1
Finite Group Schemes

Michel Brion

Abstract

These extended notes give an introduction to the theory of finite group schemes over an algebraically closed field, with minimal prerequisites. They conclude with a brief survey of the inverse Galois problem for automorphism group schemes.

1.1 Introduction

Finite group schemes are broad generalizations of finite groups; they occur in algebraic geometry, number theory, and the structure and representations of algebraic groups in positive characteristics. Unlike finite groups which exist on their own, finite group schemes depend on an additional data: a base, for example a commutative ring.

This text is an introduction to finite group schemes over an algebraically closed field. In characteristic 0, these may be identified with finite groups, as follows from Cartier's theorem (see Theorem 1.4.13 for a direct proof). But these form a much wider class in characteristic $p > 0$, as it includes the finite-dimensional restricted Lie algebras (also called p-Lie algebras). In fact, such Lie algebras form the building blocks of finite group schemes, together with finite groups; see Corollary 1.5.14 for a precise statement.

Many notions and results of group theory extend to the setting of finite group schemes, sometimes with more involved proofs; for example, Lagrange's theorem, which requires substantial developments on quotients (see Corollary 1.5.13). Still, the topic leaves much room for developments, e.g., the notion of conjugacy class is unsettled (several approaches are discussed in the appendix of the recent preprint [16]).

The theory of finite group schemes over a field k is often presented as part of that of algebraic groups (in the sense of group schemes of finite type), see [6, 32, 24]. This yields a broader view of the topic and many natural examples, but also requires quite a few results from commutative algebra and algebraic geometry.

This text aims at presenting some fundamental structure results for finite group schemes, with minimal prerequisites: basic notions of algebra and familiarity with linear algebra. For this, we deal mainly with finite schemes (rather than algebraic schemes). These can be viewed in three ways:

- algebraically, via finite-dimensional algebras (i.e., k-algebras of finite dimension as k-vector spaces),
- geometrically, via finite sets equipped with a finite-dimensional local algebra at each point,
- functorially, via points with values in finite-dimensional algebras.

We will start with the first viewpoint, where finite group schemes are identified with finite-dimensional Hopf algebras, and mainly work with the second and third ones.

The structure of this text is as follows. Section 1.2 begins with three motivating examples which will be reconsidered at later stages. We then describe a classical correspondence between finite sets and their rings of k-valued functions, where k is an algebraically closed field. These rings are exactly the reduced finite-dimensional (commutative, associative) k-algebras. Next, we define finite schemes via finite-dimensional algebras, and obtain structure results for these; in particular, Theorem 1.2.13. We then turn to the functor of points, which yields simple formulations of basic operations such as the sum and product of finite schemes. This section ends with a brief overview of notions and results on more general schemes.

In Section 1.3, we introduce finite group schemes, and generalize basic notions of group theory to this setting: (normal) subgroups, group actions, semi-direct products. Then we define infinitesimal group schemes (also known as connected, or local), and obtain a first structure result: every finite group scheme is the semi-direct product of an infinitesimal group scheme and a finite group (Theorem 1.3.13).

Section 1.4 develops Lie algebra methods for studying infinitesimal group schemes; these present some analogies with connected Lie groups.

We begin with the Lie algebra of derivations of an algebra; in characteristic $p > 0$, this is a restricted Lie algebra via the pth power of derivations. We then give overviews of restricted Lie algebras, and infinitesimal calculus on affine schemes. Next, we introduce the Lie algebra of an affine group scheme, and use it to show that finite group schemes are reduced in characteristic 0 (Theorem 1.4.13). Returning to positive characteristics, we define Frobenius kernels, present a structure result for these (Theorem 1.4.23), and some applications, e.g. to finite group schemes of prime order.

Section 1.5 deals with quotients of affine schemes by actions of finite group schemes. The intuitive notion of quotient as an orbit space does not extend readily to this setting, e.g. for infinitesimal group schemes as they have a unique k-point. A substitute is the categorical quotient, for which we obtain a key finiteness property (Theorem 1.5.4). Next, we discuss quotients by free actions and applications to the structure of finite group schemes (Corollaries 1.5.13 and 1.5.14).

The final Section 1.6 is a brief survey of some recent developments on automorphism group schemes in projective algebraic geometry. It focuses on a version of the inverse Galois problem in this setting, which asks whether a given group scheme can be realized as the full automorphism group scheme of a projective variety. The answer is positive for finite groups by a classical result (see [13, 19, 18]), but negative for many abelian varieties as recently shown in [17, 1] (see Theorem 1.6.7 for a precise statement). Also, the answer is positive in the setting of connected algebraic groups (in particular, infinitesimal group schemes) and connected automorphism group schemes; see Theorem 1.6.5, based on [4].

The exposition is essentially self-contained in Sections 1.2 and 1.3, which consider almost exclusively finite (group) schemes. Sections 1.4 and 1.5 also deal with affine (group) schemes, and rely on a few results for which we could find no direct proof; most notably, basic properties of quotients by free actions (Theorem 1.5.12). In these sections, we also use some fundamental results of commutative algebra, for which an excellent reference is [10]. Section 1.6 is more advanced, and involves notions and results of algebraic geometry which can be found in [14].

This text presents only the first steps in the theory of finite group schemes. Here are some suggestions for further reading: [25, Chap. III] for more on this topic, [37] for affine group schemes, [24] for algebraic groups (both over an arbitrary field), [28] for finite commutative group schemes over a perfect field, and [34] over an arbitrary base.

Notation and conventions. We fix an algebraically closed field k of characteristic $p \geq 0$. By an **algebra**, we mean a commutative associative k-algebra A with identity element, unless otherwise mentioned. The **dimension** of A is its dimension as a k-vector space. Given $a_1, \ldots, a_m \in A$, we denote by $(a_1, \ldots, a_m)$ the ideal of A that they generate. The polynomial algebra in n indeterminates over k is denoted by $k[T_1, \ldots, T_n]$.

1.2 Finite schemes

1.2.1 Motivating examples

Example 1.2.1. Let n be a positive integer and consider the nth power map

$$k^* \longrightarrow k^*, \quad x \longmapsto x^n.$$

This is a group homomorphism with kernel the group $\mu_n(k)$ of nth roots of unity in k. If $p = 0$ or n is prime to p, then $\mu_n(k)$ is a cyclic group of order n. Also, if $p > 0$ then $\mu_p(k)$ is trivial, since $x^p - 1 = (x-1)^p$. This still holds when k is replaced with any field extension. But if k is replaced with an algebra R having nonzero nilpotent elements, then the group of pth roots of unity $\mu_p(R)$ is nontrivial.

For any algebra R, we may view $\mu_p(R)$ as the set of algebra homomorphisms $f : A \to R$, where $A = k[T]/(T^p - 1)$. Indeed, such a homomorphism f is uniquely determined by $f(t)$, where t denotes the image of T in A.

More generally, we have for any n and any algebra R

$$\mu_n(R) = \mathrm{Hom}_{\mathrm{alg}}(k[T]/(T^n - 1), R),$$

where the right-hand side denotes the set of algebra homomorphisms. This suggests a way to encode the nth roots of unity by the algebra $k[T]/(T^n - 1)$, of dimension n (regardless of the characteristic).

Example 1.2.2. Assume that $p > 0$ and consider the pth power map, also called the Frobenius map

$$F : k \longrightarrow k, \quad x \longmapsto x^p.$$

This is a ring homomorphism with trivial kernel. But again, if k is replaced with an algebra R having nonzero nilpotents, then the pth power map has a nontrivial kernel,

$$\alpha_p(R) = \{x \in R \mid x^p = 0\} = \mathrm{Hom}_{\mathrm{alg}}(k[T]/(T^p), R).$$

This kernel is encoded by the p-dimensional algebra $k[T]/(T^p)$, equipped with additional structures which will be introduced in §1.3.1.

In the next, more advanced example, we will freely use some results on elliptic curves which can be found in [31].

Example 1.2.3. Let E be an elliptic curve with origin 0. Then E is a commutative group with neutral element 0. Thus, for any positive integer n, we have the multiplication map

$$n_E : E \longrightarrow E, \quad x \longmapsto nx.$$

If $k = \mathbb{C}$ then $E \simeq \mathbb{C}/\Lambda$ as a group, where Λ is a lattice in $\mathbb{C}$; as a consequence, $\Lambda \simeq \mathbb{Z}^2$ as a group. Thus, the kernel of n_E (the n-torsion subgroup of E) satisfies

$$\operatorname{Ker}(n_E) \simeq \left(\frac{1}{n}\Lambda\right)/\Lambda \simeq \Lambda/n\Lambda \simeq (\mathbb{Z}/n\mathbb{Z})^2.$$

In particular, $\operatorname{Ker}(n_E)$ has order n^2.

This still holds over an arbitrary (algebraically closed) field k of characteristic p, if $p = 0$ or if n is prime to p. Also, the endomorphism n_E of E has degree n^2 for any $n > 0$. But the structure of its kernel depends on the curve E if $p > 0$ divides n. For instance, $\operatorname{Ker}(p_E)$ has order p if E is ordinary, and is trivial if E is supersingular. The supersingular elliptic curves form only finitely many isomorphism classes.

To get a more uniform description of n-torsion subgroups, one considers the schematic kernel $E[n]$. This is a finite group scheme of order n^2 regardless of the characteristic, as we will see in Remark 1.5.11.

1.2.2 Algebras of functions on finite sets

Given a finite set E, we denote by $\mathcal{O}(E)$ the set of maps $f : E \to k$. Then $\mathcal{O}(E)$ is an algebra for the operations of pointwise addition and multiplication; we have an isomorphism of algebras $\mathcal{O}(E) \simeq k^n$, where $n = |E|$. We will investigate the assignment $E \mapsto \mathcal{O}(E)$ in a series of observations and lemmas.

For any $x \in E$, we denote by

$$\operatorname{ev}_x : \mathcal{O}(E) \longrightarrow k, \quad f \longmapsto f(x)$$

the evaluation at x. Then ev_x is an algebra homomorphism, and hence its kernel $\mathfrak{m}_x$ is a maximal ideal of $\mathcal{O}(E)$. Also, we define $\delta_x \in \mathcal{O}(E)$ by

$$\delta_x(y) = \begin{cases} 1 & \text{if } y = x \\ 0 & \text{otherwise.} \end{cases}$$

Then $(\delta_x)_{x \in E}$ is a basis of the k-vector space $\mathcal{O}(E)$, which satisfies

$$\delta_x^2 = \delta_x \quad (x \in E), \qquad \delta_x \delta_y = 0 \quad (x, y \in E, y \neq x), \qquad \sum_{x \in E} \delta_x = 1.$$

The idempotents of the ring $\mathcal{O}(E)$ (i.e. those $f \in \mathcal{O}(E)$ such that $f^2 = f$) are exactly the partial sums $\delta_F = \sum_{x \in F} \delta_x$, where $F \subset E$.

Lemma 1.2.4. *Every algebra homomorphism $u : \mathcal{O}(E) \to k$ is of the form ev_x for a unique $x \in E$.*

Proof Since $\sum_{x \in E} \delta_x = 1$, there exists $x \in E$ such that $u(\delta_x) \neq 0$. Then $u(\delta_x) = 1$ as $\delta_x^2 = \delta_x$. Let $y \in E \setminus \{x\}$, then $\delta_x \delta_y = 0$ and hence $u(\delta_y) = 0$. Thus, $u = \mathrm{ev}_x$. □

Next, consider another finite set F. Then every map $\varphi : E \to F$ yields a map

$$\varphi^* : \mathcal{O}(F) \longrightarrow \mathcal{O}(E), \quad g \longmapsto g \circ \varphi$$

which is clearly an algebra homomorphism.

Lemma 1.2.5. *Every algebra homomorphism $u : \mathcal{O}(F) \to \mathcal{O}(E)$ is of the form φ^* for a unique $\varphi : E \to F$.*

Proof Let $x \in E$, then the composition $\mathrm{ev}_x \circ u : \mathcal{O}(F) \to k$ is an algebra homomorphism. By Lemma 1.2.4, there exists a unique $y \in F$ such that $\mathrm{ev}_x \circ u = \mathrm{ev}_y$, that is, $u(g)(x) = g(y)$ for all $g \in \mathcal{O}(F)$. So the statement holds for the map $\varphi : E \to F$, $x \mapsto y$ and for no other map. □

We now consider the product $E \times F$ with projections $\mathrm{pr}_E : E \times F \to E$, $\mathrm{pr}_F : E \times F \to F$. Then one may readily check that the map

$$\mathrm{pr}_E^* \otimes \mathrm{pr}_F^* : \mathcal{O}(E) \otimes \mathcal{O}(F) \longrightarrow \mathcal{O}(E \times F), \delta_x \otimes \delta_y \longmapsto \delta_{(x,y)} \tag{1.1}$$

is an isomorphism of algebras. Likewise, consider the sum $E \sqcup F$ with inclusion maps $i_E : E \to E \sqcup F$, $i_F : F \to E \sqcup F$, then the map

$$(i_E^*, i_F^*) : \mathcal{O}(E \sqcup F) \longrightarrow \mathcal{O}(E) \times \mathcal{O}(F) \tag{1.2}$$

is an isomorphism of algebras.

Remark 1.2.6. Let A be an algebra, and $f : A \to k$ an algebra homomorphism. Then the kernel $\mathfrak{m}$ of f is a maximal ideal, and $A = k \oplus \mathfrak{m}$ where k is the line spanned by the identity element; this identifies f with the projection $A \to k$. In particular, f is uniquely determined by $\mathfrak{m}$.

If A is finite-dimensional (as a k-vector space), then every maximal ideal $\mathfrak{m}$ is the kernel of a unique algebra homomorphism to k. Indeed, the quotient $A/\mathfrak{m}$ is a field extension of k of finite degree, and hence equals k as the latter is algebraically closed. This yields a bijection between algebra homomorphisms from A to k and maximal ideals of A.

Clearly, every algebra $\mathcal{O}(E)$ is **reduced**, i.e., it has no nonzero nilpotent element. We will now obtain a converse:

Lemma 1.2.7. *Let A be a reduced finite-dimensional algebra, and denote by E the set of algebra homomorphisms $f : A \to k$.*

(i). *The set E is finite and the assignment*

$$A \longrightarrow \mathcal{O}(E), \quad a \longmapsto (f \mapsto f(a)) \tag{1.3}$$

is an isomorphism of algebras.

(ii). *Every quotient algebra of A is reduced.*

Proof (i) In view of Lemma 1.2.5, it suffices to show that there exists an algebra isomorphism $A \simeq \mathcal{O}(F)$ for some finite set F.

Assume that there exist nonzero ideals B, C of A such that $A = B \oplus C$. Let $1 = e + f$ be the corresponding decomposition of the identity element of A; then we easily obtain $e^2 = e$, $f^2 = f$ and $ef = 0$, and hence B (resp. C) is a subalgebra of A with identity element e (resp. f). Since A is reduced, so are B and C. Using the isomorphism (1.2) and induction on the dimension of A, we may thus assume that A admits no such decomposition.

Let $a \in A \setminus \{0\}$ and consider the multiplication map

$$a_A : A \longrightarrow A, \quad b \longmapsto ab \tag{1.4}$$

(so that the assignment $a \mapsto a_A$ is the regular representation of A). Then a_A is an endomorphism of the finite-dimensional vector space A, and hence satisfies

$$A = \operatorname{Ker}(a_A^n) \oplus \operatorname{Im}(a_A^n) \qquad (n \gg 0). \tag{1.5}$$

Moreover, $\operatorname{Ker}(a_A^n)$ and $\operatorname{Im}(a_A^n)$ are ideals of A, and $\operatorname{Im}(a_A^n) \neq 0$ as A is reduced. By our assumption, it follows that $A = \operatorname{Im}(a_A^n)$ for $n \gg 0$.

In particular, a_A is injective, and hence a is invertible. So A is a field; arguing as in Remark 1.2.6, it follows that $A = k$.

(ii) Let I be an ideal of $\mathcal{O}(E)$. Since $\sum_{x \in E} \delta_x = 1$, we have $I = \sum_{x \in E} I\delta_x$, where $I\delta_x \subset \mathcal{O}(E)\delta_x = k\delta_x$. As a consequence, $I = \oplus_{x \in F} k\delta_x$ for a unique subset $F \subset E$. Then $\mathcal{O}(E)/I \simeq \mathcal{O}(E \setminus F)$ is indeed reduced. □

Combining Lemmas 1.2.4, 1.2.5 and 1.2.7, we obtain:

Proposition 1.2.8. *The assignment $E \mapsto \mathcal{O}(E)$ yields a bijective correspondence from finite sets (and maps between such sets) to reduced finite-dimensional algebras (and homomorphisms between such algebras).*

The inverse correspondence is denoted by $A \mapsto \mathrm{Spec}(A)$ (the **spectrum** of the algebra A).

For any maps of finite sets $E \xrightarrow{\varphi} F \xrightarrow{\psi} G$, we have $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$. Thus, the category of finite sets is equivalent to the opposite of the category of reduced finite-dimensional algebras.

1.2.3 Finite schemes and finite-dimensional algebras

Definition 1.2.9. The **category of finite schemes** is the opposite category to that of finite-dimensional algebras.

In more concrete terms, finite schemes are finite-dimensional algebras, with morphisms going the other way round.

A basic example of a nonreduced algebra is the **algebra of dual numbers** $k[T]/(T^2) = k[\varepsilon] = k \oplus k\varepsilon$, where $\varepsilon^2 = 0$.

Remark 1.2.10. With the above definition, some properties of finite schemes follow readily from the dual properties of algebras. For example, any two finite schemes X, Y admit a **product**, i.e., a finite scheme Z equipped with morphisms $\mathrm{pr}_X : Z \to X$, $\mathrm{pr}_Y : Z \to Y$ (the projections) which satisfy the following universal property: for any finite scheme W equipped with morphisms $f : W \to X$, $g : W \to Y$, there exists a unique morphism $h : W \to Z$ such that $f = \mathrm{pr}_X \circ h$ and $g = \mathrm{pr}_Y \circ h$.

Indeed, any two algebras A and B admit a "coproduct", namely, the tensor product $A \otimes B$ equipped with the homomorphisms $A \to A \otimes B$, $a \mapsto a \otimes 1_A$ and $B \to A \otimes B$, $b \mapsto 1_A \otimes b$.

