Math 248B. A regularity argument of Katz–Mazur

1. Statement of main result

Fix an integer $N \geq 1$ and a prime $p \nmid N$. We wish to prove that $Y_1(N,p)$ is normal and $\mathbf{Z}[1/N]$-flat (hence of pure relative dimension 1), and even regular when $N \geq 4$. In what follows we will assume familiarity with basic ideas and results concerning p-divisible groups. In Exercise 4 of HW9, p-divisible groups were used to reduce the problem to the following regularity assertion (in which N drops out of the picture):

Theorem 1.1. *Let Γ_0 be a connected p-divisible group of dimension 1 and height 2 over an algebraically closed field of characteristic $p > 0$. Let $R \simeq W(k)[\![t]\!]$ be the universal deformation ring of Γ_0, and Γ over R be the universal deformation. Let $R \to R'$ be the 2-dimensional finite local algebra classifying order-p finite flat subgroup schemes of $\Gamma[p]$. Then R' is regular.*

We assume the reader has worked through Exercise 4 of HW9 to see why R' is identified with a completed strictly henselized local ring on $Y_1(N,p)$ at a supersingular geometric closed point y, and why it is 2-dimensional. To prove the regularity, following Katz–Mazur we will produce a pair of elements that generate the maximal ideal. The reader is referred to Chapters 5 and 6 of Katz–Mazur for a very broad discussion of the topics below. We focus our attention narrowly on what is needed to prove the Theorem above.

As a preliminary step, we record the following crucial fact (which is true in much greater generality: see Theorem 6.8.1 in Katz–Mazur):

Proposition 1.2. *The natural map $R \to R'$ is flat.*

Proof. Recall that R is the universal deformation ring for a supersingular elliptic E_0. In this respect, R' is the universal deformation ring for the pair (E_0, G_0) where $G_0 = \ker F_{E_0/k}$ is the unique infinitesimal k-subgroup scheme of order p. (Note that the universal formal deformations are algebraizable formal schemes, due to the canonical projectivity of elliptic curves, so we may and do treat the universal structure over R as an actual elliptic curve over R, not just a formal elliptic curve.) Using the theory of isogenies for elliptic curves over schemes as developed in §1 of the handout "Isogenies and level structures", the specification of an order-p finite locally free subgroup scheme G in a deformation E of E_0 is the same as specifying a deformation E' of $E_0^{(p)} = E_0/G_0$ *along with* a degree-p isogeny $f : E \to E'$ lifting $F_{E_0/k}$. In other words, we can interpret R' as the universal deformation ring for triples (E, E', f) consisting of an infinitesimal deformation E of E_0, E' of $E_0^{(p)}$, and an isogeny f lifting $F_{E_0/k}$. This new interpretation is useful because the rigidity lemma ensures that when E and E' are given, the isogeny f lifting $f_0 = F_{E_0/k}$ is unique if it exists.

That is, the deformation functor for such triples is a subfunctor of the deformation functor for pairs (E, E'), which in turn is pro-represented by the completed tensor product $W(k)[\![t,t']\!] = W(k)[\![t]\!]\widehat{\otimes}_{W(k)}W(k)[\![t']\!]$. But a map between complete local noetherian rings with a common residue field is surjective when the induced map on artinian points is always injective (a "complete local" version of the fact that a proper monomorphism of schemes is a closed immersion), so R' is a quotient of $W(k)[\![t,t']\!]$. Writing $R' = W(k)[\![t,t']\!]/J$, we have that J is a nonzero proper ideal since $\dim R' = 2$. We claim that J is principal. Once this is proved, it follows that R' is Cohen-Macalay, yet $W(k)[\![t]\!] \to R'$ is module-finite, hence injective (due to equality of dimensions), so by the regularity of $W(k)[\![t]\!]$ we can apply Miracle Flatness Theorem (23.1 in Matsumura's "Commutative Ring Theory") to conclude!

So it remains to prove that J is principal. By successive approximation (using J-adic completeness and separatedness), an element $r' \in J$ is a generator if it generates J/J^2. Let $(\mathbf{E}, \mathbf{E}')$ be the universal pair of deformations over $W(k)[\![t,t']\!]$, so the functor on complete local noetherian $W(k)[\![t,t']\!]$-algebras A (with residue field k) representing the condition that $F_{E_0/k}$ lifts to A is represented by the quotient $W(k)[\![t,t']\!]/J$. Hence, for $A = W(k)[\![t,t']\!]./J^2$ and the elliptic curves $\mathscr{E} = \mathbf{E}_A$ and $\mathscr{E}' = \mathbf{E}'_A$ and the "universal" isogeny $\phi_0 : \mathscr{E}_{A/J} \to \mathscr{E}'_{A/J}$ modulo the square-zero ideal $I = J/J^2 \subseteq A$, the condition on a complete local noetherian A-algebra A' (with residue field k) that $(\phi_0)_{A'/I}$ lifts to an isogeny over A' is exactly the condition that $A \to A'$ kills J. But by using finer deformation theory arguments, in Proposition 6.8.6 of Katz-Mazur (whose proof does not involve earlier material from that book) it is shown that the obstruction to such a lifting is always given by annihilation of a single element of the base ring A. This proves that I is principal, so J/J^2 is monogenic, and so we are done. ■

