On proper and smooth schemes over $\mathbb{Z}$

December 5, 2019

Haoyang Guo

Abstract

In this expository article, we follow Fontaine's work [Fo2] and prove a result for the cohomology of a proper and smooth schemes over $\mathbb{Z}$.

1 Introduction

Our main theorem is the following.

Theorem 1.0.1 ([Fo2], Theorem 1)**.** *Let X be a proper and smooth scheme over $\mathbb{Q}$ that has good reduction everywhere. Then we have*

$$\mathrm{H}^j(X, \Omega^i_{X/\mathbb{Q}}) = 0, \ if \ i,j \in \mathbb{N}, \ i \neq j, \ and \ i+j \leq 3.$$

Corollary 1.0.2. *There is not proper and smooth scheme X over $\mathbb{Z}$ with the sheaf of differential $\Omega^1_{X/\mathbb{Z}}$ being free (for instance, Abelian scheme over $\mathbb{Z}$). And there exists no Calabi-Yau scheme of relative dimension ≤ 3 over $\mathbb{Z}$ (for instance, $K3$ surface).*

Proof. Assume X is a scheme over $\mathbb{Z}$ with $\Omega^1_{X/\mathbb{Z}} \cong \mathcal{O}_X^d$. Then we have

$$\mathrm{H}^0(X, \Omega^1_{X/\mathbb{Z}}) = \mathrm{H}^0(X, \mathcal{O}_X)^d \neq 0,$$

a contradiction to the Theorem 1.0.1. □

Here recall that a *Calabi-Yau scheme* X over $\mathbb{Z}$ is defined as a smooth proper scheme over $\mathbb{Z}$ such that $\Omega^{\dim(X)}_{X/\mathbb{Z}} \cong \mathcal{O}_X$ and

$$\mathrm{H}^i(X, \mathcal{O}_X) = 0, \ 1 \leq i \leq \dim(X) - 1.$$

The goal of this short note is to prove the Theorem 1.0.1, following [Fo2].

2 Proof of the Main theorem

For each prime number p, we fix an embedding of $\overline{\mathbb{Q}}$ in $\overline{\mathbb{Q}}_p$. Let G be the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and G_p be the decomposition group of p in G, isomorphic to the local Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

2.1 Decomposition of the Galois representations

First we reduce the main theorem to the following result about global Galois representations:

Proposition 2.1.1. *Let V be a finitely dimensional continuous representation of $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ over $\mathbb{Q}_7$. Assume V is unramified at any prime $\ell \neq 7$ and is crystalline at 7, with its Hodge-Tate weights at 7 contained in $\{0, 1, 2, 3\}$. Then there exists a G-equivariant filtration of subrepresentations*

$$0 \subset V_3 \subset V_2 \subset V_1 \subset V_0 = V,$$

such that

$$V_i/V_{i+1} \cong \mathbb{Q}_7(i)^{n_i},$$

where $\mathbb{Q}_7(i)$ is the G-representation given by the i-th Tate twist on the one-dimensional vector space $\mathbb{Q}_7$ with trivial action.

Proof of the Theorem 1.0.1. Let X be a proper smooth scheme over $\mathbb{Q}$ that has good reduction everywhere. Consider the G-representation $V = \mathrm{H}^n_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_7)(3)$ for $n \leq 3$, which is a finitely dimensional vector space over $\mathbb{Q}_7$. Then by the assumption that X has good reduction everywhere, V is unramified at any prime $\ell \neq 7$ and it crystalline at 7. Besides, since $n \leq 3$, by the Hodge-Tate decomposition V has Hodge-Tate weights inside $[0, 3]$. So by the Proposition 2.1.1, V admits a Galois equivariant filtration with factors being direct sums of cyclotomoc characters of weight $0, 1, 2, 3$.

