypothesis (b), we have (cf. 10.8.3)

$$(\pm\Gamma) \cap \text{Fix}\,\Lambda = \Gamma \cap \text{Fix}\,\Lambda .$$

Because normalization commutes with passage to invariants, we have that $\widehat{\text{Cusps}}(\mathcal{P}[1/N])$ is the disjoint union, over the representatives Λ, of the spectra of the rings

$$(\mathbf{Z}[\zeta_{p^n}, \zeta_N, 1/N][[q]][X]/(X^{Np^n} = q))^{\Gamma \cap \text{Fix}\,\Lambda} .$$

Because $\mathbf{Z}[1/N][[q]]$ is flat over $\mathbf{Z}[1/N][q]$, the above ring may be written as

$$Z[1/N][[q]] \underset{Z[1/N,q]}{\otimes} (Z[\zeta_{p^n}, \zeta_N, 1/N, q, X]/(X^{Np^n}=q))^{\Gamma \cap \mathrm{Fix}\,\Lambda}.$$

Thus we are reduced to showing that the spectrum of

$$(Z[\zeta_{p^n}, \zeta_N, 1/N, q, X]/(X^{Np^n}=q))^{\Gamma \cap \mathrm{Fix}\,\Lambda}$$

is smooth and one-dimensional over $(Z[\zeta_{p^n}, \zeta_N, 1/N])^{\det(\Gamma \cap \mathrm{Fix}\,\Lambda}$, and that the closed reduced subscheme of it defined set-theoretically by the equation $q = 0$ is finite etale over the same ring.

We next reduce to the case when Γ_2 lies in SL.

Let $\Gamma_2' = \Gamma_2 \cap SL(2, Z/NZ)$, $\Gamma' = \Gamma_1 \times \Gamma_2'$ inside $\Gamma = \Gamma_1 \times \Gamma_2$. Then

$$\begin{aligned}\Gamma' \cap \mathrm{Fix}(\Lambda) &= (\Gamma_1 \cap \mathrm{Fix}\,\Lambda_1) \times (\Gamma_2' \cap \mathrm{Fix}\,\Lambda_2) \\ &= (\Gamma_1 \cap \mathrm{Fix}\,\Lambda_1) \times (\Gamma_2 \cap \mathrm{Fix}\,\Lambda_2 \cap SL(2, Z/NZ)),\end{aligned}$$

so that the quotient of $\Gamma \cap \mathrm{Fix}\,\Lambda$ by $\Gamma' \cap \mathrm{Fix}\,\Lambda$ is isomorphic, via the determinant, to the galois group of the finite etale galois covering

$$\begin{array}{ccc} A_\Lambda \underset{Z}{\otimes} Z[\zeta_N, 1/N] & = & (Z[\zeta_{p^n}, \zeta_N, 1/N])^{\det(\Gamma' \cap \mathrm{Fix}\,\Lambda)} \\ \Big| & & \Big| \\ A_\Lambda \underset{Z}{\otimes} B_\Lambda[1/N] & = & (Z[\zeta_{p^n}, \zeta_N, 1/N])^{\det(\Gamma \cap \mathrm{Fix}\,\Lambda)}. \end{array}$$

Therefore the situation we are considering is a descent through this finite etale galois covering of the situation

$$(Z[\zeta_{p^n}, \zeta_N, 1/N, q, X]/(X^{Np^n}=q))^{\Gamma' \cap \mathrm{Fix}\,\Lambda}$$

with respect to the ring $A_\Lambda[\zeta_N, 1/N]$. This completes the reduction to the case $\Gamma_2 \subset SL$.

Supposing now that $\Gamma_2 \subset SL$, consider the product decomposition

$$\Gamma \cap \mathrm{Fix}\,\Lambda = (\Gamma_1 \cap \mathrm{Fix}\,\Lambda_1) \times (\Gamma_2 \cap \mathrm{Fix}\,\Lambda_2).$$

In the standard bases $(k_{\Lambda_1}, \ell_{\Lambda_1})$ and $(k_{\Lambda_2}, \ell_{\Lambda_2})$ adapted to Λ_1 and Λ_2 respectively (cf. 10.2.4) we have matrix realizations

$$\Gamma_1 \cap \mathrm{Fix}\,\Lambda_1 \subset \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \subset GL(2, Z/p^nZ)$$

$$\Gamma_2 \cap \mathrm{Fix}\,\Lambda_2 \subset \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \subset GL(2, Z/NZ).$$

Let us denote by e the order of the group $\Gamma_2 \cap \mathrm{Fix}\,\Lambda_2$, f the ratio N/e, its index in $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. Then visibly the $\Gamma_2 \cap \mathrm{Fix}\,\Lambda_2$ invariants in

$$Z[\zeta_{p^n}, \zeta_N, 1/N, q, X]/(X^{Np^n}=q)$$

are the polynomials in X^e.

Introducing the new variable $T = X^e$, and replacing ζ_{p^n} by its unique f'th root which is also a p^n-th root of unity, we are reduced to studying the ring of invariants

$$(Z[\zeta_{p^n}, \zeta_N, 1/N, q, T]/(T^{fp^n}=q))^{\Gamma_1 \cap \mathrm{Fix}\,\Lambda_1},$$

where an element

$$\begin{pmatrix} A & B \\ 0 & 1 \end{pmatrix} \in \Gamma_1 \cap \mathrm{Fix}\,\Lambda_1 \subset GL(2, Z/p^nZ)$$

acts by

$$\begin{cases} \zeta_{p^n} \mapsto (\zeta_{p^n})^A \\ \zeta_N \mapsto \zeta_N \\ q \mapsto q \\ T \mapsto T(\zeta_{p^n})^B. \end{cases}$$

We must show that the ring of invariants is smooth over $A_\Lambda[\zeta_N, 1/N]$, and that the reduced closed subscheme $(q=0)^{red}$ is finite etale over $A_\Lambda[\zeta_N, 1/N]$.

The situation in question comes by the etale extension of scalars $Z \to Z[\zeta_N, 1/N]$ from the analogous situation

$$(Z[\zeta_{p^n}, T], \text{ above action of } \Gamma_1 \cap \mathrm{Fix}(\Lambda)).$$

It is at this point we make use of the hypothesis that Γ_1 satisfies (*), i.e., that if $p = 2$ and p^n is 4 or more, then $\det(\Gamma_1) \equiv 1 \bmod 4$. Obviously any subgroup of Γ_1 also satisfies (*), in particular the group $\Gamma_1 \cap \mathrm{Fix}\,\Lambda$. We thus conclude the proof by appealing to the following theorem.

THEOREM 10.10.4. *Let* $G \subset \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \subset GL(2, Z/p^nZ)$ *be a subgroup of the standard upper semi-Borel, and suppose that* G *satisfies (*) (cf. 10.10.1.1). Let us denote*

$$p^a = \#\left(G \cap \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}\right).$$

Then there exists a root of unity

$$\zeta \in Z[\zeta_{p^n}]$$

such that under the standard action of G *on* $Z[\zeta_{p^n}, T]$

$$\begin{pmatrix} A & B \\ 0 & 1 \end{pmatrix} : \begin{cases} \zeta_{p^n} \mapsto (\zeta_{p^n})^A \\ T \mapsto T(\zeta_{p^n})^B, \end{cases}$$

the ring of invariants is the polynomial ring in one variable

$$(Z[\zeta_{p^n}, T])^G = (Z[\zeta_{p^n}])^{\det(G)}[S], \quad S = \zeta T^{p^a}.$$

Proof. This is simply group-theory. Consider the exact sequence of groups

$$1 \longrightarrow G \cap \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \longrightarrow G \xrightarrow{\det} (Z/p^nZ)^\times.$$

The subgroup $G \cap \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, having order p^a, is the cyclic group generated by

$$\begin{pmatrix} 1 & p^{n-a} \\ 0 & 1 \end{pmatrix}.$$

If $G = G \cap \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, the assertion is obvious (with $\zeta = 1$). If $\det(G)$ is non-trivial, let $A \in (Z/p^nZ)^\times$ be a generator of the cyclic (by *) group $\det(G)$, and let

$$\begin{pmatrix} A & B \\ 0 & 1 \end{pmatrix}$$

be some chosen element of G with determinant A. These two elements obviously generate G.

The subring of invariants under $G \cap \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ is visibly the ring

$$Z[\zeta_{p^n}, T^{p^a}],$$

on which $\begin{pmatrix} A & B \\ 0 & 1 \end{pmatrix}$ operates by

$$\zeta_{p^n} \mapsto (\zeta_{p^n})^A$$

$$T^{p^a} \mapsto T^{p^a}(\zeta_{p^n})^{Bp^a}.$$

We will produce a root of unity $\zeta \in Z[\zeta_{p^n}]$, such that the element

$$S = \zeta T^{p^a}$$

is invariant by $\begin{pmatrix} A & B \\ 0 & 1 \end{pmatrix}$, and hence by all of G. Once we have done this, then

$$(Z[\zeta_{p^n}, T])^G = (Z[\zeta_{p^n}, T^{p^a}])\begin{pmatrix} A & B \\ 0 & 1 \end{pmatrix}$$

$$= (Z[\zeta_{p^n}, S])^{\begin{pmatrix} A & B \\ 0 & 1 \end{pmatrix}}$$

$$= (Z[\zeta_{p^n}])^{\det(G)}[S] .$$

We now search for ζ of the form $(\zeta_{p^n})^x$, such that ζT^{p^a} is invariant by $\begin{pmatrix} A & B \\ 0 & 1 \end{pmatrix}$:

$$T^{p^a}(\zeta_{p^n})^x \xmapsto{\begin{pmatrix} A & B \\ 0 & 1 \end{pmatrix}} T^{p^a}(\zeta_{p^n})^{Ax}(\zeta_{p^n})^{Bp^a} .$$

Thus the requirement is that

$$x \equiv Ax + p^a B \bmod p^n ,$$

or equivalently

$$(1-A)x \equiv p^a B \bmod p^n .$$

If $A \not\equiv 1 \bmod p$, then $1-A$ is invertible mod p^n, so we can solve uniquely for x.

If $A \equiv 1 \bmod p$, then $\det(G)$ is the subgroup

$$1 + (p^b) \subset (Z/p^nZ)^\times$$

for some $1 \le b \le n-1$. ($\le n-1$ because we have already dealt with the case $\det(G) = 1$.) If $p = 2$, then $b \ge 2$, because of condition (*). We may choose for A the generator

$$A = 1 + p^b .$$

We must show that

$$p^b x \equiv p^a B \bmod p^n$$

has a solution. If $B \equiv 0 \bmod p^n$, then $x = 0$ is a solution. If $B \not\equiv 0 \bmod p^n$, we may speak of the integer $\operatorname{ord}_p(B) \le n-1$, and we must show that

$$\operatorname{ord}_p(B) + a - b \ge 0 ,$$

given that the matrix

$$\begin{pmatrix} A & B \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+p^b & B \\ 0 & 1 \end{pmatrix}$$

has its p^{n-b}'th power in $G \cap \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, which is the cyclic group generated by

$$\begin{pmatrix} 1 & p^{n-a} \\ 0 & 1 \end{pmatrix} .$$

For any integer $m \ge 1$, one easily verifies the identity

$$\begin{pmatrix} A & B \\ 0 & 1 \end{pmatrix}^m = \begin{pmatrix} A^m & B(1+A+\cdots+A^{m-1}) \\ 0 & 1 \end{pmatrix} .$$

In our situation, this yields the congruence

$$B(1+A+\cdots+A^{(p^{n-b}-1)}) \equiv 0 \bmod p^{n-a} .$$

In terms of A, $B \in Z_p$ lifting A, $B \in Z/p^nZ$, this gives

$$B\left(\frac{A^{p^{n-b}}-1}{A-1}\right) \equiv 0 \bmod p^{n-a} ,$$

whence

$$\operatorname{ord}_p B + \sum_{\substack{\zeta^{p^{n-b}}=1 \\ \zeta \neq 1}} \operatorname{ord}_p(A-\zeta) \ge n-a .$$

But A is $\equiv 1 \bmod 2p$, so for any *non-trivial* p-power root of unity we have

$$\mathrm{ord}_p(A-\zeta) = \mathrm{ord}_p(1-\zeta) .$$

Therefore

$$\sum_{\substack{\zeta^{p^{n-b}}=1 \\ \zeta \neq 1}} \mathrm{ord}_p(A-\zeta) = \sum_{\substack{\zeta^{p^{n-b}}=1 \\ \zeta \neq 1}} \mathrm{ord}_p(1-\zeta)$$

$$= \mathrm{ord}_p\left(\left(\frac{X^{p^{n-b}}-1}{X-1}\right) \mid X=1\right)$$

$$= \mathrm{ord}_p(p^{n-b})$$

$$= n-b .$$

This yields

$$\mathrm{ord}_p(B) + n - b \geq n - a ,$$

as required. Q.E.D.

REMARK 10.10.5. Here is an example to show that the condition (*) is essential. Consider the element

$$\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathbf{Z}/4\mathbf{Z}) .$$

It has order two, and the cyclic group G it generates violates (*). Consider the ring of invariants

$$\mathbf{Z}[i,T]^G$$

under the action

$$\begin{cases} i \mapsto -i \\ T \mapsto iT . \end{cases}$$

An elementary calculation shows that the ring of invariants is

$$(\mathbf{Z}[i,T])^G = \mathbf{Z}[T+iT, iT^2]$$
$$= \mathbf{Z}[X,Y]/(X^2=2Y) ,$$

which visibly is *not regular* at the maximal ideal $(X=0, Y=0, 2=0)$.

COROLLARY 10.10.6. *Hypotheses and notations as in 10.10.3, let* k *be a finite field of characteristic* p, *and* $A \otimes B[1/N] \twoheadrightarrow k$ *a ring homomorphism.*

Suppose that $\mathcal{P}[1/N]$ *satisfies coarse base change near infinity (cf. 8.6.6, 8.5.1), (e.g.,* $\mathcal{P}[1/N]$ *representable). Then the following conditions are equivalent.*

(1) Γ_1 *is balanced.*

(2) $M(\mathcal{P}) \underset{A\otimes B}{\otimes} k$ *is a smooth curve over* k *outside the supersingular points [and the points where* $j(j-1728)$ *is not invertible].*[*]

(3) $M(\mathcal{P}) \underset{A\otimes B}{\otimes} k$ *is generically reduced (i.e., reduced outside a finite set of points).*

Proof. By the theorem, (1) $\Longrightarrow$ (2), and trivially (2) $\Longrightarrow$ (3). Suppose that Γ_1 is not balanced. Then the calculation of the previous theorem shows that

$$\mathcal{P}_{\mathrm{Tate}(q)/(A\otimes B[1/N])((q))}/\pm 1$$

is a disjoint union of schemes, indexed by representatives Λ of

$$\mathrm{Hom\ Surj}((\mathbf{Z}/p^n\mathbf{Z})^2, (\mathbf{Z}/p^n\mathbf{Z}))/\pm\Gamma_1 ,$$

such that the Λ'th component is faithfully flat over $A_\Lambda \otimes B_\Lambda[1/N]$. By hypothesis, ± 1 operates either freely or trivially on

$$\mathcal{P}_{\mathrm{Tate}(q)/(A\otimes B[1/N])((q))} .$$

[*] The phrase in brackets can be deleted, see Notes Added in Proof.

Clearly we have

$$((A\otimes B[1/N])((q))) \underset{A\otimes B[1/N]}{\otimes} k \xrightarrow{\sim} k((q)) ,$$

so

$$(\mathcal{P}_{\mathrm{Tate}(q)/k((q))})/\pm 1 = ((\mathcal{P}_{\mathrm{Tate}(q)/(A\otimes B[1/N])((q))})/\pm 1)\otimes k$$

is a disjoint union of schemes faithfully flat over the rings

$$(A_\Lambda \otimes B_\Lambda[1/N]) \underset{A\otimes B[1/N]}{\otimes} k .$$

If Γ_1 is not balanced at Λ, then A_Λ is the ring of integers in a non-trivial extension of A inside $Z[\zeta_{p^n}]$, so it is fully ramified over A at the unique place dividing p. Therefore

$$(A_\Lambda \otimes B_\Lambda[1/N]) \underset{A\otimes B}{\otimes} k$$

is *not reduced*. Therefore, if Γ_1 is not balanced, the scheme

$$\mathcal{P}_{\mathrm{Tate}(q)/k((q))}/\pm 1$$

is not reduced. Because $\mathcal{P}[1/N]$ satisfies coarse base change, we have

$$(\mathcal{P}_{\mathrm{Tate}(q)/k((q))})/\pm 1 \simeq M(\mathcal{P}\otimes k)_{k((q))} = (M(\mathcal{P})\otimes k)_{k((q))} .$$

Therefore $(M(\mathcal{P})\otimes k)_{k((q))}$ is not reduced. But the field extension

$$k(j) \hookrightarrow k((1/j)) = k((1/q))$$

is separable, so $(M(\mathcal{P})\otimes k)_{k(j)}$ is not reduced.

Because $M(\mathcal{P}) \underset{A\otimes B}{\otimes} k$ is finite over $\mathrm{Spec}(k[j])$, this means that $M(\mathcal{P})\otimes k$ cannot be "reduced outside a finite set of points." Q.E.D.

COROLLARY 10.10.7 (due to O. Gabber). *Let* $p_1,\cdots,p_r$ *be distinct primes,* $k_1,\cdots,k_r$ *integers* ≥ 1, $N_0 \geq 1$ *an integer prime to* $p_1\cdots p_r$. *Suppose we are given subgroups*

$$\begin{cases} \Gamma_0 \subset \mathrm{SL}(2, Z/N_0Z) \\ \Gamma_i \subset \mathrm{GL}(2, Z/p_i^{k_i}Z) \qquad \text{for } i = 1,\cdots,r . \end{cases}$$

Let $N = N_0 \prod p_i^{k_i}$, *and denote by*

$$\Gamma \subset \mathrm{GL}(2, Z/NZ)$$

the product subgroup

$$\Gamma = \Gamma_0\times\Gamma_1\times\cdots\times\Gamma_r .$$

Suppose that both of the following conditions are satisfied.

(a) *For* $i = 1,\cdots,r$, *the subgroup* Γ_i *satisfies* (*) *(cf. 10.10.1.1).*

(b) *Either* -1 *operates without fixed points on the cusp-labels for* Γ, *or every one of the groups* $\Gamma_0,\Gamma_1,\cdots,\Gamma_r$ *contains* -1.

Denote by $\mathcal{P}$ *the moduli problem* $[\Gamma(N)]/\Gamma$ *on* (Ell/Z). *Then the compactified coarse moduli scheme* $\bar{M}(\mathcal{P})$ *is regular except possibly at points where* $j(j-1728)$ *is not invertible or at supersingular points in characteristic* p *dividing* N.

Proof. In the notation of (10.9.7), discrim(Γ) divides $p_1\cdots p_r$, and therefore $\bar{M}(\mathcal{P})[1/p_1\cdots p_r]$ is smooth over the cyclotomic ring $(Z[\zeta_N])^{\det(\Gamma)}[1/p_1\cdots p_r]$ outside the specified exceptional points. Therefore $\bar{M}(\mathcal{P})[1/p_1\cdots p_r]$ is regular outside the specified exceptions. To see the regularity at points in characteristic $p_1,\cdots,p_r$, we apply Theorem 10.10.3 to, say, Γ_1 and $\Gamma_0\times\Gamma_2\times\cdots\times\Gamma_r$, which tells us that $\bar{M}(\mathcal{P})[1/N_0p_2\cdots p_r]$ is regular outside the specified exceptions. Q.E.D.

REMARK 10.10.8. The example already cited (10.10.5) shows that the condition (*) is essential. For if $p_1^{k_1} = 4$, and if we take for Γ_1 the subgroup of order two in $\mathrm{GL}(2, Z/4Z)$ generated by

$$\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} ,$$

then $\bar{M}(\mathcal{P})$ will be *irregular* at every cusp in characteristic two.

(10.11) *Basic examples of balanced subgroups*

(10.11.1) We again fix a prime number p, and an integer $n \geq 1$. For every subgroup H of $(\mathbf{Z}/p^n\mathbf{Z})^\times$, we denote by

$$\begin{pmatrix} H & * \\ 0 & H \end{pmatrix} \subset GL(2, \mathbf{Z}/p^n\mathbf{Z})$$

the subgroup consisting of all matrices of the form

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}, \quad A, D \in H, \quad B \in \mathbf{Z}/p^n\mathbf{Z}.$$

PROPOSITION 10.11.2. *The subgroup* $\begin{pmatrix} H & * \\ 0 & H \end{pmatrix} \subset GL(2, \mathbf{Z}/p^n\mathbf{Z})$ *is always partly balanced. It is balanced precisely for the following list of* H:

(1) *for* $n = 1$, *no restriction, i.e.,* $H =$ *any subgroup of* $\mathbf{F}_p^\times$

(2) *for* $n \geq 2$, *and* p *odd, or* $n \geq 4$ *and* $p = 2$, H *must be one of the groups* $1 + (p^a)$, *for* a *an integer* $\geq [n/2]$

(3) *for* $n = 2, 3$ *and* $p = 2$, H *is unrestricted.*

Proof. Let $\Lambda \in \mathrm{Hom}\ \mathrm{Surj}((\mathbf{Z}/p^n\mathbf{Z})^2, (\mathbf{Z}/p^n\mathbf{Z}))$ correspond to a primitive vector (x, y) (i.e., $\Lambda\begin{pmatrix} a \\ b \end{pmatrix} = ax + by$). We must compute, for each Λ, the group of determinants of

$$\begin{pmatrix} H & * \\ 0 & H \end{pmatrix} \cap \mathrm{Fix}\ \Lambda.$$

The condition that an element $\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$ fix Λ is

$$(x, y) = (x, y)\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = (Ax, Bx + Dy),$$

i.e.,

$$\begin{cases} (A-1)x = 0 \\ (1-D)y = Bx \end{cases}.$$

Case 1. x invertible in $\mathbf{Z}/p^n\mathbf{Z}$. Then $A = 1$, but D is unrestricted, because we may solve for $B = \left(\frac{1}{x}\right)(1-D)y$. Therefore *any* $\begin{pmatrix} H & * \\ 0 & H \end{pmatrix}$ is balanced at a component label Λ with x invertible.

Case 2. $x = 0$. Then A is free, and we may take $D = 1$, B arbitrary. So any $\begin{pmatrix} H & * \\ 0 & H \end{pmatrix}$ is balanced at a component label Λ with $x = 0$.

The first two cases complete the analysis for $n = 1$ (since $x \in \mathbf{F}_p$ is either invertible or zero).

Case 3. $n \geq 2$, $x = p^a \times (\text{unit})$ with $1 \leq a \leq n-1$. Then y is invertible, because (x, y) is a primitive vector. The conditions are

$$\begin{cases} A \equiv 1 & (p^{n-a}) \\ D \equiv 1 & (p^a) \end{cases}.$$

Therefore for this $\Lambda = (x, y)$, we have

$$\det\left(\begin{pmatrix} H & * \\ 0 & H \end{pmatrix} \cap (\mathrm{Fix}\ \Lambda)\right) = H \cap (1 + (p^{\min(a, n-a)})).$$

Therefore $\begin{pmatrix} H & * \\ 0 & H \end{pmatrix}$ is balanced at this Λ if and only if

$$H \subset 1 + (p^{\min(a, n-a)}).$$

The most restrictive choice of a is $a = [n/2]$, i.e.,

$$\begin{pmatrix} H & * \\ 0 & H \end{pmatrix} \text{ balanced} \iff H \equiv 1 \bmod p^{[n/2]}.$$

Now for p odd, the group $1 + (p) \subset (\mathbf{Z}/p^n\mathbf{Z})^\times$ is cyclic of order p^{n-1}, and its only subgroups are the $1 + (p^\nu)$ with $1 \leq \nu \leq n$. Similarly, if $p = 2$ and $n \geq 4$, the group $1 + (4)$ is cyclic, and its only subgroups are the $1 + (2^{\nu+2})$'s, $0 \leq \nu \leq n-2$. Q.E.D.

REMARK (10.11.3). For $p = 2$, the list of H such that $\begin{pmatrix} H & * \\ 0 & H \end{pmatrix}$ is balanced *and* satisfies (*) in the following:

$n = 1$; no restriction, any (!) subgroup of $F_2^\times$

$n = 2$; H trivial

$n = 3$; H trivial or $H = 1 + (4) = \{1, 5\}$

$n \geq 4$; $H = 1 + (2^a)$ with $a \geq [n/2]$.

(10.12) *Application to the moduli problems* $[\Gamma_0(p^n); a, a]$

(10.12.1) We have already seen (7.4.2) that we have isomorphisms of moduli problems on (Ell/Z)

$$[\Gamma(p^n)]/\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \simeq [\text{bal. } \Gamma_1(p^n)],$$

so that for any subgroup $H \subset (\mathbf{Z}/p^n\mathbf{Z})^\times$, we have

$$[\Gamma(p^n)]/\begin{pmatrix} H & * \\ 0 & H \end{pmatrix} \xrightarrow{\sim} [\text{bal. } \Gamma_1(p^n)]/H \times H .$$

We have seen (7.6.1) that this quotient is regular, finite and flat over (Ell/Z). In the particular case

$$H = 1 + (p^a) \subset (\mathbf{Z}/p^n\mathbf{Z})^\times ,$$

this quotient is (cf. 7.9.6) the moduli problem

$$[\Gamma_0(p^n); a, a] .$$

THEOREM 10.12.2. *Let* p *be a prime,* $n \geq 1$ *an integer,* $H \subset (\mathbf{Z}/p^n\mathbf{Z})^\times$ *one of the subgroups*

(1) *if* $n = 1$, *any subgroup of* $F_p^\times$

(2) *if* $n \geq 2$, *one of the subgroups* $1 + (p^a)$ *with* $a \geq [n/2]$ *for* p *odd, and* $a \geq \max(2, [n/2])$ *if* $p = 2$.

Denote by A *the ring*

$$A = (\mathbf{Z}[\zeta_{p^n}])^H \subset \mathbf{Z}[\zeta_{p^n}] ,$$

and by $\mathcal{P}$ *the moduli problem*

$$([\text{bal. } \Gamma_1(p^n)]/H \times H)^{A\text{-can}} \quad \text{on} \quad (\text{Ell}/A) .$$

Let $N \geq 3$ *be an integer prime to* p, $\Gamma \subset GL(2, \mathbf{Z}/N\mathbf{Z})$ *a subgroup,* B *the ring*

$$B = \mathbf{Z}[\zeta_N]^{\det(\Gamma)} \subset \mathbf{Z}[\zeta_N] .$$

Suppose that the moduli problem

$$\mathcal{R} = ([\Gamma(N)]/\Gamma)^{B\text{-can}} \quad \text{on} \quad (\text{Ell}/B)$$

has $\mathcal{R}[1/N]$ *representable on* $(\text{Ell}/B[1/N])$, *and that* -1 *operates without fixed points on the cusp-labels for* Γ. *Then*

(1) *The simultaneous problem* $(\mathcal{P}, \mathcal{R}[1/N])$ *on* $(\text{Ell}/A \otimes B[1/N])$ *is representable.*

(2) *Its compactified moduli scheme* $\bar{M}(\mathcal{P}, \mathcal{R}[1/N])$ *is a regular two-dimensional scheme, finite and flat over* $\bar{M}(\mathcal{R}[1/N]) \otimes_{\mathbf{Z}} A$.

(3) *Outside the supersingular points in characteristic* p, $\bar{M}(\mathcal{P}, \mathcal{R}[1/N])$ *is smooth of relative dimension one over* $A \otimes B[1/N]$.

(4) *The scheme of cusps of* $\bar{M}(\mathcal{P}, \mathcal{R}[1/N])$ *is finite etale over* $A \otimes B[1/N]$.

(5) *Over* $A \otimes B[1/Np]$, *the scheme* $\bar{M}(\mathcal{P}, \mathcal{R}[1/N])[1/p]$ *is a proper smooth curve with geometrically connected fibers.*

Proof. Apply the previous theorem (10.10.3) to the product group $\begin{pmatrix} H & * \\ 0 & H \end{pmatrix} \times \Gamma$, and remember that H is chosen so that $\begin{pmatrix} H & * \\ 0 & H \end{pmatrix}$ is *balanced.* The point to remark is that the quotient of $[\Gamma(Np^n)]$ by the product group in indeed the simultaneous problem in question, as follows from (7.3.1) and (9.4.3.6). The finite flatness of the projection map $\bar{M}(\mathcal{P}, \mathcal{R}[1/N]) \to \bar{M}(\mathcal{R}[1/N]) \otimes_{\mathbf{Z}} A$ results from the fact that it is a finite map (because it is a map of finite $\mathbf{P}^1_{A \otimes B[1/N]}$-schemes) between regular schemes of the same dimension. Q.E.D.

REMARK. This theorem will be used later in studying questions of good reduction. In those applications, one very natural choice of auxiliary

rigidifying moduli problem $\mathcal{R}$ will be $\Gamma_1(N)$, for an arbitrary integer $N \geq 4$ prime to p. In this case, the ring B is simply $\mathbf{Z}$ itself. But $[\text{bal.}\,\Gamma_1(N)]^{\text{can}}$ with $N \geq 4$ prime to p, and its $B = \mathbf{Z}[\zeta_N]$, or $[\Gamma(N)]^{\text{can}}$ with $N \geq 3$ prime to p and $B = \mathbf{Z}[\zeta_N]$, are "just as good" for studying questions of good reduction at primes over p.

(10.13) *The numerology of modular schemes, via the line bundle* $\underline{\omega}$

(10.13.1) Let R be an excellent noetherian regular ring, $\mathcal{P}$ a representable moduli problem on (Ell/R) which is finite over (Ell/R), and normal near infinity. Over the moduli scheme $\mathfrak{M}(\mathcal{P})$ we have the corresponding universal elliptic curve

$$\begin{array}{c} E \\ \downarrow f \\ \mathfrak{M}(\mathcal{P}) , \end{array}$$

and the corresponding invertible sheaf $\underline{\omega}$ on $\mathfrak{M}(\mathcal{P})$ defined by

$$\underline{\omega} = f_*\Omega^1_{E/\mathfrak{M}(\mathcal{P})} = Lie(E/\mathfrak{M}(\mathcal{P}))^\vee . \tag{10.13.1.1}$$

(10.13.2) There is a canonical way to extend $\underline{\omega}^{\otimes 2}$ to an invertible sheaf, still denoted $\underline{\omega}^{\otimes 2}$, on the compactified moduli scheme $\overline{\mathfrak{M}}(\mathcal{P})$, as follows. It suffices to specify a prolongation of $\underline{\omega}^{\otimes 2}$ as invertible sheaf from

$$\overline{\mathfrak{M}}(\mathcal{P})_{R((q))} \quad \text{to} \quad \overline{\mathfrak{M}}(\mathcal{P})_{R[[q]]} = \widehat{\text{Cusps}}(\mathcal{P}) .$$

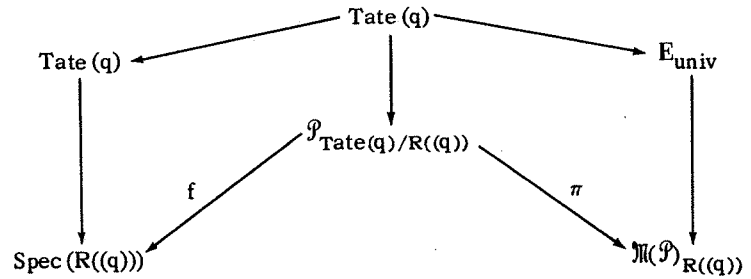
We will do this by specifying a canonical *trivialization*

$$\mathcal{O} \xrightarrow{\sim} \underline{\omega}^{\otimes 2} \quad \text{restricted to} \quad \mathfrak{M}(\mathcal{P})_{R((q))} ,$$

and then patch together

$$\begin{cases} \text{the given } \underline{\omega}^{\otimes 2} \text{ on } \mathfrak{M}(\mathcal{P}) \\ \text{the trivial } \mathcal{O} \text{ on } \overline{\mathfrak{M}}(\mathcal{P})_{R[[q]]} \end{cases}$$

along this trivialization. We construct the trivialization as follows. By (8.11.7), we have a cartesian diagram



in which π is a finite etale ± 1-torsor. Therefore $\pi^*(\underline{\omega})$ admits the nowhere vanishing section deduced by pull-back by f of the canonical one-form (8.8, T.2)

$$\omega_{\text{can}} \quad \text{on} \quad \text{Tate}(q)/\mathbf{Z}((q)) .$$

Under the action of $\pm 1 = \text{Aut}(\text{Tate}(q)/R((q)))$, the one-form ω_{can} is carried to $\pm\,\omega_{\text{can}}$. Therefore its *square* $(\omega_{\text{can}})^{\otimes 2}$ defines a trivialization of $\pi^*(\underline{\omega}^{\otimes 2})$ which is *invariant* by ± 1, so descends to give the sought-after trivialization of $\underline{\omega}^{\otimes 2}$ restricted to $\mathfrak{M}(\mathcal{P})_{R((q))}$.

The same procedure serves to extend any *even* power $\underline{\omega}^{\otimes 2k}$ of $\underline{\omega}$ to an invertible sheaf on all of $\overline{\mathfrak{M}}(\mathcal{P})$. The *extended* $\underline{\omega}^{\otimes 2k}$ is related to the extended $\underline{\omega}^{\otimes 2}$ by the formula

$$\underline{\omega}^{\otimes 2k} \text{ extended} = (\underline{\omega}^{\otimes 2} \text{ extended})^{\otimes k} ,$$

simply because $\omega_{\text{can}}^{\otimes 2k} = (\omega_{\text{can}}^{\otimes 2})^{\otimes k}$.

(10.13.3) It may or may not be possible to extend $\underline{\omega}$ itself to a line bundle on all of $\overline{\mathfrak{M}}(\mathcal{P})$ whose square is the above extension of $\underline{\omega}^{\otimes 2}$. For

an example where no such extension exists, consider the moduli problem $[\Delta = 1]$ on $(\mathrm{Ell}/\mathbf{Z}[1/6])$ defined by

$$[\Delta = 1](E/R) = \text{the set of nowhere-vanishing one-forms } \omega \text{ on } E/R \text{ such that } \Delta(E, \omega) = 1 .$$

This is clearly a finite etale μ_{12}-torsor over $(\mathrm{Ell}/\mathbf{Z}[1/6])$, which is represented by the smooth $\mathbf{Z}[1/6]$-curve in (g_2, g_3)-space

$$(g_2)^3 - 27(g_3)^2 = 1 ,$$

with universal (E, ω) given by

$$(y^2 = 4x^3 - g_2 x - g_3, dx/y) .$$

The scheme

$$[\Delta = 1]_{\mathrm{Tate}(q)/\mathbf{Z}[1/6]((q))}$$

is given by

$$\mathbf{Z}[1/6][[q^{1/12}]] ,$$

with universal object over it

$$(\mathrm{Tate}(q), \left(q^{1/12} \prod_{n \geq 1} (1 - q^n)^2\right) \omega_{\mathrm{can}}) .$$

The action of $\pm 1 = \mathrm{Aut}(\mathrm{Tate}(q))$ carries $\omega_{\mathrm{can}} \to \pm \omega_{\mathrm{can}}$, so it operates on $\mathbf{Z}[1/6][[q^{1/12}]]$ as $q^{1/12} \to \pm q^{1/12}$, with ring of invariants

$$\widehat{\mathrm{Cusps}}([\Delta = 1]) = \mathrm{Spec}(\mathbf{Z}[1/6][[q^{1/6}]]) .$$

The extended $\underline{\omega}^{\otimes 2}$ is free over $\widehat{\mathrm{Cusps}}([\Delta = 1])$ with nowhere vanishing section $\omega_{\mathrm{can}}^{\otimes 2}$. The square of the universal differential ω_{univ} is equal to

$$\left(q^{1/6} \prod_{n \geq 1} (1 - q^n)^4\right) (\omega_{\mathrm{can}})^{\otimes 2} ,$$

which shows that $(\omega_{\mathrm{univ}})^{\otimes 2}$ extends to a global section of $\underline{\omega}^{\otimes 2}$ over $\overline{\mathcal{M}}([\Delta = 1])$, which takes a *simple zero* at the cusp, and is elsewhere invertible. The scheme $\overline{\mathcal{M}}([\Delta = 1])$ is just the *complete* elliptic curve over $\mathbf{Z}[1/6]$ whose affine equation is

$$(g_2)^3 - 27(g_3)^2 = 1 ,$$

and $\underline{\omega}^{\otimes 2}$ is the inverse ideal sheaf of the origin on this elliptic curve. In particular, it has *degree one*, so it is not the square of *any* line bundle!

In the positive direction, we have the following.

PROPOSITION 10.13.4. *Let* R *be an excellent noetherian regular ring,* $\mathcal{P}$ *a representable moduli problem on* (Ell/R) *which is finite over* (Ell/R) *and normal near infinity. Let us denote by* $Z(\mathcal{P})$ *the normalization of* $R[[q]]$ *in the finite normal* $R((q))$*-scheme*

$$\mathcal{P}_{\mathrm{Tate}(q)/R((q))} .$$

Suppose that the group $\pm 1 = \mathrm{Aut}(\mathrm{Tate}(q))$ *operates freely on* $Z(\mathcal{P})$. *Then there is a natural way of extending* $\underline{\omega}$ *to a line bundle* $\underline{\omega}$ *on all of* $\overline{\mathcal{M}}(\mathcal{P})$, *in such a way that*

$$(\underline{\omega} \text{ extended})^{\otimes 2} = \underline{\omega}^{\otimes 2} \text{ extended} .$$

Proof. Because normalization commutes with quotients by finite groups, we have

$$Z(\mathcal{P})/\pm 1 \xrightarrow{\sim} \widehat{\mathrm{Cusps}}(\mathcal{P}) .$$

Let $\mathfrak{L}$ denote the *trivial* line bundle on $Z(\mathcal{P})$, which is the trivial extension of the trivial bundle

$$\omega_{\mathrm{can}} \mathcal{O} \quad \text{on} \quad \mathcal{P}_{\mathrm{Tate}(q)/R((q))} .$$

The group ± 1 operates on $\mathfrak{L}$, covering its action on $Z(\mathcal{P})$. Therefore if ± 1 operates *freely* on Z, its action on $(Z(\mathcal{P}), \mathfrak{L})$ defines a *descent* of $\mathfrak{L}$ to $\widehat{\mathrm{Cusps}}(\mathcal{P})$, to a line bundle on $\widehat{\mathrm{Cusps}}(\mathcal{P})$ extending $\underline{\omega}$ from

$\widehat{\text{Cusps}}(\mathcal{P})_{R((q))}$. Because descent is functorial, the square of the descended bundle is the descent of the square $(\omega_{can})^{\otimes 2}\,\mathcal{O}$, so this descent construction does indeed define a square root of $\underline{\omega}^{\otimes 2}$. Q.E.D.

PROPOSITION 10.13.5. *Let* R *be an excellent noetherian regular ring,* $\mathcal{P}$ *and* $\mathcal{P}'$ *two representable moduli problems, both finite over* (Ell/R) *and both normal near infinity. Let*

$$f : \mathcal{P} \to \mathcal{P}'$$

be a morphism of moduli problems over (Ell/R). *Then*

(1) *Under the induced map of modular schemes* $f : \mathcal{M}(\mathcal{P}) \to \mathcal{M}(\mathcal{P}')$ *we have*

$$f^*(\underline{\omega}) \simeq \underline{\omega}\ .$$

(2) *Under the induced map of compactified modular schemes we have*

$$\overline{f} : \overline{\mathcal{M}}(\mathcal{P}) \to \overline{\mathcal{M}}(\mathcal{P}')\ ,$$

$$\overline{f}^*(\underline{\omega}^{\otimes 2}) = \underline{\omega}^{\otimes 2}\ .$$

(3) *If* ± 1 *acts freely on* $Z(\mathcal{P}')$, *then it operates freely on* $Z(\mathcal{P})$, *and under the induced map of compactified modular schemes we have*

$$\overline{f}^*(\underline{\omega}) = \underline{\omega}\ .$$

Proof. Assertion (1) is simply the fact that formation of $\underline{\omega}_{E/S}$ commutes with arbitrary change of base $S' \to S$. Assertion (2) is clear from the construction of the extension of $\underline{\omega}^{\otimes 2}$ via the differential ω_{can} on Tate(q). Assertion (3) holds because f induces a map $Z(\mathcal{P}) \to Z(\mathcal{P}')$ which is ± 1 equivariant, so ± 1 operates "more" freely on $Z(\mathcal{P})$ than on $Z(\mathcal{P}')$, and by the functoriality of descent. Q.E.D.

PROPOSITION 10.13.6. *Hypotheses and notations as in (10.13.1) above, suppose that* $\overline{\mathcal{M}}(\mathcal{P})$ *is smooth over* R *in a neighborhood of the cusps, and that the cusps are finite etale over* R. *Then for any extension of scalars* $R \to R'$ *of excellent noetherian regular rings, the isomorphism (8.6.6)*

$$\overline{\mathcal{M}}(\mathcal{P}) \underset{R}{\otimes} R' \xrightarrow{\sim} \overline{\mathcal{M}}(\mathcal{P} \underset{R}{\otimes} R')$$

induces an isomorphism of line bundles

$$\underline{\omega}^{\otimes 2}_{\overline{\mathcal{M}}(\mathcal{P})} \underset{R}{\otimes} R' \xrightarrow{\sim} \underline{\omega}^{\otimes 2}_{\overline{\mathcal{M}}(\mathcal{P} \otimes R')}\ ,$$

and, if ± 1 *operates freely on* $Z(\mathcal{P})$, *an isomorphism*

$$\underline{\omega}_{\overline{\mathcal{M}}(\mathcal{P})} \underset{R}{\otimes} R' \xrightarrow{\sim} \underline{\omega}_{\overline{\mathcal{M}}(\mathcal{P} \underset{R}{\otimes} R')}\ .$$

Proof. Again clear from the definitions. Q.E.D.

PROPOSITIONS 10.13.7. *Let* $N \geq 1$ *be an integer,* $\Gamma \subset GL(2, Z/NZ)$ *a subgroup,* A *the ring* $(Z[\zeta_N])^{\det(\Gamma)}$, B *an excellent noetherian regular* A*-algebra;* $\mathcal{P}$ *the moduli problem*

$$([\Gamma(N)]/\Gamma)^{A-can} \underset{A}{\otimes} B \quad \text{on} \quad (Ell/B)\ .$$

Suppose that $\mathcal{P}$ *is normal near infinity, so that the scheme* $Z(\mathcal{P})$ = *the normalization of* B[[q]] *in*

$$\mathcal{P}_{\text{Tate}(q)/B((q))}$$

makes sense. If -1 *operates without fixed points on the space*

$$\text{Hom Surj}\,((Z/NZ)^2, Z/NZ)\Big/\Gamma$$

of cusp-labels for Γ, *then* ± 1 *operates freely on* $Z(\mathcal{P})$.

Proof. By (10.8.2), the scheme $\mathcal{P}_{\text{Tate}(q)/B((q))}$ is a disjoint union of schemes, indexed by Hom Surj/Γ, and ± 1 operates compatibly with its action on Hom Surj/Γ. Therefore $Z(\mathcal{P})$ is a disjoint union over the same indexing set, Hom Surj/Γ, with ± 1 acting on $Z(\mathcal{P})$ compatibly with action on Hom Surj/Γ. So if ± 1 operates freely on Hom Surj/Γ, it certainly operates freely on $Z(\mathcal{P})$. Q.E.D.

COROLLARY 10.13.8. *Hypotheses and notations as above, suppose that* B *is an* A[1/N]*-algebra. Denote by* Γ_0 *the intersection* $\Gamma \cap SL(2,\mathbf{Z}/N\mathbf{Z})$. *If* -1 *operates without fixed points on the space* Hom Surj$/\Gamma_0$ *of cusp-labels for* Γ_0, *then* ± 1 *operates freely on* $Z(\mathcal{P})$.

Proof. It suffices to check that ± 1 acts freely on $Z(\mathcal{P})$ after the finite etale base-change $B \mapsto B' = B \underset{A[1/N]}{\otimes} \mathbf{Z}[\zeta_N, 1/N]$, under which

$$Z(\mathcal{P}) \underset{B}{\otimes} B' \xrightarrow{\sim} Z(\mathcal{P} \underset{B}{\otimes} B') = Z(\mathcal{P}')$$

where $\mathcal{P}'$ is the moduli problem attached to $\Gamma_0 = \Gamma \cap SL(2, \mathbf{Z}/N\mathbf{Z})$

$$\mathcal{P}' = ([\Gamma(N)]/\Gamma_0)^{\mathrm{can}} \underset{\mathbf{Z}[\zeta_N]}{\otimes} B' \quad \text{on} \quad (\mathrm{Ell}/B').$$

Now apply the previous proposition to $\mathcal{P}'$. Q.E.D.

COROLLARY 10.13.9. *Hypotheses and notations as above, suppose that* B *is an* A[1/N]*-algebra, and that* $\mathcal{P}$ *is representable. If* N *is odd, or if* $N = 1, 2, 4$ *and* $\Gamma_0 = \Gamma \cap SL(2, \mathbf{Z}/N\mathbf{Z})$ *lies in the upper unipotent subgroup* $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, *then* ± 1 *operates freely on* $Z(\mathcal{P})$, *and consequently* $\underline{\omega}$ *"exists" on* $\overline{\mathcal{M}}(\mathcal{P})$.

Proof. Simply apply (10.7.2) or (10.7.4) to Γ_0. Q.E.D.

(10.13.9.1) Summarizing Table

SHORT TABLE OF APPLICATIONS

$\mathcal{P}$	representable over	$\underline{\omega}$ exists on $\overline{\mathcal{M}}(\mathcal{P})$
$\Gamma(N)^{\mathrm{can}}, N \geq 3$	any $\mathbf{Z}[\zeta_N, 1/N]$-algebra	yes
$\Gamma_1(N)^{\mathrm{can}}, N \geq 5$	any $\mathbf{Z}[\zeta_N, 1/N]$-algebra	yes
$\Gamma_1(N), N \geq 5$	any $\mathbf{Z}[1/N]$-algebra	yes

(10.13.10) Recall that if E/S/R is an elliptic curve over a smooth R-scheme S, $E \xrightarrow{f} S$, the Kodaira-Spencer mapping (cf. [K-2], A1.4) is an $\mathcal{O}_S$-morphism

$$T_{S/R} \to R^1 f_*(T_{E/S}) \simeq R^1 f_*(\mathcal{O}) \otimes Lie(E/S)$$
$$\simeq Lie(E/S) \otimes Lie(E/S)$$
$$\simeq (\underline{\omega}^2_{E/S})^{\vee},$$

whose $\mathcal{O}_S$-linear dual is an $\mathcal{O}_S$ linear map

$$(\underline{\omega}_{E/S})^{\otimes 2} \to \Omega^1_{S/R}.$$

One knows that this mapping is an *isomorphism* if and only if the representable moduli problem on (Ell/R) represented by E/S/R is *etale* over (Ell/R).

Thus if $\mathcal{P}$ is a representable problem which is etale over (Ell/R), we have a canonical isomorphism of line bundles on $\mathcal{M}(\mathcal{P})$

$$\underline{\omega}^{\otimes 2} \xrightarrow{\sim} \Omega^1_{\mathcal{M}(\mathcal{P})/R}.$$

THEOREM 10.13.11. *Let* R *be an excellent noetherian regular domain whose fraction field has characteristic zero. Let* $\mathcal{P}$ *be a representable moduli problem on* (Ell/R) *which is finite etale over* (Ell/R). [*Then by (8.6.8), we know that* $\overline{\mathcal{M}}(\mathcal{P})$ *is a proper smooth curve over* R, *in which the cusps are finite etale over* R *and for which* dlog(1/j) *is a basis, near the cusps, for* $\Omega^1_{\overline{\mathcal{M}}(\mathcal{P})/R}$ (log cusps).] *The Kodaira-Spencer isomorphism on* $\mathcal{M}(\mathcal{P})$

$$\underline{\omega}^{\otimes 2} \xrightarrow{\sim} \Omega^1_{\mathcal{M}(\mathcal{P})/R}$$

extends to an isomorphism on $\overline{\mathcal{M}}(\mathcal{P})$

$$\underline{\omega}^{\otimes 2} \xrightarrow{\sim} \Omega^1_{\overline{\mathcal{M}}(\mathcal{P})/R}(\log \text{ cusps}),$$

where $\underline{\omega}^{\otimes 2}$ *denotes the canonical extension described above of* $\underline{\omega}^{\otimes 2}$ *on* $\mathcal{M}(\mathcal{P})$. *For any regular noetherian excellent* R*-algebra* R′, *this remains true after the base-change* $R \to R'$.

Proof. In view of (8.6.8), and the formula

$$1/j = q \times (\text{invertible series in } \mathbf{Z}[[q]]),$$

we see that in $\widehat{\text{Cusps}}(\mathcal{P})$, $\Omega^1(\log \text{cusps})$ admits as basis $d\log(q)$. In view of the *definition* of the extension $\underline{\omega}^{\otimes 2}$ in terms of the square $(\omega_{\text{can}})^{\otimes 2}$ of the canonical differential ω_{can} on $\text{Tate}(q)$, it suffices to remark that by an explicit computation (cf. [K-2]), one knows that for the Tate curve $\text{Tate}(q)/\mathbf{Z}((q))$, the Kodaira-Spencer isomorphism carries

$$(\omega_{\text{can}})^{\otimes 2} \mapsto \frac{dq}{q}. \qquad \text{Q.E.D.}$$

REMARK. We will see later how "wrong" this theorem can become in the presence of ramification at finite distance, when the $\mathcal{P}$ in question does not "come from characteristic zero" (cf. 12.9.1).

COROLLARY 10.13.12. *Let* $N \geq 1$ *be an integer,* $\Gamma \subset GL(2, \mathbf{Z}/N\mathbf{Z})$ *a subgroup,* A *the ring* $(\mathbf{Z}[\zeta_N])^{\det \Gamma}$, $\mathcal{P}$ *the moduli problem*

$$([\Gamma(N)]/\Gamma)^{A\text{-can}} \underset{A}{\otimes} A[1/N] \quad \textit{on} \quad (\text{Ell}/A[1/N]).$$

Suppose $\mathcal{P}$ *is representable. Then* $\overline{\mathcal{M}}(\mathcal{P})$ *is a proper smooth curve over* $A[1/N]$ *with geometrically connected fibers, in which the cusps are finite etale over* $A[1/N]$. *Let us denote by*

$\Gamma_0 = \Gamma \cap SL(2, \mathbf{Z}/N\mathbf{Z})$

$g(\mathcal{P})$ = *the common genus of the geometric fibers of* $\overline{\mathcal{M}}(\mathcal{P})$ *over* $A[1/N]$

$c(\mathcal{P})$ = *the (common) number of cusps on the geometric fibers of* $\overline{\mathcal{M}}(\mathcal{P})$ *over* $A[1/N]$

$\deg(\mathcal{P})$ = *the degree with which* $\mathcal{P}$ *is finite etale over* (Ell) = 2 × (*the degree of* $\mathcal{M}(\mathcal{P})$ *as a finite flat covering of* $\text{Spec}(A[1/N][j])$

$\deg(\underline{\omega}_{\mathcal{P}})$ = *one-half the common degree of the restriction to any geometric fiber of the line bundle* $\underline{\omega}^{\otimes 2}$ *on* $\overline{\mathcal{M}}(\mathcal{P})$ *over* $A[1/N]$

= *the degree of* $\underline{\omega}$ *when that exists on* $\overline{\mathcal{M}}(\mathcal{P})$.

These quantities are related by the following formulas:

$$\begin{cases} 2\deg(\underline{\omega}_{\mathcal{P}}) = 2g(\mathcal{P}) - 2 + c(\mathcal{P}) \\ c(\mathcal{P}) = \#(\text{Hom Surj}((\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}/N\mathbf{Z})/\pm\Gamma_0) \\ \deg(\mathcal{P}) = \#(SL(2, \mathbf{Z}/N\mathbf{Z})/\Gamma_0) \\ \deg(\underline{\omega}_{\mathcal{P}}) = \frac{1}{24}\deg(\mathcal{P}) = \frac{\#(SL(2, \mathbf{Z}/N\mathbf{Z}))}{24\,\#(\Gamma_0)}. \end{cases}$$

Proof. Extending scalars from $A[1/N]$ to $\mathbf{Z}[\zeta_N, 1/N]$ amounts to replacing Γ by $\Gamma_0 = \Gamma \cap SL(2, \mathbf{Z}/N\mathbf{Z})$. The first formula is the numerical incarnation of the isomorphism

$$\underline{\omega}^{\otimes 2} \simeq \Omega^1(\log \text{cusps}) \quad \text{on} \quad \overline{\mathcal{M}}(\mathcal{P}).$$

The second has already been proven (10.9.1). The third is clear since $[\Gamma(N)]^{\text{can}}[1/N]$ is finite etale galois over $(\text{Ell}/\mathbf{Z}[\zeta_N, 1/N])$ with galois group $SL(2, \mathbf{Z}/N\mathbf{Z})$, and $\mathcal{P}$ is its quotient by Γ_0. To prove the fourth, we argue as follows. By explicit calculation ([Ig 2] and [K-2 AI, 5.5]) the theorem is true for $N = 3$, and $\Gamma_0 = \{1\}$; in this case

$$\begin{cases} \overline{\mathcal{M}} = \mathbf{P}^1, \text{ the } \mu\text{-line} \\ \text{cusps} = \{\infty\} \cup \{\text{the roots of } \mu^3 = 27\} \\ \underline{\omega} = \mathcal{O}(1) \\ \text{universal curve: } X^3 + Y^3 + Z^3 = \mu XYZ. \end{cases}$$

By (10.13.5), the ratio

$$\frac{\deg(\underline{\omega}_{\mathcal{P}})}{\deg(\mathcal{P})}$$

is independent of the particular choice of $\mathcal{P}$ of the form $[\Gamma(N)]^{can}/\Gamma_0$ for some N and some $\Gamma_0 \subset SL(2, \mathbf{Z}/N\mathbf{Z})$, for (10.13.5) allows us to replace $\mathcal{P}$ by $[\Gamma(N)]^{can}$, $[\Gamma(N)]^{can}$ by $[\Gamma(3N)]^{can}$, and finally $[\Gamma(3)]^{can}$, in which case we have checked it directly. Q.E.D.

