Group schemes over the integers and Galois representations

No Theory 5/15/2025
Casimir Kothari

In this talk I will discuss group schemes over $\mathbb{Z}$ and the relationship to Galois representations. The goal is to illustrate the interactions between integral questions about group schemes and phenomena in Galois representations. As this subject can get rather technical, I won't give many details/complete proofs.

Much of the material in the second half of the talk is from [Sch], [Se87].

1 Finite Flat Group Schemes over $\mathbb{Z}$

Definition 1.1. A finite flat commutative group scheme over a ring R is an R-scheme $G = \operatorname{Spec} A$ with a commutative group structure, such that A is finite flat as an R-module.

Throughout this talk, whenever I say group scheme I really mean finite flat commutative group scheme.

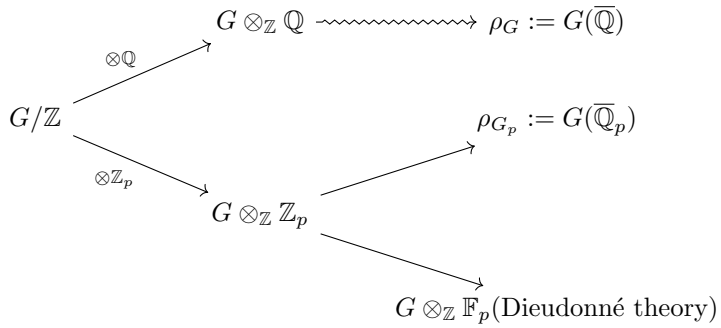
Our cases of interest: $R = \mathbb{Z}, \mathbb{Z}_p, \mathbb{Q}, \mathbb{Q}_p$, in which case the "finite flat" condition just means A is free of rank n over R for some integer n. n is called the order of the group scheme G. This order behaves as one would expect, and in particular we have e.g. that if $H \subset G$ is a subgroup scheme, then the order of H divides the order of G.

Example 1.2. The following two group schemes of order p will be our friends for the duration of the talk:

$\mathbb{Z}/p\mathbb{Z}$ is the constant group scheme associated to $\mathbb{Z}/p\mathbb{Z}$. Concretely it is the disjoint union of p copies of $\operatorname{Spec}\mathbb{Z}$ with the group law of $\mathbb{Z}/p\mathbb{Z}$, while the functor of points description is as the constant sheaf associated to $\mathbb{Z}/p\mathbb{Z}$.

μ_p is the p-th roots of unity group scheme, defined by $\mu_p(A) = \{a \in A : a^p = 1\}$ for any ring A. Concretely it is given by $\operatorname{Spec}\mathbb{Z}[x]/(x^p - 1)$, which exhibits it as a finite flat group scheme over $\mathbb{Z}$.

Let's think about what sort of data is encapsulated by a finite flat group scheme $G/\operatorname{Spec}\mathbb{Z}$. Base changing, we get a family of group schemes indexed by the places of $\mathbb{Z}$:



1.1 Interlude: A dictionary between Étale group schemes and Galois representations

Recall: a group scheme G/R is étale if G is étale (equivalently, smooth) as an R-scheme. For example, $\mathbb{Z}/p\mathbb{Z}$ is étale over $\mathbb{Z}$ but μ_p is not, since modulo p, μ_p is non-reduced owing to the equation $x^p - 1 = (x-1)^p$ in characteristic p.

Recall also that a Galois module for $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is unramified at a prime p if inertia at p acts trivially. Similarly we can speak of unramified representations of the absolute Galois group of number fields and local fields.

Here is a summary of some facts concerning étale group schemes and Galois representations.

1. Invertible order $\implies$ étale: If G/R has order n and n is a unit in the ring R, then G is étale.

   For example, any group scheme is étale over a field of characteristic 0, any p-group is étale over $\mathbb{Z}[1/p]$, and any ℓ-group for $\ell \neq p$ is étale over $\mathbb{Z}_p$.

2. Suppose that K is a field of characteristic 0 (e.g. number field or finite extension of $\mathbb{Q}_p$). Then a finite group scheme G/K yields a finite abelian group $G(\overline{K})$ with a continuous action of $\mathrm{Gal}(\overline{K}/K)$, and this association is an equivalence between group schemes over K and finite $\mathrm{Gal}(\overline{K}/K)$-modules.

