Author(s): Andrew Snowden

Attribution Key

for more information see: http://open.umich.edu/wiki/AttributionPolicy

Use + Share + Adapt

{ Content the copyright holder, author, or law permits you to use, share and adapt. }

PD-GOV **Public Domain – Government**: Works that are produced by the U.S. Government. (17 USC § 105)

PD-EXP **Public Domain – Expired**: Works that are no longer protected due to an expired copyright term.

PD-SELF **Public Domain – Self Dedicated**: Works that a copyright holder has dedicated to the public domain.

ZERO **Creative Commons – Zero Waiver**

BY **Creative Commons – Attribution License**

BY-SA **Creative Commons – Attribution Share Alike License**

BY-NC **Creative Commons – Attribution Noncommercial License**

BY-NC-SA **Creative Commons – Attribution Noncommercial Share Alike License**

GNU-FDL **GNU – Free Documentation License**

Make Your Own Assessment

{ Content Open.Michigan believes can be used, shared, and adapted because it is ineligible for copyright. }

PD-INEL **Public Domain – Ineligible**: Works that are ineligible for copyright protection in the U.S. (17 USC § 102(b)) *laws in your jurisdiction may differ

{ Content Open.Michigan has used under a Fair Use determination. }

FAIR USE **Fair Use**: Use of works that is determined to be Fair consistent with the U.S. Copyright Act. (17 USC § 107) *laws in your jurisdiction may differ

Our determination **DOES NOT** mean that all uses of this 3rd-party content are Fair Uses and we **DO NOT** guarantee that your use of the content is Fair.

To use this content you should **do your own independent analysis** to determine whether or not your use will be Fair.

Lecture 5: Group schemes 1

This is the first of three lectures on group schemes. I begin by introducing the idea of a group object in a category. I then define what a group scheme is, and explain the connection to Hopf algebras. This is followed by several important examples. For the rest of the lecture, I focus on finite commutative group schemes over fields, and cover most of the basic facts (existence of quotients, classification in the tale case, the connected–étale sequence, etc.).

A good reference for today is Tate's article "Finite flat group schemes" in the book "Modular forms and Fermat's last theorem" (MR1638478).

1 Group objects in a category

1.1 Group objects

Let $\mathcal{C}$ be a category with all finite products; denote the final object by pt. A group object in $\mathcal{C}$ is a tuple (G, m, i, e), where:

- G is an object of $\mathcal{C}$;
- m is a map $G \times G \to G$, the multiplication map;
- i is a map $G \to G$, the inversion map; and
- e is a map $\mathrm{pt} \to G$, the identity section (or identity element),

such that the usual axioms of group theory hold:

- Associativity: the following diagram commutes:

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{m \times \mathrm{id}} & G \times G \\ \downarrow{\scriptstyle \mathrm{id} \times m} & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{m} & G \end{array}$$

- Identity element: the following composition is equal to the identity:

$$G = G \times \mathrm{pt} \xrightarrow{\mathrm{id} \times e} G \times G \xrightarrow{m} G$$

  And similarly if $\mathrm{id} \times e$ is changed to $e \times \mathrm{id}$.

- Inverses: the following diagram commutes:

$$\begin{array}{ccc} G & \xrightarrow{\mathrm{id} \times i} & G \times G \\ \downarrow & & \downarrow{\scriptstyle m} \\ \mathrm{pt} & \xrightarrow{e} & G \end{array}$$

  And similarly if $\mathrm{id} \times i$ is changed to $i \times \mathrm{id}$.

These are notes for Math 679, taught in the Fall 2013 semester at the University of Michigan by Andrew Snowden.

We say that a group object G is commutative if the following diagram commutes:

$$\begin{array}{ccc} G \times G & \xrightarrow{\tau} & G \times G \\ {\scriptstyle m}\downarrow & & \downarrow{\scriptstyle m} \\ G & = & G \end{array}$$

Here τ is the switching-of-factors map.

Suppose G and H are group objects. A homomorphism from G to H is a morphism $G \to H$ in $\mathcal{C}$ such that all the relevant diagrams commute. In this way, there is a category of group objects in $\mathcal{C}$.

Example 1. An abelian variety is, by definition, a group object in the category of complete varieties. □

1.2 Functor of points

Let X be an object of $\mathcal{C}$. For an object Y of $\mathcal{C}$, let $h_X(Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X)$. Then h_X defines a contravariant functor from $\mathcal{C}$ to the category of sets. Yoneda's lemma says that X is determined from h_X, in a precise sense.

