ISOCRYSTALS ASSOCIATED TO ARITHMETIC JET SPACES
OF ABELIAN SCHEMES

JAMES BORGER AND ARNAB SAHA

Abstract. The main aim of this article is to construct a canonical $F$-isocrystal $H(A)_K$ for an abelian scheme $A$ over a $p$-adic complete discrete valuation ring of perfect residue field. This $F$-isocrystal $H(A)_K$ comes with a filtration and admits a natural map to the usual Hodge sequence of $A$. Even though $H(A)_K$ admits a map to the crystalline cohomology of $A$, the $F$-structure on $H(A)_K$ is fundamentally distinct from the one on the crystalline cohomology. When $A$ is an elliptic curve, we further show that $H(A)_K$ itself is an $F$-crystal and that implies a strengthened version of Buium’s result on differential characters in [5].

1. Introduction

The theory of arithmetic jet spaces developed by Buium draws inspiration from the theory of differential algebra over a function field. In differential algebra, given a scheme $E$ defined over a function field $K$ with a derivation $\partial$ on it, one can define the jet spaces $J^nE$ for all $n \in \mathbb{N}$ with respect to $(K, \partial)$ and they form an inverse system of schemes satisfying a universal property with respect to derivations lifting $\partial$. The ring of global functions $\mathcal{O}(J^nE)$ can be thought of as the ring of $n$-th order differential functions on $E$. In the case when $E$ is an elliptic curve and its structure sheaf $\mathcal{O}_E$ does not have a derivation lifting $\partial$ (if it does, then it is the isotrivial case and $E$ will descend to the subfield $K^{\partial=0}$ of constants), there exists a differential function $\Theta \in \mathcal{O}(J^2E)$ which is a homomorphism of group schemes from $J^2E$ to the additive group $\mathbb{G}_a$. Such a $\Theta$ is an example of a differential character of order 2 for $E$ and is known as a Manin character. Explicitly, if $E$ is given by the Legendre equation $y^2 = x(x-1)(x-t)$ over $K = \mathbb{C}(t)$ with derivation $\partial = \frac{d}{dt}$, then

$$
\Theta(x, y, x', y', x'', y'') = \frac{y}{2(x-t)^2} - \frac{d}{dt} \left[ 2(t-1) \frac{x'}{y} \right] + 2(t-1)x'y'dy'.
$$

where $x, y, x', y', x'', y''$ are the induced coordinates of the jet space $J^2E$. The existence of such a $\Theta$ is a consequence of the Picard–Fuchs equation. Using the derivation $\partial$ on $K$, we can lift any $K$-rational point $P \in E(K)$ canonically to $J^2E(K)$, and this defines a homomorphism $\nabla : E(K) \to J^2E(K)$. We emphasize that $\nabla$ is merely a map on $K$-rational points and does not come from a map of schemes. The composition $\Theta \circ \nabla : E(K) \to \mathbb{G}_a(K)$ is then a group homomorphism of $K$-points. Note that the torsion points of $E(K)$ are contained in the kernel of $\Theta$ since $\mathbb{G}_a(K)$ is torsion free. Such a $\Theta$ was used by Manin to give a proof of the Lang–Mordell conjecture for abelian varieties over function fields [12]. Later Buium gave a different proof, using other methods, but still using the Manin map [4].
Theorem 1.1. For any abelian scheme $A$ of dimension $g$, $X_{\infty}(A)_K$ is freely $K[\phi^*]$-generated by $g$ differential characters of order at most $g + 1$. 

Before we describe our main results in detail, we wish to fix a few notations. Fix a prime $p$. Let $R$ be a $p$-adic complete discrete valuation ring with maximal ideal $\mathfrak{m}$. Let $\pi$ be a generator of $\mathfrak{m}$. Let $v$ be the valuation on $R$ and $k$ is the residue field with cardinality $|k| = q$ where $q$ is a power of $p$. We assume $v$ is normalized and let $e = v(p)$ be the absolute ramification index. Let $\phi : R \rightarrow R$ be a fixed lift of Frobenius which satisfies $\phi(x) \equiv x^q \mod \mathfrak{m}$, for all $x \in R$. We also further assume that $\phi$ is an automorphism on $R$. Let $K = R[\frac{1}{\pi}]$ and set $S = \text{Spf } R$. Then one can consider the operator on $R$ given by $\delta x = \frac{\phi(x) - x^q}{\pi}$. It is called the $\pi$-derivation associated to $\phi$. For any $R$-module $M$, we define $M_K := M \otimes_R K$. 

The most important result in this paper is the construction of a canonical filtered $F$-isocrystal $H(A)_K$ which comes with a Hodge-type filtration and a morphism $H(A)_K \rightarrow H_{dR}(A)_K$ to the usual de Rham cohomology preserving the filtration. When $A$ is an elliptic curve, we in fact construct a filtered $F$-crystal $H(A)$. As a consequence, the methods that go into the construction of $H(A)$, also establish a stronger integral version of Buium’s result that $X_{\infty}(A)$ itself is freely generated by a single element as an $R[\phi^*]$-module when $A$ is an elliptic curve. The analogous construction for Drinfeld modules in equal positive characteristic was done by the authors in [3].
We prove the above result in section 7. In the differential algebra case, Buium had shown that $X_\infty(A)$ is generated by differential characters of order at most $2g$. We would like to remark that our techniques can be generalised to work in the case of differential algebra as well.

We define the lower splitting number $m_1$ to be such that $X_{m_1}(A) \neq \{0\}$ but $X_i(A) = \{0\}$ for all $0 \leq i \leq m_1 - 1$. Then it will easily follow that $m_1$ satisfies $1 \leq m_1 \leq 2$. In the case when $A$ is an elliptic curve, then $X_{m_1}(A)$ is a free $R$-module with a canonical basis element $\Theta \in X_{m_1}(A)$, depending only on our chosen etale coordinate on $A$. Also we have $m_1 = 2$ unless $A$ admits a lift of Frobenius compatible with group structure on $A$, in which case $m_1 = 1$. Then our first main theorem is a strengthened version of Buium’s result in [5].

**Theorem 1.2.** Let $A$ be an elliptic curve with lower splitting number $m_1$. Then the $R$-module $X_{m_1}(A)$ is free of rank 1, and it freely generates $X_\infty(A)$ as an $R\{\phi^*\}$-module in the sense that the canonical map $R\{\phi^*\} \otimes_R X_{m_1}(A) \to X_\infty(A)$ is an isomorphism.

Let us now proceed to our second result. Let $u : J^n A \to A$ be the usual projection map and put $N^n = \ker u$. Then $N^n$ is a formal scheme of relative dimension $n$ over Spf $R$. For each $n \geq 1$, we show in proposition 4.3 that there is a lift of Frobenius $\check{f} : N^{n+1} \to N^n$ making the system $\{N^n\}$ into a prolongation sequence with respect the obvious projection map $u : N^{n+1} \to N^n$. We call $\check{f}$ the lateral Frobenius. However, $\check{f}$ is not compatible with $i$ and $\phi : J^{n+1} A \to J^n A$ in the obvious way, that is, it is not true that $\phi \circ i = i \circ \check{f}$ holds. In fact, we can not expect it to be true because that would induce lift of Frobenius on $A$ which is not the case to start with. Instead we have $\phi^2 \circ i = \phi \circ i \circ \check{f}$.

In section 6, we construct a canonical $F$-isocrystal attached to $A$. The $F$-isocrystal, denoted $H(A)_K$, is a $K$-module which has a semi-linear operator $\check{f}^*$ (induced from $\check{f}$) on it and is of rank less than equal to $2g$. The module $H(A)_K$ also has a Hodge-type filtration and canonically maps to the de Rham cohomology of $A$, with its Hodge filtration.

**Theorem 1.3.** There exists a map of short exact sequences of $K$-modules

$$
\begin{array}{cccccc}
0 & \longrightarrow & X_{\text{prim}}(A)_K & \longrightarrow & H(A)_K & \longrightarrow & I(A)_K & \longrightarrow & 0 \\
\gamma & & \downarrow \phi & & & & \downarrow & \\
0 & \longrightarrow & (\text{Lie } A)_K^+ & \longrightarrow & H_{dR}(A)_K & \longrightarrow & H^1(A, \mathcal{O}_A)_K & \longrightarrow & 0
\end{array}
$$

where $\dim_K H(A)_K \leq 2g$.

Moreover, the operator $\check{f}^*$ on $H(A)$ descends to its image under $\Phi$.

We will define $X_{\text{prim}}(A)$ in section 7 and a more detailed result is proved in section 6, as theorem 8.2.

In fact, in the case when $A$ is an elliptic curve, we show in section 9.1 that $H(A)$ is an integral $F$-crystal over $R$ of $\text{rk}_R H(A) \leq 2$. Our method of showing the existence of this integral $F$-crystal implies theorem 1.2. Moreover, given an etale coordinate...
on $A$, there exists a canonical basis of $H(A)$ and the characteristic polynomial of $f^*$ with respect to this basis is

$$\text{char}(f) = \begin{cases} t - \gamma, & \text{if } A \text{ has a canonical lift} \\ t^2 - \phi(\lambda)t - \gamma, & \text{otherwise} \end{cases}$$

where $\lambda, \gamma \in R$ and $\pi \mid \gamma$. The coefficients $\lambda$ and $\gamma$ are modular parameters that depend on $A$ and should be viewed as differential modular forms on the moduli of elliptic curves, evaluated at $A$. These modular forms will be studied in a subsequent paper.

Note that over the points of the moduli of elliptic curves over $R$ on which $\gamma \not\equiv 0 \mod \pi$, $H(A)$ is a weakly admissible $F$-crystal. The Fontaine functor associates a $\pi$-adic Galois representation to a weakly admissible $F$-isocrystal [9, 13]. Hence the $F$-crystal $H(A)$ gives rise to new $\pi$-adic Galois representation.

To an abelian scheme $A$, the crystalline theory also attaches an $F$-isocrystal $H_{\text{crys}}(A)_K$. However, our $F$-isocrystal $H(A)_K$ is different than the crystalline one. That is because the semi-linear map on $H(A)_K$ depends on higher $\pi$-derivatives of the structure constants of the equation defining the abelian scheme whereas $H_{\text{crys}}(A)_K$ does not involve any such higher $\pi$-derivatives. A natural question is whether the two $F$-crystals determine each other in by an explicit linear-algebraic functor, as in $p$-adic Hodge theory. In the Drinfeld module setting of [3], the shtuka necessarily determines both, simply because it determines the Drinfeld module. But it would be interesting to go further and describe the functor in purely linear-algebraic terms, without going through Drinfeld modules. Similarly, it is natural to expect that one could do the same in the context of this paper using the $p$-adic shtukas of Scholze and collaborators [14].

2. Notation

Here, for the convenience of reference, we collect all the notations introduced so far. Fix a prime $p$. Let $R$ be a $p$-adic complete discrete valuation ring with maximal ideal $\mathfrak{m}$. Let $\pi$ be a generator of $\mathfrak{m}$. Let $v$ be the valuation on $R$ and $k$ is the residue field with cardinality $|k| = q$. We assume $v$ is normalised and let $e = v(p)$ be the absolute ramification index. Let $\phi : R \to R$ be a fixed lift of Frobenius which satisfies $\phi(x) \equiv x^q \mod \mathfrak{m}$, for all $x \in R$. We also further assume that $\phi$ is an automorphism on $R$. If $x_1, \cdots, x_n \in M$ forms an $R$-basis, then we will denote $M = R\langle x_1, \cdots, x_n \rangle$. For any $R$-module $M$, denote $M_K = M \otimes_R K$. Let $K = R[\frac{1}{p}]$ and call $S = \text{Spf } R$. We will consider the category of $\pi$-formal schemes over $S$. Let $A$ be an abelian scheme of dimension $g$ over $S$.

3. Witt Vectors

Witt vectors over Dedekind domains with finite residue fields were introduced in [1]. We will give a brief overview in this section.

