The goal of these notes is to prove Theorem 3.8 from the blueprint of the proof of Fermat's Last Theorem, which claims that a hardly ramified 3-adic representation is, up to semisiplification, $\chi_3 \oplus 1$. We will use a bunch of standard results about finite flat groups schemes and group representations, all known in the 1980s, together with Fontaine's ramification bound. We start by stating the preliminary results about finite flat group schemes, whcih for us will always be commutative.

Definition 1. Let R be a noetherian commutative ring. Let G', G, G'' be finite flat group schemes over R, and let $f : G' \to G$, $g : G \to G''$ be morphisms of finite flat group schemes. The sequence $0 \to G' \to G \to G'' \to 0$ is called a *short exact sequence* of finite flat group schemes, if g is faithfully flat, and f is a kernel of g, i.e., the following square is cartesian:

$$\begin{tikzcd}
G' \arrow[r] \arrow[d, "f"] & \mathrm{Spec} R \arrow[d, "e"'] \\
G \arrow[r, "g"] & G''
\end{tikzcd}$$

Proposition 1. *Let R be a noetherian commutative ring. Let G be a finite flat group scheme over R, and let G' be a closed and flat group subscheme of G. Then there exists a* quotient *G/G', i.e. a finite flat group scheme G'' over R which fits into the exact sequence $0 \to G' \to G \to G'' \to 0$.*

Proof. This follows from extremely general results on quotients from [1], so known in the 1960s. □

Proposition 2. *Let R be a henselian local ring, and let G be a finite flat group scheme. Then the connected component of the identity G^0 is a closed flat subscheme of G, and the quotient $G^{et} := G/G^0$ is etale over R;*

Proof. My go-to reference for this is [4, 3.7], but I'm sure it was known in the 1960s. □

Corollary 3. *Let R be a henselian local ring, and let $0 \to G' \to G \to G'' \to 0$ be an exact sequence of finite flat group schemes. Then*

1. *If G' and G'' are connected, then G is connected;*

2. *If G' and G'' are etale, then G is etale;*

3. *If G' is etale and G'' is connected, then the exact sequence splits: $G \cong G' \times G''$.*

Proposition 4. *Let R be complete DVR of generic characteristic 0 and residue characteristic p with absolute ramification index $e < p - 1$. Then:*

1. *Any finite flat group scheme ofer $\mathrm{Frac}(R)$ has, up to isomorphism, at most one prolongation to a finite flat group scheme over R;*

2. *The class of finite flat group schemes over* $\mathrm{Frac}(R)$ *which have a prolongation is closed under taking subgroup schemes and quotient group schemes. In particular, the category of finite flat group schemes over R is abelian.*

Proof. This is proved in English in §4 of [4], but originally due to Raynaud in the 1970s. □

Proposition 5. *(Fontaine's Ramification bound) Let K be a finite extension of $\mathbb{Q}_p$ with ramification index e. Let $n \geq 1$, and let $\rho : G_K \to GL_d(\Lambda)$ be a flat Galois representation, where Λ is a finite ring killed by p^n. Let L/K the field of invariants of the kernel of ρ. Then $v_{\mathcal{O}_L}(\mathfrak{D}_{L/K}) < e\Big(n + \frac{1}{p-1}\Big)$, where $\mathfrak{D}_{L/K}$ is the different of L/K.*

Proof. We will only use this for $K = \mathbb{Q}_3$, $n = 1$ and $d = 2$, in which case Richard gives a direct argument, but because this is Theoreme A from [3] (1985), we don't need to formalise it. □

Proposition 6. *If L/K is a tamely ramified extension of local fields of characteristic* 0 *with ramification index e, then $v_{\mathcal{O}_L}(\mathfrak{D}_{L/K}) = e - 1$.*

Proof. There is a chance this is mathlib already, but in any event this most likely dates back to the XIX century, so I wouldn't even bother tracking down the reference. □

Theorem 7. *Let $\bar{\rho} : G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{F}}_3)$ be a hardly ramified representation. Then $\bar{\rho}$ fits into an exact sequence $0 \to \bar{\chi}_3 \to \bar{\rho} \to 1 \to 0$.*

Proof. Let $L/\mathbb{Q}$ be the field of invariants of the kernel of $\bar{\rho}$. By definition of being hardly ramified, L is unramified away from 6. Moreover, the inertia group I_2 acts unipotently on $\bar{\mathbb{F}}_3^2$, therefore, $\bar{\rho}(I_2)$ is either trivial or a cyclic group of order 3. Let $N = [L : \mathbb{Q}]$, and let e_2, e_3 be the ramification indices of L above 2 and 3.