Suppose G is a group object of $\mathcal{C}$. One then verifies that $h_G(Y)$ inherits the structure of a group; for example, the multiplication map $h_G(Y) \times h_G(Y) \to h_G(Y)$ is induced from m. Furthermore, if $f\colon Y \to Y'$ is a morphism in $\mathcal{C}$, then the induced map $f^*\colon h_G(Y') \to h_G(Y)$ is a group homomorphism. Conversely, if G is an object of $\mathcal{C}$ such that each $h_G(Y)$ is endowed with the structure of a group and each f^* is a group homomorphism then G naturally has the structure of a group object of $\mathcal{C}$. In other words, giving G a group structure is the same as lifting h_G to a functor from $\mathcal{C}$ to the category of groups. Said yet again, the Yoneda embedding is an equivalence between group objects in $\mathcal{C}$ and group objects in the functor category $\mathrm{Fun}(\mathcal{C}, \mathrm{Set})$ which are representable. This point of view allows one to define group objects even if $\mathcal{C}$ doesn't have finite products.

The group object G is commutative if and only if $h_G(Y)$ is commutative for all Y.

1.3 Kernels and cokernels

The category of group objects in $\mathcal{C}$ has a zero object 1, namely the object pt endowed with its unique group structure. One therefore has a definition for kernel and cokernel of a map of group objects, namely fiber (co)product with the zero object (if it exists).

Let $f\colon G \to H$ be a homomorphism of group objects. Since $\ker(f)$ is defined by what maps to it look like, one has a good description of its functor of points: $(\ker f)(T)$ is equal to the kernel of the map $f\colon G(T) \to H(T)$. In contrast, $\mathrm{coker}(f)$ is defined by what maps out of it look like, and so its functor of points does not admit an easy description in general. In particular, it is not true that $(\mathrm{coker}\, f)(T)$ is the cokernel of $f\colon G(T) \to H(T)$.

2 Group schemes

2.1 The connection with Hopf algebras

Fix a field k. The category of affine schemes over k is anti-equivalent to the category of k-algebras. One therefore finds that an affine group scheme G over k correspond to a k-algebra A equipped with all the structure of a group object, but with the arrows going in the opposite direction:

- The multiplication map $G \times G \to G$ turns into a comultiplication map $A \to A \otimes A$.
- The inversion map $G \to G$ turns into the antipode map $A \to A$.
- The identity section $\mathrm{pt} \to G$ turns into the counit $A \to k$.
- One can furthermore translate the group axioms: for example, associativity of G means the comultiplication on A is coassociative.

A (commutative) k-algebra A equipped with a comultiplication, counit, and antipode satisfying then necessary axioms is called a (commutative) Hopf algebra. It is revealing to think of a Hopf algebra not as an algebra with comultiplication, counit, and antipode, but as a vector space with multiplication, unit, comultiplication, counit, and antipode. In this way, the data becomes completely symmetric with respecting to flipping all the arrows.

2.2 Examples

In what follows, we write $T = \mathrm{Spec}(R)$ for a test scheme.

- The additive group. Let $\mathbf{G}_a = \mathrm{Spec}(k[t])$. We have $\mathrm{Hom}(T, \mathbf{G}_a) = R$. Regarding R as an additive group, this shows that $\mathbf{G}_a$ naturally has the structure of a commutative group scheme. It is called the additive group. The comultiplication on $k[t]$ is given by $t \mapsto t \otimes 1 + 1 \otimes t$.
- The multiplicative group. Let $\mathbf{G}_m = \mathrm{Spec}(k[t, t^{-1}])$. We have $\mathrm{Hom}(T, \mathbf{G}_m) = R^\times$, the group of units in R. Again, this shows that $\mathbf{G}_m$ naturally has the structure of a commutative group scheme. The comultiplication is given by $t \mapsto t \otimes t$.
- The constant group. Let Γ_0 be an ordinary group. Let Γ be the disjoint union of $\mathrm{Spec}(k)$'s indexed by Γ_0. We have $\mathrm{Hom}(T, \Gamma) = \mathrm{Hom}(\pi_0(T), \Gamma_0)$, which is a group; therefore Γ is a group scheme, which we call the constant group scheme on Γ_0. In fact, $\Gamma = \mathrm{Spec}(A)$, where A is the ring of functions $\Gamma_0 \to k$. We can identify $A \otimes A$ with the ring of functions $\Gamma_0 \times \Gamma_0 \to k$, and then comultiplication takes a function f to the function $(x, y) \mapsto f(xy)$. In the future, we do not notationally distinguish between Γ and Γ_0.
- Roots of unity. Let $\mu_n = \mathrm{Spec}(k[t]/(t^n - 1))$. We have that $\mathrm{Hom}(T, \mu_n)$ is equal to the set of elements $x \in R$ such that $x^n = 1$. This is obviously a commutative group under multiplication, and so μ_n is a commutative group scheme. It is the kernel of the multiplication-by-n map on $\mathbf{G}_m$.
- The group scheme α_p. Assume k has characteristic p. Let $\alpha_p = \mathrm{Spec}(k[t]/(t^p))$. The set $\mathrm{Hom}(T, \alpha_p)$ is identified with the set of elements $x \in R$ which satisfy $x^p = 0$. Since k has characteristic p, this is a group under addition. It follows that α_p is a commutative group scheme. It is the kernel of the Frobenius map F_p on $\mathbf{G}_a$.