In view of the universal property, the above scheme Z is unique up to isomorphism; we will use the standard notation $Z = X \times Y$.

We will obtain a structure result for finite-dimensional algebras (Theorem 1.2.13). For this, we recall some notions from commutative algebra.

Let R be a commutative ring. The set of nilpotent elements of R is an ideal, called the **nilradical**; we denote it by $\mathfrak{n} = \mathfrak{n}(R)$. The quotient ring $A/\mathfrak{n} = A_{\mathrm{red}}$ is reduced, and $\mathfrak{n}$ is the smallest ideal with this property. Clearly, $\mathfrak{n} \subset \mathfrak{m}$ for any maximal ideal $\mathfrak{m}$ of R.

The ring R is **indecomposable** if it has no nontrivial decomposition into a direct product of rings. Equivalently, R has no idempotent $e \neq 0, 1$ (this notion appeared implicitly in the proof of Lemma 1.2.7).

Also, R is **local** if it has a unique maximal ideal $\mathfrak{m}$. Equivalently, $\mathfrak{m}$ is an ideal of R and every $x \in R \setminus \mathfrak{m}$ is invertible. The quotient ring $R/\mathfrak{m}$ is then a field, called the **residue field** of R.

We now record two auxiliary results:

Lemma 1.2.11. *Let A be a finite-dimensional algebra. Then A is indecomposable if and only if it is local. Under this assumption, the maximal ideal $\mathfrak{m}$ is the nilradical of A, with residue field k. Moreover, we have $\mathfrak{m}^n = 0$ for $n \gg 0$.*

Proof Assume that A is local with maximal ideal $\mathfrak{m}$. If $e \in A$ is indecomposable, then $e(1-e) = 0$. Thus, we have either $e \in \mathfrak{m}$ or $1 - e \in \mathfrak{m}$. In the former case, $1 - e$ is invertible, hence $e = 0$. In the latter case, we obtain similarly $e = 1$. Thus A is indecomposable.

Conversely, assume that A is indecomposable. To show that A is local, we argue as in the proof of Lemma 1.2.7. Let $a \in A$, then for $n \gg 0$, we have $\mathrm{Ker}(a_A^n) = 0$ or $\mathrm{Im}(a_A^n) = 0$ in view of the decomposition (1.5). Thus, a is nilpotent or invertible. As a consequence, A is local and its maximal ideal $\mathfrak{m}$ is the nilradical. We have $A/\mathfrak{m} = k$ by Remark 1.2.6.

It remains to show that $\mathfrak{m}^n = 0$ for $n \gg 0$. Since the powers $\mathfrak{m}^n$ form a decreasing sequence of subspaces of A, we have $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ for $n \gg 0$. This yields a finite-dimensional vector space $V = \mathfrak{m}^n$ equipped with commuting nilpotent endomorphisms $u_1, \ldots, u_N$ (the multiplication maps by elements of a basis of $\mathfrak{m}$) such that $V = u_1(V) + \cdots + u_N(V)$. So the dual vector space V^* comes with commuting nilpotent endomorphisms, the transposes $u_1^T, \cdots, u_N^T$. If $V \neq 0$ then these endomorphisms have a common nonzero kernel, i.e., there exists a nonzero $f \in V^*$ such that $f \circ u_i = 0$ for $i = 1, \ldots, n$. But then $f(V) = 0$, a contradiction. □

Lemma 1.2.12. *Let A be a local finite-dimensional algebra, $\mathfrak{m}$ its maximal ideal, and $a_1, \ldots, a_m \in \mathfrak{m}$. Then the following conditions are equivalent:*

(i). *The algebra A is generated by $a_1, \ldots, a_m$.*
(ii). *The ideal $\mathfrak{m}$ is generated by $a_1, \ldots, a_m$.*
(iii). *The vector space $\mathfrak{m}/\mathfrak{m}^2$ is generated by the images of $a_1, \ldots, a_m$.*

Proof (i)⇒(ii) Let $a \in \mathfrak{m}$. There exists $P \in k[T_1, \ldots, T_m]$ such that $a = P(a_1, \ldots, a_m)$. Then the constant term of P must be 0, and hence $a \in (a_1, \ldots, a_m)$.

Since the implication (ii)⇒(iii) is obvious, it remains to prove that (iii)⇒(i). For this, we use the decreasing filtration of A by the powers $\mathfrak{m}^n$, where $n \geq 0$, and the associated graded $\mathrm{gr}(A) = \bigoplus_{n \geq 0} \mathfrak{m}^n/\mathfrak{m}^{n+1}$. Then $\mathrm{gr}(A)$ is a graded algebra generated by $\mathfrak{m}/\mathfrak{m}^2$, and hence by the images $\bar{a}_1, \ldots, \bar{a}_m$ of $a_1, \ldots, a_m$. Given a nonzero $a \in A$, there exists a unique integer $n \geq 0$ such that $a \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1}$ (since $\mathfrak{m}^r = 0$ for $r \gg 0$). Then there exists a polynomial P as above such that $\bar{a} = P(\bar{a}_1, \ldots, \bar{a}_m)$, where $\bar{a}$ denotes the image of a in $\mathfrak{m}^n/\mathfrak{m}^{n+1}$, and $\bar{a}_i$, the image of a_i in $\mathfrak{m}/\mathfrak{m}^2$ for $i = 1, \ldots, m$. This means that $a - P(a_1, \ldots, a_m) \in \mathfrak{m}^{n+1}$. We now conclude by decreasing induction on n, using again the vanishing of $\mathfrak{m}^n$ for $n \gg 0$. □

Theorem 1.2.13. *Let A be a finite-dimensional algebra, and denote by E the (finite) set of algebra homomorphisms $f : A \to k$.*

(i). *The assignment $A \to \mathcal{O}(E)$, $a \mapsto (f \mapsto f(a))$ (1.3) induces an isomorphism of algebras $A_{\mathrm{red}} \xrightarrow{\sim} \mathcal{O}(E)$.*
(ii). *For any $x \in E$, the idempotent $\delta_x \in \mathcal{O}(E)$ lifts to a unique idempotent $e_x \in A$. Moreover, $e_x e_y = 0$ for all distinct $x, y \in E$, and $\sum_{x \in E} e_x = 1$. The idempotents of A are exactly the partial sums $\sum_{x \in F} e_x$, where $F \subset E$.*
(iii). *We have $A = \prod_{x \in E} Ae_x$ and each Ae_x is a local algebra.*

Proof (i) Let $\pi : A \to A_{\mathrm{red}} = A/\mathfrak{n}$ denote the projection. Since every homomorphism of algebras $f : A \to k$ sends $\mathfrak{n}$ to 0, the composition with π yields a bijection from $\mathrm{Hom}_{\mathrm{alg}}(A_{\mathrm{red}}, k)$ to $\mathrm{Hom}_{\mathrm{alg}}(A, k)$. So the assertion follows from Lemma 1.2.7.

We now show (ii) and (iii) simultaneously. Since the algebra A is finite-dimensional, it admits a decomposition $A = A_1 \times \cdots \times A_n$ where each A_i is indecomposable, and hence local (Lemma 1.2.11). Thus, $A_i = ke_i \oplus \mathfrak{m}_i$, where e_i is the identity element of A_i, and $\mathfrak{m}_i$ the nilradical. So $\mathfrak{m}_1 \times \cdots \times \mathfrak{m}_n$ is an ideal of A contained in $\mathfrak{n}$, and the quotient $A/\mathfrak{m}_1 \times \cdots \times \mathfrak{m}_n \simeq k^n$ is reduced. It follows that $\mathfrak{m}_1 \times \cdots \times \mathfrak{m}_n = \mathfrak{n}$; moreover, we may identify E with $\{1, \ldots, n\}$. Via this identification, each $\delta_i \in \mathcal{O}(E)$ lifts to the idempotent e_i of A. Moreover, $e_i e_j = 0$ for all distinct i, j, and $\sum_{i=1}^n e_i = 1$.

Next, we show that every idempotent $e \in A$ can be written as $\sum_{i \in F} e_i$ for some $F \subset \{1, \ldots, n\}$. We have $e = (t_1 e_1 + x_1, \ldots, t_n e_n + x_n)$ where $t_i \in k$ and $x_i \in \mathfrak{m}_i$ for $i = 1, \ldots, n$. Since $e^2 = e$, we obtain $t_i^2 + 2t_i x_i = t_i$ and $x_i^2 = x_i$. Thus, $x_i = 0$ as x_i is nilpotent. This implies the assertion.

This assertion implies in turn that each e_i is the unique lift of δ_i, completing the proof. □

In view of Theorem 1.2.13, we may reformulate the definition of finite schemes in more geometric terms:

Definition 1.2.14. A finite scheme X consists of a finite set E together with local finite-dimensional algebras $\mathcal{O}_{X,x}$ for each $x \in E$. We then say that $\mathcal{O}_{X,x}$ is the **local ring of** X **at** x.

With this definition, the algebra associated with X is

$$A = \mathcal{O}(X) = \prod_{x \in E} \mathcal{O}_{X,x}$$

and we still write $X = \mathrm{Spec}(A)$. We say that X is **local** if A is local.

Given another finite scheme Y with data $(F, (\mathcal{O}_{Y,y})_{y \in F})$, a morphism of finite schemes $f : X \to Y$ consists of a map $\varphi : E \to F$ together with algebra homomorphisms $\mathcal{O}_{Y,\varphi(x)} \to \mathcal{O}_{X,x}$ for all $x \in E$ (as follows by considering the dual homomorphism $f^* : \mathcal{O}(Y) \to \mathcal{O}(X)$ and using Theorem 1.2.13).

Remark 1.2.15. A basic invariant of a local scheme X is the dimension of $\mathcal{O}(X)$, also known as the **length** of X. There is a unique local algebra of dimension 1 (resp. 2) up to isomorphism, namely, k (resp. $k[\varepsilon]$). But this fails in dimension 3, since $k[T]/(T^3)$ and $k[T_1, T_2]/(T_1^2, T_1 T_2, T_2^2)$ are nonisomorphic (as follows e.g. from Lemma 1.2.12). In higher dimensions, there may be infinitely many nonisomorphic local algebras, for example

$$k[T_1, T_2]/(P, T_1^n, T_1^{n-1} T_2, \ldots, T_1 T_2^{n-1}, T_2^n),$$

where P is a homogeneous polynomial of degree $n-1$ in T_1, T_2, and $n \geq 5$ (exercise).

Definition 1.2.16. Let X, Y be finite schemes. We say that Y is a **subscheme** of X if the algebra $\mathcal{O}(Y)$ is a quotient of $\mathcal{O}(X)$. Then the morphism $i : Y \to X$ corresponding to the projection $\mathcal{O}(X) \to \mathcal{O}(Y)$ is called an **immersion**.

With the above notation, this is equivalent to F being a subset of E, and $\mathcal{O}_{Y,y}$ being a quotient of $\mathcal{O}_{X,i(y)}$ for any $y \in F$. Also, note that the subschemes of X correspond bijectively to the ideals of $\mathcal{O}(X)$, by assigning to Y the kernel of the projection $\mathcal{O}(X) \to \mathcal{O}(Y)$.

Definition 1.2.17. Let $X_1, \ldots, X_n$ be finite schemes, and $A_1, \ldots, A_n$ the corresponding algebras. The **sum** $X = X_1 \sqcup \cdots \sqcup X_n$ is the finite scheme $\operatorname{Spec}(A_1 \times \cdots \times A_n)$.

With an obvious notation, we then have $E = E_1 \sqcup \cdots \sqcup E_n$ and $\mathcal{O}_{X,x} = \mathcal{O}_{X_i,x}$ for all $x \in X_i$ $(i = 1, \ldots, n)$. The projections $A_1 \times \cdots \times A_n \to A_i$ correspond to immersions $X_i \to X$. Also, Theorem 1.2.13 may be reformulated as follows: every finite scheme has a unique decomposition into a sum of local finite schemes.

1.2.4 The reduced subscheme

We first obtain a useful addition to the structure theorem for finite-dimensional algebras (Theorem 1.2.13):

Proposition 1.2.18.(i). *Every finite-dimensional algebra A admits a largest reduced subalgebra A^{red}. Moreover, the composition $A^{\mathrm{red}} \to A \to A/\mathfrak{n} = A_{\mathrm{red}}$ is an isomorphism.*

(ii). *Every homomorphism of finite-dimensional algebras $f : A \to B$ induces homomorphisms $f_{\mathrm{red}} : A_{\mathrm{red}} \to B_{\mathrm{red}}$, $f^{\mathrm{red}} : A^{\mathrm{red}} \to B^{\mathrm{red}}$ such that the diagram*

$$\begin{tikzcd}
A^{\mathrm{red}} \arrow[r, "f^{\mathrm{red}}"] \arrow[d] & B^{\mathrm{red}} \arrow[d] \\
A \arrow[r, "f"] \arrow[d] & B \arrow[d] \\
A_{\mathrm{red}} \arrow[r, "f_{\mathrm{red}}"] & B_{\mathrm{red}}
\end{tikzcd}$$

commutes.

(iii). *For any finite-dimensional algebras A, B, we have natural isomorphisms of algebras*

$$A^{\mathrm{red}} \otimes B^{\mathrm{red}} \xrightarrow{\sim} (A \otimes B)^{\mathrm{red}}, \quad A_{\mathrm{red}} \otimes B_{\mathrm{red}} \xrightarrow{\sim} (A \otimes B)_{\mathrm{red}}.$$

Proof (i) With the notation of Theorem 1.2.13, the subalgebra $B = \prod_{x \in E} k e_x$ is reduced, the composition $B \to A \to A_{\mathrm{red}}$ is an isomorphism, and B contains every idempotent of A. It follows that B contains every reduced subalgebra C of A, since C is spanned by its idempotents in view of Lemma 1.2.7. This yields the assertion.

(ii) The commutativity of the top square follows from the fact that every quotient of a reduced algebra is reduced (Lemma 1.2.7 again). The commutativity of the bottom square is readily checked from the definitions.

(iii) By Lemma 1.2.7 once more and the isomorphism (1.1) (or a direct argument), the tensor product of any two reduced finite-dimensional algebras is reduced. This easily implies the assertion. □

Definition 1.2.19. A finite scheme X is **reduced** if the algebra $\mathcal{O}(X)$ is reduced.

In view of Proposition 1.2.8, the category of reduced finite schemes is equivalent to that of finite sets via the assignments $X \mapsto X(k)$ and $E \mapsto \mathcal{O}(E)$. Moreover, Proposition 1.2.18 translates as follows in the language of schemes:

Corollary 1.2.20. *Every finite scheme X has a largest reduced subscheme X_{red}. Moreover, there exists a unique morphism $r : X \to X_{\mathrm{red}}$ such that $r \circ i = \mathrm{id}_{X_{\mathrm{red}}}$, where i denotes the immersion $X_{\mathrm{red}} \to X$. The formations of X_{red} and r are functorial and commute with products.*

1.2.5 The functor of points

Definition 1.2.21. Let $X = \mathrm{Spec}(A)$ be a finite scheme, and R a finite-dimensional algebra. An R-**valued point** of X is a homomorphism of algebras $u : A \to R$. The set of R-valued points of X is denoted by $X(R) = \mathrm{Hom}_{\mathrm{alg}}(\mathcal{O}(X), R) = \mathrm{Hom}(\mathrm{Spec}(R), X)$.

With the above notation, $X(k)$ is the finite set E of Definition 1.2.14; its points are also known as the k-**points** or k-**rational points** of X. Also, every morphism of finite schemes $f : X \to Y$ induces a map $f(R) : X(R) \to Y(R)$ given by precomposition with the dual homomorphism $f^* : \mathcal{O}(Y) \to \mathcal{O}(X)$. The map $f(k) : X(k) \to Y(k)$ is the map $\varphi : E \to F$ of the above definition.

Note that $\mathrm{Spec}(k)(R) = \mathrm{Hom}_{\mathrm{alg}}(k, R)$ is a unique point for any k-algebra R. As a consequence, for any $x \in X(k)$ viewed as a morphism $x : \mathrm{Spec}(k) \to X$, we obtain a point $x(R) \in X(R)$.

Every algebra homomorphism $u : R \to S$ induces a map $X(u) : X(R) \to X(S)$ via postcomposition. Moreover, $X(\mathrm{id}_R) = \mathrm{id}_{X(R)}$ and

$X(v \circ u) = X(v) \circ X(u)$ for any algebra homomorphisms $R \xrightarrow{u} S \xrightarrow{v} T$. This yields a functor from the category of finite-dimensional algebras to that of sets: the **functor of points** of X, that we denote by h_X.

Given a functor F from finite-dimensional algebras to sets, there exists a natural isomorphism

$$\mathrm{Hom}(h_X, F) \xrightarrow{\sim} F(X), \quad u \longmapsto u(X)(\mathrm{id}_X),$$

where the left-hand side denotes the set of morphisms of functors, also known as natural transformations (Yoneda's lemma, see [9, Lem. VI-1]). In particular, we obtain natural isomorphisms

$$\mathrm{Hom}(h_X, h_Y) \simeq h_Y(X) = \mathrm{Hom}(X, Y) \simeq \mathrm{Hom}_{\mathrm{alg}}(\mathcal{O}(Y), \mathcal{O}(X)).$$

It follows that every finite scheme is uniquely determined by its functor of points. So we may view finite schemes as **representable functors** from finite-dimensional algebras to sets, i.e., functors of the form h_X.

Some operations on finite schemes have a simple formulation in terms of their functors of points. For example, given finite schemes $X_1, \dots, X_n$, their sum satisfies

$$(X_1 \sqcup \cdots \sqcup X_n)(R) = X_1(R) \sqcup \cdots \sqcup X_n(R)$$

for any finite-dimensional algebra R. Also, given two finite schemes X, Y, we have a functorial bijection

$$X(R) \times Y(R) \xrightarrow{\sim} (X \times Y)(R)$$

via the tensor product of algebra homomorphisms. In other words, the functor $R \mapsto X(R) \times Y(R)$ is represented by the product $X \times Y$.

