Chapter III. Basic theory of group schemes.

As we have seen in the previous chapter, group schemes come naturally into play in the study of abelian varieties. For example, if we look at kernels of homomorphisms between abelian varieties then in general this leads to group schemes that are not group varieties. In the next chapters we shall have to deal with group schemes more often, so it is worthwile to set up some general theory.

The present chapter mainly deals with some basic notions, covering most of what is needed to develop the general theory of abelian varieties. We begin by introducing group schemes in a relative setting, i.e., working over an arbitrary basis. After this, in order to avoid too many technicalities, we shall focus on group schemes over a field and affine group schemes.

§ 1. *Definitions and examples.*

The definition of a group scheme is a variation on that of group variety, where we consider arbitrary schemes rather than only varieties. This leads to the following, somewhat cumbersome, definition.

(3.1) Definition. (i) Let S be a scheme. A *group scheme over* S, or an *S-group scheme*, is an S-scheme $\pi\colon G \to S$ together with S-morphisms $m\colon G \times_S G \to G$ (group law, or multiplication), $i\colon G \to G$ (inverse), and $e\colon S \to G$ (identity section), such that the following identities of morphisms hold:

$$m\circ(m \times \mathrm{id}_G) = m\circ(\mathrm{id}_G \times m)\colon\ G \times_S G \times_S G \to G\,,$$
$$m\circ(e \times \mathrm{id}_G) = j_1\colon\ S \times_S G \to G\,,$$
$$m\circ(\mathrm{id}_G \times e) = j_2\colon\ G \times_S S \to G\,,$$

and

$$e\circ\pi = m\circ(\mathrm{id}_G \times i)\circ\Delta_{G/S} = m\circ(i \times \mathrm{id}_G)\circ\Delta_{G/S}\colon\ G \to G\,,$$

where $j_1\colon S\times_S G \xrightarrow{\sim} G$ and $j_2\colon G\times_S S \xrightarrow{\sim} G$ are the canonical isomorphisms. (Cf. the definitions and diagrams in (1.1).)

(ii) A group scheme G over S is said to be *commutative* if, writing $s\colon G \times_S G \to G \times_S G$ for the isomorphism switching the two factors, we have the identity $m = m\circ s\colon G \times_S G \to G$.

(iii) Let $(\pi_1\colon G_1 \to S, m_1, i_1, e_1)$ and $(\pi_2\colon G_2 \to S, m_2, i_2, e_2)$ be two group schemes over S. A *homomorphism of S-group schemes* from G_1 to G_2 is a morphism of schemes $f\colon G_1 \to G_2$ over S such that $f\circ m_1 = m_2\circ(f \times f)\colon G_1 \times_S G_1 \to G_2$. (This condition implies that $f\circ e_1 = e_2$ and $f\circ i_1 = i_2\circ f$.)

In practice it will usually either be understood what m, i and e are, or it will be unnecessary to make them explicit; in such case we will simply speak about "a group scheme G over S" without further specification. (In fact, we already did so in parts (ii) and (iii) of the definition.)

If G is a group scheme over S and if $S' \to S$ is a morphism of schemes, then the pull-back $G' := G \times_S S'$ inherits the structure of an S'-group scheme. In particular, if $s \in S$ then the fibre $G_s := G \times_S \mathrm{Spec}\big(k(s)\big)$ is a group scheme over the residue field $k(s)$.

Given an S-group scheme G and an integer n, we define $[n] = [n]_G \colon G \to G$ to be the morphism which on sections—using multiplicative notation for the group law—is given by $g \mapsto g^n$. If $n \geqslant 1$ it factors as

$$[n] = (G \xrightarrow{\Delta^n_{G/S}} G^n_S \xrightarrow{m^{(n)}} G)\,,$$

where $m^{(n)}$ is the "iterated multiplication map", given on sections by $(g_1, \ldots, g_n) \mapsto g_1 \cdots g_n$. For commutative group schemes $[n]$ is usually called "multiplication by n".

(3.2) The definitions given in (3.1) are sometimes not so practicable. For instance, to define a group scheme one would have to give a scheme G, then one needs to define the morphisms m, i and e, and finally one would have to verify that a number of morphisms agree. Would it not be much simpler to describe a group as a scheme whose points form a group? Fortunately this can be done; it provides a way of looking at group schemes that is often more natural than the definition given above.

Suppose we have a scheme X over some base scheme S. For many purposes the underlying point set $|X|$ is not a good object to work with. For instance, if X is a group variety then $|X|$ will in general not inherit a group structure. However, there is another meaning of the term "point of X", and this notion is a very convenient one. Namely, recall that if $T \to S$ is another S-scheme then by a T-valued point of X we mean a morphism of schemes $x \colon T \to X$ over S. The set of such points is denoted $X(T)$. As a particular case, suppose $S = \operatorname{Spec}(k)$ and $T = \operatorname{Spec}(K)$, where $k \subset K$ is a field extension. Then one would also refer to a T-valued point of X as a "K-rational point", or in some contexts also as a "point of X with coordinates in K".

It is useful to place our discussion in a more general context. For this, consider a category C. The example to keep in mind is the category $C = \mathsf{Sch}_{/S}$ of schemes over a base scheme S. Write $\widehat{C}$ for the category of contravariant functors $C \to \mathsf{Sets}$ with morphisms of functors as the morphisms in $\widehat{C}$. For $X \in C$, the functor $h_X = \operatorname{Hom}_C(-, X)$ is an object of $\widehat{C}$. Sending X to h_X gives a covariant functor $h \colon C \to \widehat{C}$. The basic observation is that in this process we lose no information, as made precise by the following fundamental lemma.

(3.3) Yoneda Lemma. *The functor $h \colon C \to \widehat{C}$ is fully faithful. That is, for all objects X and X' of C, the natural map $\operatorname{Hom}_C(X, X') \to \operatorname{Hom}_{\widehat{C}}(h_X, h_{X'})$ is a bijection. More generally: for every $F \in \widehat{C}$ and $X \in C$, there is a canonical bijection $F(X) \to \operatorname{Hom}_{\widehat{C}}(h_X, F)$.*

Proof. Suppose given $F \in \widehat{C}$ and $X \in C$. The identity morphism id_X is an element of $h_X(X)$. If $\alpha \in \operatorname{Hom}_{\widehat{C}}(h_X, F)$ then define $\psi(\alpha) := \alpha(\mathrm{id}_X) \in F(X)$. This gives a map $\psi \colon \operatorname{Hom}_{\widehat{C}}(h_X, F) \to F(X)$. In the other direction, suppose we have $\beta \in F(X)$. If $x \colon T \to X$ is an element of $h_X(T)$ for some $T \in C$, define $\varphi(\beta)(x) \in F(T)$ to be the image of β under $F(x) \colon F(X) \to F(T)$. Now it is straightforward to verify that this gives a map $\varphi \colon F(X) \to \operatorname{Hom}_{\widehat{C}}(h_X, F)$ which is an inverse of ψ. □

(3.4) Definition. A functor $F \in \widehat{C}$ is said to be *representable* if it is isomorphic to a functor h_X for some $X \in C$. If this holds then it follows from the Yoneda lemma that X is uniquely determined by F up to C-isomorphism, and any such X is said to *represent* the functor F.

(3.5) Continuing the discussion of (3.2), we define the notion of a group object in the category C via the embedding into $\widehat{C}$. Thus, if X is an object of C then we define a C-group law on X to be a lifting of the functor $h_X \colon C \to \mathsf{Sets}$ to a group-valued functor $\tilde{h}_X \colon C \to \mathsf{Gr}$. Concretely, to

give a group law on an object X means that for each object T in C we have to specify a group law on the set $h_X(T) = \mathrm{Hom}_C(T, X)$, such that for every morphism $f\colon T_1 \to T_2$ the induced map $h_X(f)\colon h_X(T_2) \to h_X(T_1)$ is a homomorphism of groups. An object of C together with a C-group law on it is called a *C-group*, or a *group object in C*. In exactly the same way we can define other algebraic structures in a category, such as the notion of a ring object in C.

Let us now suppose that C is a category with finite products. This means that C has a final object (the empty product), which we shall call S, and that for any two objects X and Y there exists a product $X \times Y$. If G is a group object in C then the group structure on h_G gives a morphism of functors

$$m\colon h_{G\times_S G} = h_G \times h_G \longrightarrow h_G\,.$$

The Yoneda lemma tells us that this morphism is induced by a unique morphism $m_G\colon G\times_S G \to G$. In a similar way we obtain morphisms $i_G\colon G \to G$ and $e_G\colon S \to G$, and these morphisms satisfy the relations of (3.1)(i). Conversely, data (m_G, i_G, e_G) satisfying these relations define a C-group structure on the object G.

Applying the preceding remarks to the category $\mathsf{Sch}_{/S}$ of schemes over S, which is a category with finite products and with S as final object, we see that a group scheme G over S is the same as a representable group functor on $\mathsf{Sch}_{/S}$ together with the choice of a representing object (namely G). The conclusion of this discussion is so important that we state it as a proposition.

(3.6) Proposition. *Let G be a scheme over a base scheme S. Then the following data are equivalent:*

(i) *the structure of an S-group scheme on G, in the sense of* Definition (3.1)*;*

(ii) *a group structure on the sets $G(T)$, functorial in $T \in \mathsf{Sch}_{/S}$.*

For homomorphisms we have a similar assertion: if G_1 and G_2 are S-group schemes then the following data are equivalent:

(i) *a homomorphism of S-group schemes $f\colon G_1 \to G_2$, in the sense of* Definition (3.1)*;*

(ii) *group homomorphisms $f(T)\colon G_1(T) \to G_2(T)$, functorial in $T \in \mathsf{Sch}_{/S}$.*

In practise we often identify a group scheme G with the functor of points h_G, and we use the same notation G for both of them.

Already in the simplest examples we will see that this is useful, since it is often easier to understand a group scheme in terms of its functor of points than by giving the structure morphisms m, i and e. Before we turn to examples, let us use the functorial language to define the notion of a subgroup scheme.

