Lecture 4

November 11, 2004
Notes by Nicolas Stalder

§8 Quotients of schemes by finite group schemes, part II

As before all schemes are supposed to be affine of finite type over a field k. Let $X = \operatorname{Spec} A$ be an affine scheme with an action of a finite group scheme $G = \operatorname{Spec} R$, and let $\pi : X \longrightarrow Y = \operatorname{Spec} A^G$ be the quotient map from the preceding lecture.

Definition. The *order* of G is

$$|G| := \dim_k R.$$

Note that a constant finite group scheme $\underline{\Gamma}_k$ has order $|\Gamma|$.

Definition. The action of G on X is called *free* if the morphism

$$\lambda : G \times X \xrightarrow{(m, pr_2)} X \times X$$

is a closed embedding.

Theorem 8.1. If the action of G on X is free, the quotient map $\pi : X \longrightarrow Y$ is faithfully flat everywhere of degree $|G|$, and the morphism λ above is an isomorphism.

Proof. For missing details, see [Mu70, pp. 115-6]. Set $B := A^G$. Since everything commutes with extension of k, we may assume that k is infinite. By the preceding lecture we may also localize at any prime ideal of B. Thus we may and do assume that B is local with infinite residue field. By assumption, the ring homomorphism

$$\begin{aligned} \lambda : A \otimes_B A &\longrightarrow R \otimes_k A \\ a \otimes a' &\mapsto m(a) \cdot (1 \otimes a') \end{aligned}$$

is surjective. We must prove that λ is an isomorphism, and that A is locally free over B of rank $n := |G|$.

We consider the source and the target of λ as A-modules via the action on the second factor. Note that $R \otimes_k A$ is a free A-module of rank n, and the surjectivity of λ means that $R \otimes_k A$ is generated as an A-module by $m(A)$. Note also that m is B-linear by the calculation

$$m(ab) = \lambda(ab \otimes 1) = \lambda(a \otimes b) = m(a) \cdot (1 \otimes b)$$

for all $a \in A$ and $b \in B$; hence $m(A)$ is a B-submodule of $R \otimes_k A$. We claim that $m(A)$ contains a basis of the free A-module $R \otimes_k A$. Indeed, since B is local it suffices to prove this after tensoring everything with the residue field of B, in which case it results from the following lemma:

Lemma 8.2. Consider an infinite field K, a finite dimensional K-algebra A, a finitely generated free A-module F, and a K-subspace $M \subset F$ that generates F as an A-module. Then M contains a basis of F over A.

Proof. We prove this by induction on the rank of F. The case $F = 0$ being trivial, suppose that $F \neq 0$ and choose a surjection $\varphi : F \twoheadrightarrow A$. The assumption implies that $\varphi(M)$ is not contained in any maximal ideal $\mathfrak{p} \subset A$. In other words $M \cap \varphi^{-1}(\mathfrak{p})$ is a proper subspace of M. Since K is infinite, it is well-known that M possesses an element m that does not lie in any of these finitely many subspaces. Then $\varphi(m)$ generates A, and so m generates a direct summand of F that is free of rank 1. By the induction hypothesis applied to the image of M in F/Am we can find elements of M whose images form a basis of F/Am over A. Thus these elements together with m form a basis of F over A, as desired. ☐

Now by the claim we can choose $a_1, \ldots, a_n \in A$ such that the elements $m(a_1), \ldots, m(a_n)$ are a basis of $R \otimes_k A$ over A. Thus we have an isomorphism of A-modules

$$A^{\oplus n} \longrightarrow R \otimes A, \qquad (\alpha_i)_i \mapsto \sum_{i=1}^{n} m(a_i) \cdot (1 \otimes \alpha_i). \tag{8.3}$$

Lemma 8.4. For all $a, \alpha_1, \ldots, \alpha_n \in A$:

$$m(a) = \sum_{i=1}^{n} m(a_i) \cdot (1 \otimes \alpha_i) \quad \Longleftrightarrow \quad \left(a = \sum_{i=1}^{n} a_i \alpha_i, \text{ and all } \alpha_i \in B \right)$$