   For example, group schemes over an algebraically closed field of characteristic zero are equivalent to finite abelian groups: every such group scheme is constant.

3. Suppose that K is a number field or finite extension of $\mathbb{Q}_p$. Then via the above functor, étale group schemes over $\mathcal{O}_K$ are equivalent to finite $\mathrm{Gal}(\overline{K}/K)$-modules which are everywhere unramified. This last condition can be understood in terms of field theory: adjoining the points of $G(\overline{K})$ to $\mathbb{Q}$ or $\mathbb{Q}_p$ produces a finite Galois extension, and the module $G(\overline{K})$ is unramified if and only if this extension is.

   By Minkowski's theorem, we see in particular that any étale group scheme over $\mathbb{Z}$ is constant, i.e. the associated Galois module has the trivial Galois action.

4. More generally, étale group schemes over $\mathcal{O}_K[1/p]$ are equivalent to finite $\mathrm{Gal}(\overline{K}/K)$-modules which are unramified outside of the primes of K dividing p.

Combining 1 and 4, we obtain:

Corollary 1.3. Suppose $G/\mathbb{Z}$ has order n. Then the Galois module $G(\overline{\mathbb{Q}})$ is unramified outside of the primes dividing n.

Returning to our picture above, let us say a bit about each of the branches in the diagram.

1.2 Group Schemes over $\mathbb{Q}$

By the above, finite group schemes over $\mathbb{Q}$ are equivalent to finite $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules.

Example 1.4. Over $\mathbb{Q}$, the group scheme $\mathbb{Z}/p\mathbb{Z}$ corresponds to the group $\mathbb{Z}/p\mathbb{Z}$ with the trivial Galois action: this is the trivial character $1 : G_{\mathbb{Q}} \to \mathbb{F}_p^\times$.

The group scheme μ_p corresponds to the group $\mathbb{Z}/p\mathbb{Z}$ with the cyclotomic Galois action (i.e. the cyclotomic character $\omega : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to (\mathbb{Z}/p\mathbb{Z})^\times$). Recall that this is the character that sends $\sigma \mapsto a$ where $\sigma(\zeta_p) = \zeta_p^a$.

1.3 Group Schemes over $\mathbb{Z}_p$

Suppose $G/\mathbb{Z}_p$ is a finite flat group scheme. Then we obtain a group scheme $G \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ over $\mathbb{Q}_p$ and a group scheme $G \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ over $\mathbb{F}_p$. As with the situation over $\mathbb{Q}$, the former is equivalent to the corresponding $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-module, while the latter can be understood e.g. with Dieudonné theory.

Let's explain explicitly what the situation is in a few cases.

Example 1.5 (Group Schemes of prime order $\ell \neq p$)**.** Suppose $G/\mathbb{Z}_p$ has order ℓ. Then G is étale, and the association $G \mapsto G(\overline{\mathbb{Q}}_p)$ defines an equivalence between group schemes over $\mathbb{Z}_p$ of order ℓ and unramified characters $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to (\mathbb{Z}/\ell\mathbb{Z})^\times$. Since χ is unramified, it factors through the maximal unramified quotient $\hat{\mathbb{Z}}$, and thus there are $\ell - 1$ group schemes of order ℓ over $\mathbb{Z}_p$, corresponding to $\ell - 1$ different twisted forms of the constant group scheme $\mathbb{Z}/\ell\mathbb{Z}$, or equivalently the powers of the mod ℓ cyclotomic character.

Example 1.6 (Group Schemes of order p)**.** First, étale group schemes of order p correspond to unramified characters $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathbb{F}_p^\times$. Since they are unramified, they factor through $\mathrm{Gal}(\mathbb{Q}_p^{ur}/\mathbb{Q}_p) = \hat{\mathbb{Z}}$, and hence we obtain $p-1$ étale group schemes of order p over $\mathbb{Z}_p$. These are twisted forms of $\mathbb{Z}/p\mathbb{Z}$, and they become isomorphic to $\mathbb{Z}/p\mathbb{Z}$ after extending the base to the ring of integers of the unramified extension of $\mathbb{Q}_p$ of degree $p-1$.

Cartier duality gives us $p-1$ connected group schemes (the twisted forms of μ_p, or equivalently the Cartier duals of the étale group schemes constructed above). By the classification result of Oort-Tate [OT], it turns out that these are all the group schemes of order p over $\mathbb{Z}_p$.