More generally, given two morphisms of finite schemes $f : X \to Z$, $g : Y \to Z$, we may consider the functor

$$R \longmapsto X(R) \times_{Z(R)} Y(R) = \{(u, v) \in X(R) \times Y(R) \mid f(R)(u) = g(R)(v)\}.$$

Then this functor is represented by the finite scheme

$$W = \mathrm{Spec}\,\big(\mathcal{O}(X) \otimes_{\mathcal{O}(Z)} \mathcal{O}(Y)\big)$$

where $\mathcal{O}(X)$ (resp. $\mathcal{O}(Y)$) is a $\mathcal{O}(Z)$-algebra via f^* (resp. g^*). Indeed, this follows easily from the universal property of the tensor product of algebras.

Definition 1.2.22. With the above notation and assumptions, the finite scheme W is called the **fibered product** of X and Y above Z, and denoted by $X \times_Z Y$.

In particular, consider a morphism of finite schemes $f : X \to Y$, and a k-point of Y viewed as a morphism $y : \mathrm{Spec}(k) \to Y$. Then the fibered product $X \times_Y y$ is called the (schematic) **fiber of f at y** and denoted by X_y.

The functor of points of X_y satisfies

$$X_y(R) = \{u \in X(R) \mid f(R)(u) = y(R)\} \tag{1.6}$$

for any finite-dimensional algebra R. In particular, $X_y(k)$ is the set-theoretic fiber $f(k)^{-1}(y)$.

Also, note that $X \times_Z Y$ is the subscheme of $X \times Y$ with ideal generated by the $f^*(h) \otimes 1 - 1 \otimes g^*(h)$, where $h \in \mathcal{O}(Z)$. As a consequence, X_y is the subscheme of X with ideal $f^*(\mathfrak{m}_y)\mathcal{O}(X)$, where $\mathfrak{m}_y$ denotes the maximal ideal of y in $\mathcal{O}(Y)$.

Remark 1.2.23. Some notions and results of this section extend to the setting of **affine schemes**; these form the opposite category to that of algebras (without finiteness condition). More specifically, the constructions of sums and fibered products extend unchanged; also, affine schemes may be viewed as representable functors from algebras to sets, via their functor of points. We will still use the notations $X = \mathrm{Spec}(A)$ and $A = \mathcal{O}(X)$ in the setting of affine schemes.

A basic example of affine scheme is the **affine n-space**

$$\mathbb{A}^n = \mathrm{Spec}(k[T_1, \ldots, T_n]),$$

where n is a positive integer. We have $\mathbb{A}^n \simeq \mathbb{A}^1 \times \cdots \times \mathbb{A}^1$ (n times), since $k[T_1, \ldots, T_n] \simeq k[T] \otimes \cdots \otimes k[T]$. Moreover, $\mathbb{A}^n(R) = R^n$ for any algebra R.

But there are important differences between affine and finite schemes. For example, an affine scheme may well have no k-point (just consider a nontrivial field extension of k, e.g., the field of rational functions $k(T)$). The subclass of (affine) **schemes of finite type**, also known as **algebraic schemes**, is better behaved in this respect; these correspond to the finitely generated algebras, i.e., those isomorphic to a quotient $A = k[T_1, \ldots, T_n]/I$, where I is an ideal of $k[T_1, \ldots, T_n]$. The functor of points of $X = \mathrm{Spec}(A)$ satisfies

$$X(R) = \{(x_1, \ldots, x_n) \in R^n \mid P(x_1, \ldots, x_n) = 0 \text{ for all } P \in I\}.$$

In particular, $X(k)$ is the set of zeros of I in k^n; such a set is known as an (affine) **algebraic set**.

By Hilbert's basis theorem (see [10, Thm. 1.2]), every ideal I as above is finitely generated, and hence every algebraic set is the set of common zeros of finitely many polynomials. Also, by Hilbert's Nullstellensatz (see [10, Thm. 1.6]), the maximal ideals of A are exactly the kernels of elements of $X(k) = \mathrm{Hom}_{\mathrm{alg}}(A, k)$. Moreover, A is finite-dimensional if and only if $X(k)$ is finite.

A new feature of affine schemes is the **Zariski topology**. For algebraic schemes, it can be defined as the topology on $X(k)$ with closed sets being the zeros of ideals of $k[T_1, \ldots, T_n]$ containing I. These ideals can be identified with the ideals J of A, and they correspond bijectively with the **closed subschemes** $Y = \mathrm{Spec}(A/J)$ of $X = \mathrm{Spec}(A)$ (then $Y(k)$ is closed in $X(k)$). Thus, every affine algebraic scheme is isomorphic to a closed subscheme of an affine space. Also, for finite schemes, the Zariski topology is just the discrete topology, i.e., every subset is closed.

Every algebraic scheme $X = \mathrm{Spec}(A)$ has a largest closed reduced subscheme X_{red} corresponding to the nilradical of A; moreover, $X_{\mathrm{red}}(k) \xrightarrow{\sim} X(k)$. But A may have no largest reduced subalgebra; for example, the nonreduced algebra $k[T_1, T_2]/(T_2^2)$ is generated by its reduced subalgebras $k[T_1]$ and $k[T_1 + T_2]$. Still, A has a largest reduced finite-dimensional subalgebra: the span of its idempotents (see e.g. [24, Prop. 1.29]).

An affine scheme X is called **connected** if the algebra $\mathcal{O}(X)$ is indecomposable. Every affine algebraic scheme X is the sum of finitely many connected schemes, and these are affine algebraic as well. Moreover, X is connected if and only if $X(k)$ is connected relative to the Zariski topology (see loc. cit.).

Remark 1.2.24. We briefly present some further aspects of scheme theory, which will only be used in Section 1.6; we refer to [9] for a user-friendly introduction to schemes.

There is a notion of (not necessarily affine) schemes. These are obtained by gluing affine schemes, like manifolds in differential geometry; the Hausdorff property is replaced with the property that the diagonal is closed. Schemes are equipped with the Zariski topology; the notion of closed subscheme extends readily to this setting.

A basic example is the **projective** n**-space** $\mathbb{P}^n$, obtained by gluing appropriately $n + 1$ copies of $\mathbb{A}^n$ (corresponding to the nonvanishing of homogeneous coordinates). The **projective schemes** are those isomorphic to a closed subscheme of some projective space.

A scheme is called **of finite type** (or **algebraic**) if it admits an open covering by finitely many affine schemes of finite type. Every projective scheme is of finite type. Also, every scheme of finite type has only finitely many connected components.

A scheme is **reduced** (resp. **integral**) if the algebra $\mathcal{O}(U)$ is reduced (resp. integral) for any open affine subset U. A **variety** is an integral scheme of finite type. For example, $\mathbb{A}^n$ and $\mathbb{P}^n$ are varieties, as well as elliptic curves.

By taking k-points, every closed reduced subscheme of $\mathbb{A}^n$ is identified with an **algebraic subset** of k^n, i.e., the set of common zeros of polynomials in n variables. The subvarieties of $\mathbb{A}^n$ correspond to **irreducible** algebraic subsets (those that are not the union of proper closed subsets). Likewise, we may define the algebraic subsets of $\mathbb{P}^n(k)$ as the sets of common zeros of homogeneous polynomials in $n+1$ variables; then the closed subvarieties of $\mathbb{P}^n$ can be identified with the irreducible algebraic subsets of $\mathbb{P}^n(k)$.

1.3 Finite group schemes

1.3.1 Basic definitions and examples

A group structure on a set G is given by two maps $\mu : G \times G \to G$, $(x, y) \mapsto xy$ (the multiplication map) and $\iota : G \to G$, $x \mapsto x^{-1}$ (the inverse map), together with an element $e \in G$ (the neutral element) which satisfy the group axioms. These translate into the commutativity of the following diagrams:

$$\begin{tikzcd}
G \times G \times G \arrow[r, "\mu \times \mathrm{id}"] \arrow[d, "\mathrm{id} \times \mu"'] & G \times G \arrow[d, "\mu"] \\
G \times G \arrow[r, "\mu"] & G
\end{tikzcd} \tag{1.7}$$

(i.e., μ is associative),

$$\begin{tikzcd}
G \arrow[r, "(\mathrm{id},\iota)"] \arrow[dr, "e"'] & G \times G \arrow[d, "\mu"] & G \arrow[l, "(\iota,\mathrm{id})"'] \arrow[dl, "e"] \\
& G &
\end{tikzcd} \tag{1.8}$$

(i.e., ι is the inverse map), and

$$\begin{tikzcd}
G \arrow[r, "{(e,\mathrm{id})}"] \arrow[dr, "\mathrm{id}"'] & G \times G \arrow[d, "\mu"] & G \arrow[l, "{(\mathrm{id},e)}"'] \arrow[dl, "\mathrm{id}"] \\
& G &
\end{tikzcd} \tag{1.9}$$

(i.e., e is the neutral element). Here $e : G \to G$ denotes the constant map $g \mapsto e$.

Next, let $A = \mathcal{O}(G)$. In view of the isomorphism (1.1), we may identify $\mathcal{O}(G \times G)$ with $A \otimes A$, and $\mathcal{O}(G \times G \times G)$ with $A \otimes A \otimes A$. By Lemma 1.2.5, the data of the multiplication $\mu : G \times G \to G$ is equivalent to that of an algebra homomorphism

$$\Delta = \mu^* : A \longrightarrow A \otimes A.$$

Likewise, ι corresponds to an algebra endomorphism

$$S = \iota^* : A \longrightarrow A,$$

and e to an algebra homomorphism

$$\varepsilon = e^* : A \longrightarrow k.$$

Moreover, the commutative diagrams (1.7), (1.8), (1.9) correspond to commutative diagrams

$$\begin{tikzcd}
A \arrow[r, "\Delta"] \arrow[d, "\Delta"'] & A \otimes A \arrow[d, "\Delta\otimes\mathrm{id}"] \\
A \otimes A \arrow[r, "\mathrm{id}\otimes\Delta"] & A \otimes A \otimes A
\end{tikzcd} \tag{1.10}$$

$$\begin{tikzcd}
& A \arrow[dl, "\varepsilon"'] \arrow[d, "\Delta"] \arrow[dr, "\varepsilon"] & \\
A & A \otimes A \arrow[l, "\mathrm{id}\otimes S"'] \arrow[r, "S\otimes\mathrm{id}"] & A
\end{tikzcd} \tag{1.11}$$

$$\begin{tikzcd}
& A \arrow[dl, "\mathrm{id}"'] \arrow[d, "\Delta"] \arrow[dr, "\mathrm{id}"] & \\
A & A \otimes A \arrow[l, "\mathrm{id}\otimes\varepsilon"'] \arrow[r, "\mathrm{id}\otimes\varepsilon"] & A
\end{tikzcd} \tag{1.12}$$

Here we denote again by $\varepsilon : A \to A$ the composition of $\varepsilon : A \to k$ with the inclusion of k into A.

Definition 1.3.1. A **Hopf algebra** is an algebra A equipped with algebra homomorphisms $\Delta = \Delta_A : A \to A \otimes A$ (the **comultiplication**), $S = S_A : A \to A$ (the **antipode**) and $\varepsilon = \varepsilon_A : A \to k$ (the **augmentation**) such that the diagrams (1.10), (1.11) and (1.12) commute.

Given two Hopf algebras A, B, a **homomorphism of Hopf algebras** $u : A \to B$ is an algebra homomorphism such that $\Delta_B \circ u = (u \otimes u) \circ \Delta_A$.

The latter condition corresponds to the equality $f(xy) = f(x)f(y)$ for a group homomorphism $f : G \to H$ and for all $x, y \in G$.

Actually, the notion of Hopf algebra is more general, and does not assume that A is commutative, nor that k is algebraically closed. Also, the data of Δ determines S, ε uniquely, and every homomorphism of Hopf algebras $u : A \to B$ satisfies $S_B \circ u = u \circ S_A$ and $\varepsilon_B \circ u = u \circ \varepsilon_A$ (see [37, §2.1]).

By Proposition 1.2.8 and the isomorphism (1.1), the category of finite groups is equivalent to the opposite category of reduced finite-dimensional Hopf algebras. This motivates the following:

Definition 1.3.2. The **category of finite group schemes** is the opposite to that of finite-dimensional Hopf algebras.

Equivalently, a finite group scheme is a finite scheme G equipped with morphisms $\mu : G \times G \to G$, $\iota : G \to G$ and with a k-point e such that the diagrams (1.7), (1.8) and (1.9) commute. For any finite-dimensional algebra R, we obtain a group structure on the set $G(R)$ with multiplication map $\mu(R)$, inverse map $\iota(R)$, and neutral element $e \in G(k) \subset G(R)$. Given $x, y \in G(R)$, we denote $\mu(x, y)$ by xy, and $\iota(x)$ by x^{-1}.

Alternatively, we may view finite group schemes as **representable group functors**, i.e., representable functors from the category of finite-dimensional algebras to that of groups.

Definition 1.3.3. A **subgroup scheme** of a finite group scheme G is a subscheme H such that $H(R)$ is a subgroup of $G(R)$ for any finite-dimensional algebra R. We then write $H \leq G$.

Definition 1.3.4. Let $f : G \to H$ be a homomorphism of finite group schemes. The **kernel** $\mathrm{Ker}(f)$ is the fiber of f at e_H.

We have $\mathrm{Ker}(f)(R) = \{x \in G(R) \mid f(R)(x) = e_H\} = \mathrm{Ker}(f(R))$ for any finite-dimensional algebra R. As a consequence, $N = \mathrm{Ker}(f)$ is a **normal subgroup scheme** of G, i.e., $xyx^{-1} \in N(R)$ for any such R and any $x \in G(R)$, $y \in N(R)$. We then write $N \trianglelefteq G$.

Definition 1.3.5. The **order** of a finite group scheme G is the dimension of the algebra $\mathcal{O}(G)$.

As for finite schemes, the category of reduced finite group schemes is equivalent to that of finite groups via $G \mapsto G(k)$. A quasi-inverse functor sends every finite group F to the algebra $\mathcal{O}(F)$. (This algebra is canonically isomorphic to the dual of the group algebra $k[F]$, but generally not to $k[F]$ itself. Indeed, $\mathcal{O}(F)$ is always commutative, but $k[F]$ is commutative if and only if F is commutative). Also, the notion of order of a finite group scheme generalizes that for finite groups. We will freely identify finite groups with the associated group schemes.

We now reconsider our first examples from §1.2.1:

Example 1.3.6. Given a positive integer n, let $A = k[T]/(T^n - 1)$. Then A is a k-algebra of dimension n, and one may check that A is a Hopf algebra relative to the homomorphisms

$$\Delta : A \longrightarrow A \otimes A, \quad t \longmapsto t_1 \otimes t_2,$$

$$S : A \longrightarrow A, \quad t \longmapsto t^{n-1},$$

$$\varepsilon : A \longrightarrow k, \quad t \longmapsto 1,$$

where t denotes the image of T in A. The corresponding finite group scheme is the group scheme of nth roots of unity, denoted by μ_n. Indeed, we have for any finite-dimensional algebra R

$$\mu_n(R) = \{r \in R \mid r^n = 1\}.$$

Example 1.3.7. If $p > 0$ then the local p-dimensional algebra $B = k[T]/(T^p)$ is a Hopf algebra relative to the homomorphisms

$$\Delta : B \longrightarrow B \otimes B, \quad t \longmapsto t_1 \otimes 1 + 1 \otimes t_2,$$

$$S : B \longrightarrow B, \quad t \longmapsto -t,$$

$$\varepsilon : B \longrightarrow k, \quad t \longmapsto 0$$

with a similar notation. The corresponding finite group scheme α_p satisfies for any finite-dimensional algebra R

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

Note that μ_p and α_p are isomorphic as schemes, since their algebras are isomorphic via $A \to B$, $t \mapsto t + 1$. One may show that these algebras are not isomorphic as Hopf algebras; equivalently, μ_p and α_p are not isomorphic as group schemes (see Example 1.4.17 for an alternative proof). So we obtain three distinct group schemes of order p, namely, μ_p, α_p and the cyclic group $\mathbb{Z}/p\mathbb{Z}$. We will see in Corollary 1.4.26 that these yield all group schemes of order p.

Definition 1.3.8. A finite group scheme G is **infinitesimal** if $G(k) = \{e\}$; equivalently, the algebra $\mathcal{O}(G)$ is local.

Infinitesimal group schemes are also called **local** or **connected**. If $p = 0$ then every infinitesimal group scheme is trivial (Theorem 1.4.13 below). This fails if $p > 0$ in view of the above examples of μ_p and α_p.

1.3.2 Actions of finite group schemes, semi-direct products

Definition 1.3.9. An **action** of a finite group scheme G on a finite scheme X is a morphism of schemes

$$\alpha : G \times X \longrightarrow X, \quad (g, x) \longmapsto g \cdot x$$

such that $g \cdot (h \cdot x) = gh \cdot x$ and $e \cdot x = x$ for any algebra R and any $g, h \in G(R)$, $x \in X(R)$.

The former condition is equivalent to the commutativity of the square

$$\begin{tikzcd}
G \times G \times X \arrow[r, "\mu \times \mathrm{id}"] \arrow[d, "\mathrm{id} \times \alpha"'] & G \times X \arrow[d, "\alpha"] \\
G \times X \arrow[r, "\alpha"] & X
\end{tikzcd}$$

and the latter condition, to the commutativity of the triangle

$$\begin{tikzcd}
X \arrow[r, "{(e,\mathrm{id})}"] \arrow[dr, "\mathrm{id}"'] & G \times X \arrow[d, "\alpha"] \\
 & X
\end{tikzcd}$$

Let $A = \mathcal{O}(X)$. Then the data of a G-action α on X is equivalent to that of a homomorphism of algebras

$$\rho = \alpha^* : A \longrightarrow \mathcal{O}(G) \otimes A$$

such that the following diagrams commute:

$$\begin{tikzcd}
A \arrow[r, "\rho"] \arrow[d, "\rho"'] & \mathcal{O}(G) \otimes A \arrow[d, "\rho\otimes\mathrm{id}"] \\
\mathcal{O}(G) \otimes A \arrow[r, "\Delta\otimes\mathrm{id}"] & \mathcal{O}(G) \otimes \mathcal{O}(G) \otimes A
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[r, "\rho"] \arrow[dr, "\mathrm{id}"'] & \mathcal{O}(G) \otimes A \arrow[d, "\varepsilon\otimes\mathrm{id}"] \\
& A
\end{tikzcd}$$

where $\Delta = \mu^* : \mathcal{O}(G) \to \mathcal{O}(G) \otimes \mathcal{O}(G)$ and $\varepsilon = e^* : \mathcal{O}(G) \to k$. We then say that A is a G-**algebra**, and X is a G-**scheme**. The map ρ is called the **co-action**; it equips A with the structure of a (left) comodule over the Hopf algebra $\mathcal{O}(G)$.

