p-adic Hodge Theory (Spring 2023): Week 3

Xiaorun Wu (xiaorunw@math.columbia.edu)

February 15, 2023

This week: Foundations of p-adic Hodge Theory
The goal of the next three weeks is to discuss:

1. finite flat group schemes,
2. p-divisible groups.

In particular, we will try to cover the main results of Tate's p-divisible groups [Tat67].

1 Finite flat group schemes: Basic definition and properties

The main reference for this chapter is Tate's finite flat group schemes [Tat97].

Definition 1.1. *Let S be a base scheme. An S-scheme G is a group scheme if there are maps*

1. *$m : G \times_S G \to G$ multiplication,*
2. *$e : S \to G$ unit section,*
3. *$i : G \to G$ inverse.*

satisfying the following axioms:

1. *associativity:*

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{(id,m)} & G \times G \\ \downarrow{\scriptstyle (m,id)} & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{m} & G \end{array}$$

2. *identity axiom:*

$$\begin{array}{ccc} G \times_S S \cong G & \xrightarrow{id} & G \\ & {\scriptstyle (id,e)}\searrow \quad \nearrow{\scriptstyle m} & \\ & G \times G & \end{array}$$

   and similarly for $S \times_S G \cong G$,

3. *inverse:*

$$\begin{array}{ccc} G & \xrightarrow{(id,i)} & G \times G \\ \downarrow & & \downarrow{\scriptstyle m} \\ S & \xrightarrow{e} & G \end{array}$$

Lemma 1.2. *Let G be an S-scheme. It is a group scheme if and only if $G(T)$ is a group functorial in T for all T/S.*

Proof: Yoneda's lemma.

Definition 1.3. *Let G, H be group schemes over S. A map $f : G \to H$ of S-schemes is a homomorphism if $G(T) \to H(T)$ is a group homomorphism for all T/S.*

We define $\ker(f)$ to be an S-group scheme such that

$$\ker(f)(T) = \ker(G(T) \to H(T)).$$

Equivalently, $\ker(f)$ is the fiber of the unit section.

Example 1.4. *The multiplication by n map $[n]_G : G \to G$ is defined by $g \mapsto g^n$.*

Assume $S = \operatorname{Spec}(R)$.

Definition 1.5. *Then $G = \operatorname{Spec}(A)$ is an R-group scheme if it has*

1. *$\mu : A \to A \otimes_R A$ comultiplication,*
2. *$\epsilon : A \to R$ counit,*
3. *$\iota : A \to A$ coinverse*

that correspond to multiplication, unit section, and inverse.

Example 1.6. 1. *The multiplicative group over R is*

$$\mathbb{G}_m = \operatorname{Spec}(R[t, \frac{1}{t}])$$

Then $\mathbb{G}_m(B) = B^\times$ with multiplication for any R-algebra B. Then

$$\mu(t) = t \otimes t, \epsilon(t) = 1, \iota(t) = t^{-1}$$

2. *The additive group over R is*

$$\mathbb{G}_a = \operatorname{Spec}(R[t])$$

Then $\mathbb{G}_a(B) = B$ with addition for any R-algebra B. Then

$$\mu(t) = 1 \otimes t + t \otimes 1, \epsilon(t) = 0, \iota(t) = -t.$$

3. *The nth roots of unity over R is*

$$\mu(n) = \operatorname{Spec}(R[t]/(t^n - 1)).$$

under multiplication. The functions μ, ϵ, ι are all as in 1.

4. *If R has characteristic p, we can define*

$$\alpha_p = \operatorname{Spec}(R[t]/t^p)$$

Then $\alpha_p(B) = \{b \in B | b^p = 0\}$ with addition for any R-algebra B. The functions μ, ϵ, ι are all as in (2).

5. *Let $\mathcal{A}$ be an abelian scheme over R. Then*

$$\mathcal{A}[n] = \ker([n]_{\mathcal{A}})$$

is an affine group scheme over R. This is because $[n]_{\mathcal{A}}$ is a finite morphism.