3.1. Frobenius lifts and $\pi$-derivations. Let $B$ be an $R$-algebra, and let $C$ be a $B$-algebra with structure map $u : B \to C$. In this paper, a ring homomorphism $\psi : B \to C$ will be called a lift of Frobenius (relative to $u$) if it satisfies the following:

1. The reduction mod $\pi$ of $\psi$ is the $q$-power Frobenius relative to $u$, that is, $\psi(x) \equiv u(x)^q \mod \pi C$. 


(2) The restriction of \( \psi \) to \( R \) coincides with the fixed \( \phi \) on \( R \), that is, the following diagram commutes

\[
\begin{array}{ccc}
B & \xrightarrow{\psi} & C \\
\uparrow & & \uparrow \\
R & \xrightarrow{\phi} & R
\end{array}
\]

A \( \pi \)-derivation \( \delta \) from \( B \) to \( C \) means a set-theoretic map \( \delta : B \to C \) satisfying the following for all \( x, y \in B \)

\[
\begin{align*}
\delta(x + y) &= \delta(x) + \delta(y) \\
\delta(xy) &= u(x)^q\delta(y) + \delta(x)u(y)^q + \pi \delta(x)\delta(y)
\end{align*}
\]

such that for all \( r \in R \), we have

\[
\delta(r) = \frac{\phi(r) - r^q}{\pi}.
\]

When \( C = B \) and \( u \) is the identity map, we will call this simply a \( \pi \)-derivation on \( B \).

It follows that the map \( \phi : B \to C \) defined as

\[
\phi(x) := u(x)^q + \pi \delta(x)
\]

is a lift of Frobenius in the sense above. On the other hand, for any flat \( R \)-algebra \( B \) with a lift of Frobenius \( \phi \), one can define the \( \pi \)-derivation \( \delta(x) = \frac{\delta(x) - x^q}{\pi} \) for all \( x \in B \).

Note that this definition depends on the choice of uniformizer \( \pi \), but in a transparent way: if \( \pi' \) is another uniformizer, then \( \delta(x)\pi/\pi' \) is a \( \pi' \)-derivation. This correspondence induces a bijection between \( \pi \)-derivations \( B \to C \) and \( \pi' \)-derivations \( B \to C \).

3.2. Witt vectors. We will present three different points of view on \( \pi \)-typical Witt vectors. Let \( B \) be an \( R \)-algebra with structure map \( u : R \to B \).

(1) The ring \( W(B) \) of \( \pi \)-typical Witt vectors can be defined as the unique (up to unique isomorphism) \( R \)-algebra \( W(B) \) with a \( \pi \)-derivation \( \delta \) on \( W(B) \) and an \( R \)-algebra homomorphism \( W(B) \to B \) such that, given any \( R \)-algebra \( C \) with a \( \pi \)-derivation \( \delta \) on it and an \( R \)-algebra map \( f : C \to B \), there exists a unique \( R \)-algebra homomorphism \( g : C \to W(B) \) such that the diagram

\[
\begin{array}{ccc}
W(B) & \xrightarrow{g} & C \\
\downarrow & & \downarrow f \\
B & \xleftarrow{\delta} & C
\end{array}
\]

commutes and \( g \circ \delta = \delta \circ g \). Thus \( W \) is the right adjoint of the forgetful functor from \( R \)-algebras with \( \pi \)-derivation to \( R \)-algebras. For details, see section 1 of [1] and [11].

(2) If we restrict to flat \( R \)-algebras \( B \), then we can ignore the concept of \( \pi \)-derivation and define \( W(B) \) simply by expressing the universal property above in terms of Frobenius lifts, as follows. Given a flat \( R \)-algebra \( B \), the ring \( W(B) \) is the unique (up to unique isomorphism) flat \( R \)-algebra \( W(B) \) with a lift of Frobenius (in
the sense above) \( F : W(B) \to W(B) \) and an \( R \)-algebra homomorphism \( W(B) \to B \) such that for any flat \( R \)-algebra \( C \) with a lift of Frobenius \( \phi \) on it and an \( R \)-algebra map \( f : C \to B \), there exists a unique \( R \)-algebra homomorphism \( g : C \to W(B) \) such that the diagram

\[
\begin{array}{ccc}
W(B) & \xrightarrow{g} & B \\
\downarrow & & \downarrow f \\
B & \xrightarrow{\phi} & C
\end{array}
\]

commutes and \( g \circ \phi = F \circ g \).

(3) Finally, one can also define Witt vectors in terms of the Witt polynomials. For each \( n \geq 0 \) let us define \( B^{\phi^n} \) to be the \( R \)-algebra with structure map \( R \xrightarrow{\phi} R \xrightarrow{\phi} B \) and define the ghost rings to be the product \( R \)-algebras \( \Pi^\infty \phi B = B \times B^\phi \times \cdots \) and \( \Pi^\infty \phi B = B \times B^\phi \times \cdots \). Then for all \( n \geq 1 \) there exists a restriction, or truncation, map \( T_w : \Pi^\infty \phi B \to \Pi^{n-1} \phi B \) given by \( T_w(w_0, \ldots, w_n) = (w_0, \ldots, w_{n-1}) \). We also have the left shift Frobenius operators \( F_w : \Pi^\infty \phi B \to \Pi^{n-1} \phi B \) given by \( F_w(w_0, \ldots, w_n) = (w_1, \ldots, w_n) \). Note that \( T_w \) is an \( R \)-algebra morphism, but \( F_w \) lies over the Frobenius endomorphism \( \phi \) of \( R \).

Now as sets define

\[
W_n(B) = B^{n+1},
\]

and define the set map \( w : W_n(B) \to \Pi^\infty \phi B \) by \( w(x_0, \ldots, x_n) = (w_0, \ldots, w_n) \) where

\[
w_i = x_0^{q^i} + \pi x_1^{q^i-1} + \cdots + \pi^i x_i
\]

are the Witt polynomials. The map \( w \) is known as the ghost map. (Do note that under the traditional indexing our \( W_n \) would be denoted \( W_{n+1} \).) We can then define the ring \( W_n(B) \), the ring of truncated \( \pi \)-typical Witt vectors, by the following theorem as in [10]:

**Theorem 3.1.** For each \( n \geq 0 \), there exists a unique functorial \( R \)-algebra structure on \( W_n(B) \) such that \( w \) becomes a natural transformation of functors of \( R \)-algebras.

### 3.3. Operations on Witt vectors.

Now we recall some important operators on the Witt vectors. There are the restriction, or truncation, maps \( T : W_n(B) \to W_{n-1}(B) \) given by \( T(x_0, \ldots, x_n) = (x_0, \ldots, x_{n-1}) \). Note that \( W(B) = \lim_n W_n(B) \). There is also the Frobenius ring homomorphism \( F : W_n(B) \to W_{n-1}(B) \), which can be described in terms of the ghost map. It is the unique map which is functorial in \( B \) and makes the following diagram commutative

\[
\begin{array}{ccc}
W_n(B) & \xrightarrow{w} & \Pi^\infty \phi B \\
\downarrow F & & \downarrow F_w \\
W_{n-1}(B) & \xrightarrow{w} & \Pi^{n-1} \phi B
\end{array}
\]

As with the ghost components, \( T \) is an \( R \)-algebra map but \( F \) lies over the Frobenius endomorphism \( \phi \) of \( R \).

Next we have the Verschiebung \( V : W_{n-1}(B) \to W_n(B) \) given by \( V(x_0, \ldots, x_{n-1}) = (0, x_0, \ldots, x_{n-1}) \).
Let \( V_u : \Pi^\alpha B \to \Pi^\beta B \) be the additive map given by
\[
V_u(w_0, w_n) = (0, \pi w_0, \ldots, \pi w_n).
\]
Then the Verschiebung \( V \) makes the following diagram commute:
\[
\begin{array}{ccc}
W^1 B & \overset{w}{\longrightarrow} & \Pi^\alpha B \\
\downarrow V & & \downarrow V_w \\
W^1 B & \overset{w}{\longrightarrow} & \Pi^\beta B
\end{array}
\]
For all \( n \geq 0 \) the Frobenius and the Verschiebung satisfy the identity
\[
FV(x) = \pi x.
\]
The Verschiebung is not a ring homomorphism, but it is \( k \)-linear.

Finally, we have the multiplicative Teichmüller map \([ ] : B \to W_n(B)\) given by \( x \mapsto [x] = (x, 0, 0, \ldots)\).

### 3.4. Prolongation sequences and jet spaces.

Let \( X \) and \( Y \) be schemes over \( S = \text{Spf } R \). We say a pair \( (u, \delta) \) is a prolongation, and write \( Y \overset{(u, \delta)}\rightarrow X \), if \( u : Y \to X \) is a map of schemes over \( S \) and \( \delta : \mathcal{O}_X \to u_\ast \mathcal{O}_Y \) is a \( \pi \)-derivation making the following diagram commute:

\[
\begin{array}{ccc}
R & \overset{u_\ast \mathcal{O}_Y}{\longrightarrow} & \mathcal{O}_X \\
\downarrow \delta & & \downarrow \delta \\
R & \overset{\mathcal{O}_X}{\longrightarrow} & \mathcal{O}_X
\end{array}
\]

Following [6], a prolongation sequence is a sequence of prolongations
\[
\text{Spf } R \overset{(u, \delta)}\longrightarrow T^0 \overset{(u, \delta)}\longrightarrow T^1 \overset{(u, \delta)}\longrightarrow \cdots,
\]
where each \( T^n \) is a scheme over \( S \). We will often use the notation \( T^n \) or \( \{ T_n \}_{n \geq 0} \). Note that if the \( T^n \) are flat over \( \text{Spf } R \) then having a \( \pi \)-derivation \( \delta \) is equivalent to having lifts of Frobenius \( \phi : T^{n+1} \to T^n \).

Prolongation sequences form a category \( \mathcal{C}_S \), where a morphism \( f : T^* \to U^* \) is a family of morphisms \( f^n : T^n \to U^n \) commuting with both the \( u \) and \( \delta \), in the evident sense. This category has a final object \( S^0 = \text{Spf } R \) for all \( n \), where each \( u \) is the identity and each \( \delta \) is the given \( \pi \)-derivation on \( R \).

For any scheme \( Y \) over \( S \), for all \( n \geq 0 \) we define the \( n \)-th jet space \( J^n X \) (relative to \( S \)) as
\[
J^n X(Y) := \mathrm{Hom}_S(W^*_n(Y), X)
\]
where \( W^*_n(Y) \) is defined as in [2]. We will not define \( W^*_n(Y) \) in full generality here. Instead, for simplicity of the exposition, we will define \( \mathrm{Hom}_S(W^*_n(Y), X) \) in the affine case. Write \( X = \text{Spf } A \) and \( Y = \text{Spf } B \). Then \( W^*_n(Y) = \text{Spf } W^*_n(B) \) and \( \mathrm{Hom}_S(W^*_n(Y), X) = \mathrm{Hom}_R(A, W^*_n(B)) \), the set of \( R \)-algebra homomorphisms \( A \to W_n(B) \).

Then \( J^* X := \{ J^n X \}_{n \geq 0} \) forms a prolongation sequence and is called the canonical prolongation sequence [6]. By [1, 6], \( J^* X \) satisfies the following universal property—for any \( T^* \in \mathcal{C}_S \) and \( X \) a scheme over \( S^0 \), we have
\[
\mathrm{Hom}(T^0, X) = \mathrm{Hom}_{\mathcal{C}_S}(T^*, J^* X)
\]
Let $X$ be a scheme over $S = \text{Spf} R$. Define $X^{\varphi^n}$ by $X^{\varphi^n}(B) := X(B^{\varphi^n})$ for any $R$-algebra $B$. In other words, $X^{\varphi^n}$ is $X \times_{S, \varphi^n} S$, the pull-back of $X$ under the map $\varphi^n : S \to S$. Next define

$$
\Pi^n X = X \times_S X^{\varphi} \times_S \cdots \times_S X^{\varphi^n}.
$$

Then for any $R$-algebra $B$ we have $X(\Pi^n B) = X(B) \times_S \cdots \times_S X^{\varphi^n}(B)$. Thus the ghost map $w$ in theorem 3.1 defines a map of $S$-schemes

$$
w : J^n X \to \Pi^n X.
$$

Note that $w$ is injective when evaluated on points with coordinates in any flat $R$-algebra.

