SHIMURA–TANIYAMA FORMULA

BRIAN CONRAD

As we have seen earlier in the seminar in the talk of Tong Liu, if K is a CM field and (A, i) is a complex torus with CM by K, then A is necessarily an abelian variety and moreover the pair (A, i) descends to a number field $F \subseteq \mathbf{C}$ over which it has good reduction at all places. An important formula of Shimura and Taniyama describes Frobenius actions on reductions of this abelian variety at primes of F in terms of the action by elements of K.

To be precise, fix a prime $\mathfrak{p}$ of F and let q be the cardinality of its residue field k. The reduction $\overline{A}$ of A over k has an action by L in the isogeny category over k. Since K is its own centralizer in $\mathrm{End}_k^0(\overline{A})$ for dimension reasons, it follows by $\mathbf{Z}$-finiteness of $\mathrm{End}_k(\overline{A})$ that the central element given by q-Frobenius in $\mathrm{End}_k(\overline{A})$ is induced by the action of a unique nonzero element $\pi \in \mathscr{O}_K$ via the Néron model. In particular, π acts with p-power degree and so the ideal $\pi\mathscr{O}_K$ has all prime factors over p. The problem Shimura and Taniyama took up was this: find the factorization of this ideal. More specifically, for each place w of K over p, they gave a formula for $\mathrm{ord}_w(\pi)$ in terms of q, $[K_w : \mathbf{Q}_p] = e(w|p)f(w|p)$, and the CM type associated to (A, i).

The problem is really a local one, being intrinsic to the induced CM abelian variety over the p-adic field $F_{\mathfrak{p}}$, so the proof should be local. The original proof of Shimura and Taniyama was global, and it involved a close study of tangent spaces and some mild "unramifiedness" hypotheses (for K and F) over p. These unramifiedness conditions were sufficient for their proof of the main theorem on complex multiplication, and once they had the main theorem they could use it to return to the present situation and eliminate their earlier unramifiedness conditions. Using p-divisible groups, in the final section of [Tate] Tate succeeded in doing two wonderful things: giving a purely local proof of the Shimura-Taniyama formula, and bypassing the need for unramifiedness restrictions right from the start. In fact, Tate's approach shows that the Shimura-Taniyama formula is really a special case of a general theorem for p-divisible groups with "complex multiplication" over integer rings of p-adic fields. In these notes, we flesh out the details of Tate's argument, and in so doing we also develop the required background from the theory of p-divisible groups. (The one serious result we need from that theory is the Serre–Tate equivalence between connected p-divisible groups and certain commutative formal groups over complete local noetherian rings with residue characteristic p.)

In what follows, all group schemes are tacitly understood to be commutative if we do not say otherwise.

1. CM types

Let K be a CM field, and let C be a field of charactertistic 0 (such as $\mathbf{C}$, or $\overline{\mathbf{Q}}_p$). We assume C is sufficiently large so that it splits K. Hence, the set $H = \mathrm{Hom}_{\mathbf{Q}}(K, C)$ of $\mathbf{Q}$-algebra maps has size $2g = [K : \mathbf{Q}]$, where $g = [K_0 : \mathbf{Q}]$ for the maximal totally real subfield $K_0 \subseteq K$. For each $\varphi \in H$, let C_φ denote the ring C made into an K-algebra via φ. The canonical map of $\mathbf{Q}$-algebras

$$C \otimes_{\mathbf{Q}} K \to \prod_{\varphi \in H} C_\varphi$$

defined by $c \otimes \ell \mapsto (c\varphi(\ell))_\varphi$ is an isomorphism.

Example 1.1. Let A be a g-dimensional abelian variety over a subfield $F \subseteq C$, and assume there is given an embedding $i : K \hookrightarrow \mathrm{End}_F^0(A)$, so the tangent space $t_A = \mathrm{Tan}_0(A)$ is an $F \otimes_{\mathbf{Q}} L$-module. Thus, $C \otimes_F t_A \simeq t_{A_C}$ is a module over $C \otimes_F (F \otimes_{\mathbf{Q}} K) \simeq C \otimes_{\mathbf{Q}} K \simeq \prod_{\varphi \in H} C_\varphi$, where A_C is the base change of A to an abelian variety over C. Hence, we get a corresponding isotypic decomposition $t_{A_C} \simeq \prod_{\varphi \in H}(t_{A_C})_\varphi$. By the complex-analytic theory and Lefschetz' principle (i.e., descending (A, i) to a finitely generated subfield of F that may

then be embedded into $\mathbf{C}$), it follows that $\dim_C(t_{A_C})_\varphi \leq 1$ for all $\varphi \in H$, with equality for a subset $\Phi \subseteq H$ of size g that is a set of representatives for the free action of $\mathrm{Gal}(K/K_0)$ on H. We call Φ the *CM type* of $(A,i)_{/F}$.

