Group Schemes

Samit Dasgupta and Ian Petrow

December 8, 2010

We begin with an example of a group scheme.

Example 1. Let R be a commutative ring. Define

$$GL_n(R) = \{(x_{ij}) \in R^{n\times n} : \det(x_{ij}) \in R^*\} = \mathrm{Hom}(\mathrm{Spec}\ R, G), \tag{1}$$

where

$$G = \mathrm{Spec}\ \mathbb{Z}[(x_{ij})_{i,j=1}^n, y]/(\det(x_{ij})y - 1).$$

The second equality of (1) is given explicitly by

$$A = (a_{ij}) \in GL_n(R) \longleftrightarrow \varphi : \mathbb{Z}[(x_{ij})_{i,j=1}^n, y]/(\det(x_{ij})y - 1) \to R$$

given by $x_{ij} \longmapsto a_{ij}$, $y \longmapsto \det(x_{ij})^{-1}$. $GL_n(R)$ is a group for each R, in a functorial way:

$$\mathrm{mult} : GL_n(R) \times GL_n(R) \to GL_n(R)$$
$$\mathrm{inv} : GL_n(R) \to GL_n(R).$$

come from the ring homs

$$\mathbb{Z}[(x_{ij}), y] \to \mathbb{Z}[(x'_{ij}), y'] \otimes \mathbb{Z}[(x''_{ij}), y''] \simeq \mathbb{Z}[(x_{ij})', (x_{ij})'', y', y'']$$

defined by $x_{ij} \longmapsto \sum_{k=1}^n x'_{ik}x''_{kj}$, $y \longmapsto y'y''$. And similarly for inversion.

Definition 1. Let S be a scheme. An S-group scheme is a scheme G over S together with an S-morphism $m : G \times G \to G$ such that the induced law of composition $G(T) \times G(T) \to G(T)$ makes $G(T)$ a group for every S-scheme T.

(Note: here and below, all products are over S.) An equivalent definition is that an S-group scheme is a contravariant functor from the category of schemes over S to the category of groups such that the underlying functor to the category of sets is representable.

Another (and more explicit) definition is that an S-group scheme is a scheme G over S together with an S-morphism $m : G \times G \to G$ such that

(a) (Associative Law) The diagram

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

commutes.

(b) (Identity) There exists an S-morphism $\epsilon : S \to G$ such that

$$\begin{array}{ccc} S \times G = G \times S & \xrightarrow{id \times \epsilon} & G \times G \\ \downarrow{\scriptstyle \epsilon \times id} & \searrow^{id} & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{\quad m \quad} & G \end{array}$$

commutes.

(c) (Inverse) There exists an S-morphism $inv : G \to G$ such that

$$\begin{array}{ccc} G \times G & \xrightarrow{inv \times id} & G \times G \\ \uparrow{\scriptstyle \Delta} & & \downarrow{\scriptstyle m} \\ G & \xrightarrow{\quad \epsilon \circ \pi \quad} & G \end{array} \qquad \text{and} \qquad \begin{array}{ccc} G \times G & \xrightarrow{id \times inv} & G \times G \\ \uparrow{\scriptstyle \Delta} & & \downarrow{\scriptstyle m} \\ G & \xrightarrow{\quad \epsilon \circ \pi \quad} & G \end{array}$$

commute.

Definition 2. An S-group scheme G is commutative if $G(T)$ is commutative for all S-schemes T.

This is equivalent to

$$\begin{array}{ccc} G \times G & \xrightarrow{pr_2 \times pr_1} & G \times G \\ & \searrow^{m} & \downarrow{\scriptstyle m} \\ & & G \end{array}$$

commuting.

Definition 3. A morphism of S-group schemes is an S-morphism $\varphi : G \to G'$ such that $G(T) \to G'(T)$ defined by $g \longmapsto \varphi \circ g$ is a group homomorphism for all T. Equivalently, φ is a morphism of S-group schemes if

$$\begin{array}{ccc} G \times G & \xrightarrow{\varphi \times \varphi} & G' \times G' \\ \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle m'} \\ G & \xrightarrow{\quad \varphi \quad} & G' \end{array}$$

commutes.