Chapter 11

INTERLUDE – EXOTIC MODULAR MORPHISMS AND ISOMORPHISMS

(11.1) *Motivation*

Let R be a ring, $\mathcal{P}$ and $\mathcal{P}'$ two moduli problems on (Ell/R). So far we have been content to always view $\mathcal{P}$ and $\mathcal{P}'$ as lying *over* (Ell/R), and we have only considered morphisms between them which are morphisms of moduli problems on (Ell/R) (i.e., morphisms between functors on (Ell/R)). However, it is convenient, and often essential, to view $\mathcal{P}$ and $\mathcal{P}'$ as "abstract" objects, rather than as "objects over (Ell/R)", and to have a notion of "abstract" morphism between them. For example, if $\mathcal{P}$ and $\mathcal{P}'$ are both representable, by universal families $E/\mathcal{M}(\mathcal{P})$ and $E'/\mathcal{M}(\mathcal{P}')$, then we certainly want to be able to speak of R-maps between the R-schemes $\mathcal{M}(\mathcal{P})$ and $\mathcal{M}(\mathcal{P}')$.

(11.2) *"Abstract" morphisms*[*]

With this preamble, we now define an "abstract" morphism

$$\mathcal{P} \to \mathcal{P}'$$

to be a rule which for every R-scheme S and every elliptic E/S with level $\mathcal{P}$-structure $x \in \mathcal{P}(E/S)$, assigns an elliptic curve E'/S with level $\mathcal{P}'$-structure $x' \in \mathcal{P}(E'/S)$, and which to every morphism in (Ell/R)

$$x_1 = (\alpha, f)^*(x) \in \mathcal{P}(E_1/S_1); \quad \begin{array}{ccc} E_1 & \xrightarrow{\alpha} & E \\ \downarrow & & \downarrow \\ S_1 & \xrightarrow{f} & S \end{array} \quad x \in \mathcal{P}(E/S)$$

assigns a morphism in (Ell/R) with the *same* f

[*] Interchangeably called "exotic."

$$\begin{array}{ccc} (x_1)' \in \mathcal{P}'(E_1'/S_1)\ ;\ E_1' & \xrightarrow{\alpha'} & E'\ ;\ x' \in \mathcal{P}'(E'/S) \\ \downarrow & & \downarrow \\ S_1 & \xrightarrow{f} & S \end{array}$$

such that $(x_1)' = (\alpha', f)^*(x')$, and such that the construction

$$(\alpha, f) \mapsto (\alpha', f)$$

is compatible with composition of morphisms in (Ell/R).

Clearly if both $\mathcal{P}$ and $\mathcal{P}'$ are representable, then any such abstract morphism induces a morphism of R-schemes

$$\mathcal{M}(\mathcal{P}) \to \mathcal{M}(\mathcal{P}')\ ,$$

simply by passing to isomorphism classes.

(11.3) *Some basic examples*

(11.3.1) The involution "W_N" of $[\Gamma_0(N)]$ is defined by

$$\begin{array}{c} (E/S,\ \text{cyclic subgroup } G \text{ of order } N) \\ \downarrow \\ (E' = (E \bmod G)/S,\ G' = E[N] \bmod G)\ . \end{array}$$

(11.3.2) The automorphism "W_N" of $([\text{bal.}\,\Gamma_1(N)]^{\text{can}}, [\Gamma_1(M)])$ with $(N,M) = 1$. Let us consider an E/S with both a balanced $\Gamma_1(N)$-structure

$$P;\ E \underset{\pi^t}{\overset{\pi}{\rightleftarrows}} E';\ Q$$

and a $[\Gamma_1(M)]$-structure $A \in E[M](S)$. Because $(N,M) = 1$, π and π^t each induces isomorphisms $E[M] \underset{\pi^t}{\overset{\pi}{\rightleftarrows}} E'[M]$, so that πA has exact order M on E'/S. Then "W_N" is the automorphism

$$\begin{array}{c} P;\ E \underset{\pi^t}{\overset{\pi}{\rightleftarrows}} E';\ Q;\ A \\ \downarrow \\ -Q;\ E' \underset{\pi^t}{\overset{\pi}{\rightleftarrows}} E;\ P;\ \pi A\ . \end{array}$$

The square W_N^2 of this exotic automorphism is the automorphism of $([\text{bal.}\,\Gamma_1(N)]^{\text{can}}, [\Gamma_1(M)])$ as moduli problem on $(\text{Ell}/\mathbf{Z}[\zeta_N])$ which is

$$(P, Q, A) \mapsto (-P, -Q, NA)\ .$$

(11.3.3) The two projections of $[\text{bal.}\,\Gamma_1(p^n)]^{\text{can}}$ to $[\text{bal.}\,\Gamma_1(p^{n-1})]^{\text{can}}$. The first is:

$$\begin{array}{c} P_0;\ E_0 \underset{\lambda_{1,0}}{\overset{\pi_{0,1}}{\rightleftarrows}} E_1 \rightleftarrows \cdots \underset{\lambda_{n,n-1}}{\overset{\pi_{n-1,n}}{\rightleftarrows}} E_n;\ Q_n \\ \downarrow \\ pP_0;\ E_0 \rightleftarrows \cdots \rightleftarrows E_{n-1};\ \lambda_{n,n-1}(Q_n)\ . \end{array}$$

The second is:

$$\begin{array}{c} - - - - - - - - - - - \\ \downarrow \\ \pi_{0,1}(P_0);\ E_1 \rightleftarrows \cdots \rightleftarrows E_n;\ pQ_n\ . \end{array}$$

(11.3.4) The isomorphism

$$[\Gamma_0(p^{2n}); n, n]^{\text{can}} \xrightarrow{\sim} [\Gamma(p^n)]^{\text{can}}$$

defined by

$$\begin{array}{ccccc} & & P_n & & \\ & & \cap & & \\ E_0 & \underset{\lambda_{n,0}}{\overset{\pi_{0,n}}{\rightleftarrows}} & E_n & \underset{\lambda_{2n,n}}{\overset{\pi_{n,2n}}{\rightleftarrows}} & E_{2n} \\ & & \cup & & \\ & & Q_n & & \end{array}$$

$$\downarrow$$

$$E_n\,;\ (P_n,Q_n)\,.$$

To see that the map is defined, we must show that (P_n,Q_n) is a Drinfeld p^n-basis on E_n. This is clear if p is invertible (for example, because $e_{p^n}(P_n,Q_n) = \langle P_n, \pi_{n,2n}Q_n\rangle$ is a primitive p^n'th root of unity), and therefore holds universally, because $[\Gamma_0(p^{2n});n,n]$ is flat over $\mathbf{Z}$.

The inverse map is defined by

$$E_n\,;\ (P_n,Q_n)$$

$$\downarrow$$

$$E_n/\text{cyclic } p^n\text{-group} = E_0 \xleftarrow[\text{mod } Q_n]{} E_n \xrightarrow{\text{mod } P_n} E_{2n} = E_n/\text{cyclic } p^n\text{-group}$$

$$\text{generated by } Q_n \qquad\qquad \text{generated by } P_n\,.$$

To see that this map is well defined, we must see that the lower diagram is cyclic in standard order. Since the question is f.p.p.f. local on S, we may suppose given P_0 on E_0 such that $\pi_{0,n}P_0 = P_n$. We must show that p^nP_0 generates $\operatorname{Ker}\pi_{0,n}$. We easily calculate

$$p^nP_0\,\lambda_{n,0}\pi_{0,n}P_0 = \lambda_{n,0}P_n = P_n \bmod Q_n\,,$$

and so we are reduced to the already noted fact (5.5.2) that $(P_n \bmod Q_n;\ E_0 \rightleftarrows E_n;Q_n)$ is indeed a balanced $\Gamma_1(p^n)$-structure.

(11.3.5) The isomorphism

$$[\Gamma(p^n)]/\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \xrightarrow{\sim} [\Gamma_0(p^{2n})]\,.$$

We have already noted that $[\Gamma(p^n)]$ modulo the full Cartan subgroup of $GL(2,\mathbf{Z}/p^n\mathbf{Z})$ is regular and two-dimensional. It is easy to check that its modular interpretation is this: a $[\Gamma(p^n)]/\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$-structure on E/S is a *pair* of cyclic subgroups of order p^n in E/S, say G_1 and G_2, which are *transverse* in the sense that locally f.p.p.f., if P is a generator of G_1 and if Q is a generator of G_2, then (P,Q) is a Drinfeld p^n-basis of E.

This said, the asserted isomorphism is given by

$$E\,;\ G_1,G_2$$

$$\downarrow$$

$$E \bmod G_1 \longleftarrow E \longrightarrow E \bmod G_2\,,$$

and its inverse is given by

$$E_0 \underset{\lambda_{n,0}}{\overset{\pi_{0,n}}{\rightleftarrows}} E_n \underset{\lambda_{2n,n}}{\overset{\pi_{n,2n}}{\rightleftarrows}} E_{2n}$$

$$\downarrow$$

$$E_n,\ \operatorname{Ker}(\lambda_{n,0}),\ \operatorname{Ker}(\pi_{n,2n})\,.$$

Chapter 12

NEW MODULI PROBLEMS IN CHARACTERISTIC p; IGUSA CURVES

(12.1) *Frobenius*

Throughout this chapter, p is a fixed prime number. For any $\mathbf{F}_p$-scheme S, we denote by

$$F_{abs} : S \to S \tag{12.1.1}$$

the morphism "absolute Frobenius", which on affine rings corresponds to the endomorphism $x \mapsto x^p$.

If we are given a scheme $X/S/\mathbf{F}_p$, we denote by $X^{(p)}/S$ the scheme defined by the cartesian diagram

(12.1.2)

$$\begin{array}{ccc} X^{(p)} & \longrightarrow & X \\ \downarrow & & \downarrow \\ S & \xrightarrow{F_{abs}} & S\,. \end{array}$$

If we are given a contravariant functor

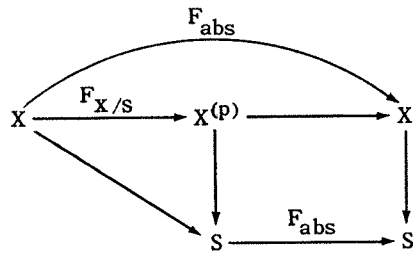
$$\mathcal{F} : (\mathrm{Sch}/S) \to (\mathrm{sets})\,, \tag{12.1.3}$$

S being an $\mathbf{F}_p$-scheme, we denote by $\mathcal{F}^{(p)}$ the functor on (Sch/S) defined by

$$\mathcal{F}^{(p)}(X/S) = \mathcal{F}(X^{(p)}/S)\,. \tag{12.1.4}$$

If $\mathcal{F}$ is representable, by an S-scheme T, then $\mathcal{F}^{(p)}$ is represented by $T^{(p)}$.

For a scheme $X/S/\mathbf{F}_p$, the absolute Frobenius of X has a canonical factorization as



where the relative Frobenius $F = F_{X/S}$

$$F : X \to X^{(p)}$$

is S-linear. If S is affine, $S = \mathrm{Spec}(A)$, then locally on X we have $X = \mathrm{Spec}(B)$ with

$$B = A[X_1, X_2 \cdots]/(\cdots f_i(X), \cdots)\,,$$

while $X^{(p)}$ is $\mathrm{Spec}(B^{(p)})$ with

$$B^{(p)} = A[X_1, X_2, \cdots]/(\cdots, f_i^{(p)}(X), \cdots)$$

where $f_i^{(p)}(X) \in A[X]$ are the polynomials obtained from the polynomials $f_i \in A[X]$ by raising coefficients to the p'th power. The relative Frobenius map $F : X \to X^{(p)}$ is the map whose effect on R-valued points, R any A-algebra, is

$$\begin{array}{ccc} (X_1, X_2, \cdots) & \longmapsto & (X_1^p, X_2^p, \cdots) \\ \text{solutions of } f_i = 0 & & \text{solutions of } f_i^{(p)} = 0\,. \end{array}$$

(12.2) *Basic lemmas*

LEMMA 12.2.1. *Let $E/S/\mathbf{F}_p$ be an elliptic curve over an $\mathbf{F}_p$-scheme. Then for every $n \geq 1$, the iterated relative Frobenius*

$$F^n : E \to E^{(p^n)}$$

is a cyclic p^n*-isogeny.*

Proof. Because E/S is smooth of relative dimension one, F^n is finite locally free of rank p^n. It is cyclic because the origin $P = 0$ is a generator of $\mathrm{Ker}(F^n)$. Q.E.D.

(12.2.2) Given $E/S/\mathbf{F}_p$, the dual isogeny to $F : E \to E^{(p)}$ is the Verschiebung denoted

$$V : E^{(p)} \to E .$$

The dual of $F^n : E \to E^{(p^n)}$ is the iterated Verschiebung

$$V^n : E^{(p^n)} \to E .$$

LEMMA 12.2.3. *Let* $E/S/\mathbf{F}_p$ *be an elliptic curve over an* $\mathbf{F}_p$*-scheme. Then for every* $n \geq 1$, *the iterated Verschiebung*

$$V^n : E^{(p^n)} \to E$$

is a cyclic p^n*-isogeny.*

Proof. By (5.5.4, (3)), the dual of a cyclic isogeny is cyclic. Q.E.D.

LEMMA 12.2.4. *Let* $E/S/\mathbf{F}_p$ *be an elliptic curve over an* $\mathbf{F}_p$*-scheme,* $n \geq 1$ *an integer. Then*

(1) *The "standard factorization" (6.7.6) of* F^n *into a sequence of* n p*-isogenies is*

$$E \xrightarrow{F} E^{(p)} \xrightarrow{F} E^{(p^2)} \longrightarrow \cdots \xrightarrow{F} E^{(p^n)} .$$

(2) *The "standard factorization" of* V^n *into a sequence of* n p*-isogenies is*

$$E^{(p^n)} \xrightarrow{V} E^{(p^{n-1})} \longrightarrow \cdots \xrightarrow{V} E .$$

Proof. By (6.7.9), it suffices to prove (1), and (1) is obvious, using the origin as generator of $\mathrm{Ker}(F^n)$ to compute its standard cyclic subgroups. Q.E.D.

LEMMA 12.2.5. *Let* $E/S/\mathbf{F}_p$ *be an elliptic curve over an* $\mathbf{F}_p$*-scheme,* $n \geq 1$ *an integer. Then the* p^{2n}*-isogeny*

$$p^n : E \to E$$

is cyclic, and its standard factorization into two cyclic p^n*-isogenies is*

$$E \xrightarrow{F^n} E^{(p^n)} \xrightarrow{V^n} E .$$

Proof. Certainly $p^n = V^n \circ F^n$, and both V^n and F^n are cyclic. It suffices to show that (F^n, V^n) are cyclic in standard order. Locally f.p.p.f. on S, we may choose a generator Q of $\mathrm{Ker}\, V^n$, and a point P on E with $F^n(P) = Q$. By the standard-order criterion (6.7.13), we must show that $p^n P$ generates $\mathrm{Ker}(F^n)$. But $p^n P = V^n F^n P = V^n Q = 0$, and 0 does generate $\mathrm{Ker}(F^n)$. Q.E.D.

COROLLARY 12.2.6. *Let* S *be an arbitrary scheme,* p *a prime number,* $n \geq 1$ *an integer, and* E/S *an elliptic curve. Then* S *is an* $\mathbf{F}_p$*-scheme if and only if the* p^{2n}*-isogeny*

$$p^n : E \to E$$

is cyclic.

Proof. If $p^n : E \to E$ is cyclic, locally f.p.p.f. on S we may choose a generator P, which will consequently have "exact order p^{2n}." Therefore $p^n P = 0$ has "exact order p^n" on E, whence by (5.3.3) S is an $\mathbf{F}_p$-scheme. Q.E.D.

PROPOSITION 12.2.7. *Let* $E/S/\mathbf{F}_p$ *be an elliptic curve over an* $\mathbf{F}_p$*-scheme,* $n \geq 1$ *an integer, and* $P \in E[p^n](S)$ *a point killed by* p^n. *The following conditions are equivalent.*

(1) P *generates* $\mathrm{Ker}(p^n : E \to E)$.

(2) $F^n(P)$ *generates* $\mathrm{Ker}(V^n : E^{(p^n)} \to E)$.

(3) (O, P) *is a Drinfeld* p^n*-basis on* E.

(4) *There exists an elliptic curve* E_n/S *and an isomorphism* $E \simeq E_n^{(p^n)}$, *under which* P *generates* $\mathrm{Ker}(V^n : E_n^{(p^n)} \to E_n)$.

Proof. That (1) $\Longleftrightarrow$ (2) is by the standard-order criterion (6.7.13), applied to the standard factorization (F^n, V^n) of p^n, and the point P. That (2) $\Longleftrightarrow$ (3) results from (5.5.5), applied to (O, P); the origin having exact order p^n and generating $\mathrm{Ker}(F^n)$, (O, P) is a p^n-basis on E if and only if $F^n(P)$ on $E^{(p^n)}$ generates the dual isogeny $V^n : E^{(p^n)} \to E$. To prove (3) $\Longrightarrow$ (4), we apply (5.5.5) to the Drinfeld p^n-basis (P,O). The point P must have "exact order p^n", so let $K \subset E$ denote the cyclic subgroup of order p^n it generates, and let E_n denote the quotient of E by K, $\pi_n : E \to E_n$ the projection. The image of the second point O in E_n must generate the dual p^n-isogeny. But this image is the origin in E_n, which as point of exact order p^n generates $\mathrm{Ker}(F^n : E_n \to E_n^{(p^n)})$. Therefore our diagram of dual isogenies is

$$\begin{array}{ccc} E & \overset{\pi_n}{\underset{F^n}{\rightleftarrows}} & E_n \\ \downarrow & & \\ E_n^{(p^n)} & & \end{array},$$

with P generating $\mathrm{Ker}(\pi_n)$. Because π_n is the dual of F^n, we have $\pi_n = V^n : E_n^{(p^n)} \to E_n$, so $E \simeq E_n^{(p^n)}$ with P generating $\mathrm{Ker}(V^n)$, as required.

To show that (4) $\Longrightarrow$ (1), let E_n be an elliptic curve over S, and $P \in E_n^{(p^n)}(S)$ a generator of $\mathrm{Ker}(V^n : E_n^{(p^n)} \to E_n)$. We must show that P is a generator of the composite

$$E_n^{(p^n)} \xrightarrow{V^n} E_n \xrightarrow{F^n} E_n^{(p^n)},$$

whose *standard* factorization is

$$E_n^{(p^n)} \xrightarrow{F^n} E_n^{(p^{2n})} \xrightarrow{V^n} E_n^{(p^n)}.$$

By the standard order criterion (6.7.13), we must show that

$$\begin{cases} p^n P \text{ generates } \mathrm{Ker}(F^n : E_n^{(p^n)} \to E_n^{(p^{2n})}) \\ F^n(P) \text{ generates } \mathrm{Ker}(V^n : E_n^{(p^{2n})} \to E_n^{(p^n)}). \end{cases}$$

The first condition holds because $p^n P = F^n V^n P = F^n O = 0$ generates $\mathrm{Ker}\, F^n$; the second because P generates $\mathrm{Ker}(V^n : E_n^{(p^n)} \to E_n)$, and the situation at hand is obtained from this one by the change of base

$$S \xrightarrow{F^n_{abs}} S. \qquad \text{Q.E.D.}$$

(12.3) *Igusa structures*

(12.3.1) DEFINITION. Let $E/S/F_p$ be an elliptic curve over an F_p-scheme, $n \geq 0$ an integer. An Igusa-structure of level p^n on E/S is a point $P \in E^{(p^n)}(S)$ which *generates* the kernel of

$$V^n : E^{(p^n)} \to E.$$

We denote by $[\mathrm{Ig}(p^n)]$ the corresponding moduli problem on (Ell/F_p):

(12.3.1.1) $[\mathrm{Ig}(p^n)](E/S) = \text{generators of } \mathrm{Ker}(V^n : E^{(p^n)} \to E)$.

PROPOSITION 12.3.2. *Let* $E/S/F_p$ *be an elliptic curve over an* F_p*-scheme,* $n \geq 1$ *an integer. Then*

(1) *a point* $P \in E(S)$ *generates* $\mathrm{Ker}(p^n : E \to E)$ *if and only if the point* $p^{n-1}P$ *generates* $\mathrm{Ker}(p : E \to E)$.

(2) *a point* $P \in E(S)$ *generates* $\mathrm{Ker}(p^n : E \to E)$ *if and only if the point* $p^{n-1}F(P) \in E^{(p)}(S)$ *generates* $\mathrm{Ker}(V : E^{(p)} \to E)$.

(3) *a point* $Q \in E^{(p^n)}(S)$ *generates* $\mathrm{Ker}(V^n : E^{(p^n)} \to E)$ *if and only if the point* $V^{n-1}(Q) \in E^{(p)}(S)$ *generates* $\mathrm{Ker}(V : E^{(p)} \to E)$.

Proof. For (1), use the fact that P generates $\mathrm{Ker}(p^n)$ if and only if (P, O) is a Drinfeld p^n-basis, and the general fact (5.5.7) that (P, Q) is a Drinfeld p^n-basis if and only if $(p^{n-1}P, p^{n-1}Q)$ is a Drinfeld p-basis. Assertion (2) is the Backing-up Theorem (6.7.11), applied to the standard factorization of $p^n : E \to E$ as $(p^{n-1}F, V)$:

$$E \xrightarrow{F} \cdots \xrightarrow{F} E^{(p^n)} \xrightarrow{V} \cdots \xrightarrow{V} E^{(p)} \xrightarrow{V} E\,.$$
$$\text{(arc: } p^{n-1}F\text{)}$$

Assertion (3) is the Backing-up theorem applied to the standard factorization of $V^n : E^{(p^n)} \to E$ as (V^{n-1}, V):

$$E^{(p^n)} \xrightarrow{V} \cdots \xrightarrow{V} E^{(p)} \xrightarrow{V} E\,.$$
$$\text{(arc: } V^{n-1}\text{)}$$

Q.E.D.

PROPOSITION 12.3.3. *Let* k *be an algebraically closed field of characteristic* p, *E/k an elliptic curve,* $P \in E^{(p)}(k)$ *a point which generates* $\mathrm{Ker}(V : E^{(p)} \to E)$. *(Such points exist because* Ker V *is cyclic, and* k *is algebraically closed.) Then*

(1) *If* $P = 0$, *then for every* $n \geq 1$ *the origin in* $E(k)$ *generates* $\mathrm{Ker}(p^n : E \to E)$, *and the origin in* $E^{(p^n)}(k)$ *generates* $\mathrm{Ker}\, V^n : E^{(p^n)} \to E$. *In particular, we have* $\mathrm{Ker}(p^n : E \to E) = \mathrm{Ker}(F^{2n} : E \to E^{(p^{2n})})$, *and we have* $\mathrm{Ker}(V^n : E^{(p^n)} \to E) = \mathrm{Ker}(F^n : E^{(p^n)} \to E^{(p^{2n})})$.

(2) *If* $P \neq 0$, *then* $V : E^{(p)} \to E$ *is etale. If we choose points* $P_n \in E^{(p^n)}(k)$ *with* $P_1 = P$, $VP_{n+1} = P_n$, *then* P_n *generates* $\mathrm{Ker}(V^n : E^{(p^n)} \to E)$, V^n *is etale, and* P_n *defines an isomorphism*

$$\mathbf{Z}/p^n\mathbf{Z} \xrightarrow{\sim} \mathrm{Ker}(V^n : E^{(p^n)} \to E)\,.$$

Proof. If $P = 0$ generates $\mathrm{Ker}(V : E^{(p)} \to E)$, then the previous proposition shows that the origin generates $\mathrm{Ker}(p^n)$ and $\mathrm{Ker}(V^n)$ for all $n \geq 1$. If $P \neq 0$ generates $\mathrm{Ker}(V : E^{(p)} \to E)$, then $\mathrm{Ker}(V)$ must be etale because over a field k, a group of rank p is either etale or connected, and in the latter case it has no non-trivial k-points. Therefore $V : E^{(p)} \to E$ is etale, so also (by the base change F^n_{abs} on k) $V : E^{(p^{n+1})} \to E^{(p^n)}$ is etale for all $n \geq 1$. By the previous proposition, P_n generates $\mathrm{Ker}(V^n)$, so by (1.8.3) it defines an isomorphism $\mathbf{Z}/p^n\mathbf{Z} \xrightarrow{\sim} \mathrm{Ker}(V^n)$ as required. Q.E.D.

COROLLARY 12.3.4. *Let* k *be an algebraically closed field of characteristic* p, *E/k an elliptic curve. Then either* $p : E(k) \to E(k)$ *is bijective, or for every* $n \geq 1$ *the group* $E[p^n](k)$ *is cyclic of order* p^n.

Proof. If $P = 0$ in the preceding proposition, then $\mathrm{Ker}(p) = \mathrm{Ker}(F^2)$ has no non-trivial k-valued points. Because k is algebraically closed the maps $p^n : E \to E$ are always *surjective* on k-valued points. If $P \neq 0$, then the P_n's of the preceding proposition give isomorphisms

$$\mathbf{Z}/p^n\mathbf{Z} \xrightarrow{\sim} \mathrm{Ker}(V^n : E^{(p^n)} \to E)\,,$$

whose Cartier duals are isomorphisms

$$\mu_{p^n} \xleftarrow{\sim} \mathrm{Ker}(F^n : E \to E^{(p^n)})\,.$$

So in this case the standard factorization of p^n as (F^n, V^n) yields the short exact sequence of k-group-schemes

$$0 \to \mu_{p^n} \to E[p^n] \to \mathbf{Z}/p^n\mathbf{Z} \to 0 .$$

Because k is algebraically closed, this exact sequence yields an isomorphism of k-points

$$E[p^n](k) \xrightarrow{\sim} \mathbf{Z}/p^n\mathbf{Z} . \qquad \text{Q.E.D.}$$

COROLLARY 12.3.5. *Let* k *be an algebraically closed field of characteristic* p, *and* E/k *an elliptic curve. Then either* $\mathrm{Ker}(p^n) = \mathrm{Ker}(F^{2n})$ *for every* $n \geq 1$, *or there exists an isomorphism of* p*-divisible groups*

$$E[p^\infty] \simeq \mu_{p^\infty} \times \mathbf{Q}_p/\mathbf{Z}_p .$$

Proof. The first case occurs when $\mathrm{Ker}(V : E^{(p)} \to E)$ is generated by $P = 0$, the second when $P \neq 0$. Then the compatible $P_n \in E^{(p^n)}(k)$ with $VP_{n+1} = P_n$, $P_1 = P$ lead as above to an exact sequence

$$0 \to \mu_{p^\infty} \to E[p^\infty] \to \mathbf{Q}_p/\mathbf{Z}_p \to 0 .$$

Any compatible choice of points $Q_n \in E(k)$ with $F^n(Q_n) = P_n$ splits it. Q.E.D.

Recall (cf. 2.9.3, 2.9.4) that an elliptic curve E over an algebraically closed field k of characteristic $p > 0$ is called *ordinary* if $E(k)$ has non-trivial points of order p, *supersingular* if not. An elliptic curve $E/S/\mathbf{F}_p$ over an $\mathbf{F}_p$-scheme is called *ordinary* if every one of its geometric fibers is ordinary.

PROPOSITION 12.3.6. *Let* $E/S/\mathbf{F}_p$ *be an elliptic curve over an* $\mathbf{F}_p$*-scheme. The following conditions are equivalent:*

(0) $E/S/\mathbf{F}_p$ *is ordinary.*

(1) *The Verschiebung* $V : E^{(p)} \to E$ *is etale.*

(2) *For some integer* $n \geq 1$, $V^n : E^{(p^n)} \to E$ *is etale.*

(3) *For every integer* $n \geq 1$, $V^n : E^{(p^n)} \to E$ *is etale.*

(4) *The tangent map of Verschiebung* $\mathrm{tg}(V) : \mathrm{Lie}(E/S)^{(p)} \to \mathrm{Lie}(E/S)$ *is an isomorphism.*

(5) *For every geometric point* $\mathrm{Spec}(k) \to S$ *of* S, *the group* $(E \underset{S}{\otimes} k)(k)$ *contains exactly* p^n *points killed by* p^n, *for every* $n \geq 1$.

(6) *For some* $n \geq 1$, *and every geometric point* $\mathrm{Spec}(k) \to S$ *of* S, *the group* $(E \underset{S}{\otimes} k)(k)$ *contains exactly* p^n *points killed by* p^n.

(7) *For every geometric point* $\mathrm{Spec}(k) \to S$ *of* S, *the group* $(E \underset{S}{\otimes} k)(k)$ *contains a non-trivial point of order* p.

(8) *For every geometric point* $\mathrm{Spec}(k) \to S$ *of* S, *the group* $(E \underset{S}{\otimes} k)(k)$ *contains infinitely many points of* p*-power order.*

Proof. Clearly each of the conditions holds if and only if it holds on each geometric fiber, so we are reduced to the case $S = \mathrm{Spec}(k)$ with k algebraically closed of characteristic p, in which case the result is immediate from (12.3.5). Q.E.D.

COROLLARY 12.3.7. *If* $E \to E'$ *is an isogeny of elliptic curves over an* $\mathbf{F}_p$*-scheme* S, *then* E/S *is ordinary if and only if* E'/S *is ordinary.*

Proof. Obvious from (8) above. Q.E.D.

(12.4) *The Hasse invariant*

(12.4.1) Given $E/S/\mathbf{F}_p$, formation of the tangent map to Verschiebung

$$\begin{aligned} \mathrm{tg}(V) \in \mathrm{Hom}_S(\mathrm{Lie}(E/S)^{(p)}, \mathrm{Lie}(E/S)) \\ = \mathrm{Hom}_S((\mathrm{Lie}(E/S))^{\otimes p}, \mathrm{Lie}(E/S)) \\ = H^0(S, (\underline{\omega}_{E/S})^{\otimes(p-1)}) \end{aligned}$$

may be viewed as defining a modular form of weight $p-1$, the *Hasse invariant*, denoted A. Here are four concrete ways to calculate this modular form. Suppose that S is affine, $S = \mathrm{Spec}(R)$ with R an $\mathbf{F}_p$-algebra, and that, (Zariski localizing on R if necessary) the invertible R-module

$$\underline{\omega}_{E/R} = H^0(E, \Omega^1_{E/R})$$

of invariant one-forms on E/R admits an R-basis ω, i.e., ω is a nowhere vanishing invariant one-form on E/R.

Let D be the invariant derivation of E/R dual to ω, and let X be a parameter for the formal group $\hat{E}/R$ which is adapted to ω in the sense that

$$\omega|\hat{E} = (1 + \text{higher terms})dX .$$

In terms of the bases $D^{(p)}$, D of $\mathrm{Lie}(E/S)^{(p)}$ and $\mathrm{Lie}(E/S)$ respectively, we have $\mathrm{tg}(V) = A(E, \omega) \in R$.

(12.4.1.1) *First calculation.* In the formal-group expression of the endomorphism "multiplication by p" as a power series in X,

$$[p](X) = V(F(X)) = V(X^p) ,$$

we see that

$$A(E, \omega) = \mathrm{tg}(V) = \text{coefficient of } X^p \text{ in } [p](X) .$$

(12.4.1.2) *Second calculation.* Use autoduality of elliptic curves to view $\mathrm{Lie}(E/R)$ as $H^1(E, \mathcal{O}_E)$. Then $\mathrm{tg}(V)$, viewed as a p-linear endomorphism of $\mathrm{Lie}(E/R)$, is the p-linear endomorphism of $H^1(E, \mathcal{O}_E)$ induced by F_{abs} on $\mathcal{O}_E$. Therefore if we denote by $\eta \in H^1(E, \mathcal{O}_E)$ the Serre-dual basis to ω, we have

$$F_{abs}(\eta) = A(E, \omega)\eta \quad \text{in} \quad H^1(E, \mathcal{O}_E) .$$

(12.4.1.3) *Third calculation.* In terms of the invariant derivation D dual to ω, we have

$$D^p = A(E, \omega) \cdot D .$$

(12.4.1.4) *Fourth calculation.* Denote by $\omega^{(p)}$ the invariant one-form on $E^{(p)}/S$ obtained by extension of scalars $S \xrightarrow{F_{abs}} S$ from ω. The Cartier isomorphism (cf. [K-1]) of sheaves on $E^{(p)}$

$$\mathcal{H}^i(F_*\Omega^\cdot_{E/S}) \xrightarrow{\mathcal{C}} \Omega^i_{E^{(p)}/S} ,$$

induces an S-linear map, the Cartier operator C,

$$\begin{array}{ccccc} H^0(E, \Omega^1_{E/S}) & \xrightarrow{\sim} & H^0(E^{(p)}, F_*\Omega^1_{E/S}) & \longrightarrow & H^0(E^{(p)}, \mathcal{H}^1(F_*\Omega^\cdot_{E/S})) \\ & \searrow^{C} & & & \downarrow \mathcal{C} \\ & & & & H^0(E^{(p)}, \Omega^1_{E^{(p)}/S}) \end{array} ,$$

and we have

$$C(\omega) = A(E, \omega) \cdot \omega^{(p)} .$$

THEOREM 12.4.2. *Over any F_p-algebra R, the value of the Hasse invariant on the Tate curve $\mathrm{Tate}(q)/R((q))$ is given by*

$$A(\mathrm{Tate}(q), \omega_{can}) = 1 .$$

Proof. The differential ω_{can} is $\phi^*_{can}(dX/X)$, where ϕ_{can} is the canonical isomorphism (8.8, T.2)

$$\phi_{can} : \widehat{\mathrm{Tate}(q)} \xrightarrow{\sim} \hat{G}_m$$

and X is the standard multiplicative coordinate on $\hat{G}_m$. The dual-to-ω_{can} derivation D of $\mathrm{Tate}(q)/R((q))$ thus induces the standard invariant derivation $X\frac{d}{dX}$ of $\hat{G}_m$. Because R is an F_p-algebra, we have

$$\left(X\frac{d}{dX}\right)^p = X\frac{d}{dX} ,$$

whence $A(\mathrm{Tate}(q), \omega_{can}) = 1$, as required. Q.E.D.

THEOREM 12.4.3 (Igusa). *The Hasse invariant has simple zeroes, i.e., if k is a perfect field of characteristic p, and R an artin local k-algebra with residue field k, then for any elliptic curve E/R, the following conditions are equivalent:*

(1) *The Verschiebung* $V : E^{(p)} \to E$ *has* $\mathrm{tg}(V) = 0$.

(2) *There exists a supersingular elliptic curve* E_0/k *and an* R*-isomorphism* $E_0 \underset{k}{\otimes} R \simeq E$.

Proof. Clearly (2) $\Longrightarrow$ (1). If $\mathrm{tg}(V) = 0$, then $\mathrm{Ker}(V)$ lies in $\hat{E}^{(p)}$. Take a coordinate X for the formal group $\hat{E}$ which linearizes the action of $\mu_{p-1} \subset Z_p^\times$, and use the induced coordinate on $\hat{E}^{(p)}$. Then the power series expression for *any* homomorphism $f : \hat{E}^{(p)} \to \hat{E}$ has the form

$$f(X) = \sum_{n \geq 1} a(n) \cdot X^n, \quad a(n) = 0 \text{ unless } n \equiv 1 \mod (p-1),$$
$$a(1) = \mathrm{tg}(f).$$

Therefore if $\mathrm{tg}(V) = 0$, we have

$$V(X) = a(p) X^p + \text{higher terms}.$$

We know that $a(p)$ lies in $R^\times$, because modulo $\max(R)$, E becomes supersingular, and $\mathrm{Ker}(V : E^{(p)} \to E) = \mathrm{Ker}(F : E^{(p)} \to E^{(p^2)})$. Therefore

$$V(X) = X^p \times (\text{invertible series in } X),$$

whence

$$\mathrm{Ker}(V : E^{(p)} \to E) = (X^p = 0) = \mathrm{Ker}(F : E^{(p)} \to E^{(p^2)}).$$

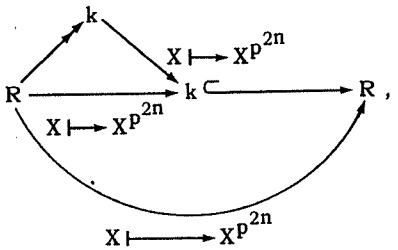
Therefore we obtain an R-isomorphism

$$\begin{array}{ccc} E^{(p)}/\mathrm{Ker}\, V & = & E^{(p)}/\mathrm{Ker}\, F \\ \big\downarrow V & & \big\downarrow F \\ E & \xrightarrow{\sim} & E^{(p^2)}. \end{array}$$

Iterating this isomorphism, we obtain

$$E \xrightarrow{\sim} E^{(p^2)} \xrightarrow{\sim} E^{(p^4)} \xrightarrow{\sim} \cdots \xrightarrow{\sim} E^{(p^{2n})} \xrightarrow{\sim} \cdots.$$

Because R is an artin local k-algebra with (perfect) residue field k, for $n >> 0$ the p^{2n}'th-power map $R \to R$ factors through the subring k of R:



whence

$$E \xrightarrow{\sim} E^{(p^{2n})} \simeq ((E \underset{R}{\otimes} k)^{(p^{2n})}) \underset{k}{\otimes} R. \qquad \text{Q.E.D.}$$

COROLLARY 12.4.4. *Let* k *be an algebraically closed field of characteristic* p, E/k *a supersingular elliptic curve,* $E/k[[T]]$ *its universal formal deformation (to artin local* k*-algebras). There exists a nowhere vanishing invariant one-form* ω *on* $E/k[[T]]$ *in terms of which* $A(E,\omega) = T$.

Proof. For any choice of ω, we have, by Igusa's theorem (12.4.3),

$$A(E,\omega) = T \times (\text{an invertible series in } T)$$
$$= T \times (a \in k^\times) \times (\phi(T) \in 1 + Tk[[T]]).$$

Then the new choice

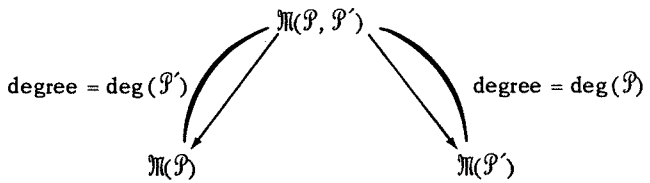
$$(a^{\frac{1}{p-1}})(\phi(T))^{\frac{1}{p-1}} \cdot \omega$$

gives the result. Q.E.D.

THEOREM 12.4.5. *Let* k *be an algebraically closed field of characteristic* p, $\mathcal{P}$ *a representable moduli problem on* (Ell/k) *which is finite etale over* (Ell/k) *of degree* $\deg(\mathcal{P})$. *Then the number of supersingular points on the modular curve* $\mathcal{M}(\mathcal{P})$ *is given by the formula*

$$\#\ \textit{supersingular points on}\ \mathcal{M}(\mathcal{P}) = \frac{p-1}{24}\deg(\mathcal{P})\ .$$

Proof. Let $\mathcal{P}$ and $\mathcal{P}'$ be two such problems. Then the simultaneous problem $(\mathcal{P},\mathcal{P}')$ is a third, and the maps



are finite etale of the indicated degrees.

Therefore it suffices to verify the formula for a single $\mathcal{P}$. Choose any integer $N \geq 3$ prime to p, a primitive N'th root of unity $\zeta_N \in k$, and consider

$$\mathcal{P} = [\Gamma(N)]^{can} \underset{Z[\zeta_N]}{\otimes} k\ .$$

On $\mathcal{M}(\mathcal{P})$, the supersingular points are the zeroes of the Hasse invariant A. By (12.4.2), A extends to a section of $\underline{\omega}^{\otimes(p-1)}$ over all of $\overline{\mathcal{M}}(\mathcal{P})$, and near the cusps it is an invertible section of $\underline{\omega}^{\otimes(p-1)}$. By Igusa's theorem, A has only *simple* zeroes. Therefore (cf. 10.13.12)

$$\begin{aligned}
&\#(\text{supersingular points on } \mathcal{M}(\mathcal{P}))\\
&= \text{total number of zeroes, counting multiplicity,}\\
&\quad \text{of } A \text{ on } \overline{\mathcal{M}}(\mathcal{P})\\
&= \deg(\underline{\omega}^{\otimes(p-1)})\\
&= (p-1)\deg(\underline{\omega}) = (p-1)\times\frac{1}{24}\deg(\mathcal{P}).
\end{aligned}$$

Q.E.D.

COROLLARY 12.4.6. *We have the formula*

$$\frac{p-1}{24} = \sum_{\substack{j\in\overline{F}_p\\ \text{supersingular}}} 1/\#\mathrm{Aut}(E_j)$$

where E_j *denotes a supersingular elliptic curve over* $\overline{F}_p$ *with* j*-invariant* j.

Proof. Let $\mathcal{P}$ be a representable moduli problem on $(\mathrm{Ell}/\overline{F}_p)$ which is finite etale over $(\mathrm{Ell}/\overline{F}_p)$ of degree $\deg(\mathcal{P})$, and consider the map

$$\mathcal{M}(\mathcal{P}) \xrightarrow{j} \mathbb{A}^1_{\overline{F}_p}\ .$$

For each $j \in \overline{F}_p$, the fiber over it is the set of isomorphism classes of pairs $(E_j, \alpha \in \mathcal{P}(E_j))$ where $E_j/\overline{F}_p$ is an elliptic curve with j-invariant j, and α is a level $\mathcal{P}$-structure on E_j. Up to $\overline{F}_p$-isomorphism, E_j is determined by its j, so the cardinality of the fiber over j is

$$\#(\mathcal{P}(E_j)/\mathrm{Aut}(E_j))\ .$$

Because $\mathcal{P}$ is representable, $\mathrm{Aut}(E_j)$ acts freely, so this cardinality is

$$\frac{\#\mathcal{P}(E_j)}{\#\,\mathrm{Aut}(E_j)} = \frac{\deg(\mathcal{P})}{\#\,\mathrm{Aut}(E_j)}\ .$$

Thus we find

$$\begin{aligned}
&\#\text{ supersingular points on } \mathcal{M}(\mathcal{P})\\
&= \sum_{\text{supersingular j}} \#(\text{fiber of } \mathcal{M}(\mathcal{P}) \xrightarrow{j} \mathbb{A}^1 \text{ over j})\\
&= \deg(\mathcal{P}) \sum_{\text{s/s j}} 1/\#\,\mathrm{Aut}(E_j)\ .
\end{aligned}$$

Comparing this with the formula

$$\#\ \text{s/s points on } \mathcal{M}(\mathcal{P}) = \frac{p-1}{24}\times\deg(\mathcal{P})$$

gives the required formula. Q.E.D.

(12.5) *Ordinary curves*

(12.5.1) DEFINITION. We denote by [ord] the moduli problem on (Ell/F_p) defined by

$$[\mathrm{ord}](E/S) = \begin{cases} \text{the set with one element, if} \\ E/S \text{ is ordinary;} \\ \text{the empty set, if not.} \end{cases}$$

LEMMA 12.5.2. *The moduli problem* [ord] *is relatively representable, affine and an open immersion over* $(\mathrm{Ell}/\mathbf{F}_p)$.

Proof. Indeed given $E/S/\mathbf{F}_p$, [ord] is relatively represented by the S-scheme

$$[\mathrm{ord}]_{E/S} = \begin{cases} \text{the open subscheme of } S \text{ where} \\ \text{the section } \mathrm{tg}(V) \text{ of the line} \\ \text{bundle } \omega^{\otimes(p-1)} \text{ is invertible,} \end{cases}$$

which locally on S is defined by inverting a single function. Q.E.D.

(12.5.3) For any moduli problem $\mathcal{P}$ on $(\mathrm{Ell}/R/\mathbf{F}_p)$, we denote by $(\mathcal{P}, \mathrm{ord})$, or $\mathcal{P}^{\mathrm{ord}}$, the simultaneous moduli problem:

$$\mathcal{P}^{\mathrm{ord}}(E/S) = \begin{cases} \text{the set of level } \mathcal{P} \text{ structures} \\ \text{on } E/S, \text{ if } E/S \text{ is ordinary;} \\ \text{the empty set, if not.} \end{cases}$$

LEMMA 12.5.4. *There exists a monic polynomial* $\Phi^{\mathrm{s.s.}}(j) \in \mathbf{F}_p[j]$ *such that for any* $E/S/\mathbf{F}_p$, E/S *is ordinary if and only if* $\Phi^{\mathrm{s.s.}}(j(E))$ *is invertible on* S. *All roots of* $\Phi^{\mathrm{s.s.}}$ *lie in* $\mathbf{F}_{p^2}$.

Proof. Because "ordinary" is checked fiber by fiber, we are reduced to the case $S = \mathrm{Spec}(k)$ with k algebraically closed of characteristic p. Whether E/k is ordinary or supersingular depends only on the isomorphism class of E/k, so only on j(E), k being algebraically closed. We must show that if E/k is supersingular, then $j(E) \in \mathbf{F}_{p^2}$. But we have seen that if E/k is supersingular, then $\mathrm{Ker}(V : E^{(p)} \to E) = \mathrm{Ker}(F : E^{(p)} \to E^{(p^2)})$, whence

$$E \xrightarrow{\sim} E^{(p^2)},$$

and this gives

$$j(E) = j(E^{(p^2)}) = j(E)^{p^2}. \qquad \text{Q.E.D.}$$

COROLLARY 12.5.5. *For any moduli problem* $\mathcal{P}$ *on* $(\mathrm{Ell}/R/\mathbf{F}_p)$ *which is relatively representable and affine over* $(\mathrm{Ell}/R/\mathbf{F}_p)$, *the coarse moduli schemes of* $\mathcal{P}$ *and* $\mathcal{P}^{\mathrm{ord}}$ *are related by*

$$M(\mathcal{P}^{\mathrm{ord}}) = M(\mathcal{P})[1/\Phi^{\mathrm{s.s.}}]$$

as schemes over $\mathrm{Spec}(R[j])$.

Proof. If $\mathcal{P}$ is representable, this is obvious from the general fact that for any $E/S/R$, we have

$$(\mathcal{P}^{\mathrm{ord}})_{E/S} = \mathcal{P}_{E/S}[1/\Phi^{\mathrm{s.s.}}].$$

In general, choose an odd prime $\ell \neq p$, and compute

$$\begin{aligned} M(\mathcal{P}^{\mathrm{ord}}) &= \mathfrak{M}(\mathcal{P}^{\mathrm{ord}}, [\Gamma(\ell)])/\mathrm{GL}(2, \mathbf{F}_\ell) \\ &= (\mathfrak{M}(\mathcal{P}, [\Gamma(\ell)])[1/\Phi^{\mathrm{s.s.}}])/\mathrm{GL}(2, \mathbf{F}_\ell) \\ &= (\mathfrak{M}(\mathcal{P}, [\Gamma(\ell)])/\mathrm{GL}(2, \mathbf{F}_\ell))[1/\Phi^{\mathrm{s.s.}}] \\ &= M(\mathcal{P})[1/\Phi^{\mathrm{s.s.}}]. \end{aligned} \qquad \text{Q.E.D.}$$

(12.6) *First analysis of the Igusa curve*

THEOREM 12.6.1 (Igusa). (1) *The moduli problem* $[\mathrm{Ig}(p^n)]$ *on* $(\mathrm{Ell}/\mathbf{F}_p)$ *is relatively representable, finite and flat over* $(\mathrm{Ell}/\mathbf{F}_p)$ *of rank* $\phi(p^n)$.
(2) *It is regular one-dimensional (so, being of finite type over* $\mathbf{F}_p$, *it is smooth of relative dimension one over* $\mathbf{F}_p$).
(3) *The group* $(\mathbf{Z}/p^n\mathbf{Z})^\times$ *operates on* $[\mathrm{Ig}(p^n)]$ *by*

$$\left(a \in (\mathbf{Z}/p^n\mathbf{Z})^\times,\ P \text{ gen of } \mathrm{Ker}\, V^n\right) \mapsto aP.$$

For every integer $0 \leq a \leq n$, *let* $1 + (p^a)$ *denote the subgroup of*

$(\mathbf{Z}/p^n\mathbf{Z})^\times$ *sitting in the exact sequence*

$$0 \to 1+(p^a) \to (\mathbf{Z}/p^n\mathbf{Z})^\times \to (\mathbf{Z}/p^a\mathbf{Z})^\times \to 0 .$$

The natural map of moduli problems on $(\mathrm{Ell}/\mathbf{F}_p)$

$$[\mathrm{Ig}(p^n)] \to [\mathrm{Ig}(p^a)]$$
$$\Big(P \text{ gen } \textit{of } \mathrm{Ker}\, V^n\Big) \mapsto V^{n-a}(P)$$

is $1+(p^a)$ *equivariant.*

(4) *The induced map*

$$[\mathrm{Ig}(p^n)]^{\mathrm{ord}} \to [\mathrm{Ig}(p^a)]^{\mathrm{ord}}$$

is a finite etale $1+(p^a)$*-torsor.*

(5) *The induced map of quotients is an isomorphism*

$$[\mathrm{Ig}(p^n)]/1+(p^a) \xrightarrow{\sim} [\mathrm{Ig}(p^a)]$$

of moduli problems on $(\mathrm{Ell}/\mathbf{F}_p)$.

(6) *For any subgroup* $H \subset (\mathbf{Z}/p^n\mathbf{Z})^\times$, *the quotient* $[\mathrm{Ig}(p^n)]/H$ *is regular one-dimensional, finite and flat over* $(\mathrm{Ell}/\mathbf{F}_p)$.

Proof. That $[\mathrm{Ig}(p^n)]$ is relatively representable, finite and flat of degree $\phi(p^n)$ is clear from (12.2.3) and (6.1.1): indeed for any $E/S/\mathbf{F}_p$, we have

$$[\mathrm{Ig}(p^n)]_{E/S} = G^\times, \text{ the scheme of generators of}$$
$$G = \mathrm{Ker}(V^n : E^{(p^n)} \to E) .$$

If $E/S/\mathbf{F}_p$ is ordinary, then $\mathrm{Ker}(V^n)$ is etale and cyclic of order p^n, so $[\mathrm{Ig}(p^n)]^{\mathrm{ord}}$ is a finite etale $(\mathbf{Z}/p^n\mathbf{Z})^\times$ torsor over $[\mathrm{ord}] = [\mathrm{Ig}(p^0)]^{\mathrm{ord}}$. The maps

$$[\mathrm{Ig}(p_n)] \to [\mathrm{Ig}(p^a)]$$
$$P \mapsto V^{n-a}(P)$$

are well defined (by the Backing-up theorem (6.7.11)), obviously $1+(p^a)$

equivariant, and are obviously finite etale $1+(p^a)$ torsors over ordinary $E/S/\mathbf{F}_p$'s. So as usual we are left with understanding what happens at the supersingular points.

Thus let k be an algebraically closed field of characteristic p, E/k a supersingular elliptic curve, $E/k[[T]]$ its universal formal deformation (to artin local k-algebras), X a parameter for the formal group $\hat{E}$. The chosen X gives a parameter on each $\hat{E}^{(p^n)}$ by extension of scalars. We must show that the finite flat $k[[T]]$-scheme

$$[\mathrm{Ig}(p^n)]_{E/k[[T]]}$$

is regular and one-dimensional. We know that it is *local*, because its k-points "are" the generators of $\mathrm{Ker}(V^n : E^{(p^n)} \to E)$ at $T = 0$ with values in k, and the unique k-point in this kernel is the origin. Therefore this local ring, being finite flat over $k[[T]]$, is certainly one-dimensional. To show it is regular, it suffices to exhibit a parameter. We claim that the "X-coordinate" of the given generator of $\mathrm{Ker}(V^n)$ is a parameter. This amounts to showing that

> if R is an artin local k-algebra,* and E/R is an elliptic curve such that 0 generates $\mathrm{Ker}(V^n : E^{(p^n)} \to E)$, then E/R is constant.

But this is clear, for 0 as point of "exact order p^n" generates $\mathrm{Ker}(F^n)$, so we find $\mathrm{Ker}(V^n) = \mathrm{Ker}(F^n)$, whence

$$\begin{array}{ccc} E^{(p^n)}/\mathrm{Ker}(V^n) & = & E^{(p^n)}/\mathrm{Ker}(F^n) \\ \Big\downarrow V^n & & \Big\downarrow F^n \\ E & \xrightarrow{\sim} & E^{(p^{2n})} . \end{array}$$

Iterating this isomorphism as in 12.4.3, we get

$$E \xrightarrow{\sim} E^{(p^{2n})} \xrightarrow{\sim} E^{(p^{4n})} \xrightarrow{\sim} \cdots E^{(p^{2mn})} \xrightarrow{\sim} \cdots ,$$

and we find that E is constant, as required.

*With residue field k.

It remains to show that the map

$$[\mathrm{Ig}(p^n)]/1 + (p^a) \longrightarrow [\mathrm{Ig}(p^a)]$$

is an isomorphism. We know it is so over the ordinary part. To see that it is so everywhere, it suffices to prove that the quotient

$$[\mathrm{Ig}(p^n)]/1 + (p^a)$$

is regular one-dimensional. For the map is then a finite map (finite because source and target are finite over $(\mathrm{Ell}/\mathbf{F}_p)$) between regular schemes of the same dimension, so automatically finite and flat.

So we are reduced to showing that for any $H \subset (\mathbf{Z}/p^n\mathbf{Z})^\times$, the quotient problem $[\mathrm{Ig}(p^n)]/H$ is regular one-dimensional. But being the quotient of a regular one-dimensional problem by a finite group, it is *normal* and one-dimensional, hence regular. Q.E.D.

