Topics in Algebraic Groups *

Zhiyuan Bai

Compiled on February 19, 2023

This document serves as a set of revision materials for the Cambridge Mathematical Tripos Part III course *Topics in Algebraic Groups* in Lent 2022. However, despite its primary focus, readers should note that it is NOT a verbatim recall of the lectures, since the author might have made further amendments in the content. Therefore, there should always be provisions for errors and typos while this material is being used.

Contents

*Based on the lectures under the same name taught by Prof. A. Scholl in Lent 2022.

1 Algebraic Geometry Continued

1.1 Finiteness Conditions

Definition 1.1. A scheme is quasicompact (qc) if it's a finite union of open affines.

In general, a topological space is quasicompact if every open cover of it has a finite subcover. Many interesting schemes are not quasicompact, e.g. $\coprod_{n\in\mathbb{Z}} \operatorname{Spec} k$ (the "constant group scheme associated to $\mathbb{Z}$ over k") for a field k.

Definition 1.2. A scheme is quasiseparated (qs) if the intersection of any two open affines is quasi-compact.

Reassuringly, you'll rarely meet non-quasiseparated schemes. One counterexample can be constructed as follows: Let $\mathbb{A}_k^\infty = \operatorname{Spec} k[T_0, T_1, \ldots]$, then $U = A_k^\infty \setminus \{(T_0, T_1, \ldots)\} = \bigcup_{n\geq 0} D(T_n)$ is not quasicompact, so the scheme X constructed by gluing two copies of $\mathbb{A}_k^\infty$ together along U would not be quasiseparated.
We say a scheme is qcqs if it's both quasicompact and quasiseparated.
There are also versions of quasicompactness and quasiseparatedness as relative notions (i.e. properties of morphisms).

Definition 1.3. A morphism $f : X \to Y$ is quasicompact (resp. quasiseparated) if for all affine $V \subset Y$, $f^{-1}(V)$ is quasicompact (resp. quasiseparated).
We say f is separated if $\Delta : X \to X \times_Y X$ is closed (equivalently, Δ is a closed immersion).

Notably, f is quasiseparated iff Δ is quasicompact.
A lot of Picard schemes are not separated as you might have seen.

Definition 1.4. A scheme is locally Noetherian iff any open affine $\operatorname{Spec} R$ in it has R Noetherian.

Equivalently, a scheme is Noetherian iff it has an affine cover $(\operatorname{Spec} R_i)_i$ where each R_i is Noetherian.

Definition 1.5. A scheme is Noetherian iff it is locally Noetherian and quasicompact.

(Locally) Noetherian schemes are nice because Noetherian rings are nice (duh!), but there are "natural" schemes that are not (locally) Noetherian. Take $X = \operatorname{Spec} \mathbb{C}[T, T^{-1}] = \mathbb{A}^1_{\mathbb{C}} \setminus \{0\}$. Topologically $X(\mathbb{C}) = \mathbb{C}^\times$ has a universal cover given by $\mathbb{C} = \mathbb{A}^1_{\mathbb{C}}$ via the exponential map, which is sadly not induced by a morphism of schemes. As a substitute, we can take $X_n = \operatorname{Spec} \mathbb{C}[T^{1/n}, T^{-1/n}]$ which admits a natural map to X. On $X(\mathbb{C})$, this natural map gives the familiar power function $\mathbb{C}^\times \to \mathbb{C}^\times, z \mapsto z^n$. We can take a limit to get $\tilde{X} = \operatorname{Spec} \mathbb{C}[\{T^{1/n}\}, T^{-1}] \to X$ which works just like a universal cover. But now $\tilde{X}$ is not locally Noetherian since the ideal generated by $\{T^{1/n} - 1\}$ is not finitely generated.
Let $\pi : \tilde{X} \to X$ be the covering map, then the fibre $\pi^{-1}(x)$ at $x = T - 1$ is an affine scheme whose complex points are exactly

$$\{(z_n)_{n\geq 1}, z_n \in \mu_n(\mathbb{C}), z_{mn}^m = z_n\} = \varprojlim_{n\geq 1} \mu_n(\mathbb{Z}) \cong \varprojlim_{n\geq 1} \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$$

where the last space is given the profinite topology.

Definition 1.6. A morphism $f : X \to Y$ is locally of finite type if for all $x \in X$, there is an open affine $U = \operatorname{Spec} B \subset X$ around x such that $f(U) \subset V = \operatorname{Spec} A \subset Y$ and B is an A-algebra of finite type via f, i.e. $B \cong A[T_1, \ldots, T_n]/I$ for some ideal I. f is locally of finite presentation if in addition that I is finitely generated.
f is of finite type if it is locally of finite type and quasicompact. It is of finite presentation if it is locally of finite presentation and qcqs.

1.2 Kähler Differentials

Let B be an A-algebra, which as you know is the data of a ring homomorphism $A \to B$.
We are going to define a B-module $\Omega_{B/A}$ of Kähler differentials equipped with a map $\mathrm{d} = \mathrm{d}_{B/A} : B \to \Omega_{B/A}$ such that $\mathrm{d}(b_1 + b_2) = \mathrm{d}b_1 + \mathrm{d}b_2, \mathrm{d}(a) = 0, \mathrm{d}(b_1 b_2) = b_1 \,\mathrm{d}b_2 + b_2 \,\mathrm{d}b_1$ for $a \in A, b_1, b_2 \in B$.
The way we construct this is quite brute force on first sight: We take $\Omega_{B/A} = P/Q$ where P is the free B-module on $\{[b] : b \in B\}$ and Q is the submodule generated by $[a], [b_1 + b_2] - [b_1] - [b_2], [b_1 b_2] - b_1[b_2] - b_2[b_1]$ for all $a \in A, b_1, b_2 \in B$. The map it comes with is, expectedly, $\mathrm{d}(b) = [b] \bmod Q$.
This certainly looks unappetising, but it is in fact universal.

Definition 1.7. An A-derivation of B into a B-module M is an additive map $\mathrm{D} : B \to M$ such that $\mathrm{D}(a) = 0, \mathrm{D}(b_1 b_2) = b_1 \mathrm{D}(b_2) + b_2 \mathrm{D}(b_1)$ for all $a \in A, b_1, b_2 \in B$.
We set $\operatorname{Der}_A(B, M)$ to be the set of A-derivations $B \to M$ which admits the natural structure of a B-module via $x \mapsto b \,\mathrm{D}(x)$.

Clearly if $\phi : M \to N$ is a B-module map and $\mathrm{D} \in \operatorname{Der}_A(B, M)$, then $\phi \circ D \in \operatorname{Der}_A(B, N)$.

Proposition 1.1. *Let M be a B-module, then the map* $\operatorname{Hom}_B(\Omega_{B/A}, M) \to \operatorname{Der}_A(B, M)$ *given by $\psi \mapsto \psi \circ \mathrm{d}_{B/A}$ is an isomorphism.*

Proof. Suppose $\mathrm{D} \in \operatorname{Der}_A(B, M)$. Consider $\bar{\psi} : P \to M$ extended from $[b] \mapsto \mathrm{D}(b)$. Then $\bar{\psi}(Q) = 0$ as D is a derivation, so it factors through some $\psi : \Omega_{B/A} = P/Q \to M$, necessarily along $\mathrm{d}_{B/A}$. This gives surjectivity. Injectivity follows from the fact that $\{\mathrm{d}b : b \in B\}$ generates $\Omega_{B/A}$. □

As universal it might be, we still want a nice description of $\Omega_{B/A}$. Consider the A-module map $\mu : B \otimes_A B \to B$ extended from $\mu(b_1 \otimes b_2) = b_1 b_2$. This is also a B-algebra map for both the B-algebra structures $b \mapsto b \otimes 1$ and $b \mapsto 1 \otimes b$. We shall take the first structure as our convention.
Let $J = \ker \mu \subset B \otimes_A B$. Then J/J^2 is a B-module whose structure does not actually depend on which B-algebra structure on $B \otimes_A B$ we take.

Proposition 1.2. *The map* $\mathrm{d}' : B \to J/J^2$ *via* $b \mapsto (1 \otimes b - b \otimes 1) \bmod J^2$ *is a derivation, with associated B-module map $\Omega_{B/A} \to J/J^2$ an isomorphism.*

Proof. It's easy to check that d' is indeed a derivation.
The candidate isomorphism is $\psi : \Omega_{B/A} \to J/J^2, \mathrm{d}(b) \mapsto \mathrm{d}'(b)$. Consider $\phi : B \otimes_A B \to \Omega_{B/A}$ extending from $b \otimes b' \mapsto b \,\mathrm{d}b'$. J is generated by $\{1 \otimes b - b \otimes 1 : b \in B\}$ as a B-module. Now $\phi((1 \otimes b - b \otimes 1)(1 \otimes b' - b' \otimes 1)) = \mathrm{d}(bb') - b \,\mathrm{d}b' - b' \,\mathrm{d}b = 0$, so ϕ factors through $\bar{\phi} : B \otimes_A B/J^2$. Via calculations we find $\bar{\phi} \circ \psi = \mathrm{id}, \psi \circ \bar{\phi}|_{J/J^2} = \mathrm{id}$. □

The construction $\Omega_{B/A}$ has nice functorial properties:

$$\begin{array}{ccc} B & \longrightarrow & B' \\ \uparrow & & \uparrow \\ A & \longrightarrow & A' \end{array}$$

commutes in the category of rings, we get a B-module map $\Omega_{B/A} \to \Omega_{B'/A'}$ which makes

$$\begin{array}{ccc} \Omega_{B/A} & \longrightarrow & \Omega_{B'/A'} \\ {\scriptstyle d}\uparrow & & \uparrow{\scriptstyle d} \\ B & \longrightarrow & B' \end{array}$$

commute. This also induces a map $\Omega_{B/A} \otimes_B B' \to \Omega_{B'/A'}$, which is sometimes an isomorphism.

Proposition 1.3. *If $B' = B \otimes_A A'$, then the map $\Omega_{B/A} \otimes_B B' \to \Omega_{B'/A'}$ is an isomorphism.*

Proof. Immediate. □

So if $S \subset B$ is a multiplicative system, then $S^{-1}\Omega_{B/A} \cong \Omega_{S^{-1}B/A}$.

Example 1.1. Take the polynomial algebra $B = A[t_1, \ldots, t_n]$, then $\Omega_{B/A} = \bigoplus_i B\,\mathrm{d}t_i$ is free. Indeed, $B \otimes_A B = A[\{t_i \otimes 1, 1 \otimes t_i\}] \cong B[\{z_i\}], z_i = 1 \otimes t_i - t_i \otimes 1 \in J$. Thus $J = (z_1, \ldots, z_n), J^2 = (\{z_i z_j\})$ and $J/J^2 \cong \bigoplus_i (z_i \bmod J^2) = \bigoplus_i B\,\mathrm{d}t_i$. Similarly, for $B = A[\{t_i : i \in I\}]$ for an index I, we have $\Omega_{B/A} = \bigoplus_{i \in I} B\,\mathrm{d}t_i$. Any A-algebra B is canonically a quotient of an A-algebra of this form by factoring $A[\{t_b : b \in B\}]$.

What's next? Well, are we even doing algebra if exact sequence doesn't make an appearance.

Proposition 1.4. *Let $A \to B \to B/I = C$, then*

$$I/I^2 \xrightarrow{\delta : b \mapsto \mathrm{d}b \otimes 1} \Omega_{B/A} \otimes_B C \longrightarrow \Omega_{C/A} \longrightarrow 0$$

is an exact sequence of C-modules.

Proposition 1.5. *Let $A \to B \to C$, then*

$$\Omega_{B/A} \otimes_B C \longrightarrow \Omega_{C/A} \longrightarrow \Omega_{C/B} \longrightarrow 0$$

is an exact sequence of C-modules.

The proofs are simple verifications and left as exercises.

Example 1.2. Suppose L/K is a finite extension of fields, then $\Omega_{L/K} = 0$ iff L/K is separable. Indeed, if we let K_1 be an intermediate subfield with K_1/K separable and L/K_1 purely inseparable, then by primitive element theorem we have $K_1 = K(\alpha) \cong K[t]/(g(t))$ for some $g \in K[t]$ irreducible and $g(\alpha) = 0, g'(\alpha) \neq 0$. Using Proposition 1.4 on $K \to K[t] \to K_1$ gives $\Omega_{K_1/K} = 0$ as $g'(\alpha) \neq 0$. If $L = K_1$, then $\Omega_{L/K} = \Omega_{L/K_1} = 0$ by Proposition 1.5. If $L \neq K_1$, then there is some $K_1 \subset K_2 \subsetneq L = K_2(\beta)$ with $\beta^p = b \in K_2$ where $p = \operatorname{char} K$. We then have $\Omega_{L/K_2} = L\,\mathrm{d}t/Lf'(t)\,\mathrm{d}t = L\,\mathrm{d}\beta \neq 0$, therefore $\Omega_{L/K} \neq 0$.

By the way, why did we want to study Kähler differentials again? Let X be a smooth manifold, then associated with it is a tangent bundle $\pi : TX \to X$. If X is embedded in $\mathbb{R}^n$, then $\pi^{-1}(x) = T_x X$ is the tangent space of X at $x \in X$, which can be altenratively and intristically defined as the set of $\mathbb{R}$-linear maps $\mathrm{D} : C^\infty(X) \to \mathbb{R}$ such that $\mathrm{D}(fg) = f(x)\,\mathrm{D}g + g(x)\,\mathrm{D}f$. For example, when $X \subset \mathbb{R}^n$ is open and $x = (0, \ldots, 0)$, the directional derivatives at $(0, \ldots, 0)$ would give the tangent space at x. So indeed $T_x X$ is the collection of $\mathbb{R}$-derivations $C^\infty(X) \to \mathbb{R}$ where $\mathbb{R}$ is given the structure of a $C^\infty(X)$-module via evaluation. Algebraizing this then motivates the definition of $\Omega_{B/A}$.
This motivation makes us wonder how one might recover some familiar notions of (co)tangent spaces from $\Omega_{B/A}$.

Proposition 1.6. *Let $(A, \mathfrak{m})$ be a local k-algebra whose residue field is k (via the same inclusion). Then $\Omega_{A/k} \otimes_A k \cong \mathfrak{m}/\mathfrak{m}^2$.*

Proof. Applying Proposition 1.4 to $k \to A \to A/\mathfrak{m} = k$ gives a surjection $\mathfrak{m}/\mathfrak{m}^2 \to \Omega_{A/k} \otimes_A k$ since $\Omega_{k/k} = 0$.
For the other direction, observe that $A = k \oplus \mathfrak{m}$ as k-vector spaces, and $R = A/\mathfrak{m}^2 = k \oplus (\mathfrak{m}/\mathfrak{m}^2)$ is a k-algebra with multiplication $(a, b)(a', b') = (aa', ab' + a'b)$. $\mathrm{D} : R \to \mathfrak{m}/\mathfrak{m}^2, (a, b) \mapsto b$ is an element of $\mathrm{Der}_k(R, \mathfrak{m}/\mathfrak{m}^2)$, hence is induced by a k-derivation $A \to \mathfrak{m}/\mathfrak{m}^2$ via $A \to R$, i.e. a linear map $\Omega_{A/k} \to \mathfrak{m}/\mathfrak{m}^2$. This factors through $\Omega_{A/k} \otimes_A k \to \mathfrak{m}/\mathfrak{m}^2$ which gives the inverse. □

Let's sheafify all these as we ultimately want to talk about geometry. Let $f : X \to Y$ be a morphism of schemes. We want to define a quasicoherent sheaf $\Omega_{X/Y}$ of $\mathcal{O}_X$-modules on X and a map $\mathrm{d} : \mathcal{O}_X \to \Omega_{X/Y}$ which is $f^{-1}\mathcal{O}_Y$-linear and on local sections satisfy $\mathrm{d}(ss') = s\,\mathrm{d}s' + s'\,\mathrm{d}s$ and $\mathrm{d}(s) = 0$ for any local section of $f^{-1}\mathcal{O}_Y$.
There are a few equivalent ways to formulate this. For open affines $U = \operatorname{Spec} B \subset X, V = \operatorname{Spec} A \subset Y$ with $f(U) \subset V$, we can identify $\Omega_{X/Y}|_U = \tilde{\Omega}_{B/A}$, the quasicoherent $\mathcal{O}_U$ induced by $\Omega_{B/A}$. Since $\Omega_{B/A}$ is compatible with localisations, this glue to define a quasicoherent $\mathcal{O}_X$-module and the maps $\mathrm{d} : B \to \Omega_{B/A}$ induce a map $\mathrm{d} : \mathcal{O}_X \to \Omega_{X/Y}$ satisfying the desired properties.
Another way to do this is the following: Recall $\Omega_{B/A} \cong J/J^2$ where $J = \ker(B \otimes_A B \to B)$. The map $B \otimes_A B \to B$ induces a map $\operatorname{Spec} B \to \operatorname{Spec} B \otimes_A B = \operatorname{Spec} B \times_{\operatorname{Spec} A} \operatorname{Spec} B$ which is the diagonal map. This inspires us to do the following: Consider the diagonal morphism $\Delta = \Delta_{X/Y} : X \to X \times_Y X$ which is an immersion (i.e. factors as $\Delta = j \circ i$ where $i : X \to U$ is a closed immersion and $j : U \to X \times_Y X$ is an open immersion). Let $\mathscr{I}_{X/U}$ be the ideal sheaf of i. We can then define $\Omega_{X/Y} = i^*(\mathscr{I}_{X/U}/\mathscr{I}^2_{X/U})$. This is quasicoherent since $\mathscr{I}_{X/U}$ is a quasicoherent sheaf of ideals (and i is a closed immersion). It's clear that these two constructions coincide.
The exact sequences we had before also have sheafified forms. Suppose $i : Z \to X$ is a closed subscheme defined by a quasicoherent sheaf of ideals $\mathscr{I} \subset \mathcal{O}_X$. Then

$$\mathscr{I}/\mathscr{I}^2 \longrightarrow i^*\Omega_{X/Y} \longrightarrow \Omega_{Z/Y} \longrightarrow 0$$

is exact, where $i^*\Omega_{X/Y} = i^{-1}\Omega_{X/Y} \otimes \mathcal{O}_Z$ is the module pullback. Moreover, if $X \to Y \to S$ are morphisms (with $f : X \to Y$), then

$$f^*\Omega_{Y/S} \longrightarrow \Omega_{X/S} \longrightarrow \Omega_{X/Y} \longrightarrow 0$$

is also exact.
Let k be a field and X a k-scheme. We define the cotangent space to X at $x \in X$ to be $\Omega_{X/k}(x) = \Omega_{X/k,x} \otimes_{\mathcal{O}_{X,x}} k(x)$, which is a $k(x)$-vector space. If in addition that $k(x) = k$ (via the k-scheme structure), then $\Omega_{X/k}(x) \cong \mathfrak{m}_x/\mathfrak{m}_x^2$ where $\mathfrak{m}_x$ is the maximal ideal of $\mathcal{O}_{X,x}$.

Definition 1.8. Let X be a k-scheme and suppose $x \in X$ has $k(x) = k$. The tangent space of X at x is $T_{X,x} = \mathrm{Hom}_k(\Omega_{X/k}(x), k)$.

Proposition 1.7. *There is a canonical bijection*

$$T_{X,x} \cong \left\{ \textit{morphisms of } k\textit{-schemes } f : \operatorname{Spec} k[\epsilon]/(\epsilon^2) \to X \textit{ with image } x \right\}$$

$k[\epsilon]/(\epsilon^2)$ is known as the ring of dual numbers of k. It has a unique prime ideal (ϵ) at which the local ring is $k[\epsilon]/(\epsilon^2)$.

Proof. To give such a morphism f is to give a local k-algebra homomorphism $\phi : \mathcal{O}_{X,x} \to k[\epsilon]/(\epsilon^2)$. As $\mathcal{O}_{X,x} = k \oplus \mathfrak{m}_x$ (noting $k(x) = k$), ϕ is determined by $\phi|_{\mathfrak{m}_x} : \mathfrak{m}_x \to k\epsilon \leq k[\epsilon]/(\epsilon^2)$. Since $\epsilon^2 = 0$, we have $\phi(\mathfrak{m}_x^2) = 0$, so $\phi|_{\mathfrak{m}_x}$ factors through an element of $\mathrm{Hom}_k(\mathfrak{m}_x/\mathfrak{m}_x^2, k\epsilon) \cong \mathrm{Hom}_k(\mathfrak{m}_x/\mathfrak{m}_x^2, k)$. □

1.3 The Functor of Points

The underlying topological space of a scheme is notoriously unintuitive. For $(a_i) \in k^n$, $(T_1 - a_1, \ldots, T_n - a_n)$ is always a closed point in $\mathbb{A}_k^n$, but when $k \neq \bar{k}$ there can be other closed points.
Also, the topological space of $X \times_S Y$ is not usually the (topological) fibre products of the underlying spaces. There are cases where fibre product is well-behaved, e.g. the fibre of a morphism. But if we take $X = Y = \operatorname{Spec} \mathbb{C}, S = \operatorname{Spec} \mathbb{Q}$, $X \times_S Y$ has uncountably many points despite X, Y, S all only have one point. If $k \neq \bar{k}$ and we take $X = Y = \mathbb{A}_k^1, S = \operatorname{Spec} k$, then the closed points of $X \times_S Y = \mathbb{A}_k^2$ aren't even the product of closed points of $\mathbb{A}_k^1$ with itself.
However, there is a good sense in which we can realise the "points" of $X \times Y$ can be viewed as the "product" of the "points" of X and the "points" of Y.
Denote the category of schemes by (Sch), the category of (unital commutative) rings by (Rings) and the category of sets by (Sets).

Definition 1.9. For schemes X, Y, the collection of Y-valued points in X is $X(Y) = \mathrm{Hom}_{(\mathsf{Sch})}(Y, X)$. When $Y = \operatorname{Spec} R$ is affine we write $X(R) = X(\operatorname{Spec} R)$ (the "R-valued points").