Say $S = \text{Spec } R$ affine, and $G = \text{Spec } A$ is an affine R-scheme. We then have the corresponding ring maps $\tilde{m} : A \to A \otimes_R A$, $\tilde{\epsilon} : A \to R$, and $\tilde{inv} : A \to A$. An R-algebra A together with these maps satisfying the commutative diagrams corresponding to (a), (b), and (c) above is called a Hopf algebra.

Examples

(1) Additive group. Define $\mathbb{G}_a(\text{Spec } B) = B$ under $+$.

$$\mathbb{G}_a = \text{Spec } R[x].$$

$$\tilde{m} : R[x] \to R[x] \otimes_R R[x] \simeq R[x', x'']$$

defined by $x \longmapsto x \otimes 1 + 1 \otimes x \longleftrightarrow x' + x''$, where x', x'' correspond to $1 \otimes x$ and $x \otimes 1$, respectively.

One can also define certain twisted versions of this group scheme. For example, if k is a characteristic p field, and $a \in k$ is not a pth power in k then consider the group scheme G over Spec k defined by $G(\text{Spec } B) = \{(x, y) \in B^2 : y^p = x - ax^p\}$. The group scheme G is a twisted form of $\mathbb{G}_a$, that is to say, it is a group scheme (under usual addition due to "freshman's binomial theorem," which becomes isomorphic to $\mathbb{G}_a$ after a base change (namely to $k(a^{1/p})$).

(2) Multiplicative group. Define $\mathbb{G}_m(\text{Spec } B) = B^*$.

$$\mathbb{G}_m = \text{Spec } R[x, y]/(xy - 1).$$

$$\tilde{m} : R[x, y]/(xy - 1) \to R[x', y', x'', y'']/(x'y' = 1, x''y'' = 1)$$

defined by $\tilde{m}(x) = x'x''$ and $\tilde{m}(y) = y'y''$. $\mathbb{G}_m$ is simply the $n = 1$ case of the group scheme GL_n.

We can define twisted forms of $\mathbb{G}_m$ as well. For example, the group scheme over $\mathbb{Q}$ defined by the equation $x^2 - 7y^2 = 1$ (using the usual multiplication in $\mathbb{Q}(\sqrt{7})$ to define the group structure) is a group scheme not isomorphic to $\mathbb{G}_m$, but it becomes isomorphic to $\mathbb{G}_m$ after a base change to $\mathbb{Q}(\sqrt{7})$.

Exercise 1. Let $D =$ any R-algebra that is finite free as an R-module. Show there is an affine R-group scheme, denoted $\mathbb{D}^*$ such that $\mathbb{D}^*(B) = (D \otimes_R B)^*$ for all commutative R-algebras B.

(3) n-th roots of unity. Let $n \geq 1$ be an integer. Define

$$\mu_n = \text{Spec } R[x]/(x^n - 1).$$

We have

$$\mu_n(B) := \{b \in B : b^n = 1\} \subset \mathbb{G}_m(B).$$

The inclusion $\mu_n \to \mathbb{G}_m$ corresponds to

$$\frac{R[x, y]}{(xy - 1)} \to \frac{R[x]}{(x^n - 1)}$$

defined by $x \longmapsto x$ and $y \longmapsto x^{n-1}$. Similarly, for positive integers m, n, we have a natural map $\mu_n \to \mu_{mn}$ corresponding to

$$R[x]/(x^{mn}-1) \longrightarrow R[x]/(x^n-1), \qquad x \mapsto x$$

(inducing the identity map $\mu_n(B) \to \mu_{mn}(B)$).