Remark 2. The schemes α_p and μ_p are isomorphic as schemes, but not as group schemes. □

2.3 Quotients

We are chiefly interested in finite commutative group schemes over k. Note that finite schemes are always affine, so such group schemes are described by finite dimensional commutative and cocommutative Hopf algebras. Examples include the constant group scheme on a finite group, μ_n, and α_p. We define the order of such a group scheme G, denoted $\#G$, to be the dimension of its Hopf algebra.

We state without proof the following theorem, first proved by Grothendieck.

Theorem 3. *Let G be a finite commutative group scheme over k and let H be a closed subgroup.*

- *Then the quotient G/H exists, and is a finite group scheme over k.*
- *The functor $h_{G/H}$ is the quotient of h_G by h_H in the category of sheaves (on the big fppf site over k). In other words, $h_{G/H}$ is the sheafification of the presheaf $T \mapsto G(T)/H(T)$.*
- *We have $\#(G/H) = \#G/\#H$.*

Proving part 1 is not difficult: it simply amounts to showing that kernels exist in the category of Hopf algebras, which can be checked explicitly. Parts 2 and 3 are more difficult.

Corollary 4. *The category of finite commutative group schemes over k is an abelian category.*

2.4 The étale case

We now study the case where G is étale over k. Recall that a finite dimensional k-algebra is étale if and only if it is a product of separable extensions of k; when k has characteristic 0, this is equivalent to being reduced.

Let A be an étale k-algebra and let k^s be the separable closure of k. Then $A \otimes k^s$ is a finite product of copies of k^s indexed by some set I. The Galois group G_k naturally permutes the set I. We have thus defined a functor

$$\Phi\colon \{\text{finite étale } k\text{-algebra}\} \to \{\text{finite } G_k\text{-sets}\}.$$

We note that $\Phi(A) = X(k^s)$, where $X = \mathrm{Spec}(A)$.

Now let I be a finite G_k-set. Let $\overline{A} = \prod_{i \in I} k^s$. Then G_k naturally acts on $\overline{A}$, through its action on both I and k^s. Let A be the invariant subalgebra. One easily sees that A is a finite dimensional algebra and étale over k. We thus have a functor

$$\Psi\colon \{\text{finite } G_k\text{-sets}\} \to \{\text{finite étale } k\text{-algebras}\}.$$

We have the following basic result:

Theorem 5. *The functors Φ and Ψ are naturally quasi-inverse.*

Translting from algebras to schemes, we obtain:

Corollary 6. *The functor*

$$\{\textit{finite étale schemes over } k\} \to \{\textit{finite } G_k\textit{-sets}\}$$

given by $X \mapsto X(k^s)$ is an equivalence.

Taking the categories of commutative group objects on each side, we obtain:

Corollary 7. *The functor*

$$\{\textit{finite étale commutative group schemes over } k\} \to \{\textit{finite } G_k\textit{-modules}\}$$

given by $G \mapsto G(k^s)$ is an equivalence.

We thus see that the study of étale group schemes is equivalent to the study of Galois representations.

2.5 The connected–étale sequence

Let $G = \mathrm{Spec}(A)$ be a finite commutative group scheme over k. Write $A = \prod A_i$ with each A_i local. There is a unique index, denoted 0, such that the counit of A factors through A_0. Let $G^\circ = \mathrm{Spec}(A_0)$, a connected closed subscheme of G. Since G° has a k-point, it is geometrically connected, and so $G^\circ \times G^\circ$ is still connected; it follows that multiplication maps $G^\circ \times G^\circ$ into G°, from which one easily sees that G° is a subgroup of G. We call G° the identity component of G.

Let A_{et} be the maximal étale subalgebra of A. Concretely, $A_{\mathrm{et}} = \prod (A_i)_{\mathrm{et}}$, where $(A_i)_{\mathrm{et}}$ is the separable closure of k in A_i. Put $G^{\mathrm{et}} = \mathrm{Spec}(A_{\mathrm{et}})$. Formation of A_{et} respects tensor products, and so if G is a group scheme then so is G^{et}, and the natural map $G \to G^{\mathrm{et}}$ is a homomorphism. The universal property of A_{et} implies the following: a map from G to an étale group scheme factors uniquely through G^{et}. Note that the natural map $G(\overline{k}) \to G^{\mathrm{et}}(\overline{k})$ is an isomorphism.