COROLLARY 12.6.2 (Igusa). *Let* k *be an algebraically closed field of characteristic* p, $\mathcal{P}$ *a representable moduli problem on* (Ell/k) *which is etale and surjective over* (Ell/k). *Then*

(1) *The covering* $\mathcal{M}(\mathcal{P}, [\mathrm{Ig}(p^n)]) \to \mathcal{M}(\mathcal{P})$ *is a finite flat map of smooth curves over* k. *It is finite etale outside the supersingular points, with galois group* $(\mathbf{Z}/p^n\mathbf{Z})^\times$. *It is fully ramified over each supersingular point of* $\mathcal{M}(\mathcal{P})$.

(2) *If* $\mathcal{M}(\mathcal{P})$ *is connected, then* $\mathcal{M}(\mathcal{P}, [\mathrm{Ig}(p^n)])$ *is connected.*

Proof. The fully-ramifiedness over supersingular points is again the fact that for E/k supersingular, and $n \geq 0$, the origin is the *unique* k-rational generator of $\mathrm{Ker}(V^n : E^{(p^n)} \to E)$. That it is a finite etale $(\mathbf{Z}/p^n\mathbf{Z})^\times$-torsor over $\mathcal{M}(\mathcal{P}^{\mathrm{ord}})$ is the special case $a = 0$ of the fact that

$$[\mathrm{Ig}(p^n)]^{\mathrm{ord}} \to [\mathrm{Ig}(p^a)]^{\mathrm{ord}}$$

is a finite etale $1+(p^a)$-torsor. The connectedness assertion (2) is an immediate consequence of having a finite flat map of noetherian schemes

$X \to Y$ with Y connected, which is fully ramified over some point of Y. For if $U \subset X$ is an open and closed subscheme, the composite $U \hookrightarrow X \to Y$ is still both finite and flat, so locally free over all of Y of some degree ≥ 1. So if $V = X - U$ is non-empty, it too is finite flat over Y, so also locally free over Y of some degree ≥ 1. Then X is a disjoint union of two surjective Y-schemes, contradicting the fully-ramifiedness. Q.E.D.

COROLLARY 12.6.3. *If* $p^n \geq 3$, *then* $[\mathrm{Ig}(p^n)]^{\mathrm{ord}}$ *is representable, by a smooth geometrically connected curve over* $\mathbf{F}_p$.

Proof. The problem $[\mathrm{Ig}(p^n)]^{\mathrm{ord}}$ is relatively representable and affine over $(\mathrm{Ell}/\mathbf{F}_p)$, so it is representable if and only if it is rigid. Thus let k be a field of characteristic p, E/k an ordinary elliptic curve, and $P \in E^{(p^n)}(k)$ a generator of $\mathrm{Ker}(V^n)$. Then P defines an isomorphism $\mathbf{Z}/p^n\mathbf{Z} \xrightarrow{\sim} \mathrm{Ker}\, V^n \hookrightarrow E^{(p^n)}$. We must see that any automorphism ε of E/k which operates *trivially* on this $\mathbf{Z}/p^n\mathbf{Z}$ is the identity.

By functoriality, any $\lambda \in \mathrm{End}(E/k)$ operates on $\mathrm{Ker}(V^n) \xleftarrow{\sim} \mathbf{Z}/p^n\mathbf{Z}$, by multiplication by some $a(\lambda) \in \mathbf{Z}/p^n\mathbf{Z}$, and $\lambda \mapsto a(\lambda)$ is a ring homomorphism

$$\mathrm{End}(E/k) \to \mathbf{Z}/p^n\mathbf{Z}.$$

We must see that the *unique* $\varepsilon \in \mathrm{Aut}(E/k)$ with $a(\varepsilon) = 1$ is $\varepsilon = 1$, if $p^n \geq 3$. We do this in cases.

Case 1. $\mathrm{Aut}(E/k) = \pm 1$. Here $a(-1) = -1 \not\equiv 1\,(p^n)$, because $p^n \geq 3$.

Case 2. $\mathrm{Aut}(E/k) \neq \pm 1$. Any automorphism $\varepsilon \neq \pm 1$ satisfies either $\varepsilon^2 + 1 = 0$ or $\varepsilon^2 + \varepsilon + 1 = 0$ or $\varepsilon^2 - \varepsilon + 1 = 0$ in the ring $\mathrm{End}(E/k)$. If such an ε has $a(\varepsilon) = 1$, then we have respectively $2 \equiv 0(p^n)$, $3 \equiv 0(p^n)$, $2 \equiv 0(p^n)$. The first and last are incorrect if $p^n \geq 3$, the middle one incorrect if $p^n \geq 4$. It remains to treat the case $p = 3$, $\varepsilon^2 + \varepsilon + 1 = 0$. But this curve has CM by $\mathbf{Q}(\zeta_3)$, so has $j = 0 = 1728$ in $\overline{\mathbf{F}}_3$ and is the unique supersingular curve in characteristic three. So this case does not arise. Q.E.D.

(12.7) *Analysis of the cusps*

THEOREM 12.7.1. *Let* R *be an* $\mathbf{F}_p$*-algebra which is noetherian, regular and excellent,* $\mathcal{P}$ *a moduli problem on* (Ell/R) *which is representable and finite over* (Ell/R), *and normal near infinity (cf. 8.6.2). Then*

(1) *the morphism of* R[[q]]*-schemes (cf. (10.13.4))*

$$Z(\mathcal{P}, [\mathrm{Ig}(p^n)]) \to Z(\mathcal{P})$$

is completely decomposed: we have a canonical isomorphism of R[[q]]*-schemes*

$$Z(\mathcal{P}, [\mathrm{Ig}(p^n)]) \xrightarrow{\sim} \coprod_{(\mathbf{Z}/p^n\mathbf{Z})^\times} Z(\mathcal{P}),$$

with ± 1 *operating compatibly with its action on* $(\mathbf{Z}/p^n\mathbf{Z})^\times$.

(2) *if the group* ± 1 *acts freely on* $Z(\mathcal{P})$ *(cf. 10.13.7-8-9), then the morphism of completed schemes of cusps (8.6.3.3)*

$$\widehat{\mathrm{Cusps}}(\mathcal{P}, [\mathrm{Ig}(p^n)]) \to \widehat{\mathrm{Cusps}}(\mathcal{P})$$

is a finite etale $(\mathbf{Z}/p^n\mathbf{Z})^\times$*-torsor.*

(3) *if* $p^n \geq 3$, *the group* ± 1 *operates freely on* $Z(\mathcal{P}, [\mathrm{Ig}(p^n)])$; *consequently (cf. (10.13.4)) the line bundle* $\underline{\omega}$ *extends to* $\overline{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p^n)])$.

Proof. We first deduce assertions (2) and (3) from (1). Assertion (3) is just the fact that for $p^n \geq 3$, the group ± 1 operates freely on the group $(\mathbf{Z}/p^n\mathbf{Z})^\times$. Assertion (2) follows from (1) because the morphism

$$\widehat{\mathrm{Cusps}}(\mathcal{P}, [\mathrm{Ig}(p^n)]) \to \widehat{\mathrm{Cusps}}(\mathcal{P})$$

is (cf. (10.13.4) and (8.11.10)) obtained from the morphism

$$Z(\mathcal{P}, [\mathrm{Ig}(p^n)]) \to Z(\mathcal{P})$$

by dividing both source and target by the group ± 1. Therefore if ± 1

acts freely on $Z(\mathcal{P})$, the second of these maps is obtained from the first by the finite etale surjective base-change

$$Z(\mathcal{P}) \to \widehat{\mathrm{Cusps}}(\mathcal{P}) = Z(\mathcal{P})/\pm 1$$

To prove (1), it suffices, by normalization, to show that we have an isomorphism of R((q))-schemes

$$(\mathcal{P}, [\mathrm{Ig}(p^n)])_{\mathrm{Tate}(q)/R((q))} \simeq \coprod_{(\mathbf{Z}/p^n\mathbf{Z})^\times} \mathcal{P}_{\mathrm{Tate}(q)/R((q))},$$

with ± 1 operating compatibly with its action on $(\mathbf{Z}/p^n\mathbf{Z})^\times$. As for any simultaneous moduli problem, we have

$$(\mathcal{P}, [\mathrm{Ig}(p^n)])_{\mathrm{Tate}(q)/R((q))}$$

$$\simeq (\mathcal{P}_{\mathrm{Tate}(q)/R((q))}) \times_{R((q))} [\mathrm{Ig}(p^n)]_{\mathrm{Tate}(q)/R((q))}.$$

We are reduced to showing that

$$[\mathrm{Ig}(p^n)]_{\mathrm{Tate}(q)/R((q))} \xrightarrow{\sim} \coprod_{(\mathbf{Z}/p^n\mathbf{Z})^\times} \mathrm{Spec}(R((q))).$$

On Tate(q)/R((q)), we have a canonical short exact sequence (cf. 8.8)

$$0 \to \mu_{p^n} \to \mathrm{Tate}(q)[p^n] \to \mathbf{Z}/p^n\mathbf{Z} \to 0$$

which defines a canonical isomorphism of R((q))-group-schemes

$$\mathrm{Ker}(V^n : \mathrm{Tate}(q)^{(p^n)} \to \mathrm{Tate}(q)) \simeq \mathbf{Z}/p^n\mathbf{Z}.$$

Therefore

$$[\mathrm{Ig}(p^n)]_{\mathrm{Tate}(q)/R((q))} \simeq (\text{the scheme of generators of } \mathbf{Z}/p^n\mathbf{Z}) \otimes_{\mathbf{Z}} R((q)).$$

Q.E.D.

COROLLARY 12.7.2. *Suppose* k *is a perfect field of characteristic* p, *and* $\mathcal{P}$ *is a representable moduli problem which is finite etale over* (Ell/k), *such that* ± 1 *acts freely on* $Z(\mathcal{P})$. *Then* $\overline{\mathcal{M}}(\mathcal{P})$ *is a complete smooth curve over* k, $\overline{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p^n)])$ *is a complete smooth curve over* k, *and the map*

$$\overline{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p^n)]) \to \overline{\mathcal{M}}(\mathcal{P})$$

is finite etale galois with group $(\mathbf{Z}/p^n\mathbf{Z})^\times$ *outside the supersingular points of* $\overline{\mathcal{M}}(\mathcal{P})$. *The map is fully ramified over each supersingular point of* $\overline{\mathcal{M}}(\mathcal{P})$, *and it is completely decomposed over the scheme of cusps of* $\overline{\mathcal{M}}(\mathcal{P})$. *If* $\overline{\mathcal{M}}(\mathcal{P})$ *is geometrically connected, so is* $\overline{\mathcal{M}}(\mathcal{P}, \mathrm{Ig}(p^n))$.

Proof. $\overline{\mathcal{M}}(\mathcal{P})$ is normal one-dimensional, so regular, and being finite over Spec(k[j]) it is of finite type over k, so smooth over k. The other assertions result from (12.6.2) and (12.7.1). Q.E.D.

(12.8) *The equation defining* Ig(p), *and a theorem of Serre*

(12.8.1) For an elliptic curve $E/S/\mathbf{F}_p$, recall that its Hasse invariant A is the global section over S of the line bundle

$$\begin{aligned}\underline{\omega}^{\otimes(p-1)} &\simeq Hom_{\mathcal{O}_S}(Lie(E/S)^{\otimes p}, Lie(E/S)) \\ &= Hom_{\mathcal{O}_S}(Lie(E^{(p)}/S), Lie(E/S))\end{aligned}$$

provided by $\mathrm{tg}(V : E^{(p)} \to E)$.

We construct a moduli problem $[A^{1/p-1}]$ on $(\mathrm{Ell}/\mathbf{F}_p)$ by defining

(12.8.1.1) $[A^{1/p-1}](E/S)$ = the set of elements $\omega \in H^0(S, \underline{\omega}_{E/S})$ such that $\omega^{p-1} = A$ in $H^0(S, \underline{\omega}^{\otimes(p-1)})$.

THEOREM 12.8.2. *There is a natural isomorphism of moduli problems on* $(\mathrm{Ell}/\mathbf{F}_p)$

$$[\mathrm{Ig}(p)] \xrightarrow{\sim} [A^{1/p-1}].$$

Construction-proof. We begin by defining the morphism in question. Suppose we are given $E/S/\mathbf{F}_p$, and a point $P \in E^{(p)}(S)$ which generates $\mathrm{Ker}(V : E^{(p)} \to E)$. We must associate to this data a global section $\omega(P) \in H^0(S, \underline{\omega}_{E/S}) = H^0(S, \Omega^1_{E/S})$ which satisfies the equation

$$\omega(P)^{\otimes(p-1)} = A.$$

We perform this construction as follows. By Cartier duality, a point $P \in \mathrm{Ker}(V : E^{(p)}(S) \to E(S))$, when viewed as a homomorphism of S-groups $\mathbf{Z}/p\mathbf{Z} \to \mathrm{Ker}(V)$, gives rise to a homomorphism of S-groups

$$\phi_P : \mathrm{Ker}(F : E \to E^{(p)}) \to \mu_p \hookrightarrow \mathbf{G}_m.$$

The standard invariant one-form dX/X on $\mathbf{G}_m$ gives rise by inverse image to an invariant one-form on $\mathrm{Ker}(F)$,

$$\phi_P^*(dX/X) \quad \text{on} \quad \mathrm{Ker}(F : E \to E^{(p)}).$$

Because S is an $\mathbf{F}_p$-scheme, the restriction map

$$\begin{pmatrix}\text{invariant one-forms} \\ \text{on } E/S\end{pmatrix} \to \begin{pmatrix}\text{invariant one-forms} \\ \text{on } \mathrm{Ker}(F)\end{pmatrix}$$

is an isomorphism. We define $\omega(P)$ to be the unique invariant one-form on E/S such that $\omega(P)|\mathrm{Ker}(F) = \phi_P^*(dX/X)$.

We must show that if P generates $\mathrm{Ker}(V)$, then

$$\omega(P)^{\otimes(p-1)} = A.$$

By "reduction to the universal case", it suffices to verify this first when S is a smooth geometrically connected curve over $\mathbf{F}_p$ containing a finite number of supersingular points, then over S-{supersingular points}.

Passing to a finite etale covering, it suffices to check in the case $S = \mathcal{M}([\mathrm{Ig}(p^n)]^{\mathrm{ord}})$, and, passing to the limit, it suffices to check over $S = \varprojlim \mathcal{M}([\mathrm{Ig}(p^n)]^{\mathrm{ord}})$. In this case, the morphism

$$\phi_P : \mathrm{Ker}(F) \to \mu_p \hookrightarrow G_m$$

is the restriction to $\mathrm{Ker}(F)$ of an isomorphism of formal groups

$$\phi : \hat{E} \xrightarrow{\sim} \hat{G}_m ,$$

and we have

$$\omega(P)|\hat{E} = \phi^*(dX/X) .$$

Then $\omega(P)$ is a nowhere-vanishing invariant one-form on $\hat{E}$, so nowhere vanishing on E, and the dual derivation D_P to $\omega(P)$ induces Xd/dX on G_m, so satisfies

$$(D_P)^p = D_P .$$

Therefore

$$A(E, \omega(P)) = 1 ,$$

i.e.,

$$A = \omega(P)^{\otimes(p-1)}$$

as required.

To see that this map

$$[\mathrm{Ig}(p)] \to [A^{1/p-1}]$$

$$P \mapsto \omega(P)$$

is an isomorphism of moduli problems on (Ell/F_p), we argue as follows. By Igusa's theorem, A has *simple* zeros. Because $p-1$ is prime to p, it follows that $[A^{1/p-1}]^{\mathrm{ord}}$ is a finite etale $F_p^\times$torsor over $[\mathrm{ord}]$, and that $[A^{1/p-1}]$ is a regular one-dimensional moduli problem, fully ramified

over each supersingular point, finite and flat of degree $p-1$ over (Ell/F_p). The morphism

$$[\mathrm{Ig}(p)] \to [A^{1/p-1}]$$

is finite, because source and target are finite over (Ell/F_p), so finite and flat, because both source and target are regular one-dimensional. Therefore it is finite and flat, necessarily of degree one, because source and target are each finite flat over (Ell/F_p) of degree $p-1$ and connected in the sense of (12.6.2 (2)). Q.E.D.

COROLLARY 12.8.3. *Let* R *be an* F_p*-algebra which is noetherian, regular and excellent,* $\mathcal{P}$ *a moduli problem on* (Ell/R) *which is representable and finite over* (Ell/R)*, and normal near infinity. Then* A *extends to a global section over* $\bar{\mathcal{M}}(\mathcal{P})$ *of* $\underline{\omega}^{\otimes(p-1)}$*. If* ± 1 *operates freely on* $Z(\mathcal{P})$ *(cf. 12.7.1), then* $\bar{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p)])$ *is the covering of* $\bar{\mathcal{M}}(\mathcal{P})$ *defined by extracting the* p-1'st *root of* A.

Proof. That A extends to a section of $\underline{\omega}^{\otimes(p-1)}$ over all of $\bar{\mathcal{M}}(\mathcal{P})$ is obvious from the way that $\underline{\omega}$ is extended from $\mathcal{M}(\mathcal{P})$ to $\bar{\mathcal{M}}(\mathcal{P})$ (cf. 10.13.2), and from the formula

$$A(\mathrm{Tate}(q), \omega_{\mathrm{can}}) = 1 .$$

The covering of $\bar{\mathcal{M}}(\mathcal{P})$ defined by extracting the p-1'st root of A is finite etale with group $F_p^\times$ over a neighborhood of the cusps. Therefore it is normal near infinity, finite over $\bar{\mathcal{M}}(\mathcal{P})$, and by the theorem it coincides with $\mathcal{M}(\mathcal{P}, [\mathrm{Ig}(p)])$ over $\mathcal{M}(\mathcal{P})$. Therefore it is the normalization of $\bar{\mathcal{M}}(\mathcal{P})$ in $\mathcal{M}(\mathcal{P}, [\mathrm{Ig}(p)])$, just as is $\bar{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p)])$. Q.E.D.

COROLLARY 12.8.4. *Hypotheses and notations as in the above corollary, suppose that* ± 1 *operates freely on* $Z(\mathcal{P})$*. Then the finite flat covering* $\bar{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p)])$ *of* $\bar{\mathcal{M}}(\mathcal{P})$ *is the relatively affine* $\bar{\mathcal{M}}(\mathcal{P})$*-scheme defined by*

$$\mathrm{Spec}_{\bar{\mathcal{M}}(\mathcal{P})}\left(\mathrm{Symm}_{\bar{\mathcal{M}}(\mathcal{P})}(\underline{\omega}^{-1})/\mathcal{J}\right)$$

where $\mathcal{J}$ *is the sheaf of ideals*

$$\mathcal{J} = (A-1)\Big(\bigoplus_{n\geq p-1} \underline{\omega}^{\otimes(-n)}\Big) .$$

Proof. The relatively affine scheme in question tautologically represents the functor on $\overline{\mathcal{M}}(\mathcal{P})$ schemes

$$\begin{array}{c} X \\ \Big\downarrow \pi \\ \overline{\mathcal{M}}(\mathcal{P}) \end{array} \longmapsto \begin{array}{l} \text{sections } a \in H^0(X, \pi^*(\underline{\omega})) \\ \text{such that } a^{p-1} = A . \end{array}$$

Q.E.D.

COROLLARY 12.8.5. *For* $\mathcal{P}$ *as in the preceding corollary, denote by*

$$pr : \overline{\mathcal{M}}(\mathcal{P}, [Ig(p)]) \to \overline{\mathcal{M}}(\mathcal{P})$$

the projection. Then we have a canonical isomorphism of locally-free sheaves on $\overline{\mathcal{M}}(\mathcal{P})$

$$pr_*(\mathcal{O}_{\overline{\mathcal{M}}(\mathcal{P},[Ig(p)])}) \xrightarrow{\sim} \bigoplus_{0\leq k\leq p-2} (\underline{\omega}^{-1})^{\otimes k} .$$

Proof. By the preceding corollary,

$$pr_*(\mathcal{O}) = \Big(\bigoplus_{k\geq 0} (\underline{\omega}^{-1})^{\otimes k}\Big) \Big/ (A-1)\Big(\bigoplus_{k\geq p-1} (\underline{\omega}^{-1})^{\otimes k}\Big)$$

$$\Big\wr \uparrow$$

$$\bigoplus_{0\leq k\leq p-2} (\underline{\omega}^{-1})^{\otimes k} .$$

Q.E.D.

COROLLARY 12.8.6. *Let* k *be field of characteristic* p, $\mathcal{P}$ *a representable moduli problem on* (Ell/k) *which is finite etale over* (Ell/k), *such that* ± 1 *acts freely on* $Z(\mathcal{P})$. *Then for the projection*

$$pr : \overline{\mathcal{M}}(\mathcal{P}, [Ig(p)]) \to \overline{\mathcal{M}}(\mathcal{P})$$

we have canonical isomorphisms of line-bundles on $\overline{\mathcal{M}}(\mathcal{P},[Ig(p)])$

$$(1) \qquad \mathcal{O} \xrightarrow{\sim} I(s.s.) \otimes pr^*(\underline{\omega}), \quad 1 \mapsto A^{1/p-1} ,$$

where I(s.s.) *denotes the ideal sheaf of the supersingular points on* $\overline{\mathcal{M}}(\mathcal{P},[Ig(p)])$, *and a canonical isomorphism*

$$(2) \qquad pr^*(\Omega^1_{\overline{\mathcal{M}}(\mathcal{P})/k}) \xrightarrow{\sim} \Omega^1_{\overline{\mathcal{M}}(\mathcal{P},[Ig(p)])/k} \otimes (I(s.s.))^{\otimes(p-2)} .$$

Proof. (1) holds because by Igusa's theorem the tautological section $A^{1/p-1}$ of $pr^*(\underline{\omega})$ on $\overline{\mathcal{M}}(\mathcal{P}, [Ig(p)])$ has simple zeroes precisely at the supersingular points of $\overline{\mathcal{M}}(\mathcal{P}, [Ig(p)])$, and elsewhere it is invertible. (2) holds because pr is etale except over the supersingular points of $\overline{\mathcal{M}}(\mathcal{P})$, where it is defined by extracting the p–1'st root of a local parameter (cf. 12.4.4). Q.E.D.

THEOREM 12.8.7. *Let* k *be a field of characteristic* p, $\mathcal{P}$ *a representable moduli problem on* (Ell/k) *which is finite etale over* (Ell/k). *Suppose that* ± 1 *acts freely on* $Z(\mathcal{P})$. *Assume that the Kodaira-Spencer isomorphism on* $\mathcal{M}(\mathcal{P})$ *extends to an isomorphism*

$$\underline{\omega}^{\otimes 2} \simeq \Omega^1_{\overline{\mathcal{M}}(\mathcal{P})/k}(\log \text{cusps}) \quad \text{on} \quad \overline{\mathcal{M}}(\mathcal{P}) ,$$

a condition which is automatically fulfilled (cf. 10.13.11) whenever $\mathcal{P}$ *is the extension of scalars of a finite etale representable problem over an excellent noetherian regular domain of generic characteristic zero. Then we have a canonical isomorphism of line bundles on* $\overline{\mathcal{M}}(\mathcal{P}, [Ig(p^n)])$

$$pr^*(\underline{\omega}^{\otimes p}) \xrightarrow{\sim} \Omega^1_{\overline{\mathcal{M}}(\mathcal{P},[Ig(p)])/k}(\log \text{cusps}) ,$$

and a canonical isomorphism of locally free sheaves on $\overline{\mathcal{M}}(\mathcal{P})$

$$pr_*(\Omega^1_{\overline{\mathcal{M}}(\mathcal{P},[Ig(p)])/k}) \xrightarrow{\sim} \bigoplus_{2\leq k\leq p} (\underline{\omega}^{\otimes k} \otimes I(\text{cusps})) .$$

Proof. Because $\mathrm{pr}: \overline{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p)]) \to \overline{\mathcal{M}}(\mathcal{P})$ is finite etale near the cusps, we have

$$\begin{aligned}
\mathrm{pr}^*(\underline{\omega}^{\otimes p}) &\simeq \mathrm{pr}^*(\underline{\omega}^{\otimes 2}) \otimes (\mathrm{pr}^*(\underline{\omega}))^{\otimes (p-2)} \\
&\simeq \mathrm{pr}^*(\Omega^1_{\overline{\mathcal{M}}(\mathcal{P})/k}(\log \text{ cusps})) \otimes (I^{-1}(\text{s.s.}))^{\otimes (p-2)} \\
&\simeq (\mathrm{pr}^*(\Omega^1_{\overline{\mathcal{M}}(\mathcal{P})/k}) \otimes I^{-1}(\text{cusps})) \otimes (I^{-1}(\text{s.s.}))^{\otimes (p-2)} \\
&\simeq \Omega^1_{\overline{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p)])/k} \otimes (I(\text{s.s.}))^{\otimes (p-2)} \otimes I^{-1}(\text{cusps}) \otimes (I^{-1}(\text{s.s.}))^{\otimes (p-2)} \\
&\simeq (\Omega^1_{\overline{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p)])/k}) \otimes I^{-1}(\text{cusps}) .
\end{aligned}$$

This gives the first isomorphism. The second is obtained by rewriting the first as

$$\Omega^1_{\overline{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p)])/k} \xrightarrow{\sim} \mathrm{pr}^*(\underline{\omega}^{\otimes p} \otimes I(\text{cusps})) ,$$

then applying pr_* :

$$\begin{aligned}
\mathrm{pr}_*(\Omega^1_{\overline{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p)])/k}) &\simeq \underline{\omega}^{\otimes p} \otimes I(\text{cusps}) \otimes \mathrm{pr}_*(\mathcal{O}) \\
&\simeq \underline{\omega}^{\otimes p} \otimes I(\text{cusps}) \otimes \left(\bigoplus_{0 \le k \le p-2} (\underline{\omega}^{-1})^{\otimes k} \right) \\
&\simeq \bigoplus_{2 \le k \le p} \underline{\omega}^{\otimes k} \otimes I(\text{cusps}) . \qquad \text{Q.E.D.}
\end{aligned}$$

THEOREM 12.8.8 (Serre) *Let* $N \ge 1$ *be an integer prime to* p, $\Gamma \subset GL(2, \mathbf{Z}/N\mathbf{Z})$ *a subgroup such that* $([\Gamma(N)]/\Gamma) \otimes_{\mathbf{Z}} \mathbf{Z}[1/N]$ *is representable,* A *the ring* $(\mathbf{Z}[\zeta_N])^{\det(\Gamma)}$, k *a field of characteristic* p, $A \to k$ *a ring homomorphism, and* $\mathcal{P}$ *the moduli problem on* (Ell/k) *defined by*

$$\mathcal{P} = ([\Gamma(N)]/\Gamma)^{A\text{-can}} \otimes_A k .$$

Suppose that ± 1 *acts freely on* $Z(\mathcal{P})$. *Then* $\mathcal{P}$ *satisfies all the hypotheses of the preceding theorem, and we have an isomorphism of* k*-vector spaces*

$$\bigoplus_{2 \le k \le p} \begin{pmatrix} \textit{holomorphic cusp forms of} \\ \textit{weight } k \textit{ on } \overline{\mathcal{M}}(\mathcal{P}) \end{pmatrix} \xrightarrow{\sim} \textit{global holomorphic one-forms on } \overline{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p)])$$

given explicitly as follows:

*to a weight-*k *cusp form* ϕ_k *on* $\overline{\mathcal{M}}(\mathcal{P})$, $2 \le k \le p$,

$$\phi_k \in H^0(\overline{\mathcal{M}}(\mathcal{P}), \underline{\omega}^{\otimes (k-2)} \otimes \Omega^1_{\overline{\mathcal{M}}(\mathcal{P})/k})$$

is associated the holomorphic one-form on $\overline{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p)])$

$$\omega(\phi_k) = \frac{\mathrm{pr}^*(\phi_k)}{(A^{1/p-1})^{k-2}} .$$

If k *contains the primitive* N*'th roots of unity, then at any cusp of* $\overline{\mathcal{M}}(\mathcal{P})$ *a uniformizing parameter is* $q^{1/f}$ *for some divisor* f *of* N; *at the cusp of* $\overline{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p)])$ *lying over this one where* $A^{1/p-1}/\omega_{\mathrm{can}} = 1$, *the same* $q^{1/f}$ *is a uniformizing parameter, and the* $q^{1/f}$*-expansions of* ϕ_k *and of* $\omega(\phi_k)$ *are related by*

$$\omega(\phi_k) \sim [\phi_k(\mathrm{Tate}(q), \omega_{\mathrm{can}}, \alpha \in \mathcal{P}(\mathrm{Tate}(q) \otimes_{k((q))} k((q^{1/f})))] d \log(q)$$

Proof. On $\overline{\mathcal{M}}(\mathcal{P})$, we have already obtained isomorphisms of locally free sheaves

$$\begin{array}{ccc}
\displaystyle\bigoplus_{0 \le k \le p-2} \omega^{\otimes k} \otimes \Omega^1_{\overline{\mathcal{M}}(\mathcal{P})} & \xrightarrow[(K-S)]{\sim} & \displaystyle\bigoplus_{2 \le k \le p} \underline{\omega}^{\otimes k} \otimes I(\text{cusps}) \\
& & \uparrow \wr \\
& & \mathrm{pr}_*(\Omega^1_{\overline{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p)])/k}) .
\end{array}$$

Taking global sections gives the required isomorphism. Q.E.D.

(12.9) *Numerology of Igusa curves*

THEOREM 12.9.1. *Let* k *be a field of characteristic* p, $\mathcal{P}$ *a representable moduli problem on* (Ell/k) *which is finite etale over* (Ell/k), *such that* ± 1 *acts freely on* $Z(\mathcal{P})$, *and for which the Kodaira-Spencer isomorphism on* $\mathcal{M}(\mathcal{P})$ *extends to an isomorphism*

$$\underline{\omega}^{\otimes 2} \simeq \Omega^1_{\overline{\mathcal{M}}(\mathcal{P})/k}(\log \text{cusps}) \quad \text{on} \quad \overline{\mathcal{M}}(\mathcal{P}) .$$

[*For example,* $\mathcal{P} = [\Gamma_1(N)] \otimes_{\mathbf{Z}} k$ *for any* $N \geq 5$ *prime to* p, *or* $\mathcal{P} = [\Gamma(N)]^{can} \otimes_{\mathbf{Z}[\zeta_N]} k$ *for any* $N \geq 3$ *prime to* p, *if* k *contains a primitive* N'th *root of unity, or* ⋯ *cf. (10.13.9).*] *Then for any* $n \geq 1$, *denoting by*

$$pr : \overline{\mathcal{M}}(\mathcal{P}, [Ig(p^n)]) \to \overline{\mathcal{M}}(\mathcal{P})$$

the projection, we have an isomorphism of line bundles on $\overline{\mathcal{M}}(\mathcal{P}, [Ig(p^n)])$

$$pr^*(\underline{\omega}^{\otimes p^n}) \simeq \Omega^1_{\overline{\mathcal{M}}(\mathcal{P}, [Ig(p^n)])/k}(\log \text{cusps}) .$$

Proof. We have already proven this for $n = 1$. We will proceed by induction on n. For each integer $n \geq 0$, let us denote by

$$\Omega(n), \quad I(n, s.s.), \quad I(n, \text{cusps})$$

the invertible sheaves on $\overline{\mathcal{M}}(\mathcal{P}, [Ig(p^n)])$

$$\Omega^1_{\overline{\mathcal{M}}(\mathcal{P}, [Ig(p^n)])}, \quad I(s.s.), \quad I(\text{cusps})$$

respectively, and let us denote by

$$pr(n) : \overline{\mathcal{M}}(\mathcal{P}, [Ig(p^{n+1})]) \to \overline{\mathcal{M}}(\mathcal{P}, [Ig(p^n)])$$

the projection induced by the morphism of moduli problems

$$[Ig(p^{n+1})] \to [Ig(p^n)]$$

$$P \mapsto V(P) .$$

LEMMA 12.9.2. *For* $n \geq 1$, *we have canonically*

$$pr(n)^*(I(n, s.s.)) = I(n+1, s.s.)^{\otimes p}$$

$$pr(n)^*(I(n, \text{cusps})) = I(n+1, \text{cusps}) .$$

Proof. For $n \geq 1$, pr(n) is fully ramified of degree p over each supersingular point, and it is finite etale over the cusps. Q.E.D.

LEMMA 12.9.3. *For* $n \geq 1$, *we have canonically*

$$pr(n)^*(\Omega(n)) = \Omega(n+1) \otimes I(n+1, s.s.)^{\otimes p^{2n}(p-1)} .$$

Proof. We may assume k algebraically closed. The map pr(n) is finite etale except over the supersingular points. So what we must show is that for each supersingular point of $\overline{\mathcal{M}}(\mathcal{P})$, corresponding to an elliptic curve E/k together with a level $\mathcal{P}$-structure, if we denote by x_n any formal parameter on $\overline{\mathcal{M}}(\mathcal{P}, [Ig(p^n)])$ at the unique supersingular point of $\overline{\mathcal{M}}(\mathcal{P}, [Ig(p^n)])$ lying over it, then

$$pr(n)^*(dx_n) = (\text{unit}) \times (x_{n+1})^{p^{2n}(p-1)} dx_{n+1}$$

This we verify as follows. The formal group $\hat{E}$ of E/k is "the" unique one-parameter group of height two over k. We wish to choose a particularly simple model for it.

By Lubin-Tate theory, there exists a one-parameter formal group over $\mathbf{Z}_p$ for which the series for multiplication by p is given by

$$[p](X) = pX + X^{p^2} .$$

(This is "the" Lubin-Tate group for $W(\mathbf{F}_{p^2})$, with parameter p.) Its reduction mod p is then a height two group, say G, over $\mathbf{F}_p$, in which

$$[p](X) = F^2(X) = X^{p^2} = V(F(X)) = V(X^p) .$$

Therefore Verschiebung is given by

$$V(X) = X^p .$$

The parameter X is already linearized for the action of μ_{p-1} (in fact for the action of μ_{p^2-1}, as is obvious from the form of $[p](X)$ and Lubin-Tate theory).

Now consider the universal formal deformation $E/k[[T]]$ of E/k (to artin local k-algebras). In terms of a formal parameter X for $\hat{E}$ which is linearized for μ_{p-1} and which coincides with the above Lubin-Tate parameter X at $T = 0$, the expression for

$$V : \hat{E}^{(p)} \to \hat{E}$$

is, for a suitable choice of T (cf. (12.4.4)),

$$V(X) = TX + a(T)X^p + (TX^{2p-1}) ,$$

$$\text{with } a(T) \equiv 1 \mod (T) .$$

We obtain parameters $X_1, X_2, \cdots$ for the unique supersingular point in $\bar{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p^n)])$, $n = 1, 2, \cdots$ lying over as follows. For X_1, we take the X-coordinate of a *generator* of $\mathrm{Ker}(V)$. By the theory of cyclicity (cf. 6.7.5), the scheme of generators $\mathrm{Ker}(V)^\times$ of $\mathrm{Ker}\, V$ is given as Cartier divisor inside $E^{(p)}$ by

$$\mathrm{Ker}(V) = [0] + \mathrm{Ker}(V)^\times .$$

Therefore X_1 is any solution of $V(X)/X = 0$, i.e., of

$$0 = T + a(T)X^{p-1} + (TX^{2p-2}) .$$

The parameter X_2 is the X-coordinate of any point on $\hat{E}^{(p^2)}$ which maps by V to the point of $\hat{E}^{(p)}$ with coordinate X_1. The expression for

$$V : \hat{E}^{(p^2)} \to \hat{E}^{(p)}$$

is given by

$$V(X) = T^pX + a(T)^p \cdot X^p + (T^pX^{2p-1}) .$$

Thus X_2 is any solution of

$$X_1 = T^pX + a(T)^pX^p + (T^pX^{2p-1}) .$$

Proceeding inductively, we have, for $n \geq 1$, the description of X_{n+1} as any solution of

$$X_n = T^{p^n}X + a(T)^{p^n}X^p + (T^{p^n}X^{2p-1}) .$$

Thus we have the equation

$$X_n = T^{p^n}X_{n+1} + a(T)^{p^n}(X_{n+1})^p + (T^{p^n}X_{n+1}^{2p-1}) .$$

Differentiating, we find

$$dX_n = T^{p^n}dX_{n+1} + (T^{p^n}X_{n+1}^{2p-2})dX_{n+1} ,$$

so certainly

$$dX_n = (\text{unit})T^{p^n} \cdot dX_{n+1} .$$

Because $\bar{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p^{n+1})])$ is fully ramified over $\bar{\mathcal{M}}(\mathcal{P})$ at each supersingular point, of degree $\phi(p^{n+1})$, we have

$$T = (X_{n+1})^{\phi(p^{n+1})} \times (\text{unit}) ,$$

so that all in all

$$dX_n = (\text{unit})(X_{n+1})^{p^{2n}(p-1)} \cdot dX_{n+1} ,$$

as required. Q.E.D.

We can now complete the proof of the theorem (12.9.1). We already have proven (cf. (12.8.6), (12.8.7)) that

$$\mathrm{pr}(0)^*(\underline{\omega}) \simeq I(1, \mathrm{s.s.})^{-1}$$

$$\mathrm{pr}(0)^*(\underline{\omega}^{\otimes p}) \simeq \Omega(1) \otimes I(1, \mathrm{cusps})^{-1}$$

The first relation, when pulled back successively by $\mathrm{pr}(1), \cdots, \mathrm{pr}(n-1)$, gives, by (12.9.2)

$$\text{(A)} \qquad \mathrm{pr}^*(\underline{\omega}) \simeq I(n, \mathrm{s.s.})^{-p^{n-1}}$$

The second gives, successively, by (12.9.3)

$$\mathrm{pr}(1)^*\mathrm{pr}(0)^*(\underline{\omega}^{\otimes p}) \simeq \Omega(2) \otimes I(2, \mathrm{s.s.})^{p^2(p-1)} \otimes I(2, \mathrm{cusps})^{-1}$$

$$\mathrm{pr}(2)^*(\quad " \quad) \simeq \Omega(3) I(3, \mathrm{s.s.})^{\otimes p^4(p-1)} \otimes I(3, \mathrm{s.s.})^{\otimes p^3(p-1)} \otimes I(3, \mathrm{cusps})^{-1}$$

$$\vdots$$

$$\text{(B)} \quad \mathrm{pr}^*(\underline{\omega}^{\otimes p}) \simeq \Omega(n) \otimes (I(n, \mathrm{s.s.})^{\otimes (p-1)[p^{2n-2} + p^{2n-3} + \cdots p^n]}) \otimes I(n, \mathrm{cusps})^{-1}$$

whence finally

$$\mathrm{pr}^*(\underline{\omega}^{\otimes p}) \simeq \Omega(n) \otimes I(n, \mathrm{cusps})^{-1} \otimes I(n, \mathrm{s.s.})^{\otimes (p^{2n-1} - p^n)} .$$

Using (A), we have

$$\mathrm{pr}^*(\underline{\omega}^{\otimes p}) = (\mathrm{pr}^*(\underline{\omega}))^{\otimes p} \simeq I(n, \mathrm{s.s.})^{-p^n} ,$$

and comparing the above two expressions we see that

$$I(n, \mathrm{s.s.})^{-p^{2n-1}} \simeq \Omega(n) \otimes I(n, \mathrm{cusps})^{-1} ,$$

which together with (A) gives the desired relation

$$\mathrm{pr}^*(\underline{\omega}^{\otimes p^n}) \simeq \Omega(n) \otimes I(n, \mathrm{cusps})^{-1} . \qquad \text{Q.E.D.}$$

COROLLARY 12.9.4. *Hypotheses and notations as in the theorem (12.9.1) suppose that* $\overline{\mathcal{M}}(\mathcal{P})$ *is geometrically connected. Let us denote, for each* $n \geq 1$

$g(n, \mathcal{P})$ = *the genus of* $\overline{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p^n)])$

$c(n, \mathcal{P})$ = *the number of cusps on* $\overline{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p^n)])$

$\mathrm{s.s.}(n, \mathcal{P})$ = *the number of supersingular points on* $\overline{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p^n)])$

$\deg(n, \mathcal{P})$ = *the degree with which* $(\mathcal{P}, [\mathrm{Ig}(p^n)])$ *is finite flat over* (Ell/k)

$\deg(\underline{\omega}_{n,\mathcal{P}})$ = *the degree of* $\mathrm{pr}^*(\underline{\omega})$ (= *"the"* $\underline{\omega}$) *on* $\overline{\mathcal{M}}(\mathcal{P}, [\mathrm{Ig}(p^n)])$.

Then we have the formulas, for all $n \geq 1$, *(compare 10.13.12)*

$$p^n \cdot \deg(\underline{\omega}_{n,\mathcal{P}}) = 2g(n, \mathcal{P}) - 2 + c(n, \mathcal{P})$$

$$c(n, \mathcal{P}) = \phi(p^n) \cdot c(\mathcal{P})$$

$$\mathrm{s.s.}(n, \mathcal{P}) = \mathrm{s.s.}(0, \mathcal{P}) = \frac{p-1}{24} \deg(\mathcal{P})$$

$$\deg(\underline{\omega}_{n,\mathcal{P}}) = \phi(p^n) \cdot \deg(\underline{\omega}_{\mathcal{P}}) = \phi(p^n) \cdot \frac{1}{24} \cdot \deg(\mathcal{P})$$

$$\deg(n, \mathcal{P}) = \phi(p^n) \deg(\mathcal{P}) .$$

(12.10) *"Exotic" projections from Igusa curves; "exotic" Igusa structures*

(12.10.1) Let k be a perfect field of characteristic p, $\sigma: k \to k$ its absolute Frobenius automorphism. For any integer $i \in \mathbf{Z}$, and any k-scheme S, we denote by $S^{(\sigma^i)}$ the k-scheme

$$S^{(\sigma^i)} = S \otimes_{k, \sigma^i} k .$$

Given a moduli problem $\mathcal{P}$ on (Ell/k), we denote by $\mathcal{P}^{(\sigma^i)}$ the moduli problem on (Ell/k) obtained from $\mathcal{P}$ by extension of scalars $k \xrightarrow{\sigma^i} k$.

For any $E/S/k$, we have canonically

$$\mathcal{P}(E/S) = \mathcal{P}^{(\sigma^i)}(E^{(\sigma^i)}/S^{(\sigma^i)}) .$$

If $\mathcal{P}$ is relatively representable, then so is $\mathcal{P}^{(\sigma^i)}$, and we have

$$(\mathcal{P}^{(\sigma^i)})_{E^{(\sigma^i)}/S^{(\sigma^i)}} = (\mathcal{P}_{E/S})^{(\sigma^i)} .$$

If $\mathcal{P}$ is representable, so is $\mathcal{P}^{(\sigma^i)}$ and we have

$$\mathfrak{M}(\mathcal{P}^{(\sigma^i)}) = \mathfrak{M}(\mathcal{P})^{(\sigma^i)} .$$

If $\mathcal{P}$ is finite over (Ell/k) and normal near infinity, so is $\mathcal{P}^{(\sigma^i)}$, and we have

$$\overline{\mathfrak{M}}(\mathcal{P}^{(\sigma^i)}) = \overline{\mathfrak{M}}(\mathcal{P})^{(\sigma^i)} .$$

For example, if $N \geq 1$ is any integer, and $\zeta_N \in k$ is a "primitive" N'th root of unity, then for $\mathcal{P}$ the moduli problem "$[\Gamma(N)]$-structures (P,Q) with $e_N(P,Q) = \zeta_N$", $\mathcal{P}^{(\sigma^i)}$ is the analogous moduli problem defined with respect to $\zeta_N^{\sigma^i}$. Similarly for $\mathcal{P}$ the moduli problem "bal. $\Gamma_1(N)$-structures with $<P,Q> = \zeta_N$." For the moduli problem $\mathcal{P} = [\Gamma_1(N)]$, or $[\Gamma_0(N)]$, we have $\mathcal{P}^{(\sigma^i)} = \mathcal{P}$, as we do for any $\mathcal{P}$ which begins life on (Ell/F_p).

(12.10.2) For any $\mathcal{P}$ on (Ell/k), any $i \geq 1$, there is a natural map of sets, for any $E/S/k$,

(12.10.2.1) $$\mathcal{P}(E/S) \to \mathcal{P}^{(\sigma^i)}(E^{(p^i)}/S) ,$$

$$\alpha \text{ on } E/S \mapsto \text{the induced structure } \alpha^{(p^i)} \text{ on } E^{(p^i)}/S .$$

which is the composite of the canonical identification

$$\mathcal{P}(E/S) = \mathcal{P}^{(\sigma^i)}(E^{(\sigma^i)}/S^{(\sigma^i)})$$

with the map on $\mathcal{P}^{(\sigma^i)}$ induced by the morphism *in* (Ell/k)

$$\begin{array}{ccc} E^{(p^i)} & \longrightarrow & E^{(\sigma^i)} \\ \downarrow & & \downarrow \\ S & \xrightarrow{F^i_{S/k}} & S^{(\sigma^i)} \end{array}$$

If $\mathcal{P}$ is relatively representable and *etale* over (Ell/k), this map (12.10.2.1) is always *bijective* (cf. SGA 4½, Rapport, 1.2).

For example, if $\mathcal{P}$ is $[\Gamma_1(N)]$, this map (12.10.2.1) is

$$E/S,\ P \text{ of exact order } N \longmapsto E^{(p^i)}/S,\ F^i(P) .$$

Similarly, if $\mathcal{P}$ is "$[\Gamma(N)]$-structures (P,Q) with $e_N(P,Q) = \zeta_N$", this map is

$$E/S, (P,Q) \longmapsto E^{(p^i)}/S,\ (F^i(P), F^i(Q)) .$$

When N is prime to p, the inverse maps are, respectively

$$E/S, \frac{1}{p^i} V^i(P) \longleftarrow E^{(p^i)}/S, P$$

$$E/S, \left(\frac{1}{p^i} V^i(P), \frac{1}{p^i} V^i(Q)\right) \longleftarrow E^{(p^i)}/S, (P,Q) .$$

When $\mathcal{P}$ is representable, the induced map on moduli schemes obtained by passing to isomorphism classes is none other than the i-fold iterated relative-to-k Frobenius,

$$F^i_{\mathfrak{M}(\mathcal{P})/k} : \mathfrak{M}(\mathcal{P}) \to \mathfrak{M}(\mathcal{P})^{(\sigma^i)} .$$

Similarly, if $\mathcal{P}$ is relatively representable, and affine over (Ell/k), the induced map of coarse moduli schemes is

$$F^i_{M(\mathcal{P})/k} : M(\mathcal{P}) \to M(\mathcal{P}^{(\sigma^i)}) = M(\mathcal{P})^{(\sigma^i)} ,$$

sitting over the i-fold relative Frobenius on the affine j-line "over k"

$$\begin{array}{ccc} M(\mathcal{P}) & \xrightarrow{F^i} & M(\mathcal{P})^{(\sigma^i)} \\ \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle j} \\ \mathrm{Spec}\,(k[j]) & \xrightarrow{F^i} & \mathrm{Spec}\,(k[j])\,. \end{array}$$

If $\mathcal{P}$ is relatively representable, finite over (Ell/k), and normal near infinity, this diagram shows that we get an induced map of compactified coarse moduli schemes

$$\begin{array}{ccc} \overline{M}(\mathcal{P}) & \xrightarrow{F^i} & \overline{M}(\mathcal{P})^{(\sigma^i)} \\ \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle j} \\ \mathbf{P}^1_k & \xrightarrow{F^i} & \mathbf{P}^1_k \end{array}$$

(12.10.3) For any representable moduli problem $\mathcal{P}$ on (Ell/k), any integer $i \geq 0$, and any integer $n \geq 0$, we denote by

$$pr_i : \mathfrak{M}(\mathcal{P}, [\mathrm{Ig}(p^n)]) \to \mathfrak{M}(\mathcal{P})^{(\sigma^i)}$$

the map deduced by passage to isomorphism classes from the construction (12.10.2.1):

$$\begin{pmatrix} E/S, \alpha \in \mathcal{P}(E/S), \\ P \in E^{(p^n)}(S) \text{ gen. of } \mathrm{Ker}(V^n) \end{pmatrix} \longmapsto \left(E^{(p^i)}/S, \alpha^{(p^i)} \right).$$

Thus pr_0 is "the" projection denoted pr earlier, and for any $i \geq 1$ we have

$$pr_i = F^i \circ pr\,,$$

i.e., the diagram below is commutative

$$\begin{array}{ccc} \mathfrak{M}(\mathcal{P}, [\mathrm{Ig}(p^n)]) & \xrightarrow{F^i} & \mathfrak{M}(\mathcal{P}^{(\sigma^i)}, [\mathrm{Ig}(p^n)]) \\ & \searrow^{pr_i} & \downarrow{\scriptstyle pr} \\ \downarrow{\scriptstyle pr} & & \\ \mathfrak{M}(\mathcal{P}) & \xrightarrow{F^i} & \mathfrak{M}(\mathcal{P}^{(\sigma^i)})\,. \end{array}$$

(12.10.4) If $\mathcal{P}$ is representable and finite etale over (Ell/k), we have a commutative diagram of compactifications

$$\begin{array}{ccc} \overline{\mathfrak{M}}(\mathcal{P}, [\mathrm{Ig}(p^n)]) & \xrightarrow{F^i} & \overline{\mathfrak{M}}(\mathcal{P}^{(\sigma^i)}, [\mathrm{Ig}(p^n)]) \\ & \searrow^{pr_i} & \downarrow{\scriptstyle pr} \\ \downarrow{\scriptstyle pr} & & \\ \overline{\mathfrak{M}}(\mathcal{P}) & \xrightarrow{F^i} & \overline{\mathfrak{M}}(\mathcal{P})^{(\sigma^i)} \\ \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle j} \\ \mathbf{P}^1_k & \xrightarrow{F^i} & \mathbf{P}^1_k\,. \end{array}$$

(12.10.5) For each $1 \leq i \leq n$, the projection

$$pr_i : \mathfrak{M}(\mathcal{P}, [\mathrm{Ig}(p^n)]) \to \mathfrak{M}(\mathcal{P}^{(\sigma^i)})$$

allows a *simple reinterpretation* of $\mathfrak{M}(\mathcal{P}, [\mathrm{Ig}(p^n)])$ as a modular scheme, for any representable $\mathcal{P}$ which is etale over (Ell/k).

For $1 \leq i \leq n$, let us denote by

$$[\mathrm{ExIg}(p^n, i)]$$

the moduli problem on $(\mathrm{Ell}/\mathbf{F}_p)$ defined by

(12.10.5.1) $[\mathrm{ExIg}(p^n, i)](E/S)$ = a point $P \in E(S)$ such that $(0, P)$ is a Drinfeld p^i-basis of E/S, plus a point $Q \in E^{(p^{n-i})}(S)$ such that $V^{n-i}(Q) = P$.

THEOREM 12.10.6. *For* $1 \leq i \leq n$, *there is an exotic isomorphism of moduli problems on* $(\mathrm{Ell}/\mathbf{F}_p)$

$$[\mathrm{Ig}(p^n)] \xrightarrow{\sim} [\mathrm{ExIg}(p^n, i)]$$

defined by

$$\begin{pmatrix} E/S \text{ plus a point} \\ P \in E^{(p^n)}(S) \text{ generating} \\ \mathrm{Ker}(V^n : E^{(p^n)} \to E) \end{pmatrix} \longmapsto \begin{pmatrix} \text{the curve } E^{(p^i)}/S, \text{ the point} \\ V^{n-i}(P) \in E^{(p^i)}(S), \text{ the point} \\ P \in (E^{(p^i)})^{(p^{n-i})}(S) \end{pmatrix}.$$

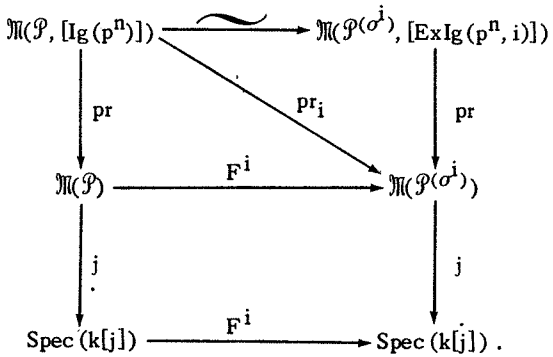
For any representable $\mathcal{P}$ *etale over* (Ell/k), k *a perfect field, this construction together with*

$$a \in \mathcal{P}(E/S) \longmapsto a^{(p^i)} \in \mathcal{P}^{(\sigma^i)}(E^{(p^i)}/S),$$

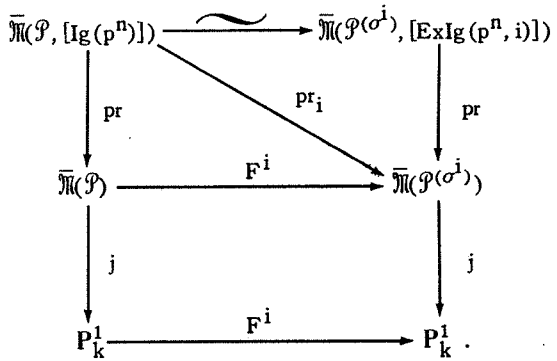
defines an exotic isomorphism of moduli problems on (Ell/k)

$$(\mathcal{P}, [\mathrm{Ig}(p^n)]) \longmapsto (\mathcal{P}^{(\sigma^i)}, [\mathrm{ExIg}(p^n, i)]).$$

The induced isomorphism of moduli schemes sits in a commutative diagram



If $\mathcal{P}$ *is finite etale over* (Ell/k), *this diagram extends to a diagram of compactified moduli schemes*



Proof. This results immediately from (12.2.7) and (12.3.2), and the preceding discussion. Q.E.D.