(4) Diagonalizable group schemes. Let X be a commutative group. Let $R[X] := \bigoplus_{x \in X} Rx$, group algebra of X over R. It is a commutative R-algebra. Define $D(X) := \text{Spec } (R[X])$, so

$$D(X)(\text{Spec } B) = \text{Hom}_{R-\text{alg}}(R[X], B) = \text{Hom}_{\text{Gps}}(X, B^*).$$

The group law is given by pointwise multiplication. Note the special cases $D(\mathbb{Z}) \simeq \mathbb{G}_m$, $D(\mathbb{Z}/n\mathbb{Z}) \simeq \mu_n$. Furthermore, under these isomorphisms the natural maps $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ induce the natural maps $\mu_n \to \mathbb{G}_m$ and $\mu_n \to \mu_{mn}$ discussed in (3) above.

Digression: Kernels, cokernels, and base change. Let $\varphi : G \to G'$ be a morphism of S-group schemes. A <u>kernel</u> of φ is a homomorphism of S-group schemes $\alpha : H \to G$ such that for all S-schemes T,

$$0 \longrightarrow H(T) \xrightarrow{\alpha_*} G(T) \xrightarrow{\varphi_*} G'(T)$$

is exact. It is unique up to unique isomorphism by universal property nonsense. We write $0 \to H \to G \to G'$. We can give an explicit construction: $H = G \times_{G'} S$. Indeed, the universal property for fibered product and that for kernel are the same. At the level of T points, we have

$$H(T) = \{(g, s) \in G(T) \times S(T) : \varphi_*(g) = \epsilon'_*(s)\}.$$

Now $S(T) = \{\pi_T : T \to S\}$, where π_T is the structure map of the S-scheme T, and $\epsilon'_*(\pi_T) = \epsilon_T$, the identity in $G(T)$. So we have that

$$H(T) = \{g \in G(T) : \varphi_*(g) = id_{G'(T)}\}$$

as desired. An example of a kernel is given by

$$0 \longrightarrow \mu_n \longrightarrow \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m \ ,$$

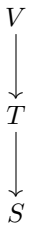
where the last map is given

$$\text{Spec } R[x, x^{-1}] \to \text{Spec } R[x, x^{-1}]$$

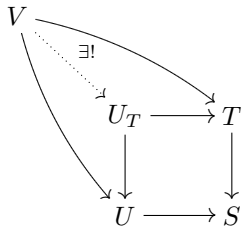
given by $x \longmapsto x^n$.

Now, <u>cokernels</u> are a much more difficult topic, just as in the case of sheaves. Given $\varphi : G \to G'$ injective between commutative group schemes, the functor $T \longmapsto G'(T)/\varphi G(T)$ need not be representable, so a naive definition of cokernel is not sufficient. Cokernels will be discussed in the talks by Simon and Mike.

Next we discuss base change. Let U, T be S-schemes. $U_T := U \times_S T$ is the "base change from S to T of U". Every T-scheme V is an S-scheme



and $U_T(V) = U(V)$. i.e.



by the universal property of fibered product. Therefore, if G is an S-group scheme, then G_T is a T-group scheme. Most of the group schemes defined so far are base changes from group schemes over $\mathbb{Z}$.

We now return to examples of group schemes.

(5) Constant group scheme. Let X be a set. The constant S-scheme X_S is by definition

$$X_S := \coprod_{x \in X} S_x$$

of copies of S indexed by X. Given an S-scheme T, an element $f \in X_S(T)$ is determined by the collection of subsets $U_x = f^{-1}(S_x) \subset T$ for $x \in X$. The U_x are open, disjoint, and cover T, and $f|_{U_x}$ is the unique S-morphism $U_x \to S_x \simeq S$. So to f we correspond the function $\varphi : T \to X$ determined by $\varphi(U_x) = x$. Therefore

$$X_S(T) = \{\text{locally constant functions } \varphi : T \to X\}.$$

In particular, if T is nonempty and connected, then $X_S(T) = X$. If X is a group, X_S is a group scheme under pointwise multiplication of locally constant functions.

Exercise 2. If $S = \operatorname{Spec} R$ is affine and X is a finite group, describe $X_S = \operatorname{Spec} A$ for an R-algebra A, and give the Hopf algebra structure on A.

