Λ-ADIC p-DIVISIBLE GROUPS, I

HARUZO HIDA

Contents

1. Introduction

Let p be a prime. Let R_0 be a discrete valuation ring of mixed characteristic unramified over $\mathbb{Z}_{(p)}$ (with finite residue field $\mathbb{F}$ of characteristic p). Let $R_\infty = \bigcup_n R_n$ for $R_n = R_0[\mu_{p^n}]$; so, R_n is a discrete valuation ring with residue field $\mathbb{F}$. Write K_n for the quotient field of R_n and $\overline{K}_\infty$ for an algebraic closure of K_∞. A Λ-adic BT group $G_{/R_0}$ (a Λ-BT group) is by definition an inductive limit of Barsotti–Tate groups G_{n/K_0} defined over K_0 such that $G_n \times_{K_0} K_n$ is the generic fiber of a Barsotti–Tate group G_{n/R_n} defined over R_n with an action of the Iwasawa algebra $\Lambda = W[[x]]$ as endomorphisms over K_0; so, Λ acts on G_{n/R_n} (resp. G_{n/K_0}) as endomorphisms of Barsotti–Tate grousp over R_n (resp. over K_0). Here W is a discrete valuation ring finite flat over $\mathbb{Z}_p$. We impose the following conditions:

- (RT) The generic fiber G_n is defined over K_0 (as an étale Barsotti–Tate group over K_0) and the action of Λ on G_{n/K_0} is also defined over K_0;
- (CT) Writing $\gamma = 1 + x$, we have $G_n = \mathrm{Ker}(\gamma^{p^n} - 1 : G \to G)$ (closed immersion);
- (DV) $G(\overline{K}_\infty) \cong \Lambda^{*r}$ for $\Lambda^* := \mathrm{Hom}_{cont}(\Lambda, \mathbb{Q}_p/\mathbb{Z}_p)$ (Pontryagin dual);
- (DL) We have a Cartier self duality $G_n[p^m] \times G_n[p^m] \to \mu_{p^m}$ over K_n which, after taking the limit, gives the duality $TG \times G(\overline{K}_\infty) \to \mu_{p^\infty}$ over K_∞. Here $TG = \varprojlim_n TG_n(\overline{K}_\infty)$ (for $TG_n = \varprojlim_m G_n[p^m](\overline{K}_\infty))$ with respect to the map $G_{n+1} \twoheadrightarrow G_n$ dual to $G_n \hookrightarrow G_{n+1}$.

The first talk of the two lectures at CRM (Montréal) in September 2005 while the author was a Clay research scholar, and the note was revised on November 3, 2009; the author is supported partially by NSF grant: DMS 0244401 and DMS 0456252.

(OD) The connected component of G_n over each strict henselization of R_n is a multiplicative group (i.e., isomorphic to a product of copies of μ_{p^∞}) for all n (so, G_n is ordinary);

(U) On the special fiber, we have the Frobenius map F and its dual V. Thus we have a splitting $G_{\mathbb{F}} = G^\circ \times G^{et}$ so that $G^\circ = \mathrm{Ker}(e_F)$ and $G^{et} = \mathrm{Ker}(e_V)$ for $e_F = \lim_{n\to\infty} F^{n!}$ and $e_V = \lim_{n\to\infty} V^{n!}$. Then we have an automorphism U of G such that U commutes with F and V and U on G^{et} lifts $F|_{G^{et}}$.

Thus a Λ-adic BT group is give by data (G_{n/R_n}) with the above compatibility conditions. If $G_{/R_0}$ and $H_{/R_0}$ are Λ-adic BT groups, a morphism $f : G \to H$ of Λ-adic BT groups is given by a Λ linear map $f : G \to H$ of abelian fppf sheaves over R_∞ such that the induced morphism $f_n : G_n \to H_n$ of Barsotti–Tate groups over R_∞ descends to a morphism $G_{n/R_n} \to H_{n/R_n}$ of Barsotti–Tate groups and it further commutes with the action of $\mathrm{Gal}(\overline{K}_\infty/K_0)$ on the generic fibers. We write $\mathrm{Hom}_{\Lambda\text{-BT}_{/R_0}}(G, H)$ for the Λ-module of such morphisms (defined genertically over K_0).