The preceding example motivates:

Definition 1.2. A *CM type* for K (over C) is a set of representatives in H for the free action by $\mathrm{Gal}(K/K_0)$.

To better understand the passage between the set Φ and the $F \otimes_{\mathbf{Q}} K$-module t_A, we record the following mechanical theorem (whose proof we recommend the reader to skip, as it is thoroughly uninteresting):

Theorem 1.3. *Let $F \subseteq C$ be a subfield and let T be an $F \otimes_{\mathbf{Q}} K$-module with $d = \dim_F T$. The following are equivalent:*

(1) *With respect to the decomposition $F \otimes_{\mathbf{Q}} K \simeq \prod_i F_i$ as a finite product of fields, the associated decomposition $\prod_i T_i$ of T satisfies $\dim_{F_i} T_i \leq 1$ for all i.*
(2) *With respect to the decomposition $C \otimes_{\mathbf{Q}} K \simeq \prod_{\varphi \in H} C_\varphi$, the associated decomposition $C \otimes_F T \simeq \prod_{\varphi \in H} T_\varphi$ satisfies $\dim_C T_\varphi \leq 1$ for all φ.*

(*When these conditions hold, clearly the set $H_T = \{\varphi \in H \,|\, T_\varphi \neq 0\}$ has size d.*) *If T' is another $F \otimes_{\mathbf{Q}} K$-module with F-dimension d such that T' satisfies these equivalent conditions, then T' and T are isomorphic as $F \otimes_{\mathbf{Q}} K$-modules if and only if $H_T = H_{T'}$ as subsets of H.*

Remark 1.4. For an arbitrary subset $H' \subseteq H$, we have not claimed $H' = H_T$ for some T of F-dimension $\#H$ satisfying the above equivalent conditions. In fact, the existence of such a T is a non-trivial condition that we will return to in a later talk in the study of reflex fields (with $d = [K_0 : \mathbf{Q}]$).

Proof. Since $F \otimes_{\mathbf{Q}} K$ is a finite product of fields, any finite module over this ring is locally free. The first condition says that T is locally free with local ranks at most 1 at all points of $\mathrm{Spec}(F \otimes_{\mathbf{Q}} K)$. The second condition says that the $C \otimes_{\mathbf{Q}} K$-module $C \otimes_F T$ is locally free with local ranks at most 1 at all points of $\mathrm{Spec}(C \otimes_{\mathbf{Q}} K)$.

Note that as $C \otimes_{\mathbf{Q}} K$-modules we have $C \otimes_F T \simeq (C \otimes_{\mathbf{Q}} K) \otimes_{F \otimes_{\mathbf{Q}} K} T$, and the ring map $F \otimes_{\mathbf{Q}} K \to C \otimes_{\mathbf{Q}} K$ is faithfully flat. Thus, for the equivalence of conditions (1) and (2) in the theorem it suffices to prove more generally that if $A \to A'$ is a faithfully flat map of rings, r is a non-negative integer, and M is a finitely presented A-module, then the quasi-coherent sheaf $\mathscr{F} = \widetilde{M}$ on $\mathrm{Spec}\, A$ is locally free with local ranks at most r at all points if and only if its quasi-coherent pullback $\mathscr{F}'$ on $\mathrm{Spec}\, A'$ is locally free with local ranks at most r at all points. A finitely presented module over a ring is locally free if and only if it is flat, so faithful flatness of $\mathrm{Spec}\, A' \to \mathrm{Spec}\, A$ gives the equivalence of local freeness for $\mathscr{F}$ and $\mathscr{F}'$. For a comparison of local ranks we may check on residue fields (since $\mathrm{Spec}\, A' \to \mathrm{Spec}\, A$ is surjective), and so we can assume A and A' are fields. This case is trivial, so we have proved the equivalence of (1) and (2).

