1 Finite flat group schemes

We start with the most general notion of a group scheme over an arbitrary base.

Definition 1.1. Let S be a scheme. A *group scheme* over S is a scheme G over S with maps $m : G \times_S G \to G$, $i : G \to G$ and $e : S \to G$ over S satisfying the commutative diagrams that characterize a group law with inversion and identity.

We won't go through the exact details of these commutative diagrams, but instead describe its consequences. If we have another S-scheme T, then we can consider the set $\mathrm{Hom}_S(T, G)$, which we will denote by $G(T)$. Then the map m induces a map

$$G(T) \times G(T) = \mathrm{Hom}_S(T, G \times_S G) \to \mathrm{Hom}_S(T, G) = G(T),$$

and similarly the map $i : G \to G$ gives a map $i : G(T) \to G(T)$, and the section $e : S \to G$ gives an element $e \in G(T)$. Then the commutative diagrams just ensure that all of these endow the set $G(T)$ with the structure of a group. By abuse of notation, I will write $G(\operatorname{Spec} R)$ as just $G(R)$.

In general, you should think of an S-group scheme G as a family of groups over S, where each fiber over a point $s \in S$ is an actual group, even though this is not literally true. Then $m : G \times_S G \to G$ is fiberwise multiplication, $i : G \to G$ is fiberwise inversion and $e : S \to G$ is fiberwise identity element, and so on.

Example 1.1.1. Here are typical examples of group schemes. Let $S = \operatorname{Spec} k$ for simplicity, but these constructions work over arbitrary rings.

- The scheme $\operatorname{Spec} k[t]$ endowed with the maps $m : \operatorname{Spec} k[x, y] \to k[t]$ given by $t \mapsto x + y$, $i : \operatorname{Spec} k[t] \to \operatorname{Spec} k[t]$ given by $t \mapsto -t$, and $e : \operatorname{Spec} k \to \operatorname{Spec} k[t]$ given by $t \mapsto 0$ is a group scheme, often denoted by $\mathbb{G}_a$. For any k-algebra R, the group $\mathbb{G}_a(R)$ is just the underlying additive group of R.
- We can similarly construct the group scheme $\mathbb{G}_m$, such that for any k-algebra R, the group $\mathbb{G}_m(R)$ is the group of multiplicative units of R. Its underlying scheme is $\operatorname{Spec} k[t, t^{-1}]$.
- There is a group scheme μ_n, such that for every k-algebra R, $\mu_n(R)$ is the group of nth roots of unity in R. Its underlying scheme is $\operatorname{Spec} k[t]/(t^n - 1)$.
- Let Γ be any (abstract) group. We can construct the constant group scheme $\underline{\Gamma}$, such that $\underline{\Gamma}(R)$ consists of the set of locally constant functions on $\operatorname{Spec} R$ with values in Γ, with the evident group structure. Its underlying scheme is the disjoint union $\bigsqcup_{g \in \Gamma} \operatorname{Spec} k$.
- Let A be any abelian variety. Then the kernel of the multiplication-by-n map is a group scheme which we will denote by $A[n]$.

The last three examples fall into an important category of group schemes that we will now isolate.

Definition 1.2. Let S be a scheme. A *finite flat group scheme* over S is a commutative group scheme $f : G \to S$ whose structure morphism f is finite and flat with $f_*\mathcal{O}_G$ a locally free $\mathcal{O}_S$-module of some constant rank $r > 0$. We call r the order of the group scheme.

Remark. The reason why we want the pushforward to be locally free over the base is so that we can define the notion of order of a finite group scheme. In the case when the base S is $\operatorname{Spec} k$ for some field k, this is automatic, and as expected, we can see that the order of both μ_n and $\underline{\mathbb{Z}/n\mathbb{Z}}$ is n, since both of their coordinate rings have dimension n over k. We can't just naively define the order to be something like the number of $\overline{k}$-valued points because if k has characteristic p, then $\mu_p(\overline{k})$ never has p points (it has only.) Similarly, with our notion of order, $A[p]$ has order p^{2g} where g is the dimension of A as expected.

Also, the reason why these are called finite flat group schemes and not finite locally free group schemes is because finite locally free is the same as finite flat when the base scheme is locally Noetherian.

Often, we will be in the case when the structure map of the group scheme is étale in addition to being finite flat.

Example 1.2.1. Let k be a field. We will consider finite flat group schemes over k.

- The constant group scheme is always étale in arbitrary characteristic.
- In characteristic 0, every finite flat group scheme is étale.
- When $\operatorname{char} k = p > 0$, then the group scheme μ_n is étale if and only if p does not divide n. This is because the polynomial $t^n - 1$ is separable if and only if p does not divide n.