(3.7) Definition. Let G be a group scheme over S. A subscheme (resp. an open subscheme, resp. a closed subscheme) $H \subset G$ is called an *S-subgroup scheme* (resp. an *open S-subgroup scheme*, resp. a *closed S-subgroup scheme*) of G if h_H is a subgroup functor of h_G, i.e., if $H(T) \subset G(T)$ is a subgroup for every S-scheme T. A subgroup scheme $H \subset G$ is said to be *normal* in G if $H(T)$ is a normal subgroup of $G(T)$ for every S-scheme T.

In what follows, if we speak about subgroup schemes it shall be understood that we give H the structure of an S-group scheme induced by that on G. An alternative, but equivalent, definition of the notion of a subgroup scheme is given in Exercise (3.1).

(3.8) Examples. 1. The *additive group*. Let S be a base scheme. The additive group over S, denoted $\mathbb{G}_{a,S}$, corresponds to the functor which associates to an S-scheme T the additive group $\Gamma(T, O_T)$. For simplicity, let us assume that $S = \mathrm{Spec}(R)$ is affine. Then $\mathbb{G}_{a,S}$ is represented by

the affine S-scheme $\mathbb{A}^1_S = \mathrm{Spec}\,\big(R[x]\big)$. The structure of a group scheme is given, on rings, by the following homomorphisms:

$\tilde{m}\colon R[x] \to R[x] \otimes_R R[x]$	given by	$x \mapsto x \otimes 1 + 1 \otimes x\,,$	defining the group law;
$\tilde{i}\colon R[x] \to R[x]$	given by	$x \mapsto -x\,,$	defining the inverse;
$\tilde{e}\colon R[x] \to R$	given by	$x \mapsto 0\,,$	defining the identity.

(See (3.9) below for further discussion of how to describe an affine group scheme in terms of a Hopf algebra.)

2. The *multiplicative group*. This group scheme, denoted $\mathbb{G}_{m,S}$, represents the functor which associates to an S-scheme T the multiplicative group $\Gamma(T, O_T)^*$ of invertible elements of $\Gamma(T, O_T)$. As a scheme, $\mathbb{G}_m = \mathrm{Spec}\,\big(O_S[x, x^{-1}]\big)$. The structure of a group scheme is defined by the homomorphisms given by

$x \mapsto x \otimes x$	defining the multiplication;
$x \mapsto x^{-1}$	defining the inverse;
$x \mapsto 1$	defining the identity element.

3. *n-th Roots of unity*. Given a positive integer n, we have an S-group scheme $\mu_{n,S}$ which associates to an S-scheme T the subgroup of $\mathbb{G}_m(T)$ of elements whose order divides n. The O_S-algebra defining this group scheme is $O_S[x, x^{-1}]/(x^n - 1)$ with the group law given as in Example 2. Put differently, $\mu_{n,S}$ is a closed subgroup scheme of $\mathbb{G}_{m,S}$.

4. *p^n-th Roots of zero*. Let p be a prime number and suppose that $\mathrm{char}(S) = p$. Consider the closed subscheme $\alpha_{p^n,S} \subset \mathbb{G}_{a,S}$ defined by the ideal (x^{p^n}); so $\alpha_{p^n,S} := \mathrm{Spec}\,\big(O_S[x]/(x^{p^n})\big)$. As is not hard to verify, this is in fact a closed subgroup scheme of $\mathbb{G}_{a,S}$. If $S = \mathrm{Spec}(k)$ for a field k of characteristic p then geometrically $\alpha_{p^n,k}$ is just a "fat point" (a point together with its $(p^n - 1)$st infinitesimal neighbourhood); but as a group scheme it has an interesting structure. If T is an S-scheme then $\alpha_{p^n}(T) = \{f \in \Gamma(T, O_T) \mid f^{p^n} = 0\}$, with group structure given by addition.

5. *Constant group schemes*. Let M be an arbitrary (abstract) group. Let $M_S := S^{(M)}$, the direct sum of copies of S indexed by the set M. If T is an S-scheme then $M_S(T)$ is the set of locally constant functions of $|T|$ to M. The group structure on M clearly induces the structure of a group functor on M_S (multiplication of functions), so that M_S becomes a group scheme. The terminology "constant group scheme" should not be taken to mean that the functor $T \mapsto M_S(T)$ has constant value M; in fact, if M is non-trivial then $M_S(T) = M$ only if T is connected.

In Examples 1–3 and 5, the group schemes as described here are all defined over $\mathrm{Spec}(\mathbb{Z})$. That is, in each case we have $G_S = G_{\mathbb{Z}} \times_{\mathrm{Spec}(\mathbb{Z})} S$ where $G_{\mathbb{Z}}$ is "the same" example but now over the basis $\mathrm{Spec}(\mathbb{Z})$. The group schemes α_{p^n} of Example 4 are defined over $\mathrm{Spec}(\mathbb{F}_p)$. The subscript "$_S$" is sometimes omitted if the basis is $\mathrm{Spec}(\mathbb{Z})$ resp. $\mathrm{Spec}(\mathbb{F}_p)$, or if it is understood over which basis we are working.

If $G = \mathrm{Spec}(A)$ is a finite k-group scheme then by the *rank* of G we mean the k-dimension of its affine algebra A. Thus, for instance, the constant group scheme $(\mathbb{Z}/p\mathbb{Z})_k$, and (for $\mathrm{char}(k) = p$) the group schemes $\mu_{p,k}$ and $\alpha_{p,k}$ all have rank p.

6. As is clear from the definitions, a group variety over a field k is the same as a geometrically integral group scheme over k. In particular, abelian varieties are group schemes.

7. Using the Yoneda lemma one easily sees that, for a group scheme G over a basis S, the morphism $i\colon G \to G$ is a homomorphism of group schemes if and only if G is commutative.

8. Let S be a basis with $\mathrm{char}(S) = p$. If G is an S-group scheme then $G^{(p/S)}$ naturally inherits the structure of an S-group scheme (being the pull-back of G via the absolute Frobenius morphism $\mathrm{Frob}_S\colon S \to S$). The relative Frobenius morphism $F_{G/S}\colon G \to G^{(p/S)}$ is a homomorphism of S-group schemes.

9. Let V be a finite dimensional vector space over a field k. Then we can form the group variety $\mathrm{GL}(V)$ over k. If $T = \mathrm{Spec}(R)$ is an affine k-scheme then $\mathrm{GL}(V)(T)$ is the group of invertible R-linear transformations of $V \otimes_k R$. If $d = \dim_k(V)$ then $\mathrm{GL}(V)$ is non-canonically (choice of a k-basis for V) isomorphic to the group variety $\mathrm{GL}_{d,k}$ of invertible $d \times d$ matrices; as a scheme the latter is given by

$$\mathrm{GL}_{d,k} = \mathrm{Spec}\left(k[T_{ij}, U;\, 1 \leqslant i, j \leqslant d]/(\det \cdot U - 1)\right),$$

where $\det \in k[T_{ij}]$ is the determinant polynomial. (So " $U = \det^{-1}$ ".) We leave it to the reader to write out the formulas for the group law.

More generally, if V is a vector bundle on a scheme S then we can form the group scheme $\mathrm{GL}(V/S)$ whose T-valued points are the vector bundle automorphisms of V_T over T. If V has rank d then this group scheme is locally on S isomorphic to a group scheme $\mathrm{GL}_{d,S}$ of invertible $d \times d$ matrices.

10. As another illustration of the functorial point of view, let us define semi-direct products. Let N and Q be two group schemes over a basis S. Consider the contravariant functor $\underline{\mathrm{Aut}}(N)\colon \mathsf{Sch}_{/S} \to \mathsf{Gr}$ which associates to an S-scheme T the group of automorphisms of N_T as a T-group scheme. Suppose we are given an action of Q on N by group scheme automorphisms; by this we mean that we are given a homomorphism of group functors

$$\rho\colon Q \to \underline{\mathrm{Aut}}(N)\,.$$

Then we can form the semi-direct product group scheme $N \rtimes_\rho Q$. The underlying scheme is just the product scheme $N \times_S Q$. The group structure is defined on T-valued points by

$$(n, q) \cdot (n', q') = \left(n \cdot \rho(q)(n'), q \cdot q'\right),$$

as expected. By (3.6) this defines an S-group scheme $N \rtimes_\rho Q$.

Here is an application. In ordinary group theory we know that every group of order p^2 is commutative. The analogue of this in the context of group schemes does not hold. Namely, if k is a field of characteristic $p > 0$ then there exists a group scheme of rank p^2 over k that is not commutative. We construct it as a semi-direct product. First note that there is a natural action of the group scheme $\mathbb{G}_m$ on the group scheme $\mathbb{G}_a$; on points it is given by the usual action of $\mathbb{G}_m(T) = \Gamma(T, O_T)^*$ on $\mathbb{G}_a(T) = \Gamma(T, O_T)$. This action restricts to a (non-trivial) action of $\mu_{p,k} \subset \mathbb{G}_{m,k}$ on $\alpha_{p,k} \subset \mathbb{G}_{a,k}$. Then the semi-direct product $\alpha_p \rtimes \mu_p$ has rank p^2 but is not commutative.

(3.9) *Affine group schemes.* Let $S = \mathrm{Spec}(R)$ be an affine base scheme. Suppose $G = \mathrm{Spec}(A)$ is an S-group scheme which is affine as a scheme. Then the morphisms m, i and e giving G its structure of a group scheme correspond to R-linear homomorphisms

$$\begin{aligned}
\tilde{m}\colon A \to A \otimes_R A \qquad & \text{called co-multiplication,} \\
\tilde{i}\colon A \to A \qquad & \text{called antipode or co-inverse,} \\
\tilde{e}\colon A \to R \qquad & \text{called augmentation or co-unit.}
\end{aligned}$$

These homomorphisms satisfy a number of identities, corresponding to the identities in the definition of a group scheme; see (3.1)(i). For instance, the associativity of the group law corresponds to the identity

$$(\tilde{m} \otimes 1) \circ \tilde{m} = (1 \otimes \tilde{m}) \circ \tilde{m} \colon A \to A \otimes_R A \otimes_R A \,.$$

We leave it to the reader to write out the other identities.