Example 1.3. 1. Let $X = \mathbb{A}_{\mathbb{Z}}^n$, then

$$X(R) = \mathrm{Hom}_{(\mathsf{Sch})}(\operatorname{Spec} R, \mathbb{A}_{\mathbb{Z}}^n) = \mathrm{Hom}_{(\mathsf{Rings})}(\mathbb{Z}[T_1, \ldots, T_n], R) = R^n$$

2. Every scheme X has a "tautological" (or "universal") point $\mathrm{id}_X : X \to X$.

Definition 1.10. The functor of points of X is the functor $\hat{h}_X : (\mathsf{Sch})^{\mathrm{op}} \to (\mathsf{Sets})$ via $Y \mapsto X(Y)$ and $(f : Y' \to Y) \mapsto (X(Y) \to X(Y'), g \mapsto g \circ f)$.

$\hat{h}_X$ is also called the presheaf associated to X, since a presheaf on a topological space can be viewed as a contravariant functor from the category of open sets on the topological space to the category of abelian groups. The notion of a morphisms between presheaves also has a category theoretic generalisation:

Definition 1.11. Suppose $\mathcal{F}, \mathcal{G} : \mathcal{C}^{\mathrm{op}} \to \mathcal{D}$ are functors. A morphism (or natural transformation) $\phi : \mathcal{F} \to \mathcal{G}$ is a collection of morphisms $\phi_Y : \mathcal{F}(Y) \to \mathcal{G}(Y)$ such that

$$\begin{array}{ccc} \mathcal{F}(Y) & \xrightarrow{\phi_Y} & \mathcal{G}(Y) \\ {\scriptstyle \mathcal{F}(g)}\downarrow & & \downarrow{\scriptstyle \mathcal{G}(g)} \\ \mathcal{F}(Y') & \xrightarrow[\phi_{Y'}]{} & \mathcal{G}(Y') \end{array}$$

commutes for every $g : Y' \to Y$.

Lemma 1.8 (Yoneda Lemma for (Sch))**.** *If X, X' are schemes,* $\mathrm{Hom}_{(\mathsf{Sch})}(X', X)$ *is in bijection with* $\mathrm{Nat}(\hat{h}_{X'}, \hat{h}_X)$*.*

Here, $\mathrm{Nat}(\hat{h}_{X'}, \hat{h}_X)$ is the collection of natural transformations from $\hat{h}_{X'}$ to $\hat{h}_X$.

Proof. For a morphism $f : X' \to X$, we identify the natural transformation given by $\phi_Y : X'(Y) \to X(Y), g \mapsto f \circ g$. Conversely, a natural transformation $\phi : \hat{h}_{X'} \to \hat{h}_X$ gives rise to the morphism $\phi_{X'}(\mathrm{id}_{X'})$. □

The same proof works in any locally small category, not just schemes. But in the case of schemes, we have some extra structure to work with which gives rise to a more intricate version of Yoneda lemma.

Definition 1.12. $h_X : (\mathsf{Rings}) \to (\mathsf{Sets})$ is the restriction of $\hat{h}_X$ to affine schemes (recall that Spec is an equivalence of categories from (Rings) to the opposite category of the category of affine schemes).

Proposition 1.9. $\mathrm{Hom}_{(\mathsf{Sch})}(X', X)$ *is in bijection with* $\mathrm{Nat}(h_{X'}, h_X)$*.*

Proof. Morphisms $Y \to X$ are determined by their restrictions to affine pieces of Y. □

For a scheme S, let (Sch/S) be the category of S-schemes (i.e. objects are morphisms $X \to S$ and morphisms are morphisms $X' \to X$ commuting with $X \to S, X' \to S$). Let (Aff/S) be the subcategory of affine S-schemes. We can similarly define $\hat{h}_{X/S} : (\mathsf{Sch}/S)^{\mathrm{op}} \to (\mathsf{Sets})$ and $\hat{h} : (\mathsf{Aff}/S)^{\mathrm{op}} \to (\mathsf{Sets})$ and they will have the same properties we described above.
An S-scheme X admits a universal point $\mathrm{id}_X : X \to X$ and a "universal pair of points" $\mathrm{pr}_1, \mathrm{pr}_2 : X \times_S X \to S$. Let's use this to explain why the diagonal morphism sneaks in when we are trying to define Kähler differentials.
Imagine we are in the eighteenth century and we want to do calculus. For a point x, we are often interested in $x' = x + \delta x$ for some "infinitesimal" δx, whatever it means. Accompanying this is $\delta f = f(x') - f(x)$ which in turn determines a "common ration" $\delta f/\delta x$. In algebraic geometry, infinitesimals are mimicked with a square zero. For an S-scheme T and a closed subscheme $T_0 \subset T$ given by the ideal sheaf $\mathscr{I} = \mathscr{I}_{T_0/T}$ with $\mathscr{I}^2 = 0$ (in particular, the morphism $T_0 \hookrightarrow T$ is a homeomorphism). One example of this is $T_0 = \mathrm{Spec}\, k, T = \mathrm{Spec}\, k[\epsilon]/(\epsilon^2)$.
Suppose $x, x' \in X(T) = \mathrm{Hom}_S(T, X)$ have $x'|_{T_0} = x|_{T_0}$ ("infinitesimal close

points"), then for a local section f of $\mathcal{O}_X$ can be associated with $\delta f = x'^* f - x^* f$.

$$\begin{array}{ccc} T & \xrightarrow{(x,x')} & X \times_S X \\ \uparrow & & \uparrow{\scriptstyle \Delta_{X/S}} \\ T_0 & \longrightarrow & X \end{array}$$

Let $\mathscr{J}$ be the ideal sheaf of $\Delta_{X/S}$, then $(x,x')^*\mathscr{J} \subset \mathscr{I}$ and thus $(x,x')^*\mathscr{J}^2 = 0$. That is, (x,x') factors through a morphism $T \to \Delta^{(1)}_{X/S}$ via $\mathrm{pr}_1, \mathrm{pr}_2$, where $\Delta^{(1)}_{X/S}$ (the "first infinitesimal neighbourhood of the diagonal") is the locally closed subscheme of $X \times_S X$ with ideal sheaf $\mathscr{J}^2$ (we can also define $\Delta^{(n)}_{X/S}$ by replacing $\mathscr{J}^2$ with $\mathscr{J}^{n+1}$). This means that $\mathrm{pr}_1, \mathrm{pr}_2 : \Delta^{(1)}_{X/S} \to X$ is the universal pair of infintesimally close points. Thus $\delta f = x'^* f - x^* f = (x,x')^*(\mathrm{pr}_2^* f - \mathrm{pr}_1^* f) = (x,x')^*(1 \otimes f - f \otimes 1 \bmod \mathscr{J}^2)$. But $1 \otimes f - f \otimes 1 \bmod \mathscr{J}^2$ is just $\mathrm{d}f$!
Let's go back to the main story line.

Definition 1.13. Suppose $\mathcal{C}, \mathcal{D}$ are (locally small) categories. A functor $F : \mathcal{C} \to \mathcal{D}$ is faithful if the natural map $\mathrm{Hom}_{\mathcal{C}}(X,Y) \to \mathrm{Hom}_{\mathcal{D}}(FX, FY)$ induced by it is injective. If in addition that it is surjective, we say it is fully faithful.

So what (the general version of) Yoneda lemma is really saying is that the functor $X \mapsto \mathrm{Hom}_{\mathcal{C}}(-, X)$ (with the latter considered as an object in the category $\mathsf{Funct}(\mathcal{C}^{\mathrm{op}}, (\mathsf{Sets}))$ of functors $\mathcal{C}^{\mathrm{op}} \to (\mathsf{Sets})$) is fully faithful. In other words, $\mathcal{C}$ can be identified with a full subcategory (i.e. with a subclass of objects and all the original morphisms between them) of $\mathsf{Funct}(\mathcal{C}^{\mathrm{op}}, (\mathsf{Sets}))$.

Definition 1.14. A functor $F : \mathcal{C}^{\mathrm{op}} \to (\mathsf{Sets})$ is represented by an object X (or simply "representable" if we don't care about X) of $\mathcal{C}$ if there is a natural isomorphism $\phi : F \to \mathrm{Hom}(-, X)$.

Yoneda lemma can then be further rephrased to the statement that the pair (X, ϕ), if exists, is unique up to unique isomorphism. That is, if (X', ϕ') also represents F, then there is a unique isomorphism $f : X' \to X$ such that the map $\phi^{-1} \circ \phi' : \mathrm{Hom}_{\mathcal{C}}(-, X') \to \mathrm{Hom}_{\mathcal{C}}(-, X)$ is given by composition with f.

Example 1.4. For $X, Y \in (\mathsf{Sch}/S)$, $X \times_S Y$ represents the functor $(\mathsf{Sch}/S)^{\mathrm{op}} \to (\mathsf{Sets}), T \mapsto X(T) \times Y(T)$. This "fixes" the problem with products of schemes.

The natural question, then, is to ask exactly which functors $(\mathsf{Sch})^{\mathrm{op}} \to (\mathsf{Sets})$ is representable. A version of this question is known as descent. If $Y = \bigcup_\alpha U_\alpha$ is an open cover of a scheme Y, then by glueing of morphisms,

$$\mathrm{Hom}_{(\mathsf{Sch})}(Y, X) \cong \{(f_\alpha : U_\alpha \to X)_\alpha : \forall \alpha, \beta, f_\alpha|_{U_\alpha \cap U_\beta} = f_\beta|_{U_\alpha \cap U_\beta}\}$$

That is,

$$X(Y) \longrightarrow \prod_\alpha X(U_\alpha) \rightrightarrows \prod_{\alpha,\beta} X(U_\alpha \cap U_\beta)$$

is an equaliser. But this looks like it's just saying that $\hat{h}_X$ is a sheaf!
Consequently, $F \equiv \mathbb{Z}$ is not representable.

1.4 Étale Morphisms

Example 1.5. Let $X \subset \mathbb{C}^2$ be a conic given by the equation $y = x^2$. We get a map $X \to \mathbb{C}$ given by $(x, y) \mapsto y$. At any $p \neq (0,0)$ in X, f is a local homeomorphism under the complex topology, and the theory of branched covers in Euclidean spaces is more or less based on such ideas.
However, being algebraic geometers, we don't have the luxury of complex topology. The one we do have, that is Zariski topology, is far too big for such kind of statements to generalise.
However, if you squint hard enough, one of the ways one justify that f is a local homeomorphism is by observing that $\mathrm{d}y/\mathrm{d}x|_p \neq 0$ whenever $p \neq (0,0)$ – this is a algebraic statement! We will use this idea to define étale morphisms which does a pretty good job at capturing the geometric picture we had for coverings.

As usual, we will start with a terrible definition, and work our ways towards a proper one.

Definition 1.15. A morphism $f : X \to Y$ is étale at $x \in X$ if there are affine opens $U = \operatorname{Spec} B \ni x, V = \operatorname{Spec} A \ni f(x)$ such that $f(U) \subset V$ and there is an identification $B = A[T_1, \ldots, T_n]/I$ via $f|_U$ where $I = (g_1, \ldots, g_n)$ and $\det J \in A[T_1, \ldots, T_n]$ does not restrict to 0 on $k(x)$ (via the canonical homomorphism to B) where $J = (\partial g_j / \partial T_i)_{ij}$ is the Jacobian.

You can see why this is a bad definition: The sheer amount of different possible choices there is both alarming and enraging. Nonetheless, we shall explore some examples and properties of étale morphisms defined in this way before we move on to a better definition.

Example 1.6. To recover our first example, we can take $A = \mathbb{C}[T_0]$ and $B = \mathbb{C}[T_0, T_1]/(T_1^2 - T_0) = A[T_1]/(g_1)$ where $g_1 = T_1^2 - T_0$. $J = \partial g_1 / \partial T_1 = 2T_1$ is invertible at every closed point $p \neq (0,0)$, hence étale at every such point. It's not hard to see that it is also étale at the generic point, which is a phenomenon that generalises, we we will see later.

Any open immersions are étale, as such morphisms are local isomorphisms and thus we can take $B = A$. It's also clear that all étale morphisms are locally of finite presentation.

Proposition 1.10. *$\{x \in X : f$ étale at $x\}$ is open.*

Proof. Suppose f is étale at x and let A, B be as in the definition, then f is étale at every $x' \in D(J \bmod I) \cong \operatorname{Spec} B[1/J]$. □

Similarly, being étale is a local property both on the source and on the target. One should also expect that being an étale morphism also has hardly anything to do with the global properties (e.g. quasicompactness, separatedness) of the morphism.

Example 1.7. Let X be the line with two origins and $f : X \to \mathbb{A}^1$ be the natural projection, then f is étale as it's a local isomorphism, but it's in general not separated.

Proposition 1.11. *Suppose $f : X \to Y$ is étale and $Y' \to Y$ is a morphism, then the base change $f' : X \times_Y Y' \to Y'$ is also étale.*

Proof. If f is locally given by $B = A[T_1, \ldots, T_n]/(g_1, \ldots, g_n)$, then f' is locally given by $B = A'[T_1, \ldots, T_n]/(\bar{g}_1, \ldots, \bar{g}_n)$ where $\bar{g}_i$ are the respective images of g_i under the base change. □

Here comes a property that will be crucial to motivate a better definition of étale morphisms

Proposition 1.12. *If f is étale, then $\Omega_{X/Y} = 0$.*

Proof. Suppose $x \in X$ and f is locally given as $B = A[T_1, \ldots, T_n]/(g_1, \ldots, g_n)$, then $\Omega_{B/A} = (\bigoplus_i B\,\mathrm{d}T_i) \,/\, \left(\sum_j B\,\mathrm{d}g_j\right)$, therefore

$$\Omega_{X/Y,x} = \Omega_{B/A} \otimes_B B_x = \operatorname{coker}\left(\left(\frac{\partial g_j}{\partial T_i}\right)_{ij} : B_x^n \to B_x^n\right) = 0$$

by hypothesis. □

As per tradition of defining a new kind of maps, we want to know if it behaves well under composition.

Proposition 1.13. *Composition of étale maps is étale.*

Proof. If $B = A[T_1, \ldots, T_n]/(g_1, \ldots, g_n), C = B[T_{n+1}, \ldots, T_m]/(g_{n+1}, \ldots, g_m)$ are étale, then we have the finite presentation $C = A[T_1, \ldots, T_m]/(g_1, \ldots, g_m)$ and its Jacobian would be upper block-diagonal with two diagonal blocks that are the Jacobians of B/A and C/B respectively. □

Example 1.8. Let L/K be a field extension, we claim that $\operatorname{Spec} L \to \operatorname{Spec} K$ is étale if and only if L/K is finite and separable. The "if" part is clear by primitive element theorem. For the "only if" part, the condition of being étale means that $L = K[T_1, \ldots, T_n]/(g_1, \ldots, g_n)$. As L is a field, $(g_1, \ldots, g_n)$ is maximal and hence L/K is finite by Noether normalisation. Separability on the other hand follows from Proposition 1.12.

Proposition 1.14. *If $f : X \to Y$ is étale, then for all $y \in Y$ the fibre $f^{-1}(y)$ is a disjoint union of spectra of finite separable extensions of $k(y)$.*

Proof. Proposition 1.11 means that we need only to consider the case $Y = \operatorname{Spec} k$. As $f : X \to \operatorname{Spec} k$ is étale, it is in particular locally of finite type. Suppose $x \in X$ is closed and consider $X' = X \times_{\operatorname{Spec} k} k' \ni x' = (x, *)$ where $k' = k(x)$. $\Omega_{X'/k} = 0$ as X' is étale over $\operatorname{Spec} k'$, so $\Omega_{X'/k'}(x') \cong m_{x'}/m_{x'}^2 = 0$. Then $m_{x'} = 0$ as $\mathcal{O}_{X',x'}$ is Noetherian, i.e. $\mathcal{O}_{X',x'} = k'$, thus $\mathcal{O}_{X,x} = k'$. This means that locally $X = \operatorname{Spec} B$ where B is a finite type k-algebra of dimension 0, i.e. a finite product of its local rings. So B is a finite product of fields, and hence X is a disjoint union of spectra of fields, all of which have to be finite separable extensions of $k = k(y)$ by the previous example. □

Example 1.9. Suppose L/K is a finite separable extension of local fields, then $\operatorname{Spec} \mathcal{O}_L \to \operatorname{Spec} \mathcal{O}_K$ is étale iff L/K is unramified, i.e. we can choose the same uniformiser $\pi_L = \pi_K$ and the extension of residue fields $\mathcal{O}_K/(\pi_K) \to \mathcal{O}_L/(\pi_L)$ is separable. We know the "only if" part from the last example. The "if" part follows from the fact that if L/K is unramified then $\mathcal{O}_L = \mathcal{O}_K[T]/(g)$ where g is separable modulo π_K.

Definition 1.16. A ring homomorphism $A \to B$ is called étale if $\operatorname{Spec} B \to \operatorname{Spec} A$ is étale.

It is not obvious that B has to have finite presentation over A for it to be étale, but it is true.
Let $B = P/I$ where $P = A[\{T_\alpha\}]$ and $I \leq P$ is an ideal. Recall from Proposition 1.4 that we have an exact sequence

$$I \otimes_P B = I/I^2 \xrightarrow{\delta} \Omega_{P/A} \otimes_P B \longrightarrow \Omega_{B/A} \longrightarrow 0$$

To be precise, δ takes $f \bmod I^2$ to $\mathrm{d}f \otimes 1$. We also know that $\Omega_{P/A} \otimes_P B = \bigoplus_\alpha B(\mathrm{d}T_\alpha \otimes 1)$ is a free B-module.

Definition 1.17. We say B/A is basic étale if there exists a presentation $B = A[T_1, \dots, T_n]/(g_1, \dots, g_n)$ with $\det J$ invertible in B.

Proposition 1.15. *B/A is basic étale iff there exists a presentation $B = P/I$ where P is a finite type A-polynomial algebra and $I \leq P$ is finitely generated such that δ is an isomorphism.*

Proof. Suppose B/A is basic étale, then we get

$$B^n \xrightarrow{(g_j)} I/I^2 \xrightarrow{\delta} \Omega_{P/A} \otimes B = \textstyle\bigoplus_{i=1}^n B(\mathrm{d}T_i \otimes 1)$$

The composite of these maps is invertible by hypothesis, which then forces δ to be an isomorphism as (g_j) is surjective.
Conversely, suppose $P = A[T_1, \dots, T_n]$ and δ is an isomorphism, then I/I^2 is free of rank n. Suppose $g_1, \dots, g_n \in I$ map to a B-basis of T/T^2. Let $M = I/(g_1, \dots, g_n)$, then $IM = (I^2 + (g_1, \dots, g_n))/(g_1, \dots, g_n) = M$. By Nakayama's lemma, there is some $h \in 1 + I$ with $hM = 0$, hence $I_h = (g_1, \dots, g_n)_h$, so

$$B = B_h = P_h/I_h = P_h/(g_1, \dots, g_n) = A[T_0, \dots, T_n]/(hT_0 - 1, g_1, \dots, g_n)$$

which is basic étale. ☐

Corollary 1.16. *Let $f : X \to Y$ be locally of finite presentation, then f is étale iff it is locally isomorphic to $\operatorname{Spec} B/\operatorname{Spec} A$ where the second statement in the preceding proposition holds.*

$\operatorname{coker} \delta = \Omega_{B/A}$ doesn't depend on presentation in general. In fact, $\ker \delta$ doesn't depend on presentation either. Given two presentations $I \to P \to B, I' \to P' \to B'$, then there is some $\phi : P \to P'$ such that

$$\begin{array}{ccccc} I & \longrightarrow & P & \longrightarrow & B \\ & & \phi\big\downarrow & \nearrow & \\ I' & \longrightarrow & P' & & \end{array}$$

commutes since P is a polynomial algebra. Then necessarily $\phi(I) \subset I'$. This gives

$$\begin{array}{ccccccc} I/I^2 & \xrightarrow{\delta} & \Omega_{P/A} \otimes_P B & \longrightarrow & \Omega_{B/A} & \longrightarrow & 0 \\ \big\downarrow & & \big\downarrow & & \big\downarrow\cong & & \\ I'/(I')^2 & \xrightarrow[\delta']{} & \Omega_{P'/A} \otimes_{P'} B & \longrightarrow & \Omega_{B/A} & \longrightarrow & 0 \end{array}$$

By some commmutative algebra, this diagram induces an isomorphism $\ker \delta \cong \ker \delta'$, which doesn't even depend on ϕ. Thus $\Gamma_{B/A} = \ker \delta = \ker \delta'$ is well-defined up to unique isomorphism.

1.5 Smooth Morphisms

On an intuitive level, smooth morphisms should be things that are "locally analytically" isomorphic to projections $\mathbb{R}^m \times Y \to Y, \mathbb{C}^m \times Y \to Y$.

Proposition 1.17. *Let $f : X \to Y$ be a morphism and $x \in X, d \geq 0$. Then the followings are equivalent:*
(i) There exists an open neighbourhood $U \subset X$ of x and $p : U \to \mathbb{A}^d_{\mathbb{Z}} \times_{\operatorname{Spec} \mathbb{Z}} Y = \mathbb{A}^d_Y$ étale at x such that $f|_U = \operatorname{pr}_Y \circ p$.
(ii) There are open affines $U = \operatorname{Spec} B \subset X, V = \operatorname{Spec} A \subset Y$ with $x \in U, f(U) \subset V$ such that B has a presentation $B = A[T_1, \ldots, T_{n+d}]/(g_1, \ldots, g_n)$ with the Jacobian having full rank n.

Definition 1.18. If any of the above happens, we say f is smooth at x of relative dimension d, and smooth if it is smooth at all $x \in X$.