COROLLARY (12.10.7) *Let* k *be a perfect field of characteristic* p. *Suppose that* $\mathcal{P}$ *is representable, finite etale over* (Ell/k), *that* ± 1 *acts freely on* $Z(\mathcal{P})$, *and that the Kodaira-Spencer isomorphism on* $\mathcal{M}(\mathcal{P})$ *extends to an isomorphism on* $\overline{\mathcal{M}}(\mathcal{P})$

$$\underline{\omega}^{\otimes 2} \simeq \Omega^1_{\overline{\mathcal{M}}(\mathcal{P})}(\log \text{ cusps}).$$

Then for $1 \leq i \leq n$, *the projection*

$$\mathrm{pr} : \overline{\mathcal{M}}(\mathcal{P}, [\mathrm{ExIg}(p^n, i)]) \to \overline{\mathcal{M}}(\mathcal{P})$$

leads to an isomorphism of invertible sheaves on $\overline{\mathcal{M}}(\mathcal{P}, [\mathrm{ExIg}(p^n, i)])$

$$\mathrm{pr}^*(\underline{\omega}^{\otimes p^{n-i}}) \simeq \Omega^1(\log \text{ cusps}).$$

Proof. This is just a rewriting of (12.9.1), in view of the above commutative diagram. Q.E.D.

COROLLARY 12.10.8. *Hypotheses as above, consider the special case* $i = n \geq 1$, *when*

$$[\mathrm{ExIg}(p^n, n)](E/S) = \{\text{points } P \in E(S) \text{ such that } (P, O) \text{ is a Drinfeld } p^n\text{-basis on } E/S\}.$$

For the projection

$$\mathrm{pr} : \overline{\mathfrak{M}}(\mathcal{P}, [\mathrm{ExIg}(p^n, n)]) \longrightarrow \overline{\mathfrak{M}}(\mathcal{P}) ,$$

we have an isomorphism of line bundles on $\overline{\mathfrak{M}}(\mathcal{P}, [\mathrm{ExIg}(p^n, n)])$

$$\mathrm{pr}^*(\underline{\omega}) \simeq \Omega^1(\log \text{ cusps}) .$$

Proof. This is the case $i = n$ of the previous result. Q.E.D.

REMARK 12.10.9. It is this remarkable formula, which is "off by a factor of two" from the formula (10.13.11)

$$\underline{\omega}^{\otimes 2} \simeq \Omega^1(\log \text{ cusps})$$

which holds on $\overline{\mathfrak{M}}(\mathcal{P})$ itself, which underlies all the phenomena of "good reduction" we will exhibit in Chapter 14.

Chapter 13

REDUCTIONS mod p OF THE BASIC MODULI PROBLEMS

(13.1) *Some general considerations on crossings at supersingular points*

(13.1.1) Let k be a field. We suppose given

$$\begin{array}{c} X \\ \downarrow \\ Y \\ \downarrow \\ \mathrm{Spec}(k) \end{array}$$

where

(1) Y is a smooth curve over k

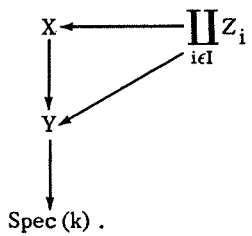
(2) X is finite and flat over Y.

We further suppose given a non-empty finite set of k-valued points of Y, which we call the "supersingular points," and we suppose that

(3) Lying over each supersingular point y_0 of Y, there is a unique closed point x_0 of X, that point is k-rational, and the complete local ring of X at x_0 is isomorphic to

$$k[[x, y]]/(\text{one equation}) .$$

We further suppose given a finite collection of k-schemes $\{Z_i\}_{i \in I}$ which sit in a diagram



We assume that

(4) For each $i \in I$, and each supersingular point y_0 of Y, there is a unique closed point $z_{i,0}$ of Z_i lying over y_0, and this point $z_{i,0}$ is k-rational;

(5) each Z_i is finite and flat over Y;

(6) each $(Z_i)^{red}$ is a smooth curve over k;

(7) for each i, $Z_i \to X$ is a closed immersion;

(8) over the open set $Y - \{\text{s.s. points}\}$ of Y, the morphism $\coprod_{i\in I} Z_i \to X$ is an isomorphism.

CROSSINGS THEOREM 13.1.3. *In the above situation, let y_0 be a supersingular point of Y, x_0 the unique closed point of X lying over it. Then the complete local ring of X at x_0 is of the form*

$$k[[x,y]]/\prod_{i\in I} f_i^{e_i},$$

where the f_i's are distinct-modulo-units irreducibles in the ring $k[[x,y]]$, and where, for each $i \in I$, the complete local ring

$$k[[x,y]]/(f_i^{e_i})$$

is isomorphic to the complete local ring of Z_i at $z_{i,0}$.

If Y is connected (respectively, geometrically connected), then so are the Z_i, and then the Z_i are the irreducible components of X.

Proof. Because Y is smooth over k, and y_0 is k-rational, the complete local ring of Y at y_0 is of the form $k[[T]]$. By hypothesis, the complete local ring of X at x_0 is of the form

$$k[[x,y]]/(\text{one equation}) .$$

Because $X \to Y$ is finite flat, the ring extension

$$\begin{array}{c} k[[x,y]]/(\text{one equation}) \\ \uparrow \\ k[[T]] \end{array}$$

is finite flat. Therefore "one equation" is neither zero nor a unit in $k[[x,y]]$. Factoring it up-to-units into powers of distinct-up-to-units irreducibles in $k[[x,y]]$, the situation looks like

$$\begin{array}{c} k[[x,y]]/\left(\prod_{j\in J} f_j^{e_j}\right) \\ \uparrow \\ k[[T]] , \end{array}$$

where the f_j's are indexed by some finite non-void indexing set J.

Now we exploit the fact that

$$\begin{array}{c} k[[x,y]]/\left(\prod f_j^{e_j}\right) \\ \uparrow \\ k[[T]] \end{array}$$

is finite and flat of some degree $d \geq 1$. Let $T_1 \in k[[x,y]]$ be any element which reduces mod $\prod f_j^{e_j}$ to T. Then the quotient

$$k[[x,y]]/\left(\prod f_j^{e_j}, T_1\right)$$

is a d-dimensional k-vector space. Therefore T_1 is a non-unit, and it is non-zero. Let us write its factorization in $k[[x,y]]$ as

$$T_1 = \prod g_k^{n_k} .$$

Then for each pair (j,k), the ring

$$k[[x,y]]/(f_j, g_k)$$

is a quotient of a finite-dimensional k-algebra, so is itself finite dimensional. Therefore we conclude that for all (j,k), f_j and g_k are distinct-up-to-units irreducibles of $k[[x,y]]$.

Now consider the ring

$$k[[x,y]][1/T_1] .$$

It is a regular one-dimensional ring with unique factorization, and its irreducibles up-to-units are exactly

$$\{\text{all irreducibles of } k[[x,y]]\} - \{\text{the irreducibles which divide } T_1\} .$$

Therefore the f_i's remain irreducible non-units in the ring

$$k[[x,y]][1/T_1] .$$

By the Chinese Remainder Theorem, we have

$$k[[x,y]][1/T_1]/\prod f_j^{e_j} \xrightarrow{\sim} \prod \left(k[[x,y]][1/T_1]/(f_j^{e_j}) \right) .$$

and each factor

$$k[[x,y]][1/T_1]/(f_j^{e_j})$$

is itself an artin local ring. Thus we have a cartesian diagram

$$\begin{array}{ccc} X & \supset & \operatorname{Spec}\left((k[[x,y]]/\prod f_j^{e_j}) \underset{k[[T]]}{\otimes} k((T)) \right) \simeq \prod \operatorname{Spec}\left((k[[x,y]]/f_j^{e_j}) \underset{k[[T]]}{\otimes} k((T)) \right) \\ \downarrow & & \downarrow \quad \swarrow \\ Y & \longleftarrow & \operatorname{Spec}(k((T))) . \end{array}$$

By hypothesis, over the open set $Y - \{\text{s.s. points}\}$, we have

$$X \xleftarrow{\sim} \coprod Z_i ,$$

so in particular over $\operatorname{Spec}(k((T))) \to Y - \{\text{s.s. points}\}$, we have

$$X \underset{Y}{\times} \operatorname{Spec}(k((T))) \xleftarrow{\sim} \coprod_{i \in I} Z_i \underset{Y}{\otimes} \operatorname{Spec}(k((T))) .$$

By assumption, Z_i has a unique closed point $z_{i,0}$ lying over x_0, this point is k-rational, and Z_i^{red} is a smooth curve. Therefore

$$Z_i \underset{Y}{\otimes} \operatorname{Spec}(k((T))) = \operatorname{Spec}(\hat{\mathcal{O}}_{Z_i, z_{i,0}} \underset{k[[T]]}{\otimes} k((T))) .$$

This scheme is irreducible, because

$$Z_i^{\text{red}} \underset{Y}{\otimes} \operatorname{Spec}(k((T))) = (Z_i \underset{Y}{\otimes} \operatorname{Spec}(k((T))))^{\text{red}}$$

is itself reduced and irreducible (being isomorphic to $k((z))$ for z a uniformizing parameter at $z_{i,0}$ on $(Z_j)^{\text{red}}$). Therefore we have an equality of $k((T))$-schemes

$$\coprod_j \operatorname{Spec}\left((k[[x,y]]/f_j^{e_j}) \underset{k[[T]]}{\otimes} k((T)) \right) \simeq \coprod_i Z_i \underset{Y}{\otimes} \operatorname{Spec}(k((T))) ,$$

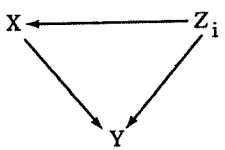
each expressed as a disjoint union of irreducible schemes. Therefore there is a bijection of the two indexing sets, under which, for each i, we have an isomorphism of $k((T))$-algebras

$$(k[[x,y]]/(f_i^{e_i})) \underset{k[[T]]}{\otimes} k((T)) \simeq \hat{\mathcal{O}}_{Z_i, z_{i,0}} \underset{k[[T]]}{\otimes} k((T)) .$$

It remains to prove the final assertion. We must explain why the above isomorphism extends to an isomorphism

$$\operatorname{Spec}(\hat{\mathcal{O}}_{Z_i, z_{i,0}}) \xrightarrow{\sim} \operatorname{Spec}(k[[x,y]]/f_i^{e_i}) .$$

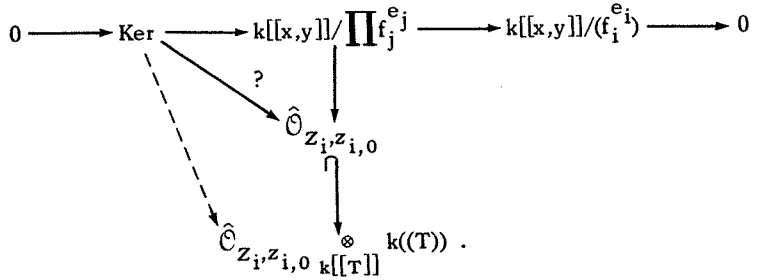
Recall that we were given a diagram



so we certainly have a homomorphism of complete local $k[[T]]$-algebras

$$k[[x,y]]/\prod_j f_j^{e_j} \to \hat{\mathcal{O}}_{Z_i,z_{i,0}}.$$

We first claim this map factors through the projection onto $k[[x,y]]/(f_i^{e_i})$. Consider the diagram



The lowest vertical arrow is injective because $\hat{\mathcal{O}}$ is flat over $k[[T]]$. We know that the dotted arrow vanishes, so we conclude that the diagonal arrow "?" also vanishes. This gives us a homomorphism

$$k[[x,y]]/(f_i^{e_i}) \to \hat{\mathcal{O}}_{Z_i,z_{i,0}}.$$

We next remark that the $k[[T]]$-algebra

$$k[[x,y]]/(f_i^{e_i})$$

is flat over $k[[T]]$ (simply because it is finite over this regular ring of

dimension one, and is itself Cohen-Macaulay of dimension one, being defined by one equation in a regular scheme of dimension two). Thus we have a homomorphism between *free* $k[[T]]$-algebras of finite rank, which is an isomorphism after inverting T. Therefore it is *injective*. It is surjective because it sits in

$$k[[x,y]]/\left(\prod f_j^{e_j}\right) \twoheadrightarrow k[[x,y]]/(f_i^{e_i}) \to \hat{\mathcal{O}}_{Z_i,z_{i,0}},$$

in which the composite is surjective because $Z_i \to X$ is a closed immersion.

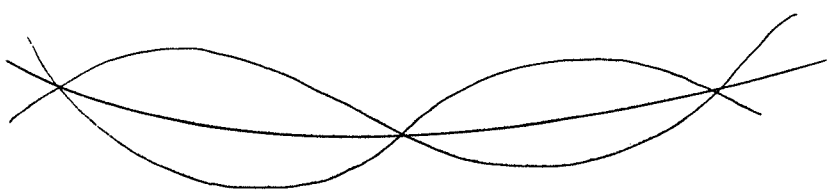
It remains to show that each Z_i is connected (resp. geometrically connected) if Y is. This is clear from the fact that Z_i has a *unique* point lying over each supersingular point of Y, and that $Z_i \to Y$ is finite and flat (compare 12.6.2). Once Z_i is connected, it is irreducible, because $(Z_i)^{red}$ is a smooth curve over k. Q.E.D.

REMARK 13.1.4. If all the Z_i are *reduced*, then the crossings theorem shows that X itself is *reduced*.

(13.1.5) *Terminology.*

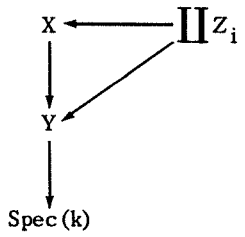
In the above situation, we will say that X is "the" disjoint union of the Z_i's with crossings at the supersingular points.

(13.1.6) *"Picture"* of three Z_i's, three supersingular points, to be visualized as intersecting strings in 3-space.



(13.1.7) *More terminology*

Suppose we are given a diagram



and a closed subscheme in Y, finite etale over $\mathrm{Spec}(k)$, of "supersingular points." Suppose that axioms 1), 2), 5), 6), 7), 8) hold, and that axioms 3) and 4) *become true* after extending scalars to a separable closure $\bar{k}$ of k. We will still say in this situation that X is the disjoint union of the Z_i's with crossings at the supersingular points.

(13.2) *Modular schemes as examples*

(13.2.1) Let Γ be a subgroup of $GL(2, \mathbf{Z}/p^n\mathbf{Z})$, A the ring $(\mathbf{Z}[\zeta_{p^n}])^{\det(\Gamma)} \subset \mathbf{Z}[\zeta_{p^n}]$. Consider the moduli problem

$$([\Gamma(p^n)]/\Gamma)^{A\text{-can}} \quad \text{on} \quad (\mathrm{Ell}/A)\,.$$

Suppose that it is a regular moduli problem. By (9.1.8), this is equivalent to the regularity of the moduli problem $[\Gamma(p^n)]/\Gamma$ on $(\mathrm{Ell}/\mathbf{Z})$, and we have seen (7.6.1) that this problem is regular for each of the following Γ's:

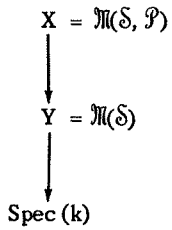
$$\begin{cases} \text{any } \Gamma \text{ contained in the "semi Borel" } \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \\ \Gamma = \begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix} \text{ for } H_1, H_2 \text{ subgroups of } (\mathbf{Z}/p^n\mathbf{Z})^\times \\ \Gamma = \begin{pmatrix} H_1 & * \\ 0 & H_2 \end{pmatrix} \text{ for } H_1, H_2 \text{ subgroups of } (\mathbf{Z}/p^n\mathbf{Z})^\times \\ \qquad\qquad \text{and } * \text{ unrestricted in } \mathbf{Z}/p^n\mathbf{Z}\,. \end{cases}$$

THEOREM 13.2.2. *Let k be a perfect field of characteristic p, $\mathcal{S}$ a representable moduli problem on (Ell/k) which is finite etale over (Ell/k), and such that all the supersingular points on $\mathcal{M}(\mathcal{S})$ are k-rational.*

1) *Let $\Gamma \subset GL(2, \mathbf{Z}/p^n\mathbf{Z})$ be a subgroup such that the moduli problem $([\Gamma(p^n)]/\Gamma)^{A\text{-can}}$ is regular, and denote by*

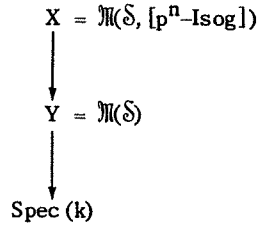
$$\mathcal{P} = ([\Gamma(p^n)]/\Gamma)^{A\text{-can}} \otimes_A k$$

the moduli problem on (Ell/k) deduced by the unique ring homomorphism $A \to k$. Then the moduli spaces



satisfy 1), 2), 3) of the Crossings Theorem (13.1.3).

2) *For any $n \geq 1$, the moduli spaces*



satisfy hypotheses 1), 2), 3) of the Crossings theorem.

Proof. Because $\mathcal{S}$ is finite etale over (Ell/k), $\mathcal{M}(\mathcal{S})$ is a smooth curve over k. The regular moduli problems (resp. $[p^n\text{-Isog}]$) are finite flat over (Ell/A) (resp. over $(\mathrm{Ell}/\mathbf{Z})$); in the first case because a finite map between regular two-dimensional schemes is flat, in the second because

we have proven it (6.8.1). Let y_0 be a k-valued point of $Y = \mathcal{M}(\mathcal{S})$ which is supersingular, corresponding to a supersingular elliptic curve E_0/k together with an element $a \in \mathcal{S}(E_0/k)$. Then a closed point of $X = \mathcal{M}(\mathcal{S}, \mathcal{P})$ lying over y_0 is the image of a closed point in $\mathcal{M}(\mathcal{S}, [\Gamma(p^n)])$ lying over y_0. But there is a *unique* closed point of $\mathcal{M}(\mathcal{S}, [\Gamma(p^n)])$ lying over y_0, and it is k-rational. To see this recall that such a closed point "is" a Drinfeld p^n-basis of $E_0 \otimes_k k'/k'$ for some finite extension field k'/k; as E_0 is supersingular we have $E_0[p^n](k') = 0$, so (0,0) is the unique possible Drinfeld p^n-basis, and it is k-rational. For $X = \mathcal{M}(\mathcal{S}, [p^n\text{–Isog}])$ the argument is similar; the unique closed point lying over y_0 is the *unique* subgroup of $E_0 \otimes_k \bar{k}$ of rank p^n, namely $\mathrm{Ker}(F_0^n)$, and it is k-rational.

It remains to explain why the complete local ring at the unique point x_0 of X lying over y_0 is of the form

$$k[[x,y]]/(\text{one equation}) .$$

In the case of $\mathcal{M}(\mathcal{S}, [p^n\text{–Isog}])$, the argument given in (6.8.2), applied to the deformation theory of p^n-isogenies over artin local k-algebras with residue field k, shows that the complete local ring of $\mathcal{M}(\mathcal{S}, [p^n\text{–Isog}])$ at any k-valued supersingular point is of the form

$$k[[x,y]]/(\text{one equation}) ,$$

where x and y are the local "T-coordinates" for the source and target of the isogeny.

In the case of $\mathcal{M}(\mathcal{S}, \mathcal{P})$, we argue as follows. The spectrum of the complete local ring of $\mathcal{M}(\mathcal{S}, \mathcal{P})$ at a k-valued supersingular point lying over $y_0 = (E_0/k, a)$ is (tautologically) equal to

$$\mathcal{P}_{E_0/k[[T]]} ,$$

where $E_0/k[[T]]$ denotes the universal deformation of E_0 to a complete local k-algebra with residue field k. Let $E/W(k)[[T]]$ denote the universal deformation of E_0 to a complete local ring with residue field k. Then $E \otimes_Z A/(A \otimes_Z W(k))[[T]]$ is the universal formal deformation of E_0 to a complete local A-algebra with residue field k (for $A = (\mathbb{Z}[\zeta_{p^n}])^{\det(\Gamma)}$, $A \otimes_Z W(k)$ is a complete discrete valuation ring with residue field k !).

By definition

$$\begin{aligned}
\mathcal{P}_{E_0/k[[T]]} &= k \otimes_A (([\Gamma(p^n)]/\Gamma)^{A\text{–can}})_{E \otimes_Z A/(A \otimes_Z W(k))[[T]]} \\
&= k \otimes_A ([\Gamma(p^n)]/\Gamma)_{E/W(k)[[T]]} \\
&= k \otimes_A \left(\begin{array}{l} \text{the spectrum of a two-dimensional complete regular} \\ \text{local A-algebra with residue field k} \end{array} \right) \\
&= k \underset{A \otimes_Z W(k)}{\otimes} \left(\begin{array}{l} \text{the spectrum of a two-dimensional complete} \\ \text{regular local } A \otimes_Z W(k)\text{-algebra with residue} \\ \text{field k.} \end{array} \right) .
\end{aligned}$$

Again because $A \otimes_Z W(k)$ is a complete discrete valuation ring with residue field k, any two-dimensional complete regular local $A \otimes_Z W(k)$-algebra with residue field k is of the form

$$(A \otimes_Z W(k))[[x,y]]/(f)$$

for some f lying in max but not in max^2. Tensoring over $A \otimes_Z W(k)$ with k, we obtain

$$\mathcal{P}_{E_0/k[[T]]} \simeq \text{the Spec of } k[[x,y]]/(\text{one equation}) . \qquad \text{Q.E.D.}$$

(13.3) *Analysis of p-power isogenies between elliptic curves*

PROPOSITION 13.3.1. *Let $E/S/F_p$ be an ordinary elliptic curve over an F_p-scheme. For every integer $n \geq 1$, the "standard factorization" of the cyclic p^{2n}-isogeny "multiplication by p^n" into two cyclic p^n-isogenies is*

$$E \xrightarrow{F^n} E^{(p^n)} \xrightarrow{V^n} E .$$

The kernel of V^n *is a finite etale* S*-group, locally (etale) on* S *isomorphic to* $\mathbb{Z}/p^n\mathbb{Z}$, *and the kernel of* F^n *is its Cartier dual, locally (etale) on* S *isomorphic to* μ_{p^n}.

Proof. The first assertion is (12.2.5). The finite etale S-scheme which makes the second true is none other than

$$[\mathrm{Ig}(p^n)]_{E/S} . \qquad \text{Q.E.D.}$$

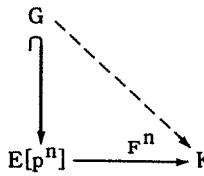
PROPOSITION 13.3.2. *Let* $E/S/\mathbb{F}_p$ *be an ordinary elliptic curve over an* $\mathbb{F}_p$*-scheme,* $n \geq 1$ *an integer, and* $G \subset E$ *a finite locally free* S*-subgroup-scheme of rank* p^n. *Then Zariski locally on* S *there exists a unique pair of integers* a, b *with* $a \geq 0$, $b \geq 0$, $a+b = n$, *such that*

1) $G \cap \mathrm{Ker}\, F^n = \mathrm{Ker}\, F^a$ *is a twisted* μ_{p^a};
2) G mod $\mathrm{Ker}\, F^a$ *is finite etale cyclic of order* p^{n-a}.

Proof. The group $E[p^n]$ sits in the short exact sequence

$$0 \longrightarrow \mathrm{Ker}\, F^n \longrightarrow E[p^n] \xrightarrow{F^n} \mathrm{Ker}\, V^n \longrightarrow 0$$

with $\mathrm{Ker}\, V^n$ a twisted $\mathbb{Z}/p^n\mathbb{Z}$. Consider the composite map



By (4.10.1), this dotted arrow maps G onto a finite etale subgroup H′ of $\mathrm{Ker}\, V^n$, which Zariski locally on S can be none other than the twisted $\mathbb{Z}/p^b\mathbb{Z}$ which is $\mathrm{Ker}(V^b : E^{(p^n)} \to E^{(p^{n-b})})$. Therefore the kernel of the dotted arrow is a finite locally free subgroup of G. But this kernel is

$G \cap \mathrm{Ker}\, F^n$, and therefore $G \cap \mathrm{Ker}(F^n)$ is a finite locally free subgroup of $\mathrm{Ker}(F^n)$. Because $\mathrm{Ker}(F^n)$ is a twisted μ_{p^n}, $G \cap \mathrm{Ker}(F^n)$ can be none other than one of the subgroups $\mathrm{Ker}(F^a : E \to E^{(p^a)})$. Comparing ranks, we see that $a+b = n$. Q.E.D.

THEOREM 13.3.3. *Let* E_0, E_n *be ordinary elliptic curves over a connected* $\mathbb{F}_p$*-scheme* S, *and let*

$$E_0 \xrightarrow{\pi_{0,n}} E_n$$

be a p^n*-isogeny,* $n \geq 1$. *Then there exist unique integers* $a, b \geq 0$, $a+b = n$, *such that this isogeny factors as*

$$E_0 \xrightarrow{F_0^a} E_0^{(p^a)} \xrightarrow[\varepsilon]{\sim} E_n^{(p^b)} \xrightarrow{V_n^b} E_n$$

where F_0 *denotes the Frobenius for* E_0, V_n *denotes the Verschiebung for* E_n, *and where* ε *is an isomorphism of elliptic curves over* S.

Proof. By the previous proposition, applied to $G = \mathrm{Ker}(\pi_{0,n})$, we have a short exact sequence

$$0 \to \mathrm{Ker}(F^a) \to G \to \text{a twisted } \mathbb{Z}/p^b\mathbb{Z} \to 0 .$$

Therefore our isogeny factors as

$$E_0 \xrightarrow{F_0^a} E_0^{(p^a)} \xrightarrow{\pi_{a,n}} E_n$$

where $\pi_{a,n}$ is a p^b-isogeny whose kernel is a twisted $\mathbb{Z}/p^b\mathbb{Z}$. Therefore its dual

$$E_0^{(p^a)} \xleftarrow[\pi_{a,n}^t]{} E_n$$

has kernel a twisted μ_{p^b}. Applying (13.3.2) to $\mathrm{Ker}\,\pi_{a,n}^t$, we see that we must have $\mathrm{Ker}(\pi_{a,n}^t) = \mathrm{Ker}(F_n^b : E_n \to E_n^{(p^b)})$. Q.E.D.

(13.3.3.4) We will call an isogeny of the form

$$E_0 \xrightarrow{F_0^a} E_0^{(p^a)} \xrightarrow{\sim} E_n^{(p^b)} \xrightarrow{V_n^b} E_n$$

a p^n-isogeny of type (a,b), or an (a,b) isogeny if p is understood. We next will analyze when an (a,b) isogeny between *ordinary* elliptic curves is *cyclic*. For this it is convenient to introduce an auxiliary rigidification.

THEOREM 13.3.5. *Let* k *be a perfect field of characteristic* p, *and* $\mathcal{P}$ *a representable moduli problem on* (Ell/k) *which is finite etale over* (Ell/k). *Consider an* (a,b) *isogeny between elliptic curves over a* k*-scheme* S:

$$E_0 \xrightarrow{F_0^a} E_0^{(p^a)} \xrightarrow[\varepsilon]{\sim} E_n^{(p^b)} \xrightarrow{V_n^b} E_n .$$

Let $a_0 \in \mathcal{P}(E_0/S)$ *be a level* $\mathcal{P}$*-structure on* E_0/S. *Denote by*

$$a_a \overset{\text{dfn}}{=\!=} (a_0)^{(p^a)} \in \mathcal{P}(\sigma^a)(E_0^{(p^a)}/S) ,$$

$\beta_n \in \mathcal{P}(\sigma^{a-b})(E_n/S)$ *the unique element such that in* $\mathcal{P}(\sigma^a)(E_n^{(p^b)}/S)$, *we have* $(\beta_n)^{(p^b)} = (\varepsilon^{-1})^*(a_a)$.

Denote by

$x_0 \in \mathcal{M}(\mathcal{P})(S)$ *the isomorphism class of* $(E_0/S, a_0)$,

$x_n \in \mathcal{M}(\mathcal{P}(\sigma^{a-b}))(S)$ *the isomorphism class of* $(E_n/S, \beta_n)$,

and by $F : \mathcal{M}(\mathcal{P}(\sigma^i)) \to \mathcal{M}(\mathcal{P}(\sigma^{i+1}))$ *the relative-to-*k *Frobenius. Then we have the following results:*

(1) $F^a(x_0) = F^b(x_n)$ *in* $\mathcal{M}(\mathcal{P}(\sigma^a))(S)$.

(2) *If* $a = 0$ *or if* $b = 0$, *then any* (a,b) *isogeny is cyclic.*

(3) *If both* $a \geq 1$ *and* $b \geq 1$, *and if the point*

$$(F^{a-1}(x_0), F^{b-1}(x_n)) \in (\mathcal{M}(\mathcal{P}(\sigma^{a-1})) \underset{k}{\times} \mathcal{M}(\mathcal{P}(\sigma^{a-1})))(S)$$

lies in the p–1*'st infinitesimal neighborhood of the diagonal (i.e., the closed subscheme defined by the* p–1*'st power of the diagonal ideal), then the* (a,b) *isogeny in question is cyclic.*

(4) *If both* $a \geq 1$ *and* $b \geq 1$, *and if* E_0/S *is ordinary, then the necessary and sufficient condition that the* (a,b) *isogeny in question be cyclic is that the point* $(F^{a-1}(x_0), F^{b-1}(x_n))$ *lie in the* p–1*'st infinitesimal neighborhood of the diagonal.*

(5) *If both* $a \geq 1$ *and* $b \geq 1$, *and if* E_0/S *is ordinary with* $j(E_0)(j(E_0)-1728)$ *invertible on* S, *then the (a,b)* isogeny *in question is cyclic if and only if the* j*-invariants of* E_0 *and* E_n *satisfy the equation*

$$(j(E_0)^{p^{a-1}} - j(E_n)^{p^{b-1}})^{p-1} = 0 .$$

Proof. Assertion (1) is obvious, for by construction $F^a(x_0)$ is the isomorphism class of $(E_0^{(p^a)}, a_a)$, $F^b(x_n)$ is the isomorphism class of $(E_n^{(p^b)}, (\varepsilon^{-1})^*(a_a))$, and ε is an S-isomorphism between them. Assertion (2) is just the fact that F^n and V^n are always cyclic isogenies (12.2.1, 12.2.3). Assertions (3) and (5) both follow from the key assertion (4). Admitting (4) for the moment, let us deduce (3) and (5). To obtain (3), we may reduce to the universal case in which S is the fibre-product

$$\begin{array}{ccc} S & \longrightarrow & \mathrm{Inf}^{p-1}(\Delta) \\ \downarrow & & \downarrow \\ \mathcal{M}(\mathcal{P}) \times \mathcal{M}(\mathcal{P}(\sigma^{a-b})) & \xrightarrow{(F^{a-1}, F^{b-1})} & \mathcal{M}(\mathcal{P}(\sigma^{a-1})) \underset{k}{\times} \mathcal{M}(\mathcal{P}(\sigma^{a-1})) \end{array} .$$

The $\mathcal{M}(\mathcal{P}^{(i)})$ are all smooth curves over k, so the bottom horizontal arrow is finite and flat (of degree p^{a+b-2}). Therefore S is finite flat

over $\mathrm{Inf}^{p-1}(\Delta)$. But $\mathrm{Inf}^{p-1}(\Delta)$ is, by either projection, finite flat over $\mathcal{M}(\mathcal{P}(\sigma^{a-1}))$ of degree $p-1$. Therefore S is finite flat over $\mathcal{M}(\mathcal{P}(\sigma^{a-1}))$. Therefore the open set S^{ord} of S over which E_0 is ordinary is schematically dense in S (because it is the inverse image of the open set $\mathcal{M}(\mathcal{P}(\sigma^{a-1}))^{\mathrm{ord}}$, which is the complement of a finite set of points in a smooth curve). By (4), our isogeny is cyclic over S^{ord}. But the condition that an isogeny be cyclic is represented by a closed subscheme of the base S. This closed subscheme contains S^{ord}, so it must be all of S.

To deduce (5) from (4), we just use the fact that the map

$$\mathcal{M}(\mathcal{P}(\sigma^{a-1})) \xrightarrow{j} \mathrm{Spec}(k[j])$$

is finite etale where $j(j-1728)$ is invertible, and the fact that by (1), the point $(F^{a-1}(x_0), F^{b-1}(x_n))$ certainly lies in $\mathrm{Inf}^{p}(\Delta)$. So if $j(j-1728)$ is invertible, we may test whether or not we actually lie in $\mathrm{Inf}^{p-1}(\Delta)$ by passing to j-invariants.

It remains to prove (4). The individual isogenies

$$E_0 \xrightarrow{F_0^a} E_0^{(p^a)}, \quad E_0^{(p^a)} \simeq E_n^{(p^b)} \xrightarrow{V_n^b} E_n,$$

are certainly cyclic, and the second one is *etale*, because E_0, and hence E_n, are ordinary. Therefore by (6.7.8), their composition is cyclic if and only if it is cyclic in standard order. Therefore our isogeny is cyclic if and only if, when it is written as the standard factorization of F_0^a, followed by the standard factorization of V_n^b, it is cyclic in standard order:

$$E_0 \xrightarrow{F_0} E_0^{(p)} \xrightarrow{F_0^{(p)}} E_0^{(p^2)} \cdots \longrightarrow E_0^{(p^{a-1})} \xrightarrow{F_0^{(p^{a-1})}} E_0^{(p^a)} \longrightarrow \cdots \longrightarrow E_n^{(p^b)}.$$

By (6.7.15), such a composite is cyclic in standard order if and only if each two-step composite is cyclic in standard order. The two-step composites consisting of adjacent F's or of adjacent V's are certainly cyclic in standard order (12.2.4). So the only "weak link" in our chain is the vertically drawn

$$E_0^{(p^{a-1})} \xrightarrow{F_0^{(p^{a-1})}} E_0^{(p^a)} \xrightarrow[\varepsilon]{\sim} E_n^{(p^b)} \xrightarrow{V_n^{(p^{b-1})}} E_n^{(p^{b-1})}.$$

This reduces us to the case $a = b = 1$. We must show that if $E_0/S/k$ is ordinary, and we are given $\alpha_0 \in \mathcal{P}(E_0/S)$, then

$$E_0 \xrightarrow{F_0} E_0^{(p)} \xrightarrow[\varepsilon]{\sim} E_2^{(p)} \xrightarrow{V_2} E_2$$

is cyclic in standard order if and only if (x_0, x_2) lies in $\mathrm{Inf}^{p-1}(\Delta)$ inside $\mathcal{M}(\mathcal{P})^{\mathrm{ord}} \underset{k}{\times} \mathcal{M}(\mathcal{P})^{\mathrm{ord}}$. The universal case of a $(1,1)$ isogeny with $\mathcal{P}$-structure on the (ordinary) source lives over $\mathrm{Inf}^{p}(\Delta)$. We must show that inside this $\mathrm{Inf}^{p}(\Delta)$, the locus of cyclicity is exactly the closed subscheme $\mathrm{Inf}^{p-1}(\Delta)$. It is enough to test the equality of two closed subschemes of a k-scheme of finite type by comparing points with values in artin local k-algebras with algebraically closed residue fields.

Thus we are reduced to the case when S is $\mathrm{Spec}(R)$, with R an artin local k-algebra with algebraically closed residue field. Over the residue field, the points x_0, x_2 simply *coincide*. So we may identify the special fibers of (E_0, α_0) and (E_2, β_2) once and for all, to a fixed (E_{00}, α_{00}). Let us also fix an isomorphism of p-divisible groups

$$E_{00}[p^\infty] \simeq \mu_{p^\infty} \times \mathbf{Q}_p/\mathbf{Z}_p.$$

Then there exist principal units (cf. 8.9)

$$q_0, q_2 \in 1 + \max(R)$$

such that the p-divisible groups of E_0/R and of E_2/R are given by

$$E_0[p^\infty] \simeq T[p^\infty] \underset{Z[q,q^{-1}]}{\otimes} R \quad \text{by} \quad q \mapsto q_0$$

$$E_2[p^\infty] \simeq T[p^\infty] \underset{Z[q,q^{-1}]}{\otimes} R \quad \text{by} \quad q \mapsto q_2 .$$

We are *given*

$$(q_0)^p = (q_2)^p .$$

We must prove that $(q_0 q_2)^{p-1} = 1$ if and only if

$$E_0 \xrightarrow{F_0} E_0^{(p)} = E_2^{(p)} \xrightarrow{V_2} E_2$$

is cyclic in standard order.

To analyze this question, we write the p-divisible groups explicitly. For any R-algebra B, with connected spectrum, $E_0[p^\infty](B)$ is the p-primary torsion subgroup of

$$(B^\times) \times (Z[1/p]) \Big/ \text{the cyclic subgroup generated by } (q_0, 1) ,$$

and similarly for E_2, with q_0 replaced by q_2. The groups for $E_0^{(p)} \simeq E_2^{(p)}$ are formed with q_0 replaced by $(q_0)^p = (q_2)^p$.

The Frobenius

$$F_0 : E_0[p^\infty](B) \to E_0^{(p)}[p^\infty](B)$$

is given by

$$(X, a/p^n) \xmapsto{F_0} (X^p, a/p^n) .$$

The Verschiebung

$$V_2 : E_2^{(p)}[p^\infty](B) \to E_2[p^\infty](B)$$

is given by

$$(X, a/p^n) \xmapsto{V_2} (X, pa/p^n) .$$

We are now in a position to apply the standard order criterion (6.7.13). Over the finite flat R-algebra

$$R' = R[Z]/(Z^p = q_2)$$

the point

$$P = (Z, 1/p) \in E_0[p](R')$$

has

$$F_0(P) = (q_2, 1/p) \in E_2^{(p)}[p](R') ,$$

and this point is visibly a generator of Ker V_2. Therefore our composite $V_2 \circ F_0$ is cyclic in standard order if and only if pP generates Ker F_0. But we readily calculate *in* $E_0[p](R')$

$$p(P) = p(Z, 1/p) = (Z^p, 1) = (q_2, 1) = (q_2/q_0, 0)$$

so our composite is cyclic in standard order if and only if q_2/q_0 *generates* Ker $F_0 \simeq \mu_p$, i.e., if and only if q_2/q_0 is a *primitive* p'th root of unity. In characteristic p,

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = (X-1)^{p-1} ,$$

so

$$\Phi_p(q_2/q_0) = 0 \Longleftrightarrow ((q_2/q_0) - 1)^{p-1} = 0$$

$$\Longleftrightarrow (q_2 - q_0)^{p-1} = 0 . \qquad \text{Q.E.D.}$$

(13.4) *Global structure of the moduli spaces* $\mathfrak{M}(\mathcal{P}, [\Gamma_0(p^n)])$, $\mathfrak{M}(\mathcal{P}, [p^n - \text{Isog}])$

(13.4.1) DEFINITION. Let $E/S/F_p$ be an elliptic curve over an F_p-scheme. Let a, b be two integers, both ≥ 0, with $a+b = n \geq 1$. A finite locally free S-subgroup-scheme $G \subset E$ of rank p^n is said to be an (a,b)-subgroup if the following two conditions are satisfied:

(1) $\mathrm{Ker}\ F^a \subset G$

(2) in the resulting factorization of the isogeny with kernel G as

$$E \xrightarrow{F^a} E^{(p^a)} \xrightarrow{\pi_{a,n}} E_n = E \bmod G\ ,$$

we have $\mathrm{Ker}(\pi^t_{a,n}) = \mathrm{Ker}(F^b_n)$.

(13.4.2) Thus if G is an (a,b) subgroup, then there exists an S-isomorphism $E^{(p^a)} \simeq E_n^{(p^b)}$.

(13.4.3) We say that G is an (a,b)-cyclic group if both conditions 1), 2) above are satisfied, and *either* $a = 0$ *or* $b = 0$, *or* the following condition is satisfied:

(3) the two elliptic curves $E^{(p^{a-1})}, E_n^{(p^{b-1})}$ over S, whose "p'th powers" $E^{(p^a)}$ and $E_n^{(p^b)}$, are S-isomorphic, are themselves "infinitesimally near each other to order $p-1$", in the sense that there exists a closed subscheme of S defined by an ideal whose $p-1$'st power is zero, over which the given isomorphism between $E^{(p^a)}$ and $E_n^{(p^b)}$ is induced by an isomorphism between $E^{(p^{a-1})}$ and $E_n^{(p^{b-1})}$.

PROPOSITION 13.4.4. *Let* k *be a perfect field of characteristic* p, $\mathcal{P}$ *a representable moduli problem on* (Ell/k) *which is finite etale over* (Ell/k). *For any integers* $a \geq 0$, $b \geq 0$ *with* $a+b = n \geq 1$, *the moduli problem on* (Ell/k) *defined by*

$$[\mathcal{P},(a,b)](E/S) = \{\alpha \in \mathcal{P}(E/S),\ \textit{plus an } (a,b)\textit{-subgroup } G \textit{ in } E/S\}$$

is represented by the finite flat $\mathcal{M}(\mathcal{P})$*-scheme of degree* p^b

$$\mathcal{M}(\mathcal{P},(a,b)) = (F^a \times F^b)^{-1}(\Delta)$$

where $F^a \times F^b$ *denotes the map*

$$F^a \times F^b : \mathcal{M}(\mathcal{P}) \times_k \mathcal{M}(\mathcal{P}(\sigma^{a-b})) \to \mathcal{M}(\mathcal{P}(\sigma^a)) \times_k \mathcal{M}(\mathcal{P}(\sigma^a))\ .$$

The projection map

$$\mathcal{M}(\mathcal{P},(a,b)) \downarrow \mathcal{M}(\mathcal{P})$$

is bijective on points with values in any perfect k*-algebra.*

The map "forget (a,b)*"*

$$\mathcal{M}(\mathcal{P},(a,b)) \to \mathcal{M}(\mathcal{P},[p^n\text{-Isog}])$$

is a closed immersion. If $(a,b) = (n,0)$ *or* $(0,n)$, *this map factors through a closed immersion into* $\mathcal{M}(\mathcal{P},[\Gamma_0(p^n)])$.

Proof. The precise description of the (a,b) problem makes clear the explicit description of $\mathcal{M}(\mathcal{P},(a,b))$. That $\mathcal{M}(\mathcal{P},(a,b)) \to \mathcal{M}(\mathcal{P},[p^n\text{-Isog}])$ is a closed immersion is clear from the fact that the (a,b)-condition is a condition on the kernel of a p^n-isogeny, so the (a,b) problem is certainly a sub-problem of $[p^n\text{-Isog}]$. Therefore the map is a monomorphism. It is a closed immersion because it is *proper*, being an $\mathcal{M}(\mathcal{P})$-map between finite flat $\mathcal{M}(\mathcal{P})$-schemes. Q.E.D.

PROPOSITION 13.4.5. *Let* k *be a perfect field of characteristic* p, $\mathcal{P}$ *a representable moduli problem on* (Ell/k) *which is finite etale over* (Ell/k). *For any integers* $a \geq 1$, $b \geq 1$, $a+b = n \geq 2$, *the moduli problem on* (Ell/k) *defined by*

$$[\mathcal{P},(a,b)\text{-cyclic}](E/S) = \{\alpha \in \mathcal{P}(E/S),\ \textit{plus an } (a,b)\textit{-cyclic subgroup } G \textit{ in } E/S\}$$

is represented by the finite flat $\mathcal{M}(\mathcal{P})$*-scheme of degree* $\phi(p^b) = p^{b-1}(p-1)$

$$\mathcal{M}(\mathcal{P},(a,b)\text{-cyclic}) = (F^{a-1} \times F^{b-1})^{-1}(\mathrm{Inf}^{p-1}(\Delta))\ .$$

where $F^{a-1} \times F^{b-1}$ *denotes the map*

$$F^{a-1} \times F^{b-1} : \mathcal{M}(\mathcal{P}) \times \mathcal{M}(\mathcal{P}^{(\sigma^{a-b})}) \to \mathcal{M}(\mathcal{P}^{(\sigma^{a-1})}) \times \mathcal{M}(\mathcal{P}^{(\sigma^{a-1})})$$

The projection map

$$\begin{array}{c} \mathcal{M}(\mathcal{P}, (a,b)\text{-cyclic}) \\ \big\downarrow \\ \mathcal{M}(\mathcal{P}) \end{array}$$

is bijective on points with values in any perfect k*-algebra.*

The map "forget (a,b)" defines a closed immersion

$$\mathcal{M}(\mathcal{P}, (a,b)\text{-cyclic}) \to \mathcal{M}(\mathcal{P}, [\Gamma_0(p^n)]) .$$

Proof. Exactly analogous to the preceding. Q.E.D.

THEOREM 13.4.6. *Let* k *be a perfect field of characteristic* p, $\mathcal{P}$ *a representable moduli problem on* (Ell/k) *which is finite etale over* (Ell/k). *For any integer* $n \geq 1$, *the finite flat* $\mathcal{M}(\mathcal{P})$*-scheme* $\mathcal{M}(\mathcal{P}, [p^n\text{–Isog}])$ *is the disjoint union, with crossings at the supersingular points, (cf. 13.1.7) of the* $n+1$ $\mathcal{M}(\mathcal{P})$*-schemes* $\mathcal{M}(\mathcal{P}, (a,b))$ *for* $a+b = n$, *where*

$$\mathcal{M}(\mathcal{P}, (a,b)) = (F^a \times F^b)^{-1}(\Delta)$$

carries the universal p^n*-isogeny of type* (a,b).

At each k*-rational supersingular point of* $\mathcal{M}(\mathcal{P}, [p^n\text{–Isog}])$, *the complete local ring is isomorphic to*

$$k[[x,y]] / \prod_{a+b=n} (x^{p^a} - y^{p^b}) ,$$

with x *and* y *the local moduli of the source and target. In this complete local ring, the closed subscheme* $\mathcal{M}(\mathcal{P}, (a,b))$ *is defined by the single equation*

$$x^{p^a} = y^{p^b} .$$

Proof. Simply apply the crossing theorem (13.1.3), via (13.2.2), (13.3.3), and (13.4.4). Q.E.D.

THEOREM 13.4.7. *Let* k *be a perfect field of characteristic* p, $\mathcal{P}$ *a representable moduli problem on* (Ell/k) *which is finite etale over* (Ell/k). *For any integer* $n \geq 1$, *the finite flat* $\mathcal{M}(\mathcal{P})$*-scheme* $\mathcal{M}(\mathcal{P}, [\Gamma_0(p^n)] \underset{\mathbf{Z}}{\otimes} k)$ *is the disjoint union, with crossings at the supersingular points, of the* $n+1$ $\mathcal{M}(\mathcal{P})$*-schemes* $\mathcal{M}(\mathcal{P}, (a,b)\text{-cyclic})$ *for* $a+b = n$, *where*

if a,b *both* ≥ 1, $\mathcal{M}(\mathcal{P}, (a,b)\text{-cyclic}) = (F^{a-1} \times F^{b-1})^{-1}(\mathrm{Inf}^{p-1}(\Delta))$ *carries the universal* (a,b)*-cyclic* p^n*-isogeny*

if $a = 0$ *or if* $b = 0$, $\mathcal{M}(\mathcal{P}, (a,b)\text{-cyclic}) = \mathcal{M}(\mathcal{P}, (a,b)) = (F^a \times F^b)^{-1}(\Delta)$ *carries the universal* p^n*-isogeny of type* (a,b), *which for* $a = 0$ *or* $b = 0$ *is automatically cyclic.*

At each k*-rational supersingular point of* $\mathcal{M}(\mathcal{P}, [\Gamma_0(p^n)] \underset{\mathbf{Z}}{\otimes} k)$, *the complete local ring is isomorphic to*

$$k[[x,y]] \Big/ (x - y^{p^n})(x^{p^n} - y) \left(\prod_{\substack{a+b=n \\ a,b \text{ both} \geq 1}} (x^{p^{a-1}} - y^{p^{b-1}})^{p-1} \right)$$

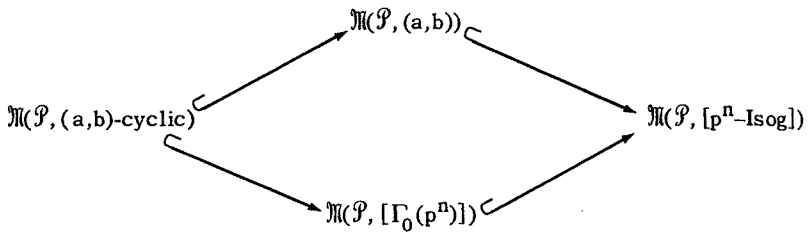
with x *and* y *the local moduli of the source and target.*

In this complete local ring, the closed subscheme $\mathcal{M}(\mathcal{P}, (a,b)\text{-cyclic})$ *is defined by the single equation:*

$$(x^{p^{a-1}} - y^{p^{b-1}})^{p-1} = 0 \quad \text{if} \quad a,b \quad \text{both} \geq 1$$

$$x^{p^a} = y^{p^b} \qquad \text{if} \quad (a,b) = (n,0) \text{ or } (0,n) .$$

A CAUTIONARY REMARK (13.4.8). It is *not* true that a p^n-isogeny which is simultaneously a cyclic isogeny and an (a,b) isogeny is necessarily (a,b)-cyclic, as soon as both a,b are ≥ 1. In other words, if both a,b are ≥ 1, $a+b=n$, the diagram of closed immersions



is *not* cartesian near the supersingular points. This may be seen easily with the explicit forms of the complete local rings we have given above. To give the idea, we write out the case $a=b=1$ explicitly. The assertion there is that the natural map of $k[[x,y]]$ algebras

$$\begin{array}{c} k[[x,y]]\Big/\left(x^p-y^p,(x-y^{p^2})(x^{p^2}-y)(x-y)^{p-1}\right) \\ \downarrow \\ k[[x,y]]/(x-y)^{p-1} \end{array}$$

is not an isomorphism, which is obvious (e.g., for degree reasons, $(x-y)^{p-1}$ is non-zero in the source ring).

In fact, the fiber-product, i.e., the scheme-theoretic intersection

$$\mathcal{M}(\mathcal{P},(a,b)) \cap \mathcal{M}(\mathcal{P},[\Gamma_0(p^n)]), \text{ inside } \mathcal{M}(\mathcal{P},[p^n\text{-Isog}])$$

is *not flat* over $\mathcal{M}(\mathcal{P})$, as soon as a,b are both ≥ 1. For at a supersingular point, the extension of complete local rings is

$$\begin{array}{c} k[[x,y]]\Big/\left(x^{p^a}-y^{p^b},(x^{p^n}-y)(x-y^{p^n})\left(\prod_{\substack{a+b=n \\ a,b\ both\ \geq 1}}(x^{p^{a-1}}-y^{p^{b-1}})^{p-1}\right)\right) \\ \uparrow \\ k[[x]]\,. \end{array}$$

Modulo (x), the upper ring becomes

$$k[[y]]/(y^{p^b},y^M) \text{ with } M = 1+p^n+\sum_{1\leq b\leq n-1}\phi(p^b)$$

i.e., it becomes

$$k[[y]]/(y^{p^b})\,.$$

So if the above scheme-theoretic intersection were finite flat over $\mathcal{M}(\mathcal{P})$, its degree would be p^b. But over $\mathcal{M}(\mathcal{P})^{ord}$, this intersection *is* $\mathcal{M}(\mathcal{P},(a,b)\text{-cyclic})$, which *is* finite flat over $\mathcal{M}(\mathcal{P})$ of degree $\phi(p^b)=p^b-p^{b-1}$.

(13.4.9) *A numerical verification*

Because both $[\Gamma_0(p^n)]$ and $[p^n\text{-Isog}]$ are finite flat over (Ell/**Z**), we can compute their degrees over (Ell/**Z**) by looking "outside p", where we find (compare 6.8.9)

degree of $[\Gamma_0(p^n)]$ over $[\Gamma(1)]$ is the number of cyclic subgroups of order p^n in $(\mathbf{Z}/p^n\mathbf{Z})^2$;

degree of $[p^n\text{-Isog}]$ over $[\Gamma(1)]$ is the number of subgroups of order p^n in $(\mathbf{Z}/p^n\mathbf{Z})^2$, which is

$$\sum_{0\leq d\leq [n/2]} (\text{number of cyclic subgroups of order } p^{n-2d} \text{ in } (\mathbf{Z}/p^{n-2d}\mathbf{Z})^2)\,.$$

The explicit calculation of the special fibers at p of these moduli problems gives

$$\text{degree of } [\Gamma_0(p^n)]\otimes k \text{ over } [\Gamma(1)]\otimes k = 1+p^n+\sum_{\substack{a+b=n \\ a,b\ both\ \geq 1}}\phi(p^b)$$

$$\text{degree of } [p^n\text{-Isog}]\otimes k \text{ over } [\Gamma(1)]\otimes k = 1+p^n+\sum_{\substack{a+b=n \\ a,b\ both\ \geq 1}}p^b\,.$$

We leave to the reader the pleasant a priori verification that these formulas, viewed as formulas for the number of cyclic (resp. arbitrary) subgroups of order p^n in $(\mathbb{Z}/p^n\mathbb{Z})^2$, are in fact correct!

(13.5) *Analysis of* $[\Gamma_1(p^n)]$ *in characteristic* p

PROPOSITION 13.5.1. *Let* E_0, E_n *be elliptic curves over an* $\mathbb{F}_p$*-scheme* S, *and let*

$$\pi_{0,n} : E_0 \to E_n$$

be a cyclic p^n*-isogeny which is* (a,b)*-cyclic for some* $a+b=n$. *Then the corresponding factorization of* $\pi_{0,n}$ *as*

$$E_0 \xrightarrow{F_0^a} E_0^{(p^a)} \xrightarrow{\sim} E_n^{(p^b)} \xrightarrow{V_n^b} E_n$$

is the standard factorization of a cyclic p^n*-isogeny into a cyclic* p^a*-isogeny followed by a cyclic* p^b*-isogeny.*

Proof. We must prove that $\mathrm{Ker}(F_0^a)$ is equal to the *standard* cyclic subgroup of $\mathrm{Ker}(\pi_{0,n})$ of order p^a. The question is f.p.p.f. local on S, so we may rigidify with an auxiliary $\Gamma(\ell)$-structure, say, for ℓ an odd prime different from p. Then we may reduce to the universal case $S = \mathcal{M}([\Gamma(\ell)]\otimes\mathbb{F}_p, (a,b)\text{-cyclic})$, which is finite flat over $\mathcal{M}([\Gamma(\ell)]\otimes\mathbb{F}_p)$. The locus of coincidence of $\mathrm{Ker}(F_0^a)$ with the standard cyclic subgroup of $\mathrm{Ker}(\pi_{0,n})$ is a closed subscheme of S, so it suffices to show it contains the schematically dense open set S^{ord}. This reduces us to the case V_n^b is *etale*, in which case the factorization is automatically standard (cf. 6.7.8). Q.E.D.