Proof. The implication "$\Leftarrow$" follows directly from the definition of $A \otimes_B A$. For the implication "$\Rightarrow$", let us explain the idea in terms of points g of G and x of X. The left hand side means: $\forall g \, \forall x : \, a(gx) = \sum a_i(gx) \cdot \alpha_i(x)$. Because of the isomorphy (8.3), the $\alpha_i \in A$ are uniquely determined by this identity. Replacing x by hx and g by gh^{-1} has the sole effect of replacing $\alpha_i(x)$ by $\alpha_i(hx)$ in this identity. Letting h vary, we see that the α_i are translation invariant, i.e., that $\alpha_i \in A^G = B$. The equation $a = \sum a_i \alpha_i$ follows by evaluation at $g = 1$.

This argument must of course be done with Z-valued points, or directly with $\mathrm{id} \in G(G)$: see [Mu70, p. 116]. ☐

Now for all $a \in A$, there exist unique $\alpha_i \in A$ as on the left hand side of Lemma 8.4. So there exist unique $\alpha_i \in B$ as on the right hand side. This means that the a_i are a basis of A as a B-module, which is thus locally free of rank n, and so faithfully flat. Also, it follows that the $a_i \otimes 1$ are a basis of $A \otimes_B A$ as an A-module via the second factor, and since λ maps these elements to a basis of $R \otimes A$, we deduce that λ is an isomorphism. $\square$

§9 Abelian categories

Let us recall some basic notions from the theory of categories (cf. also [We94]).

Definition. An *additive category* is a category $\mathcal{A}$ together with an abelian group structure on each $\mathrm{Hom}(X, Y)$, such that the composition map

$$\mathrm{Hom}(Y, Z) \times \mathrm{Hom}(X, Y) \longrightarrow \mathrm{Hom}(X, Z)$$

is bilinear, and such that there exist arbitrary finite direct sums. (In particular, there is a zero object.)

Let $X \xrightarrow{f} Y$ be a homomorphism in such an additive category $\mathcal{A}$.

Definition. (a) A homomorphism $K \xrightarrow{i} X$ is called a *kernel of* f, if for all $Z \in \mathcal{A}$, the following sequence is exact:

$$0 \longrightarrow \mathrm{Hom}(Z, K) \xrightarrow{i \circ (\ )} \mathrm{Hom}(Z, X) \xrightarrow{f \circ (\ )} \mathrm{Hom}(Z, Y).$$

(b) A homomorphism $Y \xrightarrow{p} C$ is called a *cokernel of* f, if for all $Z \in \mathcal{A}$, the following sequence is exact:

$$0 \longrightarrow \mathrm{Hom}(C, Z) \xrightarrow{(\ ) \circ p} \mathrm{Hom}(Y, Z) \xrightarrow{(\ ) \circ f} \mathrm{Hom}(X, Z).$$

Fact. If a kernel (resp. a cokernel) of f exists, it is unique up to unique isomorphism.

Notation. As usual, we will write $\ker f$ for the domain of the kernel of f, tacitly assuming the homomorphism i to be included. Same for $\operatorname{coker} f$.

Assuming that all kernels and cokernels exist, we can construct two further objects. The *coimage of* f is $\operatorname{coim} f := \operatorname{coker}(\ker f)$, whereas the *image of* f is $\operatorname{im} f := \ker(\operatorname{coker} f)$. Furthermore, using the universal properties of kernels and cokernels, we find a unique homomorphism $\operatorname{coim} f \longrightarrow \operatorname{im} f$, making the following diagram commutative:

$$\begin{array}{ccccccc} \ker f & \longrightarrow & X & \xrightarrow{f} & Y & \longrightarrow & \operatorname{coker} f \\ & & \downarrow & & \uparrow & & \\ & & \operatorname{coim} f & \xrightarrow{\exists !} & \operatorname{im} f & & \end{array}$$

Definition. An additive category $\mathcal{A}$ is called an *abelian category*, if all kernels and cokernels exist and all canonical homomorphisms $\operatorname{coim} f \longrightarrow \operatorname{im} f$ are isomorphisms.