Proof. (ii) $\implies$ (i): By reordering the variables, we may assume WLOG that $\Delta = \det((\partial g_j / \partial T_i)_{1 \leq i \leq n, 1 \leq j \leq n}) \neq 0$ at x. Consider $p : U = \operatorname{Spec} B \to \mathbb{A}^d_A \subset \mathbb{A}^d_Y$ given by $A' = A[T_{n+1}, \ldots, T_{n+d}] \to B = A'[T_1, \ldots, T_n]/(g_1, \ldots, g_n)$ which is étale at x over A'.
(i) $\implies$ (ii): Shrinking U if necessary, we may assume WLOG that $p(U) \subset \mathbb{A}^n_V$ for some affine $V = \operatorname{Spec} A \subset Y$, and that there is a distinguished open $V' = D(h) = \operatorname{Spec} A' \subset \mathbb{A}^d_V$ for some $h \in A[T_1, \ldots, T_d], A' = A[T_1, \ldots, T_d]_h$ such that $B = A'[T_{d+1}, \ldots, T_{d+n}]/(g_1, \ldots, g_n)$ has its Jacobian invertible at x. Then $B = A[T_0, T_1, \ldots, T_{n+d}]/(g_0 = hT_0 - 1, g_1, \ldots, g_n)$ satisfies (ii). $\square$

Definition 1.19. A nonsingular variety over a field k is a smooth separated k-scheme of finite type.

Proposition 1.18. *A morphism $f : X \to Y$ is smooth iff it is covered by $\operatorname{Spec} B \to \operatorname{Spec} A$ where $B = P/I = A[T_1, \ldots, T_n]/I$ is a finite presentation of A such that the map $\delta : I/I^2 \to \Omega_{P/A} \otimes_P B$ is a split injection.*

Proof. Suppose f is smooth. Since the conditions are local, we may assume $X = \operatorname{Spec} B$ is étale over $\mathbb{A}^n_A = \operatorname{Spec} P_0, P_0 = A[T_1, \ldots, T_d]$ and P is a polynomial algebra over P_0. Then $I/I^2 \cong \Omega_{P/P_0} \otimes_P B$ as $X \to \mathbb{A}^d_A$ is étale, and thus $\Omega_{P/A} \cong \Omega_{P/P_0} \oplus \bigoplus_{i=1}^d P \, \mathrm{d}T_i$ which is a split injection.
Conversely, suppose $A \to B = P/I$ is such that δ is a split injection $I/I^2 \hookrightarrow \Omega_{P/A} \otimes_P B = \bigoplus_{i=1}^n B(\mathrm{d}T_i \otimes 1)$. For $x \in \operatorname{Spec} B$, after possibly reordering T_i we may assume that $\mathrm{d}T_1 \otimes 1, \ldots, \mathrm{d}T_d \otimes 1$ generate a complement of I/I^2 in a neighbourhood $\operatorname{Spec} B_h$ of x. Replacing P by $P[T_0]$ and I by $(I, hT_0 - 1)$ allows us to further reduce to the case where $\Omega_{P/A} \otimes_P B = I/I^2 \oplus \bigoplus_{i=1}^d B(\mathrm{d}T_i \otimes 1)$. Now let $P_0 = A[T_1, \ldots, T_d]$, then $I/I^2 \cong \Omega_{P/P_0} \otimes_P B$, thus $\operatorname{Spec} B$ is étale over $\operatorname{Spec} P_0 = \mathbb{A}^d_A$. Then $\operatorname{Spec} B$ is smooth of relative dimension d at x and d is the rank of $\Omega_{P/A} \otimes B/(I/I^2)$, which is just the rank of $\Omega_{X/Y,x}$. $\square$

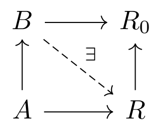
Remark. This means that $\Omega_{X/Y} = \operatorname{coker} \delta$ is locally free if X/Y is smooth. The proof also shows that if f is smooth of relative dimension d then $\Omega_{X/Y}$ has rank d.

Corollary 1.19. *Suppose $X \to \operatorname{Spec} k$ is smooth of relative dimension d and $x \in X$ is a closed point, then $\mathfrak{m}_x/\mathfrak{m}_x^2$ has dimension d.*

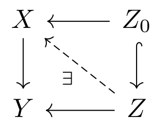
1.6 Infinitesimal Criteria

As promised, we now turn to better criteria for a map to be étale and smooth. There are two motivations for this. Firstly, a étale morphism is morally a local isomorphism. It is then very tempting to characterise this from the level of tangent space. This is however a condition too weak to work, so we turn to looking at higher order neighbourhoods ("infinitesimally close points of X and those of Y").
Another motivation comes from a more algebraic point of view. Smooth morphisms want to mimic the map $\mathbb{A}^n_Y = \operatorname{Spec} A[T_1, \dots, T_d] \to Y = \operatorname{Spec} A$. The universal property of polynomial algebras is that they lift surjections of A-algebras. If we weaken this and only look at surjections with nilpotent kernel, we actually do end up with a criterion for smoothness.

Definition 1.20. An A-algebra B is formally smooth if for any surjective A-algebra homomorphism $R \to R_0$ with square-zero kernel, the induced map $\operatorname{Hom}_A(B, R) \to \operatorname{Hom}_A(B, R_0)$ is surjective.



Definition 1.21. A morphism $f : X \to Y$ is formally smooth if for every affine Y-scheme $Z = \operatorname{Spec} R$ and closed subscheme $Z_0 \subset Z$ defined by a square-zero ideal sheaf, $\operatorname{Hom}_Y(Z, X) \to \operatorname{Hom}_Y(Z_0, X)$ is surjective.



Remark. If B/A is formally smooth, then for every surjective A-algebra homomorphism $R \to R_0$ with nilpotent kernel, $\operatorname{Hom}_A(B, R) \to \operatorname{Hom}_A(B, R_0)$ is surjective. Indeed, if $I = \ker(R \to R_0)$ is such that $I^M = 0$, then we get a chain of surjections $R = R/I^{2^k} \to \cdots \to R/I^4 \to R/I^2 \to R_0$, each with a square-zero kernel.

Analogously,

Definition 1.22. $A \to B$ (resp. $X \to Y$) is formally unramified if the map $\operatorname{Hom}_A(B, R) \to \operatorname{Hom}_A(B, R_0)$ (resp. $\operatorname{Hom}_Y(Z, X) \to \operatorname{Hom}_Y(Z_0, X)$) as in before is injective. It is formally étale if the map is an isomorphism.

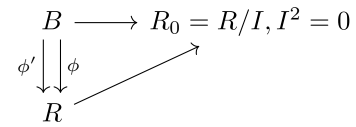
Remark. 1. If f is formally étale, then the map we considered is in fact bijective for every Z, not necessarily affine. Indeed, for general Z, we can cover it by open affines. Any morphism $Z_0 \to X$ then has a unique extension to Z on each of these affines, so they glue to give a global morphism.
2. To check f is formally smooth, it suffices to show the surjectivity locally. Suppose $Z = \bigcup_i V_i$, then $r : Z_0 \to X$ lifts to $\tilde{r}_i : V_i \to X$. They don't

necessarily glue (contrary to the étale case) due to the lack of uniqueness, but if we consider $\tilde{r}_i, \tilde{r}_j$ should differ by a section of $\underline{\mathrm{Hom}}(r^*\Omega_{X/Y}, \mathscr{I}_{Z_0/Z})$ (where $\underline{\mathrm{Hom}}$ denotes the sheaf Hom). Thus we get a Čech 1-cocycle on Z_0 with coefficients in $\underline{\mathrm{Hom}}(r^*\Omega_{X/Y}, \mathscr{I}_{Z_0/Z})$. But Z_0 is affine, so $H^1(Z_0, \underline{\mathrm{Hom}}(r^*\Omega_{X/Y}, \mathscr{I}_{Z_0/Z})) = 0$ and therefore we can modify $\tilde{r}_i$'s by the coboundary to get a global lifting.

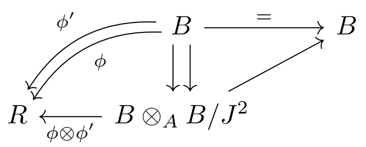
Proposition 1.20. *Suppose $B = P/I$ is a presentation where P is a polynomial algebra over A not necessarily of finite type. As usual consider $\delta : I/I^2 \to \Omega_{P/A} \otimes B$. Then B/A is*
(i) Formally smooth if δ is a split injection.
(ii) Formally étale if δ is an isomorphism.
(iii) Formally unramified if δ is surjective (i.e. $\operatorname{coker}\delta = \Omega_{B/A} = 0$).

Roughly speaking, $\ker\delta$ is the obstruction to the existence of an infinitesimal life, and $\operatorname{coker}\delta$ measures how many lifts there are, if one exists.

Proof. Let's prove (iii). B/A is formally unramified iff



implies $\phi = \phi'$. Let $J = \ker(B \otimes_A B \to B)$. The diagram



then gives the result. ☐

Definition 1.23. We say f is unramified if $\Omega_{X/Y} = 0$ and f is locally of finite type ("Raynaud condition").

Theorem 1.21. *Suppose $f : X \to Y$ is a morphism, then f is smooth (resp. étale) iff f is formally smooth (resp. formally étale) and locally of finite presentation. f is unramified iff f is formally unramified and locally of finite type.*

The last part of the theorem is just the last part of the preceding proposition. Why do we only want the morphism to be locally of finite type, instead of locally of finite presentation? It's because we want to weaken our condition so that every closed immersion is unramified. Indeed, not every closed immersion is locally of finite presentation, e.g. the immersion of the origin into $\mathbb{A}_k^\infty$.

Lemma 1.22. *Suppose C is an A-algebra and $I \subset C$ an ideal. Let $C_k = C/I^{k+1}$ for $k \geq 0$, then for all $k \geq 1$ we have $\Omega_{C/A} \otimes_C C_0 \cong \Omega_{C_k/A} \otimes_C C_0$.*

Proof. We have the exact sequence

$$I^{k+1}/I^{2k+2} \longrightarrow \Omega_{C/A} \otimes_C C_k \longrightarrow \Omega_{C_k/A} \longrightarrow 0$$

Now $- \otimes_{C_k} C_0$ is a right-exact functor, so we get another exact sequence.

$$I^{k+1} \otimes_C C_0 \longrightarrow \Omega_{C/A} \otimes_C C_0 \longrightarrow \Omega_{C_k/A} \otimes_{C_k} C_0 \longrightarrow 0$$

where the first arrow is essentially $f_0 \cdots f_k \otimes 1 \mapsto \sum_{i=1}^{k} \mathrm{d} f_i \otimes (f_0 \cdots (\hat{i}) \cdots f_k \bmod I) = 0$, so we are done. □

Proof of Theorem 1.21. We'll prove the statement about smoothness (which, incidentally, also includes the idea of proving part (i) of the Proposition 1.20). The other parts are similar.
We may assume that $Z_0 = \operatorname{Spec} R_0 \to X$ factors through $\operatorname{Spec} B \subset X$ with $B = A[T_1, \ldots, T_n]/(g_1, \ldots, g_m), m \le n$ and (WLOG) $\det((\partial g_j/\partial T_i)_{1 \le i,j \le m})$ is invertible in B. We thus have $(a_i) \in R_0^n$ such that $g_j(a_1, \ldots, a_n) = 0$ for all j.
Suppose $Z = \operatorname{Spec} R, R_0 = R/I, I^2 = 0$ To prove the "only if" part, it suffcies to produce some $(\tilde{a}_i) \in R^n$ with $g_j(\tilde{a}_1, \ldots \tilde{a}_n) = 0$. This sounds just like Hensel's lemma.
Pick any $(a_i') \in R^n$ such that $a_i' \bmod I = a_i$, then $g_j(a_1', \ldots, a_n') = c_j \in I$. As $I^2 = 0$, for any $x_1, \ldots, x_n \in I$, we have

$$g_j(a_1' + x_1, \ldots, a_n' + x_n) = g_j(a_1', \ldots, a_n') + \sum_{i=1}^{n} x_i \frac{\partial g_j}{\partial T_i}(a_1', \ldots, a_n')$$

As $\det((\partial g_j/\partial T_i)_{1 \le i,j \le m})$ is invertible, it's possible to choose $x_1, \ldots, x_n$ (with $x_{m+1}, \ldots, x_n$ all zero) such that this expression vanishes for all j. Taking $\tilde{a}_i = a_i' + x_i$ then gives what we desired.
For the "if" part, we'll show that if $\operatorname{Spec} B/\operatorname{Spec} A$ is formally smooth, then for any presentation $B = P/J$ with P a polynomial algebra over A, δ is a split injection. By the preceding lemma, $\Omega_{P/A} \otimes_P B \cong \Omega_{P_1/A} \otimes_P B$ where $P_1 = P/J^2$. So it suffices to prove that $\delta : J_1 = J/J^2 \to \Omega_{P_1/A} \otimes_{P_1} B$ is a split injection.
Consider the diagram

$$\begin{array}{ccc} B & \xrightarrow{=} & B \\ \uparrow & \searrow & \uparrow{\scriptstyle \ker = J_1, J_1^2 = 0} \\ A & \longrightarrow & P_1 \end{array}$$

where the existence of $B \to P_1$ is guaranteed by formal smoothness. This gives the splitting $P_1 \cong_A B \oplus J_1$ where $B \oplus J_1$ has multiplication $(b, f)(b', f') = (bb', f'b + fb')$. It's then easy to check that $P_1 \cong B \oplus J_1 \to J_1$ is an A-derivation, and therefore induces a unique map of P_1-modules $\sigma : \Omega_{P_1/A} \to J_1$ via $\mathrm{d}(b, f) \mapsto f$. This factors through $\bar{\sigma} : \Omega_{P_1/A} \otimes_{P_1} B \to J_1$ and $\bar{\sigma} \circ \delta = \mathrm{id}$, which means that δ is a split injection. □

Remark. In case you are gonna read some French literature, the French for "smooth" is "lisse", for "unramified" is "net/nette" and for "étale" is, of course, "étale".

Suppose $p : X \to Y, q : Y \to W$ are morphisms and q is étale. We expect p and $q \circ p$ to have some common properties seeing that q is supposed to mimic a local isomorphism (a phenomenon that often described with the word "permanence"). And they do, oftentimes.

Proposition 1.23. *If $q \circ p$ is étale (resp. smooth), so is p.*

Remark. If $q \circ p$ is unramified, so would p be. But this is apparently too easy to be part of the proposition.

Proof. Might as well assume everything is affine. Suppose $W = \operatorname{Spec} A, Y = \operatorname{Spec} B, X = \operatorname{Spec} C$. Then p, q induces $A \to B \to C$ where both B, C are finitely presented over A, thus C is also finitely presented over B. So it's enough to show that p is formally étale (resp. smooth).
Suppose

$$\begin{array}{ccc} Z_0 & \xrightarrow{s} & X \\ {\scriptstyle i}\big\downarrow & \overset{\tilde{r}}{\nearrow} & \big\downarrow{\scriptstyle p} \\ Z & \xrightarrow[r]{} & Y \\ & & \big\downarrow{\scriptstyle q} \\ & & W \end{array}$$

where $Z_0 \subset Z = \operatorname{Spec} R$ is defined by a square-zero ideal of R. Since X/W is formally smooth, there is some $\tilde{r} : Z \to X$ with $q \circ p \circ \tilde{r} = q \circ r$ and $\tilde{r} \circ i = s$. Then $\operatorname{Hom}_W(Z, Y) \cong \operatorname{Hom}_W(Z_0, Y)$ via i since q is étale. But $p \circ \tilde{r} \circ i = p \circ s = r \circ i$, so $p \circ \tilde{r} = r$ and we are done. □

Proposition 1.24. *Let $i : Y \hookrightarrow X$ be a closed immersion, then i is étale iff $X = Y \sqcup Z$ for a closed subscheme $Z \subset X$ (i.e. i is in fact an open immersion).*

Proof. The "if" part is clear. As for the "only if" direction, observe that if i is étale then it is locally of finite presentation. Assume that $i : Y = \operatorname{Spec}(A/I) \hookrightarrow \operatorname{Spec} A = X$ with I a finitely generated ideal (so the presentation is $P = A \to A/I$). Then as i is étale, $I/I^2 \cong \Omega_{P/A} \otimes_P (P/I) = 0$, so $I = I^2$. Nakayama's lemma then gives some $f \in I$ with $(1 + f)I = 0$. Then $A \to A_{1+f}$ induces an isomorphism $A/I \cong A_{1+f}$, which means that i is an open immersion onto $\operatorname{Spec} A_{1+f} \subset X$. □

Remark. More generally, we can replace the condition of i being a closed immersion by it being radicial, in the sense that i is injective on points and $k(x)/k(f(x))$ is purely inseparable.

Theorem 1.25. *Suppose X, Y are locally Noetherian and let $f : X \to Y$ be a morphism that's locally of finite presentation. Suppose $x \in X$ has $k(x) \cong k(y)$ via the induced map, where $y = f(x)$. Then f is étale at x iff $\hat{\mathcal{O}}_{Y,y} \cong \hat{\mathcal{O}}_{X,x}$ ("analytic isomorphism").*

Proof. We might as well assume that f is étale since the statement is local at x. Recall that $\hat{\mathcal{O}}_{X,x} = \varprojlim_n \mathcal{O}_{X,x}/\mathfrak{m}_x^n$. Let $n \geq 1$ and $Y_n = \operatorname{Spec} A_n, A_n = \mathcal{O}_{Y,y}/\mathfrak{m}_y^n$. Let $X_n = X \times_Y Y_n = \operatorname{Spec} B_n$ which is étale over Y_n. Thus there is a lifting s making

$$\begin{array}{ccc} X_n & \xleftarrow{x} & \operatorname{Spec} k(x) \\ {\scriptstyle f}\big\downarrow & \overset{s}{\nwarrow} & \big\downarrow{\scriptstyle y} \\ Y_n & \xrightarrow[=]{} & Y_n \end{array}$$

commute. So $f \circ s = \mathrm{id}_{Y_n}, s^* \circ f^* = \mathrm{id}_{A_n}$ (via X_n, B_n respectively). Thus s is a closed immersion and is also étale. Therefore $X_n = Y_n \sqcup Z_n$ as in the preceding proposition. So $\mathcal{O}_{Y,y}/\mathfrak{m}_y^n = \mathcal{O}_{Y_n,y} \cong \mathcal{O}_{X_n,x} = \mathcal{O}_{X,x}/\mathfrak{m}_y^n\mathcal{O}_{X,x}$. For $n = 1$, we've got the isomorphism $\mathcal{O}_{X,x}/\mathfrak{m}_y\mathcal{O}_{X,x} = \mathcal{O}_{Y,y}/\mathfrak{m}_y$, so indeed $\mathfrak{m}_x = \mathfrak{m}_y\mathcal{O}_{X,x}$. Therefore $\mathcal{O}_{Y,y}/\mathfrak{m}_y^n \cong \mathcal{O}_{X,x}/\mathfrak{m}_x^n$ for all n, giving exactly what we want.

Conversely, suppose $\hat{\mathcal{O}}_{X,x} \cong \hat{\mathcal{O}}_{Y,y}$, then $\mathfrak{m}_x = \mathfrak{m}_y\mathcal{O}_{X,x}$. Thus $\mathcal{O}_{X,x}/\mathfrak{m}_y\mathcal{O}_{X,x} = k(x) = k(y)$ which means that $\Omega_{X/Y} \otimes k(x) = 0$, i.e. $\Omega_{X/Y} = 0$ in a neighbourhood of x. Assuming $X = \operatorname{Spec} B \to Y = \operatorname{Spec} A$ with $B = P/I$ a finite presentation, then $\Omega_{B/A=0}$.

So $\delta : I/I^2 \to \Omega_{P/A} \otimes_P B = \bigoplus_{i=1}^n (\mathrm{d}T_i \otimes 1)B$ is surjective. Choose $g_i \in I$ such that $\delta(g_i \bmod I^2) = \mathrm{d}T_i \otimes 1$. Then $(\partial g_j/\partial T_i)$ is certainly invertible in B, so $X' = \operatorname{Spec} P/(g_1, \ldots, g_n) \to Y$ is étale.

Let's look at the local rings. $\mathcal{O}_{X,x} \subset \hat{\mathcal{O}}_{X,x}$ as our schemes are Noetherian, which gives

$$\begin{array}{ccc} \mathcal{O}_{X,x} & \longleftarrow & \mathcal{O}_{X',x} \\ \downarrow & & \downarrow \\ \hat{\mathcal{O}}_{X,x} & \longleftarrow & \hat{\mathcal{O}}_{X',x} \\ & \nwarrow{=} & \uparrow\cong \\ & & \hat{\mathcal{O}}_{Y,y} \end{array}$$

That is, $\mathcal{O}_{X',x} \to \mathcal{O}_{X,x}$ is injective. But $X \to X'$ is supposed to be a closed immersion, so $\mathcal{O}_{X',x} \cong \mathcal{O}_{X,x}$. This actually means that $X \to X'$ is locally an isomorphism at x. Indeed, suppose $X \to X'$ is locally $\operatorname{Spec} B \to \operatorname{Spec} A$ with $B = A/I$, then $I = (a_1, \ldots, a_n)$ is finitely generated by finite presentation. For $\mathfrak{q} \in \operatorname{Spec} B$ (say with image $\mathfrak{p} \in \operatorname{Spec} A$), we must have $I \leq \mathfrak{q}$, thus I vanishes under $A \to A_\mathfrak{p} \to B_\mathfrak{q}$. But this means that I is zero under $A \to A_\mathfrak{p}$ since $A_\mathfrak{p} \hookrightarrow B_\mathfrak{q}$. So for all j, there is some $f_i \in A \setminus \mathfrak{p}$ with $f_j a_j = 0$, showing that I in fact vanishes under $A \to A_f$ where $f = \prod_i f_i$. Then $A_f \cong B_f$, i.e. i is a local isomorphism.