Exercise 3. If G is an S-group scheme, then there is a contravariant functor from schemes over S to abelian groups that sends an S-scheme T to the group

of T-group scheme homomorphisms from G_T to $(\mathbb{G}_m)_T$. If this functor is representable, then the representing S-group scheme is called the character group of G. Show that if X is a finite, commutative group, then there is a canonical pairing $D(X)_S \times X_S \to (\mathbb{G}_m)_S$ that identifies each of $D(X)_S$, X_S with the character group of the other.

(6) An abelian scheme A/S is an S-group scheme $A \to S$ that is proper, flat, finitely presented, and has smooth and connected geometric fibers. As its name suggests, an abelian scheme is always commutative. Note: the function $s \longmapsto \dim A_s$ (where s is a point of S and A_s is the fiber over it) is locally constant on S, and we usually assume that it is in fact constant, denoted g. The case of dimension $g = 1$ is the familiar case of elliptic curves.

For all $n > 1$, consider the multiplication by n morphism $[n] : A \to A$. The kernel is a group scheme denoted $A[n]$.

$$0 \longrightarrow A[n] \longrightarrow A \longrightarrow A \longrightarrow 0.$$

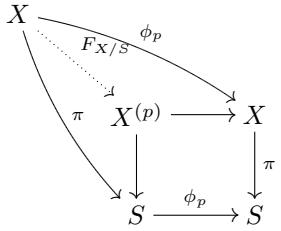
Definition 4. Let S be a locally noetherian scheme. An S-scheme X is finite and flat if and only if $\mathcal{O}_X$ is locally free of finite rank as an $\mathcal{O}_S$-module. The rank is a locally constant function on S, called the order of X.

Proposition 1. *Let S be a locally Noetherian scheme. Let $n > 1$ be an integer and let A be an abelian scheme over S of dimension g. Then $A[n]$ is a finite flat S-group scheme of order n^{2g}.*

Our next collection of examples will take place in characteristic p. Consider a scheme $S/\mathbb{F}_p$, and the map $\phi_p : S \longrightarrow S$ that induces the identity map on the topological space of S and sends a local section h of $\mathcal{O}_S$ to h^p. For example, we could take $S = \operatorname{Spec} k$ with k a field of characteristic p, and $\phi_p = x \longmapsto x^p$.

Let X be a scheme over S. We define a scheme $X^{(p)} := X \times_{S,\phi_p} S$, where the map $S \to S$ used in the fiber product is the map ϕ_p. Concretely, if $S = \operatorname{Spec} k$, k a field of characteristic p, given $X = \operatorname{Spec} A$, A a k-algebra, define a new k-algebra $A^{(p)} = k \otimes_{\phi_p,k} A$, i.e. $bc^p \otimes x = b \otimes cx$. Then $X^{(p)} = \operatorname{Spec} A^{(p)}$. Even more concretely, if $S = \operatorname{Spec} R$ is affine and X is defined by certain polynomial equations over R, then $X^{(p)}$ is defined by the same equations with each coefficient replaced by its pth power.

Furthermore, there is a natural S-morphism $F_{X/S} : X \longrightarrow X^{(p)}$ called the Frobenius map defined by the following diagram (i.e. from the universal property of the fiber product $X^{(p)}$ along with the maps $\phi_p : X \longrightarrow X$ and the structure map $\pi : X \longrightarrow S$):



In the concrete description $X = \mathrm{Spec}\, A^{(p)}$ above, the Frobenius map $F_{X/S} : X \to X^{(p)}$ is given by $A^{(p)} \to A$, $c \otimes a \longmapsto ca^p$. In our "even more concrete" description, a point on X is mapped to the point on $X^{(p)}$ in which each coordinate is raised to the pth power.

The formation of $F_{X/S}$ is functorial in X over S and is compatible with the formation of products over S. It follows that if X is an S-group scheme, then $X^{(p)}$ naturally has the structure of S-group scheme as well (by base change), and that the morphism $F_{X/S}$ is a homomorphism of S-groups.