From the functorial viewpoint, a G-action on X is an action of the group $G(R)$ on the set $X(R)$ for any finite-dimensional algebra R, which is functorial in R.

For example, the projection $\mathrm{pr}_X : G \times X \to X$ is an action, called the **trivial action**. It corresponds to the trivial action of $G(R)$ on $X(R)$ for any R as above, and to the co-action $1 \otimes \mathrm{id} : A \to \mathcal{O}(G) \otimes A$, $a \mapsto 1 \otimes a$. In the opposite direction, a G-action is called **faithful** (or **effective**) if no proper subgroup scheme acts trivially.

Remark 1.3.10. Consider again a finite G-scheme X with action morphism α. For any $g \in G(k)$, we obtain an automorphism $\alpha(g, -)$ of the scheme X, and hence an algebra automorphism $\alpha(g, -)^*$ of A. This yields in turn an action of $G(k)$ on A by algebra automorphisms, where each g acts via the inverse of $\alpha(g, -)^*$.

If G is reduced, then the data of a G-action on X is equivalent to that of a $G(k)$-action on A by algebra automorphisms. More specifically, the algebra $\mathcal{O}(G) \otimes A$ is identified with the set of maps $G(k) \to A$ equipped with pointwise addition and multiplication. This identifies the co-action $\rho : A \to \mathcal{O}(G) \otimes A$ with the map $a \mapsto (g \mapsto g \cdot a)$.

This construction can be generalized as follows: let R be a finite-dimensional algebra, and $g \in G(R) = \mathrm{Hom}(\mathcal{O}(G), R)$. Composing $\alpha^* : A \to \mathcal{O}(G) \otimes A$ with $g \otimes \mathrm{id} : \mathcal{O}(G) \otimes A \to R \otimes A$, we obtain an algebra homomorphism $A \to R \otimes A$, and hence an R-algebra endomorphism $g^* : R \otimes A \to R \otimes A$. One may check that g^* is an automorphism with inverse $(g^{-1})^*$; moreover, this yields an action of $G(R)$ on $R \otimes A$ by R-algebra automorphisms, where g acts via $(g^{-1})^*$. This action is functorial in R, and determines the G-action on X uniquely. Moreover, G acts faithfully on X if and only if the group $G(R)$ acts faithfully on $R \otimes A$ for any finite-dimensional algebra R.

Definition 1.3.11. Let $u : G \to H$ be a homomorphism of finite group schemes. Let X be a G-scheme, and Y an H-scheme. A morphism of schemes $f : X \to Y$ is **equivariant** if we have $f(g \cdot x) = u(g) \cdot f(x)$ for any algebra R and any $g \in G(R)$, $x \in X(R)$.

Example 1.3.12. Every finite group scheme G acts on itself by left multiplication: $(x, y) \mapsto xy$ for any finite-dimensional algebra R and any $x, y \in G(R)$. Also, G acts on itself by right multiplication ($(x, y) \mapsto yx^{-1}$) and by conjugation ($(x, y) \mapsto xyx^{-1}$). Moreover, every homomorphism of finite group schemes $f : G \to H$ is equivariant relative to either of these actions.

Next, let N, H be finite group schemes and $\alpha : H \times N \to N$ an action by group automorphisms, i.e., $x \cdot yz = (x \cdot y)(x \cdot z)$ for any finite-dimensional algebra R and any $x \in H(R)$, $y, z \in N(R)$. We may then form the semi-direct product $N(R) \rtimes H(R)$ for any such R. This yields a group functor, which is clearly represented by the product scheme $N \times H$ equipped with the appropriate multiplication and inverse morphisms, and with the neutral element (e_N, e_H). The corresponding finite group scheme is the **semi-direct product** $G = N \rtimes H$. We have $N \trianglelefteq G$ and $H \leq G$.

We now come to the main result of this section:

Theorem 1.3.13. *Let G be a finite group scheme. Then the reduced subscheme G_{red} is a subgroup scheme. Moreover, G has a largest infinitesimal subgroup scheme G^0, and G^0 is normal in G. We have $G = G^0 \rtimes G_{\mathrm{red}}$.*

Proof Recall from Corollary 1.2.20 that the formation of the reduced subscheme X_{red} commutes with products. In view of the commutative diagrams (1.7), (1.8) and (1.9), it follows that G_{red} is a subgroup scheme.

Likewise, the formation of $r = r_X : X \to X_{\mathrm{red}}$ commutes with products, and hence $r_G : G \to G_{\mathrm{red}}$ is a homomorphism. Let K be its kernel, then we have $G = K \rtimes G_{\mathrm{red}}$. Moreover, K is infinitesimal, since r is bijective on k-valued points. If I is an infinitesimal subgroup scheme of G, then $r_I : I \to I_{\mathrm{red}}$ is trivial. By functoriality, it follows that I is a subgroup scheme of $\mathrm{Ker}(r_G) = K$. So K is the largest infinitesimal subgroup scheme of G. □

Example 1.3.14. Assume that $p > 0$ and let n be a positive integer. Then the group scheme α_p admits an action of μ_n by group automorphisms, via $x \cdot y = xy$. So we may form the semi-direct product $G = \alpha_p \rtimes \mu_n$.

If n is prime to p, then one may readily check that $G_{\mathrm{red}} = \mu_n$. As a consequence, G_{red} is not a normal subgroup scheme of G.

On the other hand, if $n = p$ then G is a noncommutative infinitesimal group scheme of order p^2.

Remark 1.3.15. As for affine schemes, we may define the category of **affine group schemes** as the opposite to that of Hopf algebras. Alternatively, the affine group schemes are the representable group functors from the category of algebras. The notions of action, equivariant morphism, semi-direct product extend readily to the setting of affine group schemes. Also, we have an obvious notion of **closed** subgroup scheme. The (schematic) kernel of a homomorphism of affine group schemes is a closed normal subgroup scheme.

An affine group scheme G is called **algebraic** if its underlying scheme is algebraic, i.e., the algebra $\mathcal{O}(G)$ is finitely generated. Then G is called an **algebraic group** for simplicity. Basic examples of affine algebraic groups include:

- the **multiplicative group** $\mathbb{G}_m$, corresponding to the Hopf algebra $k[T, T^{-1}] \simeq k[T_1, T_2]/(T_1T_2 - 1)$ with comultiplication, antipode and augmentation given by $T \mapsto T_1 \otimes T_2$, $T \mapsto T^{-1}$ and $T \mapsto 1$ (compare with Example 1.3.6). The corresponding group functor is given by $R \mapsto (R^\times, \times)$, where $R^\times$ denotes the group of invertible elements of the algebra R,
- the **additive group** $\mathbb{G}_a$, corresponding to the Hopf algebra $k[T]$ with comultiplication, antipode and augmentation given by $T \mapsto T_1 \otimes 1 + 1 \otimes T_2$, $T \mapsto -T$ and $T \mapsto 0$ as in Example 1.3.7. The corresponding group functor is given by $R \mapsto (R, +)$,
- the **general linear group** GL_n, which represents the group functor $R \mapsto \mathrm{GL}_n(R)$ (the group of invertible $n \times n$ matrices with coefficients in R). Its Hopf algebra is $k[T_{ij}, 1 \leq i, j \leq n][1/\det(T_{i,j})]$, where the T_{ij} are the matrix coefficients. According to the formula for the product of matrices, the comultiplication satisfies

$$\Delta(T_{ij}) = \sum_{\ell=1}^{n} T_{i\ell}^{(1)} \otimes T_{\ell j}^{(2)}$$

with an obvious notation. Likewise, the antipode is given by the inverse of matrices, and the augmentation is the evaluation map at the identity matrix.

Note that $\mathbb{G}_m = \mathrm{GL}_1$ and $\mathbb{G}_a$ is the closed subgroup scheme of GL_2 with ideal $(T_{1,1} - 1, T_{2,1}, T_{2,2} - 1)$.

Likewise, given a finite-dimensional vector space V, we may define the general linear group GL_V. A homomorphism of affine group schemes $\rho : G \to \mathrm{GL}_V$ is called a **linear representation of G in V**. We say that ρ is **faithful** if its kernel is trivial; then ρ yields an isomorphism of G onto a closed subgroup scheme of GL_V (see [24, Cor. 3.35]).

If G is a finite group scheme, then its action on itself by left multiplication yields a faithful linear representation in $\mathcal{O}(G)$ (as follows from Remark 1.3.10). Thus, G is isomorphic to a closed subgroup scheme of GL_n, where $n = |G|$.

An algebraic group G is called **linear** if it is isomorphic to a closed subgroup scheme of some general linear group. Then G is clearly affine; conversely, every affine algebraic group is linear (see [24, Cor. 4.10]).

Finally, the structure theorem 1.3.13 extends partially to any affine algebraic group G: the reduced subscheme G_{red} is a subgroup scheme and the connected component of e in G is a normal subgroup scheme, denoted by G^0. Moreover, the connected components of G are exactly the cosets gG^0, where $g \in G(k)$. In particular, there are only finitely many such cosets, and $G = G^0 G_{\mathrm{red}}$. Finally, $G^0_{\mathrm{red}} = G^0 \cap G_{\mathrm{red}}$ is a group variety.

Remark 1.3.16. We will also encounter nonaffine group schemes; these may be defined as schemes G equipped with morphisms $\mu : G \times G \to G$, $\iota : G \to G$ and with $e \in G(k)$ satisfying the group axioms. The notion of **algebraic group** extends readily to this setting. For example, every elliptic curve E equipped with a k-point 0 has a unique structure of an algebraic group with neutral element 0 (see [31, §III.2]).

1.4 Lie algebras and applications

1.4.1 The Lie algebra of derivations of an algebra

Definition 1.4.1. A **derivation** of an algebra A is a k-linear map $D : A \to A$ which satisfies the Leibniz rule:

$$D(ab) = aD(b) + D(a)b \quad (a, b \in A). \tag{1.13}$$

We denote by $\mathrm{Der}(A)$ the set of derivations of A. For any $D \in \mathrm{Der}(A)$ and $a \in A$, the map $aD : A \to A$, $b \mapsto aD(b)$ is a derivation. This yields an A-module structure on $\mathrm{Der}(A)$, which is in particular a k-vector space. If A is finite-dimensional, then $\mathrm{Der}(A)$ is finite-dimensional as well.

Given $D_1, D_2 \in \mathrm{Der}(A)$, the commutator

$$[D_1, D_2] = D_1 \circ D_2 - D_2 \circ D_1$$

is easily seen to be a derivation. Moreover, the commutator map is bilinear, antisymmetric (that is, $[D, D] = 0$ for all $D \in \mathrm{Der}(A)$), and satisfies the Jacobi identity:

$$[D_1, [D_2, D_3]] + [D_2, [D_3, D_1]] + [D_3, [D_1, D_2]] = 0$$

for any $D_1, D_2, D_3 \in \mathrm{Der}(A)$. So $\mathrm{Der}(A)$ is a **Lie algebra**.

Given $D \in \mathrm{Der}(A)$ and a positive integer n, we obtain

$$D^n(ab) = \sum_{m=0}^{n} \binom{n}{m} D^m(a) D^{n-m}(b) \quad (a, b \in A) \tag{1.14}$$

by induction on n, where $D^n = D \circ \cdots \circ D$ (n times). If $p = \mathrm{char}(k) > 0$, then it follows that D^p is a derivation for any $D \in \mathrm{Der}(A)$.

Example 1.4.2. Let A be the polynomial ring $k[T_1, \ldots, T_n]$. Then $\mathrm{Der}(A)$ is a free A-module with basis the partial derivatives $\partial_i : P \to \partial P / \partial T_i$ ($i = 1, \ldots, n$). The Lie algebra structure on $\mathrm{Der}(A)$ is given by

$$[P\partial_i, Q\partial_j] = P(\partial_i Q)\partial_j - (\partial_j P)Q\partial_i$$

for all $P, Q \in A$ and all i, j. If $p > 0$ then $\partial_i^p = 0$ for all i.

More generally, let $P_1, \ldots, P_m \in k[T_1, \ldots, T_n]$ and consider the quotient $A = k[T_1, \ldots, T_n]/(P_1, \ldots, P_m)$. Denote by $t_1, \ldots, t_n$ the images of $T_1, \ldots, T_n$ in A. Then the assignment $D \mapsto (D(t_1), \ldots, D(t_n))$ identifies the A-module $\mathrm{Der}(A)$ with the kernel of the "Jacobian matrix" $(a_{ij})_{1 \le i \le n, 1 \le j \le m}$, where a_{ij} denotes the image of $\partial_i P_j$ in A.

As a consequence, $\mathrm{Der}(A)$ is a finitely generated A-module for any finitely generated algebra A.

Example 1.4.3. Let n be a positive integer, and $A = k[T]/(T^n)$. Then A is a local algebra with basis $1, t, \ldots, t^{n-1}$, where t denotes the image of T, and with maximal ideal $\mathfrak{m} = (t)$. For any $D \in \mathrm{Der}(A)$, we have $nt^{n-1}D(t) = 0$ by the Leibniz rule. Moreover, by the preceding example or a direct argument, the map $D \mapsto D(t)$ identifies the A-module $\mathrm{Der}(A)$ with the ideal $I = \{f \in A \mid nt^{n-1}f = 0\}$. We have $I = \mathfrak{m}$ if $p = 0$ or p does not divide n, and $I = A$ otherwise.

In the former case, there exists a unique $D_1 \in \mathrm{Der}(A)$ such that $D_1(t) = t$ (it arises from the derivation Td/dT of $k[T]$). Moreover, the

$D_i = t^i D_1$, where $0 \leq i \leq n-2$, form a basis of the vector space $\mathrm{Der}(A)$. We have the commutation relations

$$[D_i, D_j] = \begin{cases} (j-i)D_{i+j-1} & \text{if } i+j \leq n, \\ 0 & \text{otherwise.} \end{cases} \tag{1.15}$$

In particular, $\dim(\mathrm{Der}(A)) = n-1$ and $\mathrm{Der}(A)$ stabilizes the powers $\mathfrak{m}^i = (t^i)$ for $i = 1, \ldots, n-1$. As a consequence, the Lie algebra $\mathrm{Der}(A)$ is solvable.

In the latter case (where $p > 0$ divides n), there exists a unique $D_0 \in \mathrm{Der}(A)$ such that $D_0(t) = 1$ (arising from $d/dT \in \mathrm{Der}(k[T])$) and the vector space $\mathrm{Der}(A)$ has basis the $D_i = t^i D_0$, where $0 \leq i \leq n-1$. These satisfy the relations (1.15). In particular, $\dim(\mathrm{Der}(A)) = n$ and $\mathrm{Der}(A)$ does not stabilize $\mathfrak{m}$. But it stabilizes the powers $\mathfrak{m}^i$, where i is a positive multiple of p. If $n > p$ then $\mathfrak{m}^{n-p}$ is a nonzero subspace of A, stable by $\mathrm{Der}(A)$ and killed by D_0^p but not by D_0. As a consequence, the Lie algebra $\mathrm{Der}(A)$ is not simple. If $n = p$ then $\mathrm{Der}(A) = \mathrm{Der}\,(k[T]/(T^p))$ is the **Witt algebra**; it is solvable when $p = 2$, and simple when $p \geq 3$ (exercise).

Lemma 1.4.4. *Let A be an algebra.*

(i). *We have $D(e) = 0$ for any $D \in \mathrm{Der}(A)$ and any idempotent $e \in A$.*

(ii). *If $A = B \times C$ is decomposable, then the natural map $\mathrm{Der}(B) \times \mathrm{Der}(C) \to \mathrm{Der}(A)$ is an isomorphism of Lie algebras.*

(iii). *Assume that A is finite-dimensional. Then $\mathrm{Der}(A) = 0$ if and only if A is reduced.*

Proof (i) Since $e = e^2$, we have $D(e) = 2eD(e)$ and hence $eD(e) = 2e^2D(e) = 2eD(e) = D(e)$. It follows that $D(e) = 0$ as desired.

(ii) Denote by e the identity element of B; then $B = eA$. By (i), every $D \in \mathrm{Der}(A)$ satisfies $D(e) = 0$, and hence $D(B) \subset B$ in view of the Leibniz rule. Clearly, $D|_B \in \mathrm{Der}(B)$. Likewise, $D|_C \in \mathrm{Der}(C)$; this implies readily the statement.

(iii) If A is reduced, then it is spanned by its idempotents by Lemma 1.2.7. So $\mathrm{Der}(A) = 0$ by (i).

Conversely, assume that $\mathrm{Der}(A) = 0$. Using (ii), we may further assume that A is indecomposable; then A is local by Theorem 1.2.13. If $A \neq k$ then its maximal ideal $\mathfrak{m}$ is nonzero, and hence there exists $n \geq 2$ such that $\mathfrak{m}^{n-1} \neq 0 = \mathfrak{m}^n$ (Lemma 1.2.11). Choose a nonzero linear map $f : \mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{m}^{n-1}$ and define a linear map $D : A = k \oplus \mathfrak{m} \to A$ by

$D(1) = 0$ and $D(a) = f(\bar{a})$ for any $a \in \mathfrak{m}$ with image $\bar{a} \in \mathfrak{m}/\mathfrak{m}^2$. Then $D \neq 0$ and one may readily check that D is a derivation. □

1.4.2 Restricted Lie algebras

Given a vector space V, we denote by $\mathfrak{gl}(V)$ the Lie algebra of endomorphisms of V (relative to the commutator map). If $V = k^n$ then we get the Lie algebra of $n \times n$ matrices, denoted by $\mathfrak{gl}_n$.