COROLLARY 13.5.2. *Hypotheses and notations as in the above proposition, suppose that both* a, b *are* ≥ 1. *Then a point* $P \in E_0(S)$ *generates* $\mathrm{Ker}(\pi_{0,n})$ *if and only if the point*

$$F_0^a(P) \in E_0^{(p^a)}(S) \simeq E_n^{(p^b)}(S)$$

generates $\mathrm{Ker}(V_n^b : E_n^{(p^b)} \to E_n)$.

Proof. Simply apply the Backing-Up Theorem (6.7.11) to the standard factorization of $\pi_{0,n}$ as

$$E_0 \xrightarrow{F_0^a} E_0^{(p^a)} \xrightarrow{\sim} E_n^{(p^b)} \xrightarrow{V_n^b} E_n . \qquad \text{Q.E.D.}$$

COROLLARY 13.5.3. *Let* k *be a perfect field of characteristic* p, $\mathcal{P}$ *a representable moduli problem, finite etale over* (Ell/k). *Then for any integers* a, b *both* ≥ 0, $a+b=n$, *the moduli problem on* (Ell/k) *defined by*

$$(\mathcal{P}, [\Gamma_1(p^n)]\text{-}(a,b)\text{-cyclic})(E/S) = a \in \mathcal{P}(E/S) \text{ plus } P \in E(S) \text{ of "exact order } p^n\text{" which generates an } (a,b)\text{-cyclic subgroup in } E/S$$

is represented by the finite flat $\mathcal{M}(\mathcal{P})$*-scheme* $\mathcal{M}(\mathcal{P}, [\Gamma_1(p^n)]\text{-}(a,b)\text{-cyclic})$ *given below:*

if (a,b) = (n,0)

by the scheme of generators of $\mathrm{Ker}(F_0^n)$, *i.e., by the* $\phi(p^n)$*-'th infinitesimal neighborhood of the zero-section in the universal curve* E_{univ} *over* $\mathcal{M}(\mathcal{P})$. *Zariski locally on* $\mathcal{M}(\mathcal{P})$, *(as soon as we pick a coordinate* X *for the formal group of* E_{univ}*), this is the* $\mathcal{M}(\mathcal{P})$*-scheme*

$$\mathcal{M}(\mathcal{P}) \underset{\mathbb{F}_p}{\otimes} \mathrm{Spec}(\mathbb{F}_p[X]/(X^{\phi(p^n)}))$$

carrying the universal (0,n)*-cyclic isogeny*

$$E_{\mathrm{univ}} \xrightarrow{F^n} E_{\mathrm{univ}}^{(p^n)} ,$$

with generator the point " X *" in the formal group.*

if (a,b) = (0,n)

by $\mathcal{M}(\mathcal{P}^{(\sigma^{-n})}, [\mathrm{Ig}(p^n)])$, *carrying*

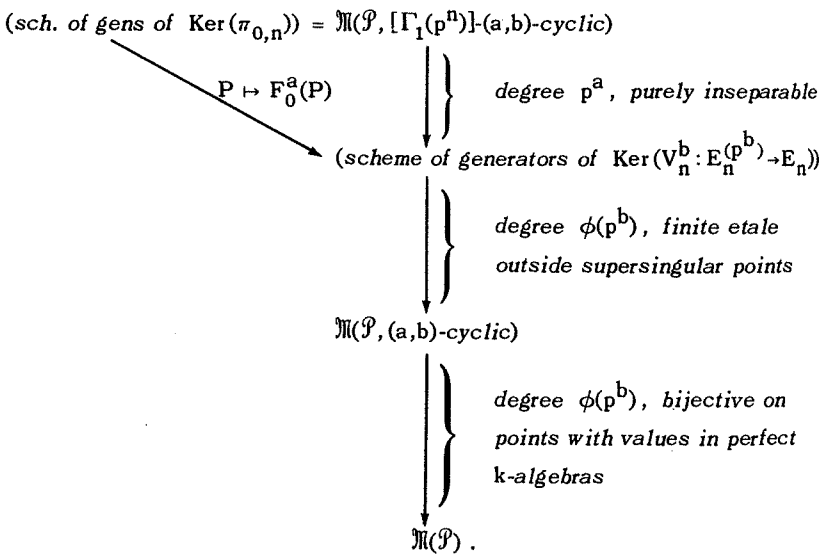
$$E^{(p^n)} \xrightarrow{V^n} E$$

with specified generator $P \in E^{(p^n)}$; *the structure of* $\mathcal{M}(\mathcal{P})$*-scheme is given by the "exotic" projection* pr_n *of total degree* $p^n\phi(p^n)$ *(cf. 12.10.6) or equivalently, by the* $\mathcal{M}(\mathcal{P})$*-scheme*

$$\mathcal{M}(\mathcal{P}, [\mathrm{ExIg}\,(p^n, n)]) \qquad \textit{(cf. 12.10.5.1).}$$

if both $a,b \geq 1$

by the finite flat $\mathcal{M}(\mathcal{P}, (a,b)$*-cyclic)-scheme of generators of the kernel of the universal* (a,b)*-cyclic* p^n*-isogeny. This is fibred over* $\mathcal{M}(\mathcal{P})$ *as a composite of finite flat maps:*



Proof. This is just a modular spelling out of the previous corollary. Q.E.D.

THEOREM 13.5.4. *Let* k *be a perfect field of characteristic* p, $\mathcal{P}$ *a representable problem which is finite etale over* (Ell/k). *Then the moduli scheme* $\mathcal{M}(\mathcal{P}, [\Gamma_1(p^n)] \underset{\mathbf{Z}}{\otimes} k)$ *is the disjoint union, with crossings at the supersingular points, of the* $n+1$ $\mathcal{M}(\mathcal{P})$*-schemes*

$$\mathcal{M}(\mathcal{P}, [\Gamma_1(p^n)]\text{-}(a,b)\text{-cyclic}), \quad \textit{for} \quad a+b=n\,.$$

Proof. Apply the crossings theorem (13.1.3). Q.E.D.

(13.5.6) Summarizing table

In the table below, $\mathcal{P}$ is a representable problem on (Ell/k), finite etale over (Ell/k), with k a perfect field. For both $[\Gamma_0(p^n)]$ and $[\Gamma_1(p^n)]$, we have found expressions for the corresponding $\mathcal{P}$-rigidified modular schemes as disjoint unions of $n+1$ curves (indexed by (a,b) with $a+b=n$) with crossings at the supersingular points. The *multiplicities* given are most easily calculated locally etale on $\mathcal{M}(\mathcal{P})^{\mathrm{ord}}$, and the formulas in the table may be checked against the computations of the section which follows.

SHORT TABLE: $\Gamma_0(p^n)$ and $\Gamma_1(p^n)$ in char p

	$\mathcal{M}(\mathcal{P}, [\Gamma_0(p^n)] \otimes k)$	$\mathcal{M}(\mathcal{P}, [\Gamma_1(p^n)] \otimes k)$
(n,0)-component degree over $\mathcal{M}(\mathcal{P})$	1	$\phi(p^n)$
multiplicity as abstract curve	1	$\phi(p^n)$
underlying abstract reduced curve, and its degree over $\mathcal{M}(\mathcal{P})$	$\mathcal{M}(\mathcal{P})$; 1	$\mathcal{M}(\mathcal{P})$; 1
(0,n)-component degree over $\mathcal{M}(\mathcal{P})$	p^n	$p^n\phi(p^n)$
multiplicity as abstract curve	1	1
underlying abstract reduced curve, and its degree over $\mathcal{M}(\mathcal{P})$	$\mathcal{M}(\mathcal{P})^{(\sigma^{-n})}$ via (E_n, β_n) degree p^n	$\mathcal{M}(\mathcal{P}, [\mathrm{ExIg}\,(p^n, n)])$ degree $p^n\phi(p^n)$
(a,b)-component with a,b both ≥ 1 degree over $\mathcal{M}(\mathcal{P})$	$\phi(p^b)$	$\phi(p^n)\phi(p^b)$
multiplicity as abstract curve	$\phi(p^{\min(a,b)})$	$\phi(p^a)$
underlying abstract reduced curve, and its degree over $\mathcal{M}(\mathcal{P})$.	if $a \geq b$, $\mathcal{M}(\mathcal{P})$, degree 1 if $a \leq b$, $\mathcal{M}(\mathcal{P})^{(\sigma^{a-b})}$, degree p^{b-a}	$\mathcal{M}(\mathcal{P}, [\mathrm{ExIg}\,(p^b, b)])$ degree $p^b\phi(p^b)$

(13.6) *Explicit calculations via the groups* $T[p^n]$ *of* $[\Gamma_0(p^n)], [\Gamma_1(p^n)]$

(13.6.1) In the previous section we gave a calculation of the moduli scheme $\mathcal{M}(\mathcal{P}, [\Gamma_0(p^n)])$ and $\mathcal{M}(\mathcal{P}, [\Gamma_1(p^n)])$ as $\mathcal{M}(\mathcal{P})$-schemes, with particular attention to their behavior at the supersingular points. In this section we will analyse what these $\mathcal{M}(\mathcal{P})$-schemes look like locally (etale) on $\mathcal{M}(\mathcal{P})^{ord}$. We have already seen that the covering

$$\begin{array}{c} \mathcal{M}(\mathcal{P}, [\mathrm{Ig}(p^n)])^{ord} \\ \downarrow \\ \mathcal{M}(\mathcal{P})^{ord} \end{array}$$

is a finite etale $(\mathbf{Z}/p^n\mathbf{Z})^\times$-torsor (cf. 12.6.1). Over this covering, the universal E has $E[p^n]$ sitting in a short exact sequence

$$0 \to \mu_{p^n} \to E[p^n] \to \mathbf{Z}/p^n\mathbf{Z} \to 0$$

for which the e_{p^n}-pairing is equal to the unique strongly alternating pairing making μ_{p^n} and $\mathbf{Z}/p^n\mathbf{Z}$ Cartier dual in the standard way (cf. 8.10.6). Therefore *Zariski locally* on $\mathcal{M}(\mathcal{P}, [\mathrm{Ig}(p^n)])^{ord}$, there exists a unit $q \in G_m(\mathcal{M}(\mathcal{P}, [\mathrm{Ig}(p^n)])^{ord})$ such that $E[p^n]$, in its exact sequence above, is pulled back via q from the group $T[p^n]$ over $G_m = \mathrm{Spec}(\mathbf{Z}[q,q^{-1}])$, sitting in its exact sequence

$$0 \to \mu_{p^n} \to T[p^n] \to \mathbf{Z}/p^n\mathbf{Z} \to 0 .$$

In fact, it is a simple matter to compute the $\mathbf{Z}[q,q^{-1}]$-schemes

$$[\Gamma_0(p^n)]_{T[p^n]/\mathbf{Z}[q,q^{-1}]}, \quad [\Gamma_1(p^n)]_{T[p^n]/\mathbf{Z}[q,q^{-1}]} .$$

PROPOSITION 13.6.2. *Let* S *be a connected* $\mathbf{Z}[q,q^{-1}]$*-scheme,* $G \subset T[p^n] \otimes S$ *a finite locally free subgroup of rank* p^n. *Then there exist unique integers* a,b *both* ≥ 0, $a+b=n$, *such that*

$$G \cap \mu_{p^n} = \mu_{p^a}$$

$$G \bmod \mu_{p^a} \xrightarrow{\sim} \mathbf{Z}/p^b\mathbf{Z}$$

and we have a commutative diagram of short exact sequences of S*-group-schemes*

$$\begin{array}{ccccccccc} 0 & \to & \mu_{p^a} & \to & G & \to & \frac{1}{p^b}\mathbf{Z}/\mathbf{Z} & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \mu_{p^n} & \to & T[p^n] & \to & \frac{1}{p^n}\mathbf{Z}/\mathbf{Z} & \to & 0 . \end{array}$$

Proof. Simply apply (4.10.1) to the composite map

$$\begin{array}{ccc} G & & \\ \downarrow & \searrow & \\ T[p^n] & \to & \frac{1}{p^n}\mathbf{Z}/\mathbf{Z} , \end{array}$$

exactly as in the proof of (13.3.2). Q.E.D.

PROPOSITION 13.6.3. *Let* S *be a* $\mathbf{Z}[q,q^{-1}]$*-scheme,* $G \subset T[p^n] \otimes S$ *a finite locally free subgroup of rank* p^n *and type* (a,b) *in the sense of the preceding proposition. Let* $P \in G(S)$ *be a point whose image in* $\frac{1}{p^n}\mathbf{Z}/\mathbf{Z}$ *is* $1/p^b$. *Then*

(1) G *is cyclic, with generator* P, *if and only if* $p^bP \in \mu_{p^a}(S)$ *is a primitive* p^a'th *root of unity.*

(2) *if* Q *is any point in* $T[p^n](S)$ *which projects onto* λ/p^b *in* $(1/p^n)\mathbf{Z}/\mathbf{Z}$, *for some* $\lambda \in (\mathbf{Z}/p^b\mathbf{Z})^\times$, *then* Q *has "exact order* p^n*" if and only if* $p^bQ \in \mu_{p^n}(S)$ *is a primitive* p^a'th *root of unity.*

Proof. First we recall that $T[p^n]$ is embedded as a closed subgroup-scheme of $G_m \times \frac{1}{p^n}\mathbf{Z}/\mathbf{Z}$ for its group-structure (8.7.2.3), so by (1.10.6) it makes intrinsic sense to speak of a point Q as having "exact order p^n", and to speak of the cyclic group of rank p^n that Q generates. We have seen that after a faithfully flat extension, $T[p^n]$ is isomorphic to the kernel of multiplication by p^n in an elliptic curve. This allows us to apply the detailed theory of cyclicity developed in Chapter 6 to $T[p^n]$.

If $b = 0$, there is nothing to prove for (1). G is the subgroup μ_{p^n}. For (2), if $Q \in \mu_{p^n}(S)$ has "exact order p^n" in $T[N]$, then the cyclic p^n-group it generates lies entirely inside $G_m \times \{0\}$ [viewing it as a Cartier divisor inside $G_m \times ((1/p^n)\mathbf{Z}/\mathbf{Z})$]. Therefore it lies inside $\mu_{p^n} = T[p^n] \cap (G_m \times \{0\})$, so must *be* μ_{p^n}. Therefore Q is necessarily a primitive p^n'th root of unity, if it lies in $\mu_{p^n}(S)$ and has "exact order p^n" in $T[p^n]$.

If $a = 0$, then G is the $\mathbf{Z}/p^n\mathbf{Z}$ generated by P, and Q generates a $\mathbf{Z}/p^n\mathbf{Z}$.

If both $a,b \geq 1$, then (1) and (2) follow from the standard order criterion (6.7.13), which automatically applies by (6.7.8). Q.E.D.

We now use the explicit form of the group $T[p^n]$. Let Q be a point in some $T[p^n](S)$ whose second coordinate is λ/p^b for some $\lambda \in (\mathbf{Z}/p^b\mathbf{Z})^\times$, normalized by $0 \leq \lambda < p^b$, say

$$Q = (X, \lambda/p^b)$$

in the standard coordinates (8.7.1.2). Then

$$p^b Q = (X^{p^b}, \lambda) \sim (X^{p^b}/q^\lambda, 0)$$

and the requirement is that

$$X^{p^b}/q^\lambda$$

be a primitive p^a'th root of unity, where $a+b = n$.

In terms of the cyclotomic polynomials, this is the condition

$$\Phi_{p^a}(X^{p^b}/q^\lambda) = 0 .$$

Thus we find

THEOREM 13.6.4. *For any* $n \geq 1$, *and any connected* $\mathbf{Z}[q,q^{-1}]$*-algebra* B, *we have a canonical isomorphism of* B*-schemes*

$$[\Gamma_1(p^n)]_{T[p^n]/B} \simeq \coprod_{\substack{0\leq b\leq n \\ a+b=n}} \coprod_{\substack{0\leq\lambda<p^b \\ (\lambda,p^b)=1}} \mathrm{Spec}\,(B[X]/\Phi_{p^a}(X^{p^b}/q^\lambda))$$

(13.6.5) Consider now a cyclic p^n-subgroup G of $T[N]$ over some connected $\mathbf{Z}[q,q^{-1}]$ scheme S, which is of type (a,b). If $a = n$, our group G is μ_{p^n}. If $a = 0$, then $b = n$ and our group contains a *unique* element of the form

$$(X, 1/p^n) .$$

This element generates it.

If both $a,b \geq 1$, then after passing to a finite locally free covering S' of S, G admits a generator of the form

$$(X, 1/p^b) .$$

The exact sequence

$$0 \to \mu_{p^a} \to G \to \left(\frac{1}{p^b}\right)\mathbf{Z}/\mathbf{Z} \to 0$$

shows that the X above is unique up to multiplication by an element of μ_{p^a}. Therefore by f.p.p.f. descent we have

$$X^{p^a} \in \Gamma(S, \mathcal{O}_S) .$$

We will now see that we can write the equation for G using X^{p^a}.

Consider any connected S-scheme S'', and any element

$$(Y, \lambda/p^b) \in G(S''), \quad 0 \leq \lambda < p^b .$$

The "difference"

$$(Y, \lambda/p^b) - \lambda(X, 1/p^b) = (Y/X^\lambda, 0)$$

lies in G and has second coordinate zero, so it must lie in μ_{p^a}. Conversely, $\mu_{p^a} \subset G$, and $\lambda(X, 1/p^b) \in G(S)$, so we conclude that

$$G(S'') = \{(Y, \lambda/p^b) \text{ with } Y^{p^a} = (X^{p^a})^\lambda\} .$$

Recall that X itself is required to satisfy

$$\Phi_{p^a}(X^{p^b}/q) = 0$$

if the point $(X, 1/p^b)$ is to have "exact order p^n." For $a \geq 1$, $b \geq 1$, we may write this

$$0 = \Phi_{p^a}(X^{p^b}/q) = \Phi_p(X^{p^{a+b-1}}/q^{p^{a-1}}) = \Phi_p((X^{p^a})^{p^{b-1}}/q^{p^{a-1}}) .$$

If we call the quantity X^{p^a} "Z", then we have a bijective correspondence over any $Z[q,q^{-1}]$-scheme S,

$$\begin{pmatrix} p^n\text{-cyclic subgroups } G \\ \text{of } T[p^n] \text{ of type } (a,b) \\ \text{with } a,b \text{ both } \geq 1, \end{pmatrix} \leftrightarrow \begin{pmatrix} \text{elements } Z \in \Gamma(S, \mathcal{O}_S) \\ \text{with} \\ \Phi_p(Z^{p^{b-1}}/q^{p^{a-1}}) = 0 . \end{pmatrix}$$

$$G_Z \leftrightarrow Z$$

where for any connected S-scheme S'',

$$G_Z(S'') = \left\{ \begin{array}{c} (Y, \lambda/p^b) \text{ with } 0 \leq \lambda < p^b, Y \in G_m(S'') \\ \text{and } Y^{p^a} = Z^\lambda \end{array} \right\} .$$

Putting this all together, we find

THEOREM 13.6.6. *For any* $n \geq 1$, *and any connected* $Z[q,q^{-1}]$*-algebra* B, *we have a canonical isomorphism of* B*-schemes*

$$[\Gamma_0(p^n)]_{T[p^n]/B} \simeq \text{Spec}(B) \coprod \text{Spec}(B[X]/(X^{p^n} - q)) \coprod \coprod_{\substack{a+b=n \\ a,b \text{ both } \geq 1}} \left(\text{Spec}(B[Z]/\Phi_p(Z^{p^{b-1}}/q^{p^{a-1}})) \right) .$$

If B is an $F_p[q,q^{-1}]$-algebra, these expressions "simplify," because in $F_p[X]$ we have, for all $a \geq 1$, the identity

$$\Phi_{p^a}(X) = (X-1)^{\phi(p^a)} .$$

THEOREM 13.6.7. *If* B *is any connected* $F_p[q,q^{-1}]$*-algebra, we have canonical isomorphisms of* B*-schemes for any* $n \geq 1$

$$[\Gamma_1(p^n)]_{T[p^n]/B} = \left\{ \begin{array}{l} \coprod_{\substack{0 \leq b \leq n-1 \\ a+b=n}} \coprod_{\substack{0 \leq \lambda < p^b \\ (\lambda, p^b)=1}} \text{Spec}(B[X]/(X^{p^b} - q^\lambda)^{\phi(p^a)}) \coprod \\ \coprod_{\text{the term } b=n} \left(\coprod_{\substack{0 < \lambda < p^n \\ (\lambda, p)=1}} \text{Spec}(B[X]/(X^{p^n} - q^\lambda)) \right) \end{array} \right. .$$

$$[\Gamma_0(p^n)]_{T[p^n]/B} = \left\{ \begin{array}{l} \text{Spec}(B) \coprod \text{Spec}(B[X]/(X^{p^n} - q)) \coprod \\ \left(\coprod_{\substack{a+b=n \\ a \geq 1, b \geq 1}} \text{Spec}(B[Z]/(Z^{p^{b-1}} - q^{p^{a-1}})^{p-1}) \right) \end{array} \right. .$$

(13.7) *The reduction* mod p *of* $[\Gamma(p^n)]^{can}$

(13.7.1) Let k be a field of characteristic p. For every integer $n \geq 1$, there is a unique ring homomorphism

$$\mathbf{Z}[\zeta_{p^n}] \to k$$

namely

$$\zeta_{p^n} \mapsto 1 .$$

Therefore the moduli problem

$$[\Gamma(p^n)]^{can} \underset{\mathbf{Z}[\zeta_{p^n}]}{\otimes} k \quad \text{on} \quad (\text{Ell}/k)$$

is given by

$$E/S \mapsto \begin{matrix}\text{Drinfeld } p^n\text{-bases } (P,Q) \\ \text{of } E/S \text{ with } e_{p^n}(P,Q)=1 .\end{matrix}$$

We will denote this moduli problem

$$[\Gamma(p^n);\ \det=1] .$$

Just as in Chapter 10, we will view such a structure on an E/S as a "$(\mathbf{Z}/p^n\mathbf{Z})^2$-generator" of $E[p^n]$, of determinant one, written

$$\phi : (\mathbf{Z}/p^n\mathbf{Z})^2 \to E[p^n] .$$

Notice that the *entire* group $GL(2, \mathbf{Z}/p^n\mathbf{Z})$ operates on the right $(\phi \mapsto \phi \circ g)$ on the moduli problem

$$[\Gamma(p^n);\ \det=1] .$$

PROPOSITION 13.7.2. *Let* $E/S/\mathbf{F}_p$ *be an ordinary elliptic curve over a connected* $\mathbf{F}_p$*-scheme,* $n \geq 1$ *an integer, and*

$$\phi : (\mathbf{Z}/p^n\mathbf{Z})^2 \to E[p^n]$$

a $[\Gamma(p^n)]$*-structure on* E/S. *Then*

(1) *The composite map* $\Lambda = F^n \circ \phi$

$$\begin{array}{ccccccccc} & & & & (\mathbf{Z}/p^n\mathbf{Z})^2 & & & & \\ & & & & \downarrow \phi \quad \searrow \Lambda & & & & \\ 0 & \longrightarrow & \text{Ker } F^n & \longrightarrow & E[p^n] & \xrightarrow{F^n} & \text{Ker}(V^n) & \longrightarrow & 0 \end{array}$$

is surjective, its kernel is a constant subgroup of $(\mathbf{Z}/p^n\mathbf{Z})^2$ *which is cyclic of order* p^n, *and the quotient*

$$\text{Quot}(\Lambda) \overset{\text{dfn}}{=\!=} (\mathbf{Z}/p^n\mathbf{Z})^2/\text{Ker}(\Lambda)$$

is a cyclic group of order p^n.

(2) *We have a commutative diagram of short exact sequences of S-group-schemes*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \text{Ker}(\Lambda) & \longrightarrow & (\mathbf{Z}/p^n\mathbf{Z})^2 & \longrightarrow & \text{Quot}(\Lambda) & \longrightarrow & 0 \\ & & \downarrow \phi|\text{Ker}(\Lambda) & & \downarrow \phi & \searrow \Lambda & \| & & \\ 0 & \longrightarrow & \text{Ker}(F^n) & \longrightarrow & E[p^n] & \longrightarrow & \text{Ker}(V^n) & \longrightarrow & 0 \end{array}$$

in which all the vertical arrows are generators.

(3) *Any choice of a* $\mathbf{Z}/p^n\mathbf{Z}$*-basis of* Quot(Λ) *defines an isomorphism* $\mathbf{Z}/p^n\mathbf{Z} \xrightarrow{\sim} \text{Ker}(V^n)$, *which allows us to view* Λ *as a surjective hom from* $(\mathbf{Z}/p^n\mathbf{Z})^2$ *to* $\mathbf{Z}/p^n\mathbf{Z}$. *The class of* Λ *in the space*

$$(\mathbf{Z}/p^n\mathbf{Z})^\times \backslash \text{Hom Surj}((\mathbf{Z}/p^n\mathbf{Z})^2, \mathbf{Z}/p^n\mathbf{Z}))$$

of component labels (10.6) for the trivial subgroup $\{1\} \subset GL(2, \mathbf{Z}/p^n\mathbf{Z})$ *is well-defined independent of choice of basis for* Quot(Λ). *We will refer to this class as the component-label of the* $[\Gamma(p^n)]$*-structure in question.*

(4) *The* $[\Gamma(p^n)]$*-structure* ϕ *has determinant one, i.e., satisfies*

$$e_{p^n}\left(\phi\begin{pmatrix}1\\0\end{pmatrix}, \phi\begin{pmatrix}0\\1\end{pmatrix}\right) = 1 ,$$

if and only if $\phi|\mathrm{Ker}(\Lambda)$ *is the zero-homomorphism.*

Proof. Assertions (1), (2), and (3) follow immediately from (1.11.2), because by hypothesis E/S is ordinary, so $\mathrm{Ker}(V^n)$ is etale over S, locally (etale) on S isomorphic to $\mathbf{Z}/p^n\mathbf{Z}$. To prove (4), we argue as follows. Choose a $\mathbf{Z}/p^n\mathbf{Z}$-basis k_Λ of $\mathrm{Ker}(\Lambda)$, and extend it to an oriented basis $(k_\Lambda, \ell_\Lambda)$ of $(\mathbf{Z}/p^n\mathbf{Z})^2$. Then ℓ_Λ projects to a $\mathbf{Z}/p^n\mathbf{Z}$-basis of $\mathrm{Quot}(\Lambda)$, and $\Lambda(\ell_\Lambda)$ defines an isomorphism $\mathbf{Z}/p^n\mathbf{Z} \xrightarrow{\sim} \mathrm{Ker}(V^n)$. The dual isomorphism

$$\mathrm{Ker}(F^n) \xrightarrow{\sim} \mu_{p^n}$$

is defined by

$$\zeta \in \mathrm{Ker}\, F^n \mapsto e_{p^n}(\zeta, \phi(\ell_\Lambda)) .$$

Now $\phi|\mathrm{Ker}(\Lambda)$ is the zero-homomorphism if and only if $\phi(k_\Lambda)$ is the zero-section of $\mathrm{Ker}\, F^n$. Using the above isomorphism we have

$$\phi(k_\Lambda) = 0 \Longleftrightarrow e_{p^n}(\phi(k_\Lambda), \phi(\ell_\Lambda)) = 1 \Longleftrightarrow \det \phi = 1 . \qquad \text{Q.E.D.}$$

(13.7.3) For each element Λ in

$$(\mathbf{Z}/p^n\mathbf{Z})^\times \backslash \mathrm{Hom\ Surj}\,((\mathbf{Z}/p^n\mathbf{Z})^2, \mathbf{Z}/p^n\mathbf{Z}) ,$$

the space of component-labels, we now *fix* a choice of oriented basis $(k_\Lambda, \ell_\Lambda)$ of $(\mathbf{Z}/p^n\mathbf{Z})^2$ such that k_Λ is a $\mathbf{Z}/p^n\mathbf{Z}$-basis of $\mathrm{Ker}(\Lambda)$.

COROLLARY 13.7.4. *Let* $E/S/\mathbf{F}_p$ *be an ordinary elliptic curve over a connected* $\mathbf{F}_p$*-scheme, and let* ϕ *be a* $[\Gamma(p^n); \det = 1]$*-structure on* E/S*, of component-label* Λ*. Then*

(1) *The point* $\phi(\ell_\Lambda) \in E(S)$ *is an* $[\mathrm{ExIg}(p^n,n)]$*-structure (12.10.5.1) on* E/S*, i.e.,* $(0, \phi(\ell_\Lambda))$ *is a Drinfeld* p^n*-basis on* E/S.

(2) *Given a point* $P \in E(S)$ *such that* (O,P) *is a Drinfeld* p^n*-basis of* E/S*, the homomorphism of S-group-schemes*

$$(\mathbf{Z}/p^n\mathbf{Z})^2 \to E[p^n]$$
$$k_\Lambda \mapsto 0$$
$$\ell_\Lambda \mapsto P$$

is a $[\Gamma(p^n); \det = 1]$*-structure on* E/S.

Proof. We have $\phi(k_\Lambda) = 0$. Q.E.D.

PROPOSITION 13.7.5. *Let* $E/S/\mathbf{F}_p$ *be an elliptic curve,* $\Lambda \in (\mathbf{Z}/p^n\mathbf{Z})^\times \backslash \mathrm{Hom\ Surj}$ *a component-label, and* (O,P) *a Drinfeld* p^n*-basis of* E/S*. Then the homomorphism of S-group-schemes*

$$(\mathbf{Z}/p^n\mathbf{Z})^2 \to E[p^n]$$
$$k_\Lambda \mapsto 0$$
$$\ell_\Lambda \mapsto P$$

is a Drinfeld p^n*-structure on* E/S*, and this construction establishes a functorial bijection*

$$\left\{\begin{array}{c}[\Gamma(p^n)]\text{-structures on } E/S \text{ with}\\ \phi|\mathrm{Ker}(\Lambda) = 0\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}[\mathrm{ExIg}(p^n,n)]\text{-structures}\\ \text{on } E/S\end{array}\right\}.$$

Proof. A tautology! Q.E.D.

THEOREM 13.7.6. *Let* k *be a perfect field of characteristic* p, $\mathcal{P}$ *a representable moduli problem on* (Ell/k) *which is finite etale over* (Ell/k). *Then*

(1) *The* $\mathcal{M}(\mathcal{P})$*-scheme* $\mathcal{M}(\mathcal{P}, [\Gamma(p^n); \det=1])$ *is the disjoint union, with crossings at the supersingular points, of the* $\mathcal{M}(\mathcal{P})$*-schemes*

$$\mathcal{M}(\mathcal{P}, [\Gamma(p^n)\text{str. } \textit{with } \phi(\operatorname{Ker}\Lambda)=0]) \simeq \mathcal{M}(\mathcal{P}, [\operatorname{ExIg}(p^n,n)]) \simeq \mathcal{M}(\mathcal{P}^{(\sigma^{-n})}, [\operatorname{Ig}(p^n)]) \textit{ via } \mathrm{pr}_n$$

indexed by

$$(\mathbf{Z}/p^n\mathbf{Z})^\times \backslash \operatorname{Hom}\operatorname{Surj}((\mathbf{Z}/p^n\mathbf{Z})^2, \mathbf{Z}/p^n\mathbf{Z}) .$$

(2) *These are all smooth curves over* k, *finite and flat over* $\mathcal{M}(\mathcal{P})$ *of degree* $p^n\phi(p^n)$. *If* $\mathcal{M}(\mathcal{P})$ *is connected (resp. geometrically connected), so are the curves* $\mathcal{M}(\mathcal{P}, [\operatorname{ExIg}(p^n,n)])$.

(3) *The compactified moduli scheme* $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma(p^n); \det=1])$, *viewed as an* $\overline{\mathcal{M}}(\mathcal{P})$*-scheme, is the disjoint union, with crossings at the supersingular points, of the compactified moduli schemes*

$$\overline{\mathcal{M}}(\mathcal{P}, [\Gamma(p^n)\text{-str. } \textit{with } \phi(\ker\Lambda)=0]) \simeq \overline{\mathcal{M}}(\mathcal{P}, [\operatorname{ExIg}(p^n,n)]) \simeq \overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-n})}, [\operatorname{Ig}(p^n)]) \textit{ via } \mathrm{pr}_n$$

indexed by

$$(\mathbf{Z}/p^n\mathbf{Z})^\times \backslash \operatorname{Hom}\operatorname{Surj} .$$

Proof. A straightforward application of the crossings theorem (13.1.3) gives (1). Assertion (2) has already been proven (12.6.2). For (3), we argue as follows. Because the component curves are all smooth over k, and finite over $\mathcal{M}(\mathcal{P})$, which is itself finite over the j-line, over the open set of the j-line where $\Phi^{s.s.}$ is invertible, we have $\mathcal{M}(\mathcal{P}, [\Gamma(p^n); \det=1])$ as a disjoint union of Igusa curves. Normalizing a neighborhood of infinity in the j-line now gives the assertion. Q.E.D.

(13.8) *Complete local ring of* $[\Gamma(p^n)]^{\mathrm{can}}$, $n \geq 1$, *at supersingular points; intersection numbers*

(13.8.1) We begin by choosing a convenient set of representatives in

$$\operatorname{Hom}\operatorname{Surj}((\mathbf{Z}/p^n\mathbf{Z})^2, \mathbf{Z}/p^n\mathbf{Z})$$

for the elements of

$$(\mathbf{Z}/p^n\mathbf{Z})^\times \backslash \operatorname{Hom}\operatorname{Surj} .$$

We view elements of Hom Surj as primitive vectors (x,y) with $x,y \in \mathbf{Z}/p^n\mathbf{Z}$, and at least one of x,y a unit. Then a set of representatives modulo the action of $(\mathbf{Z}/p^n\mathbf{Z})^\times$ is provided by the vectors

$$\begin{cases} (1,-a) & a \in \mathbf{Z}/p^n\mathbf{Z} \text{ arbitrary} \\ (-pb,1) & b \in \mathbf{Z}/p^{n-1}\mathbf{Z} \text{ arbitrary.} \end{cases}$$

(13.8.2) With the notations and hypotheses of the previous theorem (13.7.6), let $(E/k, \alpha \in \mathcal{P}(E/k))$ be a supersingular point y_0 on $\mathcal{M}(\mathcal{P})$. In terms of the universal formal deformation $E/k[[T]]$ of E/k (to artin local k-algebras with residue field k), we know that the complete local ring of $\mathcal{M}(\mathcal{P})$ at y_0 is $k[[T]]$. Choose a parameter X for the formal group of $E/k[[T]]$. Then the complete local ring of $\mathcal{M}(\mathcal{P}, [\Gamma(p^n); \det=1])$ at the unique point lying over y_0 is of the form

$$k[[x,y]]/(\text{one equation } f)$$

where $x = X(P)$ and $y = X(Q)$ are the X-coordinates of the points (P,Q) of the universal Drinfeld p^n-basis of det=1, (cf. the proof of (13.2.2), and (5.4)).

(13.8.3) The condition on the Drinfeld p^n-basis (P,Q) that the corresponding ϕ satisfy $\phi(\operatorname{Ker}\Lambda) = 0$ is visibly

$$(13.8.3.1) \qquad \begin{cases} P = aQ & \text{if } \Lambda \sim (1,-a) \\ pbP = Q & \text{if } \Lambda \sim (-pb,1) . \end{cases}$$

Let us denote, for any $a \in \mathbf{Z}_p$, the series

$$[a](X) \in k[[T]][[X]]$$

(13.8.3.2)

$$[a](X) = aX + \text{higher terms}$$

giving "multiplication by a" on the formal group of $E/k[[T]]$. If for each element $a \in \mathbf{Z}/p^n\mathbf{Z}$, and for each $b \in \mathbf{Z}/p^{n-1}\mathbf{Z}$, we choose representatives $\tilde{a},\tilde{b} \in \mathbf{Z}_p$, then we may rewrite the above conditions in terms of x,y as

(13.8.3.3)
$$\begin{cases} x = [\tilde{a}](y) & \text{if} \quad \Lambda \sim (1,-a) \\ y = [p\tilde{b}](x) & \text{if} \quad \Lambda \sim (-pb,1)\,. \end{cases}$$

THEOREM 13.8.4. *Hypotheses and notations as in (13.7.6) and (13.8.2) above, suppose that y_0 is a k-rational supersingular point on $\mathcal{M}(\mathcal{P})$. Choose a ring homomorphism $k[[T]] \to k[[x,y]]$ lifting the given $k[[T]] \to k[[x,y]]/(f)$, so that by extension of scalars the formal group law of $E/k[[T]]$ with respect to the parameter X gives rise to a formal group law over $k[[x,y]]$. In terms of this formal group law over $k[[x,y]]$, the complete local ring of $\mathcal{M}(\mathcal{P}, [\Gamma(p^n); \det = 1])$, $n \geq 1$, at the unique point lying over y_0 is isomorphic to*

$$k[[x,y]] \Big/ \left(\prod_{a \in \mathbf{Z}/p^n\mathbf{Z}} (x - [\tilde{a}](y)) \prod_{b \in \mathbf{Z}/p^{n-1}\mathbf{Z}} (y - [p\tilde{b}](x)) \right).$$

In this complete local ring, the closed subscheme $\mathcal{M}(\mathcal{P}, [\Gamma(p^n)\text{-str. with } \phi(\operatorname{Ker}\Lambda) = 0])$ (cf. 13.7.6) is defined by the single equation

$$\begin{cases} x = [\tilde{a}]y & \text{if} \quad \Lambda \sim (1,-a) \\ y = [p\tilde{b}]x & \text{if} \quad \Lambda \sim (-pb,1)\,. \end{cases}$$

In particular, $\mathcal{M}(\mathcal{P}, [\Gamma(p^n); \det = 1])$ is reduced, even at the supersingular points.

Proof. We know this local ring is of the form

$$k[[x,y]]/(f)\,,$$

with f a non-zero non-unit, and that for each component-label Λ, the corresponding closed subscheme has complete local ring

$$\begin{cases} k[[x,y]]/(f, x - [\tilde{a}](y)) & \text{if} \quad \Lambda \sim (1,-a)\,, \\ k[[x,y]]/(f, y - [p\tilde{b}](x)) & \text{if} \quad \Lambda \sim (-pb,1)\,. \end{cases}$$

But the Λ-components are themselves Igusa curves, and at their supersingular points the respective quantities y,x above are parameters (cf. the proof of (12.6.1)). Therefore in the two cases we have isomorphisms

$$\begin{cases} k[[x,y]]/(f, x - [\tilde{a}](y)) \xleftarrow{\sim} k[[y]]\,, \\ k[[x,y]]/(f, y - [p\tilde{b}](x)) \xleftarrow{\sim} k[[x]]\,. \end{cases}$$

Therefore the complete local rings of the irreducible components are given by

$$k[[x,y]]/(x - [\tilde{a}](y)) \quad \text{if} \quad \Lambda \sim (1,-a)\,,$$

$$k[[x,y]]/(y - [p\tilde{b}](x)) \quad \text{if} \quad \Lambda \sim (-pb,1)\,.$$

The assertion now follows from the crossings theorem (13.1.3). Q.E.D.

COROLLARY 13.8.5. *Hypotheses and notations as above, suppose further that $\mathcal{P}$ is the reduction mod p of a representable problem $\tilde{\mathcal{P}}$ on (Ell/W(k)) which is finite etale over (Ell/W(k)). Then we may view each Λ-component $\mathcal{M}(\mathcal{P}, [\Gamma(p^n)\text{-str. } \phi \text{ with } \phi(\operatorname{Ker}\Lambda) = 0])$ as a smooth curve in the regular surface*

$$\mathcal{M}(\tilde{\mathcal{P}}, [\Gamma(p^n)]^{\mathrm{can}})\,.$$

If Λ_1 and Λ_2 are two distinct component-labels, then the intersection-number of the Λ_1 and Λ_2-components at each supersingular point is given by the integer

$$\left(\#\left((\mathbf{Z}/p^n\mathbf{Z})^2 \Big/ \operatorname{Ker}(\Lambda_1) + \operatorname{Ker}(\Lambda_2) \right) \right)^2.$$

Proof. By definition, the intersection multiplicity in question is the k-dimension of the artinian k-algebra

$$\begin{cases} k[[x,y]]/(x-[\widetilde{a}_1](y), x-[\widetilde{a}_2](y)) & \begin{cases}\text{if } \Lambda_1 \sim (1,-a_1)\\ \text{if } \Lambda_2 \sim (1,-a_2)\end{cases} \\ k[[x,y]]/(x-[\widetilde{a}](y), y-[p\widetilde{b}](x)) & \begin{cases}\text{if } \Lambda_1 \sim (1,-a)\\ \text{if } \Lambda_2 \sim (-pb,1)\end{cases} \\ k[[x,y]]/(y-[p\widetilde{b}_1](x), y-[p\widetilde{b}_2](x)) & \begin{cases}\text{if } \Lambda_1 \sim (-pb_1,1)\\ \text{if } \Lambda_2 \sim (-pb_2,1)\end{cases}. \end{cases}$$

We are claiming that the lengths are respectively given by

$$(\#(Z_p/(p^n, \widetilde{a}_1-\widetilde{a}_2)))^2,\ 1,\ (\#(Z_p/(p^n, p\widetilde{b}_1-p\widetilde{b}_2)))^2 .$$

The third case is a special case of the first, with x and y interchanged.

In the second case, the assertion is obvious, because denoting by max the maximal ideal M of k[[x,y]], we have

$$\begin{cases} x-[\widetilde{a}](y) \equiv x \mod \max^2 \\ y-[p\widetilde{b}](x) \equiv y \mod \max^2, \end{cases}$$

so that these two quantities generate the maximal ideal.

In the first case we have

$$k[[x,y]]/(x-[a_1](y)) \xleftarrow{\sim} k[[y]],$$

with k[[y]] viewed as the complete local ring at a supersingular point on an Igusa curve. The complete local ring at the underlying point on $\mathcal{M}(\mathcal{P})$ is identified to k[[T]]. The formal group law over k[[y]] with which we are dealing is obtained from that of E/k[[T]] with respect to the parameter X by extension of scalars. The ring whose k-dimension we are computing is

$$k[[y]]/([\widetilde{a}_1](y)-[\widetilde{a}_2](y))$$

$$\simeq k[[y]]/([\widetilde{a}_1-\widetilde{a}_2](y)).$$

Now write

$$\widetilde{a}_1-\widetilde{a}_2 = (\text{unit}) \times p^\nu,\ 0 \le \nu \le n-1 .$$

(We have $\nu \le n-1$ because Λ_1 and Λ_2 are *distinct* component labels.) Making the change of variable $y \to [\text{unit}](y)$, we may assume

$$\widetilde{a}_1-\widetilde{a}_2 = p^\nu,\ 0 \le \nu \le n-1 ,$$

and our ring is

$$k[[y]]/([p^\nu](y)) .$$

We claim this has length $p^{2\nu}$. The case $\nu = 0$ is obvious, so we may suppose $1 \le \nu \le n-1$. The series $[p^\nu](X)$ is a power series in X with coefficients in the subring k[[T]] of k[[y]] with zero constant term and Weierstrass degree $p^{2\nu}$. Because the Igusa curve of level n sits over $\mathcal{M}(\mathcal{P})$ by pr_n, it is fully ramified over each supersingular point of degree $p^n\phi(p^n)$. Therefore we have the two congruences

$$[p^\nu](X) \equiv (\text{elt of } k^\times) X^{p^{2\nu}} \mod (X^{1+p^{2\nu}}, TX)$$

$$T \equiv 0 \mod (y^{p^n\phi(p^n)}) .$$

Because $\nu \le n-1$, $p^n\phi(p^n) > p^{2\nu}$, whence we find

$$[p^\nu](y) \equiv (\text{elt of } k^\times) y^{p^{2\nu}} \mod (y^{1+p^{2\nu}}),$$

as required. Q.E.D.

(13.9) *Distribution of the cusps on* $[\Gamma(p^n)]^{can}$

(13.9.1) Let $N \ge 1$ be an integer prime to p, $\Gamma \subset GL(2, Z/NZ)$ a subgroup, A the ring $(Z[\zeta_N])^{\det(\Gamma)}$. Suppose that the moduli problem

$$\mathcal{P} = ([\Gamma(N)]/\Gamma)^{A-can} \underset{A}{\otimes} A[1/N] \quad \text{on} \quad (Ell/A[1/N])$$

is representable. Then the simultaneous moduli problem

$$(\mathcal{P}, [\Gamma(p^n)]^{can}) \quad \text{on} \quad (\text{Ell}/A[1/N, \zeta_{p^n}])$$

is representable, and we have proven (10.9.4) that its compactified moduli scheme

$$\bar{\mathcal{M}}(\mathcal{P}, [\Gamma(p^n)]^{can})$$

is a two-dimensional regular scheme, proper and smooth over $A[\zeta_{p^n}, 1/N]$ outside the supersingular points in characteristic p, and that its scheme of cusps is finite etale over $A[\zeta_{p^n}, 1/N]$.

(13.9.2) The cusps are given as a disjoint union of schemes, indexed by the space

$$\pm 1 \backslash \text{Hom Surj}((\mathbf{Z}/p^n\mathbf{Z})^2, \mathbf{Z}/p^n\mathbf{Z}) \times \text{Hom Surj}((\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}/N\mathbf{Z}) / 1 \times \Gamma$$

which has a natural projection onto the space

$$(\mathbf{Z}/p^n\mathbf{Z})^\times \backslash \text{Hom Surj}((\mathbf{Z}/p^n\mathbf{Z})^2, \mathbf{Z}/p^n\mathbf{Z}) ,$$

which indexes the irreducible components of the *fiber* of

$$\begin{array}{c} \bar{\mathcal{M}}(\mathcal{P}, [\Gamma(p^n)]^{can}) \\ \downarrow \\ \text{Spec}\,(A[1/N, \zeta_{p^n}]) \end{array}$$

over any geometric point of the base with characteristic p. Recall that by (8.6.6), we know that formation of this $\bar{\mathcal{M}}$, and of its scheme of cusps, commutes with the extensions of scalars

$$A[1/N, \zeta_{p^n}] \to \text{an algebraically closed field } k \text{ of characteristic } p.$$

Therefore the finite etale k-scheme

$$\text{Cusps}\,(\mathcal{P}, [\Gamma(p^n)]^{can}) \underset{A[1/N, \zeta_{p^n}]}{\otimes} k$$

$$\xrightarrow{\sim} \text{Cusps}\,(\mathcal{P} \underset{A[1/N]}{\otimes} k, [\Gamma(p^n); \det = 1])$$

is simultaneously a disjoint union indexed by

$$\pm 1 \backslash \text{Hom Surj} \times \text{Hom Surj} / 1 \times \Gamma$$

(when thought of as coming from characteristic zero), and a disjoint union indexed by

$$(\mathbf{Z}/p^n\mathbf{Z})^\times \backslash \text{Hom Surj}((\mathbf{Z}/p^n\mathbf{Z})^2, \mathbf{Z}/p^n\mathbf{Z})$$

(partitioning in characteristic p, according to which irreducible component the cusp lies on).

THEOREM 13.9.3. *Hypotheses and notations as above, the natural projection*

$$\begin{array}{c} \pm 1 \backslash \text{Hom Surj}((\mathbf{Z}/p^n\mathbf{Z})^2, (\mathbf{Z}/p^n\mathbf{Z})) \times \text{Hom Surj}((\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}/N\mathbf{Z}) / 1 \times \Gamma \\ \downarrow \\ (\mathbf{Z}/p^n\mathbf{Z})^\times \backslash \text{Hom Surj}((\mathbf{Z}/p^n\mathbf{Z})^2, \mathbf{Z}/p^n\mathbf{Z}) \end{array}$$

is the map which assigns to a cusp-clump in characteristic zero the name of the irreducible component on which it lies in characteristic p.

Proof. This compatibility is clear from the way in which the components are labeled, and the fact that over any $\mathbf{F}_p$-algebra B, the canonical exact sequence of $B((q))$-group-schemes

$$0 \to \mu_{p^n} \to \text{Tate}\,(q)[p^n] \to \mathbf{Z}/p^n\mathbf{Z} \to 0$$

is canonically isomorphic to the exact sequence

$$0 \to \text{Ker } F^n \to \text{Tate}\,(q)[p^n] \to \text{Ker } V^n \to 0 . \qquad \text{Q.E.D.}$$

(13.10) *The reduction* mod p *of a general* p*-power level moduli problem*

(13.10.1) In this section we fix an integer $n \geq 1$, and consider an arbitrary subgroup

$$\Gamma \subset GL(2, \mathbf{Z}/p^n\mathbf{Z}) .$$

We denote by A the corresponding subring

$$A = (\mathbf{Z}[\zeta_{p^n}])^{\det(\Gamma)} \subset \mathbf{Z}[\zeta_{p^n}] .$$

For any field k of characteristic p, there is a unique ring homomorphism $A \to k$ (it sends $\zeta_{p^n} \mapsto 1$).

THEOREM 13.10.2. *Let k be a field of characteristic p, $\mathcal{P}$ a representable moduli problem on (Ell/k). Denote by $\mathcal{R}$ the moduli problem on (Ell/k) defined by*

$$\mathcal{R} = ([\Gamma(p^n)]/\Gamma)^{A-can} \underset{A}{\otimes} k .$$

Then we have

(1) *There is a natural $\mathcal{M}(\mathcal{P})$-morphism*

$$\mathcal{M}(\mathcal{P}, [\Gamma(p^n; \det = 1]) \to \mathcal{M}(\mathcal{P}, \mathcal{R})$$

which is Γ-equivariant, with Γ acting on the right on the moduli problem $[\Gamma(p^n); \det = 1]$ by $\phi \mapsto \phi \circ \gamma$, and Γ acting trivially on $\mathcal{M}(\mathcal{P}, \mathcal{R})$.

(2) *The induced $\mathcal{M}(\mathcal{P})$-morphism*

$$\mathcal{M}(\mathcal{P}, [\Gamma(p^n); \det = 1])/\Gamma \to \mathcal{M}(\mathcal{P}, \mathcal{R})$$

is surjective, radicial, and integral.

Proof. There is a natural isomorphism of moduli problems on (Ell/A)

$$([\Gamma(p^n)]/\Gamma)^{A-can} \xrightarrow{\sim} [\Gamma(p^n)]^{A-can}/\Gamma ,$$

so by general properties of quotients (7.1.3, (3)) we have a Γ-equivariant morphism of $\mathcal{M}(\mathcal{P})$-schemes

$$\mathcal{M}(\mathcal{P}, [\Gamma(p^n)]^{A-can} \underset{A}{\otimes} k) \to \mathcal{M}(\mathcal{P}, \mathcal{R})$$

such that the induced map

$$\mathcal{M}(\mathcal{P}, [\Gamma(p^n)]^{A-can} \underset{A}{\otimes} k)/\Gamma \to \mathcal{M}(\mathcal{P}, \mathcal{R})$$

is radicial, surjective and integral (A7.2.1). But the natural morphisms of moduli problems on (Ell/k)

$$([\Gamma(p^n)] \overset{\mathbf{Z}[\zeta_{p^n}]\text{-can}}{\underset{\mathbf{Z}[\zeta_{p^n}]}{\otimes}} k \hookrightarrow [\Gamma(p^n)]^{A-can} \underset{A}{\otimes} k \hookrightarrow [\Gamma(p^n)] \underset{\mathbf{Z}}{\otimes} k$$

are closed immersions which are radicial and surjective, simply because in any $\mathbf{F}_p$-algebra, the p^n'th cyclotomic polynomial is

$$\Phi_{p^n}(X) \equiv (X^{p^{n-1}} - 1)^{p-1} = (X-1)^{\phi(p^n)} ,$$

so that modulo nilpotents *any* Drinfeld p^n-basis on an $E/S/\mathbf{F}_p$ has determinant *one*. Therefore the morphism of $\mathcal{M}(\mathcal{P})$-schemes

$$\mathcal{M}(\mathcal{P}, [\Gamma(p^n); \det = 1]) \hookrightarrow \mathcal{M}(\mathcal{P}, [\Gamma(p^n)]^{A-can} \underset{A}{\otimes} k)$$

is a radicial and surjective closed immersion, which is visibly Γ-equivariant. Q.E.D.