So $X \to X'$ is étale at x, which means that f too has to be étale at x. □

Corollary 1.26. *Suppose X is a k-scheme of finite type and $x \in X$ has $k(x) = k$. Then X is smooth at x of relative dimension d iff $\hat{\mathcal{O}}_{X,x} \cong k[[T_1, \ldots, T_d]]$.*

Proof. For the "only if" part, observe that we have some étale $X \to \mathbb{A}_k^d$ locally at x where x is sent WLOG to the origin, then it induces $\hat{\mathcal{O}}_{X,x} \cong \hat{\mathcal{O}}_{\mathbb{A}_k^d,0} = k[[T_1, \ldots, T_d]]$. Conversely, $\ker \mathfrak{m}_x/\mathfrak{m}_x^2 \cong \bigoplus_i k(T_1 \bmod \mathfrak{m}_x^2)$ and any set of generators for $\mathfrak{m}_x/\mathfrak{m}_x^2$ gives an isomorphism $\hat{\mathcal{O}}_{X,x} \cong k[[T_1, \ldots T_d]]$. So WLOG $T \in \mathcal{O}_{X,x}$ which then gives $X \to \mathbb{A}_k^n$ which is étale at x. □

Remark. Any localisation $A \to S^{-1}A$ is automatically formally étale, but it's not in general étale unless $S^{-1}A$ is finitely presented over A.

Example 1.10. Let's give an example of a closed immersion that's formally étale but not étale.

For a field k, we consider the ring $A = k(1, 1, \ldots) + \bigoplus_\mathbb{N} k \subset k^\mathbb{N}$ consisting of eventually constant k-sequences. One can check that $X = \operatorname{Spec} A = \{x_n : n \in \mathbb{N} \cup \{\infty\}\}$ where $x_n = \ker(A \to k, (a_i)_i \mapsto a_n)$ for $n < \infty$ and $x_\infty = \ker(A \to k, (a_i)_i \mapsto \lim_n a_n) = \bigoplus_\mathbb{N} k$. The topological space of X, on the other hand, is homeomorphic to $\{1/(n+1) : n \in \mathbb{N}\} \cup \{0\} \subset \mathbb{R}$ (the "one-point compactification of $\mathbb{N}$", and also the simplest nontrivial profinite set) in the

natural way ($x_n \mapsto 1/(n+1), x_\infty \mapsto 0$).
$\mathcal{O}_{X,x_n} = k$ for all $x \leq \infty$ and $x_\infty \cong \operatorname{Spec} k = \operatorname{Spec} \mathcal{O}_{X,x_\infty} \hookrightarrow X$ is a closed immersion and is formally étale as a localisation, but not étale since it is not an open immersion.

1.7 Flatness

Definition 1.24. An R-module M is if any of the followings hold:
(i) The endofunctor $- \otimes_R M$ on (Mod_R) is exact, i.e. whenever

$$0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow N_3 \longrightarrow 0$$

is an exact sequence of R-modules, so is

$$0 \longrightarrow M \otimes_R N_1 \longrightarrow M \otimes_R N_2 \longrightarrow M \otimes_R N_3 \longrightarrow 0$$

(ii) For any $I \leq R$, $M \otimes_R I \to M$ is an injection (i.e. we need only to check the simplest short exact sequences).
(iii) ("Equational Flatness") If $m_1, \dots, m_r \in M, a_1, \dots, a_r \in R$ are such that $\sum_i a_i m_i 0 =$, then there exists $n_1, \dots, n_s \in M, (b_{ij})_{1 \leq i \leq n, 1 \leq j \leq s} \in R$ such that $m_i = \sum_j b_{ij} n_j$ and $\sum_i a_i b_{ij} = 0$ for all j.

If M is R-flat (i.e. M is a flat R-module), then $M_\mathfrak{p}$ is $R_\mathfrak{p}$-flat for any prime $\mathfrak{p} \in \operatorname{Spec} R$. Also, any free R-module is also R-flat. We can refine this implication with the introduction of more precise algebraic notions.

Definition 1.25. An R-module M is projective if $M \oplus M'$ is a free R-module for some R-module M'.
M is locally free if the quasicoherent $\mathcal{O}_X$-module $\tilde{M}$ (where $X = \operatorname{Spec} R$) is locally free, i.e. there are $f_1, \dots, f_r \in R$ such that $(f_1, \dots, f_r) = R$ and M_{f_i} is a free R_{f_i}-module.
M is punctually (or stalkwise) free if $M_\mathfrak{p}$ is a free $R_\mathfrak{p}$-module for all $\mathfrak{p} \in \operatorname{Spec} R$.

We then have the implication chains (free) $\Longrightarrow$ (projective) $\Longrightarrow$ (flat) and (free) $\Longrightarrow$ (locally free) $\Longrightarrow$ (punctually free) $\Longrightarrow$ (flat). All the implications are strict in general.
If M is punctually free and finitely presented, then it is certainly locally free. Without finite presentation, even for $R = \mathbb{Z}$, there can be punctually free modules that are not locally free, e.g. $M = \{m/n \in \mathbb{Q} : n \text{ square-free}\}$ (which has $M_{(p)} = p^{-1}\mathbb{Z}_{(p)}$).
Indeed, if M is finite (i.e. finitely generated), then we have a lot of reversed arrows (projective) $\Longleftrightarrow$ (locally free) $\Longleftrightarrow$ (flat and finitely presented) (note that if R is Noetherian then any flat R-module is finitely presented).
If R is local, then (free) $\Longleftrightarrow$ (locally free) $\Longleftrightarrow$ (projective) $\Longrightarrow$ (flat), and (projective) $\Longleftarrow$ (flat) if in addition that M is finite.

Definition 1.26. An A-algebra B is flat if it is flat as an A-module.
A morphism $f : X \to Y$ is flat if it is locally covered by $\operatorname{Spec} B \to \operatorname{Spec} A$ with $A \to B$ flat.

Morally, flat morphisms carry the ideal of a "continuously ranging family".

Proposition 1.27. *Suppose $f : X \to Y$ is of finite presentation. Then f is étale iff f is flat and unramified iff f is flat with étale fibres $X_y \to \operatorname{Spec} k(y), y \in Y$. f is smooth iff f is flat with smooth fibres.*

2 Group Schemes

2.1 Definition and Examples

Example 2.1. $\mathbb{A}^1_k$ should morally be a group under "addition on k", but it can't work since you don't know what to do with the generic point (0) and (if $k \neq \bar{k}$) there are more points than k. However, if R is a k-algebra, $\mathbb{A}^1_k(R) = R$ has the structure of a group.

We want to define group schemes in some sort of functorial languages.

Definition 2.1. A group scheme over S (an "S-group scheme") is an S-scheme G together with an S-morphism $m : G \times_S G \to G$ such that for any S-scheme T, $m_T : G(T) \times G(T) = (G \times_S G)(T) \to G(T)$ maks $G(T)$ a group.

By the usual covering argument, it suffices to check the cases where T is affine. When S is unspecified, we usually imply $S = \operatorname{Spec}\mathbb{Z}$.

Example 2.2. The $\operatorname{Spec}\mathbb{Z}$-scheme $\mathbb{G}_a = \operatorname{Spec}\mathbb{Z}[T]$ is a group scheme with m induced from $\mathbb{Z}[T] \mapsto \mathbb{Z}[T] \otimes_{\mathbb{Z}} \mathbb{Z}[T] = \mathbb{Z}[T_1, T_2], T \mapsto T_1 + T_2$. Then for any ring R, $\mathbb{G}_a(R) = R$ is made into a group by m which is just the additive group of R.

Suppose $T' \to T$ is an S-morphism, then we've got the commutative diagram

$$\begin{array}{ccc} G(T) \times G(T) = (G \times_S G)(T) & \xrightarrow{m_T} & G(T) \\ \downarrow & & \downarrow \\ G(T') \times G(T') = (G \times_S G)(T') & \xrightarrow[m_{T'}]{} & G(T') \end{array}$$

which makes $G(T) \to G(T')$ a group homomorphism. In particular, it sends the identity $e_T \in G(T)$ to the identity $e_{T'} \in G(T')$. So $e = e_S \in G(S)$ maps to every e_T via the S-scheme structure on T.
Similarly, taking inverses is also compatible with $T' \to T$. So we have an inverse i of the tautological point $\mathrm{id}_G \in G(G)$ which has $\forall x \in G(T), x^{-1} = i \circ x$. We can use these to give a categorical definition of a group scheme.

Definition 2.2. An S-group scheme is an S-scheme G together with an S-morphism $m : G \times_S G \to G$ such that:
(i) The diagram

$$\begin{array}{ccccc} (G \times_S G) \times_S G & \xrightarrow{m \times_S \mathrm{id}_G} & G \times_S G & \xrightarrow{m} & G \\ \| & & & \nearrow_{m} & \\ G \times_S (G \times_S G) & \xrightarrow[\mathrm{id}_G \times_S m]{} & G \times_S G & & \end{array}$$

commutes. (ii) There exists a section $e : S \to G$ of $G \to S$ with

$$\begin{array}{ccc} S \times_S G & \xrightarrow{\cong} & G \\ {\scriptstyle e \times_S \mathrm{id}_G}\downarrow & \nearrow_{m} & \\ G \times_S G & & \end{array}$$

commute.
(iii) There exists an S-morphism $i : G \to G$ such that

$$\begin{array}{ccc} G \times_S G & \xrightarrow{m} & G \\ {\scriptstyle i\times_S \mathrm{id}_G}\uparrow & & \uparrow{\scriptstyle e} \\ G & \longrightarrow & S \end{array}$$

commute.

The two definitions coincide: If we have the categorial definition, then by taking T-valued points in all these diagrams immediately make $G(T)$ a group. The converse is given by Yoneda lemma.
There is a third, purely functorial definition.

Definition 2.3. An S-group scheme is an S-scheme G whose functor of points is a functor $(\mathsf{Sch}/S)^{\mathrm{op}} \to (\mathsf{Groups})$. More precisely, for all $T \in (\mathsf{Sch}/S)$, we have a group structure on $G(T)$ such that for all $T' \to T$, the map $G(T) \to G(T')$ is a homomorphism.

Again it's enough to check affine T. This is equivalent to our previous definitions by Yoneda lemma.

Example 2.3. 1. The multiplicative group $\mathbb{G}_m = \operatorname{Spec} \mathbb{Z}[T, T^{-1}]$ has $G_m(R) = (R^\times, \times)$ which is a group that's functorial in R. Indeed, it's induced by $m : \mathbb{G}_m \times \mathbb{G}_m = \operatorname{Spec} \mathbb{Z}[T_1, T_2, (T_1T_2)^{-1}] \to \operatorname{Spec} \mathbb{Z}[T, T^{-1}]$ via $T \mapsto T_1T_2$.
2. For $n \geq 1$, the n^{th} general linear group is constructed from the affine scheme given by $\mathrm{GL}_n = \operatorname{Spec} \mathbb{Z}[\{T_{ij}\}_{1 \leq i,j \leq n}, (\det T)^{-1}]$. Of course $\mathrm{GL}_n(R)$ is then what you think it is. Since $R \to R'$ induces $\mathrm{GL}_n(R) \to \mathrm{GL}_n(R')$, GL_n is a group scheme.
3. For a field k, an elliptic curve E/k is a k-group scheme under its group law.
4. For any abstract group H and S any scheme, the S-scheme $H_S = \coprod_H S$ is an S-group scheme ("constant" group scheme).
Indeed, $H_S(T) = \{\text{locally constant maps } T \to H\}$ which is a group functorial in T.
In the case where $S = \operatorname{Spec} A$ is affine, H is finite iff H_S is affine (if H is finite then $H_S = \operatorname{Spec} A^H$, otherwise H_S not quasicompact).

For group schemes G_1, G_2 over S, a morphism of group schemes $G_1 \to G_2$ is just an S-morphism such that the induced $G_1(T) \to G_2(T)$ is a homomorphism. We can also form the product group scheme $G_1 \times_S G_2$ with the obvious multiplication.
Kernels, on the other hand, requires some subtle treatment. Suppose $f : G_1 \to G_2$ is a morphism of S-group schemes. The kernel of f is defined by the fibre product $\ker f = G_1 \times S$ over $e : S \to G_2$ and $f : G_1 \to G_2$. This is certainly an S-scheme and it is also a group scheme by $(\ker f)(T) = \ker f_T$. It's also a "normal subgroup scheme" of G_1, which we'll define in a moment.

Example 2.4. Suppose A is a ring and $n \in \mathbb{Z}$, the A-group scheme of multiplications is $\mathbb{G}_{m,A} = \operatorname{Spec} A[T, T^{-1}]$. The A-morphism $[n] : \mathbb{G}_{m,A} \to \mathbb{G}_{m,A}$ via $T \mapsto T^n$ is a morphism of A-group schemes as it induces $R^\times \to R^\times, x \mapsto x^n$ on any A-algebra R.
For $n = 0$, this is just the identity. For $n \geq 1$, the kernel of $[n]$ is known as

the groups of roots of unity $\mu_{n,A} = \ker[n] = \operatorname{Spec} A[T]/(T^n - 1)$. Note that $A[T]/(T^n - 1)$ is finite and free of rank n over A.
If $A = k$ is a field and $\operatorname{char} k \nmid n$, then $k[T]/(T^n - 1)$ is étale over k (as $(\mathrm{d}/\mathrm{d}T)(T^n - 1) = nT^{n-1}$ is invertible). If moreover k has exactly n n^{th} roots of unity, then μ_n is just $\mu_n(k)_{\operatorname{Spec} k}$ which is the disjoint union of n copies of $\operatorname{Spec} k$.
If $n = p^j$ where $p = \operatorname{char} k$, then $\mu_{p^j} = \operatorname{Spec} k[T]/(T-1)^{p^j}$. But $k[T]/(T-1)^{p^j}$ is local, so this is just a nonreduced (if $j > 0$) scheme with a single point. So μ_n doesn't have to be smooth although $\mathbb{G}_m$ is always smooth over k.

For a morphism $f : G_1 \to G_2$ of S-group schemes, we (ideally) want $\ker f$ to be a closed subscheme of G_1, but there is a small problem here.

Example 2.5. If we take $\mathrm{id}_G : G \to G$, then $\ker f = S$ viewed as $e : S \to G$. But e might not be a closed immersion: Take $S = \mathbb{A}^1_k$ and $G = U \cup U'$ the affine line with two origins ($U \cong U' = \mathbb{A}^1_k$). G is an S-scheme via the projection. To make it an S-group scheme, we need to produce an $m : G \times_S G \to G$. We have $G \times_S G = (U \times_S U) \cup (U' \times_S U') \cup (U \times_S U') \cup (U' \times_S U)$, so we can map $(U \times_S U) \cup (U' \times_S U')$ to U and $(U \times_S U') \cup (U' \times_S U)$ to U' in the obvious way. Then G is a nonseparated S-group scheme and $e : S \to G$ is not a closed immersion.
These kinds of phenomena occurs probably more often than you thought, e.g. try looking at Picard schemes.
The closed immersion $j : \operatorname{Spec} k = \{0\} \to \mathbb{A}^1_k$ allows us to view G as $j_*(\mathbb{Z}/2\mathbb{Z})$ (i.e. for any open $V \subset \mathbb{A}^1_k$, the section of G over V is $\Gamma(V, j_*(\mathbb{Z}/2\mathbb{Z}))$).

Proposition 2.1. *An S-group scheme G is separated iff $e \in G(S)$ is a closed immersion.*

Proof. The "only if" direction is exercise (in fact this true for any section of a separated morphism of schemes).
For the "if" direction, note that if e is closed then so is $G = S \times_S G \to G, e \times_S \mathrm{id}_G$.

$$\begin{array}{ccc} S \times_S G & \xrightarrow{e \times_S \mathrm{id}_G} & G \times_S G \\ {\scriptstyle \mathrm{pr}_1}\downarrow & & \downarrow{\scriptstyle \mathrm{pr}_1} \\ S & \xrightarrow[e]{} & G \end{array}$$

On the other hand, $e \times_S \mathrm{id}_G = s \circ \Delta_{G/S}$ where $s : (g, h) \mapsto (gh^{-1}, h)$ is an automorphism of $G \times_S G$ (i.e. for any T and $g, h \in G(T)$, we get $s_T : (g, h) \mapsto (gh^{-1}, h)$ which defines s by Yoneda lemma), so we are done. ☐

Corollary 2.2. *1. If $f : G_1 \to G_2$ is a morphism of S-group schemes and G_2 is separated, then* $\ker f$ *is a closed subscheme of G.*
2. If $S = \operatorname{Spec} k$ for a field k, then any group scheme over S is separated.

Proof. 1. Closed immersions are stable under fibre products.
2. The image of e is a closed point. ☐

Example 2.6. 1. For every ring R, we have a determinant map $\det(R) : \mathrm{GL}_n(R) \to R^\times = \mathbb{G}_m(R)$ which is functorial in R, hence defines a morphism $\det : \mathrm{GL}_n \to \mathbb{G}_m$. Its kernel is called the special linear group $\mathrm{SL}_n = \ker \det$.

2. Suppose k is a field, then we have a morphism of k-group schemes $[n] : G_{a,k} \to G_{a,k}$ via multiplication by n. If n is invertible in k, then this is an automorphism since it is an automorphism at the level of k-algebras. But if $\operatorname{char} k = p \mid n$, then $[n]$ is essentially the zero morphism.
3. Suppose X is a scheme over $\mathbb{F}_q$ for $q = p^n$. We have a Frobenius endomorphism $F_q : X \to X$ which is identity on the underlying topological space and looks like $x \mapsto x^q$ on $\mathcal{O}_X$. Now suppose that $X = G = \mathbb{G}_a/\mathbb{F}_p$ is the additive group scheme. The Frobenius F_p on G is then induced from $\mathbb{F}_p[T] \to \mathbb{F}_p[T], T \mapsto T^p$, which is a morphism of group schemes. Then $\ker(F_p^j) = \operatorname{Spec} \mathbb{F}_p[T]/(T^{p^j})$ which is sometimes called α_{p^j}. Like μ_{p^j}, α_{p^j} is nonreduced point. But note that μ_{p^j} is not isomorphic to α_{p^j}.

Remark. In the affine case, we have yet another way to make sense of the definition of group schemes. Suppose we have a group scheme $G = \operatorname{Spec} A \to S = \operatorname{Spec} R$ where R is a ring and A is an R-algebra. Then $m : G \times_S G = \operatorname{Spec}(A \otimes_R A) \to G$ is induced by some $\mu = m^* : A \to A \otimes_R A$ ("comultiplication"); $e : S \to G$ is induced by $\epsilon = e^* : A \to R$ ("counit/augmentation"); $i : G \to G$ is induced by $\iota = i^* : A \to A$ ("coinverse"). These are all R-algebra homomorphisms, and since m, e, i make G a group scheme, we can obtain corresponding (opposite) diagrams for μ, ϵ, ι. For example, associativity becomes

$$\begin{array}{ccccc} A & \xrightarrow{\mu} & A \otimes_R A & \xrightarrow{\mu \otimes_R \mathrm{id}_A} & (A \otimes_R A) \otimes_R A \\ & \searrow^{\mu} & & & \| \\ & & A \otimes_R A & \xrightarrow[\mathrm{id}_A \otimes_R \mu]{} & A \otimes_R (A \otimes_R A) \end{array}$$

An R-algebra equipped with (μ, ϵ, ι) is called a Hopf algebra (or bialgebra). We then have an equivalence of categories from the opposite category of affine R-group schemes and Hopf algebras over R.

Let k be a field. The r-torus over k is the k-group scheme

$$\mathbb{G}_{m,k}^r = \operatorname{Spec} k[T_1, \ldots, T_r, (T_1 \cdots T_r)^{-1}] = \operatorname{Spec} k[\Lambda]$$

where $k[\Lambda]$ is the group algebra of $\Lambda = \mathbb{Z}^r$ over k.
In general, if Λ is any abelian group and A any ring, we get the A-algebra $A[\Lambda] = \bigoplus_{\lambda \in \Lambda} A(\lambda)$ with multiplication induced from $(\lambda)(\mu) = (\lambda\mu)$. The A-group scheme $D_A(\Lambda) = \operatorname{Spec} A[\Lambda]$ is called a diagonalisable group scheme. On the level of A-algebras, we have $D_A(\Lambda)(R) = \operatorname{Hom}_A(A[\Lambda], R) = \operatorname{Hom}_{(\mathsf{Groups})}(\Lambda, R^\times)$ which is an abelian group.

Example 2.7. $D_A(\mathbb{Z}) = \mathbb{G}_{m,A}, D_A(\mathbb{Z}/n\mathbb{Z}) = \operatorname{Spec} A[T]/(T^n - 1) = \mu_{n,A}$.

Remark. 1. As $D_A(\Lambda) = D_{\mathbb{Z}}(\Lambda) \times_{\operatorname{Spec} \mathbb{Z}} \operatorname{Spec} A$, we can generalise the notion of diagonalisable groups to any scheme S by setting $D_S(\Lambda) = D_{\mathbb{Z}}(\Lambda) \times_{\operatorname{Spec} \mathbb{Z}} S$. This can also be interpreted as $\underline{\operatorname{Spec}}_{\mathcal{O}_S} \mathcal{O}_S[\Lambda]$, if you know what that means.
2. Recall that if we are in the affine case $G = \operatorname{Spec} B$ over $S = \operatorname{Spec} A$, then B is a Hopf algebra over A equipped with comultiplication $\mu = m^* : B \to B \otimes_A B$ and counit $\epsilon = e^* : B \to A$. In the case of $D_R(\Lambda)$, we simply have $R[\Lambda] \to R[\Lambda] \otimes_R R[\Lambda], (\lambda) \mapsto (\lambda) \otimes (\lambda)$.

