Workshop on group schemes and $p$-divisible groups: Homework 4.

1. Let $A$ be an abelian variety over a field $k$ with characteristic $p > 0$ and dimension $g > 0$. Use the fact that $A$ and $A'$ are isogenous to prove that the étale part of $A[p^\infty]$ has height at most $\dim A$, and that equality holds if and only if $A[\ell]$ has no $\alpha_p$ subgroups. In this case, prove that $A[p^\infty](\overline{k}) \cong \mu_{p^{\infty}}^g$. Such abelian varieties are called ordinary. (It is a hard theorem of Norman and Oort that in moduli schemes of polarized abelian varieties (with étale level structure) in characteristic $p$, the locus of ordinary abelian varieties is a Zariski-dense open set.)

2. Let $k$ be an algebraically closed field of characteristic $p > 0$. Using Dieudonné theory, construct a local-local height-$2g$ $p$-divisible group over $k$ with dimension $g$ such that it is not isogenous to its dual, and so cannot arise as the $p$-divisible group of an abelian variety over $k$. (One cannot do this unless $g \geq 4$.)

3. Prove that over a local noetherian ring $R$ with residue characteristic $p > 0$, there are no nonzero maps from an étale $p$-divisible to a connected one. (Hint: Pass to an algebraically closed residue field and use the Serre–Tate equivalence.) Give a counterexample if the noetherian condition is dropped or if we work with finite flat commutative group schemes.

4. We work with abelian varieties over a field $k$.
   (i) Prove that a complex of abelian varieties
   \[ 0 \to A' \to A \to A'' \to 0 \]
   is a short exact sequence of $k$-groups if and only if the induced complex of $\ell$-divisible groups
   \[ 0 \to A'[\ell^\infty] \to A[\ell^\infty] \to A''[\ell^\infty] \to 0 \]
   is short exact for all primes $\ell$. How can these latter conditions be encoded in terms of Tate or Dieudonné modules over an algebraic closure of $k$, and what happens if we work with just a single prime $\ell$?
   (ii) Prove that $f : A' \to A$ is a closed immersion if and only if $f^\vee$ is faithfully flat and has connected kernel, and that $f$ has finite kernel if and only if $f^\vee$ is faithfully flat.
   (iv) Generalize these results to abelian schemes by applying the above results on fibers.

5. Let $k'/k$ be a finite separable extension of fields, and let $X'$ be a $k'$-scheme of finite type.
   (i) Define the Weil restriction of scalars functor $R_{k'/k}(X')$ on $k$-schemes to be $T \mapsto X'(k' \otimes_k T)$. Prove that this functor is representable when $X'$ is an affine space over $k'$.
   (ii) Study the behavior of $R_{k'/k}$ with respect to open immersions, closed immersions, and fiber products in $X'$, and deduce that $R_{k'/k}(X')$ is always represented by a $k$-scheme of finite type and that it is a $k$-group if $X'$ is a $k'$-group.
   (iii) If $K/k$ splits $k'/k$, construct a $K$-isomorphism $K \otimes_k R_{k'/k}(X') \cong \prod_{\sigma' : K' \to K} \sigma'(X')$, where the product is taken over $k$-embeddings. Deduce that $R_{k'/k}(X')$ is geometrically connected (resp. separated, proper, geometrically smooth, projective) over $k'$ if $X'$ is so over $k'$.
   (iv) If $X'$ is a $k'$-group of finite type, identify $T_e(R_{k'/k}(X'))$ with the $k$-vector space underlying $T_e(X')$. Conclude that if $X'$ is an abelian variety of dimension $d'$, then $R_{k'/k}(X')$ is an abelian variety of dimension $[k' : k]d'$. Describe how $R_{k'/k}$ behaves on torsion subschemes, Tate modules, and Dieudonné modules. What if $k'/k$ is finite and inseparable?

