ALGEBRAIC GROUPS AND FORMAL GROUPS

PIERRE CARTIER

Translator's Note: This is a translation of Cartier's 1962 article "Groupes algèbriques et groupes formels," which introduced the Cartier duality equivalence between affine algebraic groups and formal groups over a base field. I have added a few marginal notes which I hope do not distract from the text. If you notice any errors or have any comments, please contact me at josh.mundinger@gmail.com. -J.M., November 21, 2025

[1] [2]

1. Introduction

The theory of algebraic groups over a field of nonzero characteristic is complicated by the presence of the phenomena of inseparability. One knows that there exist for example bijective homomorphisms of algebraic groups, which are not birational isomorphisms ("radicial isogenies"); further, the classical isomorphism theorem $H/H \cap K \simeq H.K/K$ (where H and K are closed subgroups of the same algebraic group) is only valid if H and K meet transversally. In an earlier work [Car59], I gave a general theory of isogenies which completed the results of I. Barsotti [Bar56]; but the object introduced to serve as the kernel of an isogeny had little in common with an algebraic group, and the theory obtained was not workable.

The recent progress of Algebraic Geometry amply demonstrates that the natural setting is that of the Schemes of A. Grothendieck [GD71]; in this theory, there is a bijective correspondence between the closed subschemes of n-dimensional affine space and the ideals of the polynomial ring in n variables; this permits the introduction of numerous distinct "varieties" with the same set of points, and in the same blow, to distinguish between the "kernels" of different radicial isogenies. In other words, if we consider the *group schemes* over a field of general characteristic, the previously mentioned difficulties evaporate. In this exposition, we introduce two limitations: we only consider *affine* schemes over a base *field*; outside of this category, the results are still too fragmentary. On the other hand, we present the theory differently than Grothendieck, in order to be able to handle real groups[3]

[1] Conference presentation in Brussels on June 6, 1962 on the occasion of the *Colloquium* on the *Theory of Algebraic Groups* organized by CBRM

[2] The numbers in brackets refer to the Bibliography at the end of this article. Translator's Note: I have replaced numbered citation keys with alphanumeric keys.

[3] Approximately, a scheme is a set of irreducible subvarieties of an algebraic variety, but not the set of its points; a group scheme is not a group! Moreover, we have extensively used the language of functors (cf. Grothendieck [Gro57]); as a reminder, a covariant (resp. contravariant) functor $T : A \to B$ is called an equivalence (resp. a duality) if every object of B is isomorphic to one of the form $T(X)$ for X in A, and if T defines a bijection from $\mathrm{Hom}(X, Y)$ to $\mathrm{Hom}(T(X), T(Y))$ (resp. to $\mathrm{Hom}(T(Y), T(X))$) for every pair of objects X and Y in A.

In a wholly other domain, J. Dieudonné [Die55; Die56] has furnished us with a great variety of new algebraic phenomena in the theory of formal groups over a field of nonzero characteristic. This theory, suitably adapted, served as a guide to the research of Barsotti and myself on abelian varieties; an example can be found in Barsotti's presentation at the same conference. But until now, the theory of algebraic groups and the theory of formal groups only had a superficial relationship. The goal of the present exposé is to make a synthesis. To do so, we will have to enlarge a little bit the notion of a formal group in such a way that every finite group may be considered as a formal group; this being done, the theory of formal groups is equivalent to that of hyperalgebras [4].

Using a suggestion of Grothendieck, we associate to every commutative algebraic group a formal group which will be its dual. The theorem of biduality is verified; for the "finite" algebraic groups, one recovers the theory of duality which is exposed[5] by P. Gabriel [Gab60]. From a heuristic point of view, we can use the following table of correspondences with the theory of topological groups:

Algebraic groups of finite type	compact Lie group
Algebraic group	compact group
Formal group	discrete group
Duality	Pontryagin duality

For the moment, we don't know how to define the objects, analogous in the above correspondence, to locally compact abelian groups which are neither discrete nor compact. The question seems important for certain geometric applications.

The present article is nothing but a summary; it contains practically no proofs, nor applications to abelian varieties. We will publish a detailed exposition of the theory elsewhere.

2. Definition of algebraic groups

Let us first show how to generalize the classical notion of an algebraic group of matrices. Let n be a positive integer; for every commutative ring A, we denote by $\mathsf{GL}(n, A)$ the set of square matrices of order n with coefficients in A whose determinant is an invertible element in A; under matrix multiplication, $\mathsf{GL}(n, A)$ is a group. To avoid the awkward restriction on the determinant, we employ the following classical trick; put $r = n^2 + 1$; we associate to every matrix g in $\mathsf{GL}(n, A)$ the point of A^r having coordinates the entries g_{ij} of the matrix g (for $1 \leq i, j \leq n$) and the inverse g_0 of the determinant of g. Let us introduce a system X of r indeterminates X_0 and X_{ij}, and the polynomial with integer coefficients:

$$D(X) = 1 - X_0 \cdot \det(X_{ij}) \tag{1}$$

Under these conditions, one identifies the set $\mathsf{GL}(n, A)$ with the set of points of A^r which annihilate the polynomial D.