6. *Let M be a finite abstract group. We can associate to it the constant group scheme M defined by*

$$\underline{M} = \amalg_{m \in M} \operatorname{Spec}(R) \cong \operatorname{Spec}\left(\prod_{m \in M} R\right).$$

Writing $A = \prod_{m \in M} R$, note that

$$A \cong \{R - \textit{valued functions on } M\}.$$

For any R-algebra B, we have that

$$\underline{M}(B) = \{\textit{locally constant function } \operatorname{Spec}(B) \to M\}.$$

with the group structure induced by M. To describe μ, note that

$$A \otimes_R A = \{R - \textit{valued functions on} M \times M\}.$$

We have that

$$\mu(f)(m, m') = f(mm')$$
$$\epsilon(f) = f(1_M)$$
$$\iota(f)(m) = f(m^{-1}).$$

Assumption. From now on, R is a Noetherian local ring, $\mathfrak{m}$ is the maximal ideal of R, k is the residue field. The assumption R local is just for simplicity.

Definition 1.7. *Let $G = \operatorname{Spec}(A)$ be an R-group scheme. It is a (commutative) finite flat group scheme of order n if*

1. *A is a locally free R-module of rank n, A is a locally free R-module of rank n,*
2. *G is commutative, in the sense that:*

$$\begin{array}{ccc} G \times G & \xrightarrow{(x,y)\mapsto(y,x)} & G \times G \\ & {\scriptstyle m}\searrow \quad \swarrow{\scriptstyle m} & \\ & G & \end{array}$$

Remark 1.8. *(1) implies that $G \to \operatorname{Spec}(R)$ is finite and flat. (2) implies that $G(T)$ is commutative for all T over $S = \operatorname{Spec}(R)$. Note that $G(T)$ may not be of order n; for example, if $T = \operatorname{Spec}(B)$ if B is highly disconnected.*

Example 1.9.

1. *The group scheme μ_n is finite flat of order n.*
2. *If R has characteristic p, α_p is a finite flat R-group scheme of order p.*
3. *Let $\mathcal{A}$ be an abelian scheme of dimension g over R. Then $\mathcal{A}[n]$ is a finite flat group scheme of order n^{2g}.*

We will assume two theorems in this section without proof.

Theorem 1.10 (Grothendieck)**.** *Suppose G is a finite flat R-group scheme of order m and $H \subseteq G$ is a closed finite flat R-subgroup scheme of order n. Then the quotient G/H exists as a finite flat R-group scheme of order m/n.*

As a result, we have a short exact sequence

$$0 \to H \to G \to G/H \to 0$$

of R-group schemes.

Theorem 1.11 (Serre)**.** *Let G be a finite flat R-group scheme of order n. Then $[n]_G$ kills G, i.e. $[n]_G$ factors through the unit section of G.*

Remark 1.12. *This is unknown for noncommutative finite flat group schemes.*

Theorem 1.13. *Suppose G is as above. Then $G_B = G \times_R B$ for any R-algebra B is a finite-flat B-group scheme.*

Proof. If $G = \operatorname{Spec}(A)$ with μ, ϵ, ι, then $G_B = \operatorname{Spec}(A_B)$ with $\mu \otimes 1$, $\epsilon \otimes 1$, $\iota \otimes 1$. □

2 Cartier duality

Definition 2.1. *Let G be as above. The Cartier dual $G^\vee$ of G is*

$$G^\vee(B) = \operatorname{Hom}_{B-group}(G_B, (\mathbb{G}_m)_B)$$

with group structure induced by $(\mathbb{G}_m)_B$.

Using this definition, it is hard to see that $G^\vee$ is a finite flat group scheme. We will describe it differently soon which will make this apparent.

Remark 2.2. *We could have defined $G^\vee = \operatorname{Hom}(G, \mathbb{G}_m)$, where the sheaf* Hom *is on the big fppf site.*

Lemma 2.3. *If $[n]_G$ kills G, then*

$$G^\vee(B) = \operatorname{Hom}_{B-group}(G_B, (\mu_n)_B).$$

Proof. Recall that $\mu_n = \ker([n]_{\mathbb{G}_m})$. □

Theorem 2.4 (Cartier duality)**.** *Let $G = \mathrm{Spec}(A)$ be an R-group scheme of order n with μ, ϵ, ι as comultiplication, counit, coinverse. Define*

$$m_A : A \otimes_R A \to A \quad \textit{right multiplication,}$$

$$p : R \to A \quad \textit{structure morphism,}$$
$$A^\vee = \mathrm{Hom}_{R-mod}(A, R).$$

Then:

1. *the maps $\mu^\vee$ and $\epsilon^\vee$ given an R-algebra structure on $A^\vee$,*
2. *$G^\vee \cong \mathrm{Spec}(A^\vee)$ with $m_A^\vee, p^\vee, \iota^\vee$ as comultiplication, count, coinverse,*
3. *$G^\vee$ is a finite flat R-group scheme of order n,*
4. *$(G^\vee)^\vee \cong G$ canonically.*

Proof. Part (1) is straightforward. Parts (3) and (4) are consequences of (2). It suffices to prove (2) but we will do this next time. □

Example 2.5. 1. *We have that $\mu_n^\vee \cong \underline{\mathbb{Z}/n\mathbb{Z}}$.*

2. *We have that $\alpha_p^\vee \cong \alpha_p$.*

As a consequence, we have the following result.