Now let T be another $F \otimes_{\mathbf{Q}} K$-module, and assume $H_T = H_{T'}$. We want to prove that T and T' are isomorphic as $F \otimes_{\mathbf{Q}} L$-modules. By (1), the problem is to prove that the kernels of the maps

$$F \otimes_{\mathbf{Q}} K \to \mathrm{End}_{F \otimes_{\mathbf{Q}} K}(T), \;\; F \otimes_{\mathbf{Q}} K \to \mathrm{End}_{F \otimes_{\mathbf{Q}} K}(T')$$

coincide. The formation of these kernels commutes with extension on F so applying the extension of scalars $F \to C$ reduces us to the case $F = C$. This special case is clear. ∎

2. Main result and remarks

Let C be an algebraic closure of $\mathbf{Q}_p$ for a prime p. Any embedding $K \hookrightarrow C$ of our CM field into C determines a place w on K over p. More specifically,

$$H = \mathrm{Hom}_{\mathbf{Q}}(K, C) = \mathrm{Hom}_{\mathbf{Q}_p}(\mathbf{Q}_p \otimes_{\mathbf{Q}} K, C) = \mathrm{Hom}_{\mathbf{Q}_p}(\prod_{w|p} K_w, C) = \coprod_{w|p} \mathrm{Hom}_{\mathbf{Q}_p}(K_w, C),$$

and the subset $H_w \subseteq H$ of embeddings $\varphi : K \hookrightarrow C$ inducing w on K corresponds to the set of $\mathbf{Q}_p$-embeddings $K_w \hookrightarrow C$. Hence, $\#H_w = [K_w : \mathbf{Q}_p]$. For *any* CM type Φ on K (with respect to C), we define $\Phi_w = \Phi \cap H_w$ inside of H.

Let (A, i) be an abelian variety of dimension g over a finite extension $F/\mathbf{Q}_p$ inside of C, equipped with CM by K over F. Replacing F with a finite extension if necessary, we may and do assume A has good reduction. Let $\mathscr{A}$ be the (proper) Néron model of A over $\mathscr{O}_F$, so $\mathscr{A}$ is an abelian scheme and K is embedded in

$$\mathrm{End}_F^0(A) = \mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{End}_{\mathscr{O}_F}(\mathscr{A}) \hookrightarrow \mathrm{End}_k^0(\mathscr{A}_k),$$

where k is the residue field of F and $\mathscr{A}_k$ denotes the reduction of $\mathscr{A}$ (so it is an abelian variety of dimension g over k).

Since K is a number field of degree $2g$ and (in the isogeny category of abelian varieties over k) it acts on the g-dimensional abelian variety $\mathscr{A}_k$, consideration of $V_\ell(\mathscr{A}_k)$ for $\ell \neq \mathrm{char}(k)$ shows that K is its own centralizer in $\mathrm{End}_k^0(\mathscr{A}_k)$. Letting q_0 denote the size of k, the q_0-Frobenius in $\mathrm{End}_k^0(\mathscr{A}_k)$ lies in the center and so lies in K. It even lies in $K^\times$. Thus, there is a unique $\pi_0 \in K^\times \subseteq \mathrm{End}_F^0(A) = \mathrm{End}_{\mathscr{O}_F}^0(\mathscr{A})$ lifting $\mathrm{Frob}_{\mathscr{A}_k, q_0}$. Since $K \cap \mathrm{End}_k(\mathscr{A}_k)$ is a $\mathbf{Z}$-finite subring of K, we must have $\pi_0 \in \mathscr{O}_K$. Our main goal is to prove:

Theorem 2.1. *With notation as above,*

$$\frac{\mathrm{ord}_w(\pi_0)}{\mathrm{ord}_w(q_0)} = \frac{\#\Phi_w}{\#H_w} \ (= \frac{\#\Phi_w}{[K_w : \mathbf{Q}_p]}).$$

Remark 2.2. The case of empty Φ_w can happen for some w, which is to say $\mathrm{ord}_w(\pi_0) = 0$.

Of course, the "same" formula may be asserted in the global setting with $\mathscr{O}_F$ replaced with the algebraic local ring at a prime over p in a number field (and A assumed to have good reduction at this prime). The proof of this "uncompleted" version is immediately reduced to the above setup. This version over number fields is the one originally given by Shimura and Taniyama, but the local version is what we needed in the development of Honda–Tate theory. Moreover, this local version will also suffice for our proof of the main theorem of complex multiplication (following the ideas of Shimura and Taniyama, but using more modern algebro-geometric language).

It is also important to note at the outset that the truth of the formula is insensitive to replacing F with a finite extension or passing to an isogenous abelian variety (as such an isogeny gives an isogeny on the necessarily proper Néron models and gives an *equality* of CM types on K with respect to C). Thus, by increasing the base field and passing to an isogenous abelian variety, we can assume that $\mathscr{O}_K$ acts on A. The key to Tate's proof of Theorem 2.1 is to replace our problem for A with a problem for its associated p-divisible group over $\mathscr{O}_F$ (whose identity component may be viewed as a formal group with complex multiplication). We shall interpret all four terms in the two fractions in the Shimura–Taniyama formula in terms of p-divisible groups, and in this way we will see that the formula is a special case of a rather general formula for p-divisible groups equipped with "complex multiplication".