A unitary R-algebra equipped with maps $\tilde{m}$, $\tilde{e}$ and $\tilde{i}$ satisfying these identities is called a *Hopf algebra* or a *co-algebra* over R. A Hopf algebra is said to be co-commutative if $s \circ \tilde{m} = \tilde{m} \colon A \to A \otimes_R A$, where $s \colon A \otimes_R A \to A \otimes_R A$ is given by $x \otimes y \mapsto y \otimes x$. Thus, the category of affine group schemes over R is anti-equivalent to the category of commutative R-Hopf algebras, with commutative group schemes corresponding to Hopf algebras that are both commutative and co-commutative. For general theory of Hopf algebras we refer to ??. Note that in the literature Hopf algebras can be non-commutative algebras. *In this chapter, Hopf algebras are assumed to be commutative.*

The ideal $I := \mathrm{Ker}(\tilde{e} \colon A \to R)$ is called the *augmentation ideal*. Note that $A = R \cdot 1 \oplus I$ as R-module, since the R-algebra structure map $R \to A$ is a section of the augmentation. Note that the condition that $e \colon S \to G$ is a two-sided identity element is equivalent to the relation

$$\tilde{m}(\alpha) = (\alpha \otimes 1) + (1 \otimes \alpha) \bmod I \otimes I \tag{1}$$

in the ring $A \otimes_R A$. For the co-inverse we then easily find the relation

$$\tilde{i}(\alpha) = -\alpha \bmod I^2 \,, \quad \text{if } \alpha \in I \,. \tag{2}$$

(Exercise (3.3) asks you to prove this.)

The above has a natural generalization. Namely, suppose that G is a group scheme over an arbitrary basis S such that the structural morphism $\pi \colon G \to S$ is affine. (In this situation we say that G is an affine group scheme over S; cf. (3.10) below.) Let $A_G := \pi_* O_G$, which is a sheaf of O_S-algebras. Then $G \cong \mathrm{Spec}(A_G)$ as S-schemes, and the structure of a group scheme is given by homomorphisms of (sheaves of) O_S-algebras

$$\tilde{m} \colon A_G \to A_G \otimes_{O_S} A_G \,, \quad \tilde{i} \colon A_G \to A_G \,, \quad \text{and} \quad \tilde{e} \colon A_G \to O_S$$

making A_G into a sheaf of commutative Hopf algebras over O_S. Note that the unit section $e \colon S \to G$ gives an isomorphism between S and the closed subscheme of G defined by the augmentation ideal $I := \mathrm{Ker}(\tilde{e})$.

§ 2. *Elementary properties of group schemes.*

(3.10) Let us set up some terminology for group schemes. As a general rule, if P is a property of morphisms of schemes (or of schemes) then we say that a group scheme G over S with structural morphism $\pi \colon G \to S$ has property P if π has this property as a morphism of schemes (or if G, as a scheme, has this property). Thus, for example, we say that an S-group scheme G is noetherian, or finite, if G is a noetherian scheme, resp. if π is a finite morphism. Other properties for which the rule applies: the property of a morphism of schemes of being quasi-compact, quasi-separated, (locally) of finite type, (locally) of finite presentation, finite and locally free, separated, proper,

flat, and unramified, smooth, or étale. Similarly, if the basis S is the spectrum of a field k then we say that G is (geometrically) reduced, irreducible, connected or integral if G has this property as a k-scheme.

Note that we call G an *affine group scheme over* S if π is an affine morphism; we do not require that G is affine as a scheme. Also note that if G is a finite S-group scheme then this does not say that $G(T)$ is finite for every S-scheme T. For instance, we have described the group scheme α_p (over a field k of characteristic p) as a "fat point", so it should have a positive dimensional tangent space. Indeed, $\alpha_p(k) = \{1\}$ but $\alpha_p\big(k[\varepsilon]\big) = \{1 + a\varepsilon \mid a \in k\}$. We find that the tangent space of α_p at the origin has k-dimension 1 and that $\alpha_p\big(k[\varepsilon]\big)$ is infinite if k is infinite.

Let us also recall how the predicate "universal(ly)" is used. Here the general rule is the following: we say that $\pi\colon G \to S$ universally has property P if for every morphism $f\colon S' \to S$, writing $\pi'\colon G' \to S'$ for the morphism obtained from π by base-change via f, property P holds for G' over S'.

Let us now discuss some basic properties of group schemes. We begin with a general lemma.

(3.11) Lemma. (i) *Let*

$$\begin{array}{ccc} X' & \xrightarrow{i} & X \\ {\scriptstyle g'}\downarrow & & \downarrow{\scriptstyle g} \\ Y' & \xrightarrow{j} & Y \end{array}$$

be a cartesian diagram in the category of schemes. If g is an immersion (resp. a closed immersion, resp. an open immersion) then so is g'.

(ii) *Let $f\colon Y \to X$ be a morphism of schemes. If $s\colon X \to Y$ is a section of f then s is an immersion. If f is separated then s is a closed immersion.*

(iii) *If $s\colon X \to Y$ is a section of a morphism f, as in* (ii)*, then s maps closed points of X to closed points of Y.*

Proof. (i) Suppose g is an immersion. This means we have a subscheme $Z \subset Y$ such that g induces an isomorphism $X \xrightarrow{\sim} Z$. If Z is an open subscheme (i.e., g an open immersion) then $Y' \times_Y Z$ is naturally isomorphic to the open subscheme $j^{-1}(Z)$ of Y', and the claim follows. If Z is a closed subscheme defined by some ideal $I \subset O_Y$ (i.e, g a closed immersion) then $Y' \times_Y Z$ is naturally isomorphic to the closed subscheme of Y' defined by the ideal generated by $j^{-1}(I)$; again the claim follows. The case of a general immersion follows by combining the two previous cases.

(ii) By (i), it suffices to show that the commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{\quad s \quad} & Y \\ {\scriptstyle s}\downarrow & & \downarrow{\scriptstyle \Delta_{Y/X}} \\ Y & \xrightarrow{\mathrm{id}_Y \times (s \circ f)} & Y \times_X Y \end{array} \tag{3}$$

is cartesian. This can be done by working on affine open sets. Alternatively, if T is any scheme then the corresponding diagram of T-valued points is a cartesian diagram of sets, as one easily checks. It then follows from the Yoneda lemma that (3) is cartesian.

(iii) Let $P \in X$ be a closed point. Choose an affine open $U \subset Y$ containing $s(P)$. It suffices to check that $s(P)$ is a closed point of U. (This is special about working with points, as opposed

to arbitrary subschemes.) But $U \to X$ is affine, hence separated, so (i) tells us that $s(P)$ is a closed point of U. Alternatively, the assertion becomes obvious by working on rings. □

(3.12) Proposition. (i) *An S-group scheme G is separated if and only if the unit section e is a closed immersion.*

(ii) *If S is a discrete scheme (e.g., the spectrum of a field) then every S-group scheme is separated.*

Proof. (i) The "only if" follows from (ii) of the lemma. For the converse, consider the commutative diagram

$$\begin{array}{ccc} G & \xrightarrow{\pi} & S \\ {\scriptstyle \Delta_{G/S}}\downarrow & & \downarrow{\scriptstyle e} \\ G \times_S G & \xrightarrow{m \circ (\mathrm{id}_G \times i)} & G \end{array}$$

For every S-scheme T it is clear that this diagram is cartesian on T-valued points. By the Yoneda lemma it follows that the diagram is cartesian. Now apply (i) of the lemma.

(ii) Since separatedness is a local property on the basis, it suffices to consider the case that S is a 1-point scheme. Then the unit section is closed, by (iii) of the lemma. Now apply (i). □

As the following example shows, the result of (ii) is in some sense the best possible. Namely, suppose that S is a scheme which is *not* discrete. Then S has a non-isolated closed point s (i.e., a closed point s which is not open). Define G as the S-scheme obtained by gluing two copies of S along $S \setminus \{s\}$. Then G is not separated over S, and one easily shows that G has a structure of S-group scheme with $G_s \cong (\mathbb{Z}/2\mathbb{Z})_{k(s)}$. Notice that in this example G is even étale over S.

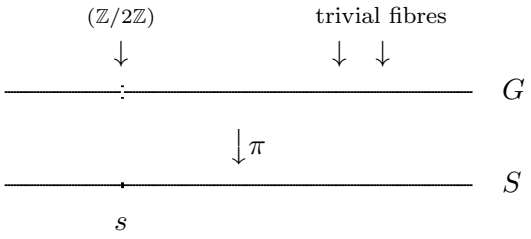

Figure 3.

(3.13) Definition. (i) Let G be an S-group scheme with unit section $e\colon S \to G$. Define $e_G = e(S) \subset G$ (a subscheme of G) to be the image of the immersion e.

(ii) Let $f\colon G \to G'$ be a homomorphism of S-group schemes. Then we define the *kernel of f* to be the subgroup scheme $\mathrm{Ker}(f) := f^{-1}(e_{G'})$ of G.

Note that the diagram

$$\begin{array}{ccc} \mathrm{Ker}(f) & \hookrightarrow & G \\ \downarrow & & \downarrow{\scriptstyle f} \\ S & \xrightarrow{e} & G' \end{array}$$

is cartesian. In particular, $\mathrm{Ker}(f)$ represents the contravariant functor $\mathsf{Sch}_{/S} \to \mathsf{Gr}$ given by

$$T \mapsto \mathrm{Ker}\Big(f(T)\colon G(T) \longrightarrow G'(T)\Big)$$

and is a normal subgroup scheme of G. If G' is separated over S then $\mathrm{Ker}(f) \subset G$ is a closed subgroup scheme.

As examples of kernels we have, taking $S = \mathrm{Spec}(\mathbb{F}_p)$ as our base scheme,

$$\mu_p = \mathrm{Ker}(F\colon \mathbb{G}_m \to \mathbb{G}_m)\,, \quad \alpha_p = \mathrm{Ker}(F\colon \mathbb{G}_a \to \mathbb{G}_a)\,,$$

where in both cases F denotes the Frobenius endomorphism.

(3.14) *Left and right translations; sheaves of differentials.* Let G be a group scheme over a basis S. Given an S-scheme T and a point $g \in G(T)$, the right translation $t_g\colon G_T \to G_T$ and the left translation $t'_g\colon G_T \to G_T$ are defined just as in (1.4). Using the Yoneda lemma we can also define t_g and t'_g by saying that for every T-scheme T', the maps $t_g(T')\colon G(T') \to G(T')$ and $t'_g(T')\colon G(T') \to G(T')$ are given by $\gamma \mapsto \gamma g$ resp. $\gamma \mapsto g\gamma$. Here we view g as an element of $G(T')$ via the canonical homomorphism $G(T) \to G(T')$.