So, consider a field k and an algebraic closure Ω of k; according to the usual definition, one says a subgroup G of $\mathsf{GL}(n, \Omega)$ is algebraic if it is the set of matrices annihilating a certain number of polynomials in $\Omega[X]$. One says G is defined over k if the ideal of polynomials in $\Omega[X]$ zero on G is generated by polynomials with

[4] In algebraic topology, one uses under the name Hopf Algebra a notion very close to that of a hyperalgebra.

[5] Gabriel uses the language of hyperalgebras, and not that of formal groups, which forces a number of contorsions.

coefficients in k; if G is such a group, one denotes $I_k(G)$ the set of polynomials of $k[X]$ which vanish on G; the group G is then the zero set of the ideal $I_k(G)$. What's more, for an ideal of $k[X]$ to be of the form $I_k(G)$ for a suitable group G, it is necessary and sufficient to verify the following conditions [6]

a) The ideal I contains D.

b) Let Y be a new series of r variables; put $Z_0 = X_0Y_0$ and $Z_{ik} = \sum_{1\leq j\leq n} X_{ij}Y_{jk}$ for $1 \leq i, k \leq n$. For every polynomial P in I, there is a relation of the form

$$P(Z) = \sum_{\alpha} L_\alpha(X)P_\alpha(Y) + \sum_{\beta} P'_\beta(X)L'_\beta(Y) \tag{2}$$

with polynomials L_α and L'_β in $k[X]$ and polynomials P_α and P'_β in I.

c) Let X'_0 be the determinant of the matrix X_{kl} and X'_{ij} the product of X_0 by the cofactor of X_{ij} in the determinant X'_0. One has $P(X') \in I$ for every polynomial P in I.

d) The ideal of $\Omega[X]$ generated by I is an intersection of prime ideals.

When k is of characteristic zero, condition d) is a consequence of the other conditions; this results from theorems mentioned later (cf. no 15). But if the field k has characteristic $p \neq 0$, it is no longer the same, as shown by the example of the ideal $I = (X^p_{11} - 1, 1 - X_0X_{11})$ in the case $n = 1$. Many reasons lead us to consider that the essential notion is not an algebraic group of matrices, but that of an ideal I satisfying hypothesis a), b) and c). Let I be such an ideal; we may define the set G_Ω of matrices g in $GL(n, \Omega)$ annihilated by all polynomials in I, and G_Ω is an algebraic subgroup of $GL(n, \Omega)$ defined over the perfect closure of k; but in general, I is different than the ideal $I_k(G_\omega)$ of polynomials vanishing on G_Ω, so that the ideal I is no longer characterized by the group G_Ω; in the example above, the group G_Ω consists only of the identity matrix! In a heuristic manner, it is necessary to consider the infinitesimal points of a group along with the "finite" points. Thanks to A. Weil [Wei53], there is a rigorous method of treating infinitesimal points; if we follow that idea, we are led to introduce for every commutative k-algebra A the set G_A of matrices g in $GL(n, A)$ which is annihilated by all polynomials in I; it turns out that G_A is a subgroup of $GL(n, A)$ and that I is the set of polynomials in $k[X]$ zero on G_A for *every* algebra A. So it is the collection of all[7] the groups G_A which constitute the "algebraic group of matrices" associated to the ideal I; for technical reasons, it is also necessary to consider along with the groups G_A the homomorphisms $G(\sigma)$ defined so: for every homomorphism of algebras σ from A to B, one defines a homomorphism of groups $G(\sigma)$ from G_A to G_B by associating to the matrix $g = (g_{ij})$ the matrix $\sigma \cdot g = (\sigma \cdot g_{ij})$.

The group scheme defined by $(X^p_{11} - 1)$ in GL_1 is μ_p, the group scheme of pth roots of unity.

Moreover, J.-P. Serre [Ser60] has recently demonstrated the necessity of considering projective limits of algebraic groups, or "proalgebraic groups". For example,

[6] If Z is the set of zeroes of the ideal I in the space Ω^r, the condition a) means $Z \subset GL(n, \Omega)$, the condition b) that Z is stable under multiplication, and c) that it is stable under inversion; finally d) expresses the Hilbert Nullstellensatz and ensures that I is the set of those polynomials vanishing on Z.