Proposition 2.6. *Suppose $R = k$ is a field. Let $f : A \to B$ be an isogeny between abelian varieties over k. Then*
$$\ker(f)^\vee \cong \ker(f^\vee).$$

We shall omit the proof here (but for reference see Serin Hong's notes).

Corollary 2.7. *Let $R = k$ be a field. Then $A[n]^\vee \cong A6 \vee [n]$. This gives*

$$A[n] \times A^\vee[n] \mapsto \mu_N,$$

called the Weil pairing.

Later, we will use a pairing
$$T_p(A) \times T_p(A^\vee) \to \mu_{p^\infty} \cong \mathbb{Z}_p(1)$$
obtained from the above corollary.

Proof of Cartier duality theorem 2.4. Let $G = \mathrm{Spec}(A)$ and μ, ϵ, ι be the comultiplication, counit, and coinverse.

Let $p : R \to A$ be the structure morphism, $m_A : A \otimes_R A \to A$ be the right multiplication. Consider

$$A^\vee = \mathrm{Hom}_R(A, R)$$

with R-algebra structure given by $\mu^\vee$ and $\epsilon^\vee$. Consider

$$G^\nabla = \mathrm{Spec}(A^\vee)$$

with $m_A^\vee$, $p^\vee$, $\iota^\vee$ as comultiplication, counit, and coninverse. We want to show that

$$G^\vee(B) \cong G^\nabla(B)$$

for all R-algebra B. We have that:

$$\begin{aligned} G^\vee(B) &\cong \mathrm{Hom}_{\mathrm{grp}}(G_B, (\mathbb{G}_m)_B) \\ &= \left\{ f \in \mathrm{Hom}_{B\text{-alg}}(B[t, t^{-1}], A_B) \;\middle|\; \begin{smallmatrix} \mu_B(f(t)) = f(t) \otimes f(t), \\ \epsilon_B(f(t)) = 1, \\ \iota_B(f(t)) = f(t)^{-1} \end{smallmatrix} \right\} \\ &= \left\{ u \in A_B^\times \;\middle|\; \begin{smallmatrix} \mu(u) = u \otimes u, \\ \epsilon(u) = 1, \\ \iota(u) = u^{-1} \end{smallmatrix} \right\} && \text{via } f \mapsto f(t) \\ &= \{ u \in A_B^\times \mid \mu(u) = u \otimes u \}, \end{aligned}$$

where the last equality follows from

$$(id_B \otimes \epsilon_B) \circ \mu_B = id_B,$$

$$(id_B \otimes \iota) \circ \mu_B = p_B \circ \epsilon_B.$$

Now, the right hand side of equation 2 is

$$\begin{aligned} G^{\nabla}(B) &= \mathrm{Hom}_{R\text{-alg}}(A^\vee, B) \\ &= \mathrm{Hom}_{B\text{-alg}}(A^\vee \otimes B, B) \\ &= \{f \in \mathrm{Hom}_{B\text{-mod}}(B, A_B) \mid \text{compatible with } m_B^\vee, p_B^\vee, \mu_B, \epsilon_B\} \\ &= \{u \in A_B^\times \mid \mu_B(u) = u \otimes u,\ \epsilon_B(u) = 1\} \\ &= \{u \in A_B^\times \mid \mu(u) = u \otimes u\}. \end{aligned}$$

This completes the proof if we check that the isomorphism respects the group structure. □