If $L \in \mathrm{End}_{\Lambda\text{-BT}_{/R_0}}(T)$ is a linear operator, we can think of the p-divisible part $G[L]^{div}$ of $\mathrm{Ker}(L : G \to G)$. By the classification of Λ-modules, if $\det(L) \neq 0$, $G[L]^{div}$ has finite corank, and it is a classical Barsotti–Tate group over R_∞. Of course, starting with a self-dual Barsotti–Tate group H with a lift U, $TH \otimes_{\mathbb{Z}_p} \Lambda^*$ gives a constant Λ-adic BT-group. We hereafter suppose that all Λ-adic BT-groups we consider are non-constant. This could be said that the representation of $\mathrm{Gal}(\overline{K}_\infty/K_0)$ on TG is a non-constant deformation of TG_1 in the sense of Mazur.

A p-ordinary Barsotti–Tate group H over a discrete valuation ring $B_{/\mathbb{Z}_{(p)}}$ with quotient field F is called a $GL(2g)$-type if it is self dual with a local ring $A \subset \mathrm{End}_{\mathrm{BT}_{/B}}(H)$ such that $TH \cong A^{2g}$. We call H minimal if A is generated by $\mathrm{Tr}(\sigma) \in A$ for all $\sigma \in \mathrm{Gal}(\overline{F}/F)$. For a Λ-adic BT group $G_{/R_0}$, if we have a local $\Lambda[U]$-algebra $\mathbb{T}$ inside $\mathrm{End}_{\Lambda\text{-BT}_{/R_0}}(G)$ such that $TG \cong \mathbb{T}^{2g}$ and $\mathbb{T}$ is self-adjoint under the duality, we call G a $GL(2g)$-type over $\mathbb{T}$. In this Λ-adic case, we call G minimal if $\mathbb{T}$ is generated by $\mathrm{Tr}(\sigma)$ and U topologically. Supposing the existence of such G (that we will see today), we can ask a lot of simple questions.

(Q1) If we are given G over a finite field $\mathbb{F}$ of characteristic p, can one lift it to characteristic 0? (Deformation question).

(Q2) Is there any systematic way of constructing such G over a given R_∞? If it exists, does it create all such G over R_∞ of $GL(2g)$-type? (Construction).

(Q3) If G is nonconstant, can $\det(U) \in \mathbb{T}^\times$ be algebraic over W? (Non-constancy)

(Q4) Let us give ourselves a Weil number $\alpha \in \overline{\mathbb{Q}} \cap W$ with $|\alpha| = \sqrt{p}$ of degree $2g$. Supposing α *ordinary* (that is, the minimal polynomial of α modulo p can only divisible by X^g not more), does $G[U - \alpha]^{div}$ descend to a discrete valuation ring? (Descent).

(Q5) Is it possible to embed the p-divisible part $G[U-\alpha]^{div}$ of $G[U-\alpha] = \mathrm{Ker}(U-\alpha)$ into an abelian scheme defined over a finite extension of R_∞? (Relation to abelian varieties).

(Q6) For a given minimal G_1 of $GL(2g)$-type with irreducible $TG_1 \otimes_{\mathbb{Z}} \overline{\mathbb{Q}}$, is there a universal G? (Universality). Here the universality is defined as follows. If we have a minimal p-divisible group H of $GL(2g)$-type with a morphism $i : G_1 \to H$ with finite kernel (so, $i \circ \mathrm{Tr}(\sigma|_{G_1}) = \mathrm{Tr}(\sigma|_H) \circ i$), we have a morphism $i_H : H \hookrightarrow G$ with finite kernel making the following diagram commutes:

$$\begin{tikzcd} G_1 \arrow[r, "i"] \arrow[d] & H \arrow[d, "i_H"] \\ G \arrow[r, equal] & G. \end{tikzcd}$$