Now by the Weil Conjecture for 7-adic cohomology of proper smooth variety over the finite field $\mathbb{F}_\ell$ (and the smooth base change theorem for 7-adic cohomology to compare the cohomology before/after the reduction of X mod ℓ), the eigenvalues of the mod-ℓ Frobenius operator on the 7-adic cohomology $\mathrm{H}^n_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_7)$ is an algebraic number of absolute value $\ell^{\frac{n}{2}}$ for any $\ell \neq 7$. In particular, since the Proposition 2.1.1 implies that V is the consecutive extension of cyclotomic characters, the absolute value of the Frobenius implies that

$$\mathrm{H}^n_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_7) = \begin{cases} 0, \ 2 \nmid n; \\ \mathbb{Q}_7(-\frac{n}{2}), \ 2|n. \end{cases}$$

In this way, $\mathrm{H}^n_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_7)$ vanishes when $n = 1, 3$, and equals to a direct sum of $\mathbb{Q}_7(-1)$ when $n = 2$. So by the Hodge-Tate decomposition for 7-adic cohomology (after the restriction from G to G_7), we get the Theorem 1.0.1. □

2.2 Fontaine-Laffaille functor

We then reduce to show the Proposition 2.1.1. Our strategy is to use the Fontaine-Laffaille functor and discuss the structure of the torsion Galois modules over $\mathbb{Z}_7$. The detailed discussion of Fontaine-Laffaille theory can be found in the their original article [FL]; for a short English survey, see [BM] Section 3.

We fix the notation in the rest of the article as follows: Let p be a prime number, k be a perfect field of characteristic p, $W = W(k)$ be the ring the Witt vector, and $K = \mathrm{Frac}(W)$. Let G_K be the Galois group $\mathrm{Gal}(\overline{K}/K)$.

Filtered Dieudonné module Recall that a *filtered Dieudonné module* M over W of weights $[0, r]$ is given by an W-module M together with the following datum:

(i) There exists a decreasing filtration of W-modules

$$M = \mathrm{Fil}^0 M \supset \mathrm{Fil}^1 M \supset \cdots \supset \mathrm{Fil}^r M.$$

(ii) For each $0 \leq i \leq r$, there exists a σ-semi-linear morphism

$$\varphi_i : \mathrm{Fil}^i M \to M,$$

such that on $\mathrm{Fil}^{i+1} M$ we have $\varphi_i(x) = p\varphi_{i+1}(x)$.

A morphism between two filtered Dieudonné module is an W-linear map that preserves the filtration and commutes with φ_i.

We denote by $\mathrm{MF}_W^{[0,r]}$ to the category of filtered Dieudonné module over W of weights $[0,r]$, and let $\mathrm{MF}_{W,f}^{[0,r]}$ be the full subcategory of $\mathrm{MF}_W^{[0,r]}$ consisting of those filtered modules of finite length over W that satisfies the following condition

$$\sum_{0\le i\le r} \varphi_i(\mathrm{Fil}^i M) = M.$$

Here we note that $\mathrm{MF}_{W,f}^{[0,r]}$ is an abelian category.

Fontaine-Laffaille functor Recall that the ring $\mathrm{A}_{\mathrm{cris}}$ is defined as the p-adic completion of the divided power envelope of $\mathrm{A}_{\mathrm{inf}}$ at the ideal $\ker(\theta) = (\xi)$, where $\theta : \mathrm{A}_{\mathrm{inf}} \to \mathcal{O}_{\mathbb{C}_p}$ is the canonical surjection and $\xi = \frac{[\epsilon]-1}{\varphi^{-1}([\epsilon])-1}$ is the element in $\mathrm{A}_{\mathrm{inf}}$. Here ϵ is the element $(1, \zeta_p, \zeta_{p^2}, \ldots)$ in $\mathcal{O}_{\mathbb{C}_p}^\flat$.