When the base scheme S is $\operatorname{Spec} k$ for some field k, we have a classification of all finite étale group schemes over k in terms of Galois theory.

Theorem 1.1. *Fix a separable closure k^{sep}/k. There is an equivalence of categories between the category of finite étale group schemes over k and the category of finite abelian groups with continuous $\operatorname{Gal}(k^{\text{sep}}/k)$-action, given by mapping a finite étale group scheme G over k to the group $G(k^{\text{sep}})$ with the natural Galois action.*

This theorem can be generalized to the case when the base scheme S is an arbitrary connected scheme. We also have the following very useful criterion for showing that a finite flat group scheme over an arbitrary base is étale.

Theorem 1.2. *Let G/S be a finite flat group scheme whose order n is a unit on S. Then G is étale over S.*

Sketch. By formal nonsense we can reduce to the case when $S = \operatorname{Spec} k$ for k algebraically closed. A theorem of Deligne says that multiplication by n on G factors through the identity section, so the induced map on the tangent space at identity must be zero. On the other hand, one can compute that the induced map is given by multiplication by n. Since n is invertible, this implies that the tangent space must be zero, so G is étale. For details, refer to Lemma 7.1.9 in [BC09]. □

Finally, we have the notion of Cartier duality for finite flat group schemes.

Definition 1.3. Let G be a finite flat group scheme over S. The *Cartier dual* of G is a finite flat group scheme $G^\vee$ over S such that for any S-scheme T, we have

$$G^\vee(T) = \operatorname{Hom}_{T\text{-Grp}}(G_T, \mathbb{G}_{m,T}).$$

One can show that the Cartier dual exists for all finite flat group schemes G/S.

Example 1.3.1. Here are a few important examples of Cartier duality.

- The Cartier dual of μ_n is $\underline{\mathbb{Z}/n\mathbb{Z}}$.
- The Cartier dual of $A[n]$ is $A^\vee[n]$, where $A^\vee$ is the dual abelian variety.

2 Raynaud's theorem

Let $K/\mathbb{Q}_p$ be a finite extension, let $\mathcal{O}_K$ be the ring of integers of K, let k be the residue field of $\mathcal{O}_K$, and let e be the ramification index of $K/\mathbb{Q}_p$.

Definition 2.1. An *prolongation* of a finite flat group scheme G_0/K is a finite flat group scheme $G/\mathcal{O}_K$ equipped with an isomorphism $G_K \to G_0$.

The following theorem of Raynaud says that prolongations are unique as long as ramification is low.

Theorem 2.1 (Raynaud). *Suppose that $e < p-1$. Let G_0 be a finite flat group scheme over K. Then any two prolongations of G_0 over $\mathcal{O}_K$ are isomorphic.*

Example 2.1.1. This bound is sharp. To see this, consider $\mathbb{Z}/p\mathbb{Z}$ and μ_p over $\mathcal{O}_K$, where $K = \mathbb{Q}_p(\zeta_p)$. This is a totally ramified extension of ramification degree $e = p-1$. Over K, $\mathbb{Z}/p\mathbb{Z}$ and μ_p are isomorphic, but they are not isomorphic over $\mathcal{O}_K$ because they have different special fibers.

3 Admissible group schemes

Let N be a prime, and let p be another prime different from N. All group schemes considered will be commutative.

Definition 3.1. A group scheme G over $\mathbb{Z}[1/N]$ is *pre-admissible* if it is finite flat and killed by a power of p. A group scheme G over $\mathbb{Z}$ is *pre-admissible* if it is quasi-finite[1], separated, killed by a power of p, and its restriction to $\mathbb{Z}[1/N]$ is finite flat (so in particular it is pre-admissible.)

Let G be a pre-admissible group over $\mathbb{Z}[1/N]$. An *admissible filtration* of G is a filtration

$$0 = F^0G \subset F^1G \subset \cdots \subset F^nG = G$$

by closed subgroups such that $F^{n+1}G/F^nG$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or μ_p for each n.

Definition 3.2. We say that a pre-admissible group over $\mathbb{Z}[1/N]$ is *admissible* if it has an admissible filtration. A pre-admissible group over $\mathbb{Z}$ is *admissible* if its restriction to $\mathbb{Z}[1/N]$ is admissible.