THEOREM 13.10.3. *Let k be a perfect field of characteristic p, $\mathcal{P}$ a representable moduli problem on (Ell/k) which is finite etale over (Ell/k), and such that $\mathcal{M}(\mathcal{P})$ is connected. For any subgroup*

$$\Gamma \subset GL(2, \mathbf{Z}/p^n\mathbf{Z}) ,$$

acting on the $\overline{\mathcal{M}}(\mathcal{P})$-scheme

$$\overline{\mathcal{M}}(\mathcal{P}, [\Gamma(p^n); \det = 1]) ,$$

we have the following results:

(1) *The quotient $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma(p^n); \det = 1])/\Gamma$ is reduced, it is smooth over k outside its supersingular points, and its supersingular points, with values in any perfect k-algebra, map bijectively to those of $\overline{\mathcal{M}}(\mathcal{P})$.*

(2) *The irreducible components of $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma(p^n); \det = 1])/\Gamma$ are connected curves over k, smooth outside the supersingular points and*

geometrically unibranch at the supersingular points. They are indexed by the space

$$(\mathbf{Z}/p^n\mathbf{Z})^\times \backslash \text{Hom Surj}((\mathbf{Z}/p^n\mathbf{Z})^2, \mathbf{Z}/p^n\mathbf{Z}) / \Gamma$$

of component labels for Γ. *Each irreducible component is finite and flat over* $\overline{\mathcal{M}}(\mathcal{P})$, *and fully ramified over each supersingular point in the sense that its geometric fiber over each supersingular point is a single point.*

(3) *For each* $\Lambda \in \text{Hom Surj}$, *denote by* $\text{Fix}^\times(\Lambda) \subset GL(2, \mathbf{Z}/p^n\mathbf{Z})$ *the fixer of the component-label* $(\mathbf{Z}/p^n\mathbf{Z})^\times\Lambda$. *In the oriented basis* $(k_\Lambda, \ell_\Lambda)$ *attached to* Λ, $\text{Fix}^\times(\Lambda)$ *is the subgroup of all matrices of the form*

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \subset GL(2, \mathbf{Z}/p^n\mathbf{Z}) .$$

This group acts on the moduli problem

$$[\text{ExIg}(p^n, n)] = \textit{Drinfeld } p^n\textit{-bases of the form } (O,P)$$

by

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : (O,P) \mapsto (O, dP) .$$

With this action understood, the normalization of the irreducible component of $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma(p^n); \det = 1])/\Gamma$ *indexed by* Λ *is the* $\overline{\mathcal{M}}(\mathcal{P})$*-scheme*

$$\overline{\mathcal{M}}(\mathcal{P}, [\text{ExIg}(p^n, n)]) / \Gamma \cap \text{Fix}^\times(\Lambda) .$$

(4) *If the group* ± 1 *acts freely on* $Z(\mathcal{P})$ *(cf. (10.13.7-8-9)), then the scheme of cusps* $j^{-1}(\infty)^{\text{red}}$ *in* $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma(p^n); \det = 1])/\Gamma$ *is finite etale over the scheme of cusps in* $\overline{\mathcal{M}}(\mathcal{P})$.

Proof. This is immediate from the description (13.7.6) of $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma(p^n); \det = 1])$ as a disjoint union, with crossings at the supersingular points, of the smooth curves

$$\overline{\mathcal{M}}(\mathcal{P}, [\Gamma(p^n)\text{str. } \phi \text{ with } \phi(\text{Ker } \Lambda) = 0]) \simeq \overline{\mathcal{M}}(\mathcal{P}, [\text{ExIg}(p^n, n)])$$

indexed by $\Lambda \in (\mathbf{Z}/p^n\mathbf{Z})^\times \backslash \text{Hom Surj}$ (cf. (12.7.1) for the last assertion).

Q.E.D.

THEOREM 13.10.4. *Let* $N \geq 1$ *be an integer prime to* p,

$$\Gamma_2 \subset GL(2, \mathbf{Z}/N\mathbf{Z})$$

a subgroup, B *the ring* $(\mathbf{Z}[\zeta_N])^{\det(\Gamma_2)}$. *Suppose that the moduli problem*

$$\mathcal{P} = ([\Gamma(N)]/\Gamma_2)^{B\text{-can}} \underset{B}{\otimes} B[1/N] \quad \textit{on} \quad (\text{Ell}/B[1/N])$$

is representable, and that -1 *operates without fixed points on the space of cusp-labels for* Γ_2. *Let*

$$\mathcal{R} = ([\Gamma(p^n)]/\Gamma_1)^{A\text{-can}} \quad \textit{on} \quad (\text{Ell}/A) .$$

Let k *be a perfect field of characteristic* p, $B[1/N] \to k$ *a ring homomorphism,*

$$A \underset{\mathbf{Z}}{\otimes} B[1/N] \to k$$

its unique extension to $A \underset{\mathbf{Z}}{\otimes} B[1/N]$. *Then*

(1) *We have a natural morphism of* $\mathcal{M}(\mathcal{P} \otimes k)$*-schemes*

$$\begin{array}{ccc} \mathcal{M}(\mathcal{P} \underset{\mathbf{Z}}{\otimes} A, \mathcal{R} \underset{\mathbf{Z}}{\otimes} B[1/N]) \underset{A \otimes B[1/N]}{\otimes} k & & \\ \Vert & & \\ \mathcal{M}(\mathcal{P} \underset{B[1/N]}{\otimes} k, \mathcal{R} \underset{A}{\otimes} k) & \longleftarrow & \mathcal{M}(\mathcal{P} \underset{B[1/N]}{\otimes} k, [\Gamma(p^n); \det = 1])/\Gamma_1 \end{array}$$

which is radicial, surjective and integral.

(2) *If* Γ_1 *is balanced (and satisfies* $*$ *in case* $p = 2$ *cf. 10.10.1.1), then by (10.10.3), the compactified moduli scheme*

$$\overline{\mathcal{M}}(\mathcal{P} \underset{\mathbf{Z}}{\otimes} A, \mathcal{R} \underset{\mathbf{Z}}{\otimes} B[1/N])$$

is smooth over $A \otimes B[1/N]$ *outside the supersingular points in characteristic* p, *with scheme of cusps finite etale over* $A \otimes B[1/N]$. *There is a natural morphism of* $\overline{\mathcal{M}}(\mathcal{P} \otimes k)$*-schemes*

$$\begin{array}{ccc} \overline{\mathcal{M}}(\mathcal{P}\otimes A, \mathcal{R}\otimes B[1/N]) \underset{A\otimes B[1/N]}{\otimes} k & & \\ \| & & \\ \overline{\mathcal{M}}(\mathcal{P} \underset{B[1/N]}{\otimes} k, \mathcal{R}\otimes k) & \longleftarrow & \overline{\mathcal{M}}(\mathcal{P} \underset{B[1/N]}{\otimes} k, [\Gamma(p^n); \det=1])/\Gamma_1 \\ & \underset{A}{} & \end{array}$$

which is radicial, surjective and integral.

(3) *If* Γ_1 *is balanced (and satisfies* $*$ *in case* $p=2$*), this morphism induces an isomorphism on the respective schemes of cusps. Under this isomorphism, the image of the cusp-clump on* $\overline{\mathcal{M}}(\mathcal{P}\otimes A, \mathcal{R}\otimes B[1/N])$ *labeled by a given cusp-label in*

$$\pm 1 \backslash \text{Hom Surj}((\mathbf{Z}/p^n\mathbf{Z})^2, \mathbf{Z}/p^n\mathbf{Z}) \times \text{Hom Surj}((\mathbf{Z}/N\mathbf{Z})^2, \mathbf{Z}/N\mathbf{Z}) / \Gamma_1 \times \Gamma_2$$

lies on the irreducible component labeled by the component-label in

$$(\mathbf{Z}/p^n\mathbf{Z})^\times \backslash \text{Hom Surj}((\mathbf{Z}/p^n\mathbf{Z})^2, \mathbf{Z}/p^n\mathbf{Z}) / \Gamma_1$$

Proof. Assertion (1) is just (13.10.2). If Γ_1 is balanced (and satisfies $*$ in case $p=2$), then the formation of both $\overline{\mathcal{M}}$ and of its scheme of cusps commutes with the extension of scalars $A\otimes B[1/N] \to k$. Assertion (2) holds because the compactified schemes in question are the normalizations of $\overline{\mathcal{M}}(\mathcal{P}\otimes k)$ in two normal, finite $\overline{\mathcal{M}}(\mathcal{P}\otimes k)$-schemes which, over $\mathcal{M}(\mathcal{P}\otimes k)$, are given with a radicial surjective $\mathcal{M}(\mathcal{P}\otimes k)$-morphism between them. This morphism extends "by normalization", and it remains radicial, surjective and integral. Assertion (3) holds because any surjective radicial map between finite etale k-schemes (cf. (13.10.3)(4) and (10.10.3(6))) is automatically an isomorphism. The labeling compatibility is clear from the construction of the labeling. Q.E.D.

CAUTIONARY REMARK 13.10.5. Even when Γ_1 is balanced, it is *not* in general true that the morphisms of 13.10.4(1) and (3) are isomorphisms outside the supersingular points. For example, if $n \geq 1$ and if Γ_1 is the entire upper unipotent subgroup

$$\Gamma_1 = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \subset GL(2, \mathbf{Z}/p^n\mathbf{Z}),$$

then one easily checks, using (13.10.3(3)) and (5.5.3), that the source and target of these morphisms have *different* degrees over $\mathcal{M}(\mathcal{P}\otimes k)$ (resp. over $\overline{\mathcal{M}}(\mathcal{P}\otimes k)$).

(13.11) *The reduction* mod p *of* $[\text{bal.}\,\Gamma_1(p^n)]^{\text{can}}$

(13.11.1) For any field k of characteristic p, there is a unique ring homomorphism $\mathbf{Z}[\zeta_{p^n}] \to k$, so the moduli problem

$$[\text{bal.}\,\Gamma_1(p^n)]^{\text{can}} \underset{\mathbf{Z}[\zeta_{p^n}]}{\otimes} k \quad \text{on} \quad (\text{Ell}/k)$$

is given by

(13.11.1.1) $E/S \mapsto$ dual cyclic p^n isogenies $E = E_0 \underset{\pi^t}{\overset{\pi}{\rightleftarrows}} E_n$

$$\text{given with } \begin{cases} P_0 \text{ a generator of } \text{Ker}(\pi) \\ Q_n \text{ a generator of } \text{Ker}(\pi^t), \end{cases}$$

such that under the canonical pairing,

$$\langle P_0, Q_n \rangle_\pi = 1 .$$

We will denote this problem

(13.11.1.2) $\qquad [\text{bal.}\,\Gamma_1(p^n); \det=1]$.

THEOREM 13.11.2. *Consider a dual pair of cyclic* p^n *isogenies between ordinary elliptic curves* E_0, E_n *over a connected* $\mathbf{F}_p$*-scheme* S*, given with generators of their kernels* P_0, Q_n*, with* $\langle P_0, Q_n \rangle = 1$.

(1) *There exists a unique pair* a,b *of non-negative integers with* $a+b=n$*, such that* $\pi_{0,n}$ *is a cyclic isogeny of type* (a,b)*, and such that* $\lambda_{n,0} = (\pi_{0,n})^t$ *is a cyclic isogeny of type* (b,a).

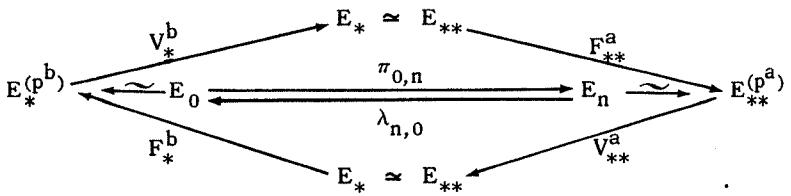
(2) *We have* $p^b P_0 = 0$*, and* $(P_0, 0)$ *is a Drinfeld* p^b*-basis for* E_0/S*. The point* P_0 *generates a* $\mathbf{Z}/p^b\mathbf{Z}$ *inside* E_0*, and the quotient of* E_0 *by this subgroup we denote* E_**. Canonically we have* $E_0 \xrightarrow{\sim} E_*^{(p^b)}$.

(3) *We have* $p^a Q_n = 0$*, and* $(Q_n, 0)$ *is a Drinfeld* p^a*-basis for* E_n/S*. The point* Q_n *generates a* $\mathbf{Z}/p^a\mathbf{Z}$ *inside* E_n*, and the quotient of* E_n *by this subgroup we denote* E_{**}*. Canonically* $E_n \xrightarrow{\sim} E_{**}^{(p^a)}$.

(4) *There is a unique isomorphism of elliptic curves over* S

$$E_* \simeq E_{**}$$

which makes the upper and lower triangles commute:



(5) *In terms of the elliptic curve* E_*, *our original isogeny diagram, in its standard* (a,b) *factorization, is*

$$E_*^{(p^b)} \underset{V^a}{\overset{F^a}{\rightleftarrows}} E_*^{(p^n)} \underset{F^b}{\overset{V^b}{\rightleftarrows}} E_*^{(p^a)} .$$

(6) *The point* $P_0 \in E_*^{(p^b)}(S)$ *is an* $[\mathrm{Ig}(p^b)]$*-structure on* E_*/S, *and the point* $Q_n \in E_*^{(p^a)}(S)$ *is an* $[\mathrm{Ig}(p^a)]$*-structure on* E_*/S.

(7) *If* $a \geq b$, *there exists a unique unit* $u \in (\mathbf{Z}/p^b\mathbf{Z})^\times$ *such that*

$$V_*^{a-b}(Q_n) = u \cdot P_0 \quad \textit{in} \quad E_*^{(p^b)}(S) ;$$

if $b \geq a$, *there exists a unique unit* $u \in (\mathbf{Z}/p^a\mathbf{Z})^\times$ *such that*

$$Q_n = u \cdot V_*^{b-a}(P_0) \quad \textit{in} \quad E_*^{(p^a)}(S) .$$

Proof. Assertion (1) is just (13.3.3). Assertions (2) and (3) are interchanged by duality, so it suffices to prove (2). Consider the standard (a,b) factorization of our cyclic isogeny

$$P_0 ; E_0 \underset{V_0^a}{\overset{F_0^a}{\rightleftarrows}} E_0^{(p^a)} \simeq E_n^{(p^b)} \underset{F_n^b}{\overset{V_n^b}{\rightleftarrows}} E_n ; Q_n .$$

According to (7.9.2), $p^b P_0$ generates $\mathrm{Ker}(F_0^a)$, $F_n^b(Q_n)$ generates $\mathrm{Ker}(V_0^a)$, and

$$<p^b P_0, F_n^b(Q_n)>_{F_0^a} = (<P_0, Q_n>_{\pi_{0,n}})^{p^b} = (1)^{p^b} = 1 .$$

But E_0/S being *ordinary*, $F_n^b(Q_n)$ defines an isomorphism

$$\mathbf{Z}/p^a\mathbf{Z} \xrightarrow{\sim} \mathrm{Ker}\, V_0^a ,$$

and the dual isomorphism

$$\mathrm{Ker}\, F_0^a \xrightarrow{\sim} \mu_{p^a}$$

is given by

$$\xi \in \mathrm{Ker}\, F_0^a \mapsto <\xi, F_n^b(Q_n)>_{F_0^a} .$$

Therefore $p^b P_0$ is the zero-section of $\mathrm{Ker}\, F_0^a$, because we have

$$<p^b P_0, F_n^b(Q_n)>_{F_0^a} = 1 .$$

Therefore $p^b P_0 = 0$. Therefore P_0 defines a map of S-groups

$$\mathbf{Z}/p^b\mathbf{Z} \to E_0 .$$

We claim this map is a closed immersion, i.e., that for every geometric point $\mathrm{Spec}(k) \to S$, the image of P in the abstract group $(E_0 \underset{S}{\times} k)(k)$ has exact order p^b in the naive sense. But this is clear, because by (7.9.2) the point $F_0^a(P_0) \in E_0^{(p^a)} \simeq E_n^{(p^b)}$ generates $\mathrm{Ker}(V_n^b)$. As E_n/S is *ordinary*, $\mathrm{Ker}(V_n^b)$ is *etale*, so $F_0^a(P_0)$ defines

$$\mathbf{Z}/p^b\mathbf{Z} \xrightarrow{\sim} \mathrm{Ker}(V_n^b) .$$

In particular, $F_0^a(P_0)$ has "naive exact order p^b" in the group of rational points of every geometric fiber of $E_0^{(p^a)}/S$, and hence P_0 has "naive exact order p^b" in every geometric fiber of E_0/S. Therefore P_0 does indeed define a closed immersion

$$\mathbf{Z}/p^b\mathbf{Z} \hookrightarrow E_0/S .$$

To see that $(P_0, 0)$ is a Drinfeld p^b-basis, consider the composite map

$$\begin{array}{ccccccccc} & & & & & & Z/p^bZ & & \\ & & & & & \swarrow & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Ker}\, F_0^b & \longrightarrow & E_0[p^b] & \xrightarrow{F_0^b} & \mathrm{Ker}\, V_0^b & \longrightarrow & 0\,. \end{array}$$

The dotted arrow is certainly injective, because any Z/p^bZ inside $E_0[p^b]$ meets $\mathrm{Ker}\, F_0^b$ only in the zero-section. Comparing ranks, it is an isomorphism, so defines a splitting

$$E_0[p^b] \simeq \mathrm{Ker}\, F_0^b \oplus (\text{the } Z/p^bZ \text{ generated by } P_0).$$

Because zero certainly generates $\mathrm{Ker}\, F_0^b$, this shows (cf. 1.11.2) that $(0, P_0)$ is a Drinfeld p^b-basis of E_0/S.

It further shows that the morphism "multiplication by p^b" on E_0 admits a *non-standard* factorization

$$\begin{array}{ccccc} E_0 & \longrightarrow & E_0/(\text{s/gp. gen. by } P_0) & \xrightarrow{F^b} & E_0\,. \\ & \searrow & & \nearrow & \\ & & p^b & & \end{array}$$

Christening the middle term E_* gives the canonical identification

$$E_*^{(p^b)} \xrightarrow{\sim} E_0\,.$$

We now come to the heart of the matter, establishing (4), the isomorphism

$$E_* \simeq E_{**}\,.$$

Once this is done, assertion (5) is obvious by "substituting" $E_0 = E_*^{(p^b)}$, $E_n = E_*^{(p^a)}$, and remembering that in the standard (a,b) factorization, the a'th term $E_a = E_0^{(p^a)} = E_n^{(p^b)}$. Assertion (6) is "mise pour memoire" in view of (2) and (3) (cf. 12.2.7). Assertion (7) holds because the quantities being compared are two generators, over a connected base, of an etale group isomorphic to $Z/p^{\min(a,b)}Z$.

To show that $E_* \simeq E_{**}$, we argue as follows. Consider the commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Z/p^aZ & \longrightarrow & Z/p^nZ & \longrightarrow & Z/p^bZ & \longrightarrow & 0 \\ & & \downarrow 0 & & \downarrow P_0 & & \downarrow P_0 & & \\ 0 & \longrightarrow & \mathrm{Ker}\,(F_0^a) & \longrightarrow & \mathrm{Ker}\,(\pi_{0,n}) & \xrightarrow{F_0^a} & \mathrm{Ker}\,(\pi_{a,n}) & \longrightarrow & 0\,. \end{array}$$

The middle vertical arrow is a generator, the term $\mathrm{Ker}(\pi_{a,n})$ is a twisted Z/p^bZ (being $\mathrm{Ker}\, V_n^b$), and $\mathrm{Ker}\, F_0^a$ is generated by zero. By (1.11.2), the final vertical arrow is a generator, hence an isomorphism. Therefore we have a *splitting*

$$\mathrm{Ker}\,(\pi_{0,n}) = \mathrm{Ker}\,(F_0^a) \oplus (\text{the } Z/p^bZ \text{ generated by } P_0),$$

so an *exotic* factorization of

$$E_0 \xrightarrow{\pi_{0,n}} E_n$$

as

$$E_0 \simeq E_*^{(p^b)} \xrightarrow{V_*^b} E_* \xrightarrow{F_*^a} E_*^{(p^a)}\,.$$

Therefore we have canonically,

$$E_n \simeq E_*^{(p^a)}\,.$$

Now E_{**} is the *quotient* of E_n by the Z/p^aZ generated in it by Q_n, while E_* is the quotient of $E_n \simeq E_*^{(p^a)}$ by $\mathrm{Ker}(V_*^a)$. Therefore what we must show is that Q_n in $E_n \simeq E_*^{(p^a)}$ *generates* $\mathrm{Ker}\, V_*^a$. We know that Q_n generates a Z/p^aZ inside E_n. So for any connected S-scheme T, the group generated by Q_n has its only T-valued points the multiples of Q_n.

So it suffices to show that Q_n lies in $\mathrm{Ker}\, V_*^a$ (for then the Z/p^aZ it generates will lie in $\mathrm{Ker}\, V_*^a$, and as the ranks are equal the two groups must coincide). To show, finally, that

$$V_*^a(Q_n) = 0\,,$$

we resort to a trick.

Because $[\Gamma(p^n)]$ is finite flat over $[\text{bal.}\,\Gamma_1(p^n)]$, it follows (9.1.9) that $[\Gamma(p^n)]^{can}$ is finite flat over $[\text{bal.}\,\Gamma_1(p^n)]^{can}$. Therefore $[\Gamma(p^n);\det=1]$ is finite flat over $[\text{bal.}\,\Gamma_1(p^n);\det=1]$. This means that at the expense of passing to an f.p.p.f. $S'\to S$ (certainly allowable for proving $V_*^a(Q_n)=0$), we may assume given a point $\widetilde{Q}\in E_0(S')$ such that

$$\begin{cases} (P_0,\widetilde{Q}) \text{ is a Drinfeld } p^n\text{-basis on } E_0/S', \text{ with} \\ \qquad e_{p^n}(P_0,\widetilde{Q})=1\ . \\ \pi_{0,n}\widetilde{Q}=Q_n=\widetilde{Q} \text{ ``mod } P_0\text{.''} \end{cases}$$

By our earlier analysis of $[\Gamma(p^n);\det=1]$-structures on ordinary curves, we know that Zariski locally on S', we have an equation either of the form

$$\widetilde{Q}=aP_0,\ \text{some}\ a\in \mathbf{Z}/p^n\mathbf{Z}$$

or of the form

$$P_0=pb\widetilde{Q},\ \text{some}\ b\in \mathbf{Z}/p^{n-1}\mathbf{Z}\ .$$

In the first case, when $\widetilde{Q}$ lies in the subgroup generated by P_0, we have $Q_n=0$, so certainly $V_*^a(Q_n)=0$ (in fact $a=0$ in this case).

In the second case, multiplying $\widetilde{Q}$ and Q_n by a *unit* in $\mathbf{Z}/p^n\mathbf{Z}$, we may suppose

$$P_0=p^\nu\widetilde{Q}\quad\text{for some}\quad \nu\geq 1\ .$$

We claim that $\nu=a$. For if $(p^\nu\widetilde{Q},\widetilde{Q})$ is a Drinfeld p^n-basis, then so is $(0,\widetilde{Q})$, hence, as E_0/S is ordinary, $\widetilde{Q}$ has "naive exact order p^n" in each geometric fiber of E_0/S. Therefore $P_0=p^\nu\widetilde{Q}$ has "naive exact order $p^{n-\nu}$" in each geometric fiber. But P_0 has "naive exact order p^b" in each geometric fiber, so necessarily $\nu=a$.

Now we use the exotic factorization of $\pi_{0,n}$ as

$$E_*^{(p^b)}\xrightarrow{V_*^b}E_*\xrightarrow{F_*^a}E_*^{(p^a)}\ ,$$

and compute

$$\begin{aligned} V_*^a(Q_n) &= V_*^a(\pi_{0,n}(\widetilde{Q})) \\ &= V_*^aF_*^aV_*^bQ \\ &= p^aV_*^b\widetilde{Q} \\ &= V_*^b(p^a\widetilde{Q}) \\ &= V_*^b(P_0)\ . \end{aligned}$$

But $V_*^b(P_0)=0$, because the curve E_* was fabricated exactly so that $E_0\simeq E_*^{(p^b)}$ with P_0 a *generator* of $\mathrm{Ker}(V_*^b)$! Q.E.D.

THEOREM 13.11.3. *Let* a,b *be integers* ≥ 0, *with* $a+b=n\geq 1$. *Fix a unit*

$$u\in(\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times\ .$$

Let $E/S/\mathbf{F}_p$ *be an elliptic curve, given with*

$$P\in E^{(p^b)}(S),\ \textit{a generator of}\ \mathrm{Ker}(V^b)$$

$$Q\in E^{(p^a)}(S),\ \textit{a generator of}\ \mathrm{Ker}(V^a)\ .$$

Suppose that

$$\begin{cases} V^{a-b}(Q)=uP & \textit{if}\ a\geq b \\ Q=uV^{b-a}(P) & \textit{if}\ b\geq a\ . \end{cases}$$

Then:

(1) *The diagram*

$$P;\ E^{(p^b)}\xrightarrow{F^a}E^{(p^n)}\xrightarrow{V^b}E^{(p^a)};\ Q$$

is a $[\text{bal.}\,\Gamma_1(p^n);\det=1]$ *structure on* $E^{(p^b)}/S$.

(2) *For any perfect field* k *of characteristic* p, *and any representable problem* $\mathcal{P}$ *on* (Ell/k) *which is finite etale over* (Ell/k), *this construction defines a closed immersion of moduli schemes*

$$\mathcal{M}(\mathcal{P}, [\mathrm{Ig}(p^{\max(a,b)})]) \hookrightarrow \mathcal{M}(\mathcal{P}^{(\sigma^b)}, [\mathrm{bal}.\Gamma_1(p^n); \det = 1]) .$$

Proof. We begin with (1). The isogeny

$$E^{(p^b)} \xrightarrow{F^a} E^{(p^n)} \xrightarrow{V^b} E^{(p^a)}$$

is certainly cyclic in standard order, as follows immediately from the two-step-criterion (6.7.15) and the fact that powers of F, V, and p are all cyclic in characteristic p (cf. 12.2.1-3-5). That $P \in E^{(p^b)}(S)$ generates the kernel of this composite is clear from the backing-up theorem (6.7.11), for as P generates $\mathrm{Ker}(V^b : E^{(p^b)} \to E)$, we certainly have that $F^a(P) = P^{(p^a)}$ on $(E^{(p^b)})^{(p^a)}$ generates $\mathrm{Ker}(V^b : E^{(p^{a+b})} \to E^{(p^a)})$. Similarly, Q generates the kernel of the dual isogeny. It remains to see that

$$<P, Q> = 1 .$$

For this we may reduce to the case $u = 1$ simply by replacing P by $\tilde{u}P$ for any $\tilde{u} \in (\mathbf{Z}/p^b\mathbf{Z})^\times$ which lifts u. The question is f.p.p.f. local on S, so we may suppose there exists a point $R \in E^{(p^n)}(S)$ with

$$\begin{cases} V^a(R) = P & \text{if } a \le b \\ V^b(R) = Q & \text{if } a \ge b . \end{cases}$$

Then we have

$$V^a(R) = P \quad \text{and} \quad V^b(R) = Q ,$$

and since one of a or b is ≥ 1, R itself must generate $\mathrm{Ker}(V^n)$, by the backing-up criterion (6.7.11) applied to V^n. Then

$$\begin{aligned} <P, Q>_{V^b F^a} &= <P, V^b(R)>_{V^b F^a} \\ &= <V^a(R), V^b(R)>_{V^b F^a} . \end{aligned}$$

Again f.p.p.f. localizing on S, we may assume given a point

$$R' \in E^{(p^b)}(S) \quad \text{with} \quad F^a(R') = R .$$

Then $p^n R' = 0$, because

$$\begin{aligned} p^n R' = p^b p^a R' = p^b V^a F^a(R') &= p^b V^a(R) \\ &= p^b P \\ &= F^b V^b P \\ &= 0 . \end{aligned}$$

Therefore

$$\begin{aligned} <P, Q>_{V^b F^a} &= <V^a(R), V^b F^a(R')>_{V^b F^a} \\ &= e_{p^n}(V^a(R), R') \\ &= e_{p^n}(R, F^a(R')) \\ &= e_{p^n}(R, R) = 1 . \end{aligned}$$

This proves (1). Therefore the map in (2) is well defined. It is an $\mathcal{M}(\mathcal{P})$-map between finite $\mathcal{M}(\mathcal{P})$-schemes, so it is certainly a finite map, so a proper map. So it is a closed immersion if and only if it is an immersion, i.e., injective on S-valued points for all k-schemes S. But this injectivity is clear, for we recover the original object (E/S, P and Q subject to u-compatibility) from either the source $(E^{(p^b)}; P)$ or the target $(E^{(p^a)}; Q)$ depending on whether $a \le b$ or $b \le a$, by the inverse of the exotic isomorphism (for $M = \max(A,B)$)

$$\mathcal{M}(\mathcal{P}, [\mathrm{Ig}(p^M)]) \xrightarrow{\sim} \mathcal{M}(\mathcal{P}^{(\sigma^M)}, [\mathrm{ExIg}(p^M, M)]) . \qquad \text{Q.E.D.}$$

THEOREM 13.11.4. *Let* k *be a perfect field of characteristic* p, $\mathcal{P}$ *a representable problem on* (Ell/k) *which is finite etale over* (Ell/k).

Then

(1) *the scheme* $\mathcal{M}(\mathcal{P}, [\text{bal.}\,\Gamma_1(p^n); \det=1])$ *is the disjoint union, with crossings at the supersingular points, of the following smooth* k*-curves:*

for each pair (a,b) *of non-negative integers with* $a+b=n$, *and for each* $u \in (\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times$, *one copy of* $\mathcal{M}(\mathcal{P}(\sigma^{-b}), [\text{Ig}(p^{\max(a,b)})])$, *mapping to* $\mathcal{M}(\mathcal{P})$ *by* pr_b *(cf. 12.10.3):*

$$\begin{array}{c} \mathcal{M}(\mathcal{P}(\sigma^{-b}), [\text{Ig}(p^{\max(a,b)})]) \\ \Big\downarrow \text{pr}_b \\ \mathcal{M}(\mathcal{P}) \end{array}$$

(2) *the compactified moduli scheme* $\overline{\mathcal{M}}(\mathcal{P}, [\text{bal.}\,\Gamma_1(p^n); \det=1])$ *is the disjoint union, with crossings at the supersingular points, of the following proper smooth* k*-curves*

for each (a,b) *with* $a+b=n$, *and for each* $u \in (\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times$, *one copy of* $\overline{\mathcal{M}}(\mathcal{P}(\sigma^{-b}), [\text{Ig}(p^{\max(a,b)})])$, *mapping to* $\overline{\mathcal{M}}(\mathcal{P})$ *by* pr_b.

Proof. Statement (1) is just the crossings theorem applied in light of our present analysis, and (2) follows just as in (13.7.6). Q.E.D.

(13.12) *The reduction* mod p *of quotients of* $[\text{bal.}\,\Gamma_1(p^n)]$ *by subgroups of* $(\mathbf{Z}/p^n\mathbf{Z})^\times \times (\mathbf{Z}/p^n\mathbf{Z})^\times$.

(13.12.1) In this section, we fix a subgroup

$$K \subset (\mathbf{Z}/p^n\mathbf{Z})^\times \times (\mathbf{Z}/p^n\mathbf{Z})^\times .$$

The first and second projections define group-homomorphisms

$$\chi_1, \chi_2 : K \to (\mathbf{Z}/p^n\mathbf{Z})^\times . \tag{13.12.1.1}$$

The group K operates on the moduli problem $[\text{bal.}\,\Gamma_1(p^n)]$, by

$$\begin{array}{ccc} P\,;\, E_0 & \rightleftarrows & E_n\,;\, Q \\ \Big\downarrow & & \Big\downarrow \\ \chi_1(k)P\,;\, E_0 & \rightleftarrows & E_n\,;\, \chi_2(k)Q\,. \end{array} \qquad k \in K \tag{13.12.1.2}$$

If we denote by

$$\widetilde{K} \subset \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \subset GL(2, \mathbf{Z}/p^n\mathbf{Z}) \tag{13.12.1.3}$$

the subgroup consisting of all matrices

$$\begin{pmatrix} k_1 & * \\ 0 & k_2 \end{pmatrix} \qquad (k_1, k_2) \in K\,;\ * \in \mathbf{Z}/p^n\mathbf{Z}\,,$$

then we have an exact sequence of groups

$$0 \to \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \to \widetilde{K} \to K \to 0 \tag{13.12.1.4}$$

whence (7.4.2(2)) a canonical isomorphism of moduli problems on (Ell/Z)

$$[\Gamma(p^n)]/\widetilde{K} \simeq [\text{bal.}\,\Gamma_1(p^n)]/K\,. \tag{13.12.1.5}$$

(13.12.2) Via this identification, we obtain from the general theorem (13.10.4) on the reduction mod p of general quotients of $[\Gamma(p^n)]$ by subgroups $\Gamma \subset GL(2, \mathbf{Z}/p^n\mathbf{Z})$, a rather concrete theorem on the reduction mod p of quotients of $[\text{bal.}\,\Gamma_1(p^n)]$ by arbitrary subgroups K of $(\mathbf{Z}/p^n\mathbf{Z})^\times \times (\mathbf{Z}/p^n\mathbf{Z})^\times$.

In order to state the result concisely, we must introduce some notation. As is customary, we put

$$A = (\mathbf{Z}[\zeta_{p^n}])^{\det(K)} \tag{13.12.2.1}$$

where by abuse of notation we write

(13.12.2.2) $$\det \overset{\text{dfn}}{=\!=} \chi_1\chi_2 : K \to (\mathbf{Z}/p^n\mathbf{Z})^\times .$$

Given a pair of non-negative integers (a,b) with $a+b=n$, we define a subgroup

$$K(a,b) \subset K$$

by

(13.12.2.3) $$K(a,b) = \{(k_1,k_2) \in K \text{ with } k_1 \equiv k_2 \bmod p^{\min(a,b)}\},$$

and a subgroup

$$\operatorname{Im} K(a,b) \subset (\mathbf{Z}/p^{\max(a,b)}\mathbf{Z})^\times$$

by

(13.12.2.4) $$\operatorname{Im} K(a,b) = \begin{cases} \chi_1(K(a,b)) \bmod p^b & \text{if } a \le b \\ \chi_2(K(a,b)) \bmod p^a & \text{if } a \ge b , \end{cases}$$

and another subgroup

$$\operatorname{Comp} K(a,b) \subset (\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times$$

by

(13.12.2.5) $$\operatorname{Comp} K(a,b) = (\chi_1/\chi_2)(K) \bmod p^{\min(a,b)} .$$

Then we have a short exact sequence

(13.12.2.6) $$0 \to K(a,b) \to K \to \operatorname{Comp} K(a,b) \to 0$$

and a homomorphism

(13.12.2.7) $$K(a,b) \twoheadrightarrow \operatorname{Im} K(a,b) .$$

THEOREM 13.12.3. *Let $N \ge 1$ be an integer prime to p, $\Gamma \subset GL(2, \mathbf{Z}/N\mathbf{Z})$ a subgroup, $B = \mathbf{Z}[\zeta_N]^{\det(\Gamma)}$ the corresponding ring. Suppose that the moduli problem*

$$\mathcal{P} = ([\Gamma(N)]/\Gamma)^{B\text{-can}} \underset{B}{\otimes} B[1/N] \quad \textit{on} \quad (\text{Ell}/B[1/N])$$

is representable, and that -1 operates without fixed points on the space of cusp labels for Γ.

Let K be a subgroup of $(\mathbf{Z}/p^n\mathbf{Z})^\times \times (\mathbf{Z}/p^n\mathbf{Z})^\times$, and suppose either p odd, or $p^n = 2$, or $\det(K) \equiv 1 \bmod 4$ (so that K satisfies condition $*$). Let $\mathcal{R}$ denote the moduli problem

$$\mathcal{R} = ([\text{bal. } \Gamma_1(p^n)]/K)^{A\text{-can}} \quad \textit{on} \quad (\text{Ell}/A) .$$

Let k be a perfect field of characteristic p, $B[1/N] \to k$ a ring homomorphism, $A \underset{\mathbf{Z}}{\otimes} B[1/N] \to k$ its unique extension to $A \underset{\mathbf{Z}}{\otimes} B[1/N]$. Then

(1) We have a radicial, surjective and integral $\overline{\mathcal{M}}(\mathcal{P} \underset{\mathbf{Z}}{\otimes} k)$-morphism

$$\overline{\mathcal{M}}(\mathcal{P} \underset{\mathbf{Z}}{\otimes} k, [\text{bal. } \Gamma_1(p^n); \det = 1])/K$$

$$\Big\downarrow$$

$$\left(\overline{\mathcal{M}}(\mathcal{P} \underset{\mathbf{Z}}{\otimes} A, \mathcal{R} \underset{\mathbf{Z}}{\otimes} B[1/N]) \underset{A \underset{\mathbf{Z}}{\otimes} B[1/N]}{\otimes} k\right)^{\text{red}} .$$

Source and target are smooth curves over k outside their supersingular points.

(2) The irreducible components of the scheme $\overline{\mathcal{M}}(\mathcal{P} \underset{\mathbf{Z}}{\otimes} k, [\text{bal. } \Gamma_1(p^n); \det = 1])/K$ are proper connected curves over k, smooth outside the supersingular points and geometrically unibranch at the supersingular points, which are finite flat over $\overline{\mathcal{M}}(\mathcal{P} \underset{\mathbf{Z}}{\otimes} k)$ and fully ramified (cf. 13.10.3, (3)) over each supersingular point. Their normalizations are:

> *for each pair (a,b) of non-negative integers with $a+b=n$, and each element u in $(\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times/\operatorname{Comp} K(a,b)$, one copy of the curve*
>
> $$\overline{\mathcal{M}}((\mathcal{P} \underset{\mathbf{Z}}{\otimes} k)^{(\sigma^{-b})}, [\text{Ig}(p^{\max(a,b)})])/\operatorname{Im} K(a,b)$$
>
> *mapping to $\overline{\mathcal{M}}(\mathcal{P} \underset{\mathbf{Z}}{\otimes} k)$ by pr_b (cf. 12.10.3).*

Proof. Applying the general theorem (13.10.4) to $\mathcal{R}$ viewed as

$$([\Gamma(p^n)]/\widetilde{K})^{A\text{-can}},$$

we obtain a radicial, surjective and integral $\overline{\mathcal{M}}(\mathcal{P}\otimes k)$-morphism

$$\overline{\mathcal{M}}(\mathcal{P}\otimes k, [\Gamma(p^n); \det = 1])/\widetilde{K}$$

$$\downarrow$$

$$\left(\overline{\mathcal{M}}(\underset{Z}{\mathcal{P}\otimes A}, \underset{Z}{\mathcal{R}\otimes B[1/N]}) \underset{A\otimes B[1/N]}{\otimes} k\right)^{red}.$$

From the exact sequence of groups

$$0 \to \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \to \widetilde{K} \to K \to 0,$$

the source of this morphism may be written

$$(\overline{\mathcal{M}}(\mathcal{P}\otimes k, [\Gamma(p^n); \det = 1]))\Big/\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}\Big/K.$$

We have a natural radicial, surjective and integral map

$$\overline{\mathcal{M}}(\mathcal{P}\otimes k, [\Gamma(p^n); \det = 1])\Big/\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \longrightarrow \overline{\mathcal{M}}(\mathcal{P}, [\text{bal. } \Gamma_1(p^n); \det = 1])$$

by (13.10.4(2)) applied to the *balanced* subgroup $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

This proves (1). Assertion (2) is simply an exercise, in view of the explicit description (13.11.4) of the irreducible components of $\overline{\mathcal{M}}(\mathcal{P}\otimes k, [\text{bal. } \Gamma_1(p^n); \det = 1])$ and of their exact modular description (13.11.3) as Igusa curves, which together allow us to "follow" the action of K on the set of irreducible components, and to identify the fixer of any (a,b)-component as the subgroup $K(a,b)$ of K, acting on the corresponding Igusa curve through its quotient $\mathrm{Im}\, K(a,b)$. Q.E.D.

COROLLARY 13.12.4. *Let $H \subset (\mathbf{Z}/p^n\mathbf{Z})^\times$ be a subgroup, and suppose that K is the subgroup $H\times H$. If $p = 2$, suppose either $p^n = 2$ or*

$H \equiv 1 \bmod 4$. Then

(1) *If $\begin{pmatrix} H & * \\ O & H \end{pmatrix}$ is balanced, e.g., if either $n = 1$ and H is arbitrary, or if $n \geq 2$ and H is one of the subgroups $1 + (p^\nu)$ with $\nu \geq [n/2]$, then we have a radicial, surjective and integral morphism*

$$\overline{\mathcal{M}}(\mathcal{P}\otimes k, [\text{bal. } \Gamma_1(p^n); \det = 1])\Big/H\times H$$

$$\downarrow$$

$$\overline{\mathcal{M}}(\mathcal{P}\otimes A, \mathcal{R}\otimes B[1/N]) \underset{A\otimes B[1/N]}{\otimes} k$$

whose source and target are both smooth curves over k outside the supersingular points.

(2) *The normalizations of the irreducible components of $\overline{\mathcal{M}}(\mathcal{P}\otimes k, [\text{bal. } \Gamma_1(p^n); \det = 1])/H\times H$ are the following:*

for each (a,b) with $a+b = n$, a,b both ≥ 0, and each $u \in (\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times/$(image of $H \bmod p^{\min(a,b)}$), one copy of

$$\overline{\mathcal{M}}((\mathcal{P}\otimes k)^{(\sigma^{-b})}, [\mathrm{Ig}(p^{\max(a,b)})])\Big/(\text{image of } H \bmod p^{\max(a,b)}),$$

mapping to $\overline{\mathcal{M}}(\mathcal{P}\otimes k)$ by pr_b.

(3) *If $n = 1$, and H is an arbitrary subgroup of $\mathbf{F}_p^\times$, then there are exactly two irreducible components, indexed by $(1,0)$ and $(0,1)$, whose normalizations are*

$$(1,0): \overline{\mathcal{M}}(\mathcal{P}\otimes k, [\mathrm{Ig}(p)])/H \text{ mapping by usual pr to } \overline{\mathcal{M}}(\mathcal{P}\otimes k).$$

$$(0,1): \overline{\mathcal{M}}((\mathcal{P}\otimes k)^{(\sigma^{-1})}, [\mathrm{Ig}(p)])/H \text{ mapping by } \mathrm{pr}_1 \text{ to } \overline{\mathcal{M}}(\mathcal{P}\otimes k).$$

(4) *If $n \geq 2$, and H is the subgroup $1 + (p^\nu)$ with $\nu \geq [n/2]$, then $H \bmod p^{\min(a,b)}$ is always trivial, so the normalizations of the irreducible components are*

for each (a,b) *with* $a+b=n$, a,b *both* ≥ 0, *and for each* $u \in (\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times$, *one copy of* $\overline{\mathfrak{M}}((\mathcal{P}\otimes k)^{(\sigma^{-b})}, [\mathrm{Ig}(p^{\min(\nu,\max(a,b))})])$ *mapping to* $\overline{\mathfrak{M}}(\mathcal{P}\otimes k)$ *by* pr_b.

Proof. Assertion (1) is a special case of (13.12.3), in virtue of the theorem (10.10.3(6)) on balanced subgroups giving *reduced* special fibers outside the supersingular points. Assertions (2), (3), (4) are just spellings-out of the previous theorem in the particular case $K = H\times H$.

Q.E.D.

Chapter 14

APPLICATION TO THEOREMS OF GOOD REDUCTION

(14.1) *General review of vanishing cycles* (cf. [SGA 7], Exp. XIII, 2)

(14.1.1) Fix a prime number p.

Let V be a strictly henselian discrete valuation ring with algebraically closed residue field k of characteristic p, and fraction field K. Let $\overline{K}$ be a separable closure of K. We follow the standard geometric notations

(14.1.1.1) $\quad s = \mathrm{Spec}(k) \hookrightarrow S = \mathrm{Spec}(V) \hookleftarrow \overline{\eta} = \mathrm{Spec}(\overline{K})$.

Fix a finite extension $E/\mathbf{Q}$, and a finite place λ of E of residue characteristic $\ell \neq p$. Let

(14.1.1.2)
$$\begin{array}{ccc} Z & & \\ \downarrow & & \\ f & & \\ \downarrow & & \\ S = \mathrm{Spec}(V) & & \end{array}$$

be a proper morphism, and let $\mathcal{F}$ be a constructible E_λ-sheaf on Z. Form the cartesian diagram

(14.1.1.3)
$$\begin{array}{ccccc} \mathcal{F}_s \overset{\mathrm{dfn}}{=\!=} i^*(\mathcal{F}); & Z_s & \overset{i}{\hookrightarrow} & Z & \overset{\overline{j}}{\hookleftarrow} \; Z_{\overline{\eta}}; \quad \mathcal{F}_{\overline{\eta}} \overset{\mathrm{dfn}}{=\!=} (\overline{j})^*(\mathcal{F}) \\ & \downarrow & & \downarrow & \downarrow \\ & s & \hookrightarrow & S & \hookleftarrow \; \overline{\eta}\,. \end{array}$$

(14.1.2) The derived category version of the Leray spectral sequence for $\bar{j}$ may be written

$$\begin{array}{ccc} R\Gamma(Z_{\bar{\eta}}, \mathcal{F}_{\bar{\eta}}) = R\Gamma(Z, R(\bar{j})_*\mathcal{F}_{\bar{\eta}}) \\ \Big\| \\ R\Gamma(Z_s, i^*R(\bar{j})_*\mathcal{F}_{\bar{\eta}}) \end{array} \qquad (14.1.2.1)$$

the vertical isomorphism because Z is proper over S. Because $\mathcal{F}_{\bar{\eta}}$ is by definition $(\bar{j})^*(\mathcal{F})$, the natural morphism of adjunction yields an arrow

$$\begin{array}{ccc} \mathcal{F} & \longrightarrow & \bar{j}_*(\bar{j})^*\mathcal{F} = \bar{j}_*\mathcal{F}_{\bar{\eta}} \\ & \searrow & \downarrow \\ & & R(\bar{j})_*\mathcal{F}_{\bar{\eta}} \end{array} \qquad (14.1.2.2)$$

whence, by restriction to the special fiber, a morphism of complexes on Z_s

$$\mathcal{F}_s = i^*\mathcal{F} \to i^*R(\bar{j})_*\mathcal{F}_{\bar{\eta}}. \qquad (14.1.2.3)$$

By definition, its mapping cone, with $\mathcal{F}_s$ viewed as lying in degree -1,

$$\mathcal{F}_s \to i^*R(\bar{j})_*\mathcal{F}_{\bar{\eta}} \qquad (14.1.2.4)$$

is denoted

$$R\Phi(\mathcal{F}), \quad \text{or} \quad R\Phi_{Z/S}(\mathcal{F}). \qquad (14.1.2.5)$$

The complex $R\Psi_{X/S}(\mathcal{F})$ on Z_s is defined by

$$R\Psi_{X/S}(\mathcal{F}) \overset{\text{dfn}}{=\!=} i^*R(\bar{j})_*\mathcal{F}_{\bar{\eta}}. \qquad (14.1.2.6)$$

The short exact sequence of complexes on Z_s

$$0 \to R\Psi_{Z/S}(\mathcal{F}) \to R\Phi_{Z/S}(\mathcal{F}) \to \left(\mathcal{F}_s, \begin{array}{c}\text{placed in}\\ \text{degree } -1\end{array}\right) \to 0 \qquad (14.1.2.7)$$

gives an exact sequence of sheaves on Z_s

$$0 \to R^{-1}\Phi_{Z/S}(\mathcal{F}) \to \mathcal{F}_s \to i^*(\bar{j})_*\mathcal{F}_{\bar{\eta}} \to R^0\Phi_{Z/S}(\mathcal{F}) \to 0 \qquad (14.1.2.8)$$

and, for all integers $i \geq 1$, an isomorphism of sheaves on Z_s

$$R^i\Psi_{Z/S}(\mathcal{F}) \xrightarrow{\sim} R^i\Phi_{Z/S}(\mathcal{F}). \qquad (14.1.2.9)$$

Passing to cohomology on Z_s, the above exact sequence of complexes gives rise to a long exact cohomology sequence

$$\begin{array}{c} \cdots \to H^i(Z_s, \mathcal{F}_s) \to H^i(Z_s, R\Psi_{Z/S}(\mathcal{F})) \to H^i(Z_s, R\Phi_{Z/S}(\mathcal{F})) \to \\ \Big\| \\ H^i(Z_{\bar{\eta}}, \mathcal{F}_{\bar{\eta}}). \end{array} \qquad (14.1.2.10)$$

Thus it is only the cohomology groups

$$H^i(Z_s, R\Phi_{Z/S}(\mathcal{F})) \qquad (14.1.2.11)$$

which prevent the specialization map

$$H^i(Z_s, \mathcal{F}_s) \to H^i(Z_{\bar{\eta}}, \mathcal{F}_{\bar{\eta}}) \qquad (14.1.2.12)$$

from being an isomorphism for all i.

(14.1.3) The inertia group

$$I_K = \mathrm{Gal}(\bar{K}/K)$$

operates naturally on the entire situation, trivially on $(Z,\mathcal{F})$ and on $(Z_s,\mathcal{F}_s)$, highly non-trivially on $(Z_{\overline{\eta}},\mathcal{F}_{\overline{\eta}})$. In particular the above exact sequence is I_K-equivariant, with I_K operating *trivially* on $H^*(Z_s,\mathcal{F}_s)$.

(14.1.4) DEFINITION. Let L/K be a finite separable extension of K. An E_λ-subspace of $H^i(Z_{\overline{\eta}},\mathcal{F}_{\overline{\eta}})$ is said to have "good reduction over L" if it is *stable* by the subgroup $I_L \subset I_K$, and if I_L operates trivially on it.

For example, *any* subspace of

$$\text{Image}\,(H^i(Z_s,\mathcal{F}_s) \to H^i(Z_{\overline{\eta}},\mathcal{F}_{\overline{\eta}}))$$

has good reduction over K itself. We will be particularly interested in the case $i = 1$. So it will be very useful to know when the specialization map

$$H^1(Z_s,\mathcal{F}_s) \to H^1(Z_{\overline{\eta}},\mathcal{F}_{\overline{\eta}})$$

is *injective*.

LEMMA 14.1.5. *Suppose we have a commutative diagram*

$$\begin{array}{ccc} \mathcal{F};\ Z & \xleftarrow{\ \pi\ } & W;\ \pi^*\mathcal{F} \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle g} & \\ & S & \end{array}$$

with $(\mathcal{F},Z,f,S)$ *as in (14.1.1) above, and* π *finite. If* $\pi_{\overline{\eta}}: W_{\overline{\eta}} \to Z_{\overline{\eta}}$ *is an isomorphism, then we have canonically on* Z_s,

$$R\Psi_{Z/S}(\mathcal{F}) = (\pi_s)_* R\Psi_{W/S}(\pi^*\mathcal{F})\,.$$

Proof. We have a commutative diagram with both squares cartesian

$$\begin{array}{ccccc} W_s & \xrightarrow{i_W} & W & \xleftarrow{\bar{j}_W} & W_{\overline{\eta}} \\ \downarrow{\scriptstyle \pi_s} & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi_{\overline{\eta}}} \\ Z_s & \xrightarrow{i_Z} & Z & \xleftarrow{\bar{j}_Z} & Z_{\overline{\eta}}\,. \end{array}$$

By definition,

$$(\pi_s)_* R\Psi_{W/S}(\pi^*\mathcal{F})$$

$$= (\pi_s)_*(i_W)^* R(\bar{j}_W)_*((\bar{j}_W)^*\pi^*\mathcal{F})$$

which, by the proper base-change theorem applied to $(\pi_s)_* = R(\pi_s)_*$, gives

$$= (i_Z)^* R(\pi)_* R(\bar{j}_W)_*((\pi_{\overline{\eta}})^*(\bar{j}_Z)^*\mathcal{F})$$

$$= (i_Z)^* R(\bar{j}_Z)_* R(\pi_{\overline{\eta}})_*(\pi_{\overline{\eta}})^*(\bar{j}_Z)^*\mathcal{F}$$

$$= (i_Z)^* R(\bar{j}_Z)_*((\bar{j}_Z)^*\mathcal{F}) = R\Psi_{Z/S}(\mathcal{F})\,. \qquad \text{Q.E.D.}$$

LEMMA 14.1.6. *In the situation of the previous lemma (14.1.5), suppose that a finite group* G *acts* k*-linearly on the special fiber* W_s *of* W, *that* G *acts trivially on* Z_s, *and that the morphism* $\pi_s: W_s \to Z_s$ *is* G*-equivariant, and induces by passage to quotients a radicial surjective integral morphism*

$$W_s/G \to Z_s\,.$$

Then we have canonical isomorphisms on Z_s

1) $\mathcal{F}_s \xrightarrow{\sim} ((\pi_s)_*\pi_s^*\mathcal{F}_s)^G$.

2) $R\Psi_{Z/S}(\mathcal{F}) \xrightarrow{\sim} (\pi_s)_* R\Psi_{W/S}(\pi^*\mathcal{F})$.

Proof. Because the etale topology is insensitive to radicial surjective integral morphisms, the situation for etale sheaves on Z_s is the same as

if Z_S actually were the quotient W_S/G. This makes 1) apparent. Assertion 2) has already been proven in the previous lemma. Q.E.D.

COROLLARY 14.1.7. *In the situation of the previous lemma (14.1.6), the two specialization maps*

$$H^i(Z_S, \mathcal{F}_S) \to H^i(Z_{\overline{\eta}}, \mathcal{F}_{\overline{\eta}})$$
$$H^i(W_S, (\pi_S)^*\mathcal{F}_S) \to H^i(W_{\overline{\eta}}, \mathcal{F}_{\overline{\eta}})$$

sit in a commutative diagram

$$\begin{array}{ccc}
H^i(Z_S, \mathcal{F}_S) & \longrightarrow & H^i(Z_{\overline{\eta}}, \mathcal{F}_{\overline{\eta}}) \\
\| & & \\
H^i(Z_S, ((\pi_S)_*(\pi_S)^*\mathcal{F}_S)^G) & & \Big\uparrow (\pi_{\overline{\eta}})^* \\
\| & & \\
H^i(W_S, (\pi_S)^*\mathcal{F}_S)^G & & \\
\downarrow & & \\
H^i(W_S, (\pi_S)^*\mathcal{F}_S) & \longrightarrow & H^i(W_{\overline{\eta}}, \mathcal{F}_{\overline{\eta}}) .
\end{array}$$

COROLLARY 14.1.8. *In the situation of the previous lemma (14.1.6), if the specialization map*

$$H^1(W_S, (\pi_S)^*\mathcal{F}_S) \to H^1(W_{\overline{\eta}}, \mathcal{F}_{\overline{\eta}})$$

is injective, then the specialization map

$$H^1(Z_S, \mathcal{F}_S) \to H^1(Z_{\overline{\eta}}, \mathcal{F}_{\overline{\eta}})$$

is also injective.