The next three exercises lead to a proof of a special case of the Oort–Tate classification of group schemes of prime order. The general case is worked out in the paper *Group schemes of prime order* by Oort and Tate.
6. Let $R$ be a commutative ring. We shall work below with group schemes over $R$, including the so-called split torus $G_m$ and the additive group $G_a$.

(i) Choose $\lambda \in R$. Define $A^\lambda := R\left[x, \frac{1}{1 + \lambda x}\right]$ and $G^\lambda := \text{Spec}(A^\lambda)$ with the comultiplication defined by $x \mapsto x \otimes 1 + 1 \otimes x + \lambda x \otimes x$, coinverse defined by $x \mapsto 1 - \frac{x}{1 + \lambda x}$ and counit defined by $x \mapsto 0$. Verify that $G^\lambda$ is a commutative and flat $S$-group with smooth geometric fibers. Verify that it coincides with $G_a$ if $\lambda = 0$.

(ii) Verify that the map $\eta_\lambda : G^\lambda \to G_m$ given by $z \mapsto 1 + \lambda x$ defines a homomorphism of group schemes. Show that it is an isomorphism if and only if $\lambda$ is a unit. Find the kernel. Is it a finite group scheme over $R$? Is it flat over $R$?

7. Assume that $\lambda$ is not a zero divisor in $R$ and that $p \in \lambda^{p^{n-1}(p-1)}R$, where $p > 0$ is a rational prime.

(i) Show that the map $\varphi_{\lambda, n} : G^\lambda \to G^\lambda[p^n]$ given by $x \mapsto \frac{(1 + \lambda x)^{p^n} - 1}{p^n}$ is a well-defined homomorphism of group schemes over $R$. [The formula means the following: writing $p = \lambda^{p^{n-1}(p-1)}r$, each coefficient of the polynomial $(1 + \lambda x)^{p^n} - 1$ in $x$ is of the form $p\lambda^{p^n}v$ for some $v \in R$ depending on the coefficient, and then $\frac{p\lambda^{p^n}v}{p^n}$ means $vR$.]

(ii) Show that $\varphi_{\lambda, n}$ is surjective for the fpqc topology and that the kernel, denoted by $G_{\lambda, n}$, is a finite locally free commutative $R$-group of order $p^n$. Deduce that $G^\lambda[p^n]$ coincides with the quotient of $G^\lambda$ by $G_{\lambda, n}$.

(iii) Verify that $\eta_{\lambda p^n} \circ \varphi_{\lambda, n} = [p^n] \circ \eta_\lambda$ where $[p^n]$ is multiplication by $p^n$ on $G_m$. Deduce that $\eta_\lambda(G_{\lambda, n}) \subset \mu_{p^n}$ and that, if $\lambda$ is a unit, $G_{\lambda, n} \simeq \mu_{p^n}$.

(iv) Let $R \to k$ be a ring map killing $\lambda$, with $k$ a field of characteristic $p$. Show that if $\lambda^{p^{n-1}(p-1)} \not\in pR$ then $G_{\lambda, n} \otimes_R k \simeq \alpha_{p^n}$, while if $\lambda^{p^{n-1}(p-1)} \in pR$ then $G_{\lambda, n} \otimes_R k \simeq \alpha_{p^{n-1}} \times \mathbb{Z}/p\mathbb{Z}$.

8. The aim of this exercise is to prove the following. Let $R$ be a discrete valuation ring with fraction field $K$ of characteristic 0. Let $H$ be a finite flat commutative group scheme over $\text{Spec}(R)$ of order $p$. Then, there exists a flat extension of discrete valuation rings $R \subset R'$ of degree $\leq p-1$ and there exists $\lambda \in R'$ such that the base change $H_{R'}$ of $H$ to $\text{Spec}(R')$ is isomorphic to the group scheme $G_{\lambda, 1}$ defined over $R'$.