Case 1 : $\bar{\rho}$ is unramified at 2. Then by applying the bound from 5, we get $|\Delta_L|^{\frac{1}{N}} < 3^{\frac{3}{2}} < 5.2.$. Because $\det \bar{\rho} = \bar{\chi}_3$, we must have $\mathbb{Q}(\omega) \subset L$. Hence, L is totally complex, and the bound from [2] apply, giving us $[L : \mathbb{Q}] \leq 4$. It follows that $\mathrm{im}\ \bar{\rho}$ is abelian of order prime to 3, and therefore, $\bar{\rho} \cong \psi_1 \oplus \psi_2$, where, by assumption, $\psi_1, \psi_2 : G_{\mathbb{Q}} \to \bar{\mathbb{F}}_3^{\times}$ must be unramified away from 3 and $\psi_1\psi_2 = \bar{\chi}_3$. It follows easily from the Kronecker-Weber theorem that $\{\psi_1, \psi_2\} = \{1, \bar{\chi}_3\}$.

Case 2: $\bar{\rho}$ is ramified at 2. It follows that $L/\mathbb{Q}$ is tamely ramified above 2. Applying the bounds from 5 and 6, we get $|\Delta_L|^{\frac{1}{N}} < 2^{1-\frac{1}{e_2}} \cdot 3^{1+\frac{1}{2}} \leq 2^{\frac{2}{3}} 3^{\frac{3}{2}} < 8.25$, and this time [2] gives us $[L : \mathbb{Q}] \leq 16$. Because in this case $6 | [L : \mathbb{Q}]$, we have $[L : \mathbb{Q}] = 6$ or 12 and $[L : \mathbb{Q}(\omega)] = 3$ or 6. Let $\sigma \in G_{\mathbb{Q}(\omega)}$ be such that $\bar{\rho}(\sigma)$ is of order 3. Then $\mathrm{im}\ \bar{\rho}$ normalises the unipotent group of order 3 generated by $\bar{\rho}(\sigma)$, and therefore $\ker(1 - \bar{\rho}(\sigma))$ is a nontrivial subreprsentation. There are two more subcases:

Subcase 1: If $\bar{\rho}(\sigma)$ and $\bar{\rho}(\sigma^2)$ are conjugate, then pick $\tau \in G_{\mathbb{Q}}$ such that $\bar{\rho}(\tau\sigma\tau^{-1}) = \bar{\rho}(\sigma^2)$. One then easily computes that $\bar{\rho}(\tau)$ acts by -1 on $\ker(1 - \bar{\rho}(\sigma))$, hence, $\ker(1 - \bar{\rho}(\sigma)) = \bar{\chi}_3$ and the quotient in trivial.

Subcase 2: If $\bar{\rho}(\sigma)$ and $\bar{\rho}(\sigma^2)$ are not conjugate, then $\mathrm{im}\bar{\rho}$ is abelian. But it contains a unipotent element. so a calculation shows that the image has to consist of the matrices of the form $\begin{pmatrix} a(\sigma) & b(\sigma) \\ 0 & a(\sigma) \end{pmatrix}$, but this would require $a(\sigma)$ to be the square root of the cyclotomic character, which doesn't exist. □

Corollary 8. *There is no nontrivial extension of $\bar{\chi}_3$ by 1 in the category of hardly ramified Galois representations.*

Definition 2. Call a Galois module M *generalised hardly ramified*, if it is unramified outside 6, flat at 3, and for any $\sigma \in I_2$ we have $(\sigma - 1)^2$ acting trivially on M. By Raynaud's theorem, such modules form an abelian category.