The Λ-adic BT group cannot descend to (an inductive limit of) $G_{n/R}$ over a finite extension $R \subset R_\infty$ of R_0 (independent of n) unless it is a constant. Here is a reason for it. Suppose that G is minimal of $GL(2)$-type and suppose that G extends as a BT-group to the integral closure of $\mathbb{Z}[\frac{1}{N}]$ in R. If G is defined over a discrete valuation ring $R = \mathbb{Z}_p$ or $\mathbb{Z}_{(p)}$. Then by Raynaud's classification of p-ordinary divisible groups [R] 4.2, the determinant of the Galois representation on TG has to be the p-adic cyclotomic character χ. Thus TG is a deformation of TG_1 which is p-ordinary and of determinant χ. If TG_1 is modular whose residual representation is irreducible over $\mathbb{Q}[\sqrt{p^*}]$ ($p^* = (-1)^{(p-1)/2}p$), by Wiles (see [W]), the universal Galois deformation ring for p-ordinary deformations unramified outside Np with fixed determinant χ is of finite rank over $\mathbb{Z}_p$. Thus TG has to be constant; so, G has to be constant. Thus if such a G exists, at least R contains the p-adic valuation ring of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty/\mathbb{Q}$.

Questions related to the above have been studied in [H86b], [MW1], [Ti] and [Oh1]. Today I will give an automorphic way of constructing such G over $\mathbb{Z}_{(p)}$. By the solution of Galois deformation problems (of ordinary type) by Mazur and Wiles–Taylor, this gives almost all such Λ-adic BT-groups, basically solving (Q2) and (Q6) for $GL(2)$-type groups.

2. Construction over $\mathbb{Q}$

Fix a prime $p \geq 5$ and a positive integer N prime to p. We consider the modular curve $X_1(Np^r)$ which classify elliptic curves E with an embedding $\mu_{Np^r} \hookrightarrow E[Np^r] = \mathrm{Ker}(Np^r : E \to E)$. Suppose $N \geq 4$ so that $X_1(Np^r)$ gives a fine moduli of the problem. Let $J_r = \mathrm{Pic}^0_{X_1(Np^r)/\mathbb{Q}}$ be the Jacobian variety. Similarly we take J^r_s to be the Jacobian variety associated to the modular curve with the congruence subgroup

$\Gamma_s^r = \Gamma_1(Np^r) \cap \Gamma_0(p^s)$. Note that

$$\Gamma_s^r \backslash \Gamma_s^r \left(\begin{smallmatrix} 1 & 0 \\ 0 & p^{s-r} \end{smallmatrix}\right) \Gamma_1(Np^r) = \left\{ \left(\begin{smallmatrix} 1 & a \\ 0 & p^{s-r} \end{smallmatrix}\right) \middle| a \mod p^{s-r} \right\}$$
$$= \Gamma_1(Np^r) \backslash \Gamma_1(Np^r) \left(\begin{smallmatrix} 1 & 0 \\ 0 & p^{s-r} \end{smallmatrix}\right) \Gamma_1(Np^r).$$

Writing $U_r^s(p^{s-r}) : J_r^s \to J_r$ for the Hecke operator of $\Gamma_s^r \left(\begin{smallmatrix} 1 & 0 \\ 0 & p^{s-r} \end{smallmatrix}\right) \Gamma_1(Np^r)$. Then we have the following commutative diagram by the above identity:

$$\begin{array}{ccc} J_r & \xrightarrow{\pi^*} & J_s^r \\ \downarrow u & \swarrow u' & \downarrow u'' \\ J_r & \xrightarrow{\pi^*} & J_s^r, \end{array}$$

where the middle u' is given by $U_r^s(p^{s-r})$ and u and u'' are $U(p^{s-r})$. Thus if we take the ordinary projector $e = \lim_{n\to\infty} U(p)^{n!}$ on $J[p^\infty]$ for $J = J_r, J_s, J_s^r$, noting $U(p^m) = U(p)^m$, we have

$$J_s^{r,ord}[p^\infty] \cong J_r^{ord}[p^\infty],$$

where "*ord*" indicates the image of e.