Let $H := \text{Spec}(B)$, let $I$ be the augmentation ideal of $B$. It is a free $R$-module of rank $p-1$. Fix a basis $\{x_1, \ldots, x_{p-1}\}$. Recall that $B^\times := \text{Hom}(B, R)$ is naturally endowed with the structure of commutative Hopf algebra. The group scheme $H^\times := \text{Spec}(B^\times)$ represents the fpqc sheaf $S \rightsquigarrow \text{Hom}_S(H, G_m)$. Define $R'$ as the normalization of $R$ in the composite of the factor fields of the finite étale $K$-algebra $B^\times \otimes_R K$. The identity map $H^\times \to H^\times$ defines a map $H \times_R H^\times \to G_m \times_R H^\times$ as group schemes over $H^\times$ (i.e., a homomorphism $B^\times[z, z^{-1}] \to B^\times \otimes_R B$ of $B^\times$-Hopf algebras). Base changing by $B^\times \to R'$ defines a homomorphism $\rho : R'[z, z^{-1}] \to R' \otimes_R B$ of $R'$-Hopf algebras. Write $\rho(z) - 1 := \sum_1^p \lambda_i \otimes x_i$ and let $\lambda$ be a generator of the ideal $(\lambda_1, \ldots, \lambda_{p-1})$ of the discrete valuation ring $R'$.

(i) Show that the map $\gamma : H_{R'} \to G^\lambda$ given by $x \mapsto \frac{\rho(z) - 1}{\lambda}$ is a non-trivial homomorphism of group schemes. From the fact that $\rho$ factors via $\mu_p$ and from Exercise 7(iii) deduce that $\gamma$ factors via $G_{\lambda, 1}$.

(ii) Prove that the kernel of $\gamma : H_{R'} \to G_{\lambda, 1}$ is trivial. (Hint: by Nakayama’s lemma and since kernels commute with base change it suffices to prove that the base change $\gamma_{R'}$ of $\gamma$ to the residue field $k'$ of $R'$ has trivial kernel).

(iii) Deducce that $\gamma : H_{R'} \to G_{\lambda, 1}$ is an isomorphism.
9. The aim of this exercise is two-fold: to give a conceptual proof of the Nagell–Lutz theorem describing torsion on certain Weierstrass models over $\mathbb{Z}$, and to give a sufficient $j$-invariant criterion for certain ordinary elliptic curves in characteristic $p > 0$ to have no nonzero $p$-torsion rational over the base field. It is assumed that you know the definition of a Néron model.

Let $R$ be a discrete valuation ring with fraction field $K$ and residue characteristic $p \geq 0$. Let $E$ be an elliptic curve over $K$ and $P \in E(K)$ a nonzero torsion point.

(i) If there exists a Weierstrass model of $E$ over $R$ such that one of the affine coordinates of $P$ does not lie in $R$, then prove that the scheme-theoretic closure of $\langle P \rangle \subseteq E(K)$ in the Néron model of $E$ is a finite flat local $R$-group. In particular, if $p > 0$ then $P$ has $p$-power order. (Hint: to prove that the quasi-finite flat closure is finite, note that it is separated and express it as an image of something $R$-proper, even $R$-finite.)

(ii) Under the assumptions in (i), if $K$ also has characteristic $p > 0$ deduce that $E$ has potentially supersingular reduction over $R$ and that $j(E) \in K$ is a $p$th power. In particular, if $j(E) \in K$ is not a $p$th power then no such $P$ exists.

(iii) By the Oort–Tate classification, the only example of a non-trivial finite flat local commutative group scheme over the maximal unramified extension of $\mathbb{Z}_p$ with $p$-power order and cyclic constant generic fiber is for $p = 2$ and the group scheme $\mu_2$. Deduce the classical Nagell-Lutz theorem: non-trivial torsion $\mathbb{Q}$-points on Weierstrass $\mathbb{Z}$-models of the form $y^2 = f(x)$ with monic cubic $f \in \mathbb{Z}[x]$ (for which nonzero 2-torsion has the form $(x_0, 0)$ with $x_0 \in \mathbb{Z}$) must be $\mathbb{Z}$-points in the affine plane.