ALGEBRAIC GROUPS

JEROEN SIJSLING

The goal of these notes is to introduce and motivate some notions from the theory of group schemes. For the sake of simplicity, we restrict to algebraic groups (as defined in the first section), though the results in these notes readily extend to more general group schemes. Our main reference is [Wat79].

1. Definitions and examples

We refer to page 84 of [Poo] for a diagrammatic (*i.e.* category-theoretical) definition of a group. **Exercise:** *Give a diagrammatic definition of a G-set.*

As mentioned in [Poo], these diagrams can be used to define the notion of *group object* in any category $\mathfrak{C}$ having finite products, and in particular a terminal object (replacing pt in the diagrams given there). The most important such special case is $\mathfrak{C} = \mathfrak{Sch}_S$, the category of schemes over a base scheme S. This category has objects (X, s_X) with X a scheme and $s_X : X \to S$ a morphism of schemes. A morphism $(X, s_X) \to (Y, s_Y)$ between objects of $\mathfrak{Sch}_S$ is a morphism of schemes $f : X \to Y$ satisfying $s_Y f = s_X$.

Finite products exist in $\mathfrak{Sch}_S$: the product of (X, s_X) and (Y, s_Y) is the fiber product of schemes $(X \times_S Y, s_X \times_S s_Y)$. A terminal object of $\mathfrak{Sch}_S$ is given by (S, id_S). Note the importance of the structural morphism s_X: in the case $S = \operatorname{Spec} k$, composing this morphism with $\operatorname{Spec} \sigma^{-1}$ for a field automorphism σ of k corresponds to conjugating the variety defining equations of the variety X with σ.

Another approach to group objects uses representable functors. Suppose we are given

- A contravariant functor $\mathcal{F} : \mathfrak{C} \to \mathfrak{Set}$ from $\mathfrak{C}$ to the category of sets $\mathfrak{Set}$;
- Group structures on the sets $\mathcal{F}(C)$ compatible with the set maps $\mathcal{F}(f)$.

Then if $\mathcal{F}$ is representable by an object G of $\mathfrak{C}$, Yoneda's lemma can be used to define a group object structure (G, m, i, e) on G. Alternatively, a group object of $\mathfrak{C}$ is a representable functor

$$\mathcal{G} : \mathfrak{C} \longrightarrow \mathfrak{Grp}$$

from $\mathfrak{C}$ to the category of groups $\mathfrak{Grp}$. Then the remarks above show that the functor $\mathcal{G}$ is representable if and only if the composition $\mathcal{U}\mathcal{G}$ is, where $\mathcal{U}$ is the forgetful functor $\mathfrak{Gps} \to \mathfrak{Set}$.

From now on, we work with group objects in the category $\mathfrak{Sch}_S$, where $S = \operatorname{Spec} k$ for a field k. Such a group object G is determined by the compatible system of groups

$$G(R) = G(\operatorname{Spec}(R))$$

obtained by taking the points of G over the spectra of k-algebras R: points over general schemes can be recovered by appropriately "gluing" the points in such $G(R)$ (that is, by taking an appropriate inverse limit).

An *affine* group scheme over k is a group object in $\mathfrak{Sch}_k$ for which the underlying variety G is affine. By the duality between affine schemes and k-algebras, this means

Date: June 25, 2010.

that G is of the form $\operatorname{Spec} k[G]$ for some k-algebra $k[G]$. The morphisms m, i and e give rise to k-algebra maps

$$\begin{aligned}\Delta : k[G] &\longrightarrow k[G] \otimes_k k[G]\\ S : k[G] &\longrightarrow k[G]\\ \epsilon : k[G] &\longrightarrow k.\end{aligned}$$

The quadruple $(k[G], \Delta, S, \epsilon)$ is called the *Hopf algebra* corresponding to the group scheme (G, m, i, e) over k.

Finally, a group scheme over k is called *algebraic* if it is represented by an algebraic variety, which means that G has an affine cover by spectra of rings that are finitely generated over k.

Examples. (i) The *additive group scheme* $\mathbf{G}_a$ satisfies

$$\mathbf{G}_a(R) = R^+$$

where R^+ is R with its additive group structure. $\mathbf{G}_a$ is represented by the k-algebra $k[G_a] = k[t]$. The corresponding Hopf algebra structure is given by

$$\begin{aligned}\Delta : t &\longmapsto t \otimes 1 + 1 \otimes t\\ S : t &\longmapsto -t\\ \epsilon : t &\longmapsto 0.\end{aligned}$$

Note that if we identify $k[t] \otimes_k k[t]$ with $k[t_1, t_2]$ by sending $t \otimes 1$ to t_1 and $1 \otimes t$ to t_2, then indeed Δ is dual to the map of varieties $\mathbf{A}_k^2 \to \mathbf{A}_k^1$ given by $(t_1, t_2) \mapsto t_1 + t_2$.