2 Tate's question

Let us return to the setting of finite flat group schemes over $\mathbb{Z}$. We say that such a group scheme is simple if it has no nontrivial subgroup schemes.

Fact: $G/\mathbb{Z}$ is simple if and only if the associated Galois module $G(\overline{\mathbb{Q}})$ is simple as a Galois module (take scheme theoretic closure of sub-module on the generic fiber).

By the group scheme version of Lagrange's theorem, any group scheme of prime order p over $\mathbb{Z}$ is simple. Moreover, the aformentioned work of Oort-Tate [OT] also tells us that the only group schemes of order p over $\mathbb{Z}$ are μ_p and $\mathbb{Z}/p\mathbb{Z}$. Motivated by this, we arrive at the following question:

Question 2.1 (Tate, 1966)**.** Are $\mu_p, \mathbb{Z}/p\mathbb{Z}$ for p prime the only simple group schemes over $\mathbb{Z}$?

The question is completely open, and there doesn't seem to be a consensus as to what the answer should be. It has the same flavor as Minkowski's theorem about $\mathbb{Q}$ having no unramified extensions, or the Abrashkin-Fontaine theorem that there are no abelian schemes over $\mathbb{Z}$.

Theorem 2.2 (Abrashkin, Fontaine, Schoof-Dembélé)**.** For every prime $p \leq 19$, the only simple p-power order finite flat group schemes over $\mathbb{Z}$ are $\mathbb{Z}/p\mathbb{Z}$ and μ_p. Assuming GRH, we can extend this to $p \leq 37$.

The goal for the remainder of the talk will be to sketch the following result.

Theorem 2.3. Suppose $G/\mathbb{Z}$ is a finite flat group scheme of order p^2. Then G is not simple.

3 Detour: Serre's conjecture

Recall the following construction:

Theorem 3.1 (Deligne)**.** Suppose f is a normalized cusp form of weight k on $\Gamma_0(N)$, which is an eigenform for the all Hecke operators $T_n, n \geq 1$, and let p be a prime not dividing N. Then there exists a continuous representation $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Z}}_p)$ characterized up to conjugation by the following properties:

1. For all primes $\ell \nmid pN$, ρ_f is unramified at ℓ;
2. We have $\mathrm{tr}(\rho_f(\mathrm{Frob}_\ell)) = a_\ell$ and $\det(\rho_f(\mathrm{Frob}_\ell)) = l^{k-1}$.

Moreover ρ_f is odd (i.e. the determinant of complex conjugation is -1) and irreducible.

Reducing mod p, we obtain a representation $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$.

Conjecture 3.2 (Serre, 1972-1987)**.** Every continuous odd irreducible $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ is modular, i.e. arises via the above construction for some eigenform $f \in S_k(\Gamma_0(N))$.

Serre's conjecture even predicted the exact weight, level, and nebentypus character of f. It was proven by Khare, Khare-Wintenberger (2005, 2008). The version relevant to us will be the following:

Theorem 3.3 (Khare, Khare-Wintenberger, Serre)**.** Serre's conjecture is true. Suppose that $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$, and let f be the associated cusp form. Then we moreover have:

1. The weight of f is 2 if and only if the following two conditions are satisfied:

(a) $\det(\rho)|_{I_p}$ is equal to the mod p cyclotomic character $\omega : I_p \to \mathbb{F}_p^\times$.

(b) The restriction $\rho|_p$ of ρ to $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ is finite flat, i.e. there exists a finite flat group scheme $G/\mathbb{Z}_p$ of order p^2 killed by p such that ρ_p is the Galois representation $G \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

2. The level of f measures the ramification of ρ at primes not equal to p. In particular, f has level 1 if and only if ρ is unramified at all $\ell \neq p$.

4 Simple group schemes cannot have order p^2

Suppose that $G/\mathbb{Z}$ is order p^2 and simple. Then G is killed by p, or $\ker(p : G \to G)$ would be a subgroup of order p. Thus the Galois module associated to G is a continuous representation $\rho = \rho_G : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$, which has the following properties:

1. ρ is unramified away from p (G is a p-group).

2. ρ is irreducible (G is simple)

Lemma 4.1. We have that $\det(\rho) : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_p^\times$ is of the form ω^i for some $0 \leq i < p-1$, where ω is the mod p cyclotomic character.