2. An auxiliary moduli problem

To get a handle on the moduli scheme for order-p finite flat subgroup schemes of $\Gamma[p]$, we need to introduce a finer moduli problem whose associated deformation ring for Γ_0 will be finite flat over R'. By Theorem 23.7 in Matsumura's "Commutative Ring Theory", a noetherian local ring is regular if it admits a flat local extension that is regular. Thus, once we construct a finer moduli problem whose deformation ring is finite flat over R', it will suffice to prove regularity for those deformation rings.

Definition 2.1. Let $C \to S$ be a smooth separated commutative group scheme with 1-dimensional fibers. For a closed S-subgroup scheme G in C such that $G \to S$ is finite locally free of constant rank n, a *generator* of G is an element $g \in G(S)$ such that the invertible ideal sheaves $\mathscr{I}_{[a](g)}$ of the points $[a](g) \in G(S)$ for $a \in \mathbf{Z}/n\mathbf{Z}$ satisfy the condition that the invertible ideal sheaf $\prod \mathscr{I}_{[a](g)}$ coincides with $\mathscr{I}_G \subset \mathscr{O}_C$.

We will develop some properties of this notion only when n is a prime. The case of more general n requires much more work (essentially because groups of prime order are cyclic, whereas groups of other orders can fail to be cyclic); it is discussed thoroughly in Katz–Mazur.

Note that the formation of the invertible ideals $\mathscr{I}_{[a](g)}$ commutes with base change on S (as we saw in class quite generally for sections of smooth separated maps with fibers of pure dimension 1), as does the formation of $\mathscr{I}_G$ (due to the *flatness* of $\mathscr{O}_G$ over S, which ensures that the short exact sequence $0 \to \mathscr{I}_G \to \mathscr{O}_C \to \mathscr{O}_G \to 0$ on C remains short exact after any base change on S). Thus, the property of being a "generator" of G commutes with any base change on S.

In the case of $\mathbf{Z}[1/n]$-schemes, there are no surprises:

Example 2.2. Suppose S is a $\mathbf{Z}[1/n]$-scheme, so $G \to S$ is finite étale. Then we claim that g is a generator of G in the sense defined above if and only if $g(\overline{s})$ generates $G(\overline{s})$ for all geometric points $\overline{s}$ of S. To prove this, first suppose that g is a generator of G. By preservation of this condition under base change to geometric fibers, we reduce to the case when $S = \operatorname{Spec} k$ for an algebraically closed field k of characteristic not dividing n. Then the finite étale G consists of n distinct k-points (and is reduced). But $\prod \mathscr{I}_{[a](g)}$ is the ideal sheaf of the closed subscheme of C supported at the multiples of g, with multiplicities equal to $n/\text{order}(g)$. But reducedness of $\mathscr{O}_G = \mathscr{O}_C/\prod \mathscr{I}_{[a](g)}$ then forces g to have order n, and hence it generates $G(k)$ since the size of $G(k)$ is n.

Conversely, suppose that $g(\overline{s})$ generates $G(\overline{s})$ for all $\overline{s}$. It follows that $g(\overline{s})$ has order exactly n, so the sections $[a](g) \in G(S)$ are pairwise disjoint. Hence, the ideal sheaf $\prod \mathscr{I}_{[a](g)}$ is the ideal sheaf of the disjoint union of the $[a](g)$ as a closed subscheme of C. But each of these lies in G, so their disjoint union does as well. That disjoint union is a rank-n finite étale closed subscheme of G, which is itself finite étale of rank n over S, so for rank reasons the $[a](g)$'s exhaust G. That is, G inside of C is the disjoint union of the $[a](g)$'s, whence its ideal sheaf in $\mathscr{O}_C$ is the product of the $\mathscr{I}_{[a](g)}$'s.

The next example is more interesting.

Example 2.3. Let E be an elliptic curve over a field k of characteristic $p > 0$, and let $G = \ker F_{E/k}$ be the kernel of the Frobenius isogeny $E \to E^{(p)}$. This is an order-p infinitesimal subgroup scheme of E, and it is the only closed subgroup scheme of E supported at the origin and of degree p over k. (Indeed, for any smooth curve over a field, at a rational point there is a unique closed subscheme of any desired finite degree supported there. This expresses the fact that a discrete valuation ring has a unique quotient of each positive length.) But there is another way to make such a closed subscheme: the pth power of the invertible ideal sheaf $\mathscr{I}_e$ of the identity section. This says exactly that e generates G. Likewise, e also generates $E[p]$ when E is supersingular (as then $E[p]$ is infinitesimal of order p^2)!