[7] To avoid well-known logical difficulties, we can use the device of universes. A universe is a set U vast enough so that one can perform on the sets appearing in U all the usual operations in Set Theory. By adding to Set Theory an axiom of the existence of a suitable universe, we can ensure that every set appears in a universe. In the case of the text, we can limit ourselves to groups G_A for A drawn from a given universe containing k.

the group of units of a field complete with respect to a discrete valuation with algebraically closed residue field, or the Galois group of an infinite algebraic extension, have every interest in being considered as proalgebraic groups. The definition on which we have settled is motivated by the desire to encompass at least the "affine" proalgebraic groups.

By definition, a "proalgebraic group" is made up of the data for every commutative algebra A, a group G_A, and for every homomorphism of algebras $\sigma : A \to B$, a homomorphism of groups $G(\sigma) : G_A \to G_B$ satisfying the following axioms:

(G1) We have $G(\tau\sigma) = G(\tau)G(\sigma)$ whenever the homomorphisms σ and τ are composable; when σ is the identity transformation of A, then $G(\sigma)$ is the identity transformation of G_A.

(G2) There exists a generic point of G; said another way, there is a commutative algebra E and a point x in G_E such that the function $\sigma \mapsto G(\sigma).x$ is, for every algebra A, a bijection from the homomorphisms from E to A to the set G_A.

In the functorial language, an algebraic group is therefore a representable functor from the category of commutative algebras to the category of groups. We know that the category of affine schemes is equivalent to the category dual to that of commutative rings; it follows that our theory is equivalent to that of affine group schemes.

Examples:

(1) Let n be a positive integer; for every commutative algebra A, set $GL(n)_A = GL(n, A)$, and for every homomorphism of algebras $\sigma : A \to B$, define the homomorphism $GL(n)(\sigma)$ by associating $\sigma \cdot g$ to g. We have thus defined an algebraic group $GL(n)$ called the *linear group on n variables.*

(2) Let G be an algebraic group. We say that an algebraic group G' is a subgroup of G if G'_A is a subgroup of G_A for every commutative algebra of A and if $G'(\sigma)$ is the restriction of $G(\sigma)$ to G'_A for every homomorphism $\sigma : A \to B$.

(3) The groups constructed previously by means of an ideal I of $k[X]$ satisfying a), b) and c) are nothing but the subgroups of $GL(n)$. If the ideal I is generated by polynomials P_α, we will say that the group associated to I is the subgroup of $GL(n)$ defined by the equations $P_\alpha = 0$.

(4) Let L be an algebra of finite rank over k; denote by I the identity transformation of L. For every commutative algebra A, let $S(L)_A$ be the additive group of the algebra $L \otimes A$, and $P(L)_A$ the multiplicative group of invertible elements in the same algebra. For every homomorphism of algebras $\sigma : A \to B$, the linear transformation $I \otimes \sigma : L \otimes A \to L \otimes B$ induces the homomorphisms $S(L)(\sigma) : S(L)_A \to S(L)_B$ and $P(L)(\sigma) : P(L)_A \to P(L)_B$. We have thus defined two algebraic groups $S(L)$ and $P(L)$ called respectively the *additive group* and *multiplicative group* of L. If $L = k$, we have obtained the groups denoted respectively $\mathbb{G}_a$ and $\mathbb{G}_m$ and called the additive group and multiplicative group with one parameter. We have $\mathbb{G}_m = GL(1)$.

(5) We say that an algebraic group G is of *finite type* if it is isomorphic to a subgroup of a group $GL(n)$. It is equivalent to suppose that there exists a generic point $x \in G_E$ such that the algebra E is finitely generated; this condition is independent of the chosen generic point. We say that G is *finite* if there exists a generic point $x \in G_E$ with E of finite rank over k.

3. General properties of algebraic groups

The notion of a homomorphism is primordial. Let G and H be two algebraic groups; a *homomorphism* $u : G \longrightarrow H$ is the data of for every commutative algebra A a homomorphism $u_A : G_A \longrightarrow H_A$ verifying the relations $u_B \cdot G(\sigma) = H(\sigma) \cdot u_A$ for every algebra homomorphism $\sigma : A \longrightarrow B$[8]. Introduce the generic points $x \in G_E$ and $y \in H_P$ for G and H; so there exists a homomorphism $\sigma : F \longrightarrow E$ characterized by the formula $u_E(x) = H(\sigma) \cdot y$; we say that u is a monomorphism if σ is surjective and an epimorphism if σ is injective; naturally, these properties do not depend on the choice of generic points. We denote by σ_G the identity endomorphism of an algebraic group.

