Recall that our goal is to prove the following result.

Theorem 1. *Let (E, p) be a pair as in the following table.*[1]

E	p
$\mathbb{Q}$	$3, 5, 7, 11, 13, 17$
$\mathbb{Q}(\sqrt{-1})$	$3, 5, 7$
$\mathbb{Q}(\sqrt{-3})$	$5, 7$

Let Γ be a finite flat commutative group scheme over Ø_E of p-power order. Then, one of the following possibilities holds.

(1) *Γ is a constant group scheme.*

(2) *Γ is a diagonalizable group scheme.*

(3) *Γ splits as a direct product of a nontrivial constant group scheme and a nontrivial diagonalizable group scheme.*

Our aim is essentially to prove a structure theorem for finite flat commutative group schemes "with everywhere good reduction" in the sense that they extend from the generic fiber to the ring of integers. Such objects will turn out to be "low degree" in a certain precise sense.[2]

Before we get into the proof, we will for the sake of convenience introduce some notation and recall a few key facts. Given $A \in \mathsf{CRing}$ and p prime, let $\mathcal{C}(A)$ denote the category of finite flat commutative group schemes over A, $\mathcal{C}_p(A) \subseteq \mathcal{C}(A)$ the full subcategory of objects with p-power order, and $\mathcal{C}[p^\infty](A) \subseteq \mathcal{C}(A)$ the full subcategory of objects killed by a p-power.[3] Given $n \geq 1$, we have $\mathcal{C}(p^n, A) \subseteq \mathcal{C}_p(A)$ and $\mathcal{C}[p^n](A) \subseteq \mathcal{C}[p^\infty](A)$ the "p^n parts" defined as expected. What do we know about these categories?

- $\mathcal{C}(A)$ embeds fully faithfully into the abelian category of fppf sheaves over $\operatorname{Spec} A$, with objects in the former category realized as certain representable objects in the latter category.
- $\mathcal{C}(k)$ is an abelian category for k a field and $\mathcal{C}_p(k), \mathcal{C}[p^\infty](k)$ are full abelian subcategories with abelian structure compatible with the abelian fppf sheaf structure. Moreover, if k is algebraically closed of characteristic $p > 0$, then the only simple objects in $\mathcal{C}(k)$ are μ_p, $\underline{\mathbb{Z}/p}$, α_p, and $\underline{\mathbb{Z}/l}$ for $l \neq p$ prime.
- $\mathcal{C}_p(A) \subseteq \mathcal{C}[p^\infty](A)$ since every object in $\mathcal{C}(A)$ is killed by its order. Similarly, $\mathcal{C}(p^n, A) \subseteq \mathcal{C}[p^n](A)$ for every $n \geq 1$.
- Let R be a mixed characteristic $(0, p)$ DVR with fraction field K and (absolute) ramification index $v_K(p) < p - 1$. Then, the generic fiber functors

  $$\bullet_K : \mathcal{C}_p(R) \to \mathcal{C}_p(K)$$

  and

  $$\bullet_K : \mathcal{C}[p^\infty](R) \to \mathcal{C}[p^\infty](K)$$

[1] Note that $E/\mathbb{Q}$ is unramified at p for every such pair since the relevant absolute discriminants are $d_{\mathbb{Q}(\sqrt{-1})} = -4$ and $d_{\mathbb{Q}(\sqrt{-3})} = -3$.

[2] Generally speaking, "low degree" objects in an appropriate category with kernels and cokernels can be classified assuming we can identify all of the simple objects as well as all extensions of simple objects by simple objects.

[3] The notation for the last category is meant to evoke torsion.

are fully faithful with images stable under taking sub-objects and quotients.[4] The full faithfulness holds as well for the "p^n parts."

- Let R be a Henselian local ring. Then, certain nice extensions live in $\mathcal{C}(R)$ and have nice properties. In more detail,
  - an extension of a connected object by a connected object is connected;
  - an extension of an étale object by an étale object is étale;
  - an extension of a connected object by an étale object is trivial (i.e., given by a direct product).
- Let R be a Noetherian domain with $p \in R$ and p-adic completion $\widehat{R}$. Associated to $G \in \mathcal{C}(R)$ are the group schemes $G_{\widehat{R}} \in \mathcal{C}(\widehat{R})$ and $G_{R[1/p]} \in \mathcal{C}(R[1/p])$ that "see" all of G in a precise way.[5] More specifically, consider the category of triples (G_1, G_2, ψ) with $G_1 \in \mathcal{C}(\widehat{R})$, $G_2 \in \mathcal{C}(R[1/p])$, and $\psi : (G_1)_{\widehat{R}[1/p]} \xrightarrow{\sim} (G_2)_{\widehat{R}[1/p]}$ using the identification $(\widehat{R})[1/p] \cong (R[1/p])^{\wedge}_p$.[6] Then, the functor $G \mapsto (G_{\widehat{R}}, G_{R[1/p]}, \mathrm{id})$ is an equivalence of categories from $\mathcal{C}(R)$ to this category of triples.