Proof. Since $\mathbb{F}_p^\times$ is abelian, $\det(\rho)$ factors through $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$. Since moreover it is unramified away from p, it factors through the Galois group of the maximal abelian extension of $\mathbb{Q}$ unramified away from p. By the Kronecker-Weber theorem, this is $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$. So the kernel of $\det(\rho)$ contains $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty}/\mathbb{Q}(\zeta_p)))$, and so $\det(\rho)$ factors through $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, and thus we get a power of the mod p cyclotomic character. □

We claim that in fact $\det(\rho) = \omega$. For this we begin with a lemma that allows us to work locally at p:

Lemma 4.2. Let $K/\mathbb{Q}_p$ be a finite unramified extension. Then if $\det(\rho)|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/K)} = \omega$, then $\det(\rho) = \omega$.

Proof. The statement says that the composition $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K) \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is a surjection. But K is unramified and hence $K \cap \mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p$, and it follows that $[K(\zeta_p) : \mathbb{Q}_p] = [K : \mathbb{Q}_p](p-1)$ and hence $[K(\zeta_p) : K] = p-1$, and we obtain the desired surjection. □

So, we can compute $\det(\rho)$ by working locally at p. Let $G_p := G \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Then there are two possibilities:

1. G_p is not simple over $\mathbb{Z}_p$: In this case there is a short exact sequence

$$0 \to A \to G_p \to B \to 0$$

with A and B order p. But we know from the Oort-Tate classification that A and B are twisted forms of μ_p or $\mathbb{Z}/p\mathbb{Z}$, and so after extending scalars to the ring of integers of an unramified extension of $\mathbb{Q}_p$, we may assume that $A, B \in \{\mathbb{Z}/p\mathbb{Z}, \mu_p\}$. So there are four possibilities for our extension structure of G.

First, we can rule out two possibilities. Indeed, I claim that we cannot have $A = B$. For instance if $A = B = \mathbb{Z}/p\mathbb{Z}$, then G_p is an extension of $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{Z}/p\mathbb{Z}$, and hence étale over $\mathbb{Z}_p$. But then G would be étale over $\mathbb{Z}$, hence constant and therefore reducible. Similarly we can rule out $A = B = \mu_p$ as then we can apply the same argument to the Cartier dual of G_p.

So it follows that G_p is an extension of μ_p by $\mathbb{Z}/p\mathbb{Z}$, or of $\mathbb{Z}/p\mathbb{Z}$ by μ_p. Recalling that over $\mathbb{Q}_p$, the representation associated to μ_p is ω while the representation associated to $\mathbb{Z}/p\mathbb{Z}$ is 1, we find that the representation associated to G_p takes the form

$$\rho_{G_p} : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}_2(\mathbb{F}_p) = \begin{pmatrix} 1 & * \\ 0 & \omega \end{pmatrix} \text{ or } \begin{pmatrix} \omega & * \\ 0 & 1 \end{pmatrix}.$$

In either case, we find $\det \rho_{G_p} = \omega$, as desired.

2. G_p is simple over $\mathbb{Z}_p$. Raynaud carried out a generalization of the Oort-Tate theorem to so-called F-vector space schemes, and one consequence of his theory is that $\det(\rho_{G_p}) = \omega$ in this case as well. This is very related to the weight 2 statement of Serre's conjecture. Unfortunately the results are too technical to get into in this talk.

So $\det(\rho) = \omega$. But ω(complex conjugation)$= -1$, and so ρ is odd. So ρ is continuous, odd, and irreducible, and hence modular by Serre's conjecture.

Let f be the associated modular form. Since ρ has cyclotomic determinant and is finite flat, f has weight 2. Since ρ is unramified away from p, f has level 1. But there are no cusp forms of weight 2 and level 1: the modular curve of level 1 is $\mathbb{P}^1$, which has genus 0! This contradiction tells us that our simple $G/\mathbb{Z}$ of order p^2 cannot exist, and we are done!

References

[Sch] René Schoof. Finite Flat Group Schemes over the integers (Youtube Talk, Link)

[Se87] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbb{Q}}/\mathbb{Q}$). Duke 54 (1987).

[OT] Oort, Tate. Group Schemes of Prime Order, 1970.