Let G' be a subgroup of G; the inclusion of G' into G is a monomorphism. We say that G' is normal if G'_A is a normal subgroup of G_A for every algebra A; so we may construct a quotient group G/G' and a canonical epimorphism $\pi : G \longrightarrow G/G'$ such that the kernel of π_A is exactly G'_A for every algebra A; we can identify G_A/G'_A as a subgroup of $(G/G')_A$, but in general, the two groups will be distinct. The construction of G/G' is quite delicate; it can be done by adapting an argument by which C. Chevalley [Che51] showed the existence of a rational homomorphism with given kernel. In every case, the properties of G/G' stated above are sufficient to characterise it up to unique isomorphism.

For example, if $\mathbb{R}$ is the real field, $G = SL_2$ and $G' \subseteq G$ is the subgroup of diagonal matrices, then $G/G' = PGL_2$, and $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ defines an element of $(G/G')_{\mathbb{R}}$ not contained in $G_{\mathbb{R}}/G'_{\mathbb{R}}$.

If u is a homomorphism from G to H, the collection N of kernels N_A of the homomorphisms u_A is a subgroup of G, called the *kernel* of u. Among the subgroups H' of H such that $H'_A \supset u_A(G_A)$ for every A, there exists a smallest one, called the *image* of u, denoted by $u(G)$; in general, we have $u(G)_A \neq u_A(G_A)$. With these definitions, we have a *canonical factorization theorem*: N is a normal subgroup of G, and there exists an isomorphism $u : G/N \longrightarrow u(G)$ such that $u = \iota \cdot u \cdot \pi$ where ι is the inclusion of $u(G)$ in H and π the canonical homomorphism from G to G/N. From this, we deduce the two classical isomorphism theorems $G/G' \simeq (G/G'')/(G'/G'')$ and $G'/(G' \cap L) \simeq G' \cdot L/L$; we also deduce that u is a monomorphism (resp. epimorphism) if and only if $N = (e)$ (resp. $u(G) = H$), and that u is an isomorphism if and only if both $N(e)$ and $u(G) = H$. There is thus no further distinction to be made between bijective homomorphisms and isomorphisms; as for isogenies, they are defined as those homomorphisms with finite kernel.

The notion of product of a family, finite or infinite, of algebraic groups is clear; the product is defined by restriction. One has the analogue of the Peter-Weyl theorem: every algebraic group is isomorphic to a subgroup of a product $\prod_i GL(n_i)$ of linear groups; we deduce that every algebraic group is a projective limit of a filtered family of subgroups of suitable linear groups $GL(n)$; apart from inseparability, our algebraic groups are thus the *affine* proalgebraic groups of Serre. From the above, we painlessly deduce a theorem analogous to the theorem of Tannakian duality for compact groups (cf [Car56a] and [Che46]); it is necessary only to note that the linear representations[9] of an algebraic group are not in general completely reducible.

recall that Cartier's "algebraic group" is an affine scheme by definition

[8] A homomorphism of algebraic groups is thus by definition a homomorphism of functors.

[9] Let V be a vector space of finite dimension n over the field k. If $L(V)$ is the algebra of endomorphisms of V, the algebraic group $P(L(V))$ is denoted $GL(V)$; the choice of a basis of V defines an isomorphism of $GL(V)$ with $GL(n)$. This being so, a linear representation of an algebraic group G in the vector space V is, by definition, a homomorphism from G to $GL(V)$. We can copy the usual theory of linear representations of groups, and define the irreducible representations, completely reducible representations, etc.

It is necessary for the following to define the *extension of scalars*. Let G be an algebraic group (over the field k) and let λ be a homomorphism from k to a field k'. For every algebra A' over k', we define the algebra A'_λ over k with the same elements, addition, and multiplication as A', but consider the external law $(u, a') \mapsto \lambda(u).a'$ (for $u \in k$ and $a' \in A'$); if σ is a k'-homomorphism of algebras from A' to B', it is again a k-homomorphism from A'_λ to B'_λ which is denoted σ_λ to avoid confusion. Now let A be an algebra over k; the algebra A^λ over k' defined by extension of scalars is the tensor product $k'_\lambda \otimes_k A$ with the usual external law; we have the rules of calculation:

$$(3) \qquad u' \otimes va = u'\lambda(v) \otimes a \qquad u' \cdot (u'' \otimes a) = (u'u'') \otimes a$$

for $u', u'' \in k'$, $v \in k$, and $a \in A$.