3. Group schemes and p-divisible groups

By the "easy" half of Tate's isogeny theorem (injectivity), valid over any field, $V_p(A)$ is a free module of rank 1 over $K \otimes_{\mathbf{Q}} \mathbf{Q}_p$. Hence, we may and do consider $T_p(A)$ as a faithful module that is free of rank 1 over $\mathscr{O}_K \otimes_{\mathbf{Z}} \mathbf{Z}_p \simeq \prod_{w|p} \mathscr{O}_{K_w}$. This gives rise to a corresponding module decomposition

$$T_p(A) \simeq \prod_{w|p} T_w(A)$$

where $T_w(A)$ is free of rank 1 over $\mathscr{O}_{K_w}$, so $T_w(A)$ has $\mathbf{Z}_p$-rank equal to $[K_w : \mathbf{Q}_p] = \#H_w$. We wish to pass from consideration of $T_p(A)$ to a suitable collection of finite flat group schemes over $\mathscr{O}_F$.

The group scheme $\mathscr{A}[p^n]$ over $\mathscr{O}_F$ is a finite flat module scheme over $\mathscr{O}_K/(p^n) \simeq \prod_{w|p} \mathscr{O}_{K_w}/(p^n)$, so we get a functorial decomposition

$$\mathscr{A}[p^n] \simeq \prod_{w|p} G_{w,n}$$

with each $G_{w,n}$ an $\mathscr{O}_{K_w}/(p^n)$-module scheme (built as a closed subgroup scheme via kernels of idempotents). Since $\prod_w G_{w,n}$ is $\mathscr{O}_F$-flat, by Serre's trick we get that all $G_{w,n}$ are finite flat over $\mathscr{O}_F$. Hence, $G_{w,n}$ is a

finite flat $\mathscr{O}_{K_w}/(p^n)$-module scheme over $\mathscr{O}_F$, and its generic fiber is identified with the w-componment of the finite étale F-scheme $A[p^n]$ that is free of rank 1 over $\mathscr{O}_{K_w}/(p^n)$ on the level of geometric points (over F).

Clearly $\pi_0 \in \mathscr{O}_K$ acts on each $G_{w,n}$ through its nonzero image in $\mathscr{O}_{K_w}$ (where it may be a unit!), and the action by π_0 on the closed fiber over k is the q_0-Frobenius endomorphism of the closed fiber due to the "universal commutativity" of the q_0-Frobenius in the category of k-schemes. The diagram

$$0 \to \mathscr{A}[p] \to \mathscr{A}[p^{n+1}] \overset{\text{“}p\text{”}}{\to} \mathscr{A}[p^n] \to 0$$

is a short exact sequence of finite flat group schemes. Thus, the left exact sequence

$$0 \to G_{w,1} \to G_{w,n+1} \overset{\text{“}p\text{”}}{\to} G_{w,n} \to 0$$

is short exact (as it may be checked on k-fibers, where it is at least left-exact and then comparison of orders gives the result). Hence, $\{G_{w,n}\}$ is a p-divisible group with height $\#H_w = [K_w : \mathbf{Q}_p]$.

Since the formation of the connected-étale sequence is compatible with finite products, the product of the sequences

$$0 \to G^0_{w,n} \to G_{w,n} \to G^{\text{ét}}_{w,n} \to 0$$

is the connected-étale sequence

$$0 \to \mathscr{A}[p^n]^0 \to \mathscr{A}[p^n] \to \mathscr{A}[p^n]^{\text{ét}} \to 0.$$

We now recall the "connected-étale sequence" for general p-divisible groups. Let $\{H_n\}_{n\geq 1}$ be a p-divisible group over a complete local noetherian ring R. The quotient mapping $H_{n+1} \to H_n$ is induced by multiplication by p on H_{n+1}, so multiplication by p on $H^{\text{ét}}_{n+1}$ uniquely factors through the étale quotient $H^{\text{ét}}_n$ of H_n (using that $H^{\text{ét}}_{n+1}$ is an étale quotient of H_{n+1}). This provides maps $H^{\text{ét}}_{n+1} \to H^{\text{ét}}_n$. There are also induced maps $H^{\text{ét}}_n \to H^{\text{ét}}_{n+1}$ that are closed immersions on the geometric closed fibers and hence are closed immersion (by Nakayama's Lemma). In particular, $H^{\text{ét}}_1$ is naturally a closed subgroup of $H^{\text{ét}}_n$ for all n. Hence, it makes sense to ask if $\{H^{\text{ét}}_n\}$ is a p-divisible group over R. There is also a directed system $\{H^0_n\}$, and it makes sense to ask if this is a p-divisible group over R. We shall now verify that both systems are p-divisible groups.