We now identify $J[p^\infty](\mathbb{C})$ with a subgroup of $H^1(\Gamma, \mathbb{T}_p$ for $\mathbb{T}_p := \mathbb{Q}_p/\mathbb{Z}_p)$ for the congruence subgroup Γ defining the modular curve whose Jacobian is J. Since $\Gamma_s^r \triangleright \Gamma_1(Np^s)$, by the inflation restriction sequence, we have the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} H^1(\frac{\Gamma_s^r}{\Gamma_1(Np^s)}, \mathbb{T}_p) & \xrightarrow{\hookrightarrow} & H^1(\Gamma_s^r, \mathbb{T}_p) & \longrightarrow & H^1(\Gamma_1(Np^s), \mathbb{T}_p)^{\gamma^{p^r}=1} & \longrightarrow & H^2(\frac{\Gamma_s^r}{\Gamma_1(Np^s)}, \mathbb{T}_p) \\ \uparrow & & \cup\uparrow & & \uparrow\cup & & \uparrow \\ ? & \longrightarrow & J_s^r[p^\infty] & \longrightarrow & J_s[p^\infty][\gamma^{p^r}-1] & \longrightarrow & ? \end{array}$$

By sheer computation, we can prove $H^j_{ord}(\frac{\Gamma_s^r}{\Gamma_1(Np^s)}, \mathbb{T}_p) = 0$ and the all the vertical arrows above are injective, we get the controllability

$$\mathrm{Ker}(\gamma^{p^r} - 1 : J_s^{ord}[p^\infty] \to J_s^{ord}[p^\infty]) = J_r^{ord}[p^\infty].$$

Define $J_\infty^{ord}[p^\infty] = \varinjlim_r J_r^{ord}[p^\infty]$. For each character $\varepsilon : \Gamma/\Gamma^{p^r} \to \mu_{p^\infty}$, by the inflation and restriction technique that $J_\infty^{ord}[p] \otimes \mathbb{Z}[\varepsilon][\gamma - \varepsilon(\gamma)] \cong J_r^{ord}[p] \otimes \mathbb{Z}[\varepsilon][\gamma - \varepsilon(\gamma)] \cong J_1^{ord}[p]$. Thus $J_\infty^{ord}[p^\infty] \otimes \mathbb{Z}[\varepsilon][\gamma - \varepsilon(\gamma)]$ is a nontrivial p-divisible group. Taking the Pontryagin dual $T = J_\infty^{ord}[p^\infty]^*$, we find a surjection $\pi : \Lambda^m \twoheadrightarrow T$ for $m = \dim_{\mathbb{F}_p} J_1^{ord}[p]$. Then for a prime $P_\varepsilon = (\gamma - \varepsilon(\gamma)) \cap \Lambda$, T/PT is the dual of $J_\infty^{ord}[p^\infty] \otimes \mathbb{Z}[\varepsilon][\gamma - \varepsilon(\gamma)]$ which is $\mathbb{Z}_p$-free of rank m (by Nakayama's lemma). Thus $\mathrm{Ker}(\pi) \subset P_\varepsilon \Lambda^m$. Moving around ε, we find that $T \cong \Lambda^m$; so, $J_\infty^{ord}[p^\infty]$ is a Λ-adic BT-group satisfying (CT) and (DV). As for the duality, the canonical polarization of J_r gives rise to the self-duality pairing $[\cdot,\cdot]$ of $J_r[p^r]$ and $J_r \cong {}^tJ_r$. Let $U^*(p)$ (resp. $T^*(n)$) be the image of $U(p)$ (resp. Hecke operator $T(n)$) under the canonical Rosati involution of J_r in $\mathrm{End}(J_r)$. The Weil involution τ associated to $\left(\begin{smallmatrix} 0 & -1 \\ Np^r & 0 \end{smallmatrix}\right)$ satisfies $\tau U(p) \tau^{-1} = U^*(p)$

and $\tau T(n)\tau^{-1} = U^*(n)$ inside $\mathrm{End}(J_{r/\mathbb{Q}[\mu_{Np^r}]})$ because τ is only defined over $\mathbb{Q}[\mu_{Np^r}]$. Thus twisting the pairing by τ and $U(p)^{-r}$, we get the self-duality pairing $\langle\cdot,\cdot\rangle_r = [\cdot, \tau \circ U(p)^{-r}(\cdot)]$ of $J_r^{ord}[p^m]$. Writing $R_s^r : J_r^{ord}[p^\infty] \hookrightarrow J_s^{ord}[p^\infty]$ for the inclusion, and $N_r^s = \sum_{j=1}^{p^{s-r}} \gamma_r^j : J_s^{ord}[p^\infty] \to J_r^{ord}[p^\infty]$ for $\gamma_r = \gamma^{p^r}$, we can verify by computation

$$\langle R_s^r(x), y\rangle_s = \langle x, N_r^s(y)\rangle_r.$$

From this we get (DL) over $\mathbb{Q}[\mu_{Np^\infty}]$.