The algebraic group G^λ over the field k' is thus defined by the formulas:

$$(4) \qquad G^\lambda_{A'} = G_{A'_\lambda} \qquad G^\lambda(\sigma) = G(\sigma_\lambda).$$

Let $x \in G_E$ be a generic point of G; let π be the homomorphism from E to $F = (E^\lambda)_\lambda$ defined by $\pi(a) = 1 \otimes a$; then the point $x' = G(\pi) \cdot x$ in $G_F = G^\lambda_{E^\lambda}$ is generic. One has $GL(n)^\lambda = GL(n)$, and if the algebraic subgroup G of $GL(n)$ is defined by the equations $P_\alpha = 0$ with coefficients in k, the algebraic subgroup G^λ of $GL(n)$ is defined by the equations $P^\lambda_\alpha = 0$ obtained by applying λ to each coefficient of each polynomial P_α.

4. Commutative algebraic groups over a perfect field

We say that an algebraic group G is *commutative* if the groups G_A are all commutative; if G and H are two commutative algebraic groups, we can define an addition on the set $\mathrm{Hom}(G, H)$ of homomorphisms from G to H. The canonical factorization theorem demonstrates that the category C of commutative algebraic groups is an abelian category in the sense of A. Grothendieck [Gro57]; moreover, by reasoning similar to that of J.-P. Serre [Ser60], we prove that for every commutative algebraic group G, there exists a *projective* commutative algebraic group P and an epimorphism of P onto G; this permits the application to C of the methods of Homological Algebra.

5.

Let G be an commutative algebraic group; we say that G is *reductive* if every linear representation of G is completely reducible. Assume k is perfect for §5 and §6; we let $\bar{k}$ be an algebraic closure of k, and $\mathfrak{G}$ the topological Galois group of $\bar{k}$ over k. For G to be reductive, it is necessary and sufficient that the algebraic group $\bar{G}$ over the field $\bar{k}$, formed by extension of scalars from G, is isomorphic to a subgroup of a product of groups each equal to $\mathbb{G}_m$.

We denote by C^r the category of reductive algebraic groups. For every commutative algebraic group G, let $X(G)$ be the set of homomorphisms from $\bar{G}$ to $\mathbb{G}_m$ (over the field $\bar{k}$); it is a commutative group on which the Galois group $\mathfrak{G}$ acts in a natural way; further, for every $\chi \in X(G)$, the set of $s \in \mathfrak{G}$ such that $s \cdot \chi = \chi$ is an open subgroup of $\mathfrak{G}$; in the terminology of J. Tate, $X(G)$ is thus a Galois module for $\mathfrak{G}$. We have thus defined a contravariant functor X from the category C^r to the category M of Galois modules for $\mathfrak{G}$; the functor is a duality.

For a reductive group G to be of finite type, it is necessary and sufficient that $X(G)$ is an abelian group of finite type. For G to be "connected", it is necessary and sufficient that $X(G)$ has no torsion; finally for G to be "simply connected" in the sense of SERRE [Ser60], it is necessary and sufficient that the group $X(G)$ be divisible. Call a connected reductive algebraic group of finite type a *torus*; the preceding demonstrates that the algebraic tori correspond via X to Galois modules for $\mathfrak{G}$ which are free abelian groups of finite type (a theorem of Tate).

this is not correct in characteristic p, since $G = \mu_p$ is reductive and connected over $\mathbb{F}_p$, but $X(\mu_p) = \mathbb{Z}/p\mathbb{Z}$.

6.

We say that a commutative algebraic group G is *unipotent* if every irreducible linear representation of G is trivial (this definition also makes sense if k is not perfect). It is equivalent to suppose that every homomorphism from $\bar{G}$ to $\mathbb{G}_m$ (over the field $\bar{k}$) is zero.

Suppose that k has characteristic zero. For a commutative algebraic group G to be unipotent, it is necessary and sufficient that it is isomorphic to a product of a family, finite or infinite, of groups equal to $\mathbb{G}_a$. In a more intrinsic way, set $V(G) = \mathrm{Hom}(G, \mathbb{G}_a)$; it is a vector space over the field k; moreover, the functor V is a duality from the category of unipotent groups with the category of k-vector spaces. For G to be of finite type, it is necessary and sufficient that the vector space $V(G)$ be of finite dimension.

Let's return to the case of a field k of general characteristic. For a commutative algebraic group to be reductive (resp. unipotent), it is necessary and sufficient that it is a projective limit of reductive (resp. unipotent) commutative algebraic groups of finite type. For the groups of finite type, the terminology: reductive–unipotent is in agreement with the usual conventions. Finally, every commutative algebraic group G decomposes in a unique way as a product $G^r \times G^u$ of a reductive group G^r and a unipotent group G^u.

7. ALGEBRAIC GROUPS OVER A FIELD OF NONZERO CHARACTERISTIC

Suppose k is of characteristic $p \neq 0$; we will encounter here the most interesting algebraic phenomena. Let's start with a few important examples.