(ii) There is also the *multiplicative group scheme* $\mathbf{G}_m$, which satisfies

$$\mathbf{G}_m(R) = R^\times.$$

Here $R^\times$ is equipped with its multipicative group structure. This is the special case $n = 1$ of the *general linear group scheme* $\mathbf{GL}_n$ determined by

$$\mathbf{GL}_n(R) = \mathrm{GL}_n(R),$$

which is represented by $k[\{t_{ij}\}_{1 \le i,j \le n}, D^{-1}]$, where $D = \det((t_{i,j})_{1 \le i,j \le n})$. In particular, $k[\mathbf{G}_m]$ is given by $k[t, t^{-1}]$.

(iii) Finally, given a group G, there exists a *constant group scheme* $\mathbf{G}$ determined by the property that

$$\mathbf{G}(R) = G$$

for any k-algebra R *whose only idempotents are 0 and 1*. One has

$$k[G] = \prod_{g \in G} k.$$

For rings R with nilpotent elements, $\mathbf{G}(R)$ may contain G as a proper subgroup.

And now for something completely different (a priori).

2. Faithful flatness

Let A be a ring. A module M over A is called *flat* if the functor

$$N \longmapsto N \otimes_A M$$

is exact. It is called *faithfully flat* over A (or *fp*, after *fidèlement plat*) if additionally

$$N \longrightarrow N \otimes_A M$$

is injective for all A-modules N. In particular, if M is fp, then

$$N = 0 \Leftrightarrow N \otimes_A M = 0.$$

This implication is in fact equivalent to faithful flatness: see Section 13.1 of [Wat79]. Finally, a ring homomorphism $f : A \to B$ is called (faithfully) flat if B, equipped with its A-module structure coming from f, is (faithfully) flat.

Some facts on faithful flatness:

(i) If B is free of positive rank over A, then B is fp over A;
(ii) In particular, any field extension is fp;
(iii) If f is fp, then f is also injective (take $M = A$).
(iv) If B is flat over A, then B is fp over A if and only if $\operatorname{Spec} B \to \operatorname{Spec} A$ is surjective.

The final property illustrates the analog between fp extensions of rings and open coverings of the corresponding affine scheme, which can be formalized by defining the *fppf topology* on such a scheme. Another such analogy is the following, illustrating a sheaf property in the fppf topology.

Proposition 2.1 ([Wat79], Section 13.1). *Suppose $A \subset B$ is an fp ring extension. Then the sequence*

$$0 \longrightarrow M \xrightarrow{g} M \otimes_A B \xrightarrow{f_1 - f_2} M \otimes_A B \otimes_A B$$

is exact. Here

$$\begin{aligned} g(m) &= m \otimes 1 \\ f_1(m \otimes b) &= m \otimes b \otimes 1 \\ f_2(m \otimes b) &= m \otimes 1 \otimes b \end{aligned}$$

Moreover, we have the following two important Theorems.

Theorem 2.2. *Let $A \subset B$ be finitely generated integral domains over a base field k. Then there exist non-zero $a \in A$ and $b \in B$ such that the morphism of localizations*

$$A_a \longrightarrow B_b$$

is well-defined and fp.

Remark. This is an analog of the geometric fact that a morphism $Y \to X$ of curves in characteristic 0 is étale over a non-empty open subset of X. This property fails in characteristic p, confounding our intuition: however, this morphism will then still be fppf over some non-empty open subset by the Theorem.

Theorem 2.3. *Let $k[H] \subset k[G]$ be an injective homomorphism of Hopf algebras. Then $k[G]$ is fp over $k[H]$.*

Remark. The idea of the proof is to use to homogeneity of the ring extension $k[H] \subset k[G]$ to extend the generic property from the previous Theorem to the morphism $k[H] \hookrightarrow k[G]$. This homogeneity results from the fact that $k[H] \subset k[G]$ corresponds to a morphism of groups $G \to H$, which "looks the same everywhere" (use translations!).