The ring $\mathrm{A}_{\mathrm{cris}}$ is a subring of the de Rham period ring $\mathrm{B}_{\mathrm{dR}}^+ = \varprojlim \mathrm{A}_{\mathrm{inf}}[\frac{1}{p}]/\xi^m$. It is equipped with a φ action, mapping ξ into the ideal $p\mathrm{A}_{\mathrm{cris}}$. Besides, the filtration of the de Rham period ring induces a canonical filtration on $\mathrm{A}_{\mathrm{cris}}$, given by

$$\mathrm{Fil}^i \mathrm{A}_{\mathrm{cris}} = \mathrm{A}_{\mathrm{cris}} \cap \xi^i \mathrm{B}_{\mathrm{dR}}^+.$$

So we can define the φ_i action on $\mathrm{Fil}^i\mathrm{A}_{\mathrm{cris}}$ as $\varphi_i = \varphi/p^i$. This makes $\mathrm{A}_{\mathrm{cris}}$ a filtered Dieudonné module, and so is the reduction $\mathrm{A}_{\mathrm{cris}}/p^n\mathrm{A}_{\mathrm{cris}}$ for $n \in \mathbb{N}$. We notice that by construction, $\mathrm{A}_{\mathrm{cris}}$ is equipped with an G_K-action that preserves the filtration and commutes with φ_i.

Now we recall the Fontaine-Laffaille functor:

Definition 2.2.1. *Let M be an object in $\mathrm{MF}_{W,f}^{[0,r]}$. The Fontaine-Laffaille functor $\underline{\mathrm{FL}}$ is is given by*

$$\underline{\mathrm{FL}}(M) := \mathrm{Hom}_{\mathrm{MF}}(M, \varinjlim \mathrm{A}_{\mathrm{cris}}/p^n\mathrm{A}_{\mathrm{cris}}),$$

which sends M to the category of finite length G_K modules over W with G_K-action induced by that on $\mathrm{A}_{\mathrm{cris}}$.

Here is one of the main result in the Fontaine-Laffaille theory:

Fact 2.2.2 (Equivalence)**.** [FL] The Fontaine-Laffille functor induces an equivalence of categories between the category $\mathrm{MF}_{W,f}^{[0,r]}$ and the category of *torsion crystalline representations over $\mathbb{Z}_p$ with weights inside* $[0,r]$.

Here recall the category of torsion crystalline representations over $\mathbb{Z}_p$ is the full subcategory of continuous G_K-modules of finite length that is of the form L_1/L_2, where $L_2 \subset L_1$ are two Galois lattices in some crystalline representation V over $\mathbb{Q}_p$.

p-adic bound of the different ideal We recall another main result in [Fo2], which we are not going to prove here:

Theorem 2.2.3. *Let r be an integer in the interval $(0, p-1)$. Let M be an object in $\mathrm{MF}_{W,f}^{[0,r]}$ that is killed by p. Suppose $U = \underline{\mathrm{FL}}(M)$ and H is the kernel of the action of $G_K = \mathrm{Gal}(\overline{K}/K)$ on U, with $L = \overline{K}^H$. Then we have*

$$v_p(\mathcal{D}_{L/K}) < 1 + \frac{r}{p-1},$$

where v_p is the p-adic valuation on L with $v_p(p) = 1$.

The proof is in the Section 3 in [Fo2], using the upper bounds of $v_p(\mathcal{D}_{L/K})$ given in 1.5 of [Fo1].

2.3 Structure of torsion representations for $p = 7$ and $r = 3$

We then study the structure of the torsion crystalline representations for $p = 7$, that is equipped with a continuous global action by $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We let the residue field k be the field $\mathbb{F}_7$ in the above discussion, and thereby we have $W = \mathbb{Z}_7$ and $K = \mathbb{Q}_7$.

Denote by $\mathcal{C}$ to be the category of finite torsion $\mathbb{Z}_7$ modules U with a continuous $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action that is unramified at any prime except possibly at 7. Here $\mathcal{C}$ is an abelian category. We let $\mathcal{C}_{\text{crys}}^{[0,3]}$ be the full subcategory of $\mathcal{C}$ consisting of those admissible modules U, in the sense that there exists some M in $\mathrm{MF}_{W,f}^{[0,3]}$ such that $U = \underline{\mathrm{FL}}(M)$.

Now we begin the discussion of torsion representations.

Lemma 2.3.1 (Triviality). *Let*

$$0 \longrightarrow U' \longrightarrow U \longrightarrow U'' \longrightarrow 0$$

be a short exact sequence in $\mathcal{C}_{\text{crys}}^{[0,3]}$, with G acting trivially on U' and U''. Then the action of G on U is trivial.