If in the above we take $T = G$ and $g = \mathrm{id}_G \in G(G)$ then the resulting translations τ and $\tau'\colon G \times_S G \to G \times_S G$ are given by $(g_1, g_2) \to (g_1 g_2, g_2)$, resp. $(g_1, g_2) \to (g_2 g_1, g_2)$. Here we view $G \times_S G$ as a scheme over G via the second projection. We call τ and τ' the *universal right (resp. left) translation*. The point is that any other right translation $t_g\colon G \times_S T \to G \times_S T$ as above is the pull-back of τ via $\mathrm{id}_G \times g$ (i.e., the pull-back via g on the basis), and similarly for left translations.

As we have seen in (1.5), the translations on G are important in the study of sheaves of differentials. We will formulate everything using right translations. A 1-form $\alpha \in \Gamma(G, \Omega^1_{G/S})$ is said to be (right) invariant if it is universally invariant under right translations; by this we mean that for every $T \to S$ and $g \in G(T)$, writing $\alpha_T \in \Gamma(T, \Omega^1_{G_T/T})$ for the pull-back of α via $G_T \to G$, we have $t_g^* \alpha_T = \alpha_T$. In fact, it suffices to check this in the universal case: α is invariant if and only if $p_1^*\alpha \in \Gamma(G \times_S G, p_1^* \Omega^1_{G/S})$ is invariant under τ. The invariant differentials form a subsheaf $(\pi_* \Omega^1_{G/S})^G$ of $\pi_* \Omega^1_{G/S}$.

For the next result we need one more notation: if $\pi\colon G \to S$ is a group scheme with unit section $e\colon S \to G$, then we write

$$\omega_{G/S} := e^* \Omega^1_{G/S}\,,$$

which is a sheaf of O_S-modules. If S is the spectrum of a field then $\omega_{G/S}$ is just cotangent space of G at the origin.

(3.15) Proposition. *Let $\pi\colon G \to S$ be a group scheme. Then there is a canonical isomorphism $\pi^* \omega_{G/S} \xrightarrow{\sim} \Omega^1_{G/S}$. The corresponding homomorphism $\omega_{G/S} \to \pi_* \Omega^1_{G/S}$ (by adjunction of the functors π^* and π_*) induces an isomorphism $\omega_{G/S} \xrightarrow{\sim} (\pi_* \Omega^1_{G/S})^G$.*

Proof. As in (1.5), the geometric idea is that an invariant 1-form on G can be reobtained from its value along the zero section by using the translations, and that, by a similar proces, an arbitrary 1-form can be written as a function on G times an invariant form. To turn this idea into a formal proof we use the universal translation τ.

As above, we view $G \times_S G$ as a G-scheme via p_2. Then τ is an automorphism of $G \times_S G$ over G, so we have a natural isomorphism

$$\tau^* \Omega^1_{G \times_S G/G} \xrightarrow{\sim} \Omega^1_{G \times_S G/G}\,. \tag{4}$$

We observe that $G \times_S G/G$ is the pull back under p_1 of G/S; this gives that $\Omega^1_{G \times_S G/G} = p_1^* \Omega^1_{G/S}$. As $\tau = (m, p_2)\colon G \times_S G \to G \times_S G$, we find that (4) can be rewritten as

$$m^* \Omega^1_{G/S} \xrightarrow{\sim} p_1^* \Omega^1_{G/S}\,.$$

Pulling back via $(e\circ\pi, \mathrm{id}_G)$: $G \to G \times_S G$ gives the isomorphism

$$\Omega^1_{G/S} \xrightarrow{\sim} \pi^* e^* \Omega^1_{G/S} = \pi^* \omega_{G/S}\,. \tag{5}$$

By adjunction, (5) gives rise to a homomorphism $\pi^*\colon \omega_{G/S} \to \pi_*\Omega^1_{G/S}$ associating to a section $\beta \in \Gamma(S, \omega_{G/S})$ the 1-form $\pi^*\beta \in \Gamma(G, \pi^*\omega_{G/S}) = \Gamma(G, \Omega^1_{G/S})$. The isomorphism (5) is constructed in such a way that $\pi^*\beta$ is an invariant form. Clearly $e^*(\pi^*\beta) = \beta$. Conversely, if $\alpha \in \Gamma(G, \Omega^1_{G/S})$ is an invariant form then $m^*(\alpha) = \tau^*\big(p_1^*(\alpha)\big) = p_1^*(\alpha)$. Pulling back (as in the above argument) via $(e\circ\pi, \mathrm{id}_G)$ then gives that $\alpha = \pi^* e^*(\alpha)$. This shows that the map $(\pi_*\Omega^1_{G/S})^G \to \omega_{G/S}$ given on sections by $\alpha \mapsto e^*\alpha$ is an inverse of π^*. □

(3.16) *The identity component of a group scheme over a field.* Let G be a group scheme over a field k. By (3.12), G is separated over k. The image of the identity section is a single closed point $e = e_G$ of degree 1.

Assume in addition that G is locally of finite type over k. Then the scheme G is locally noetherian, hence locally connected. If we write G^0 for the connected component of G containing e, it follows that G^0 is an open subscheme of G. We call G^0 the *identity component* of G.

Geometrically, one expects that the existence of a group structure implies that G, as a k-scheme, "looks everywhere the same", so that certain properties need to be tested only at the origin. The following proposition shows that for smoothness and reducedness this is indeed the case. Note, however, that our intuition is a geometric one: in general we can only expect that "G looks everywhere locally the same" if we work over $k = \overline{k}$. In the following proposition it is good to keep some simple examples in mind. For instance, let p be a prime number and consider the group scheme μ_p over the field $\mathbb{Q}$. The underlying topological space consists of two closed points: the origin $e = 1$, and a point P corresponding to the non-trivial pth roots of unity. If we extend scalars from $\mathbb{Q}$ to a field containing a pth root of unity then the identity component $(\mu_p)^0 = \{e\}$ stays connected but the other component $\{P\}$ splits up into a disjoint union of $p-1$ connected components.

(3.17) Proposition. *Let G be a group scheme, locally of finite type over a field k.*

(i) *The identity component G^0 is an open and closed subgroup scheme of G which is geometrically irreducible. In particular: for any field extension $k \subset K$, we have $(G^0)_K = (G_K)^0$.*

(ii) *The following properties are equivalent:*

- (a1) *$G \otimes_k K$ is reduced for some perfect field K containing k;*
- (a2) *the ring $O_{G,e} \otimes_k K$ is reduced for some perfect field K containing k;*
- (b1) *G is smooth over k;*
- (b2) *G^0 is smooth over k;*
- (b3) *G is smooth over k at the origin.*

(iii) *Every connected component of G is irreducible and of finite type over k.*

Proof. (i) We first prove that G^0 is geometrically connected; that it is even geometrically irreducible will then follow from (iii). More generally, we show that if X is a connected k-scheme, locally of finite type, that has a k-rational point $x \in X(k)$ then X is geometrically connected. (See EGA IV, 4.5.14 for a more general result.)

Let $\overline{k}$ be an algebraic closure of k. First we show that the projection $p\colon X_{\overline{k}} \to X$ is open and closed. Suppose $\{V_\alpha\}_{\alpha\in I}$ is an open covering of X. Then $\{V_{\alpha,\overline{k}}\}_{\alpha\in I}$ is a covering of $X_{\overline{k}}$. If each $V_{\alpha,\overline{k}} \to V_\alpha$ is open and closed then the same is true for p. Hence we may assume that X is

affine and of finite type over k. Let $Z \subset X_{\overline{k}}$ be closed. Then there is a finite extension $k \subset K$ inside $\overline{k}$ such that Z is defined over K; concretely this means that there is closed subscheme $Z_K \subset X_K$ with $Z = Z_K \otimes_K \overline{k}$. Hence it suffices to show that the morphism $p_K\colon X_K \to X$ is open and closed. But this is immediate from the fact that p_K is finite and flat. (Use HAG, Chap. III, Ex. 9.1 or EGA IV, Thm. 2.4.6.)

Now suppose we have two non-empty open and closed subsets U_1 and U_2 of $X_{\overline{k}}$. Because X is connected, it follows that $p(U_1) = p(U_2) = X$. The unique point $\overline{x} \in X_{\overline{k}}$ lying over x is therefore contained in $U_1 \cap U_2$; hence $U_1 \cap U_2$ is non-empty. This shows that $X_{\overline{k}}$ is connected.

(ii) The essential step is to prove that (a2) $\Rightarrow$ (b1); all other implications are easy. (For (b3) $\Rightarrow$ (b1) use (3.15).) One easily reduces to the case that $k = \overline{k}$ and that G is reduced at the origin. Using the translations on G it then follows that G is reduced. In this situation, the same argument as in (1.5) applies, showing that G is smooth over k.

For (iii) one first shows that G^0 is irreducible and quasi-compact. We have already shown that $(G^0)_K = (G_K)^0$ for any field extension $k \subset K$, so we may assume that $k = \overline{k}$, in which case we can pass to the reduced underlying group scheme G^0_{red}; see Exercise (3.2). Note that G^0_{red} has the same underlying topological space as G^0. By (ii), G^0_{red} is smooth over k. Every point of G^0_{red} therefore has an open neighbourhood of the form $U = \mathrm{Spec}(A)$ with A a regular ring. As a regular ring is a domain, such an affine scheme U is irreducible. Now suppose G^0_{red} is reducible. Because it is connected, there exist two irreducible components $C_1 \neq C_2$ with $C_1 \cap C_2 \neq \emptyset$. (See EGA 0_{I}, Cor. 2.1.10.) If $y \in C_1 \cap C_2$, let $U = \mathrm{Spec}(A)$ be an affine open neighbourhood of y in G^0_{red} with A regular. Then one of $C_1 \cap U$ and $C_2 \cap U$ contains the other, say $C_2 \cap U \subseteq C_1 \cap U$. But $C_2 \cap U$ is dense in C_2, hence $C_2 \subseteq C_1$. As C_1 and C_2 are irreducible components we must have $C_2 = C_1$, contradicting the assumption.