3. Kernels and cokernels

Kernels of algebraic group homomorphisms can be defined in a straightforward manner. The motivation comes from the following **Exercise:** *Prove that for a homomorphism of groups $\varphi : G \to H$, the kernel $\varphi^{-1}(e)$ equals the fiber product $G \times_H \mathrm{pt}$ (which morphisms $G \to H$ and $\mathrm{pt} \to H$ does one have to use?).*

Now fiber products exist in $\mathfrak{C} = \mathfrak{Sch}_S$, so given a homomorphism of algebraic groups, we can define

$$\ker \varphi = G \times_H \operatorname{Spec} k.$$

By the definition of the fiber product, we have on points:

$$(\ker \varphi)(R) = (G \times_H \operatorname{Spec} k)(R) = \{g \in G(R) : \varphi(g) = e\}.$$

Example. Let k be a field of characteristic p. Then the morphism

$$\mathbf{G}_a \longrightarrow \mathbf{G}_a$$
$$t \longmapsto t^p$$

is a group homomorphism. Its kernel is given by

$$\alpha_p(R) = \{r \in R : r^p = 0\}$$

and is represented by the k-algebra

$$k \otimes_{k[t^p]} k[t] \cong k[t]/(t^p).$$

(**Exercise:** *Check this isomorphism.*) Note that though non-trivial, α_p has only the trivial point over fields!

Proposition 3.1. *A morphism of algebraic groups $G \to H$ has trivial kernel if and only the map of coordinate rings $k[H] \to k[G]$ is surjective.*

Proof. If $k[H] \to k[G]$ is surjective, then the tensor product

$$k \otimes_{k[H]} k[G]$$

is isomorphic to k. Conversely, suppose that $G \to H$ has trivial kernel. Replacing $k[H]$ by its image in $k[G]$, we may suppose that $k[H]$ is contained in $k[G]$, leaving us to prove $k[H] = k[G]$. We have two maps

$$f_1, f_2 : k[G] \longrightarrow k[G] \otimes_{k[H]} k[G]$$
$$f_1 : x \longmapsto x \otimes 1$$
$$f_2 : x \longmapsto 1 \otimes x.$$

Since these maps agree on $k[H]$ by definition of the tensor product, we accordingly obtain two elements of $G(k[G] \otimes_{k[H]} k[G])$ mapping to the same element of $H(k[G] \otimes_{k[H]} k[G])$. By hypothesis, then, these maps are equal. But the equalizer of these maps equals $k[G]$ by Proposition 2.1, hence indeed $k[H] = k[G]$. □

Cokernels are more troublesome to define. Indeed, the functor

$$C(R) = G(R)/H(R).$$

need not be representable.

Example. Let $G = \mathbf{G}_m$ be the multiplicative group over $\mathbf{Q}$, and let $f : G \to G$ be given by $x \mapsto x^2$. Then $G(\mathbf{Q})/f(G(\mathbf{Q}))$ is infinite, but $G(\mathbf{C})/f(G(\mathbf{C}))$ is trivial. However, $\mathcal{F}(\mathbf{Q}) \to \mathcal{F}(\mathbf{C})$ is injective for all representable functors $\mathcal{F}$.

Inspired by Proposition 3.1, we first give the following

Proposition 3.2. *A homomorphism $G \to H$ of algebraic groups is* surjective *if the map of coordinate rings $k[H] \to k[G]$ is injective.*

Then we have

Theorem 3.3. *A homomorphism $G \to H$ is surjective if and only if for every h in $H(R)$ there exists an fp extension $R \to S$ and an g in $G(S)$ such that the images of g and h in $H(S)$ coincide.*

Proof. First suppose that $G \to H$ is surjective. Let

$$(h : k[H] \longrightarrow R) \in H(R)$$

be given. Then one can form the tensor product $k[G] \otimes_{k[H],h} R$. The morphism $R \to k[G] \otimes_{k[H],h} R$ is fp because $k[H] \to k[G]$ is. Indeed, faithful flatness is stable under base extension (see Section 13.3 of [Wat79]). Now let

$$(g : k[G] \longrightarrow k[G] \otimes_{k[H],h} R) \in G(k[G] \otimes_{k[H],h} R)$$

be given by $x \mapsto x \otimes 1$. Then we have an equality of compositions

$$(k[H] \longrightarrow k[G] \xrightarrow{g} k[G] \otimes_{k[H],h} R) = (k[H] \xrightarrow{h} R \longrightarrow k[G] \otimes_{k[H],h} R)$$

since by definition of $k[G] \otimes_{k[H],h} R$, the equality

$$y \otimes 1 = 1 \otimes h(y)$$

holds for all $y \in k[H]$. We can therefore take $S = k[G] \otimes_{k[H],h} R$ and $g \in G(S)$.