(14.1.9) We now consider the effect of extension of the ground field. Thus let L/K be a finite separable extension of K inside $\overline{K}$, and let V_L denote the integral closure of V in L. Thus V_L is itself a strictly henselian discrete valuation ring, finite over V, with the same residue field k as V itself. Let us write

$$t = \mathrm{Spec}(k) \hookrightarrow T = \mathrm{Spec}(V_L) \hookleftarrow \overline{\eta} = \mathrm{Spec}(\overline{K}) ,$$

and form the cartesian diagram

$$\begin{array}{ccc}
\mathcal{F}\,;\, Z & \xleftarrow{\lambda} & Z_T\,;\, \lambda^*\mathcal{F} \\
\downarrow & & \downarrow \\
S & \xleftarrow{} & T .
\end{array}$$

LEMMA 14.1.9.1. *In the above situation (14.1.9), $Z_S = (Z_T)_t$, and we have natural equalities*

1) $(\lambda^*\mathcal{F})_t = \lambda^*\mathcal{F}|(Z_T)_t = \mathcal{F}|Z_S = \mathcal{F}_S$.

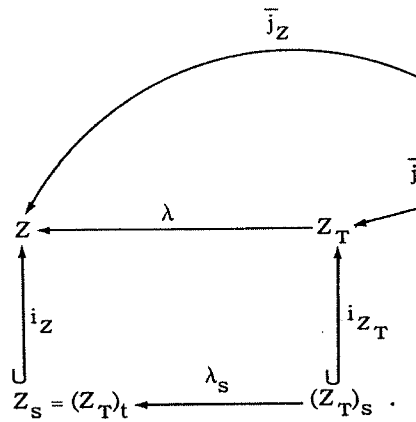
2) $R\Psi_{Z_T/T}(\lambda^*\mathcal{F}) = R\Psi_{Z/S}(\mathcal{F})$.

3) $R\Phi_{Z_T/T}(\lambda^*\mathcal{F}) = R\Phi_{Z/S}(\mathcal{F})$.

Proof. Consider λ as an S-morphism

$$\begin{array}{ccc}
Z & \xleftarrow{\lambda} & Z_T \\
 & \searrow \quad \swarrow & \\
 & S & \dashleftarrow \; T .
\end{array}$$

The map $\lambda_S : (Z_T)_S \to Z_S$ is surjective, radicial and finite, because $V_L/\pi_K V_L$ is artin local with residue field k. But S and T have the *same* $\overline{\eta} = \mathrm{Spec}(\overline{K})$, so we have a commutative diagram



Thus we readily calculate

$$\begin{aligned} R\Psi_{Z/S}(\mathcal{F}) &= (i_Z)^*R(\bar{j}_Z)_*((\bar{j}_Z)^*\mathcal{F}) \\ &= (i_Z)^*R\lambda_*R(\bar{j}_{Z_T})_*((\bar{j}_{Z_T})^*(\lambda^*\mathcal{F})) \\ &= R(\lambda_s)_*(i_{Z_T})^*R(\bar{j}_{Z_T})_*((\bar{j}_{Z_T})^*(\lambda^*\mathcal{F})) \\ &= R(\lambda_s)_*(\lambda_s)^*(R\Psi_{Z_T/T}(\lambda^*\mathcal{F})) \\ &= R\Psi_{Z_T/T}(\lambda^*\mathcal{F}) . \end{aligned}$$

The third from last equality is proper base change for λ. The last two equalities hold because λ_s is surjective, radicial and finite, so $R(\lambda_s)_* = (\lambda_s)_*$ and λ_s^* are inverse equivalences of categories.

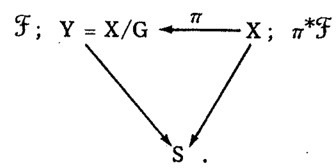
Similarly,

$$\begin{array}{c} R\Phi_{Z/S}(\mathcal{F}) = [\mathcal{F}|Z_s \to R\Psi_{Z/S}(\mathcal{F})] \\ \Vert \\ R\Phi_{Z_T/T}(\mathcal{F}) = [\lambda^*\mathcal{F}|(Z_T)_t \to R\Psi_{Z_T/T}(\lambda^*\mathcal{F})] . \end{array}$$

Q.E.D.

(14.1.10) We now consider the effect of a finite group of operators.

LEMMA 14.1.10.1. *Let* V *be a strictly henselian discrete valuation ring,* X *a projective scheme over* S = Spec (V) *on which a finite group* G *operates* V*-linearly,* Y *the quotient* X/G, *and* $\mathcal{F}$ *a constructible* E_λ*-sheaf on* Y :



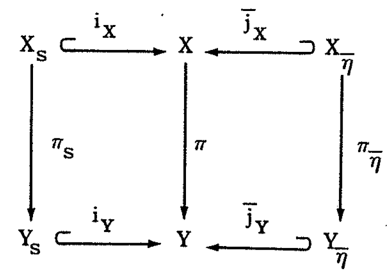
Then we have canonical isomorphisms on Y_s

1) $\mathcal{F}_s = ((\pi_s)_*(\pi_s)^*\mathcal{F}_s)^G$

2) $R\Psi_{Y/S}(\mathcal{F}) = ((\pi_s)_*R\Psi_{X/S}(\pi^*\mathcal{F}))^G$

3) $R\Phi_{Y/S}(\mathcal{F}) = ((\pi_s)_*R\Phi_{X/S}(\pi^*\mathcal{F}))^G$.

Proof. The first assertion holds because the map $X_s/G \to Y_s$ is radicial, surjective and integral. By the definition of $R\Phi$ as a mapping cone, assertion 3) follows easily once we know 1) and 2). To prove 2), we compute, using the diagram



$$\begin{aligned} (\pi_s)_*R\Psi_{X/S}(\pi^*\mathcal{F}) &= (\pi_s)_*(i_X)^*R(\bar{j}_X)_*((\bar{j}_X)^*\pi^*\mathcal{F})) \\ &= (i_Y)^*\pi_*R(\bar{j}_X)_*((\pi_{\bar{\eta}})^*(\bar{j}_Y)^*(\mathcal{F})) \\ &= (i_Y)^*R(\bar{j}_Y)_*((\pi_{\bar{\eta}})_*(\pi_{\bar{\eta}})^*(\bar{j}_Y)^*(\mathcal{F})) . \end{aligned}$$

Applying the exact functor "G-invariants", we find

$$((\pi_S)_* R\Psi_{X/S}(\pi^*\mathcal{F}))^G = (i_Y)^* R(\bar{j}_Y)_* (((\pi_{\bar{\eta}})_* (\pi_{\bar{\eta}})^* (\bar{j}_Y)^* (\mathcal{F}))^G) .$$

Because $\pi_{\bar{\eta}} : X_{\bar{\eta}} \to Y_{\bar{\eta}}$ makes $X_{\bar{\eta}}/G \xrightarrow{\sim} Y_{\bar{\eta}}$, we have, for any constructible E_λ-sheaf $\mathcal{G}$ on $Y_{\bar{\eta}}$,

$$\mathcal{G} \xrightarrow{\sim} ((\pi_{\bar{\eta}})_* (\pi_{\bar{\eta}})^* \mathcal{G})^G .$$

Taking for $\mathcal{G}$ the sheaf $(\bar{j}_Y)^*(\mathcal{F})$, we find the required isomorphism 2).

Q.E.D.

COROLLARY 14.1.11. *Hypotheses as in (14.1.10.1) above, the long exact cohomology sequence with its I_K-action*

$$\to H^i(Y_S, \mathcal{F}_S) \to H^i(Y_{\bar{\eta}}, \mathcal{F}_{\bar{\eta}}) \to H^i(Y_S, R\Phi_{Y/S}(\mathcal{F})) \to$$

is canonically isomorphic to the G-invariants in the long exact cohomology sequence

$$\to H^i(X_S, \pi_S^* \mathcal{F}_S) \to H^i(X_{\bar{\eta}}, (\pi_{\bar{\eta}})^* \mathcal{F}_{\bar{\eta}}) \to H^i(X_S, R\Phi_{X/S}(\pi^*\mathcal{F})) \to .$$

COROLLARY 14.1.12. *Hypotheses as in (14.1.10.1) above, suppose that*

$$R^i\Phi_{X/S}(\pi^*\mathcal{F}) = \begin{cases} 0 \text{ for } i \neq 1 \\ \text{a punctual sheaf, for } i = 1 . \end{cases}$$

Then we have

$$R^i\Phi_{Y/S}(\mathcal{F}) = \begin{cases} 0 \text{ for } i \neq 1 \\ \text{a punctual sheaf, for } i = 1 . \end{cases}$$

In particular, the specialization maps

$$H^1(Y_S, \mathcal{F}_S) \to H^1(Y_{\bar{\eta}}, \mathcal{F}_{\bar{\eta}})$$

and

$$H^1(X_S, \pi_S^* \mathcal{F}_S) \to H^1(X_{\bar{\eta}}, (\pi_{\bar{\eta}})^* \mathcal{F}_{\bar{\eta}})$$

are both injective.

(14.2) *Application to curves*

(14.2.1) We now suppose that V is a mixed characteristic strictly henselian discrete valuation ring with algebraically closed residue field k of characteristic p, and that we are given the following geometric data once and for all.

1) a proper and smooth curve with geometrically connected fibers

$$\begin{array}{c} Y \\ \downarrow \\ S = \mathrm{Spec}(V) . \end{array}$$

2) a closed subscheme ("the cusps") $D \subset Y$, finite etale over S.
3) a finite extension $E/\mathbf{Q}$, a finite place λ of E of residue characteristic $\ell \neq p$, and a constructible E_λ-sheaf $\mathcal{F}$ on Y, which is *lisse* when restricted to D.

Notice that, V being of generic characteristic zero, $\mathcal{F}$ is automatically *tamely ramified* along D.

(14.2.2) We will try to make do with the following convention; given *any* Y-scheme

$$\begin{array}{c} X \\ \downarrow g \\ Y , \end{array}$$

we will denote simply by $\mathcal{F}$ the sheaf $g^*(\mathcal{F})$ on X, (the usual convention when dealing with the constant sheaf).

(14.2.3) Now suppose we are given

4) a finite galois extension L/K, with galois group G;

5) a finite $Y \underset{V}{\otimes} V_L$-scheme which is normal

$$\begin{array}{c} X \\ \downarrow \rho \\ Y \underset{V}{\otimes} V_L \end{array},$$

6) a finite group Γ, given with a surjective homomorphism

$$\Gamma \xrightarrow{\text{"det"}} G,$$

and a Y-linear action of Γ on X such that $\gamma \in \Gamma$ acts $\det(\gamma)$-semilinearly. We denote by $SL \subset \Gamma$ the subgroup of elements having trivial "det" : $\Gamma \twoheadrightarrow G$.

THEOREM 14.2.4. *Hypotheses as in 14.2.1-2-3 above, suppose that* X *satisfies the following conditions*:

1) X *is flat over* V_L

2) *outside a finite set of* k*-valued "supersingular points" in the special fiber, all of which lie over* $Y - D$, X *is a smooth curve over* V_L

3) *the special fiber* $X \underset{V_L}{\otimes} k$ *is reduced*

4) *the scheme of cusps of* X, *defined as* $(\rho^{-1}(D))^{\text{red}}$, *is finite etale over* V_L.

Then we have

1) *The sheaves* $R^i\Phi_{X/V_L}(\mathcal{F})$ *vanish for* $i \neq 1$, *and* $R^1\Phi_{X/V_L}(\mathcal{F})$ *is a punctual sheaf, supported at the supersingular points.*

2) *For any subgroup* $\Gamma_1 \subset \Gamma$, *denote by* $V_1 \subset V_L$ *the subring* $(V_L)^{\det(\Gamma_1)}$, *and by* X_1 *the quotient* X/Γ_1. *Then* X_1 *is a normal scheme, finite over* $Y \underset{V}{\otimes} V_1$, *and the specialization map*

$$H^1((X/\Gamma_1)_s, \mathcal{F}) \to H^1((X/\Gamma_1)_{\overline{\eta}}, \mathcal{F})$$

is injective.

3) *For any subgroup* $\Gamma_1 \subset \Gamma$, *the specialization maps for* X/Γ_1 *over* V_1 *and for* X *over* V_L *are related by an* I_L*-equivariant commutative diagram*

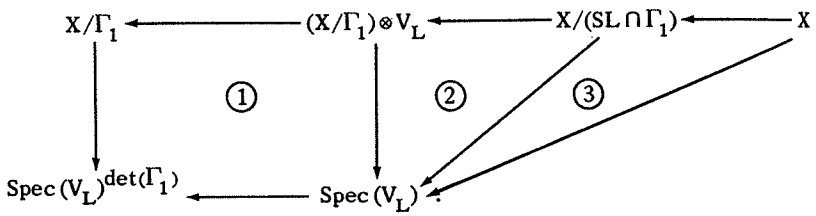
$$\begin{array}{ccc} H^1((X/\Gamma_1)_s, \mathcal{F}) & \hookrightarrow & H^1((X/\Gamma_1)_{\overline{\eta}}, \mathcal{F}) \\ \wr\downarrow & & \wr\downarrow \\ H^1(X_s/\Gamma_1, \mathcal{F}) & & H^1(X_{\overline{\eta}}/SL \cap \Gamma_1, \mathcal{F}) \\ \wr\downarrow & & \wr\downarrow \\ H^1(X_s, \mathcal{F})^{\Gamma_1} & & H^1(X_{\overline{\eta}}, \mathcal{F})^{SL \cap \Gamma_1} \\ \downarrow & & \downarrow \\ H^1(X_s, \mathcal{F}) & \hookrightarrow & H^1(X_{\overline{\eta}}, \mathcal{F}). \end{array}$$

4) *If* Γ_2 *is any subgroup of* Γ *which normalizes* Γ_1 *and which has* "det"(Γ_2) *trivial, then* Γ_2 *operates naturally and* $I_{L^{\det(\Gamma_1)}}$*-equivariantly (resp.* I_L*-equivariantly) on the top (resp. bottom) row of the above diagram, and the entire diagram is* Γ_2*-equivariant.*

Proof. We begin with 1). The sheaf $\mathcal{F}$ on X is lisse on X-{cusps}, and it is lisse when restricted to the cusps. Because we are over a base of generic characteristic zero, and the cusps are finite etale over the base, $\mathcal{F}$ is automatically tamely ramified along the cusps of X. Therefore ([SGA 7], Exp XIII, 2.1.11) all the $R^i\Phi_{X/V_L}(\mathcal{F})$ vanish along the cusps. Over X-{cusps}, $\mathcal{F}$ is lisse, and X-{cusps} is lisse over the base $\text{Spec}(V_L)$ outside a finite set of "supersingular" points in the special fiber. Therefore all the sheaves $R^i\Phi_{X/V_L}(\mathcal{F})$ are punctual, supported at the supersingular points. For dimension reasons, $R^i\Phi$ vanishes for $i \geq 2$. To see that $R^{-1}\Phi$ and $R^0\Phi$ vanish at the supersingular points, it suffices, $\mathcal{F}$ being lisse there, to show that $X \to \text{Spec}(V_L)$ is locally

zero-acyclic ([SGA 4], Exp. XV, 1.11) but this follows from its being flat with reduced geometric fibers ([SGA 4], Exp. XV, 4.1). This proves assertion 1).

We prove assertions 2) and 3) together. Consider the diagram



We apply (14.1.11, 12) to the triangle marked ③, then we apply (14.1.7) to the triangle marked ②, the group in this case being $\Gamma_1/SL \cap \Gamma_1 \xrightarrow{\sim} \det(\Gamma_1)$, and finally we apply (14.1.9.1) to the cartesian square marked ①.

Assertion 4) is clear by functoriality. Q.E.D.

COROLLARY 14.2.5. (Numerical criterion for good reduction). *Let Γ_2 be a subgroup of Γ which normalizes Γ_1 and has $\det(\Gamma_2)$ trivial. Let Σ be any E_λ-rational set of $\bar{E}_\lambda$-representations of Γ_2. For any finite-dimensional E_λ-representation M of Γ_2, let us denote by $M(\Sigma)$ the E_λ-subrepresentation of M consisting of the sum of all isotypical components of type $\sigma \in \Sigma$. Then*

1) *We always have an inequality of dimensions*

$$\dim H^1(X_S, \mathcal{F})^{\Gamma_1}(\Sigma) \leq \dim H^1(X_{\overline{\eta}}, \mathcal{F})^{SL \cap \Gamma_1}(\Sigma) .$$

2) *If this inequality is an equality, then the inclusion*

$$H^1(X_S, \mathcal{F})^{\Gamma_1} = H^1((X/\Gamma_1)_S, \mathcal{F}) \hookrightarrow H^1((X/\Gamma_1)_{\overline{\eta}}, \mathcal{F}) = H^1(X_{\overline{\eta}}, \mathcal{F})^{SL \cap \Gamma_1}$$

induces an isomorphism of Σ-components

$$H^1((X/\Gamma_1)_S, \mathcal{F})(\Sigma) \xrightarrow{\sim} H^1((X/\Gamma_1)_{\overline{\eta}}, \mathcal{F})(\Sigma) ;$$

in particular the subspace

$$H^1((X/\Gamma_1)_{\overline{\eta}}, \mathcal{F})(\Sigma)$$

has good reduction over the field $(L)^{\det(\Gamma_1)}$.

Proof. Simply apply the exact functor $M \mapsto M(\Sigma)$ to the commutative diagram

$$\begin{array}{ccccc} H^1((X/\Gamma_1)_S, \mathcal{F}) & \simeq & H^1(X_S, \mathcal{F})^{\Gamma_1} & \hookrightarrow & H^1(X_S, \mathcal{F}) \\ \downarrow & & \downarrow & & \downarrow \\ H^1((X/\Gamma_1)_{\overline{\eta}}, \mathcal{F}) & \simeq & H^1(X_{\overline{\eta}}, \mathcal{F})^{SL \cap \Gamma_1} & \hookrightarrow & H^1(X_{\overline{\eta}}, \mathcal{F}) . \end{array}$$

Q.E.D.

(14.3) *Application to modular curves: explicitation of the numerical criterion*

(14.3.1) Fix an integer $N \geq 1$ prime to p, and a subgroup

$$\Gamma \subset GL(2, Z/NZ) .$$

Denote by B the ring

$$B = (Z[\zeta_N])^{\det(\Gamma)} \subset Z[\zeta_N] .$$

We suppose that the moduli problem

$$\mathcal{P} = ([\Gamma(N)]/\Gamma)^{B\text{-can}} \otimes_B B[1/N] \quad \text{on} \quad (Ell/B[1/N])$$

is representable. As we have seen, the compactified moduli scheme

$$\begin{array}{c} \overline{\mathcal{M}}(\mathcal{P}) \\ \downarrow \\ \mathrm{Spec}\,(B[1/N]) \end{array}$$

is a proper and smooth curve over $B[1/N]$ with geometrically connected fibers, in which

$$(\overline{\mathcal{M}}(\mathcal{P}) - \mathcal{M}(\mathcal{P}))^{\mathrm{red}} = \mathrm{Cusps}\,(\mathcal{P})$$

is finite etale over $B[1/N]$.

(14.3.2) Let us temporarily denote by

$$\begin{array}{ccc} E_{\mathrm{univ}} & & \\ \downarrow{\scriptstyle f_{\mathrm{univ}}} & & \\ \mathcal{M}(\mathcal{P}) & \xrightarrow{\ j\ } & \overline{\mathcal{M}}(\mathcal{P}) \end{array} \qquad (14.3.2.1)$$

the universal elliptic curve carried by $\mathcal{M}(\mathcal{P})$. Fix a prime ℓ dividing N (to assure that ℓ is invertible on $\overline{\mathcal{M}}(\mathcal{P})$, and that $\ell \neq p$). Then

$$R^1 f_{\mathrm{univ}_*} \mathbf{Q}_\ell \qquad (14.3.2.2)$$

is a *lisse* $\mathbf{Q}_\ell$-sheaf of rank two on $\mathcal{M}(\mathcal{P})$, and on every geometric fiber of $\mathcal{M}(\mathcal{P}) \to \mathrm{Spec}\,(B[1/N])$, its geometric monodromy group is known to be an open subgroup of $SL(2, \mathbf{Q}_\ell)$. This sheaf is automatically tamely ramified along the cusps.

PROPOSITION 14.3.3. *If -1 operates without fixed points on the space of cusp-labels for $\Gamma \cap SL(2, Z/NZ)$, then the geometric local monodromy at the cusps of $R^1 f_{\mathrm{univ}_*} \mathbf{Q}_\ell$ on $\mathcal{M}(\mathcal{P})$ is unipotent of infinite order.*

Proof. Because the sheaf $R^1 f_{\mathrm{univ}_*} \mathbf{Q}_\ell$ is tame along the cusps, and the cusps are finite etale over the base $\mathrm{Spec}\,(B[1/N])$ which is connected, it

suffices to prove this on a *single geometric fiber* of $\mathcal{M}(\mathcal{P}) \to \mathrm{Spec}\,(B[1/N])$. Choose the complex embedding

$$B[1/N] \hookrightarrow Z[\zeta_N, 1/N] \hookrightarrow \mathbf{C}, \quad \zeta_N \mapsto \exp(2\pi i/N),$$

and work on the corresponding $\mathcal{M}(\mathcal{P}) \otimes \mathbf{C}$. Then we have

$$\mathcal{M}(\mathcal{P}) \underset{B[1/N]}{\otimes} \mathbf{C} = \mathcal{M}(\mathcal{P} \underset{B[1/N]}{\otimes} Z[\zeta_N, 1/N]) \underset{Z[\zeta_N, 1/N]}{\otimes} \mathbf{C},$$

so we may assume, to begin with, that $\Gamma \subset SL(2, Z/NZ)$.

On the complex manifold $(\mathcal{M}(\mathcal{P}) \otimes \mathbf{C})^{\mathrm{an}}$, we have, canonically,

$$(R^1 f_{\mathrm{univ}_*} \mathbf{Q}_\ell)^{\mathrm{an}} \simeq (R^1 f^{\mathrm{an}}_{\mathrm{univ}_*} Z) \otimes \mathbf{Q}_\ell,$$

so it suffices to look at the integral local monodromy at the cusps. At each cusp, the local monodromy is given by the transpose inverse of an element

$$A \in SL(2, Z), \quad A \bmod N \text{ lies in } \Gamma.$$

The element A^2 is unipotent of infinite order (because over a double covering of a punctured neighborhood of each cusp, the universal curve becomes a Tate curve $\mathrm{Tate}(q)$ viewed over $\mathbf{C}((q^{1/f}))$, for some divisor f of $2N$).

Therefore A has eigenvalues ± 1, necessarily equal because A lies in $SL(2, Z)$. So

$$A = \pm U$$

for some unipotent $U \in SL(2, Z)$. If $A = U$, we are done.

If not, in a suitable basis of $(Z)^2$, we have

$$A = \begin{pmatrix} -1 & a \\ 0 & -1 \end{pmatrix}.$$

In this case, the cusp-label $(1, 0)$ satisfies

$$(1, 0)A = -(1, 0).$$

Because A mod N lies in Γ, this says that -1 fixes $(1,0)$ viewed as a cusp-label for Γ. Q.E.D.

REMARK. Recall (10.13.8) that this same condition on -1 guarantees the existence of $\underline{\omega}$ on $\bar{\mathcal{M}}(\mathcal{P})$. The two conditions, namely existence of $\underline{\omega}$ on $\bar{\mathcal{M}}(\mathcal{P})$ and unipotence at infinity of $R^1 f_{univ_*}\mathbf{Q}_\ell$, seem to be equivalent, but we do not know how to prove this.

(14.3.4) For the rest of this chapter, we will *assume* that $\mathcal{P}$ satisfies the additional hypothesis:

(14.3.4.1) ± 1 operates freely on the cusp-labels for $\Gamma \cap SL(2, \mathbf{Z}/N\mathbf{Z})$.

Then for every $d \geq 0$, the sheaf

$$\text{(14.3.4.2)} \qquad \mathcal{F}(d) \overset{\text{dfn}}{=\!=} j_*(\mathrm{Symm}^d(R^1 f_{univ_*}\mathbf{Q}_\ell)) \quad \text{on} \quad \bar{\mathcal{M}}(\mathcal{P})$$

is lisse on $\mathcal{M}(\mathcal{P})$ of rank $d+1$, and its restriction to $\mathrm{Cusps}(\mathcal{P})$ is a lisse sheaf of rank one. Because we are in mixed characteristic, $\mathcal{F}(d)$ is automatically tamely ramified along the cusps.

We will make constant use of the following *fundamental property* of the sheaves $\mathcal{F}(d)$.

PROPOSITION 14.3.4.3. *Let* k *be an algebraically closed field,*

$$B[1/N] \to k$$

a ring homomorphism, C *a proper smooth connected curve over* k,

$$\begin{array}{c} C \\ \downarrow \pi \\ \bar{\mathcal{M}}(\mathcal{P}) \otimes k \end{array}$$

a finite morphism, $D \subset C$ *the inverse image of the cusps,*

$$C - D \overset{j}{\hookrightarrow} C$$

the inclusion. Then

(1) *For* $d = 0$, $\mathcal{F}(0)$ *is the constant sheaf* $\mathbf{Q}_\ell$, $H^0(C, \mathbf{Q}_\ell) \simeq \mathbf{Q}_\ell$, $H^2(C, \mathbf{Q}_\ell) \simeq \mathbf{Q}_\ell(-1)$.

(2) *For* $d > 0$, $\pi^*\mathcal{F}(d) \xrightarrow{\sim} j_* j^* \pi^* \mathcal{F}(d)$ *is lisse on* $C - D$, *and tame along* D. *It is an absolutely irreducible representation of* $\pi_1(C-D)$, *and we have* $H^0(C, \pi^*\mathcal{F}(d)) = H^2(C, \pi^*\mathcal{F}(d)) = 0$.

Proof. This is immediate from the fact that $\mathcal{F}(1)$ on $\bar{\mathcal{M}}(\mathcal{P}) \otimes k$ has geometric monodromy open in $SL(2, \mathbf{Q}_\ell)$, and unipotent non-trivial local monodromy around each cusp; because $\pi_1(C-D) \to \pi_1(\mathcal{M}(\mathcal{P}) \otimes k)$ has image of finite index, the same statements hold for $\pi^*(\mathcal{F}(1))$ on C itself. The symmetric power Symm^d, $d \geq 1$, of any two-dimensional representation whose image is open in $SL(2, \mathbf{Q}_\ell)$ is irreducible and non-trivial. The symmetric powers of any non-trivial unipotent in $SL(2, \mathbf{Q}_\ell)$ all have a single Jordan block, so one-dimensional spaces of invariants. Q.E.D.

(14.3.5) We will now apply the theory of the preceding section to this situation. Fix a ring homomorphism

$$B[1/N] \to k = \text{an algebraic closure of } \mathbf{F}_p.$$

Because $B[1/N]$ is finite etale over $\mathbf{Z}[1/N]$, this extends uniquely to a ring homomorphism

$$B[1/N] \to W(k).$$

We take

$$V = W(k), \text{ fraction field denoted } K$$

$$Y = \bar{\mathcal{M}}(\mathcal{P}) \underset{B[1/N]}{\otimes} W(k)$$

$\mathcal{F}(d)$ on Y = the sheaf $\mathcal{F}(d)$ on $\bar{\mathcal{M}}(\mathcal{P})$, pulled back to Y

$$L = \text{the galois extension } K(\zeta_{p^n}) \text{ of } K, \text{ with}$$

$$\text{galois group } G = \mathrm{Gal}(L/K) \xrightarrow{\sim} (\mathbf{Z}/p^n\mathbf{Z})^\times$$

$$X = \text{the scheme } \bar{\mathfrak{M}}(\mathcal{P}, [\text{bal. } \Gamma_1(p^n)]^{\text{can}}) \underset{B[1/N,\zeta_{p^n}]}{\otimes} (V_L)$$

$$\downarrow$$

$$Y \otimes V_L$$

Γ = the group $(\mathbf{Z}/p^n\mathbf{Z})^\times \times (\mathbf{Z}/p^n\mathbf{Z})^\times$, operating modularly on X by its standard action

$$(P, Q) \xmapsto{\alpha,\beta} (\alpha P, \beta Q)$$

on the moduli problem $[\text{bal. } \Gamma_1(p^n)]$

$$\Gamma \xrightarrow{\det} G \simeq (\mathbf{Z}/p^n\mathbf{Z})^\times \text{ is } (\alpha, \beta) \longmapsto \alpha\beta .$$

Then all the hypotheses of the general theorem (14.2.4) are satisfied. Because Γ is *abelian*, we may take for Γ_2 the anti-diagonal subgroup

$$\Delta = \{(\alpha, \alpha^{-1}) | \alpha \in (\mathbf{Z}/p^n\mathbf{Z})^\times\} \subset \Gamma ,$$

which operates $Y \otimes V_L$-linearly on X, and commutes with the det-semilinear action of Γ.

The quotient

$$X/(1 \times (\mathbf{Z}/p^n\mathbf{Z})^\times)$$

is none other than the Y-scheme

$$\bar{\mathfrak{M}}(\mathcal{P}, [\Gamma_1(p^n)]) \underset{B[1/N]}{\otimes} W(k)$$

$$\downarrow$$

$$Y = \bar{\mathfrak{M}}(\mathcal{P}) \underset{B[1/N]}{\otimes} W(k) ,$$

and the action of Δ on this quotient is by the usual action

$$P \xmapsto{(\alpha,\alpha^{-1})} \alpha P$$

of $(\mathbf{Z}/p^n\mathbf{Z})^\times$ on the moduli problem $[\Gamma_1(p^n)]$.

The generic fiber of the quotient

$$X/(1 \times (\mathbf{Z}/p^n\mathbf{Z})^\times)$$

is just the usual descent of $X \underset{V_L}{\otimes} L$ to a smooth curve over K. For any subgroup

$$H \subset (\mathbf{Z}/p^n\mathbf{Z})^\times ,$$

the generic fiber of the quotient

$$X/1 \times H$$

is the usual descent of $X \underset{V_L}{\otimes} L$ to a smooth curve over L^H, namely

$$(X/(1 \times H)) \underset{(V_L)^H}{\otimes} L^H = (X/(1 \times (\mathbf{Z}/p^n\mathbf{Z})^\times)) \underset{V}{\otimes} K \underset{K}{\otimes} (L^H)$$

$$= \bar{\mathfrak{M}}(\mathcal{P}, [\Gamma_1(p^n)]) \underset{B[1/N]}{\otimes} L^H ,$$

Applying the numerical criterion to this situation, with $\Gamma_1 = 1 \times H$, we find:

THEOREM 14.3.6. *Let Σ be any $\mathbf{Q}$-rational set of $\bar{\mathbf{Q}}$-characters of the group $\Delta \simeq (\mathbf{Z}/p^n\mathbf{Z})^\times$, and let $H \subset (\mathbf{Z}/p^n\mathbf{Z})^\times$ be a subgroup. A sufficient condition that the I_K-stable subspace*

$$H^1(\bar{\mathfrak{M}}(\mathcal{P}, [\Gamma_1(p^n)]) \underset{B[1/N]}{\otimes} \bar{K}, \mathcal{F}(d))(\Sigma)$$

have good reduction over the field $L^H = K(\zeta_{p^n})^H$ is that the inequality of dimensions

$$\dim\left(H^1(\bar{\mathfrak{M}}(\mathcal{P}, [\text{bal. } \Gamma_1(p^n)]^{\text{can}}) \underset{B[1/N,\zeta_{p^n}]}{\otimes} k, \mathcal{F}(d))^{1\times H}(\Sigma)\right)$$

$$\leq \dim\left(H^1(\bar{\mathfrak{M}}(\mathcal{P}, [\Gamma_1(p^n)]) \underset{B[1/N]}{\otimes} \bar{K}, \mathcal{F}(d))(\Sigma)\right)$$

be an equality.

KEY REMARK 14.3.7. Hypotheses and notations as in (14.3.1-5-6) above, let us denote by K_0 the fraction field of B, and by L_0 the finite extension of K_0 defined by

$$L_0 = (K_0(\zeta_{p^n}))^H .$$

Fix an embedding $L_0 \hookrightarrow \bar{K}$ extending the chosen $K_0 \hookrightarrow K$, and denote by $\mathfrak{p}$ the corresponding p-adic place of L_0, and by

$$D_{\mathfrak{p}} \subset \mathrm{Gal}(\bar{L}_0/L_0)$$

the decomposition group at $\mathfrak{p}$.

Because the group $1 \times H$ acts L_0-linearly on the $B[1/N, \zeta_{p^n}]$-scheme $\bar{\mathcal{M}}(\mathcal{P}, [\mathrm{bal.}\,\Gamma_1(p^n)]^{\mathrm{can}})$, while the scheme $\bar{\mathcal{M}}(\mathcal{P}, [\Gamma_1(p^n)])$ itself lives over $B[1/N]$, it follows that the cohomology group

$$H^1(\bar{\mathcal{M}}(\mathcal{P}, [\Gamma_1(p^n)]) \underset{B[1/N]}{\otimes} \bar{K}, \mathcal{F}(d))$$

is itself a representation of the entire galois group $\mathrm{Gal}(\bar{K}_0/K_0)$, and that the inclusion

$$H^1(\bar{\mathcal{M}}(\mathcal{P}, [\mathrm{bal.}\,\Gamma_1(p^n)]^{\mathrm{can}}) \underset{B[1/N, \zeta_{p^n}]}{\otimes} k, \mathcal{F}(d))^{1\times H}$$

$$\downarrow$$

$$H^1(\bar{\mathcal{M}}(\mathcal{P}, [\Gamma_1(p^n)]) \underset{B[1/N]}{\otimes} \bar{K}, \mathcal{F}(d))$$

is equivariant for the action of the subgroup

$$D_{\mathfrak{p}} \subset \mathrm{Gal}(\bar{L}_0/L_0) \subset \mathrm{Gal}(\bar{K}_0/K_0) ,$$

with the inertia subgroup $I_{\mathfrak{p}} \subset D_{\mathfrak{p}}$ operating trivially on the source.

Therefore, if this inclusion induces an isomorphism of Σ-components, the resulting isomorphism of Σ-components is an isomorphism in the category of unramified representations of $D_{\mathfrak{p}}$.

(14.4) *Characters and conductors*

(14.4.1) Fix an integer $n \geq 1$, and a subgroup

$$H_0 \subset (\mathbf{Z}/p^n\mathbf{Z})^\times$$

which satisfies the two following conditions:

1) H_0 has order dividing $p-1$ (so $H_0 = \{1\}$ if $p = 2$)
2) if $n = 1$, H_0 is *not* the entire group $(\mathbf{Z}/p\mathbf{Z})^\times$.

(14.4.2) A $\bar{\mathbf{Q}}$-valued character

$$\chi : \Delta \simeq (\mathbf{Z}/p^n\mathbf{Z})^\times \longrightarrow (\bar{\mathbf{Q}})^\times$$

is said to be of type (H_0, v) for v an integer $1 \leq v \leq n$ if it satisfies the following three conditions:

1) $\chi(H_0) = 1$
2) $\chi(x) = 1$ if $x \equiv 1 \bmod p^v$
3) there exists an element $y \in (\mathbf{Z}/p^n\mathbf{Z})^\times$ with $y \equiv 1 \bmod p^{v-1}$, and $\chi(y) \neq 1$.

For example, the characters of type (H_0, n) are exactly the characters of maximal conductor which kill H_0.

Every non-trivial $\bar{\mathbf{Q}}$-valued χ which is trivial on H_0 is of type (H_0, v) for the unique integer $v \in [1, n]$ such that χ has conductor p^v. When convenient, we will say that the *trivial* character is of type $(H_0, 0)$.

(14.4.3) For each $v \in [1,n]$, the set of $\bar{\mathbf{Q}}$-valued characters of type (H_0, v) is $\mathbf{Q}$-rational. In any linear representation of the group $\Delta \simeq (\mathbf{Z}/p^n\mathbf{Z})^\times$, on a vector space M over a field of characteristic zero, we denote by

(14.4.3.1) $$M(H_0, v)$$

the sum of the χ-components for all χ of type (H_0, v). Clearly we have an isomorphism of Δ-representations

$$(14.4.3.2)\qquad M(H_0, v) \simeq \begin{cases} (M)^{H_0\times(1+(p^v))}/(M)^{H_0\times(1+(p^{v-1}))} & \text{if } v \geq 2 \\ (M)^{H_0\times(1+(p))}/(M)^{\Delta} & \text{if } v = 1 . \end{cases}$$

(14.5) *The Good Reduction Theorem*

THEOREM 14.5.1. *Let* $N \geq 1$ *be an integer prime to* p, $\Gamma \subset GL(2, Z/NZ)$ *a subgroup,* B *the ring* $(Z[\zeta_N])^{\det(\Gamma)}$. *Suppose that the moduli problem*

$$\mathcal{P} = ([\Gamma(N)]/\Gamma)^{B\text{-can}} \underset{B}{\otimes} B[1/N] \quad \text{on} \quad (Ell/B[1/N])$$

is representable, and that -1 *operates without fixed points on the cusp-labels of* $\Gamma \cap SL(2, Z/NZ)$ *(cf. (10.7)).*

Let ℓ *be a prime number dividing* N, d *an integer* ≥ 0, *and* $\mathcal{F}(d)$ *the* $\mathbf{Q}_\ell$*-sheaf on* $\overline{\mathcal{M}}(\mathcal{P})$ *constructed above (14.3.4.2).*

Let $n \geq 1$, $H_0 \subset (Z/p^nZ)^\times$ *a proper subgroup of order dividing* $p-1$, *and* $1 \leq v \leq n$ *an integer. Suppose that we are in one of the following two situations:*

a) $v = n$

b) $v > [n/2]$, *and* H_0 *is trivial.*

For any ring homomorphism

$$B[1/N] \to W(k), \quad k \text{ an algebraic closure of } F_p,$$

denoting by K *the fraction field of* W(k), *the subspace*

$$H^1(\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_1(p^n)]) \underset{B[1/N]}{\otimes} \overline{K}, \mathcal{F}(d))(H_0, v)$$

has good reduction over the field

$$K(\zeta_{p^n})^{H_0\times(1+(p^v))} .$$

Proof. We will prove the theorem by verifying the numerical criterion of good reduction.

We introduce some notation:

$$(14.5.1.1)\qquad \begin{cases} X_{\overline{\eta}} = \overline{\mathcal{M}}(\mathcal{P}, [\Gamma_1(p^n)]) \underset{B[1/N]}{\otimes} \overline{K} \\ Y_{\overline{\eta}} = \overline{\mathcal{M}}(\mathcal{P}) \underset{B[1/N]}{\otimes} \overline{K} \\ X_S = \overline{\mathcal{M}}(\mathcal{P}, [\text{bal. } \Gamma_1(p^n)]^{can}) \underset{B[1/N,\zeta_{p^n}]}{\otimes} k \\ Y_S = \overline{\mathcal{M}}(\mathcal{P}) \underset{B[1/N]}{\otimes} k \end{cases}$$

and for each pair of non-negative integers (a,b) with $a+b = n$,

$$(14.5.1.2)\qquad X_S(a,b) = \overline{\mathcal{M}}((\mathcal{P} \underset{B[1/N]}{\otimes} k)^{(\sigma^{-b})}, [\text{Ig}(p^{\max(a,b)})]) ,$$

viewed as a Y_S-scheme by pr_b (cf. 12.10.5).

For each integer v in $[0, n]$, we denote by

$$H(v) \subset (Z/p^nZ)^\times$$

the subgroup

$$(14.5.1.3)\qquad H(v) = \begin{cases} (Z/p^nZ)^\times & \text{if } v = 0 \\ H_0 \times (1+(p^v)) & \text{if } 1 \leq v \leq n . \end{cases}$$

We denote by

$$\Delta(H(v)) \subset \Delta$$

the corresponding subgroup of $\Delta \simeq (Z/p^nZ)^\times$:

$$(14.5.1.4)\qquad \Delta(H(v)) = \{(a, a^{-1}) | a \in H(v)\} \subset \Delta .$$

We will prove that the inclusion coming from the vanishing cycle exact sequence is in fact an equality

$$(14.5.2)\qquad H^1(X_S, \mathcal{F}(d))^{1\times H(v)}(H_0, v) = H^1(X_{\overline{\eta}}, \mathcal{F}(d))(H_0, v) .$$

(14.5.3) We first explain why it is sufficient to verify this equality under the additional hypothesis that Γ lies in $SL(2, Z/NZ)$.

The equality in question depends only on the inverse image of $\mathcal{F}(d)$ on the $W(k)[\zeta_{p^n}]$-scheme

$$\bar{\mathcal{M}}(\mathcal{P} \underset{B[1/N]}{\otimes} W(k), [\text{bal. } \Gamma_1(p^n)]^{\text{can}} \underset{Z[\zeta_{p^n}]}{\otimes} W(k)[\zeta_{p^n}]) .$$

Because $Z[\zeta_N, 1/N]$ is finite etale over $B[1/N]$, there exists an extension of the given homomorphism $B[1/N] \to W(k)$

$$\begin{array}{ccc} Z[\zeta_N, 1/N] & \longrightarrow & W(k) \\ \uparrow & \nearrow & \\ B[1/N] & & \end{array} .$$

For any such extension, we have

$$\mathcal{P} \underset{B[1/N]}{\otimes} W(k) = (\mathcal{P} \underset{B[1/N]}{\otimes} Z[\zeta_N, 1/N]) \underset{Z[\zeta_N, 1/N]}{\otimes} W(k)$$
$$= \left([\Gamma(N)]/\Gamma \cap SL(2, Z/NZ)\right)^{Z[\zeta_N]\text{-can}} \underset{Z[\zeta_N]}{\otimes} W(k) .$$

Thus we may replace Γ by $\Gamma \cap SL(2, Z/NZ)$, and $B[1/N]$ by $Z[\zeta_N, 1/N]$, without changing what is to be proven. In this case, we have by hypothesis that -1 has no fixed points on the cusp-labels of $\Gamma \cap SL(2, Z/NZ) = \Gamma$. This permits us to make use of (13.12.3). Recall also that by (10.13.8), the line bundle $\underline{\omega}$ exists on $\bar{\mathcal{M}}(\mathcal{P})$.

We will verify—eventually—the numerical criterion in this case.

(14.5.4) To verify the numerical criterion, we must show that

$$(14.5.4.1) \quad \dim\left(H^1(X_s, \mathcal{F}(d))^{1\times H(v)}(H_0, v)\right) = \dim\left(H^1(X_{\bar{\eta}}, \mathcal{F}(d))(H_0, v)\right) .$$

In view of the explicit description (14.4.3.2) of the (H_0, v) component of a representation of Δ, this amounts to proving that

$$(14.5.4.2) \quad \dim\left(\frac{H^1(X_s, \mathcal{F}(d))^{\Delta(H(v))\times(1\times H(v))}}{H^1(X_s, \mathcal{F}(d))^{\Delta(H(v-1))\times(1\times H(v))}}\right) = \dim\left(\frac{H^1(X_{\bar{\eta}}, \mathcal{F}(d))^{\Delta(H(v))}}{H^1(X_{\bar{\eta}}, \mathcal{F}(d))^{\Delta(H(v-1))}}\right) .$$

(14.5.5) We next explain how to reduce this to an equality involving Euler characteristics.

Suppose first $d > 0$. We claim that

$$(14.5.5.1) \qquad H^0(X_s, \mathcal{F}(d)) = H^2(X_s, \mathcal{F}(d)) = 0 .$$

This is clear from the fact that, by (13.11.4), X_s is the disjoint union, with crossings at the supersingular points, of connected smooth Igusa curves, each finite over Y_s. If we denote by $\{X_s(i)\}_{i\in I}$ the set of these Igusa curves, we have, for any constructible $\mathbf{Q}_\ell$-sheaf $\mathcal{G}$ on X_s, an exact sequence

$$(14.5.5.1.1) \quad 0 \to \mathcal{G} \to \bigoplus_{i\in I} (\mathcal{G}|X_s(i)) \to \bigoplus_{x \text{ s.s.}} \mathcal{G}_x \underset{\mathbf{Q}_\ell}{\otimes} (\mathbf{Q}_\ell^I/\mathbf{Q}_\ell) \to 0 ,$$

(where in $\mathbf{Q}_\ell^I/\mathbf{Q}_\ell$, we divide by the diagonal $\mathbf{Q}_\ell$), so a long exact cohomology sequence

$$(14.5.5.1.2) \quad 0 \to H^0(X_s, \mathcal{G}) \to \bigoplus_{i\in I} H^0(X_s(i), \mathcal{G}) \to \bigoplus_{x \text{ s.s.}} \mathcal{G}_x \underset{\mathbf{Q}_\ell}{\otimes} (\mathbf{Q}_\ell^I/\mathbf{Q}_\ell) \to H^1(X_s, \mathcal{G}) \to \bigoplus_{i\in I} H^1(X_s(i), \mathcal{G}) \to 0$$

and an isomorphism

$$(14.5.5.1.3)\qquad H^2(X_S, \mathcal{G}) \xrightarrow{\sim} \bigoplus_{i\in I} H^2(X_S(i), \mathcal{G})\ .$$

For $\mathcal{G} = \mathcal{F}(d)$ with $d > 0$, the terms $H^0(X_S(i), \mathcal{F}(d))$ and $H^2(X_S(i), \mathcal{F}(d))$ both *vanish*, by (14.3.4.3).

In the case $d > 0$, we also have, again by (14.3.4.3),

$$(14.5.5.2)\qquad H^0(X_{\overline{\eta}}, \mathcal{F}(d)) = H^2(X_{\overline{\eta}}, \mathcal{F}(d)) = 0\ .$$

Therefore in the case $d > 0$, the numerical criterion boils down to the *equality*

$$(14.5.5.3)\qquad \begin{aligned} &\chi(X_S/\Delta(H(v)) \times (1\times H(v)), \mathcal{F}(d)) \\ &-\chi(X_S/\Delta(H(v-1)) \times (1\times H(v)), \mathcal{F}(d)) \\ &= \chi(X_{\overline{\eta}}/\Delta(H(v)), \mathcal{F}(d)) - \chi(X_{\overline{\eta}}/\Delta(H(v-1)), \mathcal{F}(d))\ . \end{aligned}$$

We next consider the case $d = 0$, i.e., $\mathcal{F}(d) = \mathbf{Q}_\ell$. Because X_S and $X_{\overline{\eta}}$ are connected, we have

$$(14.5.5.4)\qquad \begin{cases} H^0(X_S, \mathbf{Q}_\ell) = \mathbf{Q}_\ell, \text{ with } (\mathbf{Z}/p^n\mathbf{Z})^\times \times (\mathbf{Z}/p^n\mathbf{Z})^\times \\ \qquad\qquad \text{acting trivially.} \\ H^0(X_{\overline{\eta}}, \mathbf{Q}_\ell) = \mathbf{Q}_\ell, \text{ with } \Delta \text{ acting trivially.} \end{cases}$$

As for H^2, we have, $X_{\overline{\eta}}$ being irreducible,

$$(14.5.5.5)\qquad H^2(X_{\overline{\eta}}, \mathbf{Q}_\ell) = \mathbf{Q}_\ell(-1), \text{ with } \Delta \text{ acting trivially.}$$

The situation for X_S is more complicated. We have

$$(14.5.5.6)\qquad H^2(X_S, \mathbf{Q}_\ell) = \bigoplus_{\text{irred compts}} \mathbf{Q}_\ell(-1)\ .$$

The space of irreducible components is

$$\coprod_{a+b=n} (\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times\ .$$

The group $(\mathbf{Z}/p^n\mathbf{Z})^\times \times (\mathbf{Z}/p^n\mathbf{Z})^\times$ operates on this space preserving each (a,b)-clump: the action of (α, β) on the set

$$(\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times$$

of (a,b)-components is multiplication by " $\alpha/\beta \bmod p^{\min(a,b)}$ " (cf. 13.11.3).

In the case $n = 1$, there are exactly two irreducible components, corresponding to $(a,b) = (1,0)$ and $(0,1)$, and each is stable by the entire group $\mathbf{F}_p^\times \times \mathbf{F}_p^\times$. So in this case

$$H^2(X_S, \mathbf{Q}_\ell) = \mathbf{Q}_\ell(-1) \oplus \mathbf{Q}_\ell(-1),\ \mathbf{F}_p^\times \times \mathbf{F}_p^\times \text{ acting trivially.}$$

If $n \geq 2$, the inequality

$$v - 1 \geq [n/2] \geq \min(a, b)$$

also gives

$$v - 1 \geq 1\ .$$

In this case, the groups

$$\begin{cases} \Delta(H(v)) \times (1\times H(v)) \\ \Delta(H(v-1)) \times (1\times H(v)) \end{cases}$$

both contain the subgroup $1 \times H_0$, and both are contained in the group $H(v-1) \times H(v-1) = (H_0\times(1+(p^{v-1})))\times(H_0\times(1+(p^{v-1})))$. So both operate on the space of components through the image of $1 \times H_0$, i.e.,

$$(14.5.5.7)\qquad \begin{aligned} H^2(X_S, \mathbf{Q}_\ell)^{1\times H_0} &= H^2(X_S, \mathbf{Q}_\ell)^{\Delta(H(v))\times(1\times H(v))} \\ &= H^2(X_S, \mathbf{Q}_\ell)^{\Delta(H(v-1))\times(1\times H(v))}\ . \end{aligned}$$

So again in the case $d = 0$, the numerical criterion boils down to the equality of Euler characteristics (14.5.5.3), this time with $d = 0$.

(14.5.6) We now divide each Euler characteristic into two terms, one from the cusps and the second from the complement of the cusps. Thus let us denote by

$$\begin{cases} CX_{\overline{\eta}} = \text{the cusps of } X_{\overline{\eta}} \\ CY_{\overline{\eta}} = \text{the cusps of } Y_{\overline{\eta}} \\ CX_S = \text{the cusps of } X_S \\ CY_S = \text{the cusps of } Y_S . \end{cases}$$

The decompositions

$$X_{\overline{\eta}} = CX_{\overline{\eta}} \cup (X_{\overline{\eta}} - CX_{\overline{\eta}})$$

$$X_S = CX_S \cup (X_S - CX_S)$$

are respected by the groups of operators Δ, $(\mathbf{Z}/p^n\mathbf{Z})^\times \times (\mathbf{Z}/p^n\mathbf{Z})^\times$ respectively (because these groups operate as $Y_{\overline{\eta}}$ and Y_S-automorphisms respectively, and these decompositions of $X_{\overline{\eta}}$, X_S are the inverse images of the analogous decompositions of $Y_{\overline{\eta}}$ and Y_S respectively).

PROPOSITION 14.5.7. *Under the hypotheses of the Main Theorem (14.5.1), the "cuspidal part" of the numerical criterion holds; we have, for any* $d \geq 0$,

$$\chi(CX_S/\Delta(H(v)) \times (1 \times H(v)), \mathcal{F}(d)) - \chi(CX_S/\Delta(H(v-1)) \times (1 \times H(v)), \mathcal{F}(d))$$
$$= \chi(CX_{\overline{\eta}}/\Delta(H(v)), \mathcal{F}(d)) - \chi(CX_{\overline{\eta}}/\Delta(H(v-1)), \mathcal{F}(d)) .$$

Proof. The restriction of $\mathcal{F}(d)$ to the cusps is lisse of rank one, so this amounts to a count of the cusps: we need

$$(14.5.7.1) \quad \#(CX_S/\Delta(H(v)) \times (1 \times H(v))) - \#(CX_S/\Delta(H(v-1)) \times (1 \times H(v)))$$
$$= \#(CX_{\overline{\eta}}/\Delta(H(v))) - \#(CX_{\overline{\eta}}/\Delta(H(v-1))) .$$

We know that the scheme of cusps in

$$\overline{\mathcal{M}}(\mathcal{P}, [\text{bal. } \Gamma(p^n)]^{can})$$

is finite etale over $\mathbf{Z}[1/N, \zeta_N, \zeta_{p^n}]$, a disjoint union of sections. Therefore we have a canonical bijection of finite sets

$$CX_{\overline{\eta}} \xrightarrow{\sim} CX_S$$

which is equivariant for the action of Δ.

Therefore we may "forget about" $X_{\overline{\eta}}$; we must prove the equality

$$(14.5.7.2) \quad \#(CX_S/\Delta(H(v)) \times (1 \times H(v))) - \#(CX_S/\Delta(H(v-1)) \times (1 \times H(v)))$$
$$= \#(CX_S/\Delta(H(v))) - \#(CX_S/\Delta(H(v-1))) .$$

But the cusps of X_S are the disjoint union of the cusps on the various irreducible components (in the notation of (14.5.1.2))

$$(14.5.7.3) \quad \coprod_{a+b=n} (\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times \text{ copies of } X_S(a,b) .$$

For any subgroup (cf. 13.12.2)

$$K \subset (\mathbf{Z}/p^n\mathbf{Z})^\times \times (\mathbf{Z}/p^n\mathbf{Z})^\times ,$$

recall that we defined subgroups

$$(14.5.7.4) \quad K \supset K(a,b) = \{(k_1, k_2) \in K \text{ with } k_1 \equiv k_2 \bmod p^{\min(a,b)}\}$$

$$(14.5.7.5) \quad (\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times \supset \text{Comp } K(a,b) = \{k_2/k_1 \bmod p^{\min(a,b)}, \text{ for } (k_1, k_2) \in K\}$$

(14.5.7.6)

$$(\mathbf{Z}/p^{\max(a,b)}\mathbf{Z})^\times \supset \operatorname{Im} K(a,b) = \begin{cases} \{k_1 \bmod p^{\max(a,b)} \text{ such that} \\ \quad (k_1,k_2) \in K(a,b) \text{ for some } k_2\} \\ \quad \text{if } a \le b \\ \{k_2 \bmod p^{\max(a,b)} \text{ such that} \\ \quad (k_1,k_2) \in K(a,b) \text{ for some } k_1\} \\ \quad \text{if } a \ge b \end{cases}$$

and we proved (13.12.3) that the irreducible components of X_s/K outside the supersingular points are

(14.5.7.7) $\coprod_{a+b=n} (\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times/\text{Comp } K(a,b)$ copies of $X_s(a,b)/\text{Im } K(a,b)$.