Since local base change (with such base rings as given) is compatible with the formation of the connected-étale sequence of a finite flat group scheme, making a faithfully flat local base change on R if necessary allows us to assume that the residue field is perfect. Passing to the residue field commutes with the formation of the connected-étale sequence, and residually the connected-étale sequence is functorially *split* (since the residue field is perfect). Thus, we get left-exact sequences of reductions

$$0 \to \overline{H}^0_1 \to \overline{H}^0_{n+1} \to \overline{H}^0_n, \;\; 0 \to \overline{H}^{\text{ét}}_1 \to \overline{H}^{\text{ét}}_{n+1} \to \overline{H}^{\text{ét}}_n$$

whose product is the diagram

$$0 \to \overline{H}_1 \to \overline{H}_{n+1} \to \overline{H}_n \to 0$$

that is *exact*.

Hence, we can count orders to get $\#\overline{H}^0_n = (\#\overline{H}^0_1)^n$ and $\#\overline{H}^{\text{ét}}_n = (\#\overline{H}^{\text{ét}}_1)^n$. Thus, the left-exact diagram

$$0 \to H^0_1 \to H^0_{n+1} \to H^0_n \to 0$$

is a short exact sequence for order reasons, whence $\{H^0_n\}$ is a p-divisible group. Using the snake lemma (in the category of *fppf* abelian sheaves over $\operatorname{Spec} R$) we conclude that in the 3×3 commutative diagram of connected-étale sequences at levels 1, $n+1$, and n (with connected parts along the left side and étale parts along the right side), the short exactness for the left and middle columns gives it for the right column.

We conclude that $\{G^0_{w,n}\}_{n\geq 1}$ is a p-divisible group for each w, and that the product of these over all w is the p-divisible group $\{\mathscr{A}[p^n]^0\}_{n\geq 1}$. The same goes for the étale parts.

Remark 3.1. Since $G_{w,n}$ is a finite flat $\mathscr{O}_{K_w}/(p^n)$-module scheme whose generic fiber is free of rank 1, and by functoriality of the connected-étale sequence both $G^0_{w,n}$ and $G^{\text{ét}}_{w,n}$ are finite flat $\mathscr{O}_{L_w}/(p^n)$-module schemes whose generic fibers are finite free over $\mathbf{Z}/(p^n)$ (due to the p-divisible group property!), it follows from rank considerations on the generic fiber that exactly one of $\{G^0_{w,n}\}_{n\geq 1}$ or $\{G^{\text{ét}}_{w,n}\}_{n\geq 1}$ vanishes. Of course, which one vanishes may depend on w.

Our goal is to re-state the Shimura-Taniyama formula in Theorem 2.1 in terms of the p-divisible group $\{G_{w,n}\}$ equipped with its $\mathscr{O}_{K_w}$-action.

4. Serre–Tate theorem

The power of working with p-divisible groups is that connected ones have a good concept of "dimension". This rests on:

Theorem 4.1 (Serre–Tate)**.** *Let $(R, \mathfrak{m})$ be a complete local noetherian ring with residue characteristic p.*

(1) *If $\mathscr{G} = \{\mathscr{G}_n\}_{n\geq 1}$ is a connected p-divisible group over R with height h, then the augmented topological R-algebra $\mathscr{O}(\mathscr{G}) := \varprojlim \mathscr{O}(\mathscr{G}_n)$ is topologically isomorphic to the augmented R-algebra $R[\![X_1, \ldots, X_d]\!]$ equipped with its $(\mathfrak{m}, \underline{X})$-adic topology, and as such this is a commutative formal Lie group for which $[p]$ is finite flat of degree p^h. Moreover, $\mathscr{O}(\mathscr{G}_n)$ is the quotient ring corresponding to the p^n-torsion in this formal Lie group, and these form a cofinal system of $(\mathfrak{m}, \underline{X})$-adic quotients of $R[\![\underline{X}]\!]$.*

(2) *If $\mathscr{R} \simeq R[\![\underline{X}]\!]$ is a commutative formal group law such that the maps $[p]^* : \mathscr{R} \to \mathscr{R}$ are finite flat of some degree, necessarily of the form p^h for some $h \geq 0$, then the finite flat kernels $\mathscr{G}_n = \ker[p^n]_{\mathrm{Spf}(\mathscr{R})}$ form a p-divisible group over R that recovers $\mathscr{R}$ via the recipe in* (1)*.*

In (1), we call d the *dimension* of $\mathscr{G}$. For example, if $\mathscr{G} = \{\mathscr{A}[p^n]^0\}$ then the inverse limit in (1) recovers the complete local ring $\mathscr{O}^\wedge_{\mathscr{A},0}$ along the identity on the closed fiber, whence $d = \dim A$ in this case. Note that for the example $\{G^0_{w,n}\}$ of interest to us, there is generally no abelian scheme giving rise to it in this manner (via formal completion along the identity).