Let n be a positive integer; for every commutative ring A of characteristic p, we know how to define the ring $W_n(A)$ of Witt vectors of length n over A; moreover, for every homomorphism σ from A into a ring B of characteristic p, we define a homomorphism of the ring $W_n(A)$ into $W_n(B)$ by posing

$$W_n(\sigma)(x_0, \ldots, x_{n-1}) = (\sigma \cdot x_0, \ldots, \sigma \cdot x_{n-1}). \tag{5}$$

The collection of the additive groups $W_n(A)$ over commutative k-algebras A and the homomorphisms $W_n(\sigma)$ form a commutative algebraic group, which we denote by W_n.

Moreover, we denote by E_n the ring of endomorphisms of the commutative algebraic group E_n. First, we define two elements V and F in E_n by the formulas of Witt:

$$F_A(x_0, \ldots, x_{n-1}) = (x_0^p, \ldots, x_{n-1}^p) \tag{6}$$

$$V_A(x_0, \ldots, x_{n-1}) = (0, x_0, \ldots, x_{n-2}). \tag{7}$$

Moreover, by using the ring structure of $W_n(A)$, we define for every Witt vector w in $W_n(k) = \Lambda_n$ an operator of multiplication by W which is an endomorphism

$R(w)$ of W_n. Finally, we write:

$$F_k(w) = w^{\pi} \qquad V_k(w) = w^{\delta} \qquad\qquad (w \in \Lambda_n).$$

We have thus the system of relations:

$$\text{(8)} \qquad \begin{cases} VF = FV = p \cdot \delta_{W_n} & V^n = 0 \\ F \cdot R(w) = R(w^{\pi}) \cdot F & V \cdot R(w^{\pi}) = R(w) \cdot V \end{cases}$$

$$\text{(9)} \qquad V \cdot R(w) \cdot F = R(w^{\delta})$$

and every element of E_n is written in a unique way in the form

$$\text{(10)} \qquad \sum_{i \geq 0} R(w_i) \cdot F^i + \sum_{0 \leq j < n} V^j \cdot R(w'_j)$$

with Witt vectors w_i and w'_j in Λ_n, zero except for a finite number of entries[10] Finally, the function $w \mapsto R(w)$ is an isomorphism of Λ_n with a subring of E_n.

We have $W_1 = \mathbb{G}_a$; the endomorphism V of $\mathbb{G}_a$ is zero, and we have $F_A(x) = x^p$ for x in a commutative algebra A. In the theory of finite algebraic groups, the kernel $W_{n,r}$ of the endomorphism F^r of W_n plays an important role.

8.

We denote by φ the endomorphism of the field k defined by $\varphi(x) = x^p$. Moreover, for every commutative algebra A over k, we denote by φ_A the homomorphism $A \longrightarrow A_{\varphi}$ defined by $\varphi_A(a) = a^p$. Let G be an algebraic group; for every commutative algebra A, the homomorphism $F_A = G(\varphi_A)$ from G_A to $G_{A_{\varphi}} = G^{\varphi}_A$ is defined; the collection of the F_A is a homomorphism from G to G^{φ}, called the *Frobenius homomorphism.* If G is one of the groups $GL(n)$, $\mathbb{G}_a$, $\mathbb{G}_m$, W_n, we have $G^{\varphi} = G$ and the Frobenius homomorphism consists of raising each coordinate to the pth power; the notation F is thus consistent with that introduced for W_n.

Now suppose that G is commutative; we will define a homomorphism $V : G^{\varphi} \longrightarrow G$. Let L and A be two commutative algebras; in the tensor product $L \otimes A_{\varphi}$ we have the relation

$$\text{(11)} \qquad (\lambda x) \otimes a = x \otimes (\lambda^p a) = \lambda(x \otimes a)$$

for $\lambda \in k, x \in L$, and $a \in A$; it follows that there exists an algebra homomorphism $\tau_{L,A} : L \otimes A_{\varphi} \longrightarrow (L \otimes A)_{\varphi}$ defined by

$$\text{(12)} \qquad \tau_{L,A}(x \otimes a) = x^p \otimes a.$$

The homomorphism V is *characterized* by the relation

$$\text{(13)} \qquad \tau_{L,A_{\varphi}} \cdot u_A = u_A \cdot V_A$$

for every homomorphism u from G to the multiplicative group $P(L)$ of a commutative algebra L. We have

$$\text{(14)} \qquad V \cdot F = p \cdot \delta_G.$$

[10] Cf. J. Dieudonné [Die55], proof of theorem 1. The hypothesis that k is perfect is useless, by virtue of the relation (9) which permits the simplification of products $V^i R(w) F^j$. We remark that Dieudonné writes respectively p and t for what we write as F and V.

