# 1

# Finite group schemes

Michel Brion[a]

## 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,

[a] Université Grenoble Alpes, Institut Fourier, 100 rue des Mathématiques, 38610 Gières, France.
Michel.Brion@univ-grenoble-alpes.fr

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 [17]).

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 [7, 8, 25]. 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 $p$th 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, 20, 19]), but negative for many abelian varieties as recently shown in [18, 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 [11]. Section 1.6 is more advanced, and involves notions and results of algebraic geometry which can be found in [15].

This text presents only the first steps in the theory of finite group schemes. Here are some suggestions for further reading: [26, Chap. III] for more on this topic, [37] for affine group schemes, [25] for algebraic

groups (both over an arbitrary field), [29] 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 $n$th power map

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

This is a group homomorphism with kernel the group $\mu_n(k)$ of $n$th 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 $p$th 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 $n$th 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 $p$th 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 $p$th 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 [32].

**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 $\Lambda$ 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

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

In particular, $\mathrm{Ker}(n_E)$ 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, $\mathrm{Ker}(p_E)$ 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

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

the evaluation at $x$. Then $\mathrm{ev}_x$ 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 $\mathrm{ev}_x$ 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 $\varphi^*$ 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

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

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