The operators $F$ and $F_w$ in (3.3) induce maps $\varphi$ and $\varphi_w$ as follows

$$
\begin{array}{ccc}
J^n X & \xrightarrow{w} & \Pi^n X \\
\downarrow \varphi & & \downarrow \varphi_w \\
J^{n-1} X & \xrightarrow{w} & \Pi^{n-1} X
\end{array}
$$

where $\varphi_w$ is the left-shift operator given by

$$
\varphi_w(w_0, \ldots, w_n) = (\varphi_S(w_1), \ldots, \varphi_S(w_n)),
$$

and where $\varphi_S : X^{\varphi^i} \to X^{\varphi^{i-1}}$ is the composition given in the following diagram:

$$
\begin{array}{ccc}
X^{\varphi^i} & \xrightarrow{\sim} & X^{\varphi^{i-1}} \times_S S \\
\downarrow \varphi & & \downarrow \varphi \\
S & \xrightarrow{\varphi} & S
\end{array}
$$

Let $A$ be a group scheme over $S$. Then the ghost map $w : J^n A \to \Pi^n A$ and the truncation map $u : J^n A \to J^{n-1} A$ are group scheme homomorphisms over $S$. The Frobenius map $\phi : J^n A \to J^{n-1} A$ is a group scheme homomorphism lying over the Frobenius endomorphism $\varphi$ of $S$. In other words, the induced map $J^n A \to (J^{n-1} A)^{\varphi}$ is a homomorphism group schemes over $S$.

3.5. Character groups. Given a prolongation sequence $T^*$ we can define its shift $T^{*+n}$ by $(T^{*+n})^j := T^{n+j}$ for all $j$ [6].

$$
\text{Spf } R \xleftarrow{(u, \delta)} T^n \xrightarrow{(u, \delta)} T^{n+1} \cdots
$$

We define a $\delta$-morphism of order $n$ from $X$ to $Y$ to be a morphism $J^{*+n} X \to J^* Y$ of prolongation sequences. We define a character of order $n$, $\Theta : A \to \hat{G}_a$ to be a $\delta$-morphism of order $n$ from $A$ to $\hat{G}_a$ which is also a group homomorphism of group schemes. By the universal property of jet schemes [6], an order $n$ character is equivalent to a homomorphism $\Theta : J^n A \to \hat{G}_a$ of group schemes over $S$. We denote the group of characters of order $n$ by $X_n(A)$. So we have

$$
X_n(A) = \text{Hom}(J^n A, \hat{G}_a),
$$
which one could take as an alternative definition. Note that $X_n(A)$ comes with an $R$-module structure since $\hat{G}_a$ is an $R$-module scheme over $S$. Also the inverse system $J^{n+1}A \to J^nA$ defines a directed system

$$X_n(A) \leftarrow X_{n+1}(A) \leftarrow \cdots$$

via pull back. Each morphism $u^*$ is injective and we then define $X_\infty(A)$ to be the direct limit $\lim_{n} X_n(A)$.

Similarly, pre-composing with the Frobenius map $\phi: J^{n+1}A \to J^nA$ induces a Frobenius operator $\phi: X^n(A) \to X^{n+1}(A)$. However since $\phi: J^{n+1}A \to J^nA$ is not a morphism over Spf $R$ but instead lies over the Frobenius endomorphism $\phi$ of Spf $R$, some care is required. Consider the relative Frobenius morphism $\phi_R$, defined to be the unique morphism making the following diagram commute:

Then $\phi_R$ is a morphism of formal group schemes over Spf $R$. Now given a $\delta$-character $\Theta: J^nE \to \hat{G}_a$, define $\phi^*\Theta$ to be the composition

$$(3.8) \quad J^{n+1}A \xrightarrow{\phi_R} J^nA \times_{(\text{Spf } R), \phi} \text{Spf } R \xrightarrow{\Theta \times_1 \hat{G}_a \times_{(\text{Spf } R), \phi} \text{Spf } R \xrightarrow{\iota} \hat{G}_a}$$

where $\iota$ is the isomorphism of group schemes over $S$ coming from the fact that $\hat{G}_a$ descends to $\mathbb{Z}_p$ as group scheme. For any $R$-algebra $B$, the induced morphism on $B$-points is

$$A(W_{n+1}(B)) \xrightarrow{A(F)} A(W_n(B)) \xrightarrow{\Theta \times_1 \hat{G}_a \times_{(\text{Spf } R), \phi} \text{Spf } R \xrightarrow{\iota} \hat{G}_a} B^\phi \xrightarrow{b \mapsto b} B.$$ 

Note that this composition $A(W_{n+1}(B)) \to B$ is indeed a morphism of group schemes.

Thus we have an additive map $X_n(A) \to X_{n+1}(A)$ given by $\Theta \mapsto \phi^*\Theta$. Note that this map is not $R$-linear. However, the map

$$\phi^*: X_n(A) \to X_{n+1}(A)^\phi, \quad \Theta \mapsto \phi^*\Theta$$

is $R$-linear, where $X_{n+1}(A)^\phi$ denotes the abelian group $X_{n+1}(A)$ with $R$-module structure defined by the law $r \cdot \Theta := \phi(r)\Theta$. Taking direct limits in $n$, we obtain an $R$-linear map

$$X_\infty(A) \to X_\infty(A)^\phi, \quad \Theta \mapsto \phi^*\Theta.$$ 

In this way, $X_\infty(A)$ is a left module over the twisted polynomial ring $R\{\phi^*\}$ with commutation law $\phi^*r = \phi(r)\phi^*$.

4. LATERAL FROBENIUS

Let $B$ be an $R$-algebra and $f: R \to B$ be the structure map. Since $R$ is a discrete valuation ring, it is easy to see that $\phi$ induces a unique lift of Frobenius on
the image \( f(R) \subseteq B \). Define
\[
(4.1) \quad W_n^+(B) := \{ (x_0, \ldots, x_n) \mid x_0 \in f(R) \}
\]
Also define \( \Pi^+_n(B) \) to be the subring of \( \Pi_n(B) \) such that the first coordinate is an element of the image \( f(R) \). Define the ring homomorphisms \( R^+_1, F^+_1 : \Pi^+_n(B) \to \Pi^+_n(B) \) given by
\[
R^+_n(z_0, \ldots, z_n) = (z_0, \ldots, z_{n-1}) \quad (4.2)
\]
\[
F^+_n(z_0, \ldots, z_n) = (\phi(z_0), z_2, \ldots, z_n)
\]

**Proposition 4.1.** For all \( n \geq 1 \), there exists ring homomorphisms \( F^+_1 : W_n(B) \to W_{n-1}(B) \) satisfying
\[
\begin{align*}
W_n(B) & \xrightarrow{w} \Pi_n^+(B) \\
W^+_{n-1}(B) & \xrightarrow{w} \Pi^+_{n-1}(B)
\end{align*}
\]
Moreover, if \( F^+_1(x_0, \ldots, x_n) = (F^+_1, \ldots, F^+_1) \), then for all \( 0 \leq i \leq n - 1 \),
\[
F^+_i \equiv x_i^q \pmod{\pi}
\]

**Proof.** We will show using the ghost map \( w \). And also, it is sufficient to assume that \( B \) is \( \pi \)-torsion free. Clearly we have \( F^+_0 = \phi(x_0) \). We will prove by induction. Assume \( F^+_{h-1} = x^q_{h-1} + \pi y \) for some \( y \in B \). Then comparing the ghost coordinates, we get
\[
(F^+_0)^q + \pi(F^+_1)^{q-1} + \cdots + \pi^h F^+_h = x^q_{0} + \pi x^q_{1} + \cdots + \pi^h x_{h+1}
\]
Grouping terms we obtain
\[
F^+_h = \sum_{i=0}^{h-1} \pi^{h-i} \left( x^q_{i} - (F^+_i)^{q-1} \right) + x^q_{h} + \pi x_{h+1}
\]
and we would do this if we can show the integrality of the expression on the right hand side. Let \( L_i = \pi^{i-h} \left( x^q_{i} - (F^+_i)^{q-1} \right) \). By induction hypothesis, \( F^+_i = x^q_{i} + \pi y_i \) for some \( y_i \in R \) for all \( i \). Then
\[
L_i = \pi^{i-h} \sum_{j=1}^{q-1-h} \binom{q-1-i}{j} \pi^j (x^q_{i})^{q-1-j} y_i^j
\]
Then note that the valuation
\[
v(L_i) \geq i - h + q^{q-1-i} + (j - v(j)) \geq (h - i) v(q) + 1 - (h - i) \geq 1
\]
and we are done. \( \square \)

There is another, more structural way of understanding \( W_n^+(B) \) and \( F^+ \). Consider the usual exact sequence
\[
\begin{array}{cccc}
0 & \rightarrow & W_{n-1}(B) & \xrightarrow{V} & W_n(B) & \rightarrow & B & \rightarrow & 0.
\end{array}
\]
Then $W_n^i(B)$ is the pull-back $R \times_B W_n(B)$ of this extension through the structure map $f : R \to B$. (For simplicity, we assume $f$ is injective.) Let us now consider $F^\dagger$. Observe that the projection $W_n^\dagger(B) \to R$ has a canonical section. Indeed, the Frobenius lift $\phi$ induces a lift $\tilde{f} : R \to W_n(B)$ of $f$ and hence a section of the map $W_n^\dagger(B) \to R$. Therefore, we may identify $R \oplus W_{n-1}(B)$ with $W_n^\dagger(B)$ via the map $(r, z) \mapsto \tilde{f}(r) + V(z)$. In terms of this identification, the map $F^\dagger : W_n^\dagger(B) \to W_{n-1}(B)$ is given by

$$(r, z) \mapsto (\phi(r), F(z)).$$

**Proposition 4.2.** Let $I : W_n^\dagger(B) \to W_n(B)$ be the natural inclusion. Then

$$F^2 \circ I = F \circ I \circ F^\dagger.$$

**Proof.** It is sufficient to assume $B$ is $\pi$-torsion free. Then the ghost map $w$ is injective and hence it is sufficient to check the identity on the ghost vectors where it is clearly true. □

For any $S$-scheme $X$, with an $S$-point $P : S \to X$, for each $n$ we can define $N^n = J^n X \times_X S$ which is the following fiber product

$$\begin{array}{ccc}
J^n X & \leftarrow & N^n \\
\downarrow & & \downarrow \\
X & \leftarrow & P
\end{array}$$

If $X$ is affine and $X = \text{Spf} C$, let $P^* : C \to R$ be the map of $R$-algebras corresponding to $P : X \to S$. We will say an $R$-algebra map $h : C \to B$ satisfies ($\ast$) if it satisfies the following commutative diagram

$$\begin{array}{ccc}
C & \xrightarrow{h} & B \\
\downarrow & \searrow & \downarrow f \\
R & \xrightarrow{P^*} & B
\end{array}$$

Then the $S$-scheme $N^n$ can be described functorially as follows

(4.3) \quad \{N^n(B) = \{g : C \to W_n(B) \mid g = (g_0, \ldots, g_n), \text{ then } g_0 \text{ satisfies (}$\ast$)$\}\}

Note that if $g \in N^n(B)$ then $g(C) \subseteq W_n^\dagger(B)$. Also observe that the projection map $u : J^n X \to J^{n-1} X$ induces $u : N^n \to N^{n-1}$ for all $n \geq 1$.

**Theorem 4.3.** For each $n$, there exist a morphism $\bar{f} : N^n \to N^{n-1}$ which is lift of Frobenius and satisfies

$$\phi^{\circ 2} \circ \bar{f} = \phi \circ \bar{f} \circ \bar{f}.$$

In particular, if $X$ is smooth over $S$, then $\{N^n\}_{n=1}^\infty$ forms a prolongation sequence.