When $\mathsf{G} = W_n$, the homomorphism $\mathsf{V} : W_n^{\varphi} = W_n \to W_n$ is identical to that defined earlier. The direct *construction* of V is quite complicated and uses the following curious lemma of linear algebra [11]:

Let E be an algebra over a field k of characteristic $\mathsf{p} \neq 0$. In the algebra $\mathsf{E}^{\otimes \mathsf{p}}$, let S_p the subalgebra formed by symmetric tensors; the set of symmetrized tensors is an ideal I of S_p; then, there exists a homomorphism $u : \mathsf{S}_\mathsf{p} \to \mathsf{E}^{\varphi}$ with kernel I characterized by $u(x \otimes \cdots \otimes x) = 1 \otimes x$ for $x \in \mathsf{E}$.

9.

We are now going to state the structure theorem of unipotent commutative algebraic groups. First of all, for every integer $n > 0$, we define the homomorphisms:

$$\mathsf{G} \overset{\mathsf{F}^n}{\to} \mathsf{G}^{\varphi^n} \overset{\mathsf{V}^n}{\to} \mathsf{G}$$

We can, by suitably iterating F and V, redo the constructions of §8, by replacing p by p^n. We let U_n denote the category of commutative algebraic groups G such that the homomorphism $\mathsf{V}^n : \mathsf{G}^{\varphi^n} \to \mathsf{G}$ is zero. Moreover, for every commutative algebraic group G, we put $\mathsf{V}_n(\mathsf{G}) = \mathrm{Hom}(\mathsf{G}, W_n)$; $\mathsf{V}_n(\mathsf{G})$ has a natural structure of a left module over the ring $\mathsf{E}_n = \mathrm{Hom}(W_n, W_n)$; so V_n is a contravariant functor from the category C of commutative algebraic groups to the category of left modules over the ring E_n. We have $\mathsf{V}_n(\mathsf{G}) = 0$ if G is reductive.

Theorem 1. *Let G be a commutative algebraic group over a field k of characteristic $\mathsf{p} \neq 0$.*

a) Suppose G is of finite type. For G to be unipotent, it is necessary and sufficient that there exists an integer $n > 0$ such that $\mathsf{V}^n : \mathsf{G}^{\varphi^n} \to \mathsf{G}$ is zero.

b) Let n be a positive integer. For V^n to be zero, it is necessary and sufficient that G is isomorphic to an algebraic subgroup of the product of a family, finite or infinite, of groups W_n.

c) The functor V_n is a duality from the category U_n to the category of left modules over E_n.

The proof of a) relies on reasoning often used in the theory of linear algebraic groups; essentially, we use the characterization of unipotent matrices by the relation: $X^{\mathsf{p}^n} = 1$ for n sufficiently large, and the formula $\mathsf{V}^n\mathsf{F}^n = \mathsf{p}^n\delta_\mathsf{G}$ which demonstrates that $\mathsf{V}^n = 0$ implies $\mathsf{p}^n \cdot \delta_\mathsf{G} = 0$. The proof of b) is significantly more delicate, and uses the structure of extensions of the Witt group by another (cf. Serre [Ser59]); finally, c) results easily from b) and that W_n is an injective object in the abelian category U_n.

The structure of left modules over the ring E_n is quite well known, at least under the condition of "neglecting" modules of finite length; we can consult J. Dieudonné [Die56] O. Ore [Ore33], and P. Gabriel [Gab60]. By this type of logic, we can quite easily obtain the following result of C. Chevalley [Ser59].

Corollary. *Let k be an algebraically closed field of characteristic $\mathsf{p} \neq 0$. Every unipotent algebraic group of finite type is isogenous to a product of Witt vector groups.*

[11] Geometrically, we can say that if X is an algebraic variety, and Σ is the symmetric product of order p of X, the image in Σ of the diagonal of the product $\mathsf{X} \times \cdots \times \mathsf{X}$ is a variety isomorphic to X^{φ}.

When $n = 1$, the results of Theorem 1 are simplified. In particular, the homomorphism $V : G^{\varphi} \to G$ is zero if and only if G is isomorphic to an algebraic subgroup of a product of groups $\mathbb{G}_a$; the left modules over the ring E_1 are the vector spaces V over k, equipped with an additive operator F verifying $F(\lambda \cdot \nu) = \lambda^p \cdot F(\nu)$ for $\lambda \in k$ and $\nu \in V$. This permits addressing the study of "forms" of the group $\mathbb{G}_a$ over an imperfect field, that is, algebraic groups G which become isomorphic to $\mathbb{G}_a$ after extension of scalars from k to its algebraic closure; this is related to the study of cohomology of algebraic extensions, separable or not, problems which we discuss later.