Proof. By the Fact 2.2.2 and the assumption, there exists a short exact sequence of Filtered Dieudonné modules

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0, \tag{1}$$

whose image under the Fontaine-Laffaille functor $\underline{\mathrm{FL}}$ is the one given in the Lemma. Then we have the following claim about the Galois action and the Filtration:

Claim 2.3.2. For $U = \underline{\mathrm{FL}}(M) \in \mathcal{C}_{\text{crys}}^{[0,3]}$, the G_7 action on U is unramified if and only if $\mathrm{Fil}^1 M = 0$.

Granting the Claim, since the G-action on U' and U'' are trivial, in particular the G_7 action are unramified, we know both $\mathrm{Fil}^1 M'$ and $\mathrm{Fil}^1 M''$ vanish. So from the exactness of (1) above we get $\mathrm{Fil}^1 M = 0$, which implies that the G action on U is unramified at 7. But by assumption the G-action on $U \in \mathcal{C}_{\text{crys}}^{[0,3]}$ is also unramified at all the primes p that is not at 7. So the action of G on U is unramified everywhere, which leads to the triviality (Here we note that the kernel of this action correspond to a field extension of $\mathbb{Q}$ unramified everywhere, which is $\mathbb{Q}$ itself). ☐

The next Lemma describe the simple object in $\mathcal{C}_{\text{crys}}^{[0,3]}$, which is the one of the places we need $p = 7$.

Lemma 2.3.3 (Simple objects). *Up to isomorphism, the only simple objects in $\mathcal{C}_{\text{crys}}^{[0,3]}$ are $\mathbb{F}_7(i)$ for $i = 0, 1, 2, 3$.*

Proof. Let U be a simple object in $\mathcal{C}_{\text{crys}}^{[0,3]}$, which is a finite dimensional $\mathbb{F}_7$ vector space with a continuous G-action, unramified everywhere except possibly at 7. Let H be the kernel of this action of G on U, and let $E = \overline{\mathbb{Q}}^H$, $F = E(\zeta_7)$, $n' = [F : \mathbb{Q}(\zeta_7)]$, $n = 6n' = [F : \mathbb{Q}]$. We also let H' be the $\mathrm{Gal}(\overline{\mathbb{Q}}/E)$. Then notice that since $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_7))$ is the kernel of the cyclotomic character of G on $\mathbb{F}_7(1)$, the subgroup H' is in fact the kernel of the G-action on $V = U \oplus \mathbb{F}_7(1) \in \mathcal{C}_{\text{crys}}^{[0,3]}$.

Now by applying the Theorem 2.2.3 on V, we get

$$\begin{aligned}
\frac{1}{n} v_7(\delta_{F/\mathbb{Q}}) &= \frac{1}{n} v_7(N_{F/\mathbb{Q}}(\mathcal{D}_{F/\mathbb{Q}})) \\
&= v_7(\mathcal{D}_{F/\mathbb{Q}}) \\
&< 1 + \frac{r}{7-1} \\
&\leq 1 + \frac{3}{6}.
\end{aligned}$$

Note that from the assumption of $U \in \mathcal{C}_{\text{crys}}^{[0,3]}$, the G-action on V is ramified only at 7. This suggests that the extension $F/\mathbb{Q}$ is ramified only at 7, with the discriminant $\delta_{F/\mathbb{Q}}$ being a power of 7. So we get

$$|\delta_{F/\mathbb{Q}}|^{\frac{1}{n}} < 7^{1+\frac{3}{6}}.$$

In this way, by using the bounds of degree in terms of discriminant (Odlyzko-Poitou-Serre), we get $n \leq 208$.

We then make the following claim:

Claim 2.3.4. The extension $F/\mathbb{Q}$ is only tamely ramified at 7.