3. Construction over $\mathbb{Z}_{(p)}[\mu_{p^\infty}]$

We construct the generic fiber of a Λ-adic BT group, and in the following section, we extend it to $\mathbb{Z}_{(p)}[\mu_{p^\infty}]$. By the above construction, the Tate module $T_r = TJ_r^{ord}[p^\infty]$ carries Galois representations of Hecke eigenforms satisfying the following properties:

(1) cusp forms in $S_2(\Gamma_0(p) \cap \Gamma_1(N))$;
(2) all cusp forms in $S_2(\Gamma_1(Np^m))$ whose Neben character has p-conductor equal to p^m for $m = 1, 2, \ldots, r$.

By a theorem of Langlands (and Carayol), the ℓ-adic Galois representation ($\ell \neq p$) associated to such a Hecke eigenform f does not ramify at p on $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}[\mu_{p^r}])$ except for the case (1). In the case (1), it is semi-stable at p. Thus the abelian subvariety A_f attached to f extends a semi-abelian scheme over $\mathbb{Z}_{(p)}[\mu_{p^r}]$. Let ${}^tG_r = \sum_{f \text{ as above}} A_f \subset J_r$. Thus we have an inclusion ${}^tG_r \hookrightarrow J_r$. Let $J_r \twoheadrightarrow G_r$ be the dual quotient under the canonical polarization twisted by τ.

For any abelian subvariety A of $X = J_r$ stable under $U(q)$ for $q|Np$ and $T(n)$ for n prime to Np, if there exists an abelian subvariety B stable under the same Hecke operators such that $A + B = X$ and $A \cap B$ is finite, the abelian subvariety B is uniquely determined by A (the multiplicity one theorem). The abelian subvariety B is called the *complement* of A in X.

By definition, G_r and ${}^tG_r$ extend to a semi-abelian scheme over $\mathbb{Z}_{(p)}[\mu_{p^r}]$. The group $\mu = \mu_{p-1} \subset \mathbb{Z}_p^\times$ acts on J_r, ${}^tG_r$ and G_r by the diamond operators. If we define ${}^tG_r^{(0)}$ in ${}^tG_r$ to be the complement of abelian subvariety fixed by μ, ${}^tG_r^{(0)}$ and its dual quotient $G_r^{(0)}$ extend to an abelian scheme over $\mathbb{Z}_{(p)}[\mu_{p^r}]$. Anyway, we take the Néron model of these abelian schemes over $\mathbb{Z}_{(p)}[\mu_{p^r}]$ and take its p-divisible groups (whose p-power division group is at worst quasi-finite flat groups schemes).

Theorem 3.1. *We have* ${}^tG_r^{ord}[p^\infty] \cong J_r^{ord}[p^\infty] \cong G_r^{ord}[p^\infty]$ *canonically over* $\mathbb{Z}_{(p)}[\mu_{p^r}]$.

To prove the theorem, we first prove the following lemma.

Lemma 3.2. *Let R be a henselian discrete valuation ring with fraction field K. Let G_K and G'_K be either both Barsotti–Tate groups or both abelian schemes over K with abelian generic fiber. If G_K and G'_K are abelian schemes, let G_R and G'_R be the identity connected component of the Néron models over R of G_K and G'_K, respectively.*

If G_K and G'_K are Barsotti–Tate groups, we assume to have Barsotti–Tate groups G_R and G'_R over R whose generic fibers are isomorphic to G_K and G'_K, respectively.