For any algebra A, the space of derivations $\mathrm{Der}(A)$ is a Lie subalgebra of $\mathfrak{gl}(A)$. If $p > 0$ then $\mathrm{Der}(A)$ is stable by the pth power map of linear maps $\mathfrak{gl}(A) \to \mathfrak{gl}(A)$, $u \mapsto u^p = u \circ \cdots \circ u$ (p times). We then say that $\mathrm{Der}(A)$ is a **restricted Lie subalgebra** of $\mathfrak{gl}(A)$.

The notion of restricted Lie algebra may be defined intrinsincally, as follows. One may check that the pth power map of $\mathfrak{g} = \mathfrak{gl}(V)$ satisfies the following relations:

(a). $(tx)^p = t^p x^p \qquad (t \in k, x \in \mathfrak{g})$,

(b). $\mathrm{ad}(x^p) = \mathrm{ad}(x)^p \qquad (x \in \mathfrak{g})$,

(c). $(x+y)^p = x^p + y^p + \sum_{i=1}^{p-1} s_i(x,y) \qquad (x, y \in \mathfrak{g})$.

Here we denote by

$$\mathrm{ad} : \mathfrak{g} \longrightarrow \mathfrak{gl}(\mathfrak{g}), \quad x \longmapsto (y \mapsto [x,y])$$

the adjoint representation, and we set

$$s_i(x,y) = -\frac{1}{i} \sum_u \mathrm{ad}(x_{u(1)})\mathrm{ad}(x_{u(2)}) \cdots \mathrm{ad}(x_{u(p-1)})(x_1),$$

where u runs through the maps $\{1, 2, \ldots, p-1\} \to \{0,1\}$ which take the value 0 exactly i times. For example, $s_1(x,y) = [x,y]$ if $p = 2$. We refer to [6, II.7.3.2] or [24, Prop. 10.38] for details.

Definition 1.4.5. A **restricted Lie algebra** is a Lie algebra $\mathfrak{g}$ equipped with a self-map $x \mapsto x^{[p]}$ (the **pth power map**) satisfying the above relations (a), (b), (c).

We will see that both notions of restricted Lie (sub)algebras are equivalent. For this, we will use two universal constructions in Lie theory.

First, one associates with every Lie algebra $\mathfrak{g}$, the **enveloping algebra** $\mathrm{U}(\mathfrak{g})$ defined as the quotient of the tensor algebra $\mathrm{T}(\mathfrak{g})$ by the two-sided ideal generated by the elements

$$x \otimes y - y \otimes x - [x,y], \quad x, y \in \mathfrak{g}.$$

Then $\mathrm{U}(\mathfrak{g})$ is an associative algebra with an identity element; it is commutative if and only if $\mathfrak{g}$ is commutative. The natural map $\alpha : \mathfrak{g} \to \mathrm{U}(\mathfrak{g})$ is the universal homomorphism of Lie algebras from $\mathfrak{g}$ to an associative algebra (viewed as a Lie algebra via the commutator map). If $\mathfrak{g}$ is finite-dimensional with basis $x_1, \ldots, x_n$, then the monomials

$$\alpha(x_1)^{i_1} \cdots \alpha(x_n)^{i_n} \quad (i_1, \ldots, i_n \geq 0)$$

form a basis of $\mathrm{U}(\mathfrak{g})$ by the Poincaré–Birkhoff–Witt theorem (see for example [24, Thm. 10.36]). In particular, α is injective.

Next, assume that $p > 0$ and consider a restricted Lie algebra $\mathfrak{g}$ with pth power map $x \mapsto x^{[p]}$. The **restricted enveloping algebra** $\mathrm{U}^{[p]}(\mathfrak{g})$ is the quotient of $\mathrm{U}(\mathfrak{g})$ by the ideal generated by the elements

$$\alpha(x)^p - \alpha(x^{[p]}), \quad x \in \mathfrak{g}$$

(these are contained in the center of $\mathrm{U}(\mathfrak{g})$ in view of (b)). As above, $\mathrm{U}^{[p]}(\mathfrak{g})$ is an associative algebra with an identity element, equipped with a map $\beta : \mathfrak{g} \to \mathrm{U}^{[p]}(\mathfrak{g})$ which is the universal homomorphism of restricted Lie algebras from $\mathfrak{g}$ to an associative algebra (viewed as a restricted Lie algebra via the commutator and the pth power maps). If $\mathfrak{g}$ is finite-dimensional with basis $x_1, \ldots, x_n$ as above, then the monomials

$$\beta(x_1)^{i_1} \cdots \beta(x_n)^{i_n} \quad (0 \leq i_1, \ldots, i_n \leq p - 1)$$

form a basis of $\mathrm{U}^{[p]}(\mathfrak{g})$ (see [6, Prop. II.7.3.6] or [24, Thm. 10.40]). In particular, $\mathrm{U}^{[p]}(\mathfrak{g})$ is finite-dimensional; we have $\dim \mathrm{U}^{[p]}(\mathfrak{g}) = p^{\dim(\mathfrak{g})}$. Moreover, $\mathrm{U}^{[p]}(\mathfrak{g})$ is commutative if and only if $\mathfrak{g}$ is commutative.

As a consequence, every finite-dimensional restricted Lie algebra $\mathfrak{g}$ is equipped with a faithful finite-dimensional representation, namely, its representation in $\mathrm{U}^{[p]}(\mathfrak{g})$ by left multiplication. This yields:

Proposition 1.4.6. *Every finite-dimensional restricted Lie algebra is isomorphic to a restricted Lie subalgebra of $\mathfrak{gl}_n$ for some n.*

We also record the following easy result, see Corollary 1.4.25 for an application.

Lemma 1.4.7. *Every nonzero finite-dimensional restricted Lie algebra contains a restricted Lie subalgebra of dimension 1.*

Proof By Proposition 1.4.6, it suffices to show the assertion for a Lie subalgebra $\mathfrak{g} \subset \mathfrak{gl}_n$, stable by the pth power map.

We first consider the case where $\mathfrak{g}$ consists of nilpotent endomorphisms. Then there exists a nonzero $x \in \mathfrak{g}$ such that $x^p = 0$, and hence kx is the desired subalgebra.

So we may assume that $\mathfrak{g}$ contains a non-nilpotent element x. We have $x = y + z$ where y is diagonalizable, z is nilpotent and y, z commute; thus, $y \neq 0$. Then $x^{p^n} = y^{p^n}$ for $n \gg 0$, and hence we may assume that x is diagonalizable.

Replacing x with a scalar multiple, we may further assume that 1 is an eigenvalue of x. If all its eigenvalues are in the prime field $\mathbb{F}_p$, then $x^p = x$ and hence kx is the desired subalgebra. Otherwise, $x^p - x$ is a nonzero diagonalizable element of $\mathfrak{g}$ and $\mathrm{Ker}(x) \subsetneq \mathrm{Ker}(x^p - x)$. Iterating this argument completes the proof. □

1.4.3 Zariski tangent spaces

We begin with a slight generalization of the notion of derivation of an algebra: given an algebra homomorphism $u : A \to B$, we say that a linear map $D : A \to B$ is a **derivation** if it satisfies the Leibniz rule: $D(a_1 a_2) = u(a_1)D(a_2) + D(a_1)u(a_2)$ for all $a_1, a_2 \in A$. The set of such derivations is a B-module, denoted by $\mathrm{Der}(A, B)$.

Derivations may be viewed as "infinitesimal algebra homomorphisms". More specifically, recall the algebra of dual numbers, $k[\varepsilon] = k[T]/(T^2)$. For any algebra A, we set $A[\varepsilon] = A \otimes k[\varepsilon]$. We then have the following result, whose proof is a direct verification.

Lemma 1.4.8. *Let $u : A \to B$ be an algebra homomorphism, and $D : A \to B$ a linear map. Then D is a derivation if and only if $u + \varepsilon D : A \to B[\varepsilon]$ is an algebra homomorphism.*

We will mostly consider the case where $B = k$, and view $\mathrm{Der}(A, k)$ as a subspace of the dual vector space A^*. This subspace can be described as follows:

Lemma 1.4.9. *Let $f : A \to k$ be an algebra homomorphism with kernel $\mathfrak{m}$, so that $A/\mathfrak{m} = k$. Then the assignment $D \in \mathrm{Der}(A, k) \mapsto D|_{\mathfrak{m}} \in \mathfrak{m}^*$ induces an isomorphism of vector spaces $\mathrm{Der}(A, k) \xrightarrow{\sim} (\mathfrak{m}/\mathfrak{m}^2)^*$.*

Proof Since $A = k \oplus \mathfrak{m}$, every $D \in \mathrm{Der}(A, k)$ is uniquely determined by $D|_{\mathfrak{m}}$. Moreover, $D|_{\mathfrak{m}^2} = 0$ by the Leibniz rule, and hence $D|_{\mathfrak{m}}$ factors through a unique linear map $\delta : \mathfrak{m}/\mathfrak{m}^2 \to k$. Conversely, given such a map δ, let $D : A \to k$ be the linear map such that $D(1) = 0$ and

$D(a) = \delta(\bar{a})$ for any $a \in \mathfrak{m}$ with image $\bar{a} \in \mathfrak{m}/\mathfrak{m}^2$. Then one may readily check that D is a derivation. □

Definition 1.4.10. A **vector field** on an affine scheme X is a derivation of the algebra $A = \mathcal{O}(X)$.

The **Zariski tangent space** of X at $x \in X(k)$ is the vector space

$$T_x(X) = (\mathfrak{m}/\mathfrak{m}^2)^*,$$

where $\mathfrak{m}$ denotes the kernel of the homomorphism $x : A \to k$.

The composition of the map $\mathrm{Der}(A) \to \mathrm{Der}(A, A/\mathfrak{m}) = \mathrm{Der}(A, k)$, $D \mapsto x \circ D$ with the isomorphism $\mathrm{Der}(A, k) \xrightarrow{\sim} T_x(X)$ (Lemma 1.4.9) is the **evaluation map**

$$\mathrm{ev}_x : \mathrm{Der}(A) \longrightarrow T_x(X).$$

If X is a finite scheme, then Theorem 1.2.13 yields an isomorphism $T_x(X) \simeq (\mathfrak{m}_x/\mathfrak{m}_x^2)^*$, where $\mathfrak{m}_x$ denotes the maximal ideal of the local algebra $\mathcal{O}_{X,x}$. Also, the dimension of $T_x(X)$ is the minimal number of generators of this algebra in view of Lemma 1.2.12.

We will obtain an interpretation of the Zariski tangent space in terms of "infinitesimal calculus" on schemes. We keep the setting of Definition 1.4.10. By Lemma 1.4.8, we may identify $\mathrm{Der}(A, k)$ with the set of algebra homomorphisms $\varphi : A \to k[\varepsilon]$ such that $\pi \circ \varphi = x$, where π denotes the algebra homomorphism $k[\varepsilon] \to k$, $\varepsilon \mapsto 0$. This identifies $T_x(X)$ with the fiber at x of the map $X(\pi) : X(k[\varepsilon]) \to X(k)$. Also, we denote by σ the algebra homomorphism $k \to k[\varepsilon]$. Then $\pi \circ \sigma = \mathrm{id}$, and hence $X(\sigma)$ is a section of $X(\pi)$; it sends x to the origin of $T_x(X)$.

Next, consider a morphism of affine schemes $f : X \to Y$ and let $y = f(x) \in Y(k)$. Then we have a commutative square

$$\begin{tikzcd}
X(k[\varepsilon]) \arrow[r, "f(k[\varepsilon])"] \arrow[d, "X(\pi)"'] & Y(k[\varepsilon]) \arrow[d, "Y(\pi)"] \\
X(k) \arrow[r, "f(k)"] & Y(k),
\end{tikzcd}$$

and hence a map

$$df_x : T_x(X) \longrightarrow T_y(Y),$$

the **differential** of f at x. The algebra homomorphism $f^* : \mathcal{O}(Y) \to \mathcal{O}(X)$ induces linear maps $\mathfrak{m}_y^n \to \mathfrak{m}_x^n$ for all positive integers n, and hence a linear map $\mathfrak{m}_y/\mathfrak{m}_y^2 \to \mathfrak{m}_x/\mathfrak{m}_x^2$. One may readily check that the transpose of the latter map is the differential df_x. Also, differentials satisfy the **chain rule**: for any morphisms of affine schemes

$$X \xrightarrow{f} Y \xrightarrow{g} Z, \quad x \longmapsto y \longmapsto z,$$

we have $d(g \circ f)_x = dg_y \circ df_x$.

For any two affine schemes X, Y and any $x \in X(k)$, $y \in Y(k)$, we have a natural isomorphism

$$T_{(x,y)}(X \times Y) \xrightarrow{\sim} T_x(X) \times T_y(Y) \tag{1.16}$$

given by $(d(\mathrm{pr}_X)_x, d(\mathrm{pr}_Y)_y)$.

If G is an affine group scheme, then $G(k[\varepsilon])$ is a group equipped with a homomorphism $G(\pi) : G(k[\varepsilon]) \to G(k)$ with kernel $T_e(G)$, and with a homomorphism $G(\sigma) : G(k) \to G(k[\varepsilon])$ such that $G(\pi) \circ G(\sigma) = \mathrm{id}$. As a consequence, we have

$$G(k[\varepsilon]) = T_e(G) \rtimes G(k). \tag{1.17}$$

Moreover, every homomorphism of affine group schemes $f : G \to H$ yields a homomorphism of (abstract) groups $f(k[\varepsilon]) : G(k[\varepsilon]) \to H(k[\varepsilon])$, which restricts to the differential $df_e : T_e(G) \to T_e(H)$. If f is the immersion of a closed subgroup scheme, then df_e is injective. In the next subsection, we will equip $T_e(G)$ with the structure of a (restricted) Lie algebra, and show that df_e is a homomorphism of such algebras.

1.4.4 The Lie algebra of an affine group scheme

Let G be an affine group scheme, and $A = \mathcal{O}(G)$ with comultiplication map Δ.

Definition 1.4.11. A derivation D of A is **left invariant** if the diagram

$$\begin{tikzcd}
A \arrow[r, "D"] \arrow[d, "\Delta"'] & A \arrow[d, "\Delta"] \\
A \otimes A \arrow[r, "\mathrm{id}\otimes D"] & A \otimes A
\end{tikzcd}$$

commutes.

It is easy to check that the left invariant derivations form a restricted Lie subalgebra $\mathrm{Der}^G(A)$ of $\mathrm{Der}(A)$.

Proposition 1.4.12. *The evaluation map* $\mathrm{ev}_e : \mathrm{Der}(A) \to T_e(G)$ *restricts to an isomorphism*

$$\mathrm{Der}^G(A) \xrightarrow{\sim} T_e(G). \tag{1.18}$$

Proof Let $D \in \mathrm{Der}(A)$. Then D is left invariant if and only if the diagram

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "\Delta"'] & A[\varepsilon] \arrow[d, "\Delta[\varepsilon]"] \\ A \otimes A \arrow[r, "\mathrm{id}\otimes\varphi"] & A \otimes A[\varepsilon] \end{tikzcd}$$

commutes, where $\varphi = \mathrm{id} + \varepsilon D$. This is equivalent to the commutativity of the dual diagram

$$\begin{tikzcd} G \times G \times \mathrm{Spec}(k[\varepsilon]) \arrow[r, "\mathrm{id}\times\psi"] \arrow[d, "\mu\times\mathrm{id}"'] & G \times G \arrow[d, "\mu"] \\ G \times \mathrm{Spec}(k[\varepsilon]) \arrow[r, "\psi"] & G \end{tikzcd}$$

where $\psi : G \times \mathrm{Spec}(k[\varepsilon]) \to G$ is the morphism of affine schemes corresponding to the algebra homomorphism $\varphi : A \to A[\varepsilon]$. In turn, this is equivalent to the equality $\psi(xy, z) = x\psi(y, z)$ for any algebra R, any $x, y \in G(R)$ and any $z \in \mathrm{Spec}(k[\varepsilon])(R) = \mathrm{Hom}_{\mathrm{alg}}(R, k[\varepsilon])$. But this amounts to the equality $\psi(x, z) = x\psi(e, z)$ for any R and $x \in G(R)$, where $\psi(e, z) \in \mathrm{Hom}(\mathrm{Spec}(k[\varepsilon]), G) = G(k[\varepsilon])$. As $\psi \circ (\mathrm{id}, \pi^*) = \mathrm{id}$, we have $\psi(e, z) \in \mathrm{Ker}(G(\pi))$. So $\psi(e, z) \in T_e(G)$; this yields the assertion. □

The above proposition is a key ingredient in the proof of a central result of the theory:

Theorem 1.4.13. *If* $p = 0$ *then every finite group scheme is reduced.*

Proof By Theorem 1.3.13, it suffices to show that every infinitesimal group scheme G is trivial. Let $\mathfrak{m}$ be the maximal ideal of $\mathcal{O}(G) = A$; then $T_e(G) = (\mathfrak{m}/\mathfrak{m}^2)^*$. By Proposition 1.4.12, there exist $D_1, \dots, D_m \in \mathrm{Der}^G(A)$ such that $\mathrm{ev}_e(D_1), \dots, \mathrm{ev}_e(D_m)$ form a basis of $T_e(G)$. So we may choose $a_1, \dots, a_m \in \mathfrak{m}$ such that the images $\bar{a}_1, \dots, \bar{a}_m \in \mathfrak{m}/\mathfrak{m}^2$ form the dual basis. Equivalently, $D_i(a_j)(e) = \delta_{i,j}$ for $1 \le i, j \le m$.

Consider the algebra $R = k[[T_1, \dots, T_m]]$ consisting of the formal power series $\sum_{i_1,\dots,i_m} c_{i_1,\dots,i_m} T_1^{i_1} \cdots T_m^{i_m}$, where $i_1, \dots, i_m$ run over the nonnegative integers, and $c_{i_1,\dots,i_m} \in k$. Then R is a local k-algebra with maximal ideal $(T_1,\dots,T_m)$ (consisting of the series with constant term 0) and residue field k. Each quotient $R/(T_1,\dots,T_m)^n$ is isomorphic to the truncated polynomial ring $k[T_1,\dots,T_m]/(T_1,\dots,T_m)^n$, a local finite-dimensional algebra.