Granting the Claim, since the higher ramification subgroup G_i of $\mathrm{Gal}(F/\mathbb{Q})$ for $i \geq 1$ is trivial, by the [Se] Chap IV, Section 1, Proposition 4, we have

$$|\delta_{F/\mathbb{Q}}|^{\frac{1}{n}} = 7^{\frac{\sum_{i=0}(\#G_i - 1)}{n}} = 7^{\frac{\#G_1 - 1}{n}} = 7^{\frac{n-1}{n}} < 7.$$

In particular, by the same method for the bounds of degree as above, we get $n \leq 10$. But notice that $n = 6n'$ for $n' \geq 1$, so we get $n' = 1$ and $F = \mathbb{Q}(\zeta_7)$, which suggests that the action of G on the finite dimensional $\mathbb{F}_7$ vector space U factors though $(\mathbb{Z}/7\mathbb{Z})^*$. In this way, by the simpleness of U, it must be of the form $\mathbb{F}_7(i)$ for $0 \leq i \leq 6$. And since U is in $\mathcal{C}_{\mathrm{crys}}^{[0,3]}$, we get $0 \leq i \leq 3$.

At last, we prove the Claim:

Proof of the Claim. If $F/\mathbb{Q}$ is not tamely ramified, since $n \leq 208$ and $6|n$, the wild ramified subgroup N at 7 is of order 7, which by Sylow's theory is the unique order 7 subgroup in $\mathrm{Gal}(F/\mathbb{Q})$. We take F' to be F^N, and let n'' be $[F' : \mathbb{Q}(\zeta_7)]$, then we have

$$n' = 7n''.$$

Note that since F' is tamely ramified over $\mathbb{Q}$, by the same method as above we have $[F' : \mathbb{Q}] = 6n'' \leq 10$. In particular, this suggests that $n'' = 1$, $F' = \mathbb{Q}(\zeta_7)$ and $F/\mathbb{Q}$ is of degree 42. But note that by taking the eigenvector of the order 7 element of G in U, and by the simpleness of U, the G action on U will factor though the order 6 quotient group, which contradicts that $F/\mathbb{Q}$ is of order 42. So we are done. □

□

Remark 2.3.5. As pointed out by Fontaine (Exercise), the above proof in fact shows the following: For any object $U \in \mathcal{C}_{\mathrm{crys}}^{[0,3]}$ that is $\mathbb{F}_7$-linear and corresponds to a field extension $E/\mathbb{Q}$, the action of G factors through a subgroup of $\mathrm{Gal}(E(\zeta_7)/\mathbb{Q})$, where the order of the latter divides 42.

Remark 2.3.6. It is not impossible to use other (concrete) prime numbers instead of 7; for whatever prime we choose, the difference will be how good the bound of degree is, and how complicated the discussion of modular representations of the finite Galois group is (as in the Claim).

The next Lemma describe the Ext group for $\mathbb{F}_7$-linear objects in $\mathcal{C}_{\mathrm{crys}}^{[0,3]}$.

Lemma 2.3.7 (Extension)**.** *In $\mathcal{C}_{\mathrm{crys}}^{[0,3]}$, except when $i = 0$ and $j = 3$, any $\mathbb{F}_7$-linear extension of $\mathbb{F}_7(i)$ by $\mathbb{F}_7(j)$ is split.*

Proof. We discuss the relation of i and j.

- If $i = j$, by twisting $-i$ if needed, we reduce to the case in Lemma 2.3.1.
- Assume $i > j$, and let $U = \underline{\mathrm{FL}}(M)$ be an extension of $\mathbb{F}_7(i)$ by $\mathbb{F}_7(j)$. Let M_i and M_j be the preimage of $\mathbb{F}_7(i)$ and $\mathbb{F}_7(j)$ under the Fontaine-Laffaille functor $\underline{\mathrm{FL}}$. Then since $i > j$, by the relation between the Hodge-Tate weights of torsion crystalline representations and the filtration of filtered Dieudonné modules, the filtration of M is given by

$$M = \mathrm{Fil}^0 M = \cdots = \mathrm{Fil}^j M \supsetneq \mathrm{Fil}^{j+1} M = \cdots = \mathrm{Fil}^i M \supsetneq \mathrm{Fil}^{i+1} M = 0.$$