**Proof.** For any $R$-algebra, define $\bar{f} : N^n(B) \to N^{n-1}(B)$ as

(4.4) \quad $\bar{f}(g) = F^\dagger \circ g$, for all $g \in N^n(B)$.

The above composition makes sense as $g \in N^n(B)$ corresponds to an $R$-algebra morphism $g : C \to W_n^\dagger(B)$, where $N^n \simeq \text{Spf} C$ and hence the composition $F^\dagger \circ g \in N^{n-1}(B)$. Then it follows that $\bar{f}$ is a lift of Frobenius with respect to $u$ from prop. 4.1 and the compositional identity is an immediate consequence of prop. 4.2.
If $X$ is smooth, then the $N^n$s are flat over $S$ for all $n$. Hence the lift of Frobenius $\tilde{f} : N^n \to N^{n-1}$ corresponds to a $\pi$-derivation $\delta$ with respect to $u$ on the corresponding structure sheaves hence making the system $\{N^n\}_{n=1}^{\infty}$ into a prolongation sequence. □

Let us define $\Pi^{n,\dagger}_{\phi}A = \Pi^n A \times_A S$ as the following fiber product

$$
\begin{array}{ccc}
\Pi^{n,\dagger}_{\phi}A & \overset{i_w}{\rightarrow} & \Pi^n A \\
\downarrow & & \downarrow u_w \\
S & \overset{e}{\rightarrow} & A
\end{array}
$$

where $u_w$ is the usual projection along the first coordinate of $\Pi^n A$ and $i_w : \Pi^{n,\dagger}_{\phi}A \to \Pi^n A$ is the induced morphism. Then we have

$$
0 \longrightarrow N^n \overset{i}{\rightarrow} J^n A \overset{u}{\rightarrow} A \longrightarrow 0
$$

$$
0 \longrightarrow \Pi^{n,\dagger}_{\phi}A \overset{i_w}{\rightarrow} \Pi^n A \overset{u_w}{\rightarrow} A \longrightarrow 0
$$

**Theorem 4.4.** Let $X = A$ be a smooth group scheme over $S$. Then the morphism of group schemes $(i \circ \tilde{f} - \phi \circ i) : N^n \to J^{n-1}A$ uniquely factors through $N^1$ as

$$
\begin{array}{ccc}
N^n & \overset{i_0f-\phi i}{\rightarrow} & J^{n-1}A \\
\downarrow u & & \downarrow g \\
N^1 & \rightarrow &
\end{array}
$$

**Proof.** Let $e : S \to A$ denote the identity section. Consider the following diagram

$$
\begin{array}{ccc}
N^n & \overset{w}{\rightarrow} & \Pi^{n,\dagger}_{\phi}A \\
\downarrow x \mapsto (x,-x) & & \downarrow z \mapsto (z,-z) \\
N^n \times N^n & \overset{w}{\rightarrow} & \Pi^{n,\dagger}_{\phi}A \times \Pi^{n,\dagger}_{\phi}A \\
\downarrow i \times f & & \downarrow i_w \times i_w' \\
J^n A \times N^{n-1} & \overset{w}{\rightarrow} & \Pi^n A \times \Pi^{n-1,\dagger}_{\phi}A \\
\downarrow \phi \times i & & \downarrow \phi_w \times i_w \\
J^{n-1}A \times J^{n-1}A & \overset{w}{\rightarrow} & \Pi^{n-1} A \times \Pi^{n-1,\dagger}_{\phi}A \\
\downarrow (x_1,x_2) \mapsto x_1x_2 & & \downarrow (z_1,z_2) \mapsto z_1z_2 \\
J^{n-1}A & \overset{w}{\rightarrow} & \Pi^{n-1} A \\
\end{array}
$$

Then the composition of the left column of the above diagram is precisely $(i_0f-\phi i)$ whereas the right column sends $z = (z_1, \cdots, z_n) \mapsto (z_1, e, \cdots, e)$. Hence the map
ISOCRYSTALS ASSOCIATED TO ARITHMETIC JET SPACES OF ABELIAN SCHEMES

\[ \Pi_{g}^{n+1} A \to \Pi_{g}^{n-1} A \text{ factors as } \Pi_{g}^{n} A \to \Pi_{g}^{n+1} A \xrightarrow{\rho_{n}} \Pi_{g}^{n-1} A \text{ given by} \]
\[ (z_{1}, \cdots, z_{n}) \mapsto z_{1} \mapsto (z_{1}, e, \cdots, e) \]

Hence we have

\[ \begin{array}{c}
\xymatrix{
N^{1} \ar[r]^{w} \ar[d]_{u} & \Pi_{g}^{n+1} A \ar[d]_{g} \\
N^{n} \ar[r]_{i \circ f - \phi \circ i} \ar[d]_{w} & \Pi_{g}^{n+1} A \\
J^{n-1} A \ar[r]_{u} & \Pi_{g}^{n-1} A
}\
\end{array} \]

Now we claim that there is a unique map \( g : N^{1} \to J^{n-1} A \), as shown above, making the diagram commute. Observe that the map \( u : N^{n} \to N^{1} \) admits a section \( \sigma \) which is a morphism of schemes since \( u \) is simply the projection map. And hence we can put \( g = (i \circ f - \phi \circ i) \circ \sigma \).

It remains to prove uniqueness of \( g \) and the commutativity relation \( i \circ f - \phi \circ i = u \circ g \). By the diagram above, both these statements will follow from the injectivity of the map
\[ (J^{n-1} A)(B) \to (\Pi_{g}^{n-1} A)(B), \]
where \( N^{1} = \text{Spec } B \). So it remains to show this injectivity. By adjointness, this is equivalent to the injectivity of the map \( A(W_{n}(B)) \to A(\Pi_{g}^{n-1} B) \). To show this, it is enough to show that \( \text{Spec } \Pi_{g}^{n-1} B \to \text{Spec } W_{n}(B) \) is an epimorphism in the category of schemes. To show this, it is enough to show that the ghost map \( W_{n}(B) \to \Pi_{g}^{n-1} B \) is injective. (See [8] (9.5.6).) But this holds because \( N^{1} \) is smooth over \( S \) and hence \( B \) is flat.

5. THE KERNEL OF JET SPACES

Let \( A \) be a smooth commutative group scheme over \( S \) of relative dimension \( g \). Let \( x_{0} = (x_{01}, \cdots, x_{0g}) \) be an etale coordinate system of \( A \) around the identity section. Then by the local trivialisation of jet spaces of smooth schemes, let \( x = (x_{0}, \cdots, x_{n}) \) be the local Witt coordinates for \( J^{n} A \) around the identity section where \( x_{i} = (x_{i1}, \cdots, x_{ig}) \) and let \( (x_{1}, \cdots, x_{n}) \) denote the local coordinates around the identity section of \( N^{n} \). For every \( n \) we have the following exact sequence of group schemes
\[ 0 \to N^{n} \xrightarrow{i} J^{n} A \xrightarrow{w} A \to 0 \]

(5.1)

Let \( pr_{j} : \hat{\mathbb{G}}_{a}^{g} \to \hat{\mathbb{G}}_{a} \) denote the \( j \)-th projection for \( 1 \leq j \leq g \). Let for all \( n, H^{n} \) be defined by the short exact sequence \( 0 \to H^{n} \to N^{n} \to N^{n-1} \to 0 \). For any group scheme \( G \) of relative dimension \( g \), let \( G^{\text{for}} \) denote the formal group law associated to \( G \).

In prop. 4.1 of [7], Buium constructs a group scheme homomorphism
\[ \nu : H^{n} \to \hat{\mathbb{G}}_{a}^{g}, \]
Proposition 5.1. \( \nu \) induces an isomorphism \((H^n)_{\text{for}} \to (\mathbb{G}_a)^g\) of formal group laws over \(K\). The compositions \(\text{pr}_j \circ \nu\) form a \(K\)-basis for \(\text{Hom}(H^n, \mathbb{G}_a)_K\) for all \(j = 1, \cdots, g\). Moreover if the ramification index \(e\) satisfies \(e \leq p - 1\), then \(\nu\) is an isomorphism.

Lemma 5.2. For all \(n \geq 1\), we have \(\text{rk}_R \text{Hom}(N^n, \mathbb{G}_a) \leq ng\).

Proof. Applying \(\text{Hom}(\cdot, \mathbb{G}_a)\) to the short exact sequence in prop. 5.1 we get
\[
(2.2) \quad 0 \to \text{Hom}(N^{n-1}, \mathbb{G}_a) \to \text{Hom}(N^n, \mathbb{G}_a) \to \text{Hom}(H^n, \mathbb{G}_a) \to \text{Ext}(N^{n-1}, \mathbb{G}_a)
\]
Since \(\text{Hom}(H^n, \mathbb{G}_a) \simeq R^g\) we have \(\text{rk}_R \text{Hom}(N^n, \mathbb{G}_a) \leq \text{rk}_R \text{Hom}(N^{n-1}, \mathbb{G}_a) + g\) and hence it easily follows that \(\text{rk}_R \text{Hom}(N^n, \mathbb{G}_a) \leq ng\).  

For all \(1 \leq j \leq g\), define \(\Psi_{1j} : N^1 \to \mathbb{G}_a\) as \(\Psi_{1j} := \text{pr}_j \circ \nu\). Now, for all \(1 \leq i \leq n\) and \(1 \leq j \leq g\) define \(\Psi_{ij} : N^n \to \mathbb{G}_a\) as
\[
(5.3) \quad \Psi_{ij} := \Psi_{1j} \circ f^{(i-1)}.
\]

Proposition 5.3. For all \(1 \leq i \leq n\) and \(1 \leq j \leq g\), the set \(\{\Psi_{ij}\}\) form an \(R\)-basis for \(\text{Hom}(N^n, \mathbb{G}_a)\). In particular \(\text{rk}_R \text{Hom}(N^n, \mathbb{G}_a) = ng\).

Proof. By lemma 5.2, we have \(\text{rk}_R \text{Hom}(N^n, \mathbb{G}_a) \leq ng\). Hence it is sufficient to show that \(\{\Psi_{ij}\}\)s are linearly independent for all \(1 \leq i \leq n\) and \(1 \leq j \leq g\). For the sake of simplicity, we give the proof in the case when \(p \geq 3\) and \(e \leq p - 1\), in which case, \(\nu : N^1 \to \mathbb{G}_a^g\) also satisfies \(\nu(x_1) \equiv x_1 \mod \pi\). This proof can also be adapted to the general case.

Note that
\[
(5.4) \quad \Psi_{ij}(x_1, \cdots, x_n) \equiv x_{ij}^{(i-1)} \mod \pi.
\]
Hence \(\{\Psi_{ij}\}\)s are linearly independent mod \(\pi\) and since \(R\) is \(\pi\)-torsion free, \(\{\Psi_{ij}\}\)s are \(R\)-linearly independent by Nakayama’s lemma.

We define \(\Psi_i := (\Psi_{i1}, \cdots, \Psi_{ig}) \in \text{Hom}(N^n, \mathbb{G}_a)^g\). Then by proposition 5.3, any morphism \(\Psi \in \text{Hom}(N^n, \mathbb{G}_a)\) can be represented as
\[
(5.5) \quad \Psi = \gamma_1 \cdot \Psi_1 + \cdots + \gamma_n \cdot \Psi_n
\]
where \(\gamma_i \in \text{Mat}_{1 \times g}(R)\) and “.” denotes the usual dot product of two vectors.