We have a linear map defined via "Taylor series expansion"

$$u : A \longrightarrow R, \quad a \longmapsto \sum_{i_1,\dots,i_m\geq 0} (D_1^{i_1}\cdots D_m^{i_m} a)(e) \frac{T_1^{i_1}\cdots T_m^{i_m}}{i_1!\cdots i_m!}.$$

Using the formula (1.14), one may check that u is an algebra homomorphism. Also, we have $u(a_i) \equiv T_i \mod (T_1,\dots,T_m)^2$ for $i = 1,\dots,m$. In view of Lemma 1.2.12, it follows that the composition of u with the quotient map $R \to R/(T_1,\dots,T_m)^n$ is surjective for all $n \geq 0$. But A is finite-dimensional, and the dimension of $R/(T_1,\dots,T_m)^n$ is arbitrarily large if $m \geq 1$ and $n \gg 0$. So we must have $m = 0$, i.e., $A = k$. □

Theorem 1.4.13 is a special case of **Cartier's theorem**: if $p = 0$ then every algebraic group is reduced (see [25, p. 101, Thm.], from which the above proof is borrowed).

We now return to a finite group scheme G in arbitrary characteristic.

Definition 1.4.14. The **Lie algebra** $\mathrm{Lie}(G)$ is the Zariski tangent space $T_e(G)$ equipped with the restricted Lie algebra structure obtained via the isomorphism (1.18).

Example 1.4.15. Let $G = \mathbb{G}_a$. Then $A = k[T]$ and $\mathrm{Der}(A) = A\, d/dT$. One may readily check that $\mathrm{Der}^G(A) = k\, d/dT$. Thus, $\mathrm{Lie}(G) \simeq k$ with trivial pth power map.

Next, let $G = \mathbb{G}_m$. Then $A = k[T, T^{-1}]$ and $\mathrm{Der}(A) = A\, d/dT = A\, T d/dT$; moreover, $\mathrm{Der}^G(A) = k\, T d/dT$. So $\mathrm{Lie}(G) \simeq k$ with pth power map $x \mapsto x^p$.

Every homomorphism of affine group schemes $f : G \to H$ induces a linear map

$$\mathrm{Lie}(f) = df_e : \mathrm{Lie}(G) = T_e(G) \longrightarrow T_e(H) = \mathrm{Lie}(H).$$

Moreover, every G-action α on an affine scheme $X = \mathrm{Spec}(A)$ induces an action of the group $G(k[\varepsilon])$ on the algebra $A[\varepsilon]$ by $k[\varepsilon]$-algebra automorphisms, which lifts the $G(k)$-action on A by algebra automorphisms (Remark 1.3.10). Thus, for any $\xi \in T_e(G) = \mathrm{Ker}(G(\pi) : G(k[\varepsilon]) \to G(k))$, we obtain a $k[\varepsilon]$-automorphism of $A[\varepsilon]$ lifting id, and hence an algebra homomorphism $A \to A[\varepsilon]$, $a \mapsto a + \varepsilon D_\xi$. Then D_ξ is a derivation (Lemma

1.4.8), so that we obtain a map

$$\alpha' : T_e(G) \longrightarrow \mathrm{Der}(A), \quad \xi \longmapsto D_\xi.$$

Proposition 1.4.16. *With the above notation,* $\mathrm{Lie}(f)$ *and* α' *are homomorphisms of restricted Lie algebras.*

This follows from an alternative description of the restricted Lie algebra structure on $T_e(G)$ that we now sketch. The G-action on itself by conjugation fixes e, and hence induces a linear representation

$$\mathrm{Ad} : G \longrightarrow \mathrm{GL}_{T_e(G)},$$

the **adjoint representation** (see [24, Cor. 8.10]). The differential of Ad at e may be identified with a linear map

$$\mathrm{ad} : T_e(G) \longrightarrow \mathfrak{gl}(T_e(G)).$$

In fact, this map equips $T_e(G)$ with a restricted Lie algebra structure such that α' is a homomorphism of restricted Lie algebras for any G-action α (see [6, II.4.4.4, II.4.4.5, II.7.3.4]). In particular, the G-action on itself by right multiplication induces a homomorphism of restricted Lie algebras $T_e(G) \to \mathrm{Der}(\mathcal{O}(G))$; its image is $\mathrm{Der}^G(\mathcal{O}(G))$ by [6, II.4.4.6]). This completes the proof of Proposition 1.4.16 in view of the equivariance of f relative to the conjugation actions.

If $G = \mathrm{GL}_n$, then $T_e(G)$ is the vector space $\mathfrak{gl}_n$ of $n \times n$ matrices, and the adjoint representation is the conjugation action again. Its differential at e is the adjoint representation of $\mathfrak{gl}_n$ (see e.g. [24, Thm. 10.23]) and hence $\mathrm{Lie}(\mathrm{GL}_n) = \mathfrak{gl}_n$ as restricted Lie algebras.

Also, the Lie algebra of any closed subgroup scheme $H \leq G$ is a restricted Lie subalgebra of $\mathrm{Lie}(G)$. We illustrate this on the following:

Example 1.4.17. Let $G = \mu_n$, so that $A = k[T](T^n - 1)$. If $p = 0$ or n is prime to p, then A is reduced and hence $\mathrm{Lie}(G) = 0$ (e.g. by Lemma 1.4.4). On the other hand, if $p > 0$ divides n, then the inclusion $G \leq \mathbb{G}_m$ yields the equality $\mathrm{Lie}(G) = \mathrm{Lie}(\mathbb{G}_m)$ for dimension reasons. So $\mathrm{Lie}(G) = k$ with pth power map $x \mapsto x^p$.

Next, let $G = \alpha_p$. Then similarly, the inclusion $G \leq \mathbb{G}_a$ yields that $\mathrm{Lie}(G) = k$ with trivial pth power map.

Example 1.4.18. Let B be a finite-dimensional algebra. By assigning to any algebra R the automorphism group of the R-algebra $R \otimes B$, one obtains a group functor Aut_B. One may readily check that this group functor is represented by a closed subgroup scheme of GL_B, that we will still denote by Aut_B. We have $\mathrm{Aut}_B(k) = \mathrm{Aut}(B)$ (the automorphism group of B), and $\mathrm{Lie}(\mathrm{Aut}_B) = \mathrm{Der}(B)$ as follows from Lemma 1.4.8.

If B is reduced of dimension n, then $B \simeq k^n$ and hence $\mathrm{Aut}(B)$ is isomorphic to the symmetric group S_n (permuting the idempotents of B). Together with Lemma 1.4.4 (iii), it follows that $\mathrm{Aut}_B \simeq S_n$ as well.

On the other hand, if B is nonreduced, then $\mathrm{Aut}(B)$ is infinite. Indeed, using Theorem 1.2.13, we may assume that B is local with maximal ideal $\mathfrak{m}$; then $\mathrm{Aut}(B) \xrightarrow{\sim} \mathrm{Aut}(\mathfrak{m})$. Denote by n the smallest positive integer such that $\mathfrak{m}^n = 0$. If $n = 2$ then $\mathrm{Aut}(\mathfrak{m}) \simeq \mathrm{GL}(\mathfrak{m})$ is infinite. Otherwise, consider a linear map $f : \mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{m}^{n-1} \subset \mathfrak{m}^2$ as in the proof of Lemma 1.4.4 (iii). Then one may check that the assignment $\mathfrak{m} \to \mathfrak{m}$, $x \mapsto x+f(\bar{x})$ yields an automorphism u_f of $\mathfrak{m}$. Moreover, the assignment $f \mapsto u_f$ yields an injective homomorphism $\mathrm{Hom}(\mathfrak{m}/\mathfrak{m}^2, \mathfrak{m}^{n-1}) \to \mathrm{Aut}(\mathfrak{m})$, where the left-hand side is viewed as an additive group. Thus, $\mathrm{Aut}(\mathfrak{m})$ is infinite in this casee too, and hence Aut_B is infinite as well.

Also, Aut_B may be nonreduced if $p > 0$. Take indeed $B = k[T]/(T^p)$ and denote by t the image of T in B, as in Example 1.4.3. Then for any algebra R, the group $\mathrm{Aut}_B(R)$ consists of the maps

$$t \longmapsto a_0 + a_1 t + \cdots + a_{p-1} t^{p-1},$$

where $a_0, \ldots, a_{p-1} \in R$ satisfy $a_0^p = 0$ and $a_1 \in R^\times$. In particular, $\mathrm{Aut}_B(k) = \mathrm{Aut}(B)$ consists of the maps $t \mapsto a_1 t + \cdots + a_{p-1} t^{p-1}$, where $a_1 \in k^\times$ and $a_2, \ldots, a_{p-1} \in k$. So the reduced subgroup scheme $\mathrm{Aut}_{B,\mathrm{red}}$ is the proper closed subscheme of Aut_B with ideal (a_0).

1.4.5 The relative Frobenius morphism

In this subsection, we assume that $\mathrm{char}(k) = p > 0$. Let A be an algebra; then the Frobenius map

$$F = F_A : A \longrightarrow A, \quad a \longmapsto a^p.$$

is a ring endomorphism. But F is not an algebra endomorphism, since $F(ta) = t^p F(a)$ for all $t \in k$, $a \in A$. To correct this, we define a new algebra structure on A via $t \cdot a = t^{1/p} a$. The resulting algebra will be denoted by $A^{(p)}$. Then we obtain an algebra homomorphism

$$F_{A/k} : A^{(p)} \longrightarrow A, \quad a \longmapsto a^p,$$

or equivalently a morphism of affine schemes

$$F_{X/k} : X \longrightarrow X^{(p)},$$

where $X = \mathrm{Spec}(A)$ and $X^{(p)} = \mathrm{Spec}(A^{(p)})$. We say that $F_{X/k}$ is the **relative Frobenius morphism**. If A is finite-dimensional, then $A^{(p)}$ is finite-dimensional as well, and $\dim(A^{(p)}) = \dim(A)$; thus, $F_{X/k}$ is a morphism of finite schemes.

Next, let $f : X \to Y$ be a morphism of affine schemes and denote by $u : \mathcal{O}(Y) = B \to A$ the corresponding algebra homomorphism. Then we have $F_A \circ u = u \circ F_B$. As a consequence, u induces a homomorphism $u^{(p)} : B^{(p)} \to A^{(p)}$ such that $F_{A/k} \circ u^{(p)} = u \circ F_{B/k}$. Equivalently, we have a commutative diagram of affine schemes

$$\begin{tikzcd}
X \arrow[r, "F_{X/k}"] \arrow[d, "f"'] & X^{(p)} \arrow[d, "f^{(p)}"] \\
Y \arrow[r, "F_{Y/k}"] & Y^{(p)}
\end{tikzcd}$$

Also, we have a natural isomorphism of algebras

$$A^{(p)} \otimes B^{(p)} \xrightarrow{\sim} (A \otimes B)^{(p)},$$

and hence the relative Frobenius morphism commutes with products. Thus, for any affine group scheme G, there exists a natural structure of affine group scheme on $G^{(p)}$ such that $F_{G/k}$ is a homomorphism. Its kernel is the **Frobenius kernel**; we denote it by G_1. If G is finite, then $G^{(p)}$ is finite and we have $|G| = |G^{(p)}|$.

This construction can be iterated: given a positive integer n, we replace p with p^n and F with $F^n : A \to A$, $a \mapsto a^{p^n}$. We then denote by $A^{(p^n)}$ the ring A equipped with an algebra structure via $t \cdot a = t^{1/p^n} a$. This yields a homomorphism $F^n_{A/k} : A^{(p^n)} \to A$, and hence a morphism

$$F^n_{X/k} : X \longrightarrow X^{(p^n)},$$

the **nth iterated relative Frobenius morphism**. The above properties of the relative Frobenius morphism extend to this setting. So for any affine group scheme G, we obtain a homomorphism

$$F^n_{G/k} : G \longrightarrow G^{(p^n)},$$

where $G^{(p^n)}$ is an affine group scheme; if G is finite, then $G^{(p^n)}$ is finite of the same order. The kernel of $F^n_{G/k}$ is the **nth Frobenius kernel** G_n.

This notion gives back some of the examples of §1.2.1:

Example 1.4.19. If G is the multiplicative group $\mathbb{G}_m$, then G_n is the group scheme μ_{p^n} (the kernel of the p^nth power map), of order p^n.

Also, if G is the additive group $\mathbb{G}_a$, then $G_1 = \alpha_p$. More generally, G_n is denoted by α_{p^n}; it has order p^n as well.

Finally, the nth Frobenius kernel of an elliptic curve E has order p^n again. Moreover, we have

$$E_n \simeq \begin{cases} \mu_{p^n} & \text{if } E \text{ is ordinary,} \\ \alpha_{p^n} & \text{if } E \text{ is supersingular} \end{cases}$$

(see [25, §22, Thm.]).

In these three examples, G_n is contained in the kernel of the multiplication by p^n. This is a general fact for commutative group schemes, see [6, IV.3.4.10].

We now record some properties of the iterated relative Frobenius morphism of affine schemes:

Lemma 1.4.20. *Let X be an affine scheme, and n a positive integer.*

(i). *The morphism $F^n_{X/k}$ is bijective on k-points.*

(ii). *For any $x \in X(k)$, the fiber of $F^n_{X/k}$ at $y = F^n_{X/k}(x)$ satisfies*

$$\mathcal{O}(X_y) = \mathcal{O}(X)/(f^{p^n}, f \in \mathfrak{m}_x),$$

where $\mathfrak{m}_x$ denotes the maximal ideal of x.

(iii). *Assume in addition that X is finite. Then $F^n_{X/k}$ is an isomorphism if and only if X is reduced.*

Proof (i) Let $A = \mathcal{O}(X)$. We have to show that every algebra homomorphism $f : A^{(p)} \to k$ extends uniquely to an algebra homomorphism $A \to k$. The uniqueness follows from the fact that every element of k has a unique pth root. For the existence, let $\mathfrak{m} = \operatorname{Ker}(f)$ and $B = A/\mathfrak{m}A$. Then the algebra B has a maximal ideal, and hence there exists an algebra homomorphism $g : B \to K$, where K is a field extension of k. By construction, we have $K^p \subset k$ and hence $K = k$. So $g : B \to k$ yields the desired extension.

(ii) This follows readily from the fact that the ideal of X_y in $\mathcal{O}(X)$ is generated by $(F^n_{X/k})^*(\mathfrak{m}_x)$.

(iii) Using Theorem 1.2.13, we may assume that A is local. If $A = k$ then $(F^n_{X/k})^* = \mathrm{id}$. Otherwise, A has nonzero nilpotent elements, and hence there exists $a \in A$ such that $a^p = 0 \neq a$. Thus, $(F^n_{X/k})^*$ is not injective. □

Lemma 1.4.21. *Let G be an affine group scheme. Then the iterated*

Frobenius kernels G_n form an increasing sequence of infinitesimal subgroup schemes of G. Moreover, $\mathrm{Lie}(G_1) = \mathrm{Lie}(G_2) = \cdots = \mathrm{Lie}(G)$.

Assuming in addition that G is finite, we have:

(i). *G_n is trivial if and only if G is reduced.*

(ii). *$G_n \leq G^0$ with equality if and only if $f^{p^n} = 0$ for all $f \in \mathfrak{m}$, where $\mathfrak{m}$ denotes the maximal ideal of e in $\mathcal{O}(G)$.*

(iii). *$G_n = G^0$ for $n \gg 0$.*

Proof Recall that G_n is the fiber of $F^n_{G/k}$ at e. By Lemma 1.4.20, it follows that e is the unique k-point of G_n, and hence G_n is infinitesimal.

Using Lemma 1.4.20 again, we have

$$\mathcal{O}(G_n) = \mathcal{O}(G)/(f^{p^n}, f \in \mathfrak{m}). \tag{1.19}$$

Moreover, the ideals $(f^{p^n}, f \in \mathfrak{m})$ form a decreasing sequence, and hence the closed subschemes G_n form an increasing sequence.

Also, recall that $\mathrm{Lie}(G) = T_e(G) = T_e(G^0) = (\mathfrak{m}/\mathfrak{m}^2)^*$. Likewise, we have $\mathrm{Lie}(G_n) = (\bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2)^*$, where $\bar{\mathfrak{m}}$ denotes the maximal ideal of e in G_n. So

$$\bar{\mathfrak{m}} = \mathfrak{m}/(f^{p^n}, f \in \mathfrak{m}) \subset \mathcal{O}(G)/(f^{p^n}, f \in \mathfrak{m}) = \mathcal{O}(G_n).$$

As $f^{p^n} \in \mathfrak{m}^2$ for all $f \in \mathfrak{m}$, the natural map $\mathfrak{m}/\mathfrak{m}^2 \to \bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2$ is an isomorphism. Thus, $\mathrm{Lie}(G_n) = \mathrm{Lie}(G)$; this yields the first assertion.

We now assume that G is finite. Since G_n is infinitesimal, it is a subgroup scheme of G^0 by Theorem 1.3.13. So we may replace G with G^0, i.e., assume that G is infinitesimal.

To show (i), it suffices to check that G is trivial if G_n is trivial. But then the ideal $\mathfrak{m}$ is generated by its p^nth powers, and hence is zero by Lemma 1.2.12.

The remaining assertions from (ii) and (iii) follow from the isomorphism (1.19) and the vanishing of $\mathfrak{m}^n$ for $n \gg 0$ (Lemma 1.2.11). □

Definition 1.4.22. Let G be an infinitesimal group scheme. If G is nontrivial, then its **height** $\mathrm{ht}(G)$ is the smallest integer $n \geq 1$ such that $G_n = G$. We set $\mathrm{ht}(G) = 0$ if G is trivial.

By Lemma 1.4.21, the height of G exists and satisfies

$$\mathrm{ht}(G) = \min\{n \mid f^{p^n} = 0 \text{ for all } f \in \mathfrak{m}\},$$

where $\mathfrak{m}$ denotes the maximal ideal of the local algebra $\mathcal{O}(G)$.

Theorem 1.4.23. *Let G be an infinitesimal group scheme. Then we have* $\mathrm{ht}(G) \leq 1$ *if and only if there exists an isomorphism of algebras*

$$\mathcal{O}(G) \simeq k[T_1, \ldots, T_n]/(T_1^p, \cdots, T_n^p). \tag{1.20}$$

Moreover, the assignment $G \mapsto \mathrm{Lie}(G)$ yields an equivalence between the categories of infinitesimal group schemes of height at most 1, and of finite-dimensional restricted Lie algebras.