Lemma 2.8. *Suppose $f : H \hookrightarrow G$ is a closed embedding of finite flat R-groups. Then*

$$\ker(f)^\vee \cong (G/H)^\vee.$$

Proof. We have that

$$\begin{aligned} \ker(f)^\vee(B) &= \ker(\mathrm{Hom}(G_B, \mathbb{G}_{m,B}) \xrightarrow{f} \mathrm{Hom}(H_B, \mathbb{G}_{m,B})) \\ &= \mathrm{Hom}((G/H)_B, \mathbb{G}_{m,B}) \\ &= (G/H)^\vee(B), \end{aligned}$$

as required. □

Proposition 2.9. *Taking the Cartier dual is an exact functor.*

Proof. We want to show that if

$$0 \to G' \xrightarrow{f} G \xrightarrow{g} G'' \to 0,$$

then

$$0 \to (G'')^\vee \xrightarrow{g^\vee} G^\vee \xrightarrow{f^\vee} (G')^\vee \to 0$$

is exact. Injectivity of $g^\vee$ is easy to check, since $\ker(f^\vee) \cong (G'')^\vee$.

To check that $f^\vee$ is surjective, note that $f^\vee : G^\vee \to (G')^\vee$ induces

$$G^\vee/(G'')^\vee \to (G')^\vee.$$

Its dual is

$$(G')^{\vee\vee} \to (G^\vee/(G'')^\vee)^\vee \cong \ker(g^{\vee\vee}) = \ker(g) = G',$$

which is an isomorphism. □

3 Finite étale group schemes

Proposition 3.1. *For R is Henselian, we have that:*

$$\{\textit{finite étale group over } R\} \leftrightarrow \{\textit{finite abelian groups with a continuous } \Gamma_K\textit{-action}\}$$

$$G \mapsto G(\overline{k}).$$

Proof. Consider $\overline{m} : \mathrm{Spec}(\overline{k}) \to R$, a geometric point. Then

$$\pi_1(\mathrm{Spec}(R), \overline{m}) \cong \Gamma_k.$$

Hence

$$\{\text{finite étale group over } R\} \leftrightarrow \{\text{finite sets with a continuous } \Gamma_K\text{-action}\}$$

Passing to group objects gives the result. □

Remark 3.2. *1. This bijection is compatible with the order on each side.*

2. If $k = \overline{k}$, we have that $\Gamma_k = 1$.

Definition 3.3. *Let $G = \mathrm{Spec}(A)$. Then augmentation ideal is $I = \ker(\epsilon)$.*

Lemma 3.4. *As R-modules, $A \cong R \oplus I$.*

Proof. The structure morphism $R \to A$ splits the short exact sequence:

$$0 \to I \to A \xrightarrow{\epsilon} R \to 0,$$

giving the desired isomorphism. □

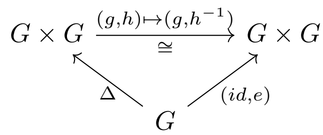
Proposition 3.5. *Let $G = \mathrm{Spec}(A)$ and I be the augmentation ideal. Then*

$$\Omega_{A/R} \cong I/I^2 \otimes_R A,$$

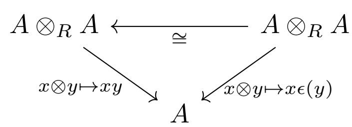
$$I/I^2 \cong \Omega_{A/R} \otimes_A A/I.$$

Remark 3.6. *The multiplication on G defines an action on $\Omega_{A/R}$. The invariant forms under the G-action are determined by the values along the unit section. Any other form is an invariant form times a form on A.*

Proof. We have the commutative diagram:



which corresponds to the commutative diagram



Let J be the kernel of the left map. Then $\Omega_{A/R} = J/J^2$ by definition. The kernel of the right hand side map is $J = A \otimes_R I$ since

$$A \otimes_R A \cong (A \otimes_R R) \oplus (A \otimes_R I)$$

and $I = \ker(\epsilon)$. Hence

$$J^2 = (A \otimes_R I)^2 = A \otimes_R I^2,$$

and so

$$J/J^2 = (A \otimes I)/(A \otimes I^2) \cong A \otimes_R I/I^2$$

showing that

$$\Omega_{A/R} \otimes_A A/I = (I/I^2 \otimes_R A) \otimes A/I = (I/I^2) \otimes_R A/I \cong I/I^2.$$

This gives the result. □

Corollary 3.7. *Let $G = \mathrm{Spec}(A)$ be a finite flat R-group scheme. Then G is étale if and only if $I = I^2$.*

Proposition 3.8. *Every constant group scheme is étale*

Proof. If $A = \prod_{m \in M} R$, then $I = \prod_{m \in id_M} R$, so that $I = I^2$. □