We have seen (12.7.1) that the entire group $(\mathbf{Z}/p^{\max(a,b)}\mathbf{Z})^\times$ operates freely on $CX_s(a,b)$, and the cusps of $X_s(a,b)$ are in fact a $(\mathbf{Z}/p^{\max(a,b)}\mathbf{Z})^\times$ torseur over the cusps of $Y_s^{(\sigma-b)}$. So for any subgroup

$$K \subset (\mathbf{Z}/p^n\mathbf{Z})^\times \times (\mathbf{Z}/p^n\mathbf{Z})^\times ,$$

we have the following formula:

(14.5.7.8) $$\#(CX_s/K) = \sum_{a+b=n} \frac{\phi(p^{\min(a,b)})\,\phi(p^{\max(a,b)})}{\#(\text{Comp } K(a,b))\,\#\text{Im}(K(a,b))}\,\#(CY_s) .$$

We will apply this formula, one (a,b)-term at a time, to the four different K's we are juggling. The computation is straightforward, and we give the result in the form of tables: in the second table, $H_0^{(2)}$ denotes the subgroup of *squares* of elements of H_0.

(14.5.7.9)

Table, if $n = 1$; $K \to$	$\Delta(H(1)) = \Delta(H_0)$	$\Delta(H(0)) = \Delta$	$\Delta(H(1)) \times (1 \times H(1)) = H_0 \times H_0$	$\Delta(H(0)) \times (1 \times H_0)$
Comp K(0,1)	1	1	1	1
Im K(0,1)	H_0	$F_p^\times$	H_0	$F_p^\times$
Comp K(1,0)	1	1	1	1
Im K(1,0)	H_0	$F_p^\times$	H_0	$F_p^\times$

(14.5.7.10)

Table, if $n \ge 2$; $K \to$ (so $v-1 \ge 1$)	$\Delta(H(v))$	$\Delta(H(v-1))$	$\Delta(H(v)) \times (1 \times H(v))$	$\Delta(H(v-1)) \times (1 \times H(v))$
Comp K(a,b) if $a \ge b \ge 1$	$H_0^{(2)}$	$H_0^{(2)}$	H_0	H_0
Im K(a,b) if $a \ge b \ge 1$	$(H_0 \cap \pm 1) \times (1 + (p^v)) \bmod p^a$	$(H_0 \cap \pm 1) \times (1 + (p^{v-1})) \bmod p^a$	$H(v) \bmod p^a$	$H_0 \times (1 + (p^{v-1})) = H(v-1) \bmod p^a$
Comp K(a,b) if $b \ge a \ge 1$	$H_0^{(2)}$	$H_0^{(2)}$	H_0	H_0
Im K(a,b) $b \ge a \ge 1$	$(H_0 \cap \pm 1) \times (1 + (p^v)) \bmod p^b$	$(H_0 \cap \pm 1) \times (1 + (p^{v-1})) \bmod p^b$	$H(v) \bmod p^b$	$H_0 \times (1 + (p^{v-1})) = H(v-1) \bmod p^b$
Comp K(0,n)	1	1	1	1
Im K(0,n)	H(v)	H(v-1)	H(v)	H(v-1)
Comp K(n,0)	1	1	1	1
Im K(n,0)	H(v)	H(v-1)	H(v)	H(v-1)

In this second table, $n \geq 2$, we now consider separately the two cases

$$\begin{cases} v = n, \ H_0 \text{ an arbitrary subgroup of order dividing } p-1 \\ v > [n/2], \ H_0 \text{ trivial.} \end{cases}$$

In the first of these cases, $v = n$, so $v-1 \geq n-1 \geq \max(a,b)$ whenever both a, b are ≥ 1. Then $H(n) = H_0$, and the table boils down to

(14.5.7.11)

Table, if $n \geq 2$ and $v = n$	$\Delta(H_0)$	$\Delta(H(n-1))$	$\Delta(H_0)\times(1\times H_0)$	$\Delta(H(n-1)\times(1\times H_0)$
Comp K(a,b) if a,b both ≥ 1	$H_0^{(2)}$	$H_0^{(2)}$	H_0	H_0
Im K(a,b) if a,b both ≥ 1	$H_0 \cap (\pm 1)$	$H_0 \cap (\pm 1)$	H_0	H_0
Comp K(a,b) if a or b = 0	1	1	1	1
Im K(a,b) if a or b = 0	H_0	H(n–1)	H_0	H(n–1)

In the second of these cases, $v > [n/2] \geq 1$, H_0 trivial, the table becomes even simpler:

(14.5.7.12)

Table, if $n \geq 2$, $v > [n/2]$, and H_0 trivial	$\Delta(H(v))$	$\Delta(H(v-1))$	$\Delta(H(v))\times(1\times H(v))$	$\Delta(H(v-1))\times(1\times H(v))$
Comp K(a,b)	1	1	1	1
Im K(a,b)	$H(v) \bmod p^{\max(a,b)}$	$H(v-1) \bmod p^{\max(a,b)}$	$H(v) \bmod p^{\max(a,b)}$	$H(v-1) \bmod p^{\max(a,b)}$

Now let us return to the formula (14.5.7.8)

$$\#(CX_s/K) = \sum_{a+b=n} \frac{\phi(p^{\min(a,b)})\phi(p^{\max(a,b)})}{\#(\text{Comp } K(a,b))\ \#(\text{Im } K(a,b))}\ \#(CY_s),$$

and temporarily christen the individual terms

$$(14.5.7.13)\quad \#(CX_s/K)(a,b) \overset{\text{dfn}}{=} \frac{\phi(p^{\min(a,b)})\phi(p^{\max(a,b)})}{\#(\text{Comp } K(a,b))\ \#(\text{Im } K(a,b))}\ \#(CY_s).$$

We claim that for *each* (a,b) with $a+b=n$, we have an equality of the individual (a,b)-components of the formula we are to prove, namely we claim

$$(14.5.7.14)\quad \#(CX_s/\Delta(H(v)))(a,b) - \#(CX_s/\Delta(H(v-1)))(a,b)$$
$$= \#(CX_s/\Delta(H(v))\times(1\times H(v)))(a,b) - \#(CX_s/\Delta(H(v-1))\times(1\times H(v)))(a,b).$$

Indeed, a look at the tables shows that in the case

$$n \geq 2,\ v = n,\ H_0 \text{ arbitrary},\ a,b \text{ both } \geq 1$$

both sides of the alleged equality *vanish*, and it shows that in all the other cases we must consider, both sides of the alleged equality are *term-by-term* equal. Q.E.D.

(14.5.8) We now return to the problem of proving the Main Theorem by proving the equality of Euler characteristics for every $\mathcal{F}(d)$, $d \geq 0$ (cf. 14.5.5.3):

$$(14.5.8.1)\quad \chi\left(X_s/\Delta(H(v))\times(1\times H(v)), \mathcal{F}(d)\right) - \chi\left(X_s/\Delta(H(v-1))\times(1\times H(v)), \mathcal{F}(d)\right)$$
$$= \chi\left(X_{\overline{\eta}}/\Delta(H(v)), \mathcal{F}(d)\right) - \chi\left(X_{\overline{\eta}}/\Delta(H(v-1)), \mathcal{F}(d)\right).$$

The sheaf $\mathcal{F}(d)$ is lisse of rank $d+1$ outside the cusps, *tamely* ramified along the cusps, and its restriction to the cusps is lisse of rank

one. Therefore each of the four Euler characteristics we are considering, written generically as $\chi(Z,\mathcal{F}(d))$, satisfies

$$\chi(Z,\mathcal{F}(d)) = \chi(Z-CZ,\mathcal{F}(d)) + \chi(CZ,\mathcal{F}(d)) \tag{14.5.8.2}$$
$$= (d+1)\chi(Z-CZ) + \#(CZ) .$$

Since we have already verified the cuspidal part of the equality, we are reduced to proving the following equality of topological Euler characteristics:

$$\chi\Big((X_S-CX_S)\Big/\Delta(H(v))\times(1\times H(v))\Big) - \chi\Big((X_S-CX_S)\Big/\Delta(H(v-1))\times(1\times H(v))\Big) \tag{14.5.8.3}$$
$$= \chi\Big((X_{\overline{\eta}}-CX_{\overline{\eta}})\Big/\Delta(H(v))\Big) - \chi\Big((X_{\overline{\eta}}-CX_{\overline{\eta}})\Big/\Delta(H(v-1))\Big) .$$

(14.5.9) *The right-hand difference*

The entire group $\Delta \simeq (\mathbf{Z}/p^n\mathbf{Z})^\times$ operates *freely* on $X_{\overline{\eta}}-CX_{\overline{\eta}}$ (e.g., outside of p, $[\Gamma_1(p^n)]$ is finite etale over $[\Gamma_0(p^n)]$ with group $(\mathbf{Z}/p^n\mathbf{Z})^\times$), and because we are in characteristic zero we have, for any subgroup $G \subset (\mathbf{Z}/p^n\mathbf{Z})^\times = \Delta$,

$$\chi((X_{\overline{\eta}}-CX_{\overline{\eta}})/G) = \left(\frac{1}{\#G}\right)\chi(X_{\overline{\eta}}-CX_{\overline{\eta}}) \tag{14.5.9.1}$$

so the right-hand difference of Euler characteristics is equal to

$$\left(\frac{1}{\#H(v)} - \frac{1}{\#H(v-1)}\right)\chi(X_{\overline{\eta}}-CX_{\overline{\eta}}) . \tag{14.5.9.2}$$

Now the covering

$$\begin{array}{c} X_{\overline{\eta}} - CX_{\overline{\eta}} \\ \Big\downarrow \\ Y_{\overline{\eta}} - CY_{\overline{\eta}} \end{array} \tag{14.5.9.3}$$

is itself finite etale of degree $p^{2n} - p^{2n-2}$ (the degree of $[\Gamma_1(p^n)]$ over

(Ell)), so we may rewrite the right-hand difference of Euler characteristics as

$$p^{2n-2}(p^2-1)\left(\frac{1}{\#H(v)} - \frac{1}{\#H(v-1)}\right)\chi(Y_{\overline{\eta}}-CY_{\overline{\eta}}) . \tag{14.5.9.4}$$

(14.5.10) *The left-hand difference*

We next analyze the left-hand difference of Euler characteristics. The curve $X_S - CX_S$ is fully ramified over $Y_S - CY_S$ at each supersingular point, so the supersingular points of $X_S - CX_S$ map isomorphically to the supersingular points of $Y_S - CY_S$. Therefore the supersingular points of $X_S - CX_S$ are individually fixed by the entire group $(\mathbf{Z}/p^n\mathbf{Z})^\times \times (\mathbf{Z}/p^n\mathbf{Z})^\times$, simply because this group operates by Y_S-automorphisms. Therefore in the left-hand difference of Euler characteristics, the contribution of the supersingular points to both terms is the same, namely $\#SS(Y_S)$, so we may rewrite the left-hand difference as

$$\chi\Big((X_S - CX_S - SS(X_S))\Big/\Delta(H(v))\times(1\times H(v))\Big) \tag{14.5.10.1}$$
$$-\chi\Big((X_S - CX_S - SS(X_S))\Big/\Delta(H(v-1))\times(1\times H(v))\Big) .$$

The open curve

$$X_S - CX_S - SS(X_S) \tag{14.5.10.2}$$

is the *disjoint* union of irreducible curves, namely

$$\coprod_{a+b=n} (\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times \text{ copies of } X_S(a,b)-CX_S(a,b)-SSX_S(a,b) . \tag{14.5.10.3}$$

For any subgroup

$$K \subset (\mathbf{Z}/p^n\mathbf{Z})^\times \times (\mathbf{Z}/p^n\mathbf{Z})^\times , \tag{14.5.10.4}$$

the quotient

$$(X_S - CX_S - SS(X_S))/K \tag{14.5.10.5}$$

is the disjoint union

$$(14.5.10.6)\qquad \coprod_{a+b=n}\left(\frac{\phi(p^{\min(a,b)})}{\#\,\mathrm{Comp}\ K(a,b)}\ \text{copies of}\right.$$
$$\left.(X_S(a,b)-CX_S(a,b)-SSX_S(a,b))\Big/\mathrm{Im}\ K(a,b)\right).$$

We now consider in detail the two groups

$$(14.5.10.7)\qquad \begin{cases} K_1 = \Delta(H(v))\times(1\times H(v)) \\ K_2 = \Delta(H(v-1))\times(1\times H(v))\,. \end{cases}$$

For ease of reference, we repeat the salient parts of our earlier tables, in the relevant cases:

	K_1	K_2
if $n=1$		
Comp K(a,b)	1	1
Im K(a,b)	H_0	$F_p^\times$
if $v=n\geq 1$		
Comp K(a,b) if a,b both ≥ 1	H_0	H_0
Im K(a,b) if both $a,b\geq 1$	H_0	H_0
Comp K(a,b) if a or b = 0	1	1
Im K(a,b) if a or b = 0	H_0	$H(n-1)$
if $v>[n/2]\geq 1$, H_0 trivial		
Comp K(a,b)	1	1
Im K(a,b)	$H(v) \bmod p^{\max(a,b)}$	$H(v-1) \bmod p^{\max(a,b)}$

We will consider separately the three cases.

(14.5.11) *Case I* ($n=1$)

In this case

$$\chi\left(\left(X_S-CX_S-SS(X_S)\right)\Big/K_1\right)-\chi\left((\ '')/K_2\right)$$
$$=\sum_{a+b=1}\left[\chi\left(\left(X_S(a,b)-CX_S(a,b)-SSX_S(a,b)\right)\Big/H_0\right)-\chi\left((\ '')/F_p^\times\right)\right].$$

Because H_0 and $F_p^\times$ have order prime to p, and operate *freely* on the Igusa curve minus its supersingular points, we may rewrite this

$$\sum_{a+b=1}\left(\frac{1}{\#H_0}-\frac{1}{\#F_p^\times}\right)\chi\left(X_S(a,b)-CX_S(a,b)-SSX_S(a,b)\right)$$
$$=2\left(\frac{1}{\#H_0}-\frac{1}{\#F_p^\times}\right)\chi\left(X_S(1,0)-CX_S(1,0)-SSX_S(1,0)\right).$$

Because $X_S(1,0)$ is the Igusa curve of level p, it minus its supersingular points is an etale $F_p^\times$-torsor over $Y_S-SS(Y_S)$, so we may rewrite the last expression as

$$2(p-1)\left(\frac{1}{\#H_0}-\frac{1}{\#F_p^\times}\right)\chi(Y_S-CY_S-SSY_S).$$

(14.5.12) *Case II* ($v=n\geq 2$)

In this case all the (a,b) terms with both a and $b\geq 1$ are identical for K_1 and K_2; the only terms which contribute to the *difference* are $(a,b)=(n,0)$ or $(0,n)$. For each of these terms, the *difference* is

$$\chi\left(\left(X_S(n,0)-CX_S(n,0)-SSX_S(n,0)\right)\Big/H_0\right)$$
$$-\chi\left((\ '')/H(n-1)\right).$$

The group H_0 operates freely on the open Igusa curve, and has order prime to p. The group $H(n-1)$ is the product of H_0 and the group of

order p, $1+(p^{n-1})$; it also operates freely. So we may "isolate" the H_0-contribution, and rewrite the above difference as

$$\frac{1}{\#H_0}\left[\chi\left(X_S(n,0)-CX_S(n,0)-SSX_S(n,0)\right)\right.$$
$$\left.-\chi\left((\ \ )/1+(p^{n-1})\right)\right].$$

Since both sides have the *same* number of supersingular points, namely $\#(SSY_S)$, we may rewrite this difference as

$$\frac{1}{\#H_0}\left[\chi\left(X_S(n,0)-CX_S(n,0)\right)-\chi\left(\left(X_S(n,0)-CX_S(n,0)\right)\Big/1+(p^{n-1})\right)\right].$$

But the quotient of $X_S(n,0)$ by $1+(p^a)$ is $X_S(a,0)$, so we may rewrite this as

$$\frac{1}{\#H_0}\left[\chi\left(X_S(n,0)-CX_S(n,0)\right)-\chi\left(X_S(n-1,0)-CX_S(n-1,0)\right)\right].$$

But this expression is the difference provided by both the (n,0) term and the (0,n) term, so all together the left-hand difference of Euler characteristics is

$$\frac{2}{\#H_0}\left[\chi\left(X_S(n,0)-CX_S(n,0)\right)-\chi\left(X_S(n-1,0)-CX_S(n-1,0)\right)\right].$$

(14.5.12) *Case III* ($v > [n/2] \geq 1$, H_0 trivial)

In this case, the left-hand difference is

$$\sum_{a+b=n}\phi(p^{\min(a,b)})\left[\chi\left(\left(X_S(a,b)-CX_S(a,b)-SS(X_S(a,b)\right)\Big/H(v)\right)\right.$$
$$\left.-\chi\left(\left(\qquad\qquad''\qquad\qquad\right)\Big/H(v-1)\right)\right].$$

The groups $H(v), H(v-1)$ operate through their images mod $p^{\max(a,b)}$. If $v-1 \geq \max(a,b)$, then both groups become *trivial* mod $p^{\max(a,b)}$, so the only terms which contribute a non-zero difference are those with

$$\max(a,b) \geq v\ .$$

For each such term, the curve $X_S(a,b)$ is an Igusa curve of level $p^{\max(a,b)}$, whose quotient by $H(v) = 1+(p^v)$ (resp. by $H(v-1) = 1+(p^{v-1})$) is the Igusa curve of level p^v (resp. p^{v-1}). Moreover, all these curves have the same number of supersingular points, namely $\#SSY_S$). All in all, the left-hand difference is

$$\sum_{\substack{a+b=n\\ \max(a,b)\geq v}}\phi(p^{\min(a,b)})\left[\chi\left(X_S(v,0)-CX_S(v,0)\right)-\chi\left(X_S(v-1,0)-CX_S(v-1,0)\right)\right].$$

(14.5.13) *Recapitulation of what remains to prove*

For ease of reference, we put together the formulas we are reduced to verifying:

(14.5.13.1) *Case I* ($n = 1$)

$$(p^2-1)\left(\frac{1}{\#H_0}-\frac{1}{\#F_p^\times}\right)\chi(Y_{\overline{\eta}}-CY_{\overline{\eta}})$$
$$=2(p-1)\left(\frac{1}{\#H_0}-\frac{1}{\#F_p^\times}\right)\chi(Y_S-CY_S-SSY_S)\ .$$

(14.5.13.2) *Case II* ($v = n \geq 2$)

$$\left(\frac{p^{2n-2}(p^2-1)}{\#H_0}\right)\left(1-\frac{1}{p}\right)\chi(Y_{\overline{\eta}}-CY_{\overline{\eta}})$$
$$=\frac{2}{\#H_0}\left[\chi\left(X_S(n,0)-CX_S(n,0)\right)-\chi\left(X_S(n-1,0)-CX_S(n-1,0)\right)\right].$$

(14.5.13.3) *Case III* ($v > [n/2] \geq 1$)

$$p^{2n-2}(p^2-1)\left(\frac{1}{p^{n-v}}-\frac{1}{p^{n+1-v}}\right)\chi(Y_{\overline{\eta}}-CY_{\overline{\eta}}) =$$
$$=\sum_{\substack{a+b=n\\ \max(a,b)\geq v}}\phi(p^{\min(a,b)})\left[\chi\left(X_S(v,0)-CX_S(v,0)\right)-\chi\left(X_S(v-1,0)-CX_S(v-1,0)\right)\right].$$

(14.5.14) *End of the proof: Case I*

We must show that

$$(p+1)\chi(Y_{\overline{\eta}}-CY_{\overline{\eta}}) = 2\chi(Y_s-CY_s-SSY_s)\ .$$

Now $Y = \overline{\mathcal{M}}(\mathcal{P})\otimes W(k)$ has good reduction, and its cusps are finite etale over the base, so

$$\chi(Y_{\overline{\eta}}-CY_{\overline{\eta}}) = \chi(Y_s-CY_s)\ ,$$

and we are reduced to proving

$$(p-1)\chi(Y_s-CY_s) = -2\#SSY_s\ .$$

In terms of the line bundle $\underline{\omega}$ on Y_s (which does indeed exist, by *hypothesis*), we have

$$\chi(Y_s-CY_s) = -2\deg(\underline{\omega})$$

by (10.13.12), and we have

$$\#SSY_s = (p-1)\deg(\underline{\omega})$$

by Igusa's theorem (cf. 12.4.3), whence the assertion. Q.E.D.

(14.5.15) *End of the proof: Case II* ($v = n \geq 2$)

The formula to be proven in this case is

$$p^{2n-3}(p^2-1)(p-1)\chi(Y_{\overline{\eta}}-CY_{\overline{\eta}})$$
$$= 2\left[\chi\left(X_s(n,0)-CX_s(n,0)\right)-\chi\left(X_s(n-1,0)-CX_s(n-1,0)\right)\right].$$

In terms of the line bundle $\underline{\omega}$ on Y_s, we have (cf. 10.13.12)

$$\chi(Y_{\overline{\eta}}-CY_{\overline{\eta}}) = -2\deg(\underline{\omega})\ ,$$

and, for every $n \geq 1$ we have (cf. 12.9.4)

$$\chi(X_s(n,0)-CX_s(n,0)) = -p^n\phi(p^n)\deg(\underline{\omega})\ .$$

The formula to be shown boils down to the assertion that for $n \geq 2$,

$$2p^{2n-3}(p^2-1)(p-1) = 2\left(p^n\phi(p^n)-p^{n-1}\phi(p^{n-1})\right)$$

whose verification we leave to the reader! Q.E.D.

(14.5.16) *End of the proof: Case III* ($v > [n/2] \geq 1$)

The formula to be proven in this case is

$$p^{n+v-3}(p^2-1)(p-1)\chi(Y_{\overline{\eta}}-CY_{\overline{\eta}}) =$$
$$=\left(\sum_{\substack{a+b=n\\ \max(a,b)\geq v}}\phi(p^{\min(a,b)})\right)\left[\chi\left(X_s(v,0)-CX_s(v,0)\right)-\chi\left(X_s(v-1,0)-CX_s(v-1,0)\right)\right].$$

In the sum over (a,b), the fact that $v > [n/2]$ means that the terms with $\max(a,b) \geq v$ occur in *pairs*,

$$(v+r, n-v-r)\ ,\ (n-v-r, v+r)$$

for $r = 0, \cdots, n-v$. So we have

$$\sum_{\substack{a+b=n\\ \max(a,b)\geq v}}\phi(p^{\min(a,b)}) = 2\sum_{r=0}^{n-v}\phi(p^{n-v-r})$$
$$= 2\sum_{r=0}^{n-v}\phi(p^r)$$
$$= 2\#(\mathbf{Z}/p^{n-v}\mathbf{Z})$$
$$= 2p^{n-v}\ ,$$

and the formula to be proven becomes

$$p^{2v-3}(p^2-1)(p-1)\chi(Y_{\overline{\eta}}-CY_{\overline{\eta}})$$
$$= 2\left[\chi\left(X_s(v,0)-CX_s(v,0)\right)-\chi\left(X_s(v-1,0)-CX_s(v-1,0)\right)\right],$$

for $v \geq 2$. But this is exactly the formula we just checked in Case II.

Q.E.D.

(14.6) *Explicitation of the Good Reduction Theorem*

(14.6.1) Throughout this section, we adopt the hypotheses and notations of the good reduction theorem (14.5.1).

With the notations $X_S, X_S(a,b), \cdots$ of (14.5.1.1), we have proven that the *inclusion* of the vanishing cycle exact sequence

$$H^1(X_S, \mathcal{F}(d)) \hookrightarrow H^1(X_{\overline{\eta}}, \mathcal{F}(d))$$

induces an *equality*

$$(14.6.2) \qquad H^1(X_S, \mathcal{F}(d))^{1\times H(v)}(H_0, v) = H^1(X_{\overline{\eta}}, \mathcal{F}(d))(H_0, v) .$$

We wish to *explicitly describe* the cohomology group

$$H^1(X_S, \mathcal{F}(d))^{1\times H(v)}(H_0, v)$$

in terms of the cohomology of certain Igusa curves.

Recall from (14.5.5.1.2) the cohomology exact sequence

$$(14.6.3) \quad 0 \to H^0(X_S, \mathcal{F}(d)) \to \bigoplus_{\substack{a+b=n \\ u\in(\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times}} H^0(X_S(a,b), \mathcal{F}(d))$$

$$\to \bigoplus_{\substack{\text{s.s. points} \\ y \text{ of } Y_S}} \mathcal{F}(d)_y \otimes_{\mathbf{Q}_\ell} (\mathbf{Q}_\ell^I/\mathbf{Q}_\ell) \to H^1(X_S, \mathcal{F}(d)) \to \bigoplus_{\substack{a+b=n \\ u\in(\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times}} H^1(X_S(a,b), \mathcal{F}(d)) \to 0 .$$

Because $\mathcal{F}(d)$ is the inverse image of a sheaf on Y_S, while the entire group $(\mathbf{Z}/p^n\mathbf{Z})^\times \times (\mathbf{Z}/p^n\mathbf{Z})^\times$ operates Y_S-linearly on X_S, this entire group acts on the term

$$\bigoplus_{y\in SSY_S} \mathcal{F}(d)_y \otimes_{\mathbf{Q}_\ell} (\mathbf{Q}_\ell^I/\mathbf{Q}_\ell)$$

as $\oplus$ (id $\otimes$ (permutation action on I)).

Therefore its (H_0, v)-component under the action of Δ is trivial (proof: by hypothesis $v-1 \geq [n/2] \geq \min(a,b)$ for any $a+b=n$, so the entire subgroup $(1+(p^{v-1}))^\times \times (1+(p^{v-1}))^\times$ of $(\mathbf{Z}/p^n\mathbf{Z})^\times \times (\mathbf{Z}/p^n\mathbf{Z})^\times$, and in particular its intersection with Δ, acts trivially on the indexing set I of irreducible components, because

$$I = \coprod_{a+b=n} (\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times$$

with action of (α, β) multiplication by β/α). So we have an isomorphism

$$(14.6.4) \qquad H^1(X_S, \mathcal{F}(d))(H_0, v) \xrightarrow{\sim}$$

$$\left(\bigoplus_{\substack{a+b=n \\ u\in(\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times}} H^1(X_S(a,b), \mathcal{F}(d)) \right)(H_0, v) ,$$

and passing to $1 \times H(v)$ invariants as well we obtain an isomorphism

$$(14.6.5) \qquad H^1(X_S, \mathcal{F}(d))^{1\times H(v)}(H_0, v) \xrightarrow{\sim}$$

$$\left(\bigoplus_{\substack{a+b=n \\ u\in(\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times}} H^1(X_S(a,b), \mathcal{F}(d)) \right)^{1\times H(v)}(H_0, v) .$$

The entire group $(\mathbf{Z}/p^n\mathbf{Z})^\times \times (\mathbf{Z}/p^n\mathbf{Z})^\times$ respects the (a,b)-decomposition, so we may rewrite this

$$(14.6.6) \qquad \bigoplus_{a+b=n} [(\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times \text{ copies of } H^1(X_S(a,b), \mathcal{F}(d))]^{1\times H(v)}(H_0, v) .$$

$$\simeq \bigoplus_{a+b=n} \frac{[(\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times \text{ copies of } H^1(X_S(a,b), \mathcal{F}(d))]^{\Delta(H(v))\times(1\times H(v))}}{[\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad]^{\Delta(H(v-1))\times(1\times H(v))}}$$

A glance at the table following (14.5.10.7) shows that only the terms (a, b) with $\max(a,b) \geq v$ contribute, and that their contribution is

(14.6.7) $\bigoplus_{\substack{a+b=n \\ \max(a,b)\geq v}} (\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times$ copies of

$$H^1(X_S(a,b)/(1+(p^v)), \mathcal{F}(d))(H_0, v) .$$

The quotient

(14.6.8) $$X_S(a,b)/(1+(p^v))$$

is given explicitly as

(14.6.9) $$\overline{\mathcal{M}}((\mathcal{P}\otimes k)^{(\sigma^{-b})}, [\mathrm{Ig}(p^{\max(a,b)})])/(1+(p^v))$$
$$= \overline{\mathcal{M}}((\mathcal{P}\otimes k)^{(\sigma^{-b})}, [\mathrm{Ig}(p^v)]) ,$$

viewed as $\overline{\mathcal{M}}(\mathcal{P}\otimes k)$-scheme by pr_b (cf. (12.10.3)).

We summarize these explicit results in the three cases.

(14.6.10) *Case I, II* ($v = n \geq 1$)

$$H^1(X_{\overline{\eta}}, \mathcal{F}(d))(H_0, n) \text{ has good reduction over } (K(\zeta_{p^n}))^{H_0} ,$$
$$\simeq H^1(\overline{\mathcal{M}}(\mathcal{P}\otimes k, [\mathrm{Ig}(p^n)]), \mathcal{F}(d))(H_0, n) \oplus$$
$$\oplus H^1(\overline{\mathcal{M}}((\mathcal{P}\otimes k)^{(\sigma^{-n})}, [\mathrm{Ig}(p^n)]), \mathcal{F}(d))(H_0, n) .$$

(14.6.11) *Case III* ($v > [n/2] \geq 1$, H_0 trivial)

$$H^1(X_{\overline{\eta}}, \mathcal{F}(d))(H_0, v) \text{ has good reduction over } K(\zeta_{p^v})$$
$$\simeq \bigoplus_{\substack{a+b=n, \max(a,b)\geq v \\ u\in(\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times}} H^1(\overline{\mathcal{M}}((\mathcal{P}\otimes k)^{(\sigma^{-b})}, [\mathrm{Ig}(p^v)])(H_0, v) .$$

(14.7) *Application to Jacobians*

(14.7.1) Let p be a prime number, $n \geq 1$, and $H_0 \subset (\mathbf{Z}/p^n\mathbf{Z})^\times$ a proper subgroup, of order dividing $p-1$. Let $N \geq 5$ be an integer prime to p (so that the moduli problem $\mathcal{P} = [\Gamma_1(N)]\otimes\mathbf{Z}[1/N]$ satisfies all the hypotheses of the good reduction theorem).

Let us denote by

$$J_1(Np^n)$$

the abelian variety over $\mathbf{Q}$ which is the *Jacobian* of

$$\overline{\mathcal{M}}([\Gamma_1(Np^n)]\otimes\mathbf{Q}) .$$

This $J_1(Np^n)$ visibly has good reduction over $\mathbf{Z}[1/Np]$ —simply because $\overline{\mathcal{M}}([\Gamma_1(Np^n)] \otimes_{\mathbf{Z}} \mathbf{Z}[1/Np])$ is a proper smooth curve over $\mathbf{Z}[1/Np]$ with geometrically connected fibers, whose Pic^0 is an abelian scheme over $\mathbf{Z}[1/Np]$ extending $J_1(Np^n)$.

The group $(\mathbf{Z}/p^n\mathbf{Z})^\times$ operates on $J_1(Np^n)$ through its modular action $P \mapsto aP$ on the moduli problem $[\Gamma_1(p^n)]$, so in the category of $\mathbf{Q}$-abelian varieties up to isogeny we can speak of the direct factor of type (H_0, v) for any $1 \leq v \leq n$:

$$J_1(Np^n)(H_0, v) \hookrightarrow J_1(Np^n) .$$

THEOREM 14.7.2.

(1) *If* $v = n$, *the* $\mathbf{Q}$*-abelian variety up to isogeny* $J_1(Np^n)(H_0, n)$ *acquires good reduction at the unique* p*-adic place of the field* $(\mathbf{Q}(\zeta_{p^n}))^{H_0}$, *and its special fiber at this place is* $\mathbf{F}_p$*-isogenous to the direct sum of two copies of the* $\mathbf{F}_p$*-abelian variety up to isogeny*

$$\mathrm{Jac}\,(\overline{\mathcal{M}}([\Gamma_1(N)]\otimes\mathbf{F}_p, [\mathrm{Ig}(p^n)])(H_0, n) .$$

(2) *If* $v > [n/2] \geq 1$, *and* H_0 *is trivial, the* $\mathbf{Q}$*-abelian variety up to isogeny* $J_1(Np^n)(H_0, v)$ *acquires good reduction at the unique* p*-adic place of* $\mathbf{Q}(\zeta_{p^v})$, *and its special fiber at this place is* $\mathbf{F}_p$*-isogenous to the direct sum*

$$\bigoplus_{\substack{a+b=n, \max(a,b)\geq v \\ u\in(\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times}} \mathrm{Jac}(\overline{\mathcal{M}}([\Gamma_1(N)]\otimes\mathbf{F}_p, [\mathrm{Ig}(p^v)])(H_0, v)$$

($2p^{n-v}$ *copies of the isogeny-direct factor of* $\mathrm{Jac}\,(\overline{\mathcal{M}}([\Gamma_1(N)]\otimes\mathbf{F}_p, [\mathrm{Ig}(p^v)])$ *of maximal conductor* p^v *under the action of* $(\mathbf{Z}/p^n\mathbf{Z})^\times$).

Proof. This follows from the special case $d = 0$, $\mathcal{F}(d)$ = the constant sheaf $\mathbf{Q}_\ell$, of the good reduction theorem, by the Neron-Ogg-Shafarevic criterion of good reduction (cf. [Se-Ta 2]), the Key Remark (14.3.7), and Tate's isogeny theorem [Ta 1]. Q.E.D.

NOTES ADDED IN PROOF

Notes on Chapter 2

Let E/S be an elliptic curve, $N \geq 1$ and $M \geq 1$ two integers, and $P, Q \in E[NM](S)$. Then we have

$$(e_{NM}(P,Q))^M = e_{NM}(MP,Q) = E_N(MP,MQ) ,$$

the last equality by applying (2.8.4.1) to the situation

$$E = E_0 = E_1 = E_2 ,\ \pi_1 = N ,\ \pi_2 = M ,\ P_0 = MP \in \mathrm{Ker}(\pi_1) ,\ P_2 = Q \in \mathrm{Ker}(\pi_1^t \circ \pi_2^t) .$$

This compatibility occurs implicitly in 2.9.1's description of $\mathcal{B}_N$. Taking $M = 2$ and $P = Q$, we find

$$1 = (e_{2N}(P,P))^2 = e_N(2P,2P) , \text{ for } P \in E[2N](S) ,$$

the first equality by 2.8.3. Because $[2]: E \to E$ is f.p.p.f. surjective, any point R in $E[N](S)$ is locally f.p.p.f. of the form $2P$ for $P \in E[2N](S)$, whence we have

$$e_N(R,R) = 1 \text{ for } R \in E[N](S) .$$

Notes on Chapter 4

Contrary to what is implicitly asserted in Section 4.12, the property "being of given dimension" is not in general local for the etale topology, or even for the Zariski topology (e.g., the spectrum of a discrete valuation ring, or the disjoint union of two schemes of different dimensions). It is rather the property "non-empty, and every non-empty Zariski open set is n-dimensional" which is local for the etale topology, and it is in this

stronger sense that the phrase "$\mathcal{P}$ is n-dimensional" is to be interpreted, for $\mathcal{P}$ a relatively representable moduli problem on (Ell), or on (Ell/k) for k a field.

For a scheme which is locally of finite type over $\mathbf{Z}$ or over a field, "n-dimensional" in this stronger sense is equivalent to the property "equidimensional, and n-dimensional", i.e., "non-empty, and every irreducible component is n-dimensional"; this last property, for such schemes, is equivalent to the property "non-empty, and the local ring at every closed point is n-dimensional" (cf. EGA IV, 10.6.1 (i), 10.6.2, 10.7.1, as well as 5.2.5(ii)). The point here is that for a scheme X which is locally of finite type over $\mathbf{Z}$ (resp., over a specified field k), a point $x \in X$ is closed in X if and only its residue field is a finite field (resp., a finite extension of k); thus for any open neighborhood U of x, $x \in U \subset X$, the point x is closed in U if and only if it closed in X. [It is this property which "fails" for X the spectrum of a discrete valuation ring.]

If $f: X \to Y$ is a finite flat surjective morphism of locally noetherian schemes, the property "non-empty, and the local ring at every closed point is n-dimensional" holds for X if and only if it holds for Y. [Because f is finite, $x \in X$ is closed in X if and only if $y = f(x)$ is closed in Y. Because f is finite surjective, the inverse image of $\mathrm{Spec}(\hat{\mathcal{O}}_{Y,y})$ is the disjoint union of the $\mathrm{Spec}(\hat{\mathcal{O}}_{X,x_i})$, over the finite non-empty set of points $x_i \in X$ with $f(x_i) = y$. Because f is finite and flat, each $\mathrm{Spec}(\hat{\mathcal{O}}_{X,x_i})$ is individually finite and flat over $\mathrm{Spec}(\hat{\mathcal{O}}_{Y,y})$, and so necessarily surjective as well, because its open image contains the closed point. By (EGA IV, 5.4.1 (ii)), we conclude that $\dim(\hat{\mathcal{O}}_{X,x}) = \dim(\hat{\mathcal{O}}_{Y,y})$ for $x \in X$, $y = f(x)$. Applying this to closed points, we have the result.]

Similarly, for $f: X \to Y$ as above, the property "equidimensional and n-dimensional" holds for X if and only if it holds for Y. [Apply the equality $\dim(\hat{\mathcal{O}}_{X,x}) = \dim(\hat{\mathcal{O}}_{Y,f(x)})$, proven above, to points where this dimension is zero to conclude that $x \in X$ is a maximal point of X (i.e., a generic point of an irreducible component of X) if and only if $y = f(x)$ is a maximal point of Y. As f is proper as well, this means that if X_α is an irreducible component of X, then $f(X_\alpha)$ is an irreducible component, say Y_β, of Y, and every irreducible component of Y is of this form. Because the induced map $X_\alpha^{\mathrm{red}} \to Y_\beta$ is finite and surjective, we have $\dim(X_\alpha) = \dim(Y_\beta)$, again by EGA IV, 5.4.1 (ii).]

Applying either of these equivalences, we see that for $\mathcal{P}$ a relatively representable moduli problem on (Ell) (respectively, on (Ell/k) for k a field) which is surjective finite and flat over (Ell) (resp. over (Ell/k)), then $\mathcal{P}$ is automatically "two-dimensional" (resp., "one-dimensional") in the strong sense. [For if E/S is a modular family, then S is locally a smooth curve over $\mathbf{Z}$ (resp., over k), and $\mathcal{P}_{E/S} \to S$ is finite flat surjective by hypothesis.] For such a $\mathcal{P}$, if $\mathcal{P}'$ is a second relatively representable moduli problem on (Ell) (resp. on (Ell/k)) which is finite over (Ell) (resp. over (Ell/k)), and if $\mathcal{P} \to \mathcal{P}'$ is a finite flat surjective morphism of relatively representable moduli problems, then $\mathcal{P}'$ is itself finite flat surjective over (Ell) (resp. over (Ell/k)), by a standard sorite on faithfully flat morphisms (cf. Bourbaki, *Comm. Alg.* I, §3.4, Prop. 7). Therefore $\mathcal{P}'$ is itself "two-dimensional" (resp., "one-dimensional") in the strong sense. If in addition $\mathcal{P}$ is regular, then $\mathcal{P}'$ is also regular, being surjective and flat "under" $\mathcal{P}$ (cf. EGA IV, 6.5.2). This argument occurs in proving 6.6.1 and 7.5.1.

If $\mathcal{P}$ and $\mathcal{P}'$ are two relatively representable moduli problems on (Ell) (resp. on (Ell/k)), both of which are regular and "n-dimensional" in the strong sense, then any finite morphism of moduli problems $\mathcal{P} \to \mathcal{P}'$ is automatically finite and flat. This observation is used repeatedly throughout the book, always accompanied by the catch-phrase "a finite map between regular schemes of the same dimension is automatically flat." This catch-phrase is trivially false as stated unless the schemes in question are equidimensional as well (think of the disjoint union of a line and a point mapping to a line). The correct statement is "a finite morphism $f: X \to Y$ between locally noetherian schemes both of which are regular

and equidimensional of dimension n is automatically flat." [Proof: Because Y is regular and locally noetherian, it is the disjoint union of its irreducible components Y_α, each of which is open and closed in Y. Looking at the situation over each Y_α with $f^{-1}(Y_\alpha)$ non-empty, we reduce to the case Y irreducible. Because X is regular and locally noetherian, it is the disjoint union of its irreducible components X_β, each open and closed in X, so we may examine the situation on each X_β individually. Thus we may and will assume both X and Y irreducible, locally noetherian, regular n-dimensional. Because $f: X \to Y$ is finite, we have $\dim(X) \leq \dim f(X) \leq \dim(Y)$, by EGA IV, 5.4.1 (i). Therefore f is surjective. Combining EGA IV, 5.6.4 with 5.6.5.3, we see that, because f is finite, we have $\dim(\mathcal{O}_{X,x}) = \dim(\mathcal{O}_{Y,f(x)})$. The result now follows, by [EGA IV, 15.4.2, e') $\Longrightarrow$ b)]. Indeed, the same chain of reasoning and references gives the same conclusion if one replaces "finite" by "quasi-finite" and " X regular" by " X Cohen-McCauley" in the hypotheses.] The reader will check that wherever the catch-phrase "a finite map between regular schemes of the same dimension is automatically flat" appears in the text, it is applied either to schemes which are in fact equidimensional, or to moduli problems which have already been proven to be "n-dimensional" in the strong sense (cf. 1.12.7, 2.3.1, 5.5.2, 5.5.3, 7.5.2, 7.9.6, 10.12.2, 12.6.1, 12.8.2, 13.2.2).

Notes on Chapters 8 and 10

The smoothness of coarse moduli schemes outside supersingular points in "bad" characteristics (cf. 10.9.7, 10.10.3 (5), 10.10.6 (2)) is more easily proven by viewing these schemes as quotients of suitable fine moduli schemes (cf. 8.1.1), and applying the following quite general theorem.

THEOREM. *Let* S *be a regular noetherian scheme,* $X \to S$ *a smooth affine curve over* S, *and* G *a finite group operating* S*-linearly on* X. *Then the quotient* X/G *is a smooth curve over* S.

Proof. It suffices to check smoothness at points which are closed in their fibers. Localizing, completing, and "algebraically closing the residue field" (cf. EGA. O, 10.3.1 and 10.3.1 (5)) at a point $s \in S$, we reduce to the case $S = \mathrm{Spec}(A)$, with A a complete noetherian regular local ring with algebraically closed residue field. Then the complete local ring of X at a closed point x of its special fiber X_s is A-isomorphic to A[[T]], the isotropy group $G_x \subset G$ of x acts A-linearly on A[[T]], and the complete local ring of X/G at the image of x is the ring of invariants of G_x acting on A[[T]].

The theorem therefore results from the following proposition (compare 7.5.2), applied to the image of G_x in $\mathrm{Aut}(A[[T]])$.

PROPOSITION. *Let* A *be a complete noetherian local domain,* T *an indeterminate, and* $G \subset \mathrm{Aut}_A(A[[T]])$ *a finite group of* A*-linear automorphisms. Then*

$$(A[[T]])^G = A[[N_G(T)]] .$$

Proof. We have obvious inclusions

$$A[[T]] \supset (A[[T]])^G \supset A[[N_G(T)]] .$$

Just as in 7.5.2, we see that A[[T]] is spanned over $A[[N_G(T)]]$ by the elements $1, T, \cdots, T^{\#G-1}$. Therefore these elements certainly span A[[T]] over $(A[[T]])^G$. By galois theory, these elements must be linearly independent over $(A[[T]])^G$, so a fortiori linearly independent over $A[[N_G(T)]]$. Therefore A[[T]] is a free module with basis $1, T, \cdots, T^{\#G-1}$ over *both* $(A[[T]])^G$ *and* over $A[[N_G(T)]]$, whence the inclusion

$$(A[[T]])^G \supset A[[N_G(T)]]$$

must be an equality. Q.E.D.

Related to the discussion of coarse base change in Chapter 8 (cf. 8.1.6), we have the following theorem.

THEOREM. *Let* S *be a regular noetherian scheme,* $X \to S$ *a smooth affine curve over* S, *and* G *a finite group operating* S*-linearly on* X. *Suppose that for every geometric point* s *of* S, *the action of* G *on the fiber* X_s *is free on an open dense set of* X_s. *Then for any regular noetherian* S′ *and any morphism* $S' \to S$, *the canonical map* $(X \underset{S}{\times} S')/G \to (X/G) \underset{S}{\times} S'$ *is an isomorphism.*

Proof. The question is Zariski local on S′, which we may suppose connected, and hence irreducible. Source and target are smooth curves over S′ by the previous theorem, so both are regular noetherian schemes, equidimensional of the same dimension. By general properties of quotients, the map in question is finite, surjective (and radicial), so we may conclude that it is finite, flat, and surjective. To see that it is of degree one over $(X/G) \underset{S}{\times} S'$, it suffices to check over the dense open set where the action is free. Q.E.D.

REFERENCES

[A-K 1] Altman, A., and Kleiman, S., *Introduction to Grothendieck Duality Theory*, Springer Lecture Notes in Mathematics 146, 1970.

[A-K 2] ———, Compactification of the Picard Scheme, Adv. Math. 35, 1980, 50-112.

[Cmn 1] Casselman, W., On abelian varieties with many endomorphisms, and a conjecture of Shimura's, Inv. Math. 12 1971, 225-236.

[Cmn 2] ———, On representations of GL_2 and the arithmetic of modular curves, in *Modular Functions of One Variable II*, Springer Lecture Notes in Mathematics, 1973, 108-141.

[Ca] Cassels, J. W. S., Diophantine equations with special reference to elliptic curves, J. Lond. Math. Soc. 41, 1966, 193-291.

[De 1] Deligne, P., Formes modulaires et représentations ℓ-adiques, Exposé 355, *Seminaire N. Bourbaki*, 1968/69, Springer Lecture Notes in Mathematics 179, 1969.

[De 2] ———, Courbes elliptiques: formulaire (d'apres J. Tate), in *Modular Functions of One Variable IV*, Springer Lecture Notes in Mathematics 476, 1975, 53-73.

[De-Il] Deligne, P., and Illusie, L., Relèvement des surfaces K3 en caractéristique nulle, in *Surfaces Algébriques*, Springer Lecture Notes in Mathematics 868, 1981, 58-79.

[De-Mu] Deligne, P., and Mumford, D., Irreducibility of the space of curves of given genus, Publ. Math. IHES, 36, 1969.

[De-Ra] Deligne, P., and Rapoport, M., Les schémas de modules de courbes elliptiques, in *Modular Functions of One Variable II*, Springer Lecture Notes in Mathematic 349, 1973, 143-316.

[De-Ga] Demazure, M., and Gabriel, P., *Groupes Algébriques*, Tome I, Masson & Cie, Paris, North Holland Publishing Company, Amsterdam, 1970.

[De-Gi-Ray] Demazure, M., Giraud, J., and Raynaud, M., Schémas Abéliens, Séminaire de Géometrie Algébrique 1967-68, Faculté des Sciences de l'Université de Paris; Orsay (notes polycopiées).

[Deu] Deuring, M., Die Typen der Multiplikatorenring elliptischen Funktionenkorper, Abh. Hamb. 16, 1949, 32-47.

[Dr 1] Drinfeld, V. G., Elliptic modules (Russian), Math. Sbornik 94, 1974, 594-627 (English translation: Math. USSR, Sbornik, Vol. 23, 1973, No. 4).

[Dr 2] _____Coverings of p-adic symmetric domains (Russian), Funk. Anal. i. Prilozen, 10, 1976, No. 2, 29-40.

[E] Eichler, M., Eine Verallgemeinerung der abelschen Integrale, Math. Zeit, 67, 1957, 267-298.

[EGA] *Eléments de Géometrie Algébrique*, Ch. I, II, III, IV, Pub. Math. IHES, 4(I), 8(II), 11,17(III), 20, 24, 28, 32(IV).

[H] Hasse, H., Zur Theorie der Abstrakten elliptischen Funktionenkorper, I, II, II, J. Reine Angew. Math. 175, 1936.

[Ig 1] Igusa, J., Class number of a definite quaternion with prime discriminant, Proc. Nat'l. Acad. Sci., 44, 1958, 312-314.

[Ig 2] _____, Kroneckerian model of fields of elliptic modular functions, Amer. J. Math. 81, 1959, 561-577.

[Ig 3] _____, Fiber Systems of Jacobian varieties III, Amer. J. Math. 81, 1959, 453-476.

[Ig 4] _____, On the transformation theory of elliptic functions, Amer. J. Math. 81, 1959, 453-476.

[Ig 5] _____, On the algebraic theory of elliptic modular functions, J. Math. Soc. Japan 20, 1968, 96-106.

[Ih] Ihara, Y., Hecke polynomials as congruence ζ-functions in elliptic modular case, Ann. Math. 85, 1967.

[K-1] Katz, N., Nilpotent connections and the monodromy theorem: applications of a result of Turritin, Publ. Math. IHES, 39, 1970, 355-412.

[K-2] _____, P-adic properties of modular schemes and modular forms, in *Modular Functions of One Variable III*, Springer Lecture Notes in Mathematics 350, 1973, 70-189.

[K-3] _____, An overview of Deligne's proof of the Riemann Hypothesis for varieties over finite fields, in *Mathematical Developments Arising From Hilbert Problems*, Proc. Sym. P.A. Math. XXVIII, AMS, 1976, 275-305.

[K-4] _____, P-adic interpolation of real analytic Eisenstein series, Ann. Math. 104, 1976, 459-571.

[K-5] _____, Serre-Tate local moduli, in *Surfaces Algébriques*, Springer Lecture Notes in Mathematics 868, 1981, 138-202.

[La] Langlands, R. P., Modular forms of ℓ-adic representations, in *Modular Functions of One Variable II*, Springer Lecture Notes in Mathematics, 349, 1973, 361-500.

[Lu] Lubin, J., One parameter formal Lie groups over p-adic integer rings, Ann. Math. 83, 1964, 464-484.

[Lu-Ta] Lubin, J., and Tate, J., Formal complex multiplication in local fields, Ann. of Math. 81, 1965, 380-387.

[M-W] Mazur, B., and Wiles, A., Class fields of abelian extensions of Q. Invent. Math. 76, 1984, 179-330.

[Mes] Messing, W., *The Crystals Associated to Barsotti-Tate Groups; with Applications to Abelian Schemes*, Springer Lecture Notes in Mathematics, 264, 1972.

[Mum 1] Mumford, D., The Picard groups of the moduli problem, in *Arithmetic Algebraic Geometry*, ed. O.F.G. Schilling, Harper & Row, 1965.

[Mum 2] _____, *Lectures on curves on an algebraic surface*, Ann. of Math. Studies 59, Princeton Univ. Press, 1966.

[Mum 3] _____, *Geometric Invariant Theory*, Springer-Verlag, 1965.

[Mum 4] _____, *Abelian Varieties*, Oxford University Press, 1970.

[Nag] Nagata, M., *Local Rings*, Interscience Publishers, NY and London, 1962.

[Oda] Oda, T., The first de Rham cohomology group and Dieudonné modules, Ann. Sci. Ec. Norm. Sup., 5e série, t.2, 1969, 63-135.

[Oort-Tate] Oort, F., and Tate, J., Group schemes of prime order, Ann. Scient. Ecole Norm. Sup., 4e série, t.3, 1970, 1-21.

[Ra 1] Raynaud, M., Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes, Séminaire N. Bourbaki, 1964/65, Exposé 286, W.A. Benjamin, 1966.

[Ra 2] _____, Specialization du foncteur de Picard, Publ. Math. IHES, 38, 1970, 27-76.

[Roq] Roquette, P., *Analytic Theory of Elliptic Functions over Local Fields*, Göttingen, Vanderhoeck und Ruprecht, 1970.

[Se] Serre, J.-P., *Abelian ℓ-adic Representations and Elliptic Curves*, W.A. Benjamin, 1968.

[Se-Ta 1] Serre, J.-P., and Tate, J., mimeographed notes from the 1964 AMS Summer Institute in Algebraic Geometry at Woods Hole.

[Se-Ta 2] _____, Good reduction of abelian varieties, Annals of Math., 88, 1968, 492-517.

[SGA] *Séminaire de Géométrie Algébrique I, III, IV, 4 1/2, VII pt. I, VII pt. 2*, Springer Lecture Notes in Mathematics, 224(I), 151-2-3(III), 269-270-305(IV), 569(4 1/2), 288(VII pt. 1), 340(VII pt. 2).

[Sh 1] Shimura, G., Correspondances modulaires et les fonctions ζ des courbes algébriques, J. Math. Soc. Jap. 10, 1958, 1-28.

[Sh 2] _____, Sur les Integrales Attachés aux Formes Automorphes, J. Math. Soc. Japan, 11, 1959, 291-311.

[Sh 3] _____, *Introduction to the Arithmetic Theory of Automorphic Functions*, Pub. Math. Soc. Japan, No. 11, Iwanami Shoten and Princeton University Press, 1971.

[Ta 1] Tate, J., Endomorphisms of abelian varieties over finite fields, Inv. Math. 2, 1966, 134-144.

[Ta 2] _____, Classes d'isogénie des variétés abéliennes sur un corps fini (d'apres T. Honda), Exposé 352, Séminaire Bourbaki 1968/69, Springer Lecture Notes in Mathematics 179, 1971.

[Ta 3] _____, The arithmetic of elliptic curves, Invent. Math. 23, 1974, 179-206.

[Ta 4] _____, P-divisible groups, in *Proceedings of a Conference on Local Fields*, NUFFIC Summer School held at Driebergen in 1966, Springer-Verlag, 1967.

Library of Congress Cataloging in Publication Data

Katz, Nicholas M., 1943-
Arithmetic moduli of elliptic curves.

Bibliography: p.
1. Curves, Elliptic. 2. Moduli theory. 3. Geometry, Algebraic. I. Mazur, Barry. II. Title.
QA567.K3 1984 516.3'5 83-43079
ISBN 0-691-08349-5
ISBN 0-691-08352-5 (pbk.)

Nicholas M. Katz is Professor of Mathematics at Princeton University. Barry Mazur is William Petschek Professor of Mathematics at Harvard University.