Workshop on group schemes and p-divisible groups: Homework 2.

1. (*i*) Using the structure theorem and Frobenius morphisms, prove that a finite group scheme over a field is killed by its order. (Exer. 3(*ii*) in HW1 gives a non-commutative group of order p^2.)

(*ii*) On the bus to the Belgian army in 1969, Deligne proved that any *commutative* finite locally free group scheme is killed by its order. Show how to reduce the general (non-commutative and unsolved) case to that of an artin local base ring with algebraically closed residue field.

(*iii*) If G is a group scheme locally of finite type over a field k, prove that the tangent map

$$dm(e,e) : \mathrm{T}_e(G) \times \mathrm{T}_e(G) \simeq \mathrm{T}_{(e,e)}(G \times G) \to \mathrm{T}_e(G)$$

is ordinary addition, and deduce that if G is a finite k-group killed by a nonzero integer N not divisible by $\mathrm{char}(k)$ then G is étale.

2. (*i*) Prove Serre's trick: if $X \times_S Y$ is S-flat and $X(S) \neq \emptyset$ then Y is S-flat.

(*ii*) Use (*i*) to prove that if $A = A_1 \times A_2$ is a product of rings and G is a finite locally free A-module scheme over S then the functorial decomposition $G(T) = G_1(T) \times G_2(T)$ according to the decomposition of A has G_1 and G_2 each represented by finite locally free closed A-submodule schemes of G. Deduce "primary decomposition" for finite locally free commutative group schemes killed by a nonzero integer.

3. Let S be an $\mathbf{F}_p$-scheme and X an S-scheme.

(*i*) Prove that $F_{X/S}$ is natural in X and that its formation commutes with base change on S and products in X (over S). Deduce that if X is an S-group then $F_{X/S}$ is an S-group map (where $X^{(p)}$ is made into an S-group via base change).

(*ii*) Assume $S = \mathrm{Spec}(k)$ for a finite field k of size p^n. Prove that $F_{X/S,n} = F_X^n$, and for any k-algebra A describe $F_{X/S,n} : X(A) \to X(A)$ in terms of a functorial operation on A.

4. Let R be a commutative ring and $u \in R^\times$ with $u^i - 1 \in R^\times$ for all $0 < i < N$. For any R-algebra A, define $\mathrm{KM}_{u,N}(A)$ to be the set of $a \in A^\times$ such that $a^N = u^i$ with $i : \mathrm{Spec}\, A \to \{0, \dots, N-1\}$ a locally constant function. (Such an i is unique if it exists.)

(*i*) Define a composition law on $\mathrm{KM}_{u,N}(A)$ by the rule $a \cdot a' = aa'$ if $a^N = u^i$ and $a'^N = u^j$ with $i + j < N$ and $a \cdot a' = aa'/u$ otherwise. Prove that this is a commutative N-torsion group structure that is functorial in A.

(*ii*) Prove that $\mathrm{KM}_{u,N}$ is represented by a finite locally free commutative R-group of order N^2, and that it naturally sits in a short exact sequence $0 \to \mu_N \to \mathrm{KM}_{u,N} \to \mathbf{Z}/N\mathbf{Z} \to 0$.

(*iii*) Give an example of a commutative finite flat group scheme over $\mathbf{Z}_p$ whose connected-étale sequence is non-split.

(*iv*) Compute the Cartier dual of $\mathrm{KM}_{u,N}$.

5. Let k be a perfect field of characteristic $p > 0$.

(*i*) Compute the Dieudonné modules of α_{p^n}, $\mathbf{Z}/p^n\mathbf{Z}$, and μ_{p^n} for all $n \geq 1$.

(*ii*) Prove that if H_1 is the p-torsion of a p-divisible group over k, then the complex

$$0 \to H_1[F] \to H_1 \xrightarrow{F} H_1^{(p)}[V] \to 0$$

is a short exact sequence. (Hint: Use Dieudonné modules.)

(*iii*) Prove that if k is algebraically closed, then there are exactly 4 isomorphism classes of local-local p-torsion commutative k-groups of order p^2: $\alpha_p \times \alpha_p$, α_{p^2}, $\alpha_{p^2}^\vee$, and $E[p]$ for a supersingular elliptic curve E over k. What are the Cartier duals of these?

6. Let R be a Dedekind domain with fraction field K, X a finite flat R-scheme.

(i) Define a natural inclusion-preserving bijection between the set of closed subschemes of X_K and the set of R-flat closed subschemes of X via the inverse operations of scheme-theoretic closure and passage to the K-fiber. If X_K is étale, deduce that there are finitely many R-flat closed subschemes of X. What if X_K is not étale?