6. The \(F\)-isocrystal

Let \(x_0 = (x_{01}, \cdots, x_{0g})\) be an etale coordinate system of \(A\) around the identity section. Then by the local trivialisation of jet spaces of smooth schemes, let \(x = (x_0, \cdots, x_n)\) be the local Witt coordinates for \(J^nA\) around the identity section where \(x_1 = (x_{i1}, \cdots, x_{ig})\). Then in this coordinate system, if the lift of Frobenius map \(\phi : J^{n+1}A \to J^nA\) is given by
\[
(6.1) \quad \phi(x_0, \cdots, x_{n+1}) = (y_0, \cdots, y_n)
\]
then \( y_0 = (x_{01}^q + \pi x_{11}, \ldots, x_{0g}^q + \pi x_{1g}) \). Let \( A_g \) be a \( g \times g \) matrix given by

\[
A_g = \begin{pmatrix}
q x_{01}^{q-1} & 0 & \cdots & 0 \\
0 & q x_{02}^{q-1} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & q x_{0g}^{q-1}
\end{pmatrix}
\]

Let \( \pi_g \) denote the \( g \times g \) identity matrix. Then the \((n+1)g \times (n+2)g\) derivative matrix of \( \phi \) is given by

\[
\begin{pmatrix}
A_g & \pi \pi_g & * \\
0 & 0 & *
\end{pmatrix}
\]

where 0 is the \( ng \times g\)-zero matrix. Hence when the derivative matrix is evaluated at the identity section \( x = 0 \) we get

\[
D \phi = \begin{pmatrix}
0_g & \pi \pi_g & * \\
0 & 0 & *
\end{pmatrix}
\]

where \( 0_g \) is the \( g \times g\)-zero matrix.

Recall that \( \text{Ext}^2(A, \hat{G}_n) \) parametrises isomorphism classes of extensions of \( A \) by \( \hat{G}_n \), along with a splitting of the corresponding short exact sequence of the Lie algebras. The \( R\)-module \( \text{Ext}^2(A, \hat{G}_n) \) is also interpreted as the de Rham cohomology associated to the abelian scheme \( A \). For all \( n \geq 1 \), we will define maps from \( \text{Hom}_A(N^n, \hat{G}_n) \) to \( \text{Ext}^2(A, \hat{G}_n) \). These maps are obtained by push-outs of \( J^n A \) by \( \Psi \in \text{Hom}(N^n, \hat{G}_n) \). Now consider the exact sequence

\[
0 \to N^n \xrightarrow{i} J^n A \xrightarrow{u} A \to 0
\]

Given a \( \Psi \in \text{Hom}_A(N^n, \hat{G}_n) \) consider the push out

\[
\begin{array}{c}
0 \to N^n \xrightarrow{i} J^n A \xrightarrow{u} A \xrightarrow{0} \\
\downarrow \Psi \downarrow \downarrow s \Psi \downarrow \downarrow \downarrow A^*_\Psi \\
0 \to \hat{G}_n \xrightarrow{i} A^*_\Psi \xrightarrow{0} A \xrightarrow{0}
\end{array}
\]

where \( A^*_\Psi = J^n A \xrightarrow{u \circ D u} A \) and \( \Gamma(N^n) = \{(i(z), -\Psi(z)) | z \in N^n\} \subset J^n A \times N^n \) and \( g_\Psi(x) = [x, 0] \in A^*_\Psi \).

Based on the choice of local etale coordinates \( x_0 \) for \( A \), we obtain local etale Witt coordinates for \( J^n A \). This gives us a basis for \( \text{Lie} J^n A \) which we will still denote as \( x = (x_0, \ldots, x_n) \). Let \( s_{\text{Witt}} : \text{Lie} J^n A \to \text{Lie} N^n \) be given by \( s_{\text{Witt}}(x_0, \ldots, x_n) = (x_1, \ldots, x_n) \). Thus we have the following split exact sequence of \( R\)-modules

\[
0 \to \text{Lie} N^n \xrightarrow{D_i} \text{Lie} J^n A \xrightarrow{D u} \text{Lie}(A) \to 0
\]

Let \( v \) be the corresponding splitting \( v : \text{Lie} A \to \text{Lie} J^n A \) satisfying \( s_{\text{Witt}} = 1 - v \circ D u \). Then \( v \) is given by \( v(x_0) = (x_0, 0, \ldots, 0) \).

Let \( s_\Psi \) denote the induced splitting of the push out extension

\[
0 \to \text{Lie} \hat{G}_n \xrightarrow{s_\Psi} \text{Lie}(A^*_\Psi) \xrightarrow{0} \text{Lie}(A) \to 0
\]
It is given explicitly by \( \hat{s}_\Psi : \text{Lie} J^n A \times \hat{\text{G}_a} \to \hat{\text{G}_a} \)
\[
\hat{s}_\Psi(x, y) := D\Psi(s_{\text{Whit}}(x)) + y
\]
and
\[
s_\Psi : \text{Lie}(A^*_\Psi) = \frac{\text{Lie} J^n A \times \hat{\text{G}_a}}{\text{Lie} \Gamma(N^n)} \to \hat{\text{G}_a}
\]
This induces the following morphism of exact sequences
\[
(6.5) \quad 0 \rightarrow X_n(A) \rightarrow \text{Hom}_A(N^n, \hat{\text{G}_a}) \rightarrow \text{Ext}(A, \hat{\text{G}_a})
\]
\[
\Psi \rightarrow (A^*_\Psi, s_\Psi)
\]
\[
0 \rightarrow \text{Lie}(A)^* \rightarrow \text{Ext}^2(A, \hat{\text{G}_a}) \rightarrow \text{Ext}(A, \hat{\text{G}_a}) \rightarrow 0
\]

**Proposition 6.1.** Let \( \Theta \) be a character in \( X_n(A) \), and put \( \Psi = i^*\Theta \in \text{Hom}(N^n, \hat{\text{G}_a}) \).

1. The map \( X_n(A) \rightarrow \text{Lie}(A)^* \) of (6.5) sends \( \Theta \) to \(-D\Theta \circ v\).
2. Let \( \hat{\Theta} = \phi^*\Theta \), then \(-D\hat{\Theta} \circ v = 0\).

**Proof.** (1): Let us recall in explicit terms how the map is given. For the split extension \( A \times \hat{\text{G}_a} \), the retractions \( \text{Lie}(A) \times \hat{\text{G}_a} = \text{Lie}(A \times \hat{\text{G}_a}) \to \hat{\text{G}_a} \) are in bijection with maps \( \text{Lie}(A) \to \hat{\text{G}_a} \), a retraction \( s \) corresponding to map \( x_0 \mapsto s(x_0, 0) \). Therefore to determine the image of \( D\Theta \), we need to identify \( \text{Lie} A^*_\Psi \) with the split extension and then apply this map to \( s_\Psi \).

A trivialization of the extension \( \text{Lie} A^*_\Psi \) is given by the map
\[
\frac{\text{Lie} J^n A \times \hat{\text{G}_a}}{\text{Lie} \Gamma(N^n)} = \text{Lie} A^*_\Psi \rightarrow \text{Lie}(A) \times \hat{\text{G}_a}
\]
defined by \([a, b] \mapsto (u(a), D\Theta(a) + b)\). The inverse isomorphism \( H \) is then given by the expression
\[
H(x, y) = [v(x), y - D\Theta(v(x))],
\]
and so the composition \( \text{Lie}(A) \to \text{Lie}(A) \times \hat{\text{G}_a} \to \text{Lie}(A^*_\Psi) \to \hat{\text{G}_a} \) is simply \(-D\Theta \circ v\).

(2): We have \( \hat{\Theta} = \Theta \circ \phi \) and hence \( D\hat{\Theta} \circ v = D\Theta \circ D\phi \circ v \). But note that by equation (6.3), \( D\phi \circ v = 0 \) and hence we are done. \( \square \)

**Proposition 6.2.** If \( \Psi \in i^*\phi^*(X_n(A)) \), then the class \( (A^*_\Psi, s_\Psi) \in \text{Ext}^2(A, \hat{\text{G}_a}) \) is zero.

**Proof.** We know from diagram (6.5) that \( A^*_\Psi \) is a trivial extension since \( \Psi \) lies in \( i^*X_{n+1}(A) \). Now as in part (2) of proposition 6.1, we have, in the notation of that proposition, \(-D\hat{\Theta} \circ v = 0\) and therefore the class in \( \text{Ext}^2(E, \hat{\text{G}_a}) \) is zero by part (1). \( \square \)

**Proposition 6.3.** If \( \Theta \in X_n(A) \), then \((\phi \circ i - i \circ f)^*\Theta = \pi \Psi \) for some \( \Psi \in \text{Hom}(N^1, \hat{\text{G}_a}) \).
Then note that

\[ \phi : \text{Proposition 6.4.} \]

\[ \text{to the chosen coordinates be } D \]

\[ \text{induces a map } u \]

\[ \text{because we have } f \]

\[ \text{u} \]

\[ (6.6) \]

\[ \text{Then } u \]

\[ \text{implies that } \pi \]

\[ \text{y} \]

\[ \text{H}_{n+1}(A) \]

\[ \text{Let } \delta \]

\[ \text{is given by } g_\delta(z_1) = (z_1, 0, \cdots, 0) \]

\[ \text{and } u(x_1) = \pi x_1. \]

Then if \( g(x_1) = (y_0, \cdots, y_n) \) then the \( y_i \)'s satisfy

\[ y_0 = \pi x_1 \]

\[ y_0^q + \pi y_1^{q^{-1}} + \cdots + \pi^i y_i = 0, \text{ for all } i = 1, \cdots, n \]

Hence it is easy to see that \( \pi | y_i \) for all \( i = 0, \cdots, n \).

Now given a \( \delta \)-character \( \Theta(x_0, \cdots, x_n) \in X_n(A) \), we have \( \Theta(0, \cdots, 0) = 0 \). Then the composition \( \Theta \circ g : N^1 \to \hat{G}_a \) is given by \( x_1 \mapsto \Theta(y_1, \cdots, y_n) \). This clearly implies that \( \pi | \Theta(y_0, \cdots, y_n) \) and hence we are done. \( \square \)

The \( \phi \)-linear map \( \phi^* : X_{n-1}(A) \to X_n(A) \) induces a linear map \( X_{n-1}(A)^\phi \to X_n(A) \), which we will abusively also denote \( \phi^* \). We then define

\[ H_n(A) = \frac{\text{Hom}(N^n, \hat{G}_a)}{i^*\phi^*(X_{n-1}(A)^\phi)} \]

Then \( u : N^{n+1} \to N^n \) induces \( u^* : \text{Hom}(N^n, \hat{G}_a) \to \text{Hom}(N^{n+1}, \hat{G}_a) \). And since \( u^*i^*\phi^*(X_n(A)) = i^*u^*\phi^*(X_n(A)) = i^*\phi^*u^*(X_n(A)) \subset i^*\phi^*(X_{n+1}(A)) \), it also induces a map \( u^* : H_n(A) \to H_{n+1}(A) \). Define \( H(A) = \lim_{\to} H_n(A) \).

Similarly, \( f : N^{n+1} \to N^n \) induces \( f^* : \text{Hom}(N^n, \hat{G}_a) \to \text{Hom}(N^{n+1}, \hat{G}_a) \), which descends to a \( \phi \)-linear morphism of \( R \)-modules

\[ f^* : H_n(A) \to H_{n+1}(A) \]

because we have \( f^*i^*\phi^*(X_{n-1}(A)) = i^*\phi^*f^*(X_{n-1}(A)) \subset i^*\phi^*X_n(A) \). This then induces a \( \phi \)-linear endomorphism \( f^* : H(A) \to H(A) \).

For any \( \delta \)-character \( \Theta \in X_n(A) \), let the derivative at the identity with respect to the chosen coordinates be \( D\Theta = (A_0, \cdots, A_n) \) where \( A_j \in \text{Mat}_{1 \times g}(R) \).

**Proposition 6.4.** Let \( \Theta \) be a character in \( X_n(A) \).

1. We have

\[ i^*\phi^*\Theta = f^*(i^*\Theta) + \gamma.\Psi_1, \]

where \( \gamma = \pi A_0 \).