  In particular, the embedding of $\mathrm{Fil}^i M \subset M$ induces a section of the projection $M \longrightarrow M''$, which makes M splits. So after applying the Fontaine-Fallaille functor, we see U splits as representation of G_7 (Note that a priori not the whole G). However, note that the G_7-action on $\mathbb{F}_7(i) \oplus \mathbb{F}_7(j)$ has kernel living inside $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_7)) \subset G$, while the G action on U is unramified at all the other primes. In this way, if U is nonsplit as an G-representation, we get a degree 7 extension of $\mathbb{Q}(\zeta_7)$ (see the Remark 2.3.5) that is unramified everywhere, which does not exist. So we are done.

- Assume $i < j$, U is nonsplit, and up to a twist we may assume $i = 0$. Then the matrix form of the G action has the form
$$\begin{pmatrix} \chi^j & * \\ & 1 \end{pmatrix}.$$
By the non-splitness of the representation, the image of G in this subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$ contains an element of order 7.

  We let H be the kernel of this action, $E = \overline{\mathbb{Q}}^H$, and $F = E(\zeta_7)$. Then as in the Remark 2.3.5, the field extension $F/\mathbb{Q}(\zeta_7)$ is of order 7 and unramified at every prime except at 7. This implies that the extension $F/\mathbb{Q}(\zeta_7)$ is wildly ramified, and $F/\mathbb{Q}$ is totally ramified at 7 and unramified at all the other prime numbers. We then make the following claim:

  Claim 2.3.8. The lower ramification index of order 7 elements in $\mathrm{Gal}(F/\mathbb{Q})$ is exactly equal to j.

  Granting this, the norm of the discriminant $\delta_{F/\mathbb{Q}}$ satisfies
$$|\delta_{F/\mathbb{Q}}|^{\frac{1}{42}} = 7^{\frac{1\cdot(42-7)+(j+1)\cdot 6}{42}} = 7^{\frac{41+6j}{42}}.$$
If $j \leq 2$, then the above value is smaller than 11.66, which by the upper bound of the degree using Odlyzko-Poitou-Serre method implies
$$[F : \mathbb{Q}] \leq 28,$$
contradicting to equality $[F : \mathbb{Q}] = 42$. So we are done.

□

Corollary 2.3.9. *In the category $\mathcal{C}^{[0,3]}_{\mathrm{crys}}$, the extension group $\mathrm{Ext}^1_{\mathcal{C}^{[0,3]}_{\mathrm{crys}}}(\mathbb{F}_7(i), \mathbb{F}_7(j))$ is trivial unless the following possible situations:*

- *When $i = 0$ and $j = 3$.*
- *When $i = j$, where the only nontrivial extension is $\mathbb{Z}/7^2(i)$.*

Proof. We first assume $i \neq j$, Then the only possible nonsplit $\mathbb{F}_7$-linear extension is given by the Lemma 2.3.7. If U is not killed by 7, then as an abelian group it is isomorphic to $\mathbb{Z}/7^2 e$, which is cyclic. We take U' to be the subrepresentation generated by $7e$, then in the category $\mathcal{C}^{[0,3]}_{\mathrm{crys}}$ we have
$$0 \longrightarrow U' \longrightarrow U \longrightarrow U/U' \longrightarrow 0,$$
where both U' and U/U' are $\mathbb{F}_7$-linear. Note that since the multiplication by 7 commutes with the G-action, U' and U/U' are isomorphic. In particular the Jordan-Hölder factors of U are two copies of isomorphic simple objects, which contradicts to the assumption of $i \neq j$.

At last, when $i = j$, by twisting $(-i)$ this reduces to the extension of $\mathbb{F}_7$ by $\mathbb{F}_7$ in the category of abelian groups, where the only nonsplit extension is $\mathbb{Z}/7^2$.