The tensor product $A \otimes_{A_{\mathrm{et}}} k$ (where the map $A_{\mathrm{et}} \to k$ is the counit) is the universal quotient of A in which the idempotent defining A_0 is identified with 1, and is therefore equal to A_0. In other words, G° is the fiber product of G with the trivial group over G^{et}. We have thus proved the sequence

$$0 \to G^\circ \to G \to G^{\mathrm{et}} \to 0$$

is exact. This sequence is called the connected–étale sequence.

Suppose now that k is perfect, i.e., every finite extension of k is separable. Then the separable closure of k in A_i coincides with the algebraic closure, and maps isomorphically onto the residue field of A_i. It follows that the map $G^{\mathrm{red}} \to G^{\mathrm{et}}$ is an isomorphism of schemes. Since k is perfect, a product of reduced schemes is still reduced, and so G^{red} is a closed subgroup of G. We have thus shown that, in this case, the connected–étale sequence splits. Furthermore, since there are no non-zero maps from an étale group scheme to a connected group scheme, the splitting is canonical. In other words, we have a canonical decomposition $G = G^\circ \times G^{\mathrm{et}}$.

Example 8. We now give an example where the connected–étale sequence does not split. This is not the most elementary example, but it is a natural one. Let X be some moduli scheme of elliptic curves over $\mathbf{F}_p$ (say $X_0(N)$), and let $\mathcal{E} \to X$ be the universal family of elliptic curves. Let k be the function field of X (which is not perfect), and let E/k be the generic fiber of $\mathcal{E}$.

Then E is not defined over the $\overline{\mathbf{F}}_p$: indeed, the function $j\colon X \to \mathbf{P}^1$ is not constant, and so $j \in k$, which is the j-invariant of E, is transcendental over $\mathbf{F}_p$. In particular, E is ordinary.

Let $G_n = E[p^n]$, a finite commutative group scheme over k. Since E is ordinary, $G_n(\overline{k})$ is non-zero, and so G_n^{et} is non-trivial. Since G_n is not étale, G_n° must also be non-trivial. We claim that the connected–étale sequence for G_n is non-split, for n large enough. Indeed, suppose to the contrary it split for all n. Then we have a decomposition $G_\infty = G_\infty^{\mathrm{et}} \times G_\infty^\circ$ of p-divisible groups. It follows that $\mathrm{End}(G_\infty) = \mathbf{Z}_p \oplus \mathbf{Z}_p$. Thus, by the Tate conjecture (a theorem in this case), $\mathrm{End}(E)$ has rank two over $\mathbf{Z}$, and thus E has CM. But this implies E is defined over $\overline{\mathbf{F}}_p$, a contradiction. □

2.6 Order invertible implies étale

Let $G = \mathrm{Spec}(A)$ be a finite connected commutative group scheme, so A is a local ring. Let $I \subset A$ be the kernel of the counit map. Then $A = k \oplus I$, where k is the span of the unit. We let $\pi\colon A \to I/I^2$ be the projection map, which is easily seen to be a derivation. Let $x_1, \ldots, x_n$ be elements of I mapping to a basis for I/I^2. Define $D_i\colon A \to A$ to be the composition

$$A \to A \otimes A \to A \otimes I/I^2 \to A$$

where the first map is comultiplication, the second is $\mathrm{id} \otimes \pi$, and the third is induced from the map $I/I^2 \to k$ taking x_i to 1 and x_j to 0 for $i \neq j$. This is easily seen to be a derivation.

Proposition 9. *(a) Suppose k has characteristic 0. Then the natural map $\varphi\colon k[x_i] \to A$ is an isomorphism. (b) Suppose k has characteristic p and $x_i^p = 0$ for all i. Then the natural map $\varphi\colon k[x_i]/(x_i^p) \to A$ is an isomorphism.*

Proof. Clearly, φ is surjective. In each case, one has $\varphi \frac{\partial}{\partial x_i} = D_i \varphi$, since both derivations agree on the x_i. This implies $\ker(\varphi)$ is stable by $\frac{\partial}{\partial x_i}$, which, by induction on degree, implies that it is either 0 or the unit ideal. Since it is not the unit ideal, we conclude that φ is injective. □

Corollary 10. *If k has characteristic 0 then G is trivial.*

Proof. The proposition shows that G is isomorphic to affine n-space for some n. By finiteness, $n = 0$, which establishes the corollary. □

Corollary 11. *If k has characteristic p then $\#G$ is a power of p.*

Proof. Let G_1 be the kernel of the Frobenius map $F_p\colon G \to G^{(p)}$, which is a group homomorphism, and let $G_2 = G/G_1$. The proposition shows that G_1 has order p^n, where $n = \dim(I/I^2)$. The result now follows from induction, since $\#G = (\#G_1)(\#G_2)$. □

Corollary 12. *Suppose G is a finite commutative group scheme such that $\#G$ is invertible in k. Then G is étale.*