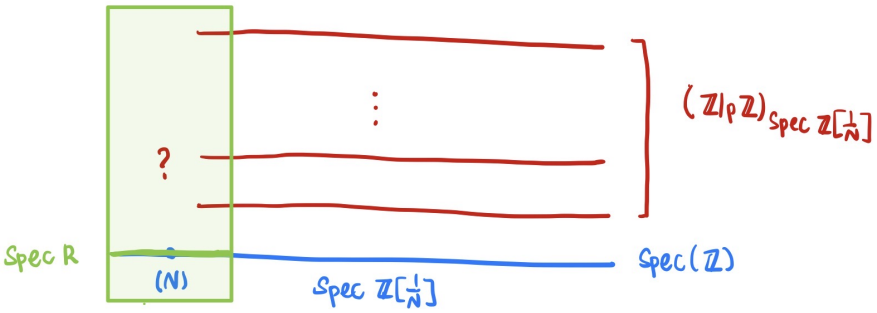
We are interested in such groups because they arise naturally as p-power torsion of the Néron model of an abelian variety over $\mathbb{Z}[1/N]$. We will also need to know how we can extend pre-admissible group schemes over $\mathbb{Z}[1/N]$ to those over $\mathbb{Z}$. For this the following theorem will be very useful.

Fix an embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_N$, which gives us an inertia subgroup I_N in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Theorem 3.1. *Let G' be a pre-admissible group scheme over $\mathbb{Z}[1/N]$. Then giving an extension of G' to a pre-admissible group scheme G over $\mathbb{Z}[1/N]$ (up to canonical isomorphism) amounts to giving a sub $\mathrm{Gal}(\overline{\mathbb{Q}}_N/\mathbb{Q}_N)$-module H in $G(\overline{\mathbb{Q}})^{I_N}$. Moreover, this G is finite if and only if $H = G(\overline{\mathbb{Q}})$ (so this only exists when I_N acts trivially on $G(\overline{\mathbb{Q}})$.)*

[1] finite type and every point is an isolated point of its fibre. This is the same thing as locally of finite type, quasi-compact with finite fibres. A good way to visualize these is via Zariski's main theorem, which says that if the base is qcqs, every quasi-finite separated map factors through an open immersion into a finite map.

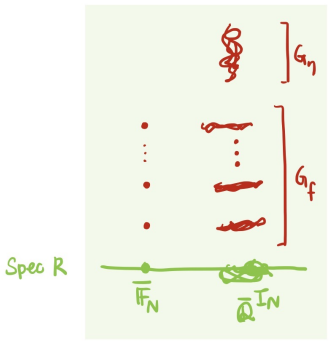
Sketch. We will construct the map in one direction, and leave the rest to Brian Conrad's notes in [Con04]. Suppose that we have a pre-admissible group scheme G over $\mathbb{Z}$ which extends G'. Then since G is killed by a power of p, G is a étale quasi-finite group over $\mathbb{Z}[1/p]$. Consider the strict henselization of $\mathbb{Z}_{(N)}$, which is the integral closure of $\mathbb{Z}_{(N)}$ in $\mathbb{Z}_N^{\mathrm{un}}$, where the latter is the ring of integers of $\mathbb{Q}_N^{\mathrm{un}}$ which is the maximal unramified extension of $\mathbb{Q}_N$ in $\overline{\mathbb{Q}}_N$. This ring clearly lies in the image of ι, so we can consider it as a subring of $\overline{\mathbb{Q}}$ which we will denote by R. Then one can show that the field of fractions of R is $\overline{\mathbb{Q}}^{I_N}$ and that the residue field is $\overline{\mathbb{F}}_N$. The space $\operatorname{Spec} R$ should be thought of as a infinitesimal neighbourhood of the point (N) (more precisely it is the stalk at (N) of the structure sheaf of $\operatorname{Spec} \mathbb{Z}$ in the étale topology.) Here is a picture to illustrate what is going on, in the case when the group scheme over $\mathbb{Z}[1/N]$ that we are trying to extend is $\mathbb{Z}/p\mathbb{Z}$.



Consider the base change of G to R, which we will continue to denote by G. By the structure theorem for quasi-finite, separated schemes over henselian local rings and using the fact that G is etale over R, we can write

$$G = G_f \sqcup G_\eta,$$

where G_f is finite étale over R, and G_η has empty special fiber. Since R is strictly henselian, G_f is a disjoint union of the base R.



In particular, there is a bijection

$$G_f(\overline{\mathbb{Q}}^{I_N}) \to G_f(\overline{\mathbb{F}}_N) = G(\overline{\mathbb{F}}_N).$$

The inverse of this then gives a map $G(\overline{\mathbb{F}}_N) \to G_f(\overline{\mathbb{Q}}^{I_N}) \to G(\overline{\mathbb{Q}}^{I_N}) = G(\overline{\mathbb{Q}})^{I_N}$. The assertion regarding finiteness and the proof of the equivalence is described in full detail in [Con04]. □

In light of this theorem, for any given pre-admissible group G' over $\mathbb{Z}[1/N]$, there are two special extensions to $\mathbb{Z}$, which we will denote by $G^\flat$ and $G^\sharp$. These are obtained by choosing H to be either the trivial subgroup, or the entire $G(\overline{\mathbb{Q}})^{I_N}$ respectively.