2. For \( n \geq 1 \), we have

\[ i^*(\phi^o)^n*\Theta = (f^{n-1})^*i^*\phi^*\Theta. \]

**Proof.** (1): Let \( \gamma \in R^g \) be such that

\[ (i^*\phi^* - f^*)\Theta = \gamma.\Psi_1 \]

Then note that

\[ i^*\phi^*\Theta \equiv \gamma.\Psi_1 \mod (\Psi_2, \cdots, \Psi_{2g}, \cdots, \Psi_{(n+1)}, \cdots, \Psi_{(n+1)g}). \]
in \( \text{Hom}(N^{n+1}, \hat{G}_a) \). Then by equation (6.3) the derivative matrix \( D(\Theta \circ \phi \circ i) \) at the identity section is

\[
(\pi A_0, *, \cdots, *)
\]

Hence we have

\[
(6.8) \quad \gamma = \pi A_0.
\]

(2): This is another way of expressing \( \phi^{\rho n} \circ i = \phi \circ i \circ f^{(n-1)} \), which follows from theorem 4.3 by induction. \( \square \)

**Proposition 6.5.** For any \( n \geq 0 \), the diagram

\[
\begin{array}{ccc}
X_n(E)/X_{n-1}(E) & \overset{\phi^*}{\longrightarrow} & X_{n+1}(E)/X_n(E) \\
\downarrow i^* & & \downarrow i^* \\
\text{Hom}_A(N^n, \hat{G}_a)/\text{Hom}_A(N^{n-1}, \hat{G}_a) & \overset{f^*}{\longrightarrow} & \text{Hom}_A(N^{n+1}, \hat{G}_a)/\text{Hom}_A(N^n, \hat{G}_a)
\end{array}
\]

is commutative. The morphisms \( i^* \) and \( \phi^* \) are injective, and \( f^* \) is bijective.

**Proof.** For \( n \geq 1 \), commutativity of the diagram follows from proposition 6.4; for \( n = 0 \), since \( X_0(A) = 0 \) the result follows.

The maps \( i^* \) are injective because the projections \( J^n A \to J^{n-1} A \) and \( N^n \to N^{n-1} \) have the same kernel, and \( f^* \) is an isomorphism by proposition 5.3. It follows that \( \phi^* \) is an injection. \( \square \)

7. The exact sequences

For every \( n \) we have the following short exact sequence

\[
(7.1) \quad 0 \to N^n \to J^n A \to A \to 0
\]

Applying \( \text{Hom}(-, \hat{G}_a) \) to the above short exact sequence gives us

\[
(7.2) \quad 0 \to X_n(A) \to \text{Hom}(N^n, \hat{G}_a) \overset{\partial}{\longrightarrow} \text{Ext}(A, \hat{G}_a)
\]

Note that \( \text{Ext}(A, \hat{G}_a) \simeq R^n \). Let \( I_n := \text{image}(\partial) \). We define \( m_1 \) as the lower splitting number if \( X_{m_1}(A) \neq \{0\} \) and \( X_{m_1-1}(A) = \{0\} \).

**Lemma 7.1.** We have \( m_1 = 1 \) or \( 2 \).

**Proof.** We know that for all \( n \), \( X_n(A) = \text{ker}(\partial) \). We know that \( \text{rk}_R \text{Ext}(A, \hat{G}_a) = g \) and by cor. 5.3 we have \( \text{rk}_R \text{Hom}(N^n, \hat{G}_a) = ng \) and since \( X_n(A) = \text{ker}(\partial) \), the result follows. \( \square \)

We define the upper splitting as the smallest number \( m_u \) such that \( \text{rk}_R I_n \) is constant for all \( n \geq m_u - 1 \). Note that \( m_u \) exists since for all \( n \), \( \text{rk}_R I_n \leq \text{rk}_R \text{Ext}(A, \hat{G}_a) = g \).

We define a differential character \( \Theta \in X_n(A)_K \) to be primitive if

\[ \Theta \notin u^*X_{n-1}(A)_K + \phi^*X_{n-1}(A)_K. \]

Define \( h_i = \text{rk} I_i - \text{rk} I_{i-1} \) for all \( i \geq 1 \). Then clearly \( h_1 \) is the rank of \( I_1 \). For each \( i \), let \( l_i = \text{rk} X_i(A)_K - \text{rk}(u^*X_{i-1}(A)_K + \phi^*X_{i-1}(A)_K) \). We will call the primitive rank of \( X_i(A)_K \) as \( l_i \).
For every $i$, let $\text{mult}(i)$ be a non-negative integer. We say $\mathcal{B}_i := \{\Theta_{ij}\}_{j=1}^{\text{mult}(i)}$ is a primitive basis for $X_i(A)_K$ if their images in $X_i(A)_K/(u^*X_{i-1}(A)_K + \phi^*X_{i-1}(A)_K)$ are distinct and forms a $K$-basis. Let $\mathcal{B}$ be a set such that it generates $X_{\infty}(A)_K$ as a $K[\phi^*]$-module. For each $i$, denote $\mathcal{B}_i = \mathcal{B} \cap (X_i(A)_K \setminus X_{i-1}(A)_K)$. We define $\mathcal{B}$ to primitively generate $X_{\infty}(A)_K$ if, for all $i$, $\mathcal{B}_i$ is a primitive basis for $X_i(A)_K$.

Let one that can always construct such a $\mathcal{B}$ by taking the union of $\mathcal{B}_i$ for all $i$, where $\mathcal{B}_i$ is a primitive basis for $X_i(A)_K$.

Let $S_n(\mathcal{B}_i) = \{\phi^h\Theta | \text{ for all } 0 \leq h \leq (n-i) \text{ and } \Theta \in \mathcal{B}_i\}$.

Define

$$X_{\text{prim}}(A) := \text{lim}_{\rightarrow} X_n(A)/\phi^*X_{n-1}(A).$$

**Proposition 7.2.** Let $\mathcal{B}$ primitively generate $X_{\infty}(A)_K$. Then for all $n$, the set $S_n(\mathcal{B}_1) \cup \cdots \cup S_n(\mathcal{B}_n)$ is $K$-linearly independent.

**Proof.** We will prove by contradiction. Suppose the set $S_n(\mathcal{B}_1) \cup \cdots \cup S_n(\mathcal{B}_n)$ is not $K$-linearly independent, then there exists a $K$-linear relation among the elements. We may assume that the highest order of the terms appearing in the relation with non-zero coefficients is $n$. Then there exists $a_{ijh}$ such that we have

$$\{a_{11}i^*(\phi^*(n-i))\Theta_{i1} + \cdots + a_{1\text{mult}(i)}i^*(\phi^*(n-i))\Theta_{i\text{mult}(i)}\} + \cdots + \{a_{n1}i^*(\phi^*(n-i))\Theta_{n1} + \cdots + a_{n\text{mult}(i)}i^*(\phi^*(n-i))\Theta_{n\text{mult}(i)}\} \equiv 0 \mod \text{Hom}(N^{n-1}, \hat{G}_a)$$

Let $l' \in \{1, \cdots, l\}$ be such that $a_{l'h_0} \neq 0$ for some $h_0$ and $a_{l'h} = 0$ for all $j > l'$ and all $h = 1, \cdots, \text{mult}(i_j)$. Then the above relation becomes

$$\{a_{11}i^*(\phi^*(n-i))\Theta_{i1} + \cdots + a_{1\text{mult}(i)}i^*(\phi^*(n-i))\Theta_{i\text{mult}(i)}\} + \cdots + \{a_{l'1}i^*(\phi^*(n-i))\Theta_{l'1} + \cdots + a_{l'\text{mult}(i)}i^*(\phi^*(n-i))\Theta_{l'\text{mult}(i)}\} \equiv 0 \mod \text{Hom}(N^{n-1}, \hat{G}_a)$$

(7.3)

Using the assumption that $\phi$ is an automorphism of $R$, we may define

$$\Theta := \{a_{11}^{-1}i^*(\phi^{-(i_{l'-i})})\Theta_{i1} + \cdots + a_{1\text{mult}(i)}^{-1}i^*(\phi^{-(i_{l'-i})})\Theta_{i\text{mult}(i)}\} + \cdots + \{a_{l'1}^{-1}i^*(\phi^{-(i_{l'-i})})\Theta_{l'1} + \cdots + a_{l'\text{mult}(i)}^{-1}i^*(\phi^{-(i_{l'-i})})\Theta_{l'\text{mult}(i)}\}$$

The image of $\Theta$ in the quotient $X_{i_{l'}}(A)_K/(u^*X_{i_{l'}-1}(A)_K + \phi^*X_{i_{l'}-1}(A)_K)$ is non-zero, since the image of $\mathcal{B}_{i_{l'}}$ generates the quotient and at least one of the $a_{l'h}$ are non-zero. Therefore, we must have $\Theta \in X_{i_{l'}}(A)_K \setminus X_{i_{l'}-1}(A)_K$ and hence we have $i^*\Theta \neq 0 \mod \text{Hom}(N^{n-1}, \hat{G}_a)$. Recall from proposition 6.5 that

$$i^*(\phi^{-(n-i)}i^*\Theta) \equiv i^*\phi^{-(n-i)}\Theta \mod \text{Hom}(N^{n-1}, \hat{G}_a)$$

(7.4)

But this contradicts equation (7.3) since $i^*\phi^{-(n-i)}\Theta$ is the expression on the left hand side of the equivalence relation. Therefore we must have that the set $S_n(\mathcal{B}_1) \cup \cdots \cup S_n(\mathcal{B}_n)$ is $K$-linearly independent. 

\[\square\]
Proposition 7.3. We have
\[ \text{rk}_K(u^*X_{n-1}(A)_K + \phi^*X_{n-1}(A)_K) = nl_1 + (n-1)l_2 + \cdots + 2l_{n-1}. \]

Proof. Let \( B_i \) be a primitive basis for \( X_i(A)_K \) for all \( i \). Then the cardinality of \( B_i \) is \( l_i \). Then the set \( S_n(B_1) \cup \cdots \cup S_n(B_{n-1}) \) spans \( u^*X_{n-1}(A)_K + \phi^*X_{n-1}(A)_K \). By proposition 7.4, they are \( K \)-linearly independent and hence forms a \( K \)-basis. The result follows from the fact that the cardinality of \( S_n(B_1) \cup \cdots \cup S_n(B_{n-1}) \) is \( nl_1 + (n-1)l_2 + \cdots + 2l_{n-1} \). \( \square \)

Lemma 7.4. For all \( n \geq 2 \), \( l_n = h_{n-1} - h_n \).

Proof. For \( n = 1 \), we have \( l_1 = g - h_1 \). For \( n = 2 \), we have
\[
l_2 = (2g - (h_1 + h_2)) - \text{rk}_K(u^*X_1(A)_K + \phi^*X_1(A)_K)
= (2g - (h_1 + h_2)) - 2l_1, \text{ by prop. 7.3}
= h_1 - h_2
\]
Now by induction let’s assume the result is true for \( 2, \cdots, n-1 \). Then we get the sum
\[
l_n = ng - (h_1 + \cdots + h_n) - \text{rk}_K(u^*X_{n-1}(A)_K + \phi^*X_{n-1}(A)_K)
= ng - (h_1 + \cdots + h_n) - (nl_1 + (n-1)l_2 + \cdots + 2l_{n-1}), \text{ by prop. 7.3.}
= ng - (h_1 + \cdots + h_n) - (n(g - h_1) + (n-1)(h_1 - h_2) + (n-2)(h_2 - h_3) + \cdots + 3(h_{n-3} - h_{n-2}) + 2(h_{n-2} - h_{n-1}))
= h_{n-1} - h_n \quad \square
\]

Lemma 7.5. For all \( n \geq 1 \), \( h_n \) is a (weakly) decreasing function of \( n \).

Proof. We know \( l_n \geq 0 \) for all \( n \) and hence by lem. 7.4 we have \( h_{n-1} - h_n \geq 0 \) which implies \( h_u \leq h_{n-1} \) and we are done. \( \square \)

Corollary 7.6. If \( h_N = 0 \) for some \( N \) then \( h_n = 0 \) for all \( n \geq N \).