To prove quasi-compactness of G^0, take a non-empty affine open part $U \subset G^0$. Then U is dense in G^0, as G^0 is irreducible. Hence for every $g \in G^0(k)$ the two sets $g \cdot U^{-1}$ and U intersect. It follows that the map $U \times U \to G^0$ given by multiplication is surjective. But $U \times U$ is quasi-compact, hence so is G^0.

Now we look at the other connected components, working again over an arbitrary field k. If $H \subset G$ is a connected component, choose a closed point $h \in H$. Because G is locally of finite type over k, there is a finite normal field extension $k \subset L$ such that L contains the residue field $k(h)$. As in the proof of (i), the projection $p\colon H \otimes_k L \to H$ is open and closed. One easily shows that all points in $p^{-1}(h)$ are rational over L. If $\tilde{h} \in p^{-1}(h)$ is one of these points then using the translation $t_{\tilde{h}}$ one sees that the connected component $C(\tilde{h})$ of H_L containing $\tilde{h}$ is isomorphic to G^0_L as an L-scheme. Then $p(C(\tilde{h})) \subset H$ is irreducible, closed and open. As H is connected it follows that $p(C(\tilde{h})) = H$ and that H is irreducible. Finally, the preceding arguments show that $H \otimes_k L$ is the union of the components $C(\tilde{h})$ for all $\tilde{h}$ in the finite set $p^{-1}(h)$. As each of these components is isomorphic to G^0_L, which is quasi-compact, it follows that H is quasi-compact. □

(3.18) Remarks. (i) Let G be a k-group scheme as in the proposition. Suppose that $G \otimes_k K$ is reduced (or that $O_{G,e} \otimes_k K$ is reduced) for some non-perfect field K containing k. Then it is not necessarily true that G is smooth over k. Here is an example: Suppose $K = k$ is a non-perfect field of characteristic p. Choose an element $\alpha \in k$ not in k^p. Let G be the k-scheme $G = \mathrm{Spec}\,\big(k[X,Y]/(X^p + \alpha Y^p)\big)$. View $\mathbb{A}^2_k = \mathrm{Spec}\,\big(k[X,Y]\big)$ as a k-group scheme by identifying it with $\mathbb{G}_{a,k} \times \mathbb{G}_{a,k}$. Then G is a closed subgroup scheme of $\mathbb{A}^2_k$. One easily checks that G is reduced, but clearly it is not geometrically reduced (extend to the field $k(\sqrt[p]{\alpha})$), and therefore G is not a smooth group scheme over k.

(ii) In (iii) of the proposition, let us note that the connected components of G are in general *not* geometrically irreducible; see the example given before the proposition.

(3.19) Remark. Let G be a group scheme, locally of finite type over a field k. In case G is affine, we have seen in (3.9) that we can study it through its Hopf algebra. For arbitrary G there is no immediate substitute for this, not even if we are only interested in the local structure of G at the origin. Note that the group law does not, in general, induce a co-multiplication on the local ring $O_{G,e}$. We do have a homomorphism $O_{G,e} \to O_{G\times_k G,(e,e)}$ but $O_{G\times_k G,(e,e)}$ is in general of course not the same as $O_{G,e} \otimes_k O_{G,e}$; rather it is a localisation of it. In some cases, however, something slightly weaker already suffices to obtain interesting conclusions. In the proof of the next result we shall exploit the fact that, with $\mathfrak{m} \subset O_{G,e}$ the maximal ideal, we do have a homomorphism $\tilde{m}\colon O_{G,e} \to (O_{G,e}/\mathfrak{m}^q) \otimes_k (O_{G,e}/\mathfrak{m}^q)$ for which the analogue of (1) in section (3.9) holds.

Another possibility is to consider the completed local ring $\hat{O}_{G,e}$. The group law on G induces a co-multiplication $\tilde{m}\colon \hat{O}_{G,e} \to \hat{O}_{G,e}\hat{\otimes}_k\hat{O}_{G,e}$ (completed tensor product). In this way we can associate to a group variety G a (smooth) formal group $\hat{G} = \mathrm{Spf}\big(\hat{O}_{G,e}\big)$. We shall further go into this in ??.

(3.20) Theorem. (Cartier) *Let G be a group scheme, locally of finite type over a field k of characteristic zero. Then G is reduced, hence smooth over k.*

Proof. We follow the elementary proof due to Oort [2]. Let $A := O_{G,e}$ be the local ring of G at the identity element. Write $\mathfrak{m} \subset A$ for the maximal ideal and $\mathrm{nil}(A) \subset A$ for the nilradical. Since we are over a perfect field, the reduced scheme G_{red} underlying G is a subgroup scheme (Exercise (3.2)), and by (ii) of Prop. (3.17) this implies that $A_{\mathrm{red}} := A/\mathrm{nil}(A)$ is a regular local ring. Writing $\mathfrak{m}_{\mathrm{red}} := \mathfrak{m}/\mathrm{nil}(A) \subset A_{\mathrm{red}}$, this gives

$$\dim(A) = \dim(A_{\mathrm{red}}) = \dim_k(\mathfrak{m}_{\mathrm{red}}/\mathfrak{m}_{\mathrm{red}}^2) = \dim_k\big(\mathfrak{m}/\mathfrak{m}^2 + \mathrm{nil}(A)\big)\,.$$

In particular, we see that it suffices to show that $\mathrm{nil}(A) \subset \mathfrak{m}^2$. Indeed, if this holds then $\dim(A) = \dim(\mathfrak{m}/\mathfrak{m}^2)$, hence A is regular, hence $\mathrm{nil}(A) = 0$.

Choose $0 \neq x \in \mathrm{nil}(A)$, and let n be the positive integer such that $x^{n-1} \neq 0$ and $x^n = 0$. Because A is noetherian, we have $\cap_{q\geqslant 0}\,\mathfrak{m}^q = (0)$, so there exists an integer $q \geqslant 2$ with $x^{n-1} \notin \mathfrak{m}^q$. Consider $B := A/\mathfrak{m}^q$ and $\bar{\mathfrak{m}} := \mathfrak{m}/\mathfrak{m}^q \subset B$, and let $\bar{x} \in B$ denote the class of $x \in A$ modulo $\mathfrak{m}^q$. As remarked above, the group law on G induces a homomorphism $\tilde{m}\colon A \to B \otimes_k B$. Just as in (3.9), the fact that $e \in G(k)$ is a two-sided identity element implies that we have

$$\tilde{m}(x) = (\bar{x}\otimes 1) + (1\otimes\bar{x}) + y \qquad \text{with } y \in \bar{\mathfrak{m}} \otimes_k \bar{\mathfrak{m}}\,. \tag{6}$$

(See also Exercise (3.3).) This gives

$$\begin{aligned} 0 = \tilde{m}(x^n) = \tilde{m}(x)^n &= ((\bar{x}\otimes 1) + (1\otimes\bar{x}) + y)^n \\ &= \sum_{i=0}^{n} \binom{n}{i} \cdot (\bar{x}\otimes 1)^{n-i} \cdot ((1\otimes\bar{x}) + y)^i\,. \end{aligned}$$

From this we get the relation

$$n\cdot(\bar{x}^{n-1}\otimes\bar{x}) \in \Big((\bar{x}^{n-1}\cdot\bar{\mathfrak{m}})\otimes_k B + B\otimes_k \bar{\mathfrak{m}}^2\Big) \subset B\otimes_k B\,.$$

But $\mathrm{char}(k) = 0$, so that n is a unit, so that even $(\bar{x}^{n-1} \otimes \bar{x}) \in (\bar{x}^{n-1} \cdot \bar{\mathfrak{m}}) \otimes_k B + B \otimes_k \bar{\mathfrak{m}}^2$. Now remark that a relation of the form $y_1 \otimes y_2 \in J_1 \otimes_k B + B \otimes_k J_2$ implies that either $y_1 \in J_1$ or $y_2 \in J_2$. (To see this, simply view B, J_1 and J_2 as k-vector spaces.) But by the Nakayama Lemma, $\bar{x}^{n-1} \in \bar{x}^{n-1} \cdot \bar{\mathfrak{m}}$ implies $\bar{x}^{n-1} = 0$, which contradicts our choice of q. We conclude that $\bar{x} \in \bar{\mathfrak{m}}^2$; hence $x \in \mathfrak{m}^2$, and we are done. □

The conclusion of this theorem does not hold over fields of positive characteristic. For example, if $\mathrm{char}(k) = p > 0$ then the group schemes $\mu_{p,k}$ and $\alpha_{p,k}$ are not reduced, hence not smooth over k. (The argument of the above proof breaks down if n is divisible by p.)

§ 3. *Cartier duality.*

(3.21) *Cartier duality of finite commutative group schemes.* We now discuss some aspects of finite commutative group schemes that play an important role in the study of abelian varieties. In particular, the Cartier duality that we shall discuss here comes naturally into play when we discuss the dual of an abelian variety; see Chapter 7.

The Cartier dual of a group scheme can be defined in two ways: working functorially or working with the underlying Hopf algebras. We first give two constructions of a dual group; after that we prove that they actually describe the same object.