Exercise 4. Prove that the formation of $X^{(p)}$ over S is naturally compatible with base change on S, and that in this way the formation of $F_{X/S}$ is naturally compatible with base change on S as well. (Note: X is not necessarily an S-group scheme in this exercise.)

Examples of the Frobenius morphism:

- $G = \mathbb{G}_m/S$, $G^{(p)} \simeq \mathbb{G}_m/S$, $F_{\mathbb{G}_m/S} = [p] : \mathbb{G}_m \longrightarrow \mathbb{G}_m$, $\ker F_{\mathbb{G}_m/S} = \mu_p$.

- $G = \mathbb{G}_a/S$, $G^{(p)} \simeq \mathbb{G}_a/S$, $F_{\mathbb{G}_a/S} : \mathbb{G}_a \xrightarrow{t \mapsto t^p} \mathbb{G}_a$. Define $\alpha_p := \ker F_{\mathbb{G}_a/S}$, so $\alpha_p(B) = \{b \in B : b^p = 0\}$. Over $S = \mathrm{Spec}\, R$, we have $\alpha_p = \mathrm{Spec}\, R[x]/x^p$.

- μ_p acts nontrivially on α_p (restricting the action of $\mathbb{G}_m$ on $\mathbb{G}_a$ by scaling), so we get a noncommutative k-group scheme $\alpha_p \rtimes \mu_p$ of order p^2!

- In SGA3, Exposé $\mathrm{VII_A}$, Sections 4.2–4.3, it is shown for any $\mathbb{F}_p$-scheme S how to assign to any *flat* commutative S-group G an S-group map $V_{G/S} : G^{(p)} \to G$ with the following properties: it is functorial in G, compatible with any base change on S, and satisfies $V_{G/S} \circ F_{G/S} = [p]_G$ and $F_{G/S} \circ V_{G/S} = [p]_{G^{(p)}}$. Moreover, in the special case of finite locally free commutative S-groups to be discussed by Simon, there will be an operation $G \rightsquigarrow G^\vee$ called *Cartier duality* under which $V_{G/S}$ is Cartier dual to $F_{G^\vee/S}$. One can cheat and use this final description as a definition for that special case, but then it is a useless notion until one does real work to prove the desired good behavior for composition with relative Frobenius homomorphisms.

  Here are two elementary special cases. Since $[p] = 0$ on $\mathbb{G}_a$ and the relative Frobenius of $\mathbb{G}_a$ is faithfully flat, necessarily $V_{\mathbb{G}_a/S} = 0$. Thus, by functoriality $V_{\alpha_p/S} = 0$ too. Since $F_{\mathbb{G}_m/S} = [p]$ on $\mathbb{G}_m$ (relative to its $\mathbb{F}_p$-structure that identifies it with its own Frobenius twist over S), we have $V_{\mathbb{G}_m/S} = \mathrm{id}$. hence, by functoriality $V_{\mu_p/S}$ is the identity on μ_p.

- If k is an algebraically closed field of char p, the only commutative group schemes over k of order p are $(\mathbb{Z}/p\mathbb{Z})_k, \mu_p, \alpha_p$. (In fact, all group schemes of order p over k are commutative, so these are the only ones.)

- Let k be an algebraically closed field of characteristic p, and E an elliptic curve over k. Consider the Frobenius map $F_{E/k} : E \to E^{(p)}$. By the previous remark, $\ker F_{E/k}$ is one of $(\mathbb{Z}/p\mathbb{Z})_k, \mu_p$, or α_p. However, since $F_{E/k}$ is a purely inseparable isogeny, the case $(\mathbb{Z}/p\mathbb{Z})_k$ is impossible. We have
$$\ker F_{E/k} \cong \begin{cases} \mu_p & E \text{ is ordinary} \\ \alpha_p & E \text{ is supersingular.} \end{cases}$$