Corollary 7.7. If \( h_N = 0 \), then \( l_n = 0 \) for all \( n \geq N + 1 \).

Proof. If follows from the fact that \( l_{n+1} = h_n - h_{n+1} \). \( \square \)

Proposition 7.8. (1) For all \( n \geq m_u + 1 \), we have \( l_n = 0 \). In other words, there are no primitive characters of order greater than \( m_u \).

(2) We have \( m_1 \leq m_u \).

Proof. (1): By definition of \( m_u \), we have \( h_{m_u} = h_{m_u+1} = \cdots = 0 \). This implies by lemma 7.4 that \( l_n = 0 \) for all \( n \geq m_u + 1 \).

(2): Since we know that \( m_1 \) is either 1 or 2, then clearly any \( K \)-basis of \( X_{m_1}(A)_K \) is also a primitive basis. Therefore \( m_1 \) is the least number for which a non-trivial primitive basis exists. But there are no further primitive characters in \( X_n(A)_K \) for all \( n \geq m_u + 1 \). Therefore we must have \( m_1 \leq m_u \). \( \square \)

Here we would like to note that as a consequence of corollary 7.8, if \( B \) primitively generates \( X_\infty(A)_K \), then \( B \) can be written as
\[ B = B_{i_1} \cup \cdots \cup B_{i_j} \]
where \( m_1 = i_1 < \cdots < i_l = m_u \) and \( B_{i_j} \) is a primitive basis for \( X_{i_j}(A)_K \) for all \( j \).
**Theorem 7.9.** For any abelian scheme $A$ of dimension $g$, $X_\infty(A)_K$ is freely $K[\phi^\ast]$-generated by $g$ differential characters of order at most $g + 1$. In other words $m_u \leq g + 1$.

**Proof.** Note that $X_\infty(A)_K$ is freely generated by the primitive characters because of proposition 7.2. For $m_1 = 2$, we want to show that $X_\infty(A)_K$ is $K[\phi^\ast]$-generated by $X_2(A)_K$. Hence it is sufficient to show that $l_n = 0$ for all $n \geq 3$. Since $m_1 = 2$, we have $h_1 = g$. Since $\operatorname{rk}_K \operatorname{Ext}(E, \hat{G}_a)_K = g$, we have $h_2 = h_3 = \cdots = 0$. Then by lemma 7.4, we have $l_3 = l_4 = \cdots = 0$ and we are done.

If $m_1 = 1$, then $h_1 > 0$. Note that $\sum h_i \leq g$ and since $h_1$'s are a weakly decreasing sequence of non-negative integers, we must have $h_i = 0$ for all $i \geq g + 1$ and hence $m_u \leq g + 1$. □

**Corollary 7.10.** We have

$$X_{\text{prim}}(A)_K \cong X_{m_u}(A)_K / \phi^\ast X_{m_u - 1}(A)_K$$

Moreover, $B_{i_1} \cup \cdots \cup B_{i_r}$ is a $K$-basis for $X_{\text{prim}}(A)_K$.

**Proof.** For all $n \geq m_u$, $S_n(B_{i_1}) \cup \cdots \cup S_n(B_{i_r})$ generates $X_n(A)_K$ as a $K$-module. Whereas, $(S_n(B_{i_1}) \setminus B_{i_1}) \cup \cdots \cup (S_n(B_{i_r}) \setminus B_{i_r})$ generates $\phi^\ast X_{n-1}(A)_K$ as a $K$-module. Therefore $X_n(A)_K / \phi^\ast X_{n-1}(A)_K$ is generated by $B_{i_1} \cup \cdots \cup B_{i_r}$ as a $K$-module for all $n \geq m_u$ and hence in particular $X_{\text{prim}}(A)_K \cong X_{m_u}(A)_K / \phi^\ast X_{m_u - 1}(A)_K$. □

**Corollary 7.11.** If $g = 1$, then $m_1 = m_u = m$ and $X_{\text{prim}}(A)_K \cong X_m(A)_K$.

**Proof.** If $m_1 = 1$, then note that $h_1 = 0$. Since $h_n$ is a weakly decreasing function in $n$, we have $h_0 = h_1 = h_2 = \cdots = 0$. Therefore the rank of $I_n$ is 0 for all $n \geq 0$ and hence $m_u = 1$.

If $m_1 = 2$, then note that $h_1 = 1$ since $\partial : \operatorname{Hom}(\mathbb{N}^1, \hat{G}_a)_K \to \operatorname{Ext}(A, \hat{G}_a)_K$ is injective. But since $\operatorname{rk}_K \operatorname{Ext}(A, \hat{G}_a)_K = 1$, we have $h_2 = h_3 = \cdots = 0$. Therefore $\operatorname{rk} I_i$ is constant for all $i \geq 1$ and hence $m_u = 1$.

\[\square\]

8. The $F$-isocrystal and Hodge sequence of $A$

In this section, based on our choice of etale coordinates we construct canonical $K$-basis of our filtered isocrystal $H(A)$. We also show the exact sequence corresponding to this filtration admits a canonical map to the Hodge sequence of $A$.

**Proposition 8.1.** The morphism

$$u^\ast : H_n(A)_K \to H_{n+1}(A)_K$$

is injective. For $n \geq m_u$, it is an isomorphism.
Proof. Consider the following diagram of exact sequences:

\[
\begin{array}{ccccccc}
0 & \rightarrow & X_n(A)_{K} & \rightarrow & X_{n-1}(A)_{K} & \rightarrow & 0 \\
& & \uparrow i^{*} \phi^{*} & & \downarrow \phi & & \\
& & \text{Hom}(N^{n+1}, \hat{G}_a)_{K} & \rightarrow & H_{n+1}(A)_{K} & \rightarrow & 0 \\
& & \downarrow u^{*} & & \downarrow u^{*} & & \\
& & \text{Hom}(N^n, \hat{G}_a)_{K} & \rightarrow & H_{n}(A)_{K} & \rightarrow & 0 \\
& & 0 & \rightarrow & 0 & \rightarrow & 0
\end{array}
\]

Then \(i^{*} \phi^{*} : X_n(A)/X_{n-1}(A) \rightarrow \text{Hom}(N^{n+1}, \hat{G}_a)/\text{Hom}(N^n, \hat{G}_a)\) is injective by proposition 6.5 and hence \(H_n(A)_{K} \rightarrow H_{n-1}(A)_{K}\) is injective for all \(n\).

It is sufficient to show that \(u^{*} : H_n(A)_{K} \rightarrow H_{n+1}(A)_{K}\) is surjective for all \(n \geq m_n\). Let \(X_n(A)\) be primitively generated by the \(g\)-elements \(B_{i_1} \cup \cdots \cup B_{i_r}\) as in theorem 7.9. Then the image of \((S_n(B_{i_1}) \cup S_n(B_{i_2}) \cup \cdots \cup S_n(B_{i_r}))\) forms a \(K\)-basis for \(X_n(A)_{K}/u^{*}X_{n-1}(A)_{K}\) for all \(n \geq m_n\). Hence \(r_{K}X_n(A)_{K}/u^{*}X_{n-1}(A)_{K} = g = \text{Hom}(N^n, \hat{G}_a)_{K}/\text{Hom}(N^{n-1}, \hat{G}_a)_{K}\) which implies \(i^{*} \phi^{*}\) is surjective for all \(n \geq m_n\) and hence \(u^{*} : H_n(A) \rightarrow H_{n+1}(A)\) is surjective.

Finally the morphism \(\text{Hom}_A(N^n, \hat{G}_a) \rightarrow \text{Ext}^2(A, \hat{G}_a)\) of diagram (6.5) vanishes on \(\phi^{*}(X_{n-1}(A))\), by proposition 6.2, and hence induces a morphism of exact sequences

\[
\begin{array}{cccccc}
0 & \rightarrow & X_n(A) & \rightarrow & H_n(A) & \rightarrow & I_n(A) & \rightarrow & 0 \\
& & \tau & & \downarrow \phi & & \\
0 & \rightarrow & \text{Lie}(A)^{*} & \rightarrow & \text{Ext}^2(A, \hat{G}_a) & \rightarrow & \text{Ext}(A, \hat{G}_a) & \rightarrow & 0
\end{array}
\]

where \(I_n(A)\) denotes the image of \(\partial : \text{Hom}(N^n, \hat{G}_a) \rightarrow \text{Ext}_A(A, \hat{G}_a)\).

**Theorem 8.2.** There exists a map of short exact sequences of \(K\)-modules

\[
\begin{array}{cccccc}
0 & \rightarrow & X_{\text{prim}}(A)_{K} & \rightarrow & H(A)_{K} & \rightarrow & I(A)_{K} & \rightarrow & 0 \\
& & \tau & & \downarrow \phi & & \\
0 & \rightarrow & (\text{Lie} A)^{*}_{K} & \rightarrow & \text{Ext}^2(A, \hat{G}_a)_{K} & \rightarrow & \text{Ext}(A, \hat{G}_a)_{K} & \rightarrow & 0
\end{array}
\]

where \(r_{K}H(A)_{K} \leq 2g\).

Moreover \(\Phi\) is injective if and only if \(\gamma\) is invertible.
By corollary 7.10, we have \( \text{rk}_K X_{\text{prim}}(A)_K = g \) and \( \text{rk}_K I(A)_K \leq g \) and hence \( \text{rk}_K H(A) \leq 2g \).

Let \( \Theta_1, \ldots, \Theta_g \) be a basis for \( X_{\text{prim}}(A)_K \). For each \( \Theta_i : J^n A \to \hat{G}_n \), let the derivative matrix at the identity be \( D\Theta_i = (A_{0i}, \ldots, A_{ni}) \) where \( A_{jis} \) are \((1 \times g)\)-matrices. Let \( \gamma_i \in \mathbb{R}^g \) be such that

\[
(i^* \phi^* - j^* i^*)\Theta_i = \gamma_i \Psi_1
\]

By proposition 6.4 we have

\[
\gamma_i = \pi A_{0i}
\]

Therefore the \( g \times g \) matrix of \( \Upsilon \) with respect to our basis is given by \((A_{01}, \ldots, A_{0g})\) and satisfying

\[
\gamma = \pi(A_{01}, \ldots, A_{0g}).
\]

It is enough to show that \( \Upsilon \) is injective if and only if \( \gamma \neq 0 \). Now \( \Upsilon(\Theta_i) = -D\Theta_i \circ v = -A_{0i} \) and hence the matrix for \( \Upsilon \) is given by \( \frac{1}{\pi} \gamma \) and we are done. \( \square \)

9. The Elliptic Curve Case

When \( A \) is an elliptic curve over \( S \), then by corollary 7.11 we have \( m = m_1 = m_n \leq 2 \). The following are two possible choices of \( \Theta_m \in X_m(A)_K \):

If \( m = 1 \), by proposition 6.5, there exists \( \Theta_1 \in X_1(A)_K \) such that \( i^* \Theta_1 = \Psi_1 \).

If \( m = 2 \), again by proposition 6.5, there exists \( \Theta_2 \in X_2(A)_K \) such that \( i^* \Theta_2 = \Psi_2 - \lambda \Psi_1 \). We have \( i^* \phi^* \Theta_2 = \Psi_3 - \phi(\lambda) \Psi_2 - \gamma \Psi_1 \). Then \( \partial \Psi_2 = \lambda_1 \partial \Psi_1 \) and \( \partial \Psi_3 = \phi(\lambda) \Psi_2 + \gamma \Psi \).