To generalise phenomena from the geometry of tori,

Proposition 2.3. $\mathrm{Hom}_A(D_A(\Lambda), \mathbb{G}_{m,A}) \cong \Lambda$ *if* $\mathrm{Spec}\, A$ *is (nonempty and) connected.*

Proof. For $\lambda \in \Lambda$, $A[T, T^{-1}] \to A[\Lambda], T \mapsto (\lambda)$ is a homomorphism of A-Hopf algebras (where $A[T, T^{-1}]$ is given the natural comultiplication $\mu(T) = T \otimes T$). This gives a map $D_A(\Lambda) \to \mathbb{G}_{m,A}$. Conversely, suppose $D_A(\Lambda) \to \mathbb{G}_{m,A}$ is given by $\phi : A[T, T^{-1}] \to A[\Lambda], \phi(T) = \sum_\lambda a_\lambda(\lambda) \in k[\Lambda]^\times$. But since ϕ commutes with comultiplication, we have

$$\sum_{\lambda,\lambda'} a_\lambda a_{\lambda'}(\lambda) \otimes (\lambda') = \sum_\lambda a_\lambda(\lambda) \otimes (\lambda)$$

So $a_\lambda = a_\lambda^2$ for all λ and $a_\lambda a_{\lambda'} = 0$ for any $\lambda' \neq \lambda$. But $\mathrm{Spec}\, A$ is connected iff the only idempotents in A are $0, 1$. These a_λ cannot all be zero since $\phi(T) \in A[\Lambda]^\times$. If $a_\lambda = 1$ then $a_{\lambda'} = 0$ for all $\lambda' \neq \lambda$, so $\phi(T) = (\lambda)$ which gives the inverse. □

Definition 2.4. An S-group scheme G is commutative if $G(T)$ is an abelian group for all S-scheme T.

Equivalently, the diagram

$$\begin{array}{ccc} G \times_S G & \xrightarrow{m} & G \\ {\scriptstyle (x,y)\mapsto(y,x)}\downarrow & \nearrow_{m} & \\ G \times_S G & & \end{array}$$

commutes.

Definition 2.5. For $g \in G(T)$, we can define the conjugation map $\mathrm{inn}_g : G_T \to G_T = G \times_S T$ by requiring it to induce, for any T-scheme T', $G_T(T') \to G_T(T'), x \mapsto (g')x(g')^{-1}$ (where g' is the image of g).

So G is commutative iff for any T and any $g \in G(T)$, we have $\mathrm{inn}_g = \mathrm{id}_{G_T} \in \mathrm{Aut}(G_T)$.
Morally, we should be able to define a group scheme Z_G by requiring $Z_G(T) = \{g \in G(T) : \mathrm{inn}_g = \mathrm{id}\}$. But why should it be a (sub)group scheme? This turns out to be not entirely obvious at all.

Theorem 2.4. *Suppose k is a field and G is a k-group scheme locally of finite type, then Z_G is a closed subgroup scheme of G.*

Remark. $Z_G(T)$ might not be the centre of $G(T)$ in general. Take $k = \mathbb{Q}$, then it's possible to construct a group scheme G (over k) such that $G \cong \mu_{3,\mathbb{Q}} \sqcup \mu_{3,\mathbb{Q}}$, $G(\bar{\mathbb{Q}}) \cong S^3$ and in general $G(R) = \mu_3(R) \rtimes (\mathbb{Z}/2\mathbb{Z})_{\mathbb{Q}}(R)$ where $\mathbb{Z}/2\mathbb{Z}$ acts on μ_3 by $1 : z \mapsto z^{-1}$. If $\mu_3(R)$ is trivial, then $G(R) = (\mathbb{Z}/2\mathbb{Z})_{\mathbb{Q}}(R)$ (which is $\mathbb{Z}/2\mathbb{Z}$ if $\mathrm{Spec}\, R$ is connected) and its centre is $G(R)$. But $G(\bar{\mathbb{Q}}) \cong S_3$ which has trivial centre.

2.2 Finite Locally Free Group Schemes; Duality

Recall that $f : X \to Y$ is finite if for every open affine $V = \mathrm{Spec}\, A \subset Y$, $f^{-1}(V) = \mathrm{Spec}\, B$ is also affine for an A-algebra B which is finite as an A-module. As usual one can simply check an open affine covering of Y.

f is finite and locally free if for some open affine covering $V_i = \operatorname{Spec} A_i$ of Y, $f^{-1}(V_i) = \operatorname{Spec} B_i$ where B is an A-algebra that is finite and free as an A-module. Recall that for a finite A-module M, if M is locally free then M is flat, and the converse is true if A is Noetherian. So if Y is locally Noetherian, then f is finite locally free iff f is finite and flat.
We are interested in finite locally free S-group schemes.

Example 2.8. The constant S-group scheme attached to any finite group is a finite locally free S-group scheme. Other examples include $\mu_{n,S}$, $D_S(\Lambda)$ for Λ finite, $\alpha_{p^j,k}$ for a field k of characteristic p ($S = \operatorname{Spec} k$), etc..
Another important class of examples is given by the elliptic curves over R (which are, näively, $E \subset \mathbb{P}^2_R$ given by a Weierstrass equation with invertible discriminant) which has group law $\oplus : E \times_{\operatorname{Spec} R} E \to E$ making E/R a commutative group scheme. For every $n \geq 1$, $[n] : E \to E$ is finite and locally free, so $\ker[n]$ (often denoted as $E[n]$ or ${}_nE$) is a finite locally free R-group scheme.

If $S = \operatorname{Spec} A$ and $G = \operatorname{Spec} B$ are affine with B a finite locally free Hopf algebra over A (i.e. a Hopf algebra whose structure makes $G \to S$ finite locally free). Suppose G is commutative, then B is cocommutative, i.e.

$$\begin{array}{ccc} B & \xrightarrow{\mu} & B \otimes_A B \\ & \searrow^{\mu} & \downarrow{\scriptstyle x\otimes y \mapsto y \otimes x} \\ & & B \otimes_A B \end{array}$$

commutes. The dual $B^\vee = \operatorname{Hom}_A(B, A)$ is locally free and $(B^\vee)^\vee = B$. The transposes $\mu^\vee : B^\vee \otimes_A B^\vee \to B^\vee, \epsilon^\vee : A \to B^\vee$ make $B^\vee$ a commutative A-algebra. The multiplication and unit in B then becomes comultiplication and counit in $B^\vee$. The transpose of the antipode becomes the antipode of $B^\vee$. So we get another finite locally free group scheme $G^\vee$ over A, called the Cartier dual of G.
We have $(G^\vee)^\vee = G$. Also, if G is an S-group scheme (not necessarily affine), we can define $G^\vee$ by gluing over affines. This can alternatively done via $G^\vee = \underline{\operatorname{Spec}}_{\mathcal{O}_S} f_* \mathcal{O}_G^\vee$, where f is the structure morphism of G.
For $G = (\mathbb{Z}/n\mathbb{Z})_S$, we have $G^\vee = \mu_{n,S}$. In general,

Proposition 2.5. *Suppose Λ is a finite abelian group and Λ_S the associated constant group scheme, then $(\Lambda_S)^\vee = D_S(\Lambda)$.*

Proof. Assume $S = \operatorname{Spec} A$, then $\Lambda_S = \operatorname{Spec}(A^\Lambda)$. The group scheme structure on Λ_S corresponds to a comultiplication $A^\Lambda \to A^\Lambda \otimes_A A^\Lambda = A^{\Lambda \times \Lambda}$. On the other hand, $D_S(\Lambda) = \operatorname{Spec} A[\Lambda]$ has comultiplication $A[\Lambda] \to A[\Lambda] \otimes_A A[\Lambda] = A[\Lambda \times \Lambda], (\lambda) \mapsto (\lambda) \otimes (\lambda) = (\lambda, \lambda)$. The map $A^\Lambda \times k[\Lambda] \to A, (f, \lambda) \mapsto f(\lambda)$ provides the way to interchange the respective (co)multiplication. □

So $D_S(\Lambda)^\vee = \Lambda_S$.
Let's compute some more Cartier duals.

Proposition 2.6. *Let p be a prime, then $\alpha_p^\vee \cong \alpha_p$.*

Proof. $\alpha_{p,\mathbb{F}_p} = \operatorname{Spec} B$ where $B = \mathbb{F}_p[T]/(T^p)$. It has comultiplication $\mu : B \to B \otimes_{\mathbb{F}_p} B, T \mapsto T \otimes 1 + 1 \otimes T$. Let $e_i = T^i \in B$ for $0 \leq i < p$, then

$$e_i e_j = \begin{cases} e_{i+j} & \text{if } i + j < p \\ 0 & \text{otherwise} \end{cases}, \mu(e_k) = \sum_{i=0}^{k} \binom{k}{i} e_i \otimes e_{k-i}$$

The unit is e_0 whereas the counit is $\epsilon : e_0 \mapsto 1, e_i \mapsto 0$ for all $i > 0$. Let $(e_i^\vee)$ be the dual basis, then

$$\mu^\vee(e_1^\vee \otimes e_j^\vee) = \begin{cases} \binom{i+j}{i} e_{i+j}^\vee & \text{if } i+j < p \\ 0 & \text{otherwise} \end{cases}, \epsilon^\vee : 1 \mapsto e_0^\vee$$

whereas the dual of multiplication on B becomes $e_k^\vee \mapsto \sum_{i+j=k} e_i^\vee \otimes e_j^\vee$. Let $e_i^* = i! e_i^\vee$ for $0 \leq i < p$, then

$$\mu^\vee(e_i^* \otimes e_j^*) = \begin{cases} e_{i+j}^* & \text{if } i+j < p \\ 0 & \text{otherwise} \end{cases}$$

The comultiplication gives $T^\vee \mapsto T^\vee \otimes 1 + 1 \otimes T^\vee$ which too is what's expected, hence B is self-dual. □

Corollary 2.7. *For any (nonempty) $\mathbb{F}_p$-scheme S, $\alpha_{p,S}$ is not isomorpphic as an S-group scheme to $\mu_{p,S}$.*

Remark. α_{p^2}, on the other hand, is not self-dual. In fact we have $\alpha_{p^2} \cong \operatorname{Spec} \mathbb{F}_p[T_1, T_2]/(T_1^p, T_2^p)$ as a scheme.

Let's look for some other descriptions of dual. Recall that finite abelian groups G admit their duals via $G^\vee = \operatorname{Hom}(G, \mathbb{C}^\times)$.

Theorem 2.8. *Suppose G is a locally free commutative S-group scheme, then for any S-scheme T, we have*

$$G^\vee(T) \cong \operatorname{Hom}_{(\mathsf{GroupSch}/T)}(G_T, \mathbb{G}_{m,T})$$

with the isomorphism functorial in T.

Proof. Suffices to consider the case $S = T = \operatorname{Spec} A, G = \operatorname{Spec} B$. We have $G^\vee(S) = \operatorname{Hom}_A(B^\vee, A)$ and that

$$\begin{aligned} \operatorname{Hom}_{(\mathsf{GroupSch}/S)}(G, \mathbb{G}_m) &= \operatorname{Hom}_{(\mathsf{Hopf}/A)}(A[T, T^{-1}], B) \\ &= \{t \in B^\times : \mu(t) = t \otimes t, \epsilon(t) = 1\} \end{aligned}$$

Every $t \in B$ gives rise to $\phi_t : B^\vee \to A$ via $\phi_t(\alpha) = \alpha(t)$. For $\alpha, \beta \in B^\vee$, their product is essentially $\alpha \cdot \beta(b) = (\alpha \otimes \beta)(\mu(b))$ and the unit is $b \mapsto \epsilon(b)$. So ϕ_t is an A-algebra homomorphism iff $1 = \phi_t(1) = \epsilon(t)$ (so t is a unit as B is a finite A-algebra) and $\phi_t(\alpha \cdot \beta) = \alpha(t)\beta(t)$ for any $\alpha, \beta \in B^\vee$ (equivalently $\mu(t) = t \otimes t$). □

Example 2.9. $\alpha_p^\vee \cong \alpha_p$, so there is a morphism $f : \alpha_p \times \alpha_p \to \mathbb{G}_m$ (everything over $\mathbb{F}_p$) which is bilinear and nondegenerate on points. With a little more work, one can show that f is the map

$$(x, y) \mapsto \sum_{i=1}^{p-1} \frac{(xy)^k}{i!}$$

Remark. The rank of an S-group scheme $f : G \to S$ is $\operatorname{rk}(G/S) = \operatorname{rk}_{\mathcal{O}_S} f_* \mathcal{O}_G$. For a finite group Λ, we have $\operatorname{rk}(\Lambda_S) = |\Lambda|$ and, if Λ is abelian, $|\Lambda| = \operatorname{rk} D_S(\Lambda)$. We also have $\operatorname{rk} \alpha_{p^j} = p^j$. In general, we have $\operatorname{rk} G^\vee = \operatorname{rk} G$.

Theorem 2.9. *Suppose either G is commutative or S is reduced, then for any S-scheme T and $g \in G(T)$, we have $\operatorname{ord} g \mid \operatorname{rk}(G/S)$.*

Example 2.10. 1. Consider a field extension $k/\mathbb{F}_p$, then $\alpha_p(k[\epsilon]/(\epsilon^2)) = \epsilon k$ which can be arbitrarily large.
2. $\alpha_p \times \alpha_p = \operatorname{Spec} k[T_1, T_2]/(T_1^p, T_2^p)$. For $(a : b) \in \mathbb{P}^1(k)$, we have the subscheme $aT_1 + bT_2 = 0$ which is a subgroup scheme of rank p (and in fact isomorphic to α_p).
3. $H = \{(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix})\} \subset \mathrm{GL}_{2,k}$ contains $G = (\begin{smallmatrix} \mu_p & \alpha_p \\ 0 & 1 \end{smallmatrix})$. G has rank p^2 and is not commutative. One observe the discrepancy between groups and group schemes: Any group with order p^2 has to be commutative, but G is a noncommutative group scheme with rank p^2. Fortunately, all is not lost. It turns out that every group scheme of rank p is commuative (Tate-Oort).

A morphism of (finite locally free commutative) group schemes $f : G \to H$ gives rise to a dual morphism $f^\vee : H \to G$, and $(G \times_S H)^\vee \cong G^\vee \times_S H^\vee$. In fact, we can make an abelian category whose objects are finite locally free commutative group schemes over S and whose morphisms are some (but not all) morphisms of group schemes. In this category, we will have $\operatorname{coker}(f : G \to H) = \ker(f^\vee : H^\vee \to G^\vee)^\vee$. The reason why we cannot take all the morphisms is that there exists finite locally free commutative S-group schemes G, H with $f : G \to H$ which is not flat (which means that $\ker f$ is not locally free).

Example 2.11. If $S = \operatorname{Spec} \mathbb{Z}$ and $G = (\mathbb{Z}/2\mathbb{Z})_S$, $H = \mu_{2,S} = \operatorname{Spec} \mathbb{Z}[T]/(T^2 - 1)$. The obvious map $G \to H$ is an isomorphism except at $(2) \in \operatorname{Spec} \mathbb{Z}$, i.e. it's an isomorphism over $\operatorname{Spec} \mathbb{Z}[1/2]$. So $\ker f|_{\operatorname{Spec} \mathbb{Z}[1/2]}$ is trivial, but $\ker f \times \operatorname{Spec} \mathbb{F}_2 = (\mathbb{Z}/2\mathbb{Z})_{\mathbb{F}_2}$, so f is not flat.

2.3 Algebraic Group Schemes over Fields

Let k be a field and G a group scheme over k. G has some nice properties.

Lemma 2.10. *G is separated.*

Proof. The diagonal morphism of G is a base change of $e : S \to G$, which is a closed immersion if $S = \operatorname{Spec} k$. □

Lemma 2.11. *The multiplication $m : G \times_k G \to G$ is open.*

Proof. Consider the isomorphism $s : G \times_k G \to G \times_k G$ (the "shear map") defined on points by $(x, y) \mapsto (xy, y)$. We then have

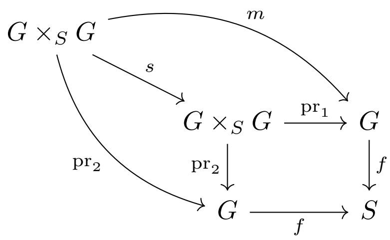
$$\begin{array}{ccc} G \times_k G & \xrightarrow{s} & G \times_k G \\ & {\scriptstyle m} \searrow & \downarrow {\scriptstyle \mathrm{pr}_1} \\ & & G \end{array}$$

As projections are open for schemes over a field, we conclude that m is open. □

$\Omega_{G/k}$ is free and is canonically isomorphic to $\Omega_{G/k}(e) \otimes_k \mathcal{O}_G$ where $\Omega_{G/k}(e) = \Omega_{G/k,e}/\Omega_{G/k,e}\mathfrak{m}_e$. This is a part of a more general fact.

Proposition 2.12. *Suppose $f : G \to S$ is any group scheme (with e the unit section), then $\Omega_{G/S} \cong f^*(e^* \Omega_{G/S})$.*

Proof. Let $s : G \times_S G \to G \times_S G$ be the shear map. The commutative diagram we've seen can be extended to



So $\mathrm{pr}_1^* \Omega_{G/S} = \Omega_{G\times_S G/G} \cong s^*\Omega_{G\times_S G/G} = s^* \mathrm{pr}_1^* \Omega_{G/S} = m^*\Omega_{G/S}$. We have $\mathrm{pr}_1 \circ (ef, \mathrm{id}_G) = ef : G \to G$ and $m \circ (ef, \mathrm{id}_G) = \mathrm{id}_G$ which gives the result. □

Lemma 2.13. *Subgroup schemes are closed. More precisely, if $i : H \hookrightarrow G$ is an immersion which is also a k-group scheme morphism, then i is closed.*

This is false if we don't assume i to be a morphism between group schemes, as e.g. $\mathbb{G}_m \hookrightarrow \mathbb{G}_a$ is not closed.

Definition 2.6. G/k is (locally) algebraic if it's (locally) of finite type over k.

Example 2.12. 1. Any constant group is locally algebraic and it's algebraic iff the original group is finite.
2. GL_n /k and its closed subgroups ("linear algebraic groups") are algebraic.
3. Elliptic curves and in general abelian varieties are algebraic.

Theorem 2.14 (Cartier's Theorem)**.** *Suppose G/k is locally algebraic and* $\mathrm{char}\, k = 0$*, then G is smooth.*

Proof. It suffices to show that $G \times_k \bar{k}$ is smooth over $\bar{k}$. So we can assume WLOG that $k = \bar{k}$.
Smoothness is an open condition, and the closed points (which are just the k-points as we've assumed $k = \bar{k}$) are dense (as G is locally of finite type over k). So it suffices to show that G is smooth at any closed point $g \in G(k)$. Assume that $g = e$ (which is sufficient since we can translate).
Let $\mathrm{Spec}\, B \subset G$ be an open neighbourhood of e, then $\Omega_{B/k}$ is a free B-module of finite rank (as B is of finite type). Also, $\Omega_{B/k}^\vee = \mathrm{Der}_k(B, B)$ surjects to $\Omega_{B/k}^\vee \otimes_e k = (\mathfrak{m}_e/\mathfrak{m}_e^2)^\vee = \mathrm{Der}_k(B, k) = \{k\text{-linear } \partial : B \to k : \partial(fg) = f(e)\partial g + g(e)\partial f\}$ by e^*. Let $t_1, \ldots, t_d \in \mathfrak{m}_e$ be such that $(t_i \bmod \mathfrak{m}_e^2)_i$ is a basis for $\mathfrak{m}_e/\mathfrak{m}_e^2$, and $\mathrm{D}_1, \cdots, \mathrm{D}_d \in \mathrm{Der}_k(B, B)$ such that $(e^*\mathrm{D}_i)_i$ is the dual basis to $(t_i \bmod \mathfrak{m}_e^2)_i$.
Then $k[T_1, \ldots, T_d] \to \mathcal{O}_{G,e}/\mathfrak{m}_e^N, T_i \mapsto t_i$ is surjective as the monomials in t_i's generate $\mathfrak{m}_e^n/\mathfrak{m}_e^{n+1}$. So we get a surjective map $\alpha : k[[T_1, \ldots, T_d]] \to \hat{\mathcal{O}}_{G,e}$. For the other way around, consider

$$\mathcal{O}_{G,e} \to k[[T_1, \ldots, T_d]], f \mapsto \sum_{n_1,\ldots,n_d \geq 0} \frac{1}{n_1! \cdots n_d!} (\mathrm{D}_1^{n_1} \cdots \mathrm{D}_d^{n_d} f)(e) T_1^{n_1} \cdots T_d^{n_d}$$

which we can do since $\mathrm{char}\, k = 0$. This is a ring homomorphism by some easy induction, and it extends to a map $\beta : \hat{\mathcal{O}}_{G,e} \to k[[T_1, \ldots, T_d]]$. It is surjective as $\beta(t_i) \equiv T_1 \pmod{(T_1 \cdots T_n)^2}$.
Now $\beta\alpha$ is a surjective ring endomorphism of $k[[T_1, \ldots, T_d]]$, so it has to be injective. Therefore α is bijective and hence an isomorphism. □

2.4 Étale Group Schemes; Frobenius and Verschiebung

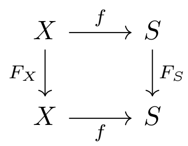
Recall that X is a scheme étale over a field k iff X is a disjoint union $\coprod_i \operatorname{Spec} k_i$ where k_i are finite separable extensions of k. Consider the separable closure k^{sep}/k with Galois group $\Gamma_k = \operatorname{Gal}(k^{\text{sep}}/k)$, then

$$X(k^{\text{sep}}) = \coprod_i \operatorname{Hom}_k(k_i, k^{\text{sep}})$$

is a set with a continuous (i.e. stabilisers are open) left action of Γ_k. By Galois theory, there's an equivalence of categories between the category of étale k-schemes and continuous Γ_k-sets. Consequently, the category of étale group schemes over k is equivalent to the category of abstract groups Λ with a continuous action $\Gamma_k \to \operatorname{Aut}(\Lambda)$. In particular, G is étale over k iff $G \times_k k^{\text{sep}}$ is a constant group scheme.

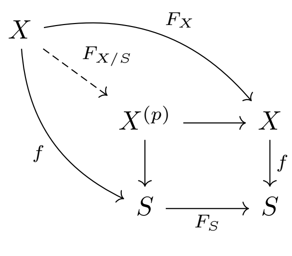
If k has characteristic 0, then every finite group scheme over k is étale, so the classification of finite group schemes over k is just the classification of finite groups and the actions of Γ_k (neither of which is nowhere near being trivial). How about positive characteristics?