We now define some invariants of admissible groups following Mazur.

- Let $\ell(G) = \log_p(|G_{\mathbb{Q}}|)$ where $|G_{\mathbb{Q}}|$ is the order of $G_{\mathbb{Q}}$.
- Let $\delta(G) = \log_p(|G_{\mathbb{Q}}|) - \log_p(|G_{\mathbb{F}_N}|)$.
- Let $\alpha(G)$ be the number of $\mathbb{Z}/p\mathbb{Z}$'s appearing in an admissible filtration of G over $\mathbb{Z}[1/N]$.
- Let $h^i(G)$ be $\log_p(|H^i_{\text{fppf}}(\text{Spec}(\mathbb{Z}), G)|)$ for $i = 0, 1$.

Here, $H^i_{\text{fppf}}(\text{Spec}(\mathbb{Z}), G)$ denotes the fppf cohomology groups of G over $\text{Spec}\,\mathbb{Z}$. We recall their definition. Given a scheme S, we can define its big fppf site to be the category of all S-schemes, where the coverings are given by families of S-morphisms $\{f_i : U_i \to U\}_{i\in T}$, where each $f_i : U_i \to U$ is flat and locally of finite presentation, and we have $\bigcup_{i\in T} f_i(U_i) = U$. We will denote this site by S_{fppf}. Given any sheaf $\mathcal{F}$ of abelian groups on this site, we can define the cohomology groups $H^i_{\text{fppf}}(S, \mathcal{F})$ in the usual way, by taking right derived functors of the global sections functor $\mathcal{F} \mapsto \mathcal{F}(S)$. In particular, given a commutative group scheme G over S, we can regard it as a sheaf of abelian groups on the big fppf site over S, and the cohomology groups $H^i_{\text{fppf}}(S, G)$ are defined to be the cohomology groups of this sheaf. In particular, $H^0(S, G)$ is just $G(S)$, and $H^1(S, G)$ is naturally in bijection with isomorphism classes of *fppf G-torsors* on S.

Definition 3.3. An admissible group G is *elementary* if $\ell(G) = 1$.

Proposition 3.2. *There are four elementary admissible groups over $\mathbb{Z}$, namely $\mathbb{Z}/p\mathbb{Z}$, $(\mathbb{Z}/p\mathbb{Z})^\flat$, μ_p and $\mu_p^\flat$.*

Proof. By definition there are only two elementary admissible groups over $\mathbb{Z}[1/N]$, namely $\mathbb{Z}/p\mathbb{Z}$ and μ_p. Both of these have unramified $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action at N, and the group of $\overline{\mathbb{Q}}$-points has size p, so there are exactly two ways to extend them as mentioned above. □

Proposition 3.3. *The invariants of the elementary admissible groups are given as follows.*

	$\mathbb{Z}/p\mathbb{Z}$	$(\mathbb{Z}/p\mathbb{Z})^\flat$	μ_p	$\mu_p^\flat$
δ	0	1	0	1
α	1	1	0	0
h^0	1	0	ϵ'	0
h^1	0	0	ϵ'	ϵ

where ϵ' is 0 if p odd and 1 if $p = 2$, and ϵ' is 0 if p odd and $N \not\equiv 1 \mod p$, or if p is even and $N = 3 \mod 4$, and 1 otherwise.

Proposition 3.4. *Let G be an admissible group over $\mathbb{Z}$. Then $h^1(G) - h^0(G) \leq \delta(G) - \alpha(G)$.*

Proof. Let $0 \to G_1 \to G_2 \to G_3 \to 0$ be a short exact sequence of admissible groups over $\mathbb{Z}$. The right hand side of the inequality is additive, whereas the left hand side is subadditive:

$$h^1(G_2) - h^0(G_2) \leq h^1(G_1) - h^0(G_1) + h^1(G_3) - h^0(G_3).$$

This follows easily from the long exact sequence in fppf cohomology. Now since every admissible group over $\mathbb{Z}$ has a filtration by closed subgroups where each quotient is an elementary admissible group, we can reduce this proposition in the case when G is an elementary admissible group. This then follows from the computations in Proposition 3.3. □

This inequality will be crucial in the proof of Theorem B, where it will be used to bound the rank of an abelian variety satisfying the hypotheses in the theorem.

References

[BC09] Oliver Brinon and Brian Conrad. *CMI summer school notes on p-adic Hodge theory*. 2009. URL: https://math.stanford.edu/~conrad/papers/notes.pdf.

[Con04] Brian Conrad. *Classification of quasi-finite étale separated schemes*. 2004. URL: https://math.stanford.edu/~conrad/vigregroup/vigre03/zmt.pdf.