For the converse, take $R = k[H]$: we will use the lift of the *universal point*

$$(1 : k[H] \xrightarrow{\mathrm{id}} k[H]) \in H(k[H]).$$

By hypothesis, there is a faithfully flat extension $f : k[H] \longrightarrow S$ and a

$$(g : k[G] \longrightarrow S) \in G(S)$$

such that g and 1 have the same image in $H(S)$. We accordingly obtain a factorization

$$(k[H] \xrightarrow{f} S) = (k[H] \xrightarrow{1} k[H] \xrightarrow{f} S) = (k[H] \longrightarrow k[G] \xrightarrow{g} S).$$

Since f, being fp, is injective, so is $k[H] \to k[G]$. $\square$

Let $G \to H$ be a surjective group homomorphism, and let K be its kernel. Then the Theorem states that we have an exact sequence

$$1 \to K \to G \to H \to 1$$

of sheaves *for the fppf topology* on $\mathfrak{Sch}_k$: this need not be an exact sequence in the Zariski topology by the Example above. This is why Section 8.2 of [Poo] uses fppf cohomology: in order to obtain the long exact sequences used there, one needs to start with a short exact sequence of sheaves.

Now let G be an algebraic group over k, and let N be a normal subgroup of G. Then it is easy enough to prove that there is at most one surjective homomorphism $G \to Q$ with kernel N (see Section 15.4 of [Wat79]). The following Theorem, however, is much less trivial. It is Theorem 5.1.17 in [Poo] stripped of the needless fppf verbiage.

Theorem 3.4. *Let N be a normal subgroup scheme of an affine algebraic group G over a field k. Then there exists an* affine *algebraic group Q over k and a surjective homomorphism $G \to Q$ with kernel N.*

Example. Let $k = \mathbf{C}$ and take $G = \mathbf{GL}_2$. Let H be the non-normal closed subgroup of G with $\mathbf{C}$-points

$$\left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \in \mathrm{GL}_2(\mathbf{C}) \right\}.$$

Then the quotient $(G/H)(\mathbf{C}) = G(\mathbf{C})/H(\mathbf{C})$ is isomorphic with $\mathbf{P}^1(\mathbf{C})$. Indeed, $G(\mathbf{C})$ acts transitively on the set of 1-dimensional subspaces of $\mathbf{C}^2$, and the stabilizer of the subspace $(*\ 0)^T$ is given by $H(\mathbf{C})$. Now $\mathbf{P}^1(\mathbf{C})$ is not affine, whence part of the substance of the theorem.

A proof of Theorem 3.4 is given in Chapter 16 of [Wat79]. It constructs a representation $\rho : G \to \mathbf{GL}_n$ with kernel N. In the case

$$1 \longrightarrow \mathbf{G}_m \longrightarrow \mathbf{GL}_n \longrightarrow \mathbf{PGL}_n \longrightarrow 1,$$

for example, one can take ρ to be the conjugation action of $\mathbf{GL}_n$ on itself, realizing the affine algebraic group $\mathbf{PGL}_n$ as a subgroup of $\mathbf{GL}_{n^2}$.

We conclude by giving a few criteria for injectivity and surjectivity, for which we refer to Chapter 6 of [Mil]. Let $\bar{k}$ denote the algebraic closure of a field k.

Proposition 3.1. *Suppose* $\mathrm{char}\, \mathrm{k} = 0$. *Then a homomorphism $G \to H$ of algebraic groups has trivial kernel if and only if the homomorphism $G(\bar{k}) \to H(\bar{k})$ has trivial kernel.*

Proposition 3.2. *Let $G \to H$ be surjective. Then so is $G(\bar{k}) \to H(\bar{k})$. If H is smooth, then the converse holds as well. In particular, this holds if* $\mathrm{char}\, k = 0$.

Counterexamples to these Theorems in characteristic p can be constructed by using the non-smooth group α_p from the Example at the beginning of this Section. **Exercise:** *Find these counterexamples.*

References

[Mil] J. S. Milne, *Basic Theory of Algebraic Groups*, Notes available at `http://www.jmilne.org/math/CourseNotes/ala.html`.

[Poo] Bjorn Poonen, *Rational points on varieties*, Notes available at `http://www-math.mit.edu/~poonen/papers/Qpoints.pdf`.

[Wat79] William C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, vol. 66, Springer-Verlag, New York, 1979. MR MR547117 (82e:14003)