The significance of the theorem is that it provides an equivalence of categories between the category of connected p-divisible groups over R and the category of commutative formal Lie groups over R that have "finite height" (in the sense of $[p]^*$ being finite flat); this latter property is something we may check by working over the residue field of R because formal power series rings $R[\![\underline{X}]\!]$ in finitely many variables are R-flat (as R is noetherian).

Proof. To prove (2), granting (1), we have to show that for the augmentation ideal $\mathscr{I}$, the ideals $[p^n]^*(\mathscr{I})$ are $(\mathfrak{m}, \underline{X})$-adically cofinal. But $[p]^*(X_j) = pX_j + (\deg \geq 2)$ with $p \in \mathfrak{m}$ (!), so the cofinality is obvious.

Now we turn to the proof of (1). First granting the result over the residue field (which is where the real idea is needed), let us explain the lengthy deduction of the general case. Choose an augmented topological isomorphism $\mathscr{O}(\overline{\mathscr{G}}) \simeq k[\![\underline{X}]\!]$. Pick liftings $R[\![\underline{X}]\!] \to \mathscr{O}(\mathscr{G}_n)$ of the quotient maps $k[\![\underline{X}]\!] \twoheadrightarrow \mathscr{O}(\overline{\mathscr{G}}_n)$, and arrange these choices to be compatible with change in n. This can be arranged because $\mathscr{O}(\mathscr{G}_{n+1}) \to \mathscr{O}(\mathscr{G}_n)$ is a surjection between *finite free* R-modules.

By Nakayama's Lemma, the mapping $R[\![\underline{X}]\!] \to \mathscr{O}(\mathscr{G}_n)$ to a finite free R-module target is surjective, whence due to R-module splittings of the surjections $\mathscr{O}(\mathscr{G}_{n+1}) \twoheadrightarrow \mathscr{O}(\mathscr{G}_n)$ we get two conclusions: (i) $\varprojlim \mathscr{O}(\mathscr{G}_n)$ is topologically isomorphic as an R-module to a product of countably many copies of R, and (ii) the natural map $R[\![\underline{X}]\!] \to \varprojlim \mathscr{O}(\mathscr{G}_n)$ is *surjective* and splits in the sense of R-modules. By the construction of the countable product decomposition in (i) for the inverse limit as an R-module, it follows that the formation of the module splitting in (ii) is compatible with passage to the quotient modulo $\mathfrak{m}$, whence by the result assumed over the residue field the kernel of the surjection in (ii) lies in $\cap_{m\geq 1}\mathfrak{m}^m R[\![\underline{X}]\!] = 0$.

Hence, our map of R-algebras

$$R[\![\underline{X}]\!] \to \varprojlim \mathscr{O}(\mathscr{G}_n)$$

is an isomorphism. This is even a topological isomorphism: its formation commutes with passage to quotients modulo any $\mathfrak{m}^N$ ($N \geq 1$), and for artinian R the ideals $\mathfrak{a}_n = \ker(R[\![\underline{X}]\!] \twoheadrightarrow \mathscr{O}(\mathscr{G}_n)$ are a system of *open* ideals (as each $\mathscr{O}(\mathscr{G}_n)$ has finite length), so a beautiful theorem of Chevalley [Mat, Exercise 8.7] (see hint in the back of the book!) gives the cofinality of the $\mathfrak{a}_n$'s. This is the desired topological aspect for the isomorphism.

As a consequence of the topological nature of the isomorphism, artinian points can be "read off" from the inverse limit description, and so we get a *functorial* formal group law on $R[\![\underline{X}]\!]$ (via the group laws on the $\mathscr{G}_n$'s), with the formation of this group law commuting with passage to the residue field. Hence, $[p]^*$ is *finite flat* (as this is assumed known after reduction over the residue field, and can be pulled up by $\mathfrak{m}$-adic completeness and the local flatness theorem). We likewise see that $\mathscr{G}_n$ is the p^n-torsion on our formal group

law over R because this is true on the level of artinian points (by *construction* of the formal group law on the inverse limit). Consequently, taking $n = 1$ shows that the finite flat map $[p]^*$ has degree p^h, completing the argument over R (granting the results over the residue field).