We say a scheme S has characteristic p if $p\mathcal{O}_S = 0$, or equivalently S is an $\mathbb{F}_p$-scheme. We have the absolute Frobenius $F_S : S \to S$ is the morphism which is the identity on points and $F_S^{\#} : \mathcal{O}_S \to \mathcal{O}_S$ is $x \mapsto x^p$. If $f : X \to S$ is a morphism of schemes with characteristic p, then the diagram



commutes. It would be convenient if we can linearise this. Suppose $x = (x_1, \ldots, x_n) \in \mathbb{A}^n(k)$ has $g(x_1, \ldots, x_n) = 0$ for some $g \in k[T_1, \ldots, T_n]$, then $g^{(p)}(x_1^p, \ldots, x_n^p) = 0$ where $g^{(p)}$ is obtained by raising each of its coefficients to power p.

Definition 2.7. Let $X^{(p)} = X^{(p/S)} = X \times_{S,f,F_S} S$ (the "p-conjugate of X"). Then there is a unique S-morphism $F_{X/S}$, called the relative Frobenius, making



commute.

Example 2.13. If $X = \operatorname{Spec} A[\{T_i\}]/(\{g_j\}) \to S = \operatorname{Spec} A$, then $X^{(p)} = \operatorname{Spec} \operatorname{Spec} A[\{T_i\}]/(\{g_j^{(p)}\}) = \operatorname{Spec} B \otimes_{A,\phi_A} A$ where $\phi_A : A \to A$ is given by $x \mapsto x^p$. We sometimes write $\phi_{A,*}B = B \otimes_{A,\phi_A} A$ as $b \otimes a^p = ab \otimes 1$ It's also common to denote by $\phi_{B/A}$ the induced map $\phi_{B/A} = F_{X/S}^* : B \otimes_{A,\phi_A} A \to B, b \otimes a \mapsto ab^p$.

If G/S is a group scheme of characteristic p, then $F_{G/S} : G \to G^{(p)}$ is a morphism of S-group schemes due to the functoriality of the Frobenius. If $S = \operatorname{Spec} \mathbb{F}_p$, then $F_{X/S} = F_X$. If $X = X_0 \times_{\mathbb{F}_p} S$, then $X^{(p)} = X_0 \times_{\mathbb{F}_p} S = X$ (via $F_{X_0} \times \mathrm{id}_S$). If $G = \Lambda_S$ is a constant group scheme, then $G^{(p)} = G$ and $F_{G/S} = \mathrm{id}_G$ as $G = G_0 \times_{\mathbb{F}_p} S, G_0 = \Lambda_{\mathbb{F}_p} = \prod_\Lambda \operatorname{Spec} \mathbb{F}_p$. If G is any diagonalisable group, then $G^{(p)} = G$ and $F_{X/S} = [p]$. Indeed, we can just check this for $D_{\mathbb{F}_p}(\Lambda) = \operatorname{Spec} \mathbb{F}_p[\Lambda]$ where $[p]^* : (\lambda) \mapsto (\lambda^p)$ (writing Λ multiplicatively). So $[p]^* = \phi_{\mathbb{F}_p}[\Lambda]$.
Thus $\ker F_{G/S}$ is trivial if G is constant, $\ker[p]$ if G is diagonalisable, $\alpha_{p,S}$ if $G = \mathbb{G}_{a,S}$. All of them is in $\ker[p]$. This turns out to be a general fact for commutative group schemes.

Theorem 2.15. *Suppose G/S is a flat commutative group scheme of characteristic p. Then there exists a map $V_{G/S} : G^{(p)} \to G$ (called the "shift" or "Verschiebung") of S-group schemes with $V_{G/S} \circ F_{G/S} = [p]$.*
Furthermore, $V_{G/S}$ is functorial in the sense that

$$\begin{array}{ccc} G^{(p)} & \xrightarrow{V_{G/S}} & G \\ {\scriptstyle f^{(p)} = f \times \mathrm{id}_S}\downarrow & & \downarrow{\scriptstyle f} \\ H^{(p)} & \xrightarrow[V_{H/S}]{} & H \end{array}$$

commutes for any map $f : G \to H$ of flat commutative S-group schemes G, H of characteristic p.

Proof. We will construct $V_{G/S}$ as follows: Suppose $G = \operatorname{Spec} B/S = \operatorname{Spec} A$ where A is an $\mathbb{F}_p$-algebra. $[p]^* : B \to B$ is the composition of comultiplication and multiplication maps between B and $\bigotimes_A^p B$. Consider the set of symmetric invariants $(\bigotimes_A^p B)^{S_p}$ which admits a map from B as G is commutative.
For any A-module M, we have an obvious map $\gamma : \bigotimes_A^p M \to (\bigotimes_A^p M)^{S_p}$ by sending $x_1 \otimes \cdots \otimes x_p$ to $\sum_{\sigma \in S_p} x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(p)}$ for any A-module M. If M is free over A, then there is an isomorphism $\eta : \operatorname{coker} \gamma \to M \otimes_{A, \phi_A} A, x_1 \otimes \cdots \otimes x \mapsto x \otimes 1$. Indeed, suppose $M = \bigoplus_{i \in I} Ae_i$, then $\operatorname{Im} \gamma$ is generated by the elements

$$t_i = \sum_{\sigma \in S_p} e_{i_{\sigma(1)}} \otimes \cdots \otimes e_{i_{\sigma(p)}}, i = (i_1, \dots, i_p) \in I^p$$

whereas $(\bigotimes_A^p M)^{S_p}$ is generated by

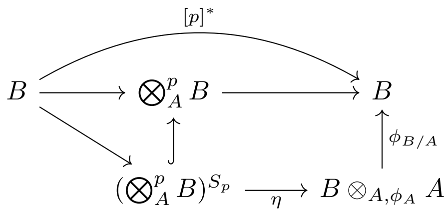
$$t'_i = \sum_{\sigma \in S_p / \Delta_i} e_{i_{\sigma(1)}} \otimes \cdots \otimes e_{i_{\sigma(p)}}$$

where Δ_i is the stabiliser of i. Consequently $t_i = |\Delta_i| t'_i$. So $\operatorname{coker} \gamma$ is generated by $e_i \otimes \cdots \otimes e_i, i \in I$. Write $\delta : M \to (\bigotimes_A^p M)^{S_p}, m \mapsto m \otimes \cdots \otimes m$. If $m = \sum_i m_i e_i$, then

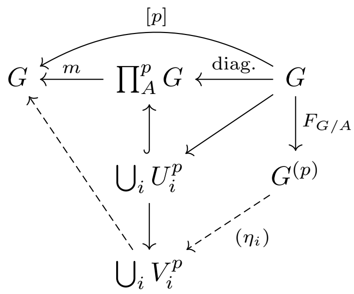
$$\delta(m) = \left(\sum_i m_i e_i \right) \otimes \cdots \otimes \left(\sum_i m_i e_i \right) \equiv \sum_i m_i^p e_i \otimes \cdots \otimes e_i \pmod{\operatorname{Im} \gamma}$$

As $\delta(am) = a! \delta(m)$, δ induces an isomorphism $M \otimes_p A \to \operatorname{coker} \gamma$.
Let's apply this result to $B = M$. Since the multiplication map $\bigotimes_A^p B \to B$

vanishes on $\operatorname{Im}\gamma$, we have a factorisation



So for G affine, $V_{G/A}$ is simply the composition of η and comultiplication.
For G not necessarily affine (but still over A), we write $G = \bigcup_i U_i, U_i = \operatorname{Spec} B_i$. We have the maps $U_i^p = \operatorname{Spec}(\bigotimes_A^p B_i) \to V_i^p = \operatorname{Spec}((\bigotimes_A^p B_i)^{S_p})$. The diagram we had for the affine case translates to



For not necessarily affine S, we can just glue on the base. $\square$

Example 2.14. For a constant group scheme $G = \Lambda_S$, we have $F_{G/S} = \mathrm{id}$, so $V_{G/S} = [p]$. For $G = \mathbb{G}_{m,S}$, $F_{G/S} = [p]$ is surjective, so $V_{G/S} = \mathrm{id}$.
For $G = \mathbb{G}_{a,S}$, $[p] = 0$ and $F_{G/S}$ is surjective, so $V_{\mathbb{G}_a/S} = 0$.
For G an elliptic curve E over a field k, then $F_{E/k} : E \to E^{(p)}$ is an isogeny of degree p, so $V_{E/k}$ is essentially the dual isogeny of the Frobenius.

Proposition 2.16. *$F_{G/S} \circ V_{G/S} \in \operatorname{End}(G^{(p)}/S)$ is also given by $[p]$.*

Proof. Apply the functoriality of the Verschiebung to $f = F_{G/S} : G \to G^{(p)}$. Then $F_{G/S} \circ V_{G/S} = V_{G^{(p)}/S} \circ F_{G^{(p)}/S} = [p]_{G^{(p)}}$ by some easy diagram chasing involving $F_{G^{(p)}/S} : G^{(p)} \to (G^{(p)})^{(p)} = G^{(p^2)}$. $\square$

Theorem 2.17. *Suppose G/S is a finite locally free commutative group scheme of characteristic p. Then $V_{G/S}^\vee = F_{G^\vee/S}$.*

Proof. Let's assume $G = \operatorname{Spec} B, S = \operatorname{Spec} A$. We have $(B \otimes_\phi A)^\vee = \{l' : B \to A \text{ additive} : \forall a \in A, b \in B, l'(ab) = a^p l'(b)\}$. We want to identify it with $B^\vee \otimes_\phi A$. Indeed, the isomorphism is given by the natural map $B^\vee \otimes_\phi A \to (B \otimes_\phi A)^\vee, l \otimes 1 \mapsto l^p$. We know that the Verschiebung has the form $B \to (\bigotimes_A^p B)^{S_p} \to B \otimes_\phi A$. Dualising this gives $B^\vee \leftarrow \operatorname{Sym}_A^p B^\vee \leftarrow B^\vee \otimes \phi A$. The second arrow is $\eta^\vee : l \otimes 1 \mapsto l \otimes \cdots \otimes l \in \operatorname{Sym}_A^p B^\vee$, so the whole composition is simply $\phi_{B^\vee/A}$. $\square$

Let's now go back to $S = \operatorname{Spec} k$ for k a field and G/k algebraic (i.e. of finite type).

Definition 2.8. G is unipotent if it's isomorphic to a (closed) subgroup scheme of the group of unipotent (i.e. unit upper triangular) matrices $U_{n,k} \subset \mathrm{GL}_{n,k}$.

Example 2.15. $\mathbb{G}_a \cong U_2$ is unipotent over any k.

Let $G \subset U_{n,k}$. Consider the tangent spaces $T_{G,e} = \ker(G(k[\epsilon]/(\epsilon^2)) \to G(k))$ which is a k-subspace of

$$T_{U_n,e} = \left\{ I + \epsilon X : X = \begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix} \right\}$$

In characteristic 0, the usual theory of Lie groups works, and if G is connected then we can describe G using $T_{G,e}$ (which is just the Lie algebra of G).

Theorem 2.18. *If* $\operatorname{char} k = 0$ *and G is connected, commutative and unipotent, then* $G \cong \mathbb{G}_a^d$ *for some d.*

Proof. As $G \subset U_n$, we have the identification of G with $T_{G,e} \otimes \mathbb{G}_a$ (in general if U is a vector space over k then $U \otimes \mathbb{G}_a$ is the affine scheme whose R-points are $U \otimes_k R$) given by log, exp where as usual $\exp(X) = \sum_n X^n/n! \in U_n, \log(g) = \sum_n (-1)^{n-1}(g-1)^n/n$, which are both just finite sums actually. They are isomorphisms of schemes, and for commutative G they are also isomorphisms of group schemes. □

If G is not commutative, we can still compute the group law on G in terms of Lie algebra structure on $T_{G,e}$. This however is not true in characteristic p as we have the Witt group schemes.

2.5 Witt Group Schemes

Suppose $\operatorname{char} k = p > 0$, then there are unipotent groups that are not smooth, e.g. $\alpha_{p^j,k} \subset \mathbb{G}_a = U_2$ is unipotent but not smooth. Note that $\alpha_{p^j,k}$ and $\mathbb{G}_a$ even have the same tangent space (i.e. k), so indeed tangent spaces don't tell us a great deal about the group schemes. Even if we restrict our attention to smooth commutative groups, things are still more complicated than characteristic 0.

Example 2.16. Take

$$G = \left\{ \begin{pmatrix} 1 & x & y \\ & 1 & x \\ & & 1 \end{pmatrix} \right\} \subset U_3 \subset \mathrm{GL}_3$$

over some field k, then $G \cong \mathbb{A}^2$ as schemes. This is commutative by trivial matrix multiplications. If $\operatorname{char} k \neq 2$, there is an isomorphism of group schemes $G \to \mathbb{G}_a^2$ via the logarithm map

$$\begin{pmatrix} 1 & x & y \\ & 1 & x \\ & & 1 \end{pmatrix} \mapsto (x, y - (1/2)x^2)$$

If $\operatorname{char} k = 2$, then this argument fails. Indeed, $G, \mathbb{G}_a^2$ are not even isomorphic as $[2] = 0$ on $\mathbb{G}_a^2$ but not on G.

Not all is lost. We know that we still have $G \cong \mathbb{A}^2$ as a scheme. We also have morphisms of group schemes $i : \mathbb{G}_a \hookrightarrow G$ via $y \mapsto \begin{pmatrix} 1 & & y \\ & 1 & \\ & & 1 \end{pmatrix}$ and $q : G \to \mathbb{G}_a$ via $\begin{pmatrix} 1 & x & y \\ & 1 & x \\ & & 1 \end{pmatrix} \mapsto x$. So for any k-algebra R, we have an exact sequence

$$0 \longrightarrow R \xrightarrow{i_k} G(R) \xrightarrow{q_k} R \longrightarrow 0$$

So G is a nontrivial extension of $\mathbb{G}_a$ by $\mathbb{G}_a$. For $k = \mathbb{F}_2$, we have $\mathbb{G}(\mathbb{F}_2) \cong \mathbb{Z}/4\mathbb{Z}$.

The group scheme G constructed above for $p = 2$ is a special case of the Witt group scheme W_2.

We will construct ring schemes $W_n / \operatorname{Spec} \mathbb{F}_p, 1 \leq n \leq \infty, W = W_\infty$ with the property that $W_n \cong \mathbb{A}^n = \operatorname{Spec} \mathbb{F}_p[T_0, \ldots, T_{n-1}], W = \operatorname{Spec} \mathbb{F}_p[\{T_i\}_{i \in \mathbb{N}}]$ as schemes. A commutative ring scheme is what you think it is: It's a scheme whose Yoneda embedding lands in the category of commutative rings. So for an $\mathbb{F}_p$-algebra R, we want $W_n(R) = R^n, W(R) = R^{\mathbb{N}}$ with unusual addition and multiplication.

We will see that $W_1 = \mathbb{G}_a$ and there are morphisms of ring schemes $R_n : W_{n+1} \to W_n, (T_0, \ldots, T_n) \mapsto (T_0, \ldots, T_{n-1})$ with $\ker R_n = \{(0, \ldots, 0, x)\} \cong \mathbb{G}_a$. And the realisation of W shall be via $W = \varprojlim_n W_n$ with respect to this system. We'll have $W_n(\mathbb{F}_p) \cong \mathbb{Z}/p^n\mathbb{Z}, W(\mathbb{F}_p) = \mathbb{Z}_p$. More generally, if k is a perfect field with characteristic p, $A = W(k)$ will be a complete DVR with uniformiser p and residue field k. Concretely, $x \in A$ would have the form $\sum_{i \geq 0} [x] p^i$ where $[x]$ is the Teichmüller representative of x in k. The identification $A \cong W(k)$ is via sending $\sum_i [x_i] p^i$ to the Witt vector $(x_0, x_1^p, x_2^{p^2}, \ldots)$. In particular, $[p]$ takes $(x_0, \ldots, x_{n-1})$ to $(0, x_0^p, \ldots, x_{n-2}^p)$. We can write $[p] = V \circ F$, and ideed the Verschiebung is simply V which is the shift map $(x_0, \ldots, x_{n-1}) \mapsto (0, x_0, \ldots, x_{n-2})$. Note that when k is perfect, $pW(k) = \{(0, x_1, \ldots)\}$ as F is bijective. But this is not true if k is not perfect.

To construct W_n, we need to define addition and multiplication morphisms using some polynomials, and we'll start from characteristic 0.

Definition 2.9. Let $\mathbb{W}_n = \operatorname{Spec} \mathbb{Z}[T_0, \ldots, T_{n-1}] = \mathbb{A}^n_{\mathbb{Z}}$. Consider the polynomial $\Phi = (\Phi_0, \ldots, \Phi_{n-1}) : \mathbb{W}_n \to \mathbb{G}^n_{a,\mathbb{Z}}$ where Φ_i are the Witt polynomials (also written as W_i) given by $\Phi_0(T_0) = T_0, \Phi_1(T_0, T_1) = T_0^p + pT_1$ and in general $\Phi_j(T_0, \ldots, T_j) = T_0^{p^j} + pT_1^{p^{j-1}} + \cdots + p^j T_j$. These are also called "phantom components".

We can extend all these to $\Phi : \mathbb{W} = \varprojlim_n \mathbb{W}_n \to \mathbb{G}_a^{\mathbb{N}}$.

Once p is invertible, it's possible to invert Φ. In other words, $\Phi \times_{\mathbb{Z}} \mathbb{Z}[1/p] : \mathbb{W}_n \times_{\mathbb{Z}} \mathbb{Z}[1/p] \to \mathbb{G}^n_{a,\mathbb{Z}[1/p]}$ is an isomorphism of schemes. This defines a unique ring scheme structure on $\mathbb{W}_n \times_{\mathbb{Z}} \mathbb{Z}[1/p]$ for which Φ is a morphism of ring schemes. That is, if R is a $\mathbb{Z}[1/p]$-algebra, then $\Phi : \mathbb{W}_n(R) \to R^n$ is a bijection making $\mathbb{W}_n(R)$ a ring. This ring structure is equivalent to the family of polynomials $S_n, P_n \in (\mathbb{Z}[1/p])[X_0, \ldots, Y_0, Y_1, \ldots]$ with $\forall x, y \in \mathbb{W}_n(R)$, we have $x +_{\mathbb{W}} y = (S_0(x,y), S_1(x,y), \ldots), x \times_{\mathbb{W}} y = (P_0(x,y), P_1(x,y), \ldots)$, i.e. $\Phi_j(S_0(X,Y), S_1(X,Y), \ldots) = \Phi_j(X) + \Phi_j(Y), \Phi_j(P_0(X,Y), P_1(X,Y), \ldots) = \Phi_j(X) \times \Phi_j(Y)$.

Example 2.17. For $j = 0$, $\Phi_0 = T_0$, so $S_0 = X_0 + Y_0, P_0 = X_0 Y_0$. For $j = 1$,

$\Phi_1 = T_0^p + pT_1$ and thus $(X_0+Y_0)^p + pS_1 = (X_0^p + pX_1) + (Y_0^p + pY_1)$, so

$$S_1 = X_1 + Y_1 + \frac{X_0^p + Y_0^p - (X_0+Y_0)^p}{p} = X_1 + Y_1 - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} X_0^i Y_0^{p-i}$$

Similarly $P_1 = X_0^p Y_1 + X_1 Y_0^p + pX_1Y_1$.

One realise that all these polynomials have integer coefficients. It's a miracle that this is true in general.

Theorem 2.19. *For all $n \geq 0$, $S_n, P_n \in \mathbb{Z}[\{X_i, Y_i\}]$.*

Consequently, $\mathbb{W}_n, \mathbb{W}$ are ring schemes over $\mathbb{Z}$ via S_n, P_n. The axioms they have to satisfy for this to work are polynomial identities involving $S_n, P_n, 1 = (1, 0, 0, \ldots), 0 = (0, 0, \ldots)$, but we already know that they hold in $\mathbb{Z}[1/p]$.

Proof. (Dwork) First define $F, V : \mathbb{W} \to \mathbb{W}$ via the obvious choices $F = (T_0^p, T_1^p, \ldots), V = (0, T_0, T_1, \ldots)$. F is a morphism of schemes and

$$\Phi_j \circ f = \Phi_j(T_0^p, \ldots, T_j^p) = \sum_{i=0}^{j} p^i T_i^{p^{j-i+1}} = \Phi_{j+1} - p^{j+1}T_{j+1}$$

On the other hand,

$$\Phi_j \circ V = \Phi_j(0, T_0, \ldots, T_{j-1}) = \sum_{i=1}^{j} p^i T_{i-1}^{p^{j-i}} = p\Phi_{j-1}$$

So V is additive, i.e. it's an endomorphism of the group scheme $\mathbb{W} \times_{\mathbb{Z}} \mathbb{Z}[1/p]$. The proof follows from the following discussion. ☐

Lemma 2.20 (Dwork's Lemma)**.** *Suppose $x = (x_0, x_1, \ldots), y = (y_0, y_1, \ldots) \in \mathbb{W}(R)$ for some ring R and $k, n \geq 1$, then the followings are equivalent:*
(i) $x_m \equiv y_m \pmod{p^k R}$ for all $0 \leq m \leq n$.
(ii) $\Phi_j(x) \equiv \Phi_j(y) \pmod{p^{k+j} R}$ for all $0 \leq j \leq n$.

Proof. Follows from the definition of Φ. ☐

Theorem 2.21. *Let $q \in \mathbb{Z}[X, Y], R = \mathbb{Z}[\{X_i, Y_i\}_{i \in \mathbb{N}}]$, and $Q_j \in R[1/p], j \in \mathbb{N}$ be the unique polynomials such that $\forall j, \Phi_j(Q_0, \ldots, Q_j) = q(\Phi_j(X), \Phi_j(Y))$. Then $Q_j \in R$.*

$q = X + Y, Q_j = S_j$ and $q = XY, Q_j = P_j$ are the cases we need.