Proof of Theorem 1. To begin, the category $\mathcal{C}_p(\varnothing_E)$ seems at first to be not so workable. The remedy for this is provided by the following result.

Proposition 2. *Let $F := E(\Gamma(\overline{E}))$.*

(a) *The extension F/E is unramified.*

(b) *Given $\mathfrak{p}$ a prime of F lying above p, $\mathcal{C}_p(\varnothing_E)$ embeds fully faithfully into $\mathcal{C}_p(\varnothing_{E_\mathfrak{p}})$.*

The advantage of this result is twofold. First, since F/E is unramified, $\mathcal{C}_p(\varnothing_{E_\mathfrak{p}})$ embeds fully faithfully via the generic fiber functor into the abelian category $\mathcal{C}_p(E_\mathfrak{p})$ and so we may identify $\mathcal{C}_p(\varnothing_{E_\mathfrak{p}})$ as a full abelian subcategory. Second, since $\mathcal{C}_p(\varnothing_E)$ embeds fully faithfully into $\mathcal{C}_p(\varnothing_{E_\mathfrak{p}})$, we may consider composition series for objects in $\mathcal{C}_p(\varnothing_E)$ in a very hands-on way. To that end, let

$$0 = \Gamma_0 \subsetneq \Gamma_1 \subsetneq \cdots \subsetneq \Gamma_{m-1} \subsetneq \Gamma_m = \Gamma$$

be a composition series for Γ. The idea is build Γ up from successive quotients associated to this series, which we can explicitly describe by the following proposition.

Proposition 3.

(a) *The only simple objects in $\mathcal{C}_p(\varnothing_E)$ are μ_p and $\underline{\mathbb{Z}/p}$.*

(b) $\mathrm{Ext}^1_{\varnothing_E}(\underline{\mathbb{Z}/p}, \mu_p) = 0$.

(c) *More generally,* $\mathrm{Ext}^1_{\varnothing_E}(G_e, G_c) = 0$ *for $G_c, G_e \in \mathcal{C}_p(\varnothing_E)$ with G_e étale and G_c connected.*

[4] This result of Raynaud is one key way in which ramification enters the picture for us.

[5] Intuition for this comes from the fact that $R[1/p]$ "knows about" R away from p while $\widehat{R}$ "knows about" R on an infinitesimal neighborhood of p, hence the two together should give a global picture.

[6] Note the implicit identification between "algebraic" and "topological" p-adic completion when both make sense.

The complement to this is something we noted previously, namely that $\mathrm{Ext}^1_{\emptyset_E}(\mu_p, \underline{Z/p}) = 0$. This holds because...

Suppose there exists $0 < i < m$ such that $\Gamma_i/\Gamma_{i-1} \cong \mu_p$ and $\Gamma_{i+1}/\Gamma_i \cong \underline{\mathbb{Z}/p}$. The extension

$$\begin{tikzcd} 0 \arrow[r] & \mu_p \arrow[r] & \Gamma_{i+1}/\Gamma_{i-1} \arrow[r] & \underline{\mathbb{Z}/p} \arrow[r] & 0 \end{tikzcd}$$

is trivial and so we can find $\Gamma'_i \leq \Gamma_{i+1}$ such that $\Gamma'_i/\Gamma_{i-1} \cong \mu_p$ and $\Gamma_{i+1}/\Gamma'_i \cong \underline{\mathbb{Z}/p}$. Replace Γ_i in the composition series by Γ'_i. Repeating this process sufficiently many times, we may assume there exists $0 < j < m$ such that

$$\Gamma_i/\Gamma_{i-1} \cong \begin{cases} \mu_p, & 0 < i \leq j, \\ \underline{\mathbb{Z}/p}, & j < i \leq m. \end{cases}$$

It follows that Γ/Γ_j is constant and Γ_j is diagonalizable, and hence that there is a splitting $\Gamma \cong \Gamma_j \times \Gamma/\Gamma_j$ since $\mathrm{Ext}^1_{\emptyset_E}(\Gamma/\Gamma_j, \Gamma_j) = 0$. □

The key, then, is really Proposition 3.