(ii) Let X' be a second such R-scheme and $f : X' \to X$ an R-map. If $Z \subseteq X$ and $Z' \subseteq X'$ are R-flat closed subschemes prove that $f|_{Z'}$ factors through Z if and only if $f_K|_{Z'_K}$ factors through Z_K. If X is an R-group then relate K-subgroups of X_K and flat closed R-subgroups of X.

(iii) Generalize to separated R-schemes X, using flat closed subschemes (resp. flat closed subgroups), and give a counterexample if separatedness is not assumed.

(iv) Assume R is a discrete valuation ring with residue characteristic $p > 0$, and that E is an elliptic curve over K with multiplicative reduction. The smooth locus of a minimal Weierstrass model for E over R is a flat separated R-group $\mathscr{E}$ with geometric closed fiber $\mathbf{G}_m$. Use the fibral flatness criterion to prove that the quasi-finite map $p : \mathscr{E} \to \mathscr{E}$ is flat, and deduce that $\mathscr{E}[p]$ is a quasi-finite flat closed R-subgroup of $\mathscr{E}$ with K-fiber $E[p]$. Prove that $\mathscr{E}[p]$ is *not* finite over R.

7. Let R be a Dedekind domain of generic characteristic 0, and let $G_\eta = \mathrm{Spec}(A)$ be a finite commutative group scheme over its fraction field K.

(i) An *R-model* for G_η is a finite flat R-group scheme whose K-fiber is equipped with an isomorphism to G_η. Prove that the isomorphism classes of R-models for G_η are in bijective correspondence with finite flat R-subalgebras of A that are "stable under the Hopf structure".

(ii) Since the Cartier dual algebra $A^\vee$ is K-étale, the normalization of R in this algebra is an R-lattice $L^\vee$ in $A^\vee$. Let $L \subseteq A$ be the dual R-lattice. Prove that L is contained in the normalization $\widetilde{A}$ of R in A, and use the K-étaleness of A and $A^\vee$ to deduce that there are only finitely many R-models for G_η. Is this finiteness true if $\mathrm{char}(K) = p > 0$ and A is K-étale with p-power order?

8. If $0 \to G' \to G \to G'' \to 0$ is a short exact sequence of finite locally free commutative group schemes over R then prove $\mathrm{disc}(G) = \mathrm{disc}(G')^{|G''|}\mathrm{disc}(G'')^{|G'|}$ as ideals in R.

9. Let X be a flat scheme locally of finite type over a complete local noetherian ring R with residue field k. Let $x \in X(R)$ be a section.

(i) If X has smooth geometric closed fiber, prove that $\mathscr{O}^\wedge_{X,x_0}$ (x_0 the closed point of the section) is isomorphic to a formal power series ring over R in finitely many variables.

(ii) Prove a version of Yoneda's lemma for complete local noetherian R-algebras as covariant functors on the category of *artinian* finite local R-algebras. Such functors are called *pro-representable*.

(iii) If X is an R-group, show that the functor pro-represented by $\mathscr{O}^\wedge_{X,x_0}$ is naturally a group functor. In the setting in (i), construct a formal Lie group structure on $\mathscr{O}^\wedge_{X,x_0}$ over R.

10. In HW1 we saw how to functorially view S-schemes as "sheaves" with respect to the Zariski topology and also with respect to *fpqc* (*fidèlement plat quasi-compact*, or faithfully flat and quasi-compact) coverings of S-schemes: a contravariant set-valued functor F on the category of S-schemes is an *fpqc* sheaf if it restricts to a sheaf on the Zariski topology of every S-scheme and if for any *fpqc* morphism $X' \to X$ over S the map $F(X) \to F(X')$ is an injection onto the subset of elements with the same image under the two maps $F(X') \rightrightarrows F(X' \times_X X')$. Note that such functors are also sheaves with respect to *fppf* coverings (*fidèlement plat de présentation finie*, or faithfully flat and locally finitely presented) since *fppf* coverings admit *fpqc* refinements Zariski-locally on the target.

(i) Let $G = \{G_n\}$ be a p-divisible group over a scheme S. For any affine scheme $\mathrm{Spec}\, A$ over S, define $\underline{G}(A) = \varinjlim G_n(A)$. Prove that this satisfies the sheaf axioms for the Zariski topology on affine schemes, use this to define $\underline{G}(X)$ as a contravariant functor in S-schemes X, and check $\underline{G}(X)[p^n] = G_n(X)$ compatibly with change in $n \geq 1$.

(ii) Prove that the group functor on S-schemes built in (i) satisfies the *fpqc* covering condition, and that $p : \underline{G} \to \underline{G}$ is a surjection of *fppf* sheaves in the sense that for any $\gamma \in \underline{G}(X)$ there exists a Zariski covering $\{X_i\}$ of X and faithfully flat finitely presented maps $X_i' \to X_i$ such that the pullback of γ into $\underline{G}(X_i')$ is a multiple of p for all i.