Examples. The category of abelian groups, the category of modules over a ring R, the category of sheaves of abelian groups on a topological space.

Fact. In an abelian category, all the usual diagram lemmas hold, for example the Snake Lemma, the 5-Lemma, and the 3×3-Lemma.

§10 The category of finite commutative group schemes

In this subsection, we work in the category of finite commutative group schemes over a field k. The aim is to show that this category is abelian.

Let $f : G \longrightarrow H$ be a homomorphism of finite commutative group schemes, and let $\phi : A \longleftarrow B$ be the corresponding homomorphism of Hopf algebras. It may be checked that $\phi(B)$ is again a Hopf algebra, and thus, setting $\overline{G} := \operatorname{Spec} \phi(B)$, we may factor f as

$$G \xrightarrow{p} \overline{G} \xrightarrow{i} H,$$

where $\overline{G}$ is again a finite commutative group scheme, and the morphisms are homomorphisms. Note also that i is a closed embedding, since $B \longrightarrow \phi(B)$ is surjective. Looking at the coordinate rings, we can see easily that i is a monomorphism and p is an epimorphism, in the categorical sense.

Proposition 10.1. The kernel of f exists and is a closed subgroup scheme of G.

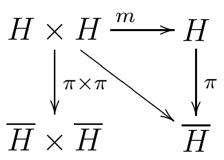
Proof. If the kernel exists, then for all Z we have

$$\begin{aligned} \operatorname{Hom}(Z, \ker f) &= \ker\big(\operatorname{Hom}(Z,G) \longrightarrow \operatorname{Hom}(Z,H)\big) \\ &= \left\{ Z \longrightarrow G \;\middle|\; \begin{array}{ccc} Z & \longrightarrow & G \\ \downarrow & & \downarrow f \\ * & \xrightarrow{\varepsilon} & H \end{array} \text{ commutes} \right\} \\ &= \operatorname{Hom}(Z, G \times_H *) \end{aligned}$$

In fact, the fibre product $G \times_H *$, i.e., the scheme theoretic inverse image in G of the unit section of H, is a closed subgroup scheme of G. Tracing backwards, we see that it has the universal property of the kernel of f. □

Proposition 10.2. The quotient $\overline{H} := H/\overline{G}$, given by Theorem 7.1, carries a unique structure of group scheme such that $\pi : H \longrightarrow \overline{H}$ is a homomorphism. Moreover, π is an epimorphism, and $\overline{G} = \ker \pi$.

Proof. Let $\overline{G}$ act on H by left translation. This action is free, so Theorem 8.1 applies. To get the group structure, we consider the commutative diagram:



One checks that $(H \times H)/(\overline{G} \times \overline{G}) \cong \overline{H} \times \overline{H}$ naturally as schemes. By the universal property of this quotient, since the diagonal arrow is $\overline{G} \times \overline{G}$-invariant, we find a unique map $\overline{H} \times \overline{H} \xrightarrow{\overline{m}} \overline{H}$ making the above square commutative. Likewise, the morphisms $* \xrightarrow{\varepsilon} H \xrightarrow{i} H$ induce morphisms $* \xrightarrow{\overline{\varepsilon}} \overline{H} \xrightarrow{\overline{i}} \overline{H}$. Also, the uniqueness part of the universal property can be used every time to deduce that $\overline{m}$ satisfies the axioms of a commutative group structure for which π is a homomorphism. This proves the first sentence of this Proposition.