□

Our next Lemma describe the decomposition of the $\mathbb{F}_7$-linear object in $\mathcal{C}^{[0,3]}_{\mathrm{crys}}$, under a assumption of its Jordan-Hölder factors:

Lemma 2.3.10 (Decomposition)**.** *Assume U is an object in $\mathcal{C}^{[0,3]}_{\mathrm{crys}}$ that has no quotient isomorphic to $\mathbb{F}_7$. Then U can be written as*
$$U = \bigoplus_{i=1}^{3} N_i(i),$$
where N_i are torsion $\mathbb{Z}_7$-modules with trivial G-action.

Proof. We first notice the following two observations:

Claim 2.3.11. Any cyclic object in $\mathcal{C}_{\text{crys}}^{[0,3]}$ that has no quotient isomorphic to $\mathbb{F}_7$ is isomorphic to $\mathbb{Z}/7^n(i)$ for some $n \in \mathbb{N}$ and $i = 1, 2, 3$.

Claim 2.3.12. Any indecomposable object $U \in \mathcal{C}_{\text{crys}}^{[0,3]}$ that has no quotient isomorphic to $\mathbb{F}_7$ is cyclic, i.e. as an G-module it can be generated by one element in U.

We first assume those two Claims. Then the Lemma can be done by induction on the order of U: When U is of order 7, then it is $\mathbb{F}_7$ linear of dimension one, hence equals to some $\mathbb{F}_7(i)$ for $i = 1, 2, 3$. For general U, we can write it in terms of an extension sequence in $\mathcal{C}_{\text{crys}}^{[0,3]}$:

$$0 \longrightarrow U' \longrightarrow U \longrightarrow \mathbb{F}_7(i) \longrightarrow 0, \tag{$*$}$$

for some $i \neq 0$. Then we notice that U' also satisfies the assumption; otherwise by taking an quotient of U' by a sub G-module U'', the above sequence can produce the following short sequence

$$0 \longrightarrow \mathbb{F}_p(0) \longrightarrow U/U'' \longrightarrow \mathbb{F}_7(i) \longrightarrow 0,$$

which by the Lemma 2.3.7 is split. So we get a contradiction.

Now we discuss the decomposition of U'

- Assume U' is indecomposable. Then by the Claim above it has the form $\mathbb{Z}/7^n(j)$ for $j \neq 0$, and the sequence $(*)$ becomes

  $$0 \longrightarrow \mathbb{Z}/7^n(j) \longrightarrow U \longrightarrow \mathbb{F}_7(i) \longrightarrow 0.$$

  If this sequence splits, then we are done. Otherwise, either $i = j$ and by twisting and the Lemma 2.3.1 we are done, or $i \neq j$ and U is cyclic, hence the result follows from the above two Claims.

- If $U' = U'_1 \oplus U'_2$ is decomposable, then by the induction both U/U'_1 and U/U'_2 satisfies the Lemma and has the decomposition. Note that U is a submodule of $U/U'_1 \oplus U/U'_2$, so we are done.

Proof of the Claim 2.3.11. Let U be a cyclic object in $\mathcal{C}_{\text{crys}}^{[0,3]}$ that has no quotient isomorphic to $\mathbb{F}_7$. We prove by induction on the order of U. If U is of order 7, then it is of dimension one over $\mathbb{F}_7$, which is done by the Lemma 2.3.3. Assume in general. Let $U' \cong \mathbb{F}_7(j)$ be a simple subobject of U. Then since the quotient U/U' is cyclic without quotient isomorphic to $\mathbb{F}_7$, by induction $U/U' \cong \mathbb{Z}/7^m(i)$ for some $i \neq 0$. So we get the following short exact sequence in $\mathcal{C}_{\text{crys}}^{[0,3]}$:

$$0 \longrightarrow \mathbb{F}_7(j) \longrightarrow U \longrightarrow \mathbb{Z}/7^m(i) \longrightarrow 0,$$

with U being cyclic. So by the Corollary 2.3.9 and the exact sequence of $\mathbb{Z}/7^m(i)$ formed by 7-power subgroups, the above sequence is nonsplit only when $i = j$ (note that $i \neq 0$). In this way, by twisting with $(-i)$, we reduce to a cyclic extension of $\mathbb{Z}/7^m$ by $\mathbb{F}_7$ in the category of abelian groups, which is done. □