Proof. Assume $Q_j \in R$ for $0 \leq j < n$, then we have

$$\begin{aligned} \Phi_n(Q) = q(\Phi_n(X), \Phi_n(Y)) &\equiv q(\Phi_{n-1}(X^p), \Phi_{n-1}(Y^p)) \\ &\equiv \Phi_{n-1}(Q(X^p, Y^p)) \pmod{p^n R} \end{aligned}$$

and

$$p^n Q_n = \Phi_n(Q_0, \ldots, Q_{n-1}) - \Phi_{n-1}(Q_0^p, \ldots, Q_{n-1}^p)$$

Now for any $j < n$ we have $Q_j(X, Y)^p \equiv Q_j(X^p, Y^p) \pmod{p}$, so by the preceding lemma we have $p^n Q_n \equiv 0 \pmod{p^n R}$, i.e. $Q_n \in R$. ☐

We have a morphism $\mathbb{A}^1_{\mathbb{Z}} \to W, R \ni x \mapsto [x] = (x, 0, \ldots)$ known as the Teichmüller map. This satisfies $(x_0, x_1, \ldots) = \sum_{n\geq 0} V^n([x_n])$ and $[a](x_0, x_1, \ldots) = (ax_0, a^p x_1, a^{p^2} x_2, \ldots)$ (both can be seen from computations in Φ). In particular, $[a][x] = [ax]$.
We can now define $W_n = \mathbb{W}_n \times_{\mathbb{Z}} \mathbb{F}_p, W = \mathbb{W} \times_{\mathbb{Z}} \mathbb{F}_p$ (so $\Phi : W \to \mathbb{A}^{\mathbb{N}}_{\mathbb{F}_p}$ is given by $(T_j) \mapsto (T_0, T_0^p, T_0^{p^2}, \ldots)$). As functors, W is simply the restriction of $\mathbb{W}$ to $\mathbb{F}_p$-algebras.

Proposition 2.22. *On W, F is a ring scheme morphism and FV, VF are the multiplication by p map on the appropriate scheme.*

Proof. If $pR = 0$, then F_R is simply $x \mapsto x^p$ which is a ring homomorphism, so F is a morphism of ring schemes. Let $F \circ V = (G_0, G_1, \ldots)$ and suppose multiplication by p is given by $(G'_0, G'_1, \ldots)$ for $G_j, G'_j \in \mathbb{Z}[X_0, \ldots, X_j]$. We want to show that $G'_j \equiv G_j \pmod p$ for all j. Indeed,

$$\begin{aligned}\Phi_n(G(x)) = \Phi_n(FVx) &= \Phi_{n+1}(Vx) - p^{n+1}(Vx)_{n+1} = p\Phi_n(x) - p^{n+1}x_n \\ &= \Phi_n(G'(x)) - p^{n+1}x_n\end{aligned}$$

So we are done by Lemma 2.20. □

2.6 Finite Group Schemes over a Perfect Field

Let k be a perfect field. If $\operatorname{char} k = 0$ and G is a finite group scheme over k, then G is smooth, étale, therefore determined by the finite group $G(\bar{k})$ and the action of $\mathrm{Gal}(\bar{k}/k)$ on it.
From now on, we are interested in the case where k is a perfect field of characteristic $p > 0$. Suppose G/k is a finite group scheme, then we can consider the closed subscheme $G_{\mathrm{red}} \subset G$. It is in fact that it's a closed subgroup scheme. Indeed, since it's reduced and finite it is a disjoint union of $\operatorname{Spec} k_i$ for k_i/k finite (hence separable). So G_{red} is étale. This means that $G_{\mathrm{red}} \times G_{\mathrm{red}}$ is étale hence reduced over k, therefore $G_{\mathrm{red}} \times G_{\mathrm{red}} \subset G \times G \to G$ factors through $G_{\mathrm{red}} \subset G$, meaning that G_{red} is a closed subgroup scheme. Even better, since G_{red} is étale and the closed immersion $G_{\mathrm{red}} \to G$ is defined by a nilpotent ideal, there exists (by formal étaleness) a unique retraction $\pi : G \to G_{\mathrm{red}}$ which is a homeomorphism. By uniqueness, it's immediate that π is a morphism of group schemes. Let's compute its kernel. Since π is a homeomorphism and $\mathcal{O}_{G_{\mathrm{red}},e} = k$, we have $\ker \pi = G_0 = \operatorname{Spec} \mathcal{O}_{G,e}$, which is simply the (unique) connected component of G containing e. We therefore have the sequence

$$0 \longrightarrow G_0 \hookrightarrow G \underset{\curvearrowleft}{\xrightarrow{\pi}} G_{\mathrm{red}} \longrightarrow 0$$

G_0 is a normal subgroup scheme of G, i.e. for any k-algebra R, $G_0(R)$ is a normal subgroup of $G(R)$. Or equivalently, for any k-algebra R, for all $g \in G(R)$, the map $\mathrm{Inn}_g : G \times_k R \to G \times_k R$ induces an automorphism of $G_0 \times_k R$. So the sequence tells us that $G(R)$ is a semidirect product $G_0(R) \rtimes G_{\mathrm{red}}(R)$. However, $G_{\mathrm{red}}(R)$ doesn't have to be a normal subgroup: Say $G_0 = \mu_p, (\mathbb{Z}/p\mathbb{Z})^\times \subset \mathrm{Aut}(\mu_p)$, then $\mu_p \rtimes (\mathbb{Z}/p\mathbb{Z})^\times$ (over $\mathbb{F}_p$) can be noncommutative.
We have $G_0 \times_k G_{\mathrm{red}} \hookrightarrow G \times_k G \to G$ which is an isomorphism of schemes since they have isomorphic functor of points. When G is commutative, this is an isomorphism of group schemes.

Theorem 2.23. *Suppose G is finite and connected (so $G_{\text{red}} = \{e\} = \operatorname{Spec} k$). Then $\operatorname{rk}_k G = \dim_k \mathcal{O}_{G,e}$ is a power of p.*

Proof. As G is connected, $\mathcal{O}_{G,e} = k \oplus \mathfrak{m}_e$ and $\mathfrak{m}_e^N = 0$ for some N. So $F^n_{G/k} = F_{G^{(p^{n-1})}/k} \circ \cdots \circ F_{G^{(p)}/k} \circ F_{G/k}$ is zero for sufficiently large n. This allows us to reduce to the case where $F_{G/k} = 0, G = \operatorname{Spec} B, B = k \oplus \mathfrak{m}, \mathfrak{m}^p = 0$. So $B = k[T_1, \dots, T_d]/I$ where $T_1, \dots, T_d$ generate $\mathfrak{m}/\mathfrak{m}^2$ (Nakayama's lemma). I contains the ideal $(T_1^p, \dots, T_d^p)$.
We claim that $I = (T_1^p, \dots, T_d^p)$ which shows $\dim_k B = p^d$. Why is this claim true? Recall that since G is a group scheme, $\Omega_{B/k}$ is free, and it's isomorphic to $(\mathfrak{m}/\mathfrak{m}^2) \otimes_k B$. So it's freely generated by $\mathrm{d}T_1, \dots, \mathrm{d}T_d$. Suppose there is some $0 \neq f \in I$ containing a monomial $T_1^{a_1} \cdots T_d^{a_d}$ where $0 \leq a_i < p$ are not all zero. Choose f and the monomial such that $a_1 + \cdots + a_d$ is minimal. We have $\mathrm{d}f = 0$, so $\partial f / \partial T_j \in I$ for each j, which contradicts this minimality. □

Now consider finite $G = G_0 \times G_{\text{red}}$ commutative, where G_0 is connected and G_{red} is étale. By Cartier duality, $G_0^\vee = (G_0^\vee)_0 \times (G_0^\vee)_{\text{red}}, G_{\text{red}}^\vee = (G_{\text{red}}^\vee)_0 \times (G_{\text{red}}^\vee)_{\text{red}}$. Therefore $G_0 = ((G_0^\vee)_0)^\vee \times ((G_0^\vee)_{\text{red}})^\vee$ and likewise for G_{red}.
So we get a decomposition $G = G^{\text{cc}} \times G^{\text{ce}} \times G^{\text{ec}} \times G^{\text{ee}}$ where G^{cc} is connected with connected Cartier dual, G^{ce} is connected with étale Cartier dual, etc..
By the theorem, the first three have p-power rank. G^{ee} has rank prime to p: $G^{\text{ee}} \times_k \bar{k}$ is constant, so $(G^{\text{ee}}_{\bar{k}})^\vee \cong \prod_i \mu_{m_i, \bar{k}}$. As this is étale, $(p, m_i) = 1$.
G is connected iff $F_{G/k}$ is nilpotent and G is étale iff $F_{G/k}$ is an isomorphism. Recall that $V_{G/k}$ is the dual of $F_{G^\vee/k}$. So F, V are both nilpotent on G^{cc}; F is nilpotent while V is an isomorphism on G^{ce}; F is an isomorphism while V is nilpotent on G^{ec}.

Definition 2.10. A simple finite commutative group scheme G/k is one that does not have any nonzero proper subgroup scheme.

For simple G, we must have G is one of $G^{\text{cc}}, G^{\text{ce}}, G^{\text{ec}}, G^{\text{ee}}$. Suppose $k = \bar{k}$. If $G = G^{\text{ec}}$ (so G étale and $G^\vee$ connected), then G is constant and has order a power of p, i.e. $G \cong (\mathbb{Z}/p\mathbb{Z})_k, F = \mathrm{id}, V = 0$. Dually, if $G = G^{\text{ce}}$ then $G \cong \mu_{p/k}, F = 0, V = \mathrm{id}$.
Suppose now that $G = G^{\text{cc}}$ (over any field with characteristic p). We claim that if G is simple then $G \cong \alpha_p, F = V = 0$. This is not at all obvious.

Lemma 2.24. *Suppose G/k is a finite commutative group scheme, then $T_{G,e} \cong \operatorname{Hom}_{(\mathsf{GrpSch}/k)}(G^\vee, \mathbb{G}_a)$.*

Proof. Suppose $G = \operatorname{Spec} B$. Then $T_{G,e} = \ker(G(k[\epsilon]/(\epsilon^2)) \to G(k)) = \{B \to_k k[\epsilon]/(\epsilon^2), x \mapsto x \mapsto e^*(x) + \epsilon \ell(x)\}$ where $e^* : B \to k$ is the counit. This is isomorphic to $\{\ell : B \to_k k : \ell(xy) = \ell(x)e^*(y) + \ell(y)e^*(x)\}$, which is then isomorphic to $\operatorname{Hom}_{(\mathsf{Hopf}/k)}(k[T], B^\vee)$ (by sending ℓ to $T \mapsto \ell$). But this is just $\operatorname{Hom}_{(\mathsf{GrpSch}/k)}(G^\vee, \mathbb{G}_a)$. □

Now suppose $G = G^{\text{cc}}$ is simple, then $F_{G/k} = 0$ since otherwise $\ker F$ is a nontrivial subgroup (as we already know that F isn't an isomorphism). As $G^\vee$ is connected and nonzero, we have $T_{G^\vee,e} \neq 0$. The lemma then shows that there is a nonzero group scheme morphism $G \to \mathbb{G}_a$, which must have trivial kernel as G is simple. Therefore $G \to \ker(F_{\mathbb{G}_a/k}) = \alpha_p$ is a closed immersion. But α_p

already has rank p, so $G \cong \alpha_p$.
Suppose S is an $\mathbb{F}_p$-scheme, then

$$\begin{aligned}\mathrm{Hom}_{(\mathsf{GrpSch}/S)}(\mu_{p,S}, (\mathbb{Z}/p\mathbb{Z})_S) = 0 &= \mathrm{Hom}_{(\mathsf{GrpSch}/S)}(\alpha_{p,S}, (\mathbb{Z}/p\mathbb{Z})_S) \\ &\cong \mathrm{Hom}_{(\mathsf{GrpSch}/S)}(\mu_{p,S}, \alpha_{p,S})\end{aligned}$$

by Cartier duality. On the other hand, Cartier duality also shows that we have $\mathrm{Hom}_{(\mathsf{GrpSch}/k)}(\alpha_p, \mu_p) \cong \mathrm{Hom}_{(\mathsf{GrpSch}/k)}((\mathbb{Z}/p\mathbb{Z})_k, \alpha_{p,k}) = 0$ as $\alpha_p(k) = 0$. But in general $\mathrm{Hom}_{(\mathsf{GrpSch}/S)}(\alpha_{p,S}, \mu_{p,S}) = \alpha_p(S) \neq 0$.

Proposition 2.25. $\mathrm{Hom}_{(\mathsf{GrpSch}/k)}(\mu_p, \mathbb{G}_a) = \mathrm{Hom}_{(\mathsf{GrpSch}/k)}(\mu_p, W_n) = 0$ *for all* $n \geq 1$.

Proof. $V_{\mu_p/k}$ is an isomorphism, but $V_{W_n/k}$ is nilpotent. Any $\mu_p \to W_n$ commutes with V, so it must be zero. □

2.7 Dieudonné Theory

The aim here is to establish a contravariant functor from the category of commutative finite k-group schemes of p-power rank to the category of $W(k)$-modules $M(G)$ of finite length (i.e. finitely generated and killed by a power of p) equipped with additive maps $F, V : M(G) \to M(G)$ such that $Fa = \sigma(a)F, V\sigma(a) = aV, FV = VF = p$ for any $a \in W(k)$ ("Dieudonné modules"). Here σ is the Frobenius of $W(k)$, i.e. $(x_0, x_1, \ldots) \mapsto (x_0^p, x_1^p, \ldots)$.
Turns out this is an equivalence of categories, is additive in the sense that $M(G \times G') = M(G) \oplus M(G')$, has $\mathrm{length}_{W(k)} M(G) = d \iff \mathrm{rk}_k G = p^d$, and that $M(G^\vee)$ is in some sense a dual of $M(G)$.
There are various constructions of $M(G)$. The classical method is as follows:
First of all, we assume $G^\vee$ is connected (this is in fact equivalent to G being unipotent). Such G is killed by $V^n_{G/k}$ for some $n > 0$, since $G^\vee$ is killed by $F^n_{G^\vee/k}$ for some n. We can then set $M(G) = \mathrm{Hom}_{(\mathsf{GrpSch}/k)}(G, W_{n,k})$. If $n = 1$, i.e. $V_{G/k} = 0$, then this is $\mathrm{Hom}(G, \mathbb{G}_{a,k}) = T_{G^\vee,e}$.
We'd like this to be a $W(k)$-module whose structure is independent of the choice of n. If $V^n_{G/k} = 0$, then we have the natural map

$$V \circ - : \mathrm{Hom}_{(\mathsf{GrpSch}/k)}(G, W_n) \to \mathrm{Hom}_{(\mathsf{GrpSch}/k)}(G, W_{n+1})$$

which is an isomorphism, so indeed the group structure $M(G)$ is independent of n. We'd quite like to take the obvious $W(k)$-module structure. We have the surjective morphism $W(k) \to W_n(k)$ which allows the action of W on W_n as a ring scheme. To make this compatible with V, we need a correction action $W(k) \ni x : W_n \to W_n, (y_0, \ldots, y_{n-1}) \mapsto (x_0^{p^{1-n}}, \ldots, x_{n-1}^{p^{1-n}})(y_0, \ldots, x_{n-1})$. We have $M(G^{(p)}) = \mathrm{Hom}(G, (W_{n,k})^{(p^{-1})}) = M(G) \otimes_\sigma W(k)$, and $F^*_{G/k} : M(G^{(p)}) = M(G) \otimes_\sigma W(k) \to M(G)$ which gives rise to our desired F. V is constructed similarly.
It's a fact that this contravariant functor that takes groups killed by $V^n_{G/k}$ to Dieudoinné modules killed by V^n is an equivalence of categories, and its inverse can be given by taking $G(R) = \mathrm{Hom}_{W(k),F,V}(M(G), W_n(R))$ (we can in fact write down the affine algebra for G explicitly – see Grothendieck's Montreal lectures).
If $G, G^\vee$ are both connected, then it's not hard to see that $M(G^\vee) \cong M(G)^\vee =$

$\mathrm{Hom}_{W(k)}(M(G), W(k)[1/p]/W(k))$ with F being the transpose of V and vice versa.
There is only one possible definition for general G. Write $G = G^{\mathrm{ec}} \times G^{\mathrm{cc}} \times G^{\mathrm{ce}}$ and define $M(G) = M(G^{\mathrm{ec}} \times G^{\mathrm{cc}}) \times M((G^{\mathrm{ce}})^\vee)^\vee$ which, albeit is awful, works.

Remark. We can loose the dependence on n by defining $\mathrm{CW}^u = \varinjlim_n (W_n \to W_{n+1} \to \cdots)$ ("unipotent covectors"). For example, $\mathrm{CW}^u(\mathbb{F}_p) = \mathbb{Q}_p/\mathbb{Z}_p$. Fontaine constructed a "completion" CW of this with the property that any $G \neq 0$ has a nonzero morphism to CW. In fact, $\mathrm{CW}(R) = \{(\ldots, x_{-2}, x_{-1}, x_0) \in R^{\mathbb{N}} : \exists N, (x_{-N}, x_{-N-1}, \ldots,) \text{ nilpotent}\}$.
And we can write $M(G) = \mathrm{Hom}(G, \mathrm{CW}^u)$ if $G^\vee$ is connected.

3 Quotients and Descents

3.1 Fpqc Sheaves

What are cokernels of morphisms of commutative group schemes? There are some difficulties in defining it.

Example 3.1. Take $[n] : \mathbb{G}_m \to \mathbb{G}_m$ which has kernel μ_n and $\mu_n(R) = \ker([n] : R^\times \to R^\times)$. What about its cokernel? Morally, we want $\mathrm{coker}[n](R) = \mathrm{coker}[n]_R = R^\times/(R^\times)^n$ on points. But this cannot be the functor of points of a scheme X, e.g. we would have $X(\mathbb{Q}) = \mathbb{Q}^\times/(\mathbb{Q}^\times)^n \hookrightarrow X(\bar{\mathbb{Q}}) = \bar{\mathbb{Q}}^\times/(\bar{\mathbb{Q}}^\times) = \{1\}$.

Let X be a topological space. Recall that a map of abelian sheaves $\phi : \mathcal{F} \to \mathcal{G}$, taking kernels on each open set gives a sheaf $\ker\phi$, but taking cokernels in general only gives presheaves. We used sheafification to make sense of $\mathrm{coker}\,\phi$. Perhaps we could do a similar thing here.
This isn't completely crazy. For $X \in (\mathsf{Sch}/S)$, its functor of points does have a sheaf property, in the sense that for any $T \in (\mathsf{Sch}/S)$ and any open cover $T = \bigcup_i U_i$, we have

$$X(T) = \mathrm{Hom}_S(T, X) \cong \left\{ (f_i) \in \prod_i X(U_i) : \forall i, j, f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j} \right\}$$

Another way to write this is the following: We have an obvious morphism $\pi : U = \coprod_i U_i \to T$. The projections $\mathrm{pr}_1, \mathrm{pr}_2 : U \times_T U \to U$ have the form $U_i \cap U_j \hookrightarrow U_i, U_i \cap U_j \hookrightarrow U_j$ under the identification $U \times_T U = \coprod_{i,j} U_i \times_T U_j = \coprod_{i,j} (U_i \cap U_j)$. So we can write $X(T) = \{f \in X(U) : f \circ \mathrm{pr}_1 = f \circ \mathrm{pr}_2 \in X(U \times_T U)\}$. Grothedieck had the idea of generalising this to more general morphisms $\pi : U \to T$. But for which π can we have $X(T) = \{f \in X(U) : f \circ \mathrm{pr}_1 = f \circ \mathrm{pr}_2 \in X(U \times_T U)\}$? Taking $T = \mathbb{A}^1_k, U = \mathbb{G}_{m,k} \sqcup \{0\}$ shows that this does not hold in general.
We first start with an incomplete (weaker) definition.

Definition 3.1 (Incomplete)**.** A functor $F : (\mathsf{Sch}/S)^{\mathrm{op}} \to (\mathsf{Sets})$ is called an fpqc (*fidèlement plat quasi-compacte*, "faithfully flat and quasicompact") sheaf on S if:
(i) We have an isomorphism $F(\coprod_{i \in I} U_i) \cong \prod_{i \in I} F(U_i), U_i \in (\mathsf{Sch}/S)$ compatible with inclusions $U_i \hookrightarrow \coprod_{i \in I} U_i$ (in particular $F(\varnothing) = \{*\}$ is the final object in (Sets)).

(ii) For every surjective, flat and quasicompact morphism $\pi : U \to T$ in (Sch/S), we have the isomorphism $F(T) \cong \{s \in F(U) : \mathrm{pr}_1^*(s) = \mathrm{pr}_2^*(s) \in F(U \times_T U)\}$ via π^*.

Before giving the complete definition, let's first see some examples.

Theorem 3.1 (Grothendieck)**.** *If $X \in (\mathsf{Sch}/S)$, then its functor of points $\hat{h}_X$ is an fpqc sheaf on S.*

Example 3.2. Take $T = S = \operatorname{Spec} k, U = \operatorname{Spec} K$ where K/k is a finite Galois extension with Galois group G. We have $U \times_T U = \operatorname{Spec} K \otimes_k K$. We have an isomorphism

$$K \otimes_k K \to \prod_G K, x \otimes y \mapsto (xg(y))_{g \in G}$$

More generally, if K/k is finite separable and L/k contains a Galois closure of K, then

$$K \otimes_k L \cong \prod_{\sigma : K \hookrightarrow L} L$$

Anyways, this gives us $U \otimes_T U \cong \coprod_G U$. Under this identification, pr_1 is id_U on each copy of U in $\coprod_G U$ and pr_2 is $a_g = \operatorname{Spec}(g) : U \to U$ on the g^{th} copy. If X is a k-scheme and $F = \hat{h}_X$, then $\{x \in X(U) : x \circ \mathrm{pr}_1 = x \circ \mathrm{pr}_2\} = \{x \in X(K) : \forall g \in G, g(x) = x\} = X(k) = X(T)$ by Galois theory.