The functorial approach is based on the study of *characters*, by which we mean homomorphisms of the group scheme to the multiplicative group $\mathbb{G}_m$. More precisely, suppose G is any commutative group scheme over a basis S. Then we can define a new contravariant group functor $\mathit{Hom}(G, \mathbb{G}_{m,S})$ on the category of S-schemes by

$$\mathit{Hom}(G, \mathbb{G}_{m,S})\colon T \mapsto \mathrm{Hom}_{\mathsf{GSch}_{/T}}(G_T, \mathbb{G}_{m,T})\,.$$

Next we define a dual object in terms of the Hopf algebra. For this we need to assume that G is commutative and finite locally free over S. As in (3.9) above, write $A := \pi_* O_G$. This A is a finite locally free sheaf of O_S-modules which comes equipped with the structure of a sheaf of co-commutative O_S-Hopf algebras. (Recall that all our Hopf algebras are assumed to be commutative.) Thus we have the following maps:

algebra structure map	$a\colon O_S \to A\,,$	augmentation	$\tilde{e}\colon A \to O_S\,,$
ring multiplication	$\mu\colon A \otimes_{O_S} A \to A\,,$	co-multiplication	$\tilde{m}\colon A \to A \otimes_{O_S} A\,,$
		co-inverse	$\tilde{i}\colon A \to A\,.$

We define a new sheaf of co-commutative O_S-Hopf algebras A^D as follows: first we set $A^D := \mathit{Hom}_{O_S}(A, O_S)$ as an O_S-module. The above maps induce O_S-linear maps

$$\begin{aligned} &a^D\colon A^D \to O_S\,, && \tilde{e}^D\colon O_S \to A^D\,,\\ &\mu^D\colon A^D \to A^D \otimes_{O_S} A^D\,, && \tilde{m}^D\colon A^D \otimes_{O_S} A^D \to A^D\,,\\ & && \tilde{i}^D\colon A^D \to A^D\,. \end{aligned}$$

We give A^D the structure of a sheaf of O_S-algebras by defining $\tilde{m}^D$ to be the multiplication and $\tilde{e}^D$ to be the algebra structure morphism. Next we define a Hopf algebra structure by using μ^D as the co-multiplication, $\tilde{i}^D$ as the co-inverse, and a^D as the co-unit. We leave it to the

reader (Exercise (3.8)) to verify that this gives A^D a well-defined structure of a co-commutative O_S-Hopf algebra. Schematically, if we write the structure maps of a Hopf algebra in a diagram

$$\begin{array}{ccc} & \vdots & \\ \text{multiplication} & \vdots & \text{co-multiplication} \\ & \text{antipode} & \\ \text{algebra structure map} & \vdots & \text{augmentation map} \\ & \vdots & \end{array}$$

then the diagram corresponding to A^D is obtained from that of A by first dualizing all maps and then reflecting in the dotted line.

We write $\alpha\colon A \to (A^D)^D$ for the O_S-linear map which sends a local section $s \in A(U)$ to the section ev_s = "evaluation at s" $\in \mathit{Hom}_{O_S}\big(\mathit{Hom}_{O_S}(A, O_S), O_S\big)(U)$.

(3.22) Theorem. (Cartier Duality) *Let $\pi\colon G \to S$ be a commutative S-group scheme which is finite and locally free over S. Write $A := \pi_* O_G$, and define the sheaf of co-commutative Hopf algebras A^D over O_S as above. Then $G^D := \mathrm{Spec}(A^D)$ is a commutative, finite locally free S-group scheme which represents the contravariant functor $\mathit{Hom}(G, \mathbb{G}_{m,S})\colon \mathsf{Sch}_{/S} \to \mathsf{Gr}$ given by*

$$T \mapsto \mathrm{Hom}_{\mathsf{GSch}_{/T}}(G_T, \mathbb{G}_{m,T})\,.$$

The homomorphism $(G^D)^D \to G$ induced by the map $\alpha\colon A \to (A^D)^D$ is an isomorphism.

Proof. That G^D is indeed a commutative group scheme is equivalent to saying that A^D is a sheaf of co-commutative Hopf algebras, which we have left as an exercise to the reader. That G^D is again finite and locally free over S (of the same rank as G) is clear, and so is the claim that $(G^D)^D \to G$ is an isomorphism.

Note that the functor $G \mapsto G^D$ is compatible with base-change: if T is an S-scheme and G is a commutative, finite locally free S-group scheme then $(G_T)^D \cong (G^D)_T$ canonically. In particular, to prove that G^D represents the functor $\mathit{Hom}(G, \mathbb{G}_{m,S})$ we may assume that the basis is affine, say $S = \mathrm{Spec}(R)$, and it suffices to show that $G^D(S)$ is naturally isomorphic to the group $\mathrm{Hom}_{\mathsf{GSch}_{/S}}(G, \mathbb{G}_{m,S})$. As S is affine we may view A simply as an R-Hopf algebra (i.e., replace the sheaf A by its R-algebra of global sections).

Among the identities that are satisfied by the structure homomorphisms we have that $(\tilde{e} \otimes \mathrm{id}) \circ \tilde{m}\colon A \to R \otimes_R A \cong A$ is the identity and that $(\tilde{i}, \mathrm{id}) \circ \tilde{m}\colon A \to A$ is equal to the composition $a \circ \tilde{e}\colon A \to R \to A$. In particular, if $b \in A$ is an element with $\tilde{m}(b) = b \otimes b$ then it follows that $\tilde{e}(b) \cdot b = b$ and that $\tilde{i}(b) \cdot b = \tilde{e}(b)$. It follows that

$$\{b \in A^* \mid \tilde{m}(b) = b \otimes b\} = \{b \in A \mid \tilde{m}(b) = b \otimes b \quad \text{and} \quad \tilde{e}(b) = 1\}\,.$$

Write A^{gl} for this set. (Its elements are sometimes referred to as the "group-like" elements of A.) One easily checks that A^{gl} is a subgroup of A^*.

With these remarks in mind, let us compute $\mathrm{Hom}_{\mathsf{GSch}_{/S}}(G, \mathbb{G}_{m,S})$ and $G^D(S)$. The R-algebra homomorphisms $f\colon R[x, x^{-1}] \to A$ are given by the elements $b \in A^*$, via the correspondence $b := f(x)$. The condition on $b \in A^*$ that the corresponding map f is a homomorphism of Hopf algebras is precisely that $\tilde{m}(b) = b \otimes b$. Hence we find a natural bijection $\mathrm{Hom}_{\mathsf{GSch}_S}(G, \mathbb{G}_{m,S}) \xrightarrow{\sim} A^{\mathrm{gl}}$, and one readily verifies this to be an isomorphism of groups.

Every R-module homomorphism $A^D \to R$ is of the form $\mathrm{ev}_b\colon \lambda \mapsto \lambda(b)$ for some $b \in A$. Conversely, if $b \in A$ then one verifies that

$$\mathrm{ev}_b(1) = 1 \quad \Longleftrightarrow \quad \tilde{e}(b) = 1$$

and

$$\mathrm{ev}_b \text{ is a ring homomorphism} \quad \Longleftrightarrow \quad \tilde{m}(b) = b \otimes b\,.$$

This gives a bijection $G^D(S) \xrightarrow{\sim} A^{\mathrm{gl}}$, and again one easily verifies this to be an isomorphism of groups. □

(3.23) Definition. Let $\pi\colon G \to S$ be a commutative S-group scheme which is finite and locally free over S. Then we call G^D the *Cartier dual* of G. Similarly, if $f\colon G_1 \to G_2$ is a homomorphism between commutative, finite locally free S-group schemes then we obtain an induced homomorphism $f^D\colon G_2^D \to G_1^D$, called the Cartier dual of f.

(3.24) Examples. 1. Take $G = (\mathbb{Z}/n\mathbb{Z})_S$. Then it is clear from the functorial description of the Cartier dual that $G^D = \mu_{n,S}$. Hence $(\mathbb{Z}/n\mathbb{Z})$ and μ_n are Cartier dual to each other. Note that $(\mathbb{Z}/n\mathbb{Z})_S$ and $\mu_{n,S}$ may well be isomorphic. For instance, if $S = \mathrm{Spec}(k)$ is the spectrum of a field and if $\zeta \in k$ is a primitive nth root of 1 then we obtain an isomorphism $(\mathbb{Z}/n\mathbb{Z})_k \xrightarrow{\sim} \mu_{n,k}$ sending $\bar{1}$ to ζ. In particular, if $k = \overline{k}$ and $\mathrm{char}(k) \nmid n$ then $(\mathbb{Z}/n\mathbb{Z})_k \cong \mu_{n,k}$. By contrast, if $\mathrm{char}(k) = p > 0$ and p divides n then $(\mathbb{Z}/n\mathbb{Z})_k$ and $\mu_{n,k}$ are *not* isomorphic.

2. Let S be a scheme of characteristic $p > 0$. We claim that $\alpha_{p,S}$ is its own Cartier dual. Of course this can be shown at the level of Hopf algebras, but the functorial interpretation is perhaps more instructive. As Cartier duality is compatible with base-change it suffices to do the case $S = \mathrm{Spec}(\mathbb{F}_p)$.

Recall that if R is a ring of characteristic p then $\alpha_p(R) = \{r \in R \mid r^p = 0\}$ with its natural structure of an additive group. If we want to make a homomorphism $\alpha_p \to \mathbb{G}_m$ then the most obvious guess is to look for an "exponential". Indeed, if $r \in \alpha_p(R)$ then

$$\exp(r) = 1 + r + \frac{r^2}{2!} + \cdots + \frac{r^{p-1}}{(p-1)!}$$

is a well-defined element of R^*, and $r \mapsto \exp(r)$ defines a homomorphism $\alpha_p(R) \to \mathbb{G}_m(R)$. Now remark that α_p (like $\mathbb{G}_a$) is not just a group scheme but has a natural structure of a functor in rings. The self-duality $\alpha_p \xrightarrow{\sim} \alpha_p^D = \mathit{Hom}_{\mathsf{ShGr}_{/\mathbb{F}_p}}(\alpha_p, \mathbb{G}_m)$ is obtained by sending a point $\xi \in \alpha_p(T)$ (where T is an $\mathbb{F}_p$-scheme) to the homomorphism of group schemes $\alpha_{p,T} \to \mathbb{G}_{m,T}$ given (on points with values in T-schemes) by $x \mapsto \exp(\xi \cdot x)$.

3. After the previous example, one might guess that α_{p^n} is self-dual for all n. This is not the case. Instead, $(\alpha_{p^n})^D$ can be described as the kernel of Frobenius on the group scheme W_n of Witt vectors of length n. See Oort [3], § 10. For a special case of this, see also Exercise ??.

§ 4. *The component group of a group scheme.*

If X is a topological space then $\pi_0(X)$ denotes the set of connected components of X. The purpose of this section is to discuss a scheme-theoretic analogue of this for schemes that are

locally of finite type over a field k. To avoid confusion we shall use the notation π_0 in the topological context and ϖ_0 for the scheme-theoretic analogue.

If X/k is locally of finite type then $\varpi_0(X)$ will be an étale k-scheme, and $X \mapsto \varpi_0(X)$ is a covariant functor. Furthermore, if G is a k-group scheme, locally of finite type over k, then $\varpi_0(G)$ inherits a natural structure of a group scheme; it is called the component group (scheme) of G.