- Let $G_n = \ker F^n_{E/k} : E \to E^{(p^n)}$, a connected k-subgroup scheme of order p^n. (One should be careful to note that F^n_p is an abuse of notation here, since it is the composition of Frobenius maps between different varieties, i.e. $F^n_{E/k} = F_{E^{(p^{n-1})}/k} \circ \cdots \circ F_{E^{(p)}/k} \circ F_{E/k}$). Since E is a smooth curve, it has a unique infinitesimal closed subscheme supported at 0 with any desired length. Therefore
$$\varprojlim_n \mathcal{O}(G_n) \simeq \widehat{\mathcal{O}_{E,0}},$$
the formal group of E. (In general, the identity component of the p-divisible group of an abelian variety in characteristic p recovers its formal group; these concepts will be defined and discussed later).

- If R is an absolutely unramified p-adic DVR, there does not exist a finite flat commutative group scheme over R with special fiber α_p. The takeaway point of this example is that ramification of the base DVR constrains the possibilites of finite flat commutative R groups. This is proven using Oort-Tate, and was generalized by Raynaud. This will be discussed later by Melanie and Rebecca.

We now explain how the Oort–Tate/Raynaud classification of finite flat group schemes of exponent p leads to a proof of the following famous theorem of Nagell and Lutz.

Theorem 1 (Nagell–Lutz)**.** *Suppose $y^2 = x^3 + Ax + Bx + C$ is an elliptic curve E over $\mathbb{Q}$, with $A, B, C \in \mathbb{Z}$. Then for any nontrivial $P = (x, y) \in E(\mathbb{Q})_{tors}$, we have $x, y \in \mathbb{Z}$.*

We will prove the Nagell–Lutz theorem using techniques from the theory of group schemes as much as possible; in particular, the Weierstrass model will only be used at the very end of the proof (to eliminate the possibility of non-integral 2-torsion points P). We first prove a lemma using Raynaud's classification as a black box.

Lemma 1. *Let $d = p^r$ be a prime power. If the constant $\mathbb{Q}$-group scheme $(\mathbb{Z}/d\mathbb{Z})_{\mathbb{Q}}$ has a connected finite flat model H over $\mathbb{Z}_{(p)}$ then necessarily $d = p = 2$ and $H \cong \mu_2$.*

Proof. Raynaud's results imply that for $p > 2$, there is *at most one* finite flat group scheme over $\mathbb{Z}_{(p)}$ with a given generic fiber over $\mathbb{Q}$. As the constant group scheme $\mathbb{Z}/p^r\mathbb{Z}$ provides an example, and is not connected, we are reduced to the case $p = 2$.

When $d = 2$, uniqueness again follows from Raynaud under our connectedness hypothesis, and μ_2 provides an example. Hence it remains to eliminate the possibility $d = 2^r$ with $r > 1$. The schematic closure method (to be discussed by Melanie) implies that all subgroups of the generic fiber inherit the hypothesis of admitting a connected finite flat model, so it suffices to rule out the case $r = 2$, i.e. $d = 4$.

To this end, suppose we have a connected finite flat group scheme H over $\mathbb{Z}_{(2)}$ with generic fiber $\mathbb{Z}/4\mathbb{Z}$. Applying the schematic closure method we obtain a short exact sequence of finite flat commutative $\mathbb{Z}_{(2)}$-groups

$$0 \longrightarrow H_1 \longrightarrow H \longrightarrow H_2 \longrightarrow 0$$

where H_1 and H_2 are connected with generic fibers $\mathbb{Z}/2\mathbb{Z}$. Thus, by the uniqueness established for $r = 1$, we see that H_1 and H_2 must be isomorphic to μ_2. To get a contradiction, we work over $A = W(\mathbb{F}_2)$ and use the operation of Cartier duality, denoted D, to be discussed by Simon. This exact "duality" operation swaps μ_n with $\mathbb{Z}/n\mathbb{Z}$, so $D(H_A)$ is an extension of $\mathbb{Z}/2\mathbb{Z}$ by $\mathbb{Z}/2\mathbb{Z}$, and in particular is étale (as that can be checked on the special fiber, where it follows from the étale property for outer terms in a short exact sequence, say by counting the number of geometric points). But A is a complete dvr with algebraically closed residue field, so finite étale A-schemes are constant. Hence, $D(H_A)$ is constant. Yet its generic fiber over $A[1/2]$ is $D(\mathbb{Z}/4\mathbb{Z}) = \mu_4$ which over $A[1/2]$ is *not* constant. This is a contradiction as desired. □