The case of prime order has the following special feature:

Proposition 2.4. *Let (E,G) over R' denote the universal deformation of $(E_0, \ker F_{E_0/k})$. There is a finite faithfully flat local extension of R' that is universal for the property of G acquiring a generator after base change.*

Proof. By Proposition 1.2, note that R' is $W(k)$-flat, hence $\mathbf{Z}$-flat. Our problem makes sense more generally for any pair (E,G) over any ring A, and we will consider it in that generality. (The locality property in the case of initial interest is automatic, since $\ker F_{E_0/k}$ in E_0 has a unique generator, namely 0.) Let F be the functor on A-algebras A' that assigns the set of generators of $G_{A'}$ in $E_{A'}$. We will prove that this is represented by a finite A-scheme (to be denoted $G^\times$; e.g., for $G = \mu_p = \operatorname{Spec} A[t]/(t^p - 1)$ the scheme $G^\times$ turns out to be the scheme $\operatorname{Spec} A[t]/(\Phi_p)$ of "primitive pth roots of unity, proved in 1.12.9 in Katz–Mazur). Then when A is $\mathbf{Z}$-flat (as in the case of interest) we will prove that $G^\times \to \operatorname{Spec} A$ is a flat surjection, so this will complete the proof .

Recall that $\mathscr{I}_G$ is an invertible ideal sheaf in $\mathscr{O}_E$, and its formation commutes with any base change on A (due to the A-flatness of G), so any power $\mathscr{I}_G^n$ defines a closed A-subscheme $G^{(n)} \subset E$ that is A-finite (due to being quasi-finite and proper) and also A-flat (due to the local flatness criterion from Matsumura, also used in the proof of the fibral flatness criterion from HW7). Thus, for any $g \in G(A')$ the "generator" condition is a problem of equality for two A'-points of the projective A-scheme $\mathrm{Hilb}^p_{G^{(p)}/A}$ from Exercise 3 in HW8. As such, it follows that the functor F on A-algebras is represented by a projective A-scheme $G^\times$. But F is also a subfunctor of G since $F(A')$ is the subset of elements in $G(A') = G_{A'}(A')$ that are generators of $G_{A'}$ in $E_{A'}$, so $G^\times$ represents a subfunctor of G. The A-scheme $G^\times$ is proper, and any proper monomorphism is a closed immersion (since proper quasi-finite maps are finite by Zariski's Main Theorem, and finite monomorphisms are closed immersions due to Nakayama's Lemma). Thus, $G^\times$ is a finite A-scheme.

Lemma 2.5. *All geometric fibers of $G^\times \to A$ have rank at most $p-1$.*

Proof. Passing to geometric points, we may assume that $A = k$ is an algebraically closed field. Thus, G is either the constant group $\mathbf{Z}/p\mathbf{Z}$ or $\mathrm{char}(k) = p$ and G is μ_p or α_p. If $G = \mathbf{Z}/p\mathbf{Z}$ then its closed subscheme $G^\times$ is readily seen to be $(\mathbf{Z}/p\mathbf{Z})^\times = G - \{0\}$. Now suppose $\mathrm{char}(k) = p$ and $G = \mu_p$ or α_p (so the elliptic curve E is respectively ordinary or supersingular). We have to prove that the closed subscheme $G^\times$ in G is not equal to G. In other words, we just have to construct some k-algebra B and $g \in G(B)$ that is not a generator of G_B in E_B. Consider any k-finite B and $g \in G(B)$ corresponding to some $z \in \mathfrak{m}_B$, so it generates G_B inside of the formal group precisely when $\prod_{i=0}^{p-1}(X - [i](z))$ is not a unit multiple of X^p in $B[\![X]\!]$. The term for $i = 0$ is X, and the others are $X - zu_i$ for $u_i \in B$ lifting $i \in k^\times$, so $u_i \in B^\times$. Thus, the product has linear term that is a $B^\times$-multiple of z^{p-1}, so provided that $z^{p-1} \neq 0$ in B we are done. Take $B = k[t]/(t^p)$ and $z = t$. ∎

Now assume that A is $\mathbf{Z}$-flat. The restriction of $G^\times \to \operatorname{Spec} A$ over $\operatorname{Spec} A[1/p]$ is étale surjective. Indeed, over $A[1/p]$ the group G becomes finite étale of order p, and its geometric fibers are all $\mathbf{Z}/p\mathbf{Z}$ there. Hence, over some étale cover of $\operatorname{Spec} A[1/p]$ the pullback of G becomes the constant group $\mathbf{Z}/p\mathbf{Z}$ (HW8, Exercise 4(iii)), for which it is clear by inspection that the scheme $G^\times$ is the constant scheme associated to $(\mathbf{Z}/p\mathbf{Z})^\times$ (check!).