Now we have to treat the case when $R = k$ is a field of characteristic p. In this case we have to go beyond formal manipulations as above. The brilliant idea of Serre and Tate is to recast everything in terms of the system of torsion by finite iterates of relative Frobenius, rather than powers of p. Since we are in the equicharacteristic case over a field, each of the *local* finite flat k-groups $\mathscr{G}_n$ is killed by some iterate $F_{\mathscr{G}_n}^{\nu(n)}$ of the relative Frobenius. But for $m \geq n$ we have $\mathscr{G}_m[F^n] \subseteq \mathscr{G}_n$ (since $p = VF$), so the kernels $\mathscr{G}[F^n]$ make sense as *finite* flat local k-groups and as an inverse system these are "commensurable" with respect to the $\mathscr{G}_n$'s. Hence, it suffices to find a topological k-algebra isomorphism

$$k[\![\underline{X}]\!] \simeq \varprojlim \mathscr{O}(\mathscr{G}[F^n])$$

inducing isomorphisms $k[\![\underline{X}]\!]/(\underline{X}^{p^r}) \simeq \mathscr{O}(\mathscr{G}[F^r])$ for all $r \geq 1$. Note that all $\mathscr{G}[F^r]$'s have the *same* tangent space along the identity, say of dimension d, so $\#\mathscr{G}[F] = p^d$ by the structure theorem for finite local commutative group schemes over a field of characteristic p. Hence, we may construct k-algebra surjections

$$k[\![X_1, \ldots, X_d]\!]/(X_1^{p^r}, \ldots, X_d^{p^r}) = k[X_1, \ldots, X_d]/(X_1^{p^r}, \ldots, X_d^{p^r}) \twoheadrightarrow \mathscr{O}(\mathscr{G}[F^r])$$

respecting change in $r \geq 1$, so we will be done *if* these surjections are necessarily isomorphisms. That is, we want $\#\mathscr{G}[F^r] = p^{rd}$ for all $r \geq 1$.

If we can make abstract exact sequence sequences

$$0 \to \mathscr{G}[F] \to \mathscr{G}[F^{r+1}] \to \mathscr{G}[F^r] \to 0$$

for all r, then we can compute the desired orders by induction on r. Since $\mathscr{G}[F^{r+1}] \subseteq \mathscr{G}_{r+1}$ and $\mathscr{G}[F^r] \subseteq \mathscr{G}_r$ with $[p] : \mathscr{G}_{r+1} \to \mathscr{G}_r$ *faithfully flat* (!), the identity $p = FV$ gives the required exact sequences of finite flat k-groups. ∎

By the Serre–Tate theorem, we can now make sense of $G_w^\wedge = \{G_{w,n}^0\}_{n \geq 1}$ as a formal $\mathscr{O}_{K_w}$-module scheme over $\mathscr{O}_F$. We therefore have an isomorphism of formal groups

$$\prod_{w|p} G_w^\wedge \simeq \{\mathscr{A}[p^n]^0\}_{n \geq 1} \simeq \mathscr{A}_0^\wedge,$$

with the right side equal to the formal group of the abelian scheme $\mathscr{A}$. In particular, the total dimension (in the sense of formal groups) is $\dim A = \#\Phi$.

Now comes a crucial step that translates the numerator on the right side of the Shimura–Taniyama formula into something related to the integral structure:

Theorem 4.2. *With notation as above,* $\dim G_w^\wedge = \#\Phi_w$.

Proof. We want to compute the $\mathscr{O}_F$-rank of the tangent space to the "formal group" $G_w^\wedge$ along its identity section. Since the tangent space is identified with the collection of $\mathscr{O}_F[\varepsilon]$-points lifting the 0-section modulo ε, from the functorial description

$$\prod_{w|p} G_w^\wedge(\mathscr{O}_F[\varepsilon]) \simeq \mathscr{A}_0^\wedge(\mathscr{O}_F[\varepsilon])$$

we see $\mathrm{Tan}_0(G_w^\wedge)$ is the $\mathscr{O}_{K_w} \otimes_{\mathbf{Z}_p} \mathscr{O}_F$-module component of the $\mathscr{O}_K \otimes_{\mathbf{Z}} \mathscr{O}_F$-module $\mathrm{Tan}_0(\mathscr{A}_0^\wedge)$. Therefore, it is enough to prove that $(\mathrm{Tan}_0(\mathscr{A}_0^\wedge))[1/p]$ as an $K \otimes_{\mathbf{Q}} F$-module has $K_w \otimes_{\mathbf{Q}_p} F$-component with F-dimension $\#\Phi_w$. But $\mathrm{Tan}_0(\mathscr{A}_0^\wedge) \simeq \mathrm{Tan}_0(\mathscr{A})$ (!), so inverting p on this gives t_A as an $K \otimes_{\mathbf{Q}} F$-module. Hence, our problem is reduced to showing that the $K \otimes_{\mathbf{Q}} C$-module $t_A \otimes_F C = t_{A_C}$ has w-component with C-dimension $\#\Phi_w$. But this is obvious due to how Φ relates to t_{A_C} and how Φ_w is *defined* (as $H_w \cap \Phi$). ∎