We start with some generalities on étale group schemes. Let us recall here that, according to our conventions, an étale morphism of schemes $f\colon X \to Y$ is only required to be locally of finite type; see ??.

(3.25) *Étale group schemes over a field.* Let k be a field. Choose a separable algebraic closure k_s and write $\Gamma_k := \mathrm{Gal}(k_s/k)$. Then Γ_k is a pro-finite group, (see Appendix ??) and Galois theory tells us that $L \mapsto \mathrm{Gal}(k_s/L)$ gives a bijection between the field extensions of k inside k_s and the closed subgroups of Γ_k. Finite extensions of k correspond to open subgroups of Γ_k. A reference is Neukirch [1], Sect. 4.1.

By a Γ_k-set we mean a set Y equipped with a continuous left action of Γ_k. The continuity assumption here means that for every $y \in Y$ the stabilizer $\Gamma_{k,y} \subset \Gamma_k$ is an open subgroup; this implies that the Γ_k-orbits in Y are finite.

Let $S := \mathrm{Spec}(k)$. If X is a connected étale scheme over S, then X is of the form $X = \mathrm{Spec}(L)$, with L a finite separable field extension of k. An arbitrary étale S-scheme can be written as a disjoint union of its connected components, and is therefore of the form $X = \amalg_{\alpha\in I} \mathrm{Spec}(L_\alpha)$, where I is some index set and where $k \subset L_\alpha$ is a finite separable extension of fields. Hence the description of étale S-schemes is a matter of Galois theory. More precisely, if $\mathsf{Et}_{/k}$ denotes the category of étale k-schemes there is an equivalence of categories

$$\mathsf{Et}_{/k} \xrightarrow{\text{eq}} \left(\Gamma_k\text{-sets}\right).$$

associating to $X \in \mathsf{Et}_{/k}$ the set $X(k_s)$ with its natural Γ_k-action. To obtain a quasi-inverse, write a Γ_k-set Y as a union of orbits, say $Y = \amalg_{\alpha\in I}(\Gamma_k \cdot y_\alpha)$, let $k \subset L_\alpha$ be the finite field extension (inside k_s) corresponding to the open subgroup $\mathrm{Stab}(y_\alpha) \subset \Gamma_k$, and associate to Y the S-scheme $\amalg_{\alpha\in I} \mathrm{Spec}(L_\alpha)$. Up to isomorphism of S-schemes this does not depend on the chosen base points of the Γ_k-orbits, and it gives a quasi-inverse to the functor $X \mapsto X(k_s)$.

This equivalence of categories induces an equivalence between the corresponding categories of group objects. This gives the following result.

(3.26) Proposition. *Let $k \subset k_s$ and $\Gamma_k = \mathrm{Gal}(k_s/k)$ be as above. Associating to an étale k-group scheme G the group $G(k_s)$ with its natural Γ_k-action gives an equivalence of categories*

$$\begin{pmatrix}\text{étale}\\ k\text{-group schemes}\end{pmatrix} \xrightarrow{\text{eq}} \left(\Gamma_k\text{-groups}\right),$$

where by a Γ_k-group we mean an (abstract) group equipped with a continuous left action of Γ_k by group automorphisms.

The proposition tells us that every étale k-group scheme G is a k-form of a constant group scheme. More precisely, consider the (abstract) group $M = G(k_s)$. Then we can form the constant group scheme M_k over k, and the proposition tells us that $G \otimes k_s \cong M_k \otimes k_s$. If G is finite étale over k then we can even find a finite separable field extension $k \subset K$ such that $G_K \cong M_K$. So we can think of étale group schemes as "twisted constant group schemes".

For instance, if $\mathrm{char}(k)$ is prime to n then μ_n is a finite étale group scheme, and $\mu_n(k_s)$ is (non-canonically) isomorphic to $\mathbb{Z}/n\mathbb{Z}$. The action of Γ_k on $\mu_n(k_s)$ is given by a homomorphism $\chi\colon \Gamma_k \to (\mathbb{Z}/n\mathbb{Z})^*$; here the rule is that if $\zeta \in {k_s}^*$ is an n-th root of unity and $\sigma \in \Gamma_k$ then ${}^\sigma\zeta = \zeta^{\chi(\sigma)}$.

Now we turn to the scheme $\varpi_0(X)$ of connected components of X.

(3.27) Proposition. *Let X be a scheme, locally of finite type over a field k. Then there is an étale k-scheme $\varpi_0(X)$ and a morphism $q\colon X \to \varpi_0(X)$ over k such that q is universal for k-morphisms from X to an étale k-scheme. (By this we mean: for any k-morphism $h\colon X \to Y$ with Y/k étale, there is a unique k-morphism $g\colon \varpi_0(X) \to Y$ such that $h = g \circ q$.) The morphism q is faithfully flat, and its fibres are precisely the connected components of X.*

Before we give the proof, let us make the last assertion more precise. If P is a point of $\varpi_0(X)$ then $\{P\}$ is a connected component of $\varpi_0(X)$, as the topological space of an étale scheme is discrete. The claim is then that $q^{-1}(P)$, as an open subscheme of X, is a connected component of X, for all points $P \in \bigl|\varpi_0(X)\bigr|$.

Proof. Consider the set $\pi_0^{\mathrm{geom}}(X) := \pi_0\bigl(|X \otimes_k k_s|\bigr)$ with its natural action of Γ_k. First we show that the action of Γ_k is continuous. Let $\mathscr{C} \subset X_{k_s}$ be a connected component. Let $\mathscr{D} \subset X$ be the connected component containing the image of $\mathscr{C}$ under the natural morphism $X_{k_s} \to X$. Then $\mathscr{C}$ is one of the connected components of $\mathscr{D} \otimes_k k_s$. As $\mathscr{D}$ is locally of finite type over k, there is a point $x \in |\mathscr{D}|$ such that $k(x)$ is a finite extension of k. Let k' be the separable algebraic closure of k inside $k(x)$, and let $k'' \subset k_s$ denote the normal closure of k'. Then by EGA IV, Prop. (4.5.15), all connected components of $\mathscr{D} \otimes_k k''$ are geometrically connected. Hence the stabilizer of $\mathscr{C}$ contains the open subgroup $\mathrm{Gal}(k_s/k'') \subset \Gamma_k$, and is therefore itself open.

Define

$$\varpi_0^{\mathrm{geom}}(X) := \coprod_{\alpha \in \pi_0^{\mathrm{geom}}(X)} \mathrm{Spec}(k_s)^{(\alpha)}\,,$$

the disjoint union of copies of $\mathrm{Spec}(k_s)$, one copy for each element of $\pi_0^{\mathrm{geom}}(X)$. Consider the morphism $q^{\mathrm{geom}}\colon X_{k_s} \to \varpi_0^{\mathrm{geom}}(X)$ that on each connected component $X^{(\alpha)} \subset X_{k_s}$ is given by the structural morphism $X^{(\alpha)} \to \mathrm{Spec}(k_s)^{(\alpha)}$. (So a point $P \in X_{k_s}$ is sent to the copy of $\mathrm{Spec}(k_s)$ labelled by the component of X_{k_s} that contains P.) Because the Γ_k-action on the set $\pi_0^{\mathrm{geom}}(X)$ is continuous, there is an étale k-scheme $\varpi_0(X)$ such that we have an isomorphism $\beta\colon \varpi_0(X)\bigl(k_s\bigr) \xrightarrow{\sim} \pi_0^{\mathrm{geom}}(X)$ of sets with Galois action. Up to isomorphism of k-schemes, this scheme is unique, and we have a unique isomorphism $\varpi_0(X) \otimes_k k_s \xrightarrow{\sim} \varpi_0^{\mathrm{geom}}(X)$ that gives the identity on k_s-valued points. (Here we fix the identification β.) Then q^{geom} can be viewed as a morphism

$$q^{\mathrm{geom}}\colon X \otimes_k k_s \to \varpi_0(X) \otimes_k k_s\,,$$

which is Γ_k-equivariant. By Galois descent this defines a morphism $q\colon X \to \varpi_0(X)$ over k. (See also Exercise (3.9).)

Next we show that the fibres of q are the connected components of X. Over k_s this is clear from the construction. Over k it suffices to show that distinct connected components of X are mapped to distinct points of $\varpi_0(X)$. But the connected components of X correspond to the Γ_k-orbits in $\pi_0^{\mathrm{geom}}(X)$, so the claim follows from the result over k_s.

We claim that the morphism $q\colon X \to \varpi_0(X)$ has the desired universal property. To see this, suppose $h\colon X \to Y$ is a k-morphism with Y/k étale. Then $Y \otimes_k k_s$ is a disjoint union of copies of $\mathrm{Spec}(k_s)$. It readily follows from our construction of $\varpi_0(X)$ and q that there is

a unique morphism $g^{\mathrm{geom}}\colon \varpi_0(X) \otimes_k k_s \to Y \otimes_k k_s$ such that $h^{\mathrm{geom}}\colon X_{k_s} \to Y_{k_s}$ factors as $h^{\mathrm{geom}} = g^{\mathrm{geom}} \circ q^{\mathrm{geom}}$. Moreover, g^{geom} is easily seen to be Galois-equivariant; hence we get the desired morphism $g\colon \varpi_0(X) \to Y$ with $h = g \circ q$.

Finally we have to show that q is faithfully flat. But this can be checked after making a base change to k_s, and over k_s it is clear from the construction. □

(3.28) In the situation of the proposition, we refer to $\varpi_0(X)$ as the scheme of connected components of X. If $f\colon X \to Y$ is a morphism of schemes that are locally of finite type over k then we write $\varpi_0(f)\colon \varpi_0(X) \to \varpi_0(Y)$ for the unique morphism such that $q_Y \circ f = \varpi_0(f) \circ q_X\colon X \to \varpi_0(Y)$.