Corollary 9. *Let $\rho : G_{\mathbb{Q}} \to GL_2(\mathcal{O})$ be a hardly ramified 3-adic representation, so that $\mathcal{O}$ is the ring of integers of a finite extension of $\mathbb{Q}_3$. Let π be the uniformiser of $\mathcal{O}$. Let $\bar{\rho}_k$ be the mod π^k reduction of ρ. Then all of the Jordan-Holder factors of $\bar{\rho}_k$ in the category of Galois $\mathcal{O}$-modules are isomorphic to either $\bar{\chi}_3$ or 1. Here I mean 1 as $\mathcal{O}/\pi$ with trivial Galois action.*

Proof. Using 4, express $\bar{\rho}_k$ inductively as an extension of a hardly ramified $\bar{\mathbb{F}}_3$-representations, and apply the theorem. □

Definition 3. Call a Galois-module *pseudo-constant* if it is an iterated extension of constant modules, and *pseudo-diagonalisable* if it is an iterated extension of diagonalisable modules.

Theorem 10. *Any generalised hardly ramified Galois module, which is an iterated extension of $\mathbb{Z}/3$'s and μ_3's is an extension of a pseudo-constant module by a pseudo-diagonalisable module.*

Proof. Let M be a generalised hardly ramified Galois module. Consider the Jordan-Holder series of $M : 0 = M_0 \subseteq \ldots M_n = M$. Assume that $M_i \subset M_{i+1} \subset M_{i+2}$ are such that M_{i+1}/M_i is contant, and M_{i+2}/M_{i+1} is diagonalisable. But then M_{i+2}/M is a product $\mathbb{Z}/3 \times \mu_3$, and so you can take $M'_{i+1} = M_1 \cdot \mu_3$ and continue. □

Theorem 11. *A pseudo-constant generalised hardly ramified module is constant, and a pseudo-diagonalisable hardly ramified module is diagonalisable.*

Proof. By Cartier duality, it suffices to prove the first statement. So let M be a pseudo-constant module. By 3, if you base change M to $\mathbb{Z}_3$, then M is etale, therefore the action of the Galois group on M is unramified at 3, and tamely ramified at 2. We also know that the image of the Galois action must be a 3-group. But it easilt follows from the Kronecker-Weber theorem that there is no degree 3^i extension which is unramified except at 2 and tamely ramified at 2. □

Theorem 12. *Let $\rho[3^k] : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}/3^k)$ be a hardly ramified representation. Then $\rho[3^k]$ fits into an exact sequence $\mu_{3^k} \to \rho[3^k] \to \mathbb{Z}/3^k \to 0$.*

Proof. Induction on k. If $k = 1$, this is the previous theorem. In general, apply the induction assumption to the subrepresentation $\rho[3^{k-1}]$ of $\rho[3^k]$, which is annihilated by 3^{k-1}, giving an inclusion $\mu_{3^{k-1}} \to \rho[3^{k-1}] \to \rho[3^k]$. The quotient $\rho[3^k]/\rho[3^{k-1}]$ is also hardly ramified and killed by 3, so by the previous theorem there is an embedding of μ_3 into this quotient. We can move it around in the Jordan-Holder series to get an extension $\mu_{3^{k-1}} \to H \to \mu_3$, which is diagonalisable. If it splits, then we have an embedding $\mu_3 \times \mu_3 \to \rho[3]$, which must be an isomorphism. But this contradicts the $k = 1$ case. Hence, H is not split, and therefore, $H \cong \mu_{3^k}$. □

References

[1] M. Demazure, A. Grothendieck, SGA 3, Tome 1 (Proprietes Generales des schemas en groupes), 1962/64

[2] G. Poitou Sur les petits discriminants, Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 18, no 1 (1976-1977),exp. no 6, p. 1-17

[3] J.-M. Fontaine, Il n'y a pas de variete abelienne sur $\mathbb{Z}$, Inventiones mathematicae 81, 515-538 (1985)

[4] J. Tate, Finite flat group schemes, in : G. Cornell, J. H. Silverman, G. Stevens, Modular Forms and Fermat's Last Theorem, 1995