We refer to [24, Chap. 11.h] for the broad lines of the proof, and to [6, II.7.4] for the full details. We will only sketch the construction of a quasi-inverse functor: given a finite-dimensional restricted Lie algebra $\mathfrak{g}$, one considers its restricted enveloping algebra $\mathrm{U} = \mathrm{U}^{[p]}(\mathfrak{g})$ (§1.4.2), and equips it with algebra homomorphisms

$$\Delta : \mathrm{U} \longrightarrow \mathrm{U} \otimes \mathrm{U}, \quad x \in \mathfrak{g} \longmapsto x \otimes 1 + 1 \otimes x,$$

$$S : \mathrm{U} \longrightarrow \mathrm{U}, \quad x \in \mathfrak{g} \longmapsto -x,$$

$$\varepsilon : \mathrm{U} \longrightarrow k, \quad x \in \mathfrak{g} \longmapsto 0.$$

Then U is a finite-dimensional Hopf algebra, which is co-commutative (i.e., the image of Δ is fixed pointwise by the involution $x \otimes y \mapsto y \otimes x$ of $U \otimes U$), but not necessarily commutative. Thus, the dual vector space is a finite-dimensional commutative Hopf algebra, which yields a finite group scheme $G(\mathfrak{g})$. One then checks that $G(\mathfrak{g})$ is infinitesimal with Lie algebra $\mathfrak{g}$.

The equivalence of categories of Theorem 1.4.23 extends to actions of group schemes: given an infinitesimal group scheme G of height 1 and a scheme $X = \mathrm{Spec}(A)$, the G-actions on X correspond bijectively to the homomorphisms of restricted Lie algebras $\mathrm{Lie}(G) \to \mathrm{Der}(A)$ via $\alpha \mapsto \alpha'$ (see [6, II.7.3.10]). In view of Example 1.4.17, it follows that the actions of μ_p (resp. α_p) correspond bijectively to the vector fields D such that $D^p = D$ (resp. $D^p = 0$).

We now present applications of Theorem 1.4.23 to the structure of finite group schemes:

Corollary 1.4.24. *Let G be an infinitesimal group scheme of height 1. Then we have $|G| = p^n$, where $n = \dim(\mathrm{Lie}(G))$.*

Proof The isomorphism (1.20) implies that $|G| = \dim(\mathcal{O}(G)) = p^n$, since the monomials $T_1^{i_1} \cdots T_n^{i_n}$, where $0 \leq i_1, \ldots, i_n \leq p-1$, yield a basis of $k[T_1, \ldots, T_n]/(T_1^p, \ldots, T_n^p)$. Also, this isomorphism identifies the maximal ideal $\mathfrak{m}$ of $\mathcal{O}(G)$ with the image of the maximal ideal

$(T_1, \dots, T_n)$ of $k[T_1, \dots, T_n]$. Since $(T_1^p, \dots, T_n^p) \subset (T_1, \dots, T_n)^2$, this yields in turn an isomorphism $\mathfrak{m}/\mathfrak{m}^2 \simeq (T_1, \dots, T_n)/(T_1, \dots, T_n)^2$. Thus, $\dim(\mathrm{Lie}(G)) = \dim(\mathfrak{m}/\mathfrak{m}^2) = n$. □

Corollary 1.4.25. *Every nonreduced finite group scheme contains a subgroup scheme isomorphic to μ_p or α_p.*

Proof This follows by combining Theorem 1.4.23 with Lemmas 1.4.7 and 1.4.21. □

Corollary 1.4.26. *Every finite group scheme of prime order ℓ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ if $\ell \neq p$, and to $\mathbb{Z}/p\mathbb{Z}$, μ_p or α_p if $\ell = p$.*

Proof By Theorem 1.3.13, we have $\mathcal{O}(G) \simeq \mathcal{O}(G^0) \otimes \mathcal{O}(G_{\mathrm{red}})$ as algebras. Counting dimensions, this yields $|G| = |G^0| \cdot |G_{\mathrm{red}}|$. Thus, the assumption that $|G| = \ell$ implies that G is infinitesimal or reduced. In the latter case, we have $G \simeq \mathbb{Z}/\ell\mathbb{Z}$. In the former case, G contains a subgroup scheme H isomorphic to μ_p or α_p by Corollary 1.4.25. Thus, we have $\ell = p$; moreover, the resulting algebra homomorphism $\mathcal{O}(G) \to \mathcal{O}(H)$ is surjective, and hence bijective for dimension reasons. □

Finally, we mention a remarkable structure result for the algebras of infinitesimal group schemes (see [6, Cor. III.3.6.3] or [24, Thm. 11.29]):

Theorem 1.4.27. *Let G be an infinitesimal group scheme. Then there exists an isomorphism of algebras*

$$\mathcal{O}(G) \simeq k[T_1, \dots, T_n]/(T_1^{p^{a_1}}, \dots, T_n^{p^{a_n}}),$$

where $a_1, \dots, a_n$ are positive integers.

By considering a monomial basis of $\mathcal{O}(G)$ as in the proof of Corollary 1.4.24, this yields $|G| = \dim(\mathcal{O}(G)) = p^{a_1 + \cdots + a_n}$. In particular, every infinitesimal group scheme is a p-group. We will obtain an alternative proof of this result in Corollary 1.5.15.

1.5 Quotients

Throughout this section, we consider a finite group scheme G.

Definition 1.5.1. Let X be an affine G-scheme, and $f : X \to Y$ a morphism. We say that f is **G-invariant** if $f(g \cdot x) = f(x)$ for any algebra R and any $g \in G(R)$, $x \in X(R)$.

The invariance condition is equivalent to the equality $f \circ \alpha = f \circ \mathrm{pr}_X$, where $\alpha : G \times X \to X$ denotes the action, and $\mathrm{pr}_X : G \times X \to X$ the projection. In turn, this is equivalent to the equality $\alpha^* \circ f^* = (1 \otimes \mathrm{id})^* \circ f^*$ for the algebra homomorphism $f^* : \mathcal{O}(Y) \to \mathcal{O}(X)$.

Remark 1.5.2. Assume that $p > 0$ and consider an action $G \times X \to X$. Then the induced morphism $G^{(p^n)} \times X^{(p^n)} \to X^{(p^n)}$ is an action as well, and the nth relative Frobenius morphism $F^n_{X/k} : X \to X^{(p^n)}$ is equivariant relative to the homomorphism $F^n_{G/k} : G \to G^{(p^n)}$. Indeed, this follows readily from the functorial properties of relative Frobenius morphisms.

If in addition G is infinitesimal of height n, then $F^n_{X/k}$ is G-invariant.

Observe that every affine G-scheme X is equipped with a G-invariant morphism $q : X \to Y$ which satisfies the following universal property: for any invariant morphism of affine schemes $\varphi : X \to Z$, there exists a unique morphism $\psi : Y \to Z$ such that $\varphi = \psi \circ q$. Indeed, let $A = \mathcal{O}(X)$ and consider the **algebra of invariants**

$$A^G = \{a \in A \mid \alpha^*(a) = \mathrm{pr}_X^*(a)\}.$$

Then the inclusion of A^G into A corresponds to a morphism of affine schemes $q : X \to Y$. Moreover, the morphism φ corresponds to an algebra homomorphism $\mathcal{O}(Z) \to A$ with image contained in A^G. So q satisfies the above universal property. We say that q is the **categorical quotient** of X by G and we denote Y by X/G.

The following properties of the categorical quotient are easily verified:

Lemma 1.5.3. *Let G be a finite group scheme, and X, Y two affine G-schemes with categorical quotients $q_X : X \to X/G$, $q_Y : Y \to Y/G$.*

(i). *Every G-equivariant morphism $f : X \to Y$ induces a morphism $f/G : X/G \to Y/G$ such that $f/G \circ q_X = q_Y \circ f$.*

(ii). *If G acts trivially on Y, then there exists a natural isomorphism*

$$(X \times Y)/G \xrightarrow{\sim} X/G \times Y. \tag{1.21}$$

(iii). *The finite group $G(k)$ acts on X/G^0 and there exists a natural isomorphism*

$$(X/G^0)/G(k) \xrightarrow{\sim} X/G. \tag{1.22}$$

Also, for any algebraic affine G-scheme X, the scheme X/G is algebraic in view of the following:

Theorem 1.5.4. *Let A be a finitely generated G-algebra. Then the algebra of invariants A^G is finitely generated and the A^G-module A is finitely generated as well.*

Proof We may choose $a_1, \ldots, a_m \in A$ such that $A = k[a_1, \ldots, a_m]$.

We first treat the case where G is reduced. Consider the polynomials

$$P_i(T) = \prod_{g \in G} (T - g \cdot a_i) \in A[T] \quad (i = 1, \ldots, m).$$

Then $P_i(a_i) = 0$ and P_i has degree $|G| = N$. Moreover, the coefficients of $P_i(T)$ are G-invariant, since G permutes the $g \cdot a_i$. In other words, $P_i(T) \in A^G[T]$ for all i. Let B denote the subalgebra of A generated by the coefficients of the P_i. Then B is finitely generated and contained in A^G. Moreover, we have $a_i^N \in B + Ba_i + \cdots + Ba_i^{N-1}$ for $i = 1, \ldots, m$, since $P_i(a_i) = 0$. By induction, it follows that $a_i^r \in B + Ba_i + \cdots + Ba_i^{N-1}$ for $r \geq N$ and $i = 1, \ldots, m$. As a consequence, the B-module A is generated by the monomials $a_1^{i_1} \cdots a_m^{i_m}$, where $0 \leq i_1, \ldots, i_m \leq N - 1$. In particular, A is a finite B-module. Using again the finite generation of B, this yields that $A^G \subset A$ is a finite B-module as well. In turn, this yields the assertions in this case.

Next, we treat the case where G is infinitesimal. Let $n = \mathrm{ht}(G)$, then $a^{p^n} \in A^G$ for any $a \in A$ in view of Remark 1.5.2. Thus, $C = k[a_1^{p^n}, \ldots, a_m^{p^n}]$ is a subalgebra of A^G. Also, the C-module A is generated by the monomials $a_1^{i_1} \cdots a_m^{i_m}$, where $0 \leq i_1, \ldots, i_m \leq p - 1$. This yields the assertions by arguing as in the first case.

For an arbitrary finite group scheme G, the algebra A^{G^0} is equipped with an action of $G(k)$ such that $(A^{G^0})^{G(k)} = A^G$. So we conclude by combining the two above cases. □

Remark 1.5.5. Given an affine algebraic G-scheme X, the categorical quotient is an orbit space in the following sense: the natural map $X(k)/G(k) \to (X/G)(k)$ is bijective. Indeed, this is a consequence of [10, Ex. 13.4] if G is reduced. Also, q is bijective if G is infinitesimal (use Lemma 1.4.20 and Remark 1.5.2). This yields the assertion for an arbitrary G in view of Lemma 1.5.3 (iii).

In other words, the set-theoretic fibers of q at k-rational points are exactly the $G(k)$-orbits. But the natural map $X(R)/G(R) \to (X/G)(R)$ is not necessarily bijective for an algebra R. For example, consider the action of μ_n on $\mathbb{A}^1 = \mathrm{Spec}(k[T])$ by multiplication: $x \cdot y = xy$. Then $k[T]^{\mu_n} = k[T^n]$ and hence q is not surjective on (say) $k(T)$-valued points. Also, note that the fiber of q at 0 is the nonreduced scheme $\mathrm{Spec}(k[T]/(T^n))$.

Remark 1.5.6. Invariant theory of finite groups is related to Galois theory as follows. Assume that G is a finite group of automorphisms of an algebra A, which is an integral domain with fraction field K. This yields a G-action on K by field automorphisms; the invariant subfield K^G is easily seen to be the fraction field of A^G. By Galois theory, we have $G = \mathrm{Aut}_{K^G}(K)$ and K is a finite extension of K^G of degree $|G|$. As a consequence, $G = \mathrm{Aut}_{A^G}(A)$ and the A^G-module A has rank $|G|$.

This does not extend to finite group schemes if $p > 0$. For example, consider the action of μ_p on $\alpha_p^n = \alpha_p \times \cdots \times \alpha_p$ (n times) via $y \cdot (x_1, \ldots, x_n) = (yx_1, \ldots, yx_n)$ and form the corresponding semi-direct product $G = \alpha_p^n \rtimes \mu_p$. Then G acts on $\mathbb{A}^1$ via

$$(x_1, \ldots, x_n, y) \cdot t = yt + x_1 + x_2 t^p + \cdots + x_n t^{p^{n-1}}$$

and the algebra of G-invariants of $\mathcal{O}(\mathbb{A}^1) = k[T]$ is $k[T^p]$. So $|G| = p^{n+1}$ and $[K : K^G] = p$ for the induced G-action on $K = k(T)$.

This failure is explained by the fact that the extension K/K^G is purely inseparable for a (functorial) action of an infinitesimal group scheme G on a field K. More specifically, if $\mathrm{ht}(G) \leq n$ then $f^{p^n} \in K^G$ for any $f \in K$ (Remark 1.5.2). In particular, the extension K/K^G has exponent p if $\mathrm{ht}(G) = 1$.

Definition 1.5.7. An action of G on an affine scheme X is **free** if the group $G(R)$ acts freely on the set $X(R)$ for any algebra R.

More specifically, if $g \in G(R)$ and $x \in X(R)$ satisfy $g \cdot x = x$, then $g = e$.

Example 1.5.8. The group scheme G acts freely on itself by left multiplication, and also by right multiplication. But the G-action on itself by conjugation is not free (if G is nontrivial), since this action fixes e.

Remark 1.5.9. Assume that G is a finite group acting faithfully on an affine variety X. Then there exists a nonempty open subset $U \subset X$ which is G-stable (i.e., $g \cdot x \in U$ for all $g \in G$ and $x \in U$) and on which G acts freely. Indeed, the fixed point locus $X^g = \{x \in X \mid g \cdot x = x\}$ is a proper closed subset of X for any $g \in G$. Thus, we may take for U the free locus $X \setminus \bigcup_{g \in G} X^g$.

This does not extend to actions of finite group schemes in view of the example in Remark 1.5.6 (exercise).

Definition 1.5.10. A morphism of affine schemes $f : X \to Y$ is **finite locally free (of rank n)** if the $\mathcal{O}(Y)$-module $\mathcal{O}(X)$ is finitely generated and projective (of constant rank n).

By [10, Ex. 4.12], this is equivalent to the existence of $g_1, \ldots, g_m \in \mathcal{O}(Y)$ such that $(g_1, \ldots, g_m) = \mathcal{O}(Y)$ and the $\mathcal{O}(Y)[\frac{1}{g_i}]$-module $\mathcal{O}(X)[\frac{1}{g_i}]$ is free (of rank n) for $i = 1, \ldots, m$. Here $\mathcal{O}(Y)[\frac{1}{g_i}]$ denotes the localization of $\mathcal{O}(Y)$ by g_i, and likewise for $\mathcal{O}(X)[\frac{1}{g_i}]$.

For example, the projection $\mathrm{pr}_Y : X \times Y \to Y$ is finite locally free if and only if X is finite; then pr_Y has rank $n = \dim(\mathcal{O}(X))$. Also, the immersion $i : X \to X \sqcup Y$ is finite locally free, but not of constant rank if X, Y are nonempty.

Remark 1.5.11. The notion of a finite locally free morphism extends to (not necessarily affine) schemes as follows: a morphism of schemes $f : X \to Y$ is finite locally free if for any affine open subset V of Y, the preimage $U = f^{-1}(V)$ is affine and $f|_U : U \to V$ is finite locally free. For example, given an elliptic curve E with origin 0 and a positive integer n, the morphism $n_E : E \to E$, $x \mapsto nx$ of Example 1.2.3 is finite locally free of rank n^2 (as follows from [14, Ex. IV.4.2]). Thus, the schematic kernel $E[n]$ is a finite group scheme of order n^2.

Theorem 1.5.12. *Let $X = \mathrm{Spec}(A)$ be a scheme of finite type equipped with a free action of G, and $q : X \to X/G = \mathrm{Spec}(A^G)$ the categorical quotient.*

(i). *The morphism q is finite locally free of rank $|G|$.*
(ii). *The morphism $G \times X \to X \times X$, $(g, x) \mapsto (x, g \cdot x)$ induces an isomorphism $G \times X \xrightarrow{\sim} X \times_{X/G} X$.*

The second assertion means that the categorical quotient by a free action of G is a **principal G-bundle** in the sense of topologists.

We refer to [25, §12, Thm. 1] or [24, Thm. B.18] for the proof of the above result, and record an important consequence:

Corollary 1.5.13. *Let $H \leq G$ be a subgroup scheme, and $q : G \to G/H$ the categorical quotient by the action via right multiplication.*

(i). *The morphism q is finite locally free of rank $|H|$.*
(ii). *We have $|G| = [G : H]\,|H|$, where $[G : H] = \dim(\mathcal{O}(G/H)) = \dim(\mathcal{O}(G)^H)$.*
(iii). *The G-action on itself by left multiplication yields a unique action on G/H such that q is equivariant.*

(iv). *If H is normal in G, then G/H has a unique structure of a finite group scheme such that q is a homomorphism.*

Proof (i) This follows from Example 1.5.8 and Theorem 1.5.12.

(ii) By (i), the algebra $\mathcal{O}(G)$ is a projective module of constant rank $|H|$ over its subalgebra $\mathcal{O}(G)^H$. This yields the assertion by counting dimensions.

(iii) Consider the H-action on $G \times G$ via $h \cdot (g_1, g_2) = (g_1, g_2 h^{-1})$. Then the multiplication map $\mu : G \times G \to G$ is equivariant, and hence induces a morphism $\alpha : G \times G/H \to G/H$ as categorical quotients commute with products by schemes with a trivial action (Lemma 1.5.3 (i) and (ii)). Using this commutation property again, one may check that α is an action.

(iv) This is proved by a similar argument. □

With the above assumptions, the quotient G/H is called a **homogeneous space**. The structure theorem for the algebras of infinitesimal group schemes (Theorem 1.4.27) extends unchanged to their homogeneous spaces in view of [6, III.3.6.2].