(1) *Suppose we have a surjective morphism $f_K : G_K \to G'_K$ and an endomorphism $g_K : G_K \to G_K$ such that $\mathrm{Ker}(f_K : G_K \to G'_K) \subset \mathrm{Ker}(g_K : G_K \to G_K)$. Then for the extensions $f : G \to G'$ and $g : G \to G$ over R, $\mathrm{Ker}(f)$ is a closed subscheme of $\mathrm{Ker}(g)$;*

(2) *Suppose we have an injective morphism $f_K : G'_K \to G_K$ and an endomorphism $g_K : G_K \to G_K$ such that $\mathrm{Coker}(f_K : G'_K \to G_K)$ is the surjective image of $\mathrm{Coker}(g_K : G_K \to G_K)$. Then, for the extensions $f : G' \to G$ and $g : G \to G$ over R, $\mathrm{Coker}(f)$ is a quotient group of $\mathrm{Coker}(g)$.*

Proof. We first prove the assertion (1). Let A be a K-algebra. By the surjectivity of f_K, for each $x \in G'(A)$, we can find a fppf extension A'/A such that there exists $y \in G(A')$ with $f_K(y) = x$. Then $g_K(y) \in G(A')$ is well defined independently of the choice of y. Then by fppf descent, we conclude that $g_K(y) \in G(A)$. Thus we get a morphism of group functors $G'_K \to G_K$ sending x to $g_K(y)$. Since a functor morphism gives a unique morphism of schemes (Yoneda's lemma), we get a morphism $f'_K : G'_K \to G_K$ such that $f'_K \circ f_K = g_K$.

First suppose that G_K and G'_K are abelian schemes. Since G and G' are the connected components of the Néron models of G_K and G'_K, respectively (see [NMD] Proposition 7.4.3), any generic morphism ϕ_K of these schemes extends to a unique morphism over R. Then f'_K and f_K extend to morphisms $f' : G' \to G$ and $f : G \to G'$ over R, respectively, and f and f' satisfies $f' \circ f = g$, which shows that $\mathrm{Ker}(f)$ is a closed subscheme of $\mathrm{Ker}(g)$.

If G and G' are Barsotti–Tate groups, we only need to verify that extensions f and f' exist. This extension properties follows from [T] Theorem 4.

The second assertion is the dual of the first. □

Now we prove the theorem:

Proof. Note that over $\mathbb{Q}$, by the definition, $J_r^{ord}[p^\infty] \subset {}^tG_r^{ord}[p^\infty]$. Let $B = \mathrm{Ker}(J_r \to G_r)$ which is the complement of ${}^tG_r$. By definition, e kills $B[p^\infty]$; so, it kills the p-primary part of $H = B \cap {}^tG_r$. Thus over $\mathbb{Q}$, we have the identity in the theorem. Since H is finite, H is killed by $M \cdot U(p)^L$ for an integer M prime to p and another integer L sufficiently large. We apply the first statement of the lemma to the projection $f_{\mathbb{Q}} : {}^tG_{\mathbb{Q}} \to G_{\mathbb{Q}}$ and $g_{\mathbb{Q}} = M \cdot U(p)^L$. Thus by the lemma, we have $\mathrm{Ker}(f) \subset \mathrm{Ker}(M \cdot U(p)^L)$; so, we get an injection ${}^tG_r^{ord}[p^\infty] \hookrightarrow G_r^{ord}[p^\infty]$ which are p-divisible group of the same corank; so, the injection is a surjection. □

Corollary 3.3. *The natural morphism $i : {}^tG_r^{ord}[p^\infty] \to {}^tG_s^{ord}[p^\infty]$ is a closed immersion for $s > r$.*

Proof. We can factor the isomorphism $\iota_r : {}^tG_r^{ord}[p^\infty] \cong G_r^{ord}[p^\infty]$ as $\iota_r = {}^ti \circ \iota_s \circ i$. This shows that i is a closed immersion. □

Theorem 3.4. *Over $\mathbb{Z}_{(p)}[\mu_{p^s}]$, the natural inclusion ${}^tG_r^{ord}[p^\infty]$ into ${}^tG_s^{ord}[p^\infty]$ is a closed immersion whose image is equal to the kernel* $\mathrm{Ker}(\gamma^{p^r}-1)$ *on ${}^tG_s^{ord}[p^\infty]$ for all $s > r$.*