Proof of the Claim 2.3.12. We induct on the number of generators in U. If U is cyclic, then this is the Claim 2.3.11. Assume U has n minimal generators $e_1, \dots, e_n$. Let U' be the subrepresentation generated by $e_1, \dots, e_{n-1}$, and let U'' be the one generated by e_n. By induction, we have $U' = N(i)$ and $U'' = \mathbb{Z}/7^m(j)$, for N being an torsion $\mathbb{Z}_7$-module. Besides, since e_l are minimal, the intersection $U' \cap U''$ are nontrivial subrepresentation of both U' and U''. In this way, since the Jordan-Hölder factors of $U' \cap U''$ contributes to that of both U' and U'', we see $i = j$. Hence we are done by Lemma 2.3.1. □

□

2.4 Proof of the Proposition 2.1.1

At last, we finish the proof of the Proposition 2.1.1. We will show the following torsion variant first, with the use of the tools we developed in the last subsection.

Proposition 2.4.1. *Let* $U = \underline{\mathrm{FL}}(M)$ *be an object in* $\mathcal{C}_{\mathrm{crys}}^{[0,3]}$. *Then there exists an* G*-equivariant filtration of subrepresentations*

$$0 \subset U_3 \subset U_2 \subset U_1 \subset U_0 = U,$$

such that $U_i/U_{i+1} \cong N_i(i)$ *is the* i*-th Tate twist of a finite* $\mathbb{Z}_7$ *module* N_i.

Proof. We prove this by the induction of orders. When $\#U$ is 7, it is an $\mathbb{F}_7$-linear space of dimension one, and is done by the Lemma 2.3.3. In general, if U has no quotient isomorphic to $\mathbb{F}_7$, then this is done by the Lemma 2.3.10.

Otherwise, we can get the following short exact sequence in $\mathcal{C}_{\mathrm{crys}}^{[0,3]}$:

$$0 \longrightarrow U' \longrightarrow U \longrightarrow \mathbb{F}_7 \longrightarrow 0. \qquad (*)$$

By the induction, U' admits the required filtration U'_i. So we take the quotient of $(*)$ by U'_1, and get

$$0 \longrightarrow U'/U'_1 \longrightarrow U/U'_1 \longrightarrow \mathbb{F}_7 \longrightarrow 0.$$

By assumption, G acts trivially on both U'/U'_1 and $\mathbb{F}_7$. Thus the Lemma 2.3.1 implies that U/U'_1 has trivial action. Hence the filtration

$$0 \subset U'_3 \subset U'_2 \subset U'_1 \subset U_0 = U$$

does the job.

□

Proof of the Proposition 2.1.1. We take an G-lattice L inside of V and consider the sequ ence given by $L/7^n L \in \mathcal{C}_{\mathrm{crys}}^{[0,3]}$. Then the result follows from the above Proposition. □

References

[BM] C. Breuil; W. Messing. Torsion étale and crystalline cohomologies. (English summary) Cohomologies p-adiques et applications arithmétiques, II. Astérisque No. 279 (2002), 81124.

[Fo1] J. M. Fontaine. Il n'y a pas de variété abélienne sur $\mathbb{Z}$. (French) [There are no abelian varieties over $\mathbb{Z}$.] Invent. Math. 81 (1985), no. 3, 515538.

[Fo2] J. M. Fontaine. Schémas propres et lisses sur $\mathbb{Z}$. (French) [Proper and smooth schemes over $\mathbb{Z}$] Proceedings of the Indo-French Conference on Geometry (Bombay, 1989), 4356, Hindustan Book Agency, Delhi, 1993.

[FL] J. M. Fontaine; G. Laffaille. Construction de représentations p-adiques. (French) [Construction of p-adic representations] Ann. Sci. École Norm. Sup. (4) 15 (1982), no. 4, 547608 (1983).

[Se] J-P. Serre. Local fields. Translated from the French by Marvin Jay Greenberg. Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979. viii+241 pp.

[Sta] The Stacks Project Authors. Stacks Project, `http://stacks.math.columbia.edu.`