Proof of Theorem 1. Fix a prime p and let $R = \mathbb{Z}_{(p)}$. Let $W \subseteq \mathbb{P}^2_R$ be

$$\{(x, y, z) : zy^2 = x^3 + Ax^2z + Bxz^2 + Cz^3\},$$

and let W^{sm} be the open smooth locus. Let $\epsilon = [0, 1, 0] \in W^{\mathrm{sm}}(R)$. Suppose that $Q = [x, y, 1] \in W(\mathbb{Q})$ is a nontrivial torsion point such that one of x or y has denominator divisible by p. Thus, Q reduces to the reduction of ϵ (denoted $\tilde{\epsilon}$) in $\mathbb{P}^2(\mathbb{F}_p)$ since the origin of a Weierstrass cubic is its unique point on the line at infinity. In particular $Q \in \mathbb{P}^2(\mathbb{Q}) = \mathbb{P}^2(R)$ is contained in $W^{\mathrm{sm}}(R)$.

Let $\mathcal{E}$ be the Neron model of E over R. (Recall: $\mathcal{E}$ is a separated, smooth scheme over R with general fiber E over $\mathbb{Q} = \mathrm{Frac}(R)$, such that for any scheme T over R and $\mathbb{Q}$-map $T_{\mathbb{Q}} \xrightarrow{\phi} E$, there is a unique extension to an R-morphism $T \xrightarrow{\Phi} \mathcal{E}$.)

By the Neron mapping property, there exists a unique $\Psi : W^{\mathrm{sm}} \to \mathcal{E}$ extending $W^{\mathrm{sm}}_{\mathbb{Q}} \simeq E$, and this map sends $\epsilon \mapsto$ (identity of $\mathcal{E}(R)$), so $Q \in W^{\mathrm{sm}}(R)$ maps to a point $\Psi(Q) \in \mathcal{E}(R)$ with reduction equaling the origin of $\mathcal{E}_{\mathbb{F}_p}$.

Let N be the order of Q, and let d be a prime power fully dividing N (i.e. $(d, N/d) = 1$). Let $P = (N/d)\Psi(Q) \in \mathcal{E}(R)$, with order d and reduction equaling

the origin of $\mathcal{E}_{\mathbb{F}_p}$. Define a morphism $(\mathbb{Z}/d\mathbb{Z})_R \xrightarrow{\Phi} \mathcal{E}$ by $a \mapsto aP$. (More precisely, the map Φ is defined as follows: recall $(\mathbb{Z}/d\mathbb{Z})_R = \coprod_{a\in\mathbb{Z}/d\mathbb{Z}} \operatorname{Spec} R$, so a map $(\mathbb{Z}/d\mathbb{Z})_R \xrightarrow{\Phi} \mathcal{E}$ corresponds to an assignment of an element of $\mathcal{E}(R)$ for each $a \in \mathbb{Z}/d\mathbb{Z}$. We choose this element to be aP. The fact that $dP = 0$ implies that this is a map of group schemes over R.)

Let G be the scheme theoretic image of Φ. It is the smallest closed subscheme through which Φ factors. The subscheme G is $\mathbb{Z}_{(p)}$-flat since $\mathbb{Z}_{(p)}$ is Dedekind and Φ has flat source, so by the subgroup property of the generic fiber it follows (as will be discussed by Melanie) that the scheme-theoretic image is a subgroup scheme. Furthermore, $(\mathbb{Z}/d\mathbb{Z})_R$ is proper over R and $\mathcal{E}$ is separated over R. Together these imply that G is the image of Φ topologically and is a finite flat group scheme over R of order d, and $G_{\mathbb{Q}} \simeq (\mathbb{Z}/d\mathbb{Z})_{\mathbb{Q}}$.