Proof of Proposition 3. The idea is to induct on $|G_e||G_c|$, which must be a power of p. The base case is $|G_e| = p = |G_c|$, in which case we necessarily have G_e, G_c simple and so $G_e \cong \underline{\mathbb{Z}/p}$ and $G_c \cong \mu_p$ from which we get the desired result. Now consider the case $|G_e| > p$. Then, we can find $G'_e \leq G_e$ such that $G'_e \cong \underline{\mathbb{Z}/p}$ and G_e/G'_e is nontrivial. We have an exact sequence

$$\begin{tikzcd} \mathrm{Hom}_{\emptyset_E}(\mathbb{Z}/p, G_c) \arrow[r] & \mathrm{Ext}^1_{\emptyset_E}(G_e/G'_e, G_c) \arrow[r] & \mathrm{Ext}^1_{\emptyset_E}(G_e, G_c) \arrow[r] & \mathrm{Ext}^1_{\emptyset_E}(\underline{\mathbb{Z}/p}, G_c) \end{tikzcd}$$

The second and fourth terms both vanish by the inductive hypothesis. The first term vanishes since any homomorphism from an étale group scheme to a connected group scheme factors through the reduction of the connected group scheme and so is trivial. It follows that $\mathrm{Ext}^1_{\emptyset_E}(G_e, G_c) = 0$ as desired. Similar reasoning applies to the case $|G_c| > p$.

(a)

(b)

(c)

□

Proposition 4. *Let (E, p) be as in the table, $\Gamma \in \mathcal{C}[p]$, and $F := E(\Gamma(\overline{E}))$. Then, ...*

Proof. By replacing Γ by $\Gamma \times \mu_p$ if necessary, we may arrange that Γ contains a closed subgroup isomorphic to μ_p and hence $E(\zeta_p) \subseteq F$. Furthermore, we may assume without loss of generality that $F/\mathbb{Q}$ is Galois.[7] Borrowing Oh's notation, let

$$\begin{aligned} n &:= [F:\mathbb{Q}] \\ n_0 &:= [F:E] \\ n_0' &:= [F:E(\zeta_p)] \\ a &:= [E:\mathbb{Q}] \in \{1,2\}, \end{aligned}$$

so that $n = an_0$ and $n_0 = (p-1)n_0'$. We have the following.

- $F/E(\zeta_p)$ is unramified away from p.
- $E(\zeta_p)$ has class number 1 and so is its own Hilbert class field – i.e., the maximal unramified abelian extension of $E(\zeta_p)$ is trivial.
- $E/\mathbb{Q}$ is unramified at p. This is simply because

$$\Delta_{E/\mathbb{Q}} = \begin{cases} 1, & E = \mathbb{Q}, \\ -4, & E = \mathbb{Q}(\sqrt{-1}), \\ -3, & E = \mathbb{Q}(\sqrt{-3}). \end{cases}$$

□

Proposition 5. *Let k be an algebraically closed field of odd prime characteristic p, $K := \mathrm{Frac}(W(k))$, and $\Gamma \in \mathcal{C}[p](W(k))$ containing a subgroup isomorphic to μ_p. Fix an algebraic closure $\overline{K}$ and let $L := K(\Gamma(\overline{K}))$. Then, one of the following holds.*

1. *L/K is cyclic of degree $p-1$ and there exist $r, s \in \mathbb{Z}$ such that $\Gamma \cong \mu_p^s \times (\underline{\mathbb{Z}/p})^r$*
2. *L/K has degree $p(p-1)$ and there exist $r, s \in \mathbb{Z}$ and a non-split short exact sequence*

$$0 \longrightarrow \mu_p^s \longrightarrow \Gamma \longrightarrow (\underline{\mathbb{Z}/p})^r \longrightarrow 0$$

3. *L/K is cyclic of degree $p^2 - 1$.*
4. *L/K has degree $\geq p^2(p-1)$.*

What's the idea of the proof? Since p is unramified in $W(k)$, the generic fiber functor $\mathcal{C}[p](W(k)) \to \mathcal{C}[p](K)$ is fully faithful. At the same time, $G \mapsto G(\overline{K})$ is an equivalence of categories from $\mathcal{C}[p](K)$ to the category of finitely generated $\mathbb{F}_p[G_K]$-modules, for G_K the absolute Galois group of K. Thus, we may think of Γ as an object of the latter category and explicitly use the nice structure of this category to analyze Jordan-Hölder decompositions of Γ.

[7] If $E \neq \mathbb{Q}$ then $E/\mathbb{Q}$ is quadratic and so $\mathrm{Gal}(E/\mathbb{Q})$ has generator σ of order 2. Replace Γ by $\Gamma \times \sigma(\Gamma)$ if necessary.