Proof. For simplicity, we write $\mathcal{G}_r$ for $G_r^{ord}[p^\infty]$. Look at the inclusion $i : \mathcal{G}_r \to \mathcal{G}_s$. Since i is a closed immersion, $\mathcal{H} := \mathrm{Im}(i)$ is a Barsotti–Tate subgroup of $\mathcal{G}_s$. Since $\mathcal{G}_s[p^n] \twoheadrightarrow \mathcal{G}_s[p^n]/\mathcal{H}[p^n]$ is an epimorphism of fppf abelian sheaves, $\mathcal{G}_s[p^n]/\mathcal{H}[p^n] = (\mathcal{G}/\mathcal{H})[p^n]$ is a finite flat group scheme. Thus $\mathcal{G}_s/\mathcal{H}$ is a Barsotti–Tate group. Generically, $\gamma^{p^r}-1 : \mathcal{G}_{s/K_s} \to \mathcal{G}_{s/K_s}$ factors through $\mathcal{G}_s/\mathcal{H}$ inducing an isomorphism $\mathrm{Im}(\gamma^{p^r}-1)_{/K_s} \cong (\mathcal{G}_s/\mathcal{H})_{/K_s}$; so, by Lemma 3.2, $\gamma^{p^r}-1$ factors through $\mathcal{G}_s/\mathcal{H}$ over R_r, getting a morphism $\pi : \mathcal{G}_s/\mathcal{H} \to \mathrm{Im}(\gamma^{p^r}-1)$. Restricting the projection $\mathcal{G}_s \twoheadrightarrow \mathcal{G}_s/\mathcal{H}$ to $\mathrm{Im}(\gamma^{p^r}-1) \subset \mathcal{G}_s$, we get a morphism: $\mathrm{Im}(\gamma^{p^r}-1) \to \mathcal{G}_s/\mathcal{H}$ of fppf abelian sheaves, which is generically the inverse of π, and hence we have $\mathrm{Im}(\gamma^{p^r}-1) \cong \mathcal{G}_s/\mathcal{H}$ over R_s. Thus we must have $\mathcal{H} = \mathrm{Ker}(\gamma^{p^r}-1)$ over R_s (as the category of fppf abelian sheaves is an abelian category), showing $\mathrm{Ker}(\gamma^{p^r}-1) = \mathrm{Im}(i : \mathcal{G}_r \to \mathcal{G}_s)$ as desired. □

References

Books

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

[MFG] H. Hida, *Modular Forms and Galois Cohomology*, Cambridge Studies in Advanced Mathematics **69**, Cambridge University Press, Cambridge, England, 2000.

[MFM] T. Miyake, *Modular Forms*, Springer, New York-Tokyo, 1989.

[NMD] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron Models*, Sp-ringer, New York, 1990.

Articles

[GS] R. Greenberg and G. Stevens, p-adic L–functions and p–adic periods of modular forms, Inventiones Math. **111** (1993), 407–447

[H86a] H. Hida, Iwasawa modules attached to congruences of cusp forms, Ann. Sci. Ec. Norm. Sup. 4th series **19** (1986), 231–273.

[H86b] H. Hida, Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms, Inventiones Math. **85** (1986), 545–613.

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

[MTT] B. Mazur, J. Tate and J. Teitelbaum, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, Inventiones Math. **84** (1986), 1–48

[MW] B. Mazur and A. Wiles, Class fields of abelian extensions of **Q**. Inventiones Math. **76** (1984), 179–330

[MW1] B. Mazur and A. Wiles, On p–adic analytic families of Galois representations, Compositio Math. **59** (1986), 231–264

[Oh1] M. Ohta, On the p-adic Eichler-Shimura isomorphism for Λ-adic cusp forms, J. reine angew. Math. **463** (1995), 49–98

[Oh2] M. Ohta, Ordinary p–adic étale cohomology groups attached to towers of elliptic modular curves, Compositio Math. **115** (1999), 241–301

[Oh3] M. Ohta, Ordinary p–adic étale cohomology groups attached to towers of elliptic modular curves. II, Math. Ann. **318** (2000), 557–583

[R] M. Raynaud, Schémas en groupes de type $(p, \dots, p)$. Bull. Soc. Math. France **102** (1974), 241–280

[T] J. Tate, p-divisible groups, Proc. Conf. on local filds, Driebergen 1966, Springer 1967, 158–183.

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

[W] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. **141** (1995), 443–551.