The fiber ranks of $G^\times \to \operatorname{Spec} A$ over geometric points s of $\operatorname{Spec} A$ are all at most $p-1$ (Lemma 2.5), yet over $\operatorname{Spec} A[1/p]$ the map is finite flat of degree $p-1$. By a special case of Mumford's theorem on flattening stratifications (see 6.4.3 in Katz-Mazur for an exposition), a finite map between noetherian schemes with all fiber ranks at most some integer n universally becomes finite locally free of rank n over some closed subscheme of the base. Thus, there is a closed subscheme Z of $\operatorname{Spec} A$ that is universal for the property of $G^\times \to \operatorname{Spec} A$ becoming finite locally free of rank $p-1$ after base change. But over $\operatorname{Spec} A[1/p]$ this map is already finite locally free of rank $p-1$, so $Z[1/p] = \operatorname{Spec} A[1/p]$. In other words, the ideal in A that cuts out Z becomes 0 in $A[1/p]$. But $A \to A[1/p]$ is *injective*, so the ideal of Z vanishes. That is, $Z = \operatorname{Spec} A$, so $G^\times \to \operatorname{Spec} A$ is finite locally free of rank $p-1$. This completes the proof of Proposition 2.4. ∎

3. Proof of main result

By Proposition 2.4, to prove the regularity of the universal deformation ring R' for $(E_0, \ker F_{E_0/k})$, it suffices to instead prove regularity for its finite faithfully flat cover given by the deformation ring R'' classifying pairs $(E, g \in E[p])$ consisting of a deformation E of E_0 and a section g of $E[p]$ such that g generates an order-p finite flat closed subgroup scheme of $E[p]$ (necessarily lifting $\ker F_{E_0/k}$). This latter condition means that the invertible ideal sheaf $\prod_{i=0}^{p-1} \mathscr{I}_{[i](g)}$ on E, whose zero scheme is a finite flat subscheme of E containing 0, is a subgroup scheme. (See the paragraph preceding Lemma 2.5 for a discussion of why this ideal sheaf has zero scheme that is finite flat over the base.)

Over R'' there is a universal deformation $(E'', P \in E''[p](R''))$. Under the Serre–Tate equivalence between p-divisible groups over R'' and commutative formal groups over R'' on which $[p]$ is an isogeny, consider the formal group corresponding to the connected p-divisible group $E''[p^\infty]$. (This is the same as the formal group of E''.) Upon choosing a formal coordinate X, it makes sense to evaluate this on the universal point P to get an element $X(P) \in \mathfrak{m}_{R''}$. The natural local composite map $W(k)[\![t]\!] = R \to R' \to R''$ is finite flat, and provides another element $t \in \mathfrak{m}_{R''}$. Since $\dim R'' = 2$, its regularity (and hence that of R') will follow from:

Proposition 3.1. *The maximal ideal $\mathfrak{m}_{R''}$ is generated by $X(P)$ and t.*

Proof. We first claim that p vanishes in the quotient $R''/(X(P))$. Over this ring, the *origin* generates a finite flat subgroup scheme. That is, the pth infinitesimal neighborhood of the identity section (which is finite flat over the base) is a subgroup scheme of the elliptic curve, or equivalently of its formal group. So to prove $p = 0$ in this ring, it suffices to prove more generally over any ring A that if $X^p = 0$ is a formal subgroup scheme of a formal group law $A[\![X]\!]$ over A then necessarily $p = 0$ in A. The group law $m(X, Y) \in A[\![X, Y]\!]$ must have the form $m(X, Y) = X + Y + \dots$ where the omitted terms are in degrees ≥ 2. The condition that $X^p = 0$ is a formal subgroup scheme implies that $m(X, Y)^p \subseteq (X^p, Y^p)$. (This encodes stability under composition, omitting stability under inversion.) But $m(X, Y)^p = (X + Y)^p + \dots$ where the omitted terms are in degrees $\geq p + 1$. Hence, membership in (X^p, Y^p) implies that $(X + Y)^p - X^p - Y^p \in (X^p, Y^p)$ over A. The coefficient of $X^{p-1}Y$ is p, so we get $p = 0$ in A as desired.

Since $R''/(X(P))$ is a k-algebra, and $R/(p) = k[\![t]\!]$ classifies deformations of E_0, the quotient $R''/(X(P), t)$ classifies *trivial* deformations of the type classified by R''. Hence, this quotient must be k (i.e., it represents the 1-point functor). ■