Corollary 3.9. *Let $R = k = \overline{k}$ be a field of characteristic p. Then $\underline{\mathbb{Z}/p\mathbb{Z}}$ is the unique finite étale k-group scheme of order p. In particular, $\mathbb{Z}/p\mathbb{Z}, \mu_p, \alpha_p$ are mutually non-isomorphic as finite flat groups of order p.*

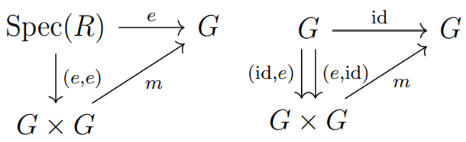
Proposition 3.10. *Let $G = \mathrm{Spec}(A)$ be a finite flat R-group scheme. Then G is étale if and only if the image of the unit section is open. Moreover, if the order of G is invertible in R, then G is étale.*

Proof. We have $\epsilon : \mathrm{Spec}(R) \to \mathrm{Spec}(A)$. The image of the unit section is $\mathrm{Spec}(A/I)$ which is open if and only if $I = I^2$. □

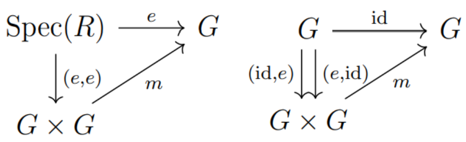
Proposition 3.11. *Let $G = \mathrm{Spec}(A)$ be a finite flat R-group scheme. If the order G is invertible in R, then G is étale.*

Corollary 3.12. *Every finite flat group scheme over a field of characteristic 0 is étale.*

Proof of proposition 3.11. Let n be the order of G. We claim that $[n]_G$ induces multiplication by n on I/I^2. We have the diagrams



which corresponds to



For all $x \in I$, $\epsilon \otimes \epsilon(\mu(x)) = 0$.

Since $A \cong R \oplus I$, we have that

$$A \otimes A \cong R \otimes R \oplus R \otimes I \oplus I \otimes R \oplus I \otimes I,$$

so

$$\mu(x) = a \otimes 1 + 1 \otimes b + I \otimes I$$

for $a, b \in I$. For $x = a = b$, we get

$$\mu(x) = 1 \otimes x + x \otimes 1 + I \otimes I$$

for all $x \in I$. Hence μ acts as $1 \otimes x + x \otimes 1$ on I/I^2. By induction, the assertion follows (indeed, $[n] = m \circ ([n-1], id)$ and we can run a similar argument).

We know that $[n]$ kills G by Serre's Theorem (Recall in the remark). Hence $[n]$ factors as follows:

$$[n] : G \to R \xrightarrow{e} G.$$

This gives

$$\Omega_{A/R} \to \Omega_{R/R} = 0 \to \Omega_{A/R},$$

so the induced map on $\Omega_{A/R}$ is 0. Thus $[n]_G$ induces the zero map on

$$\Omega_{A/R} \otimes_A A/I \cong I/I^2.$$

As n is invertible, multiplication by n on I/I^2 should be an isomorphism. □

Recall Serre's theorem:

Theorem 3.13 (Serre)**.** *Let G be a finite flat R-group scheme of order n. Then $[n]_G$ kills G, i.e. $[n]_G$ factors through the unit section of G.*

4 The connected étale sequence

Let R be a Henselian local ring with residue field k.

Lemma 4.1. *An R-group G is étale if and only if G_k is étale.*

Proof. Étaleness is a fiberwise property. □

Lemma 4.2. *Let $T = \mathrm{Spec}(B)$ be a finite scheme over R. The following are equivalent*

1. *T is connected,*
2. *B is a henselian local finite R-algebra,*
3. *Γ_k acts transitively on $T(\overline{k})$.*

Proof. Clearly, (2) implies (1), because local implies connected. For (1) implies (2), suppose $B = \prod B_i$ for henselian local finite R-algebras. Then $\mathrm{Spec}(B_i)$ is a connected component of $\mathrm{Spec}(B)$. To show that (1) is equivalent to (3), let k_i be the residue field of B_i. Then

$$T(\overline{k}) = \mathrm{Hom}_{R\text{-alg}}(B, \overline{k}) = \amalg \mathrm{Hom}_k(k_i, \overline{k}),$$

and $\mathrm{Hom}(k_i, \overline{k})$ is a Γ_k-orbit. ☐

Proposition 4.3. *Let $G = \mathrm{Spec}(A)$ and G^0 be a connected component of the unit section. Then $G^0(\overline{k}) = 0$.*