Remark. If $U = \coprod_{i \in I} U_i$ where $U_i \subset T$ are open subschemes, then $\pi : U \to T$ might not be quasicompact, e.g. I might be infinite, and the open immersions might not be quasicompact (e.g. $\mathbb{A}_k^\infty \setminus \{0\} \hookrightarrow \mathbb{A}_k^\infty$). But we still want to capture these cases if we want a morally correct definition of fpqc sheaves.

Definition 3.2. A morphism $\pi : U \to T$ is fpqc if it's flat, surjective, and for every open quasicompact $W \subset T$ there is some open quasicompact $V \subset U$ with $\pi(V) = W$.

Clearly if π is flat, surjective and quasicompact, then it's fpqc ($V = \pi^{-1}(W)$ will do). The correct definition of fpqc sheaves is then

Definition 3.3. A functor $F : (\mathsf{Sch}/S)^{\mathrm{op}} \to (\mathsf{Sets})$ is called an fpqc sheaf on S if:
(i) We have an isomorphism $F(\coprod_{i \in I} U_i) \cong \prod_{i \in I} F(U_i), U_i \in (\mathsf{Sch}/S)$ compatible with inclusions $U_i \hookrightarrow \coprod_{i \in I} U_i$.
(ii) For every fpqc morphism $\pi : U \to T$ in (Sch/S), we have an isomorphism $F(T) \cong \{s \in F(U) : \mathrm{pr}_1^* s = \mathrm{pr}_2^* s \in F(U \times_T U)\}$ via π^*.

Remark. Why do we want to capture some weak form of quasicompactness anyways? Recall that there exists flat closed immersions $Z \hookrightarrow T$ that are not open. The example was $T = (\mathbb{N} \cup \{\infty\}) \cong \{1/(n+1) : n \in \mathbb{N}\} \cup \{0\}$ over $\operatorname{Spec} k$ with the closed immersion $\operatorname{Spec} k \hookrightarrow T$.
Let $Z \hookrightarrow T$ be any such example, then $U = Z \sqcup (T \setminus Z) \to T$ is flat and surjective. Take $X = U$, then $U \times_T U = U$ and the identity $U \to X$ doesn't come from a map $T \to X$.

Remark. There are variants of the notion of fpqc sheaves. One is fppf sheaves, where we restrict to surjective flat morphisms that are locally finitely presented. We also have étale sheaves, where we restrict to surjective étale morphisms. All of these are examples of "sheaves for a Grothendieck topology".

Theorem 3.2. *Let $A \to B$ be a ring homomorphism. The followings are equivalent:*
(i) $\operatorname{Spec} B \to \operatorname{Spec} A$ *is flat and surjective.*
(ii) For every complex $M_1 \to M_2 \to M_3$ of A-modules

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

is exact iff

$$0 \longrightarrow M_1 \otimes_A B \longrightarrow M_2 \otimes_A B \longrightarrow M_3 \otimes_A B \longrightarrow 0$$

Note that the "only if" part of (ii) is just flatness.

Definition 3.4. If any of these holds, we say $A \to B$ is faithfully flat. We say a morphism $X \to Y$ is faithfuly flat if it's flat and surjective.

Many properties of schemes can then be checked after faithfully flat base change. For example, if $f : X \to Y, g : Y' \to Y$ are faithfully flat, then f is smooth iff the base change $X' = X \times_Y Y' \to Y'$ is smooth.

3.2 Sheaf Cokernel

Suppose now that $f : G \to H$ is a morphism of commutative group schemes. They represent some fpqc sheaves $\hat{h}_G, \hat{h}_H$. The cokernel of $\hat{h}_G \to \hat{h}_H$ isn't necessarily a sheaf as we've seen ($[n] : \mathbb{G}_m \to \mathbb{G}_m$). Just as for sheaves on topological spaces, there is a sheafification functor ("fpqc sheafification") $F \to F^{\text{sh}}$ from $(\mathsf{Presheaves})$ to $(\mathsf{fpqcSheaves})$ which is universal for maps into sheaves, i.e. $\operatorname{Hom}_{(\mathsf{Presheaves})}(F, G) \cong \operatorname{Hom}_{(\mathsf{fpqcSheaves})}(F^{\text{sh}}, G)$ for any sheaf G. This would also be the left-adjoint of the forgetful functor $(\mathsf{fpqcSheaves}) \to (\mathsf{Presheaves})$. The details are as follows: Start with a presheaf $F : (\mathsf{Sch}/S) \to (\mathsf{Sets})$.

Definition 3.5. F is a separated presheaf if $F(T) \to \{s \in F(U) : \operatorname{pr}_1^* s = \operatorname{pr}_2^* s \in F(U \times_T U)\}$ is an inclusion for any fpqc $U \to T$.

Define $F^+ : (\mathsf{Sch}/S) \to (\mathsf{Sets})$ by setting

$$F^+(T) = \varinjlim_{(U_i \to T)} \left\{ s \in \prod_i F(U_i) : \operatorname{pr}_1^* s = \operatorname{pr}_2^* s \in \prod_i F(U_i \times_T U_i) \right\}$$

where the direct limit is taken over families of morphisms $(U_i \to T)$ with $\coprod_i U_i \to T$ fpqc.
If F is separated, then F^+ is a sheaf. On the other hand, F^+ is separated for any F. So we can set the $F^{\text{sh}} = (F^+)^+$.
There are, however, some serious set-theoretic issues, since it's possible that the collection of families of morphisms we are taking limit over does not necessarily form a set. There are several standard ways to get around this (introducing Grothendieck universes, bounding cardinality, using a different topology like fppf, etc.), which we'll neither cover nor worry about.

Definition 3.6. The sheaf cokernel $\operatorname{coker} f$ of f is the fpqc sheafification of $\operatorname{coker}(\hat{h}_G \to \hat{h}_H)$.

Example 3.3. Suppose $f = [n] : \mathbb{G}_m \to \mathbb{G}_m$, then the presheaf cokernel is $R \mapsto (R^\times)/(R^\times)^n$. Given any R and $a \in R^\times$, there always exists some faithfully flat $R \to R'$ such that a becomes an n^{th} power in R' (e.g. $R = R[X]/(X^n - a)$, which is even free over R), so the sheaf cokernel is 0.

When is the sheaf cokernel representable by a group scheme? The fully faithful functor $(\mathsf{Sch}/S) \to (\mathsf{fpqcSheaves}/S), X \mapsto \hat{h}_X$ isn't an equivalence of categories – there are plenty of fpqc sheaves that are not representable.
To investigate this, one thing one need to ask is how one might realise the notion of gluing on fpqc sheaves, and how they compare to gluing of sheaves, schemes, morphisms, etc.. This relates to the concept of descents.

3.3 Gluing and Descents

How did we glue schemes? We took a family of schemes $(X_i)_{i\in I}$ and $U_{ij} \subset X_i$ open with isomorphisms $h_{ij} : U_{ij} \to U_{ji}$ such that $h_{ii} = \mathrm{id}$ and the diagram

$$\begin{array}{ccc} U_{ij} \cap U_{ik} & \xrightarrow{h_{ij}} & U_{ji} \cap U_{jk} \\ {\scriptstyle h_{ik}}\downarrow & \swarrow {\scriptstyle h_{jk}} & \\ U_{ki} \cap U_{kj} & & \end{array}$$

And we produce a scheme Y with open immersions $q_i : X_i \hookrightarrow Y$ with a nice map $\coprod_i X_i \to Y$ compatible with the h_{ij}'s.
There is a relative version of this. Suppose $T = \cup_i U_i$ and we have U_i-schemes $f_i : X_i \to U_i$ with $h_{ij} : X_i|_{U_i \cap U_j} = f_i^{-1}(U_i \cap U_j) \to X_j|_{U_i\cap U_j}$ such that $h_{ii} = \mathrm{id}$ and $h_{ik} = h_{jk} \circ h_{ij}$ on $U_i \cap U_j \cap U_k$. Then there is some $Y \to T$ with isomorphisms $q_i : X_i \to Y|_{U_i}$ satisfying $h_{ij} = q_j^{-1} \circ q_i$.
Phrased differently, given $f : X = \coprod_i X_i \to U = \coprod_i U_i$, we have an $(U \times_T U)$-isomorphism

$$\begin{array}{ccc} X \times_{\mathrm{pr}_1, U} (U \times_T U) = X \times_T U & \xrightarrow{\cong} & X \times_{\mathrm{pr}_2, U} (U \times_T U) = U \times_T X \\ {\scriptstyle f\times \mathrm{id}_U}\downarrow & \swarrow {\scriptstyle \mathrm{id}_U \times f} & \\ U \times_T U & & \end{array}$$

So the cocycle condition is just asserting the commutativity of the cocycle diagram

$$\begin{array}{ccc} (X \times_T U) \times_T U & \xrightarrow{\mathrm{pr}_{12}^* h} & (U \times_T X) \times_T U \\ {\scriptstyle \mathrm{pr}_{13}^* h}\downarrow & \swarrow {\scriptstyle \mathrm{pr}_{23}^* h} & \\ U \times_T U \times_T X & & \end{array}$$

where $h : X \times_T U \to U \times_T X$ is given by $(x, y) \mapsto (y, x)$ (so indeed $\mathrm{pr}_{12}^* h = h \times \mathrm{id}_U$).
The result of gluing is then $Y \to T$ with an isomorphism $g : X \to Y \times_T U$ such that the gluing diagram

$$\begin{array}{ccc} X \times_T U & \xrightarrow[\cong]{h} & U \times_T X \\ {\scriptstyle q\times \mathrm{id}_U}\downarrow\cong & & \cong\downarrow{\scriptstyle \mathrm{id}_U \times q} \\ Y \times_T (U \times_T U) & \xrightarrow[\cong]{} & (U \times_T U) \times_T Y \end{array}$$

commutes.
Now let $\pi : U \to T$ be fpqc and $X \to U$ a U-scheme. When can we find a T-scheme $Y \to T$ (the "descent" of X to T) such that $X \cong Y \times_T u$?

Example 3.4. Suppose $U = \operatorname{Spec} K \to T = \operatorname{Spec} k$ with K/k a field extension. For a K-scheme X, we are asking when does there exist a k-scheme Y with $X = Y \times_k K$ and, if so, how many are there.

Definition 3.7. An isomorphism $h : X \times_T U \to U \times_T X$ is a descent datum if the cocycle diagram commutes. We say h is effective if there exists $Y \to T$ and an isomorphism $q : X \to Y \times_T U$ such that the gluing diagram commutes.

It's quite clear that all descent Y of X to T arises from an effective descent datum. When is a descent datum effective, then?

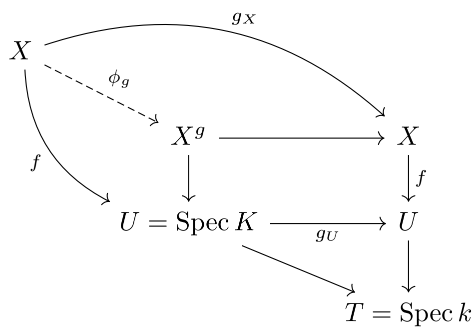
Example 3.5 (Galois Descent)**.** Suppose K/k is a finite Galois extension with Galois group G. This gives $U = \operatorname{Spec} K \to T = \operatorname{Spec} k$. G acts on K from the left, so we can make it a left action on U by associating each $g \in G$ with $g_U = ({}^a g)^{-1} : \operatorname{Spec} K \to \operatorname{Spec} K$. Recall that $U \times_T U = \coprod_G U$.
A descent datum for a K-scheme X is the same as giving, for each $g \in G$, an automorphism g_X fitting into the commutative diagram

$$\begin{array}{ccc} X & \xrightarrow[\cong]{g_X} & X \\ \downarrow & & \downarrow \\ \operatorname{Spec} K & \xrightarrow[\cong]{g_U} & \operatorname{Spec} K \end{array}$$

such that $(gh)_X = g_X h_X$ for all $g, h \in G$.

Theorem 3.3 (Weil)**.** *If X/k is quasiprojective and there exists $(g_X)_{g\in G}$ as above, then there is Y/k with an isomorphism $q : X \to Y \times_k K$ such that $g_X = \mathrm{id}_Y \times g_U$. Furthermore, (Y, q) is unique up to isomorphism.*

Remark. The classical way to express the descent datum in this case is the diagram



So to give $G \to \operatorname{Aut}(X), g \mapsto g_X$ with $f \circ g_X = g_U \circ f$ is the same as giving, for all $g \in G$, an isomorphism $\phi_g : X \to X^g$ with $(\phi_g)^h \phi_h = \phi_{gh}$, which can be viewed as a cocycle condition.

Galois descent is a particular case about quotients of schemes by finite groups, by viewing Y as "the quotient $G\backslash X$".

3.4 Quotients

Theorem 3.4. *Suppose X is a scheme and $G \subset \mathrm{Aut}(X)$ is a finite group. Suppose that for any $x \in X$, the orbit Gx is contained in an open affine (e.g. when X is a quasiprojective variety). Then there exists $q : X \to Y$ with the properties that:*
(i) q is G-invariant, i.e. $\forall g \in G, q \circ g = q$, and the fibres of q are G-orbits.
(ii) q is integral.
(iii) For any T, $Y(T) = G\backslash X(T)$ ("q is the categorical quotient").
(iv) $(q_*\mathcal{O}_X)^G = \mathcal{O}_Y$.

Write $Y = G\backslash X$ (or X/G if the action is on the right). This in particular implies Theorem 3.3 (take $X \to U = \mathrm{Spec}\, K$, then $G\backslash U = \mathrm{Spec}\, K^G = \mathrm{Spec}\, k$ and $Y = G\backslash X \to \mathrm{Spec}\, k$ has $X \cong Y \times_k K$ by (iii)).

Proof. First assume $X = \mathrm{Spec}\, B$ is affine, then $G \subset \mathrm{Aut}(B)$. Consider $Y = \mathrm{Spec}\, B^G$ with q induced by $B^G \to B$. Then (iii) and (iv) are immediate. (ii) becomes the statement that B is integral over B^G, which is true since $\prod_{g\in G}(t - g(b)) \in B^G[t]$. q is clearly G-invariant as well. The second part of (i) is some commutative algebra.
As for the general case, we'll show that X can be covered by G-invariant open affines. Once we've done this, we can simply take the quotient of these affines by G and glue.
Let $x \in X$. By hypothesis, $Gx \subset U$ for some open affine U. Let $V = \bigcap_{g\in G} gU$ which certainly contains Gx and is G-invariant. V might not be affine, but as Gx is finite and is contained in an affine open, there is some affine open $V' \subset V$ containing Gx (prime avoidance lemma). Now form the intersection $V'' = \bigcap_{g\in G} gV'$ which is affine since each gV' is affine and U is separated, and is G-invariant. □

Sadly, quotients don't exist in general.

Example 3.6 (Group Scheme without Galois Descent)**.** Let K be a field and $f : X \to U = \mathbb{A}^1_K$ a group scheme over U that's the line with three origins x_0, x_1, x_2 (so it's pretty much $i_*\mathbb{Z}/3\mathbb{Z}, i : \{0\} \hookrightarrow U$). Take $K = \mathbb{Q}(\sqrt{-3})$ and $k = \mathbb{Q}$, which has $G = \mathrm{Gal}(K/k) = \{1, g\}$. Let $\sigma \in \mathrm{Aut}(X/U)$ be such that it fixes x_0 and swaps x_1, x_2 (so it's $[-1]$ on $\mathbb{Z}/3\mathbb{Z}$). This defines an action of G on X covering the obvious action $\mathrm{id}_{\mathbb{A}^1} \times g_{\mathrm{Spec}\, K}$ on U by $g_X = \sigma \times g_{\mathrm{Spec}\, K}$. Then $G\backslash U = \mathbb{A}^1_{\mathbb{Q}}$ and $G\backslash f^{-1}(0) = \mu_{3,\mathbb{Q}}$ (noting $f^{-1}(0) = \mathrm{Spec}\, \mathbb{Q} \sqcup \mathrm{Spec}\, K$).
If there exists a scheme quotient $h : Y = G\backslash X \to \mathbb{A}^1_{\mathbb{Q}}$, then we have $h^{-1}(0) = \mu_{3,\mathbb{Q}}$. So we can choose a nonorigin point $y \in h^{-1}(0)$. We must have $y \times_k K = \{x_1, x_2\} \subset f^{-1}(0)$. As Y is a scheme, there is an open affine $V \subset Y$ containing y. $V \times_k K \subset X$ then is an open affine of X containing x_1, x_2 but not x_0, contradiction.
Although this quotient doesn't exist as a scheme, it does exist as an algebraic space.

Definition 3.8. Suppose X is an S-scheme and G an S-group scheme. An action of G on X is a morphism $a : G \times_S X \to X$ such that for any S-scheme T, $G(T) \times X(T) \to X(T)$ is a group action. A free action of G on X is such that $G(T) \times X(T) \to X(T)$ is a free group action, i.e. has trivial stabilisers.

The categorical quotient of X by G is an S-morphism $q : X \to Y$ which is G-invariant in the sense that $\forall g \in G(T), x \in X(T), q_T(gx) = q_T(x)$, and universal as such in the sense that for any G-invariant $q' : X \to Y'$ factors uniquely through q.
The orbit Gx of $x \in X$ is $a(\mathrm{pr}_2^{-1}(x))$.

Theorem 3.5. *Suppose G is finite locally free, acts on X, and Gx is contained in an open affine for any $x \in X$. Then there exists a categorical quotient $Y = G\backslash X$. Moreover, if the action is free, then this is simply the sheaf quotient, i.e. Y is the quotient of fpqc sheaves.*

Theorem 3.6. *Suppose G/S is a flat group scheme of finite type with S locally Noetherian, and $H \subset G$ is a closed subgroup scheme also flat over S. If either* $\dim S \leq 1$ *or H is proper over S, then the quotient sheaf is representable.*

These conditions are necessary: There is an example with $k = \mathbb{F}_2, S = \mathbb{A}^2_k, G = \mathbb{G}^2_{a,S}$ and $H \subset G$ is a closed subgroup scheme, étale over S (in fact $H \cong S \sqcup S \setminus \{0\}$ as a scheme) such that G/H doesn't exist. If the morphism is affine, we however do have nice things.

Theorem 3.7. *Suppose $\pi : U \to T$ is fpqc and $f : X \to U$ is affine. Then every descent datum for X is effective.*

Write $X = \underline{\mathrm{Spec}}_{\mathcal{O}_U} \mathcal{B}$ with $\mathcal{B}$ a quasicoherent sheaf of $\mathcal{O}_U$-algebras. So it suffices to prove descent for quasicoherent sheaves.
Suppose $\mathcal{F}$ is a quasicoherent $\mathcal{O}_U$-module, then a descent datum for $\mathcal{F}$ is essentially an isomorphism $g : \mathrm{pr}_1^* \mathcal{F} \to \mathrm{pr}_2^* \mathcal{F}$ such that on $U \times_T U \times_T U$ the diagram

$$\begin{array}{ccc} (\mathrm{pr}'_1)^*\mathcal{F} & \xrightarrow[\cong]{\mathrm{pr}_{12}^* g} & (\mathrm{pr}'_2)^*\mathcal{F} \\ {\scriptstyle \mathrm{pr}_{13}^* g}\downarrow & \swarrow {\scriptstyle \mathrm{pr}_{23}^* g} & \\ (\mathrm{pr}'_3)^*\mathcal{F} & & \end{array}$$

commutes. Note that if $\mathcal{G}$ is a quasicoherent $\mathcal{O}_T$-module, then $\pi^* G$ has a canonical descent datum $g_{\mathrm{triv}} : \mathrm{pr}_1^* \pi^* \mathcal{G} \to \mathrm{pr}_2^* \pi^* \mathcal{G}$ as $\pi \circ \mathrm{pr}_1 = \pi \circ \mathrm{pr}_2$. The theorem then follows from the following (stronger) statement.

Theorem 3.8. *Suppose $\pi : U \to T$ is fpqc, then then $\Phi : \mathcal{G} \mapsto (\pi^*\mathcal{G}, g_{\mathrm{triv}})$ is an equivalence of categories between the category of quasicoherent $\mathcal{O}_T$-modules and the category of pairs $(\mathcal{F}, g)$ with $\mathcal{F}$ a quasicoherent $\mathcal{O}_U$-sheaf and g a descent datum.*

Proof. It's a mere formality to reduce to the case $U = \mathrm{Spec}\, B \to T = \mathrm{Spec}\, A$ with B a faithfully flat A-algebra. Note also that if there is a section $s : T \to U$ of π, then $(\mathcal{F}, g) \mapsto s^*\mathcal{F}$ should be an inverse functor, so the theorem would be true in this case.
On affines, Φ takes an A-module M to $(M \times_A B, g_{\mathrm{triv}})$, which lives in the category $\mathscr{C}$ of pairs (N, g) with N a B-module and $g : N \otimes_A B \to B \otimes_A N$ an isomorphism of $B \otimes_A B$-modules. Consider $\Psi : \mathscr{C} \to (\mathsf{Mod}_A)$ sending (N, g) to $\{n \in N : g(n \otimes 1) = 1 \otimes n\} = \ker(\delta g : N \to B \otimes_A N, n \mapsto g(n \otimes 1) - 1 \otimes n)$. This is a right adjoint to Φ. We want to show that $M \to \Psi\Phi M, N \to \Phi\Psi(N, g)$ are isomorphisms. This can be checked after faithfully flat base change $A \to A'$

(where B becomes $B' = A' \otimes_A B$). But B is faithfully flat over A, so we can take $A' = B$ and $\operatorname{Spec} B' = \operatorname{Spec} B \otimes_A B \to \operatorname{Spec} A' = \operatorname{Spec} B$ has a section given by the diagonal! $\square$