(iii) Conversely, if Γ is a contravariant commutative group sheaf for the *fppf* topology on the category of S-schemes such that (a) $\Gamma(X)$ is p^∞-torsion for quasi-compact X, (b) the group sheaf $\Gamma[p^n]$ is represented by a finite locally free S-group for all $n \geq 1$, and (c) $p : \Gamma \to \Gamma$ is surjective in the sense of (ii), then prove that $G = \{\Gamma[p^n]\}$ is a p-divisible group over S and $\underline{G} \simeq \Gamma$. (By results from descent theory, representatibility for $\Gamma[p]$ implies the same for all $\Gamma[p^n]$'s.)

11. (i) If $0 \to G' \to G \to G'' \to 0$ is a complex of commutative finite locally free group schemes (i.e., the composite is zero), prove that it is short exact if and only if it is so on geometric fibers.

(ii) Deduce that if a diagram of finite locally free commutative group schemes induces a short exact sequence of sheaves for the *fpqc* or *fppf* topologies, then it is short exact in the sense that the second map is faithfully flat and the first is an isomorphism onto its scheme-theoretic kernel. Also prove that $\mathbf{Z}/p\mathbf{Z} \to \mu_p$ over $S = \mathrm{Spec}(\mathbf{Z}_p[\zeta_p])$ defined by $1 \mapsto \zeta_p \in \mu_p(S)$ does *not* factor as a faithfully flat S-group map followed by a closed immersion of S-groups.

12. Let $G = \{G_n\}$ be a p-divisible group over a scheme S and let $H \subseteq G_N$ be a finite locally free closed subgroup for some $N \geq 1$.

(i) For $r, n \geq N$, prove that the map $G_{n+r}/H \to G_r/H$ induced by p^n is faithfully flat (hint: factor it through G_r as a composite of faithfully flat maps), and note that its kernel is $(G_{n+r}/H)[p^n]$ (so this p^n-torsion is *flat*). Prove that this kernel is independent of r; denote it K_n for $n \geq N$.

(ii) Identify K_n with $K_{n+1}[p^n]$, and show that the map $K_{n+1} \to K_n$ induced by p on K_{n+1} is faithfully flat (hint: pass to geometric fibers!) and that its kernel is independent of n. We call this K_1, and likewise define K_m for all $m < N$.

(iii) Show that the directed system $K = \{K_n\}$ is a p-divisible group, and that $G \to K$ is initial among maps of p-divisible groups $G \to G'$ killing H. We write G/H to denote K.

(iv) Prove that a map of p-divisible groups $f : G \to G'$ factors through some p^N on G if and only if it has the form $G \to G/H$ for some finite locally free subgroup $H \subseteq G_N$, in which case H is *unique* and is denoted $\ker f$. A map f having this form locally over S (and so $f^\vee$ does too) is called an *isogeny*, and $\ker f$ makes sense globally. Can you relate $\ker f$ and $\ker f^\vee$¿

(v) Prove that if a map between p-divisible groups over a complete local noetherian ring with residue characteristic p is an isogeny on a geometric closed fiber then it is an isogeny. (Hint: Use the Serre–Tate equivalence.) How about other adic base rings or locally noetherian base schemes?

13. Let k be a perfect field of characteristic $p > 0$.

(i) If $G = \{G_n\}$ is a p-divisible group over k, define $\mathbf{D}(G) = \varprojlim \mathbf{D}(G_n)$. Prove that this is a D_k-module whose underlying $W(k)$-module is finite free, and that $\mathbf{D}(G)/p^n\mathbf{D}(G) \simeq \mathbf{D}(G_n)$ for all $n \geq 1$. Show that $G \rightsquigarrow \mathbf{D}(G)$ is an equivalence of categories between the category of p-divisible groups over k and the category of such D_k-modules. How does connectivity translate in terms of $\mathbf{D}(G)$?

(ii) In terms of (i), characterize isogenies of p-divisible groups in the sense of Exercise 12(iv). How does contravariant Dieudonné theory translate the data of an isogeny and its kernel in terms of semi-linear algebra data? Discuss the case of the (relative) Frobenius and Verschiebung morphisms.

(iii) Prove that if $\gamma \in \mathrm{Aut}_k(G)$ is an finite-order automorphism of a p-divisible group $G = \{G_n\}$ and $\gamma|_{G_1}$ is the identity then γ is the identity if $p \neq 2$. Give a counterexample and corrected version if $p = 2$. (Hint: Look at Dieudonné modules.)