Proof. Let $G^0 = \mathrm{Spec}(A^0)$. Then A^0 is a henselian local finite R-algebra. We get a surjective homomorphism $A^0 \to R$. The residue field of A^0 is k. Then $G^0(\overline{k}) = \mathrm{Hom}_k(k, \overline{k}) = 0$. ☐

Theorem 4.4 (Connected–étale sequence)**.** *Let $G = \mathrm{Spec}(A)$ be a finite-flat R-group scheme. Then G^0 is a closed subgroup of G $G^{ét} = G/G^0$ is a finite étale group over R. We have a short exact sequence*

$$0 \to G^0 \to G \to G^{ét} \to 0.$$

Proof. We have that $G^0 \times G^0$ is connected, since

$$(G^0 \times G^0)(\overline{k}) = G^0(\overline{k}) \times G^0(\overline{k}) = 0.$$

We hence have that $m(G^0 \times G^0) \subseteq G^0$ and $\iota(G^0) \subseteq G^0$, so G^0 is a closed subgroup. The unit section of $G^{\text{ét}}$ is G^0/G^0 which is open, since G^0 is open in G. ☐

Corollary 4.5. *A finite flat group scheme G is connected if and only $G(\overline{k}) = 0$.*

Corollary 4.6. *A finite flat group scheme G is étale if and only if $G^0 = 0$.*

Corollary 4.7. *If $f : G \to H$ is a group homomorphism with H is étale, then f uniquely factors through $G^{ét}$.*

Proof. We have that $f(G^0) \subseteq H^0 = 0$, so we get the result using the universal property of $G^{\text{ét}}$. ☐

Proposition 4.8. *Let $R = k = \overline{k}$ be a field. Then the connected–étale sequence splits. (This is also true if $R = k$ is a perfect field.)*

Proof. We want to show that there is a section of $G \twoheadrightarrow G^{\text{ét}}$. Consider

$$G^{\text{red}} = \mathrm{Spec}(A/\mathfrak{n})$$

☐

where n is the nilradical of A. We claim that G^{red} is a subgroup of G. Since a product of reduces schemes is reduced, $G^{red} \times G^{red}$ is reduced. Hence

$$m(G^{red} \times G^{red}) \subseteq G^{red}, \quad \iota(G^{red}) \subseteq G^{red}.$$

Moreover, G^{red} is étale because it is finite and reduced over k.
It suffices to show that the map $G \twoheadrightarrow G^{\text{ét}}$ induces $G^{red} \cong G^{\text{ét}}$. Since k is reduced, $G^{red}(k) = G(k)$ and we also know that $G(k) = G^{\text{ét}}(k)$.

Example 4.9. *Consider an elliptic curve E over $\overline{\mathbb{F}}_p$. We have a connected–étale sequence for the p-torsion:*

$$0 \to E[p]^0 \to E[p] \to E[p]^{ét} \to 0.$$

We know that $E[p](\overline{\mathbb{F}}_p)$ has order 1 or p. Hence $E[p]^{ét}(\overline{\mathbb{F}}_p)$ has order p if E is ordinary of 1 if E is supersingular. Assume E is ordinary. Hence $E[p]$ ét is étale of order p. By corollary 3.9, we have

$$E[p]^{ét} \cong \underline{\mathbb{Z}/p\mathbb{Z}}.$$

Moreover,

$$(E[p]^{ét})^\vee \cong (\underline{\mathbb{Z}/p\mathbb{Z}})^\vee \cong \mu_p \hookrightarrow E[p]^\vee = E^\vee[p] \cong E[p].$$

Since μ_p is connected, $\mu_p \hookrightarrow E[p]^0$, so $\mu_p \cong E[p]^0$. Hence the connected-étale sequence is

$$0 \to \mu_p \to E[p] \to \underline{\mathbb{Z}/p\mathbb{Z}} \to 0.$$

By proposition 4.8,

$$E[p] \cong \mu_p \times \underline{\mathbb{Z}/p\mathbb{Z}}.$$

Remark 4.10. *If E is supersingular, we know that $E[p]^{ét}$ is trivial. Then $E[p]$ is self-dual and we have a short exact sequence:*

$$0 \to \alpha_p \to E[p] \to \alpha_p \to 0.$$