Corollary 4.3. *The directed system* $G_w = \{G_{w,n}\}_{n \geq 1}$ *is a* p*-divisible group over* $\mathscr{O}_F$ *with height* $\#H_w$, $\dim G_w^0 = \#\Phi_w$, *and an action by* $\mathscr{O}_{K_w}$ *with* $\pi_0 \in \mathscr{O}_{K_w}$ *acting as a lift of the* q_0*-Frobenius on the closed fiber.*

5. A theorem on p-divisible groups

In view of the preceding corollary, it suffices to prove the following general result in order to complete the proof of Theorem 2.1:

Theorem 5.1. *Let Γ be a p-divisible group over the integer ring $\mathscr{O}_F$ of a p-adic local field F such that $\dim \Gamma^0 = d$ and the height is $h > 0$. Assume that on Γ there is an action by the integer ring $\mathscr{O}_K$ for a p-adic field K such that $[K : \mathbf{Q}_p] = h$; that is, $T_p(\Gamma_{/F})$ is an $\mathscr{O}_K$-module of rank 1.*

If there is an element $\pi \in \mathscr{O}_K - \{0\}$ lifting the action of Frob_k on Γ_k then $d/h = \mathrm{ord}_F(\pi)/\mathrm{ord}_F(q)$, where q is the cardinality of the residue field k of $\mathscr{O}_F$.

Proof. The meaning of the theorem is that π^h and q^d are unit multiples. Using the short exact sequences

$$0 \to \Gamma_n^0 \to \Gamma_n \to \Gamma_n^{\text{ét}} \to 0$$

and passing to generic fibers, we get a short exact sequence

$$0 \to T_p(\Gamma^0_{/F}) \to T_p(\Gamma_{/F}) \to T_p(\Gamma^{\text{ét}}_{/F}) \to 0$$

as $\mathscr{O}_K$-modules that are finite free as $\mathbf{Z}_p$-modules. Since the middle term has rank 1 over $\mathscr{O}_K$, either $\Gamma^0 = 0$ or $\Gamma^{\text{ét}} = 0$.

If $\Gamma^0 = 0$ (so Γ is étale) then $d = 0$ and Frob_k is an isomorphism on Γ_k, so π acts as an *automorphism*. This rules out the possibility of π^r being a unit multiple of p for some $r \geq 1$ (as the action by p has nontrivial kernel on Γ), whence $\pi \in \mathscr{O}_K - \{0\}$ must be a unit.

It remains to assume $\Gamma^{\text{ét}} = 0$, so $\Gamma = \Gamma^0$ is connected. We have $\mathscr{O}(\Gamma) \simeq \mathscr{O}_F[\![Y_1, \ldots, Y_d]\!]$, and the mapping $[p]^* : \mathscr{O}(\Gamma) \to \mathscr{O}(\Gamma)$ is finite flat of order $p^h = \|p\|_K$. Clearly the map $x \mapsto \deg([x]_\Gamma)$ is a multiplicative map from $\mathscr{O}_K - \{0\}$ to $p^{\mathbf{Z}}$ sending units to 1 and p to $\|p\|_K$, so it must agree with the normalized absolute value. Hence, $\deg[x]_\Gamma = \|x\|_K$. We therefore want π^h and q^d acting on Γ to have the same degree. Since $\deg[p]_\Gamma = p^h$, we have $\deg[q]_\Gamma = q^h$. Thus, $\deg[q^d]_\Gamma = q^{dh}$, so we want $\deg[\pi]_\Gamma = q^d$. But this latter degree can be computed on Γ_k, and by hypothesis on this closed fiber the action of π is the q-Frobenius. On the k-algebra $\mathscr{O}(\Gamma) \simeq k[\![Y_1, \ldots, Y_d]\!]$ this Frobenius endomorphism clearly is finite flat with degree q^d, so we are done. ∎

References

[Mat] H. Matsumura, *Commutative ring theory*, Cambridge Univ. Press, 1994, Cambridge.
[Tate] J. Tate, Classes d'isogénie des variétés abéliennes sur un corps fini. *Séminaire Bourbaki*, 21:95–110, 1968.

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA
E-mail address: bdconrad@math.lsa.umich.edu