(3.29) Let G be a k-group scheme, locally of finite type. The connected components of G_{k_s} are geometrically connected; see EGA IV, Prop. (4.5.21). Therefore $\pi_0^{\mathrm{geom}}(G) := \pi_0\big(|G_{k_s}|\big)$ is equal to $\pi_0\big(|G_{\overline{k}}|\big)$. The natural map $q^{\mathrm{geom}}\colon G(\overline{k}) \to \pi_0^{\mathrm{geom}}(G)$ is surjective and has $G^0(\overline{k})$ as its kernel. As $G^0(\overline{k})$ is normal in $G(\overline{k})$, the set $\pi_0^{\mathrm{geom}}(G)$ inherits a group structure such that q^{geom} is a homomorphism. It is clear from the construction that $\mathrm{Aut}(\overline{k}/k)$ acts on $\pi_0^{\mathrm{geom}}(G)$ through group automorphisms. On the other hand, this action factors through $\mathrm{Aut}(\overline{k}/k) \twoheadrightarrow \mathrm{Gal}(k_s/k) =: \Gamma_k$; hence we find that Γ_k acts on $\pi_0^{\mathrm{geom}}(G)$ through group automorphisms.

We can view $\varpi_0^{\mathrm{geom}}(G)$ as the constant group scheme associated to the abstract group $\pi_0^{\mathrm{geom}}(G)$, and because Γ_k acts on $\pi_0^{\mathrm{geom}}(G)$ through group automorphisms, the étale scheme $\varpi_0(G)$ over k inherits the structure of a k-group scheme. It is clear from the constructions that $q^{\mathrm{geom}}\colon G_{k_s} \to \varpi_0^{\mathrm{geom}}(G)$ is a Γ_k-equivariant homomorphism of group schemes. It follows that $q\colon G \to \varpi_0(G)$ is a homomorphism of k-group schemes.

The conclusion of this discussion is that $\varpi_0(G)$ has a natural structure of an étale group scheme over k, and that $q\colon G \to \varpi_0(G)$ is a homomorphism. We refer to $\varpi_0(G)$ as the component group scheme of G.

Another way to show that $\varpi_0(G)$, for G a k-group scheme, inherits the structure of a group scheme is to use the fact that $\varpi_0(G \times_k G) \cong \varpi_0(G) \times_k \varpi_0(G)$; see Exercise 3.10. The group law on $\varpi_0(G)$ is the map

$$\varpi_0(m)\colon \varpi_0(G \times_k G) \cong \varpi_0(G) \times_k \varpi_0(G) \longrightarrow \varpi_0(G)$$

induced by the group law $m\colon G \times_k G \to G$.

Exercises.

(3.1) Show that the following definition is equivalent to the one given in (3.7): If G is a group scheme over a basis S then a subgroup scheme of G is a subscheme $H \subset G$ such that (a) the identity section $e\colon S \to G$ factors through H; (b) if $j\colon H \hookrightarrow G$ is the inclusion morphism then the composition $i \circ j\colon H \hookrightarrow G \to G$ factors through H; (c) the composition $m \circ (j \times j)\colon H \times_S H \to G \times_S G \to G$ factors through H.

(3.2)

(i) Let G be a group scheme over a perfect field k. Prove that the reduced underlying scheme $G_{\mathrm{red}} \hookrightarrow G$ is a closed subgroup scheme. [*Hint:* you will need the fact that $G_{\mathrm{red}} \times_k G_{\mathrm{red}}$ is again a reduced scheme; see EGA IV, § 4.6. This is where we need the assumption that k is perfect.]

(ii) Show, by means of an example, that G_{red} is in general not normal in G.

(iii) Let k be a field of characteristic p. Let $a \in k$, and set $G := \mathrm{Spec}\big(k[x]/(x^{p^2} + ax^p)\big)$. Show that G is a subgroup scheme of $\mathbb{G}_{a,k} = \mathrm{Spec}\big(k[x]\big)$.

(iv) Assume that k is not perfect and that $a \in k \setminus k^p$. Show that $|G|$, the topological space underlying G, consists of p closed points, say $|G| = \{Q_1, Q_2, \ldots, Q_p\}$, where $Q_1 = e$ is the origin. Show that G is reduced at the points Q_i for $i = 2, \ldots, p$ but not geometrically reduced. Finally show that the reduced underlying subscheme $G_{\mathrm{red}} \hookrightarrow G$ is not a subgroup scheme.

(3.3) Prove the relations (1) and (2) in (3.9). Also prove relation (6) in the proof of Theorem (3.20).

(3.4) Let G be a group scheme over a field k. Write $T_{G,e} = \mathrm{Ker}\big(G(k[\varepsilon]) \to G(k)\big)$ for the tangent space of G at the identity element. Show that the map $T_e(m)\colon T_{G,e} \times T_{G,e} \to T_{G,e}$ induced by the group law $m\colon G \times_k G \to G$ on tangent spaces (the "derivative of m at e") is given by $T_e(m)(a, b) = a + b$. Generalize this to group schemes over an arbitrary base.

(3.5) Let k be a field.

(i) If $f\colon G_1 \to G_2$ is a homomorphism of k-group schemes, show that

$$T_{\mathrm{Ker}(f),e} \cong \mathrm{Ker}\big(T_e(f)\colon T_{G_1,e} \to T_{G_2,e}\big)\,.$$

(ii) If $\mathrm{char}(k) = p > 0$, write $G[F] \subset G$ for the kernel of the relative Frobenius homomorphism $F_{G/k}\colon G \to G^{(p)}$. Show that $T_{G[F],e} \cong T_{G,e}$.

(iii) If G is a finite k-group scheme and $\mathrm{char}(k) = p$, show that G is étale over k if and only if $F_{G/k}$ is an isomorphism. [*Hint:* in the "only if" direction, reduce to the case that $k = \overline{k}$.]

(3.6) Let $S = \mathrm{Spec}(R)$ be an affine base scheme. Let $G = \mathrm{Spec}(A)$ be an affine S-group scheme such that A is free of finite rank as an R-module. Choose an R-basis $e_1, \ldots, e_d$ for A, and define elements $a_{ij} \in A$ by $\tilde{m}(e_j) = \sum_{i=1}^{d} e_i \otimes a_{ij}$. Let $R[T_{ij}, U]/(\det \cdot U - 1)$ be the affine algebra of $\mathrm{GL}_{d,R}$, where $\det \in k[T_{ij}]$ is the determinant of the matrix $\big(T_{ij}\big)$. Show that there is a well-defined homomorphism of R-algebras

$$\varphi\colon R[T_{ij}, U]/(\det \cdot U - 1) \longrightarrow A$$

with $T_{ij} \mapsto a_{ij}$. Show that the corresponding morphism $G \to \mathrm{GL}_{d,R}$ is a homomorphism and gives an isomorphism of G with a closed subgroup scheme of $\mathrm{GL}_{d,R}$. [*Hint:* write $M_{d,R}$ for the ring scheme over R of $d \times d$ matrices. First show that we get a morphism $f\colon G \to M_{d,R}$ such that $f(g_1 g_2) = f(g_1) f(g_2)$ for all g_1, $g_2 \in G$. Next show that $f(e_G)$ is the identity matrix, and conclude that f factors through the open subscheme $\mathrm{GL}_{d,R} \subset M_{d,R}$. Finally show that φ is surjective. Use the relations between $\tilde{m}$, $\tilde{e}$ and $\tilde{\imath}$.]

(3.7) Let k be a field of characteristic p. Consider the group variety $G := \mathrm{GL}_{d,k}$. Let $A = \mathrm{Spec}\big(k[T_{ij}, U]/(\det \cdot U - 1)\big)$ be its affine algebra. Recall that we write $[n]_G\colon G \to G$ for the morphism given on points by $g \mapsto g^n$.

(i) Let $I \subset A$ be the augmentation ideal. Let $[p]\colon A \to A$ be the homomorphism of k-algebras corresponding to $[p]_G$. Show that $[p](I) \subseteq I^p$.

(ii) Let $H = \mathrm{Spec}(B)$ be a finite k-group scheme. Let $J \subset B$ be the augmentation ideal. Show that $[p](J) \subseteq J^p$. [*Hint:* use the previous exercise.] For an application of this result, see Exercise (4.4).

(3.8) Let $\pi\colon G \to S$ be an affine S-group scheme. Set $A := \pi_* O_G$, so that $G \cong \mathrm{Spec}(A)$ as an S-scheme. Let $A^D := \mathit{Hom}_{O_S}(A, O_S)$. Show that with the definitions given in (3.21), A^D is a sheaf of co-commutative O_S-Hopf algebras.

(3.9) Let k be a field, $k \subset k_s$ a separable algebraic closure, and write $\Gamma := \mathrm{Gal}(k_s/k)$. Let X be a scheme, locally of finite type over k, and let Y be an étale k-scheme. Note that Γ naturally acts on the schemes X_{k_s} and Y_{k_s}. If $\varphi\colon X_{k_s} \to Y_{k_s}$ is a Γ-equivariant morphism of schemes over k_s, show that φ is defined over k, i.e., there is a (unique) morphism $f\colon X \to Y$ over k such that $f_{k_s} = \varphi$. [*Hint:* First reduce to the case that X is affine and that X and Y are connected. Then work on rings.]

(3.10) Let X and Y be two schemes that are locally of finite type over a field k. Let $q_X\colon X \to \varpi_0(X)$ and $q_Y\colon Y \to \varpi_0(Y)$ be the morphisms as in Prop. (3.27). By the universal property of $\varpi_0(X \times_k Y)$, there is a unique morphism

$$\rho\colon \varpi_0(X \times_k Y) \to \varpi_0(X) \times_k \varpi_0(Y)$$

such that $\rho \circ q_{(X\times Y)} = (q_X \circ \mathrm{pr}_X, q_Y \circ \mathrm{pr}_Y)$. Show that ρ is an isomorphism. In particular, conclude that if $k \subset K$ is a field extension then $\varpi_0(X_K)$ is naturally isomorphic to $\varpi_0(X)_K$. [*Hint:* Reduce to the case $k = k_s$. Use that if C and D are connected schemes over k_s then $C \times_{k_s} D$ is again connected. See EGA IV, Cor. (4.5.8), taking into account loc. cit., Prop. (4.5.21).]

Notes. Proposition (3.17) is taken from SGA 3, Exp. $\mathrm{VI_A}$. The example following Proposition (3.12) is taken from ibid., Exp. $\mathrm{VI_B}$, §5. A different proof of Prop. (3.27) can be found in the book of Demazure and Gabriel [1].