Recall that by assumption, P reduces to the origin of the special fiber. The same is therefore true of all multiples, so G is local. In particular this implies that the prime power d must be a power of p, since otherwise d is a unit in R and the special fiber of G would be étale. By Lemma 1, a finite flat local group scheme over $R = \mathbb{Z}_{(p)}$ with $G_{\mathbb{Q}} \simeq (\mathbb{Z}/d\mathbb{Z})_{\mathbb{Q}}$ can only occur when $d = p = 2$ and $G \simeq (\mu_2)_R$. Therefore, we find that the order N of our original point Q must be 2. However, $(x, y) \in E[2](\mathbb{Q})$ if and only if $y = 0$ and $x^3 + Ax^2 + Bx + C = 0$ with $x \in \mathbb{Q}$. But then in fact $x \in \mathbb{Z}$. □

We now mention a curious open problem, based on the following theorem of Deligne (a proof of which is given in the Oort–Tate paper).

Theorem 2 (Deligne)**.** *If G is a finite flat commutative group scheme of order n over a locally noetherian scheme S, then G is killed by its order ($[n] = \epsilon \circ \pi : G \to G$).*

The analogue for G non-commutative is not known, except in the case $S = \operatorname{Spec} k$, or $S = \operatorname{Spec} k[\varepsilon]/(\varepsilon^2)$ by work of René Schoof.

Finite étale group schemes.

Definition 5. Let S be a locally Noetherian scheme. A morphism $Y \to S$ is finite étale if it is finite, flat and unramified, i.e. for all $s \in S$, the fiber $Y_s = \operatorname{Spec} A_s$ for a separable algebra $A_s/k(s)$, where $k(s)$ is the residue field at s. ($A_s \simeq \prod k_i$, k_i finite separable field extension of $k(s)$.)

Say $S = \operatorname{Spec} k$. Let $\pi = Gal(k^{\mathrm{sep}}/k)$. A π-set is a set M on which π acts with open stabilizers. (So a finite π-set is a finite set M on which π acts through a finite discrete quotient.) Define a functor

$$\{\text{finite étale } k\text{-schemes}\} \longrightarrow \{\text{finite } \pi\text{-sets}\}$$
$$X = \operatorname{Spec} A \longmapsto X(k^{\mathrm{sep}}) = \operatorname{Hom}_k(A, k^{\mathrm{sep}})$$

with $\sigma \in \pi$ acting on $f : A \to k^{\mathrm{sep}}$ by $(\sigma f)(a) = \sigma(f(a))$. (In the reverse direction $Y \mapsto \operatorname{Map}_\pi(Y, k^{\mathrm{sep}})$.) These functors induce an equivalence of categories

that restricts to an equivalence of categories between the category of finite étale commutative k-group schemes and finite π-modules.

More generally we get an equivalence of categories between the category of finite étale S-schemes and the category of finite $\pi_1(S,\alpha)$-sets, where α is some geometric point of S. ($\pi_1(S,\alpha) :=$ group of automorphisms of the functor $Y \longmapsto Y(\alpha)$ from (f. ét sch $/S$) $\to$ (Sets). So $\sigma \in \pi_1(S,\alpha)$ is a permutation σ_Y of $Y(\alpha)$ for all Y that are functorial, i.e. given $Y \to Y'$, the diagram

$$\begin{array}{ccc} Y(\alpha) & \longrightarrow & Y'(\alpha) \\ \Big\downarrow{\scriptstyle \sigma_Y} & & \Big\downarrow{\scriptstyle \sigma'_Y} \\ Y(\alpha) & \longrightarrow & Y'(\alpha) \end{array}$$

commutes.) The functor giving this equivalence of categories is just $Y \mapsto Y(\alpha)$. Again, this equivalence restricts to an equivalence between the categories of finite étale commutative S-group schemes and finite $\pi_1(S,\alpha)$-modules.