By the construction of $\overline{H}$ as a quotient, π is an epimorphism. Next, the morphism $\lambda : \overline{G} \times H \xrightarrow{(m,\mathrm{pr}_2)} H \times_{\overline{H}} H$ is an isomorphism by Theorem 8.1. Thus for all $h \in H(Z)$ we have

$$h \in \ker(\pi)(Z) \iff \pi(h) = e \iff \exists\, \overline{g} \in \overline{G}(Z) :\ h = \overline{g}e = \overline{g}$$

which is true if and only if $h \in \overline{G}(Z)$. Therefore, $\ker(\pi) = \overline{G}$. $\square$

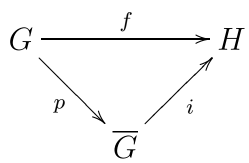
Proposition 10.3. (a) $\operatorname{coker} f$ exists and is isomorphic to $\overline{H}$.

(b) $\operatorname{im} f$ is isomorphic to $\overline{G}$.

Proof. Since $f = i \circ p$ and p is an epimorphism, we have $\operatorname{coker} f = \operatorname{coker} i$. Moreover $\operatorname{coker} i = \overline{H}$ by the universal property of the quotient, proving (a). Part (b) follows from (a) together with Proposition 10.2. $\square$

Proposition 10.4. $\operatorname{coim} f$ is isomorphic to $\overline{G}$.

Proof. A direct proof in greater generality is given in [Mu70, p. 119]. In our case, it is easier to use Cartier duality. Since this is an antiequivalence of categories, it interchanges kernels and cokernels, and hence images and coimages. Also, clearly the diagram



dualizes to the diagram

$$\begin{array}{ccc} G^* & \xleftarrow{\ f^*\ } & H^* \\ & {\scriptstyle p^*}\nwarrow \quad \swarrow{\scriptstyle i^*} & \\ & \overline{G}^* & \end{array}$$

Thus $(\operatorname{coim} f)^* = \operatorname{im}(f^*) = \overline{G}^*$, and hence $\operatorname{coim} f = \overline{G}$. □

Combining these four propositions, we deduce:

Theorem 10.5. The category of finite commutative group schemes over a field k is abelian.

Theorem 10.6. (a) The following conditions are equivalent:

- (i) f is a kernel.
- (ii) f is a monomorphism.
- (iii) $\ker f = 0$.
- (iv) ϕ is surjective.
- (v) f is a closed embedding.

(b) The following conditions are equivalent:

- (i) f is a cokernel.
- (ii) f is an epimorphism.
- (iii) $\operatorname{coker} f = 0$.
- (iv) ϕ is injective.
- (v) f is faithfully flat.

Proof. For both items, the equivalences $(i) \iff (ii) \iff (iii)$ hold in all abelian categories. In (a), the implication $(iii) \implies (iv)$ results from Proposition 10.4, the equivalence $(iv) \iff (v)$ is clear, and the direction $(v) \implies (i)$ follows from Proposition 10.2. In (b), the implication $(i) \implies (v)$ results from Proposition 10.3 (a) and Theorem 8.1, the direction $(v) \implies (iv)$ is clear, and the implication $(iv) \implies (i)$ is a special case of Proposition 10.4. □

Theorem 10.7. For any short exact sequence of finite group schemes

$$0 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 0$$

we have $|G| = |G'| \cdot |G''|$.

Proof. Combine Proposition 10.3 (a) with the faithful flatness of Theorem 8.1. □

Theorem 10.8. For any field extension $k'|k$, the additive functor $G \mapsto G \times_k k'$ is exact and preserves group orders.

Proof. Base extension commutes with fiber products; hence by the proof of Proposition 10.1 also with kernels. It also commutes with Cartier duality, and so (cf. the proof of Proposition 10.4) also with cokernels. □

Note. Cartier duality is an exact functor, and we have used this already several times.

Note. Theorems 10.5, 10.6 and 10.8 hold more generally in the category of affine commutative group schemes over k, but are harder to prove. The main problem in general is still the construction of quotients. For this, see [DG70]. Also, the inclusion of categories is exact, i.e., kernels and cokernels in the smaller category remain the same in the bigger category.