**Proposition 9.1.** For \( n \geq m \),

\[
H_n(A)_K \simeq \begin{cases} 
K\langle \Psi_1 \rangle, & \text{if } m = 1 \\
K\langle \Psi_1, \Psi_2 \rangle, & \text{if } m = 2
\end{cases}
\]

**Proof.** We know that \( H_m(A) = \text{Hom}(N^m, \hat{G}_n) \). Then the result follows from the above discussion and proposition 8.1. \( \square \)

**Proposition 9.2.** We have

\[
I_n(A) \otimes K \simeq \begin{cases} 
K\langle \Psi_1, \ldots, \Psi_n \rangle, & \text{if } n \leq m - 1 \\
K\langle \Psi_1, \ldots, \Psi_{m-1} \rangle, & \text{if } n \geq m - 1
\end{cases}
\]

**Proof.** The case \( n \leq m - 1 \) is clear. So suppose \( n \geq m - 1 \). Then \( \text{Hom}_A(N^j, \hat{G}_n) \otimes K \) has basis \( \Psi_1, \ldots, \Psi_j \), and \( X_n(A) \otimes K \) has basis \( \Theta_m, \ldots, (\phi^{n-m})^* \Theta_m \). Since each \( (\phi^{n-j})^* \Theta_m \) equals \( \Psi_{m+j} \) plus lower order terms, \( K\langle \Psi_1, \ldots, \Psi_{m-1} \rangle \) is a complement to the subspace \( X_n(E) \) of \( \text{Hom}_A(N^n, \hat{G}_n) \). Therefore the map \( \partial \) from \( K\langle \Psi_1, \ldots, \Psi_{m-1} \rangle \) to the quotient \( I_n(A) \) is an isomorphism. \( \square \)
Lemma 9.3. Consider the $\phi$-linear endomorphism $F$ of $K^m$ with matrix

$$
\begin{pmatrix}
0 & 0 & \ldots & 0 & \mu_m \\
1 & 0 & \ldots & 0 & \mu_{m-1} \\
0 & 1 & \ldots & 0 & \mu_{m-2} \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \ldots & 1 & \mu_1
\end{pmatrix},
$$

for some given $\mu_1, \ldots, \mu_m \in K$. If $K^m$ admits an $R$-lattice which is stable under $F$, then we have $\mu_1, \ldots, \mu_m \in R$.

Proof. The proof uses Dieudonné–Manin theory and follows similar lines in the equal characteristic case that is shown in lem. 9.7 in [3]. $\square$

Theorem 9.4. If $A$ splits at $m = 2$, then $\lambda \in R$.

Proof. Let $\gamma$ be the element associated to $\Theta_2$ as in proposition 6.4. We will prove the cases when $\gamma = 0$ and $\gamma \neq 0$ separately.

Case $\gamma = 0$ When $\gamma = 0$ we have $f^*i^* = i^*\phi^*$, and hence for all $n \geq 1$, this induces a $\phi$-linear map $f^*: I_n(A) \to I_n(A)$ as follows

$$
\begin{array}{cccccc}
0 & \longrightarrow & X_n(A) & \stackrel{i^*}{\longrightarrow} & \text{Hom}(N^n, \hat{\mathbb{G}}_a) & \stackrel{\partial}{\longrightarrow} & I_n(A) & \longrightarrow & 0 \\
& & \uparrow \phi & & \uparrow \rho & & \uparrow \varphi & & \\
0 & \longrightarrow & X_{n-1}(A) & \stackrel{i^*}{\longrightarrow} & \text{Hom}(N^{n-1}, \hat{\mathbb{G}}_a) & \stackrel{\partial}{\longrightarrow} & I_{n-1}(A) & \longrightarrow & 0
\end{array}
$$

Let $I(A) = \lim_{\rightarrow} I_n(A) \subseteq \text{Ext}(A, \hat{\mathbb{G}}_a)$. Then by proposition 9.2, the vector space $I(A)_K$ has a $K$-basis $\partial \Psi_1$, and with respect to this basis, the $\phi$-linear endomorphism $f^*$ has matrix $\Gamma_0 = (\lambda)$.

Note that $I(A)$ is a finitely generated $R$-module since it is a submodule of $\text{Ext}(A, \hat{\mathbb{G}}_a)$ which is a finitely generated free $R$-module. Since $\Gamma_0$ is an endomorphism of $I(A)$ and hence an integral lattice of $I(A)_K$, we conclude that $\lambda$ is integral.

Case $\gamma \neq 0$ Let $H(A) = \lim_{\rightarrow} H_n(A)$. Let us consider the matrix $\Gamma$ of the $\phi$-linear endomorphism $f$ of $H(A)_K$ with respect to the $K$-basis $\Psi_1, \Psi_2$ given by proposition 9.1. Then we have

$$
i^*\phi^*\Theta_2 = f^*(\Psi_2) - \phi(\lambda)\Psi_2 + \gamma \Psi_1.
$$

Therefore we have

$$
f^*(\Psi_2) \equiv \phi(\lambda)\Psi_2 - \gamma \Psi_1 \mod i^*\phi^*(X_2^\phi)
$$

and hence

$$
\Gamma = \begin{pmatrix}
0 & -\gamma \\
1 & \phi(\lambda)
\end{pmatrix}
$$
We will now apply lemma 9.3 to the operator \( f^* \) on \( \mathbf{H}(A)_K \), but to do this we need to produce an integral lattice \( M \). Consider the commutative square

\[
\begin{array}{ccc}
\mathbf{H}(A) & \xrightarrow{\Phi} & \text{Ext}^2(A, \hat{\mathbb{G}}_a) \\
\downarrow & & \downarrow j \\
\mathbf{H}(A)_K & \xrightarrow{\Phi_K} & \text{Ext}^2(A, \hat{\mathbb{G}}_a)_K.
\end{array}
\]

Let \( M \) denote the image of \( \mathbf{H}(A) \) in \( \mathbf{H}(A)_K \). It is clearly stable under \( f^* \). But also the maps \( \Phi_K \) and \( j \) are injective, by theorem 8.2 and because \( \text{Ext}^2(A, \hat{\mathbb{G}}_a) \simeq R^* \); so \( M \) agrees with the image of \( \mathbf{H}(A) \) in \( \text{Ext}^2(A, \hat{\mathbb{G}}_a) \) and is therefore finitely generated.

We can then apply lemma 9.3 and deduce \( \phi(\lambda) \in R \). This implies \( \lambda \in R \), since \( R/\pi R \) is a field and hence the Frobenius map on it is injective.

**Corollary 9.5.**

(1) The element \( \Theta_m \in \mathbf{X}_m(A)_K \) lies in \( \mathbf{X}_m(A) \).

(2) For \( n \geq m \), all the maps in the diagram

\[
\begin{array}{ccc}
\mathbf{X}_n(A)/\mathbf{X}_{n-1}(A) & \xrightarrow{\phi^*} & \mathbf{X}_{n+1}(A)/\mathbf{X}_n(A) \\
\downarrow i^* & & \downarrow i^* \\
\text{Hom}(N^n, \hat{\mathbb{G}}_a)/\text{Hom}_A(N^{n-1}, \hat{\mathbb{G}}_a) & \xrightarrow{f^*} & \text{Hom}_A(N^{n+1}, \hat{\mathbb{G}}_a)/\text{Hom}_A(N^n, \hat{\mathbb{G}}_a)
\end{array}
\]

are isomorphisms.

**Proof.** (1): By theorem 9.4, the element \( i^* \Theta_m \) of \( \text{Hom}_A(N^m, \hat{\mathbb{G}}_a)_K \) actually lies in \( \text{Hom}_A(N^m, \hat{\mathbb{G}}_a) \), and therefore by the exact sequence (7.2) we have \( \Theta_m \in \mathbf{X}_m(A) \).

(2): By proposition 6.5, we know \( f^* \) is an isomorphism.

By proposition 6.5, the maps \( i^* \) are injective for all \( n \geq m \). So to show they are isomorphisms, it is enough to show they are surjective. The \( R \)-linear generator \( \Psi_m \) of \( \text{Hom}_A(N^n, \hat{\mathbb{G}}_a)/\text{Hom}_A(N^{n-1}, \hat{\mathbb{G}}_a) \) is the image of \( \Theta_m \), which by part (1), lies in \( \mathbf{X}_m(A) \). Therefore \( i^* \) is surjective for \( n = m \). Then because \( f^* \) is an isomorphism, it follows by induction that \( i^* \) is surjective for all \( n \geq m \).

Finally, \( \phi^* \) is an isomorphism because all the other morphisms in the diagram are.

We knew before that \( i^*(\phi^*)^* \Theta_m \) agrees with \( \Psi_{m+j} \) plus lower order rational characters, but the corollary above implies that these lower order characters are in fact integral.

**Theorem 9.6.** Let \( A \) be an elliptic curve that splits at \( m \).

(1) For any \( n \geq m \), the composition

\[
\begin{array}{ccc}
\mathbf{X}_n(A) & \longrightarrow & \text{Hom}_A(N^n, \hat{\mathbb{G}}_a) \\
\downarrow & & \downarrow \\
\text{Hom}_A(N^n, \hat{\mathbb{G}}_a)/\text{Hom}_A(N^{n-1}, \hat{\mathbb{G}}_a)
\end{array}
\]

is an isomorphism of \( R \)-modules.

(2) \( \mathbf{X}_n(A) \) is freely generated as an \( R \)-module by \( \Theta_m, \ldots, (\phi^*)^{n-m} \Theta_m \).

**Proof.** (i): By corollary 9.5, the induced morphism on each graded piece is an isomorphism. It follows that the map in question is also an isomorphism.
(ii): This follows formally from (i) and the fact, which follows from 9.5, that the map (9.1) sends any $(φ^*)^j Θ_m$ to Ψₘ₊ʲ plus lower order terms. □

**Theorem 9.7.** Let $A$ be an elliptic curve that splits at $m$. Then the $R$-module $X_m(A)$ is free of rank $1$, and it freely generates $X_∞(A)$ as an $R\{φ^*\}$-module in the sense that the canonical map $R\{φ^*\} ⊗ R X_m(A) → X_∞(A)$ is an isomorphism.

**Proof.** This follows from theorem 9.6. □

9.1. The integral $F$-crystal $H(A)$ for an elliptic curve $A$. The above results show that for an elliptic curve $A$, $H(A)$ is in fact an $F$-crystal such that $H(A)_K$ is the isocrystal constructed in theorem 8.2. Indeed by theorem 9.6, we have $H(A) ≃ \left\{ \begin{array}{ll} R⟨Ψ₁⟩, & \text{if } m = 1, \\
R⟨Ψ₁, Ψ₂⟩, & \text{if } m = 2 \end{array} \right.$

We also have isomorphisms for $n ≥ m$

$R⟨Θ_m⟩ = X_{prim}(A) → X_n(A)/φ^*(X_{n-1}(A)^φ)$.

The filtration on $H(A)$ is given by $H(A) ≥ X_{prim}(A)$. The action of the semi-linear operator $f^*$ with respect to the above choice of basis of $H(A)$ is described by the matrices $Γ_0$ (in $m = 1$ case) and $Γ$ (in $m = 2$ case) as in the proof of theorem 9.4.

Therefore the characteristic polynomial of the semi-linear operator $f^*$ on $H(A)$ with respect to the same choice of basis of $H(A)$ is given by

$\text{char}(f) = \left\{ \begin{array}{ll} t - γ, & \text{if } m = 1 \\
t^2 - φ(λ)t - γ, & \text{if } m = 2 \end{array} \right.$

where $π | γ$.

Combining these, we have the following map between exact sequences of $R$-modules, as in (8.1):

$\begin{array}{ccccccc}
0 & → & X_{prim}(A) & → & H(A) & → & I(A) & → & 0 \\
\downarrow Υ & & & & & & & & \downarrow Φ \\
0 & → & \text{Lie}(A)^* & → & H_{DR}(A) & → & \text{Ext}(A, \hat{G}_a) & → & 0
\end{array}$

where $Υ$ sends $Θ_m$ to $γ/π$ (in coordinates). It follows that $Φ$ is injective if and only if $γ ≠ 0$. However, we do note that the map $Φ$ is not compatible between the two $F$-crystal structure on $H(A)$ and the crystalline structure on $H_{DR}(A)$.

**References**


*E-mail address: james.borger@anu.edu.au, arnab.saha@anu.edu.au*

*Australian National University*