In turn, this yields further structure results for finite group schemes:

Corollary 1.5.14. *Every finite group scheme G admits a canonical sequence of normal subgroup schemes*

$$e = N_0 \leq N_1 \leq \cdots \leq N_n = G^0$$

such that every quotient N_i/N_{i-1} has height 1.

Proof Take $N_1 = G_1$ (the Frobenius kernel) and argue by induction on $|G|$ by using Corollary 1.5.13. □

Corollary 1.5.15. *If G is infinitesimal, then $|G| = p^n$ for some $n \geq 0$.*

Proof This follows readily by combining Corollaries 1.4.24, 1.5.13 (ii) and 1.5.14. □

Corollary 1.5.16. *The simple finite group schemes are exactly the finite simple groups and the infinitesimal group schemes of height* 1 *associated with the simple finite-dimensional restricted Lie algebras.*

There is a well-known and widely used classification of finite simple groups. The simple finite-dimensional restricted Lie algebras have also been classified, except in small characteristic. More specifically, these Lie algebras are in bijective correspondence with the simple finite-dimensional Lie algebras (see e.g. [36, Thm. 4.1]). These have been classified by Block, Wilson, Strade and Premet: in characteristic $p \geq 7$, they are either of classical type (e.g., $\mathfrak{gl}_n/kI_n$ if n is prime to p) or of Cartan type (e.g., the Jacobson-Witt algebra $\mathrm{Der}(k[T_1, \ldots, T_n]/(T_1^p, \ldots, T_n^p))$ unless $n = 1$ and $p = 2$). If $p = 5$, one gets in addition the Melikian algebras. We refer to [33] for a full account of these developments, and [36] for a nice survey. In characteristics $p = 2, 3$, there are many additional simple (restricted) Lie algebras, see e.g. the recent preprint [5].

1.6 The inverse Galois problem for group schemes

In its original form, the inverse Galois problem may be stated as follows:

Question 1.6.1. Given a finite group G, does there exist a Galois extension of the field of rational numbers with Galois group G?

This classical problem is unsolved, even if many finite groups have been realized as Galois groups over $\mathbb{Q}$; this includes all solvable groups by a theorem of Shafarevich (see [26, (9.5.1)]).

A fruitful approach, initiated by Hilbert, consists in realizing G as a Galois group over the field of rational functions $\mathbb{Q}(T_1, \ldots, T_n)$. Then G can be realized as a Galois group over $\mathbb{Q}$ by specializing $T_1, \ldots, T_n$ appropriately (as a consequence of Hilbert's irreducibility theorem; see e.g. [30, §3.4]). This applies for example to the symmetric group S_n: consider its action on the field of rational functions $k(U_1, \ldots, U_n)$ by permuting the variables. Then the field of invariants $k(U_1, \ldots, U_n)^{S_n}$ is generated by the elementary symmetric functions, and hence is isomorphic to $k(T_1, \ldots, T_n)$.

We refer to [20] for a recent survey of the inverse Galois problem over an arbitrary field K, which asks which finite groups occur as Galois groups over K. It is known that every finite group G can be realized as a Galois group over any **algebraic function field of one variable** K over k, i.e., K/k is a finitely generated field extension of transcendence degree 1. More specifically, there exist infinitely many Galois extensions L/K such that the equalities $G = \mathrm{Aut}_K(L) = \mathrm{Aut}_k(L)$ hold (see [13] for $k = \mathbb{C}$, and [18] for the general case).

In view of the correspondence between algebraic function fields of one variable and algebraic curves (see [14, Cor. I.6.12]), it follows that every nonsingular projective curve X admits a **ramified Galois covering**

$q : Y \to X$ with group G, i.e., Y is a nonsingular projective curve equipped with a faithful action of G, and q is the categorical quotient. Moreover, G is the full automorphism group $\mathrm{Aut}(Y)$.

The automorphism group of a nonsingular projective curve X can be described in terms of the genus $g = g(X)$ as follows. If $g = 0$ then X is isomorphic to the projective line $\mathbb{P}^1$, and hence $\mathrm{Aut}(X) \simeq \mathrm{Aut}(\mathbb{P}^1) = \mathrm{PGL}_2(k)$. If $g = 1$ then choosing a point $0 \in X(k)$, we get a commutative algebraic group structure on the elliptic curve X, with neutral element 0. Thus, X acts on itself by translations. One may check that $\mathrm{Aut}(X) = X \rtimes \mathrm{Aut}(X, 0)$, where X denotes the subgroup of translations, and $\mathrm{Aut}(X, 0)$ stands for the subgroup fixing the origin. Moreover, $\mathrm{Aut}(X, 0)$ is finite of order dividing 24 (see [31, Thm. III.10.1]). Finally, if $g \geq 2$ then $\mathrm{Aut}(X)$ is finite of order at most $84(g - 1)$ (see [14, Ex. IV.2.5]). In particular, $\mathrm{Aut}(X)$ is the group of k-points of an algebraic group for any nonsingular projective curve X.

More generally, one associates to any projective scheme X the **automorphism group scheme** Aut_X. Its points with values in an algebra R are the automorphisms of $X \times \mathrm{Spec}(R)$ of the form $(x, y) \mapsto (f(x, y), y)$, where $f : X \times \mathrm{Spec}(R) \to X$ is a morphism. (We may view f as a family of automorphisms of X parameterized by $\mathrm{Spec}(R)$). In particular, $\mathrm{Aut}_X(k) = \mathrm{Aut}(X)$. Also, the Lie algebra $\mathrm{Lie}(\mathrm{Aut}_X)$ (the kernel of the group homomorphism $\mathrm{Aut}_X(k[\varepsilon]) \to \mathrm{Aut}_X(k)$, $\varepsilon \mapsto 0$) is identified with the Lie algebra $\mathrm{Vect}(X)$ of vector fields on X. The scheme Aut_X is **locally of finite type**, i.e., it admits an open covering by affine schemes of finite type (but Aut_X is not necessarily an algebraic group, see Example 1.6.4 below). Given a group scheme G, the G-actions on X correspond bijectively to the homomorphisms of group schemes $G \to \mathrm{Aut}_X$.

The construction of Aut_X is due to Grothendieck in a much more general setting, see [12]; it has been extended to proper schemes over an arbitrary field by Matsumura and Oort (see [23]). If X is a finite scheme, this gives back the group scheme Aut_B of Example 1.4.18, where $B = \mathcal{O}(X)$; in particular, Aut_X is not necessarily reduced if $p > 0$. Also, if X is a nonsingular projective curve, then Aut_X is a reduced algebraic group (as a consequence of the above description of $\mathrm{Aut}(X)$ together with a Lie algebra argument). In view of the above discussion, this yields:

Proposition 1.6.2. *Every finite group can be realized as the automorphism group scheme of a nonsingular projective curve.*

By contrast, there are strong restrictions on infinitesimal subgroup schemes of nonsingular projective curves. For example, their Lie algebra has dimension at most 3. If one considers a possibly singular projective curve X, then there are still strong restrictions on the Lie algebra of Aut_X as follows from [29, Thm. 12.1]. The same holds for several classes of nonsingular projective surfaces, see [35, 21, 22].

By analogy with the inverse Galois problem, one may ask:

Question 1.6.3. Which group schemes can be realized as the automorphism group scheme of a projective scheme X? One may further impose geometric conditions on X, e.g., restrict to nonsingular varieties.

This question is wide open, even if our understanding of automorphism group schemes has improved significantly during the last years. Before mentioning some recent developments, we review a classical structure result on the group scheme Aut_X, where X is a proper scheme. Since this group scheme is locally of finite type, its connected component of the identity is a normal subgroup scheme of finite type, denoted by Aut_X^0 and called the **connected automorphism group scheme**. Moreover, the quotient group scheme

$$\mathrm{Aut}_X/\mathrm{Aut}_X^0 = \pi_0(\mathrm{Aut}_X)$$

exists; it is a discrete group scheme which parameterizes the connected components of Aut_X (see [6, II.5.1]). Thus, we may view $\pi_0(\mathrm{Aut}_X)$ as an abstract group. This **component group** is countable (as follows from [12]), and generally infinite in view of the following:

Example 1.6.4. Let E be an elliptic curve with origin 0, and $X = E \times E$. One may check that $\mathrm{Aut}_X = X \rtimes \mathrm{Aut}_{X,(0,0)}$, where X acts on itself by translation. Moreover, $\mathrm{Aut}_X^0 = X$ and $\pi_0(\mathrm{Aut}_X) \simeq \mathrm{Aut}_{X,(0,0)}$. In particular, $\pi_0(\mathrm{Aut}_X)$ contains the group $\mathrm{GL}_2(\mathbb{Z})$ acting on X via $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot (z, w) = (az + bw, cz + dw)$.

In this example, one may easily show that $\pi_0(\mathrm{Aut}_X)$ is an arithmetic group; as a consequence, it admits a finite presentation. More generally, the group $\pi_0(\mathrm{Aut}_X)$ is arithmetic for any **abelian variety**, i.e., a projective group variety. But there exist complex nonsingular projective varieties X such that Aut_X is discrete and non-finitely generated; see [15] for the first example of such a variety, in dimension 6, and [8] for further examples in dimension 2. Such examples also exist when p is odd and k is not the algebraic closure of its prime field, see [27].

So the component group of Aut_X is quite mysterious. By contrast, the identity component can be any prescribed connected algebraic group:

Theorem 1.6.5. *Let G be a connected algebraic group. Then there exists a projective variety X such that $G \simeq \mathrm{Aut}^0_X$. If $p = 0$, one may further take X nonsingular.*

Taking for G an infinitesimal group scheme of height 1 and using the equivalence of categories of Theorem 1.4.23 and its version for actions of group schemes (see [6, II.7.3.10]), this yields:

Corollary 1.6.6. *Assume that $p > 0$ and let $\mathfrak{g}$ be a finite-dimensional restricted Lie algebra. Then there exists a projective variety X such that $\mathfrak{g} \simeq \mathrm{Vect}(X)$.*

Also, Question 1.6.3 has been answered for abelian varieties:

Theorem 1.6.7. *Let A be an abelian variety with origin 0. Then there exists a projective variety X such that $A \simeq \mathrm{Aut}_X$ if and only if the group $\mathrm{Aut}(A, 0)$ is finite. Under these conditions, one may further take X nonsingular.*

This result was first obtained by Lombardo and Maffei over the field of complex numbers (see [17]), and then extended in [1] to an algebraically closed ground field. As a consequence, every elliptic curve E can be realized as the automorphism group scheme of a nonsingular projective variety, but $E \times E$ admits no such realization.

Part of Theorem 1.6.7 has been generalized in [3, Thm. 2]; this yields a necessary condition for a reduced connected algebraic group G to be the full automorphism group scheme of a nonsingular projective variety. But this only gives restrictions when G is not affine. So Question 1.6.3 is still unanswered for linear algebraic groups.

One may also consider Question 1.6.3 over an arbitrary ground field k (not necessarily algebraically closed). Here again, some results have been obtained recently: Proposition 1.6.2 extends to an arbitrary field, see [2]. It also extends to a finite field k and a finite commutative group scheme of order prime to the characteristic, as a consequence of the main result of [7]. Also, Theorem 1.6.5 holds over an arbitrary field (see [4]), as well as Theorem 1.6.7 by a result of Florence (see [11]).

Acknowledgements. Many thanks to Sami Al–Asaad, Pascal Fong, Matilde Maccan, David Stewart and an anonymous referee, for their careful reading of preliminary versions of this text and their valuable comments.

References

[1] J. Blanc, M. Brion, "Abelian varieties as automorphism groups of smooth projective varieties in arbitrary characteristics," preprint, `https://arxiv.org/abs/2102.02459` 1.1, 1.6

[2] D. Bragg, "Automorphism groups of curves over arbitrary fields," preprint, `https://arxiv.org/abs/2304.02778` 1.6

[3] M. Brion, "Automorphism groups of almost homogeneous varieties," in: Facets of algebraic geometry. A collection in honor of William Fulton's 80th birthday. Volume 1, London Math. Soc. Lecture Note Series **472**, pp. 54–76, Cambridge Univ. Press, 2022. 1.6

[4] M. Brion, S. Schröer, "The inverse Galois problem for connected algebraic groups," preprint, `https://arxiv.org/abs/2205.08117` 1.1, 1.6

[5] D. Cushing, G. Stagg, D. Stewart, "A Prolog assisted search for new simple Lie algebras," preprint, `https://arxiv.org/abs/2207.01094` 1.5

[6] M. Demazure, P. Gabriel, "Groupes algébriques," Masson, Paris, 1970. 1.1, 1.4.2, 1.4.2, 1.4.4, 1.4.19, 1.4.5, 1.4.5, 1.5, 1.6, 1.6

[7] R. Darda, T. Yasuda, "Inverse Galois problem for semicommutative finite group schemes," preprint, `https://arxiv.org/abs/2210.01495` 1.6

[8] T. Dinh, K. Oguiso, "A surface with discrete and nonfinitely generated automorphism group," Duke Math. J. **168** (2019), 941–966. 1.6

[9] D. Eisenbud, J. Harris, "The geometry of schemes," Graduate Texts Math. **197**, Springer, New York, 2000. 1.2.5, 1.2.24

[10] D. Eisenbud, "Commutative algebra with a view towards algebraic geometry," Graduate Texts Math. **150**, Springer, New York, 1996. 1.1, 1.2.23, 1.5.5, 1.5

[11] M. Florence, "Realization of Abelian varieties as automorphism groups," preprint, `https://arxiv.org/abs/2102.02581` 1.6

[12] A. Grothendieck, "Techniques de construction et théorèmes d'existence en géométrie algébrique IV: les schémas de Hilbert," Sém. Bourbaki, Vol. **6** (1960–1961), Exp. 221, 249–276. 1.6, 1.6

[13] L. Greenberg, "Maximal groups and signatures," in: Discontinuous groups and Riemann surfaces, pp. 207–226. Princeton Univ. Press, Princeton, N.J., 1974. 1.1, 1.6

[14] R. Hartshorne, "Algebraic geometry," Graduate Texts Math. **52**, Springer, New York, 1977. 1.1, 1.5.11, 1.6

[15] J. Lesieutre, "A projective variety with discrete, non-finitely generated automorphism group," Inventiones Math. **212** (2018), 189-211. 1.6

[16] C. Liedtke, "A McKay correspondence in positive characteristic," preprint, `https://arxiv.org/abs/2207.06286` 1.1

[17] D. Lombardo, A. Maffei, "Abelian varieties as automorphism groups of smooth projective varieties," Int. Math. Res. Not. (2020), 1942-1956. 1.1, 1.6

[18] M. Madan, M. Rosen, "The group of automorphisms of a function field," Proc. Amer. Math. Soc. **115** (1992), 923–929. 1.1, 1.6

[19] D. Madden, R. Valentini, "The group of automorphisms of algebraic function fields," J. Reine Angew. Math. **343** (1983), 162–168. 1.1

[20] G. Malle, B. Matzat, "Inverse Galois theory. 2nd edition," Springer Monographs in Mathematics, Springer, Berlin, 2018. 1.6

[21] G. Martin, "Infinitesimal automorphisms of algebraic varieties and vector fields on elliptic surfaces," Algebra & Number Theory, to appear. 1.6

[22] G. Martin, "Automorphism group schemes of bielliptic and quasi-bielliptic surfaces," EpiGA **6** (2022), Article no. 9. 1.6

[23] H. Matsumura, F. Oort, "Representability of group functors, and automorphisms of algebraic schemes," Invent. math. **4** (1967), 1–25. 1.6

[24] J. S. Milne, "Algebraic groups. The theory of group schemes of finite type over a field," Cambridge Stud. Adv. Math. **170**, Cambridge Univ. Press, Cambridge, 2017. 1.1, 1.2.23, 1.3.15, 1.4.2, 1.4.2, 1.4.4, 1.4.5, 1.4.5, 1.5

[25] D. Mumford, "Abelian varieties," Oxford Univ. Press, Oxford, 1970. 1.1, 1.4.4, 1.4.19, 1.5

[26] J. Neukirch, A. Schmidt, K. Wingberg, "Cohomology of number fields. 2nd ed.," Grundlehren Math. Wiss. **323**, Springer, Berlin, 2008. 1.6

[27] K. Oguiso, "A surface in odd characteristic with discrete and non-finitely generated automorphism group," Adv. Math. **375** (2020). 1.6

[28] R. Pink, "Finite group schemes," course notes available at `https://people.math.ethz.ch/~pink/ftp/FGS/CompleteNotes.pdf` 1.1

[29] S. Schröer, N. Tziolas, "The structure of Frobenius kernels for automorphism group schemes," Algebra & Number Theory, to appear. 1.6

[30] J.-P. Serre, "Topics in Galois theory. Notes written by Henri Darmon. 2nd ed.," Research Notes in Math. **1**, Wellesley, MA, 2007. 1.6

[31] J. H. Silverman, "The arithmetic of elliptic curves. Second edition," Grad. Texts Math.**106**, Springer, New York, 2009. 1.2.1, 1.3.16, 1.6

[32] M. Demazure, A. Grothendieck, "Séminaire de Géométrie Algébrique du Bois Marie, 1962–64, Schémas en groupes (SGA3)," Tome I. Propriétés générales des schémas en groupes, Doc. Math. **7**, Soc. Math. France, Paris, 2011. 1.1

[33] H. Strade, “Simple Lie algebras over fields of positive characteristic. I, II, III,” de Gruyter Expositions in Mathematics **38**, **42**, **57**, de Gruyter, Berlin, 2013–2017. 1.5

[34] J. Tate, “Finite flat group schemes,” in: Modular forms and Fermat’s last theorem, pp. 121–154, Springer, New York, 1997. 1.1

[35] N. Tziolas, “Automorphisms of smooth canonically polarized surfaces in positive characteristic,” Adv. Math. **310** (2017), 235–289; corrigendum ibid., 585–593. 1.6

[36] F. Viviani, “ Simple finite group schemes and their infinitesimal deformations,” Rend. Sem. Mat. Univ. Politec. Torino **68** (2010), 171–182. 1.5

[37] W. Waterhouse, “Introduction to affine group schemes,” Graduate Texts Math. **66**, Springer, New York, 1979. 1.1, 1.3.1

Université Grenoble Alpes, Institut Fourier, 100 rue des Mathématiques,
38610 Gières, France