10. Formal groups

We present formal groups in the same manner as algebraic groups. A formal group G will thus be defined as a functor from commutative algebras to groups; instead of imposing the existence of a generic point, let us assume the following axiom:

(G3) There exists a family of commutative algebras E_a *of finite rank over* k *and points* $x_a \in G_{E_a}$ *with the following properties:*

a) If σ *and* τ *are two different homomorphisms from* E_a *to an algebra* A*, then* $\sigma \cdot x_A \neq \tau \cdot x_a$.

b) Given algebras $A_1, \dots, A_n$ *and points* $g_i \in G_{A_i}$ *for* $1 \leq i \leq n$*, there exists an index* a *and homomorphisms* $\sigma_i : E_a \to A_i$ *such that* $\sigma_i \cdot x_a = g_i$.

We can repeat for formal groups a good portion of §3; we define homomorphisms, monomorphisms, epimorphisms, subgroups and quotient groups, and the same for extension of scalars. The canonical factorization lemma is again true, but the proof is different; it follows that commutative formal groups form an abelian category. Finally, if k has characteristic $p \neq 0$, we can define the homomorphisms

$$G \overset{F^n}{\to} G^{\varphi^n} \overset{V^n}{\to} G$$

and we have $V^n \cdot F^n = p^n \cdot \delta_G$. The only important difference is that in general, the *infinite* product of formal groups does not exist.

If G is a formal group, we call a *function* on G a family of transformations $f_A : G_A \to A$ (for every commutative algebra A) satisfying the relations

$$\sigma \cdot f_A = f_B \cdot G(\sigma) \tag{15}$$

for every algebra homomorphism $\sigma : A \to B$. The set of functions on G will be denoted $\mathcal{O}(G)$; it is an algebra in a natural way; for every commutative algebra A and every $x \in G_A$, we define an algebra homomorphism $\chi_X : \mathcal{O}(G) \to A$ by $\chi_x(f) = f_A(x)$. The algebras A being considered discrete, we equip $\mathcal{O}(G)$ with the coarsest topology such that each of the homomorphisms χ_x is continuous; then, $\mathcal{O}(G)$ is a topological commutative ring which is separable and complete; every neighborhood of 0 contains an open ideal, and every open ideal is of finite codimension. Finally, for every algebra A, the function $x \mapsto \chi_x$ is a bijection from G_A to the set of homomorphisms $\mathcal{O}(G) \to A$ whose kernel is an open ideal.

We call a *distribution* on the group G a linear form T on $\mathcal{O}(G)$ whose kernel is open; the vector space of distributions is denoted $U(G)$; we denote by $U^+(G)$ the set of distributions T such that $\langle T, 1 \rangle = 0$. By analogy to the theory of distributions on Lie groups, we can define the convolution product on $U(G)$, under which $U(G)$ is an associative algebra; this algebra is commutative if and only if the formal group

G is commutative. “By dualizing the multiplication” of the ring $\mathcal{O}(G)$, we can define a homomorphism $P : U(G) \to U(G)\otimes U(G)$ called the coproduct. The list of properties of P is too long to be repeated here; we can refer to [Car56b, Exposé 2], where we omit anything concerning filtrations. In brief, we say that $U(G)$ is a *hyperalgebra.*

Let A be an algebra; we can identify $U(G)\otimes A$ as a set of linear transformations $\mathcal{O}(G) \to A$, since $U(G)$ is a subspace of the dual of the vector space $\mathcal{O}(G)$. We define three homomorphisms of algebras $U(G)\otimes A \to U(G)\otimes U(G)\otimes A$ by the formulas

$$P'(T\otimes a) = P(T)\otimes a \qquad \epsilon(T\otimes a) = T\otimes 1\otimes a, \qquad \epsilon'(T\otimes a) = 1\otimes T\otimes a \tag{16}$$

So, we have $\chi_x \cdot \chi_y = \chi_{xy}$ for $x, y \in G_A$, and the transformation $x \mapsto \chi_x$ is a bijection from G_A to the set of elements Z in $U(G)\otimes A$ congruent to $1\otimes 1$ modulo $U^+(G)\otimes A$ and such that $P'(z) = \epsilon(z)\cdot\epsilon'(z)$. In fact, there is only one product and coproduct on $U(G)$ such that these properties are satisfied for every commutative algebra A.

In modern terms, Z is the set of grouplike elements of the Hopf algebra $U(G)\otimes A$.

Finally, the functor U associating a formal group G to its hyperalgebra $U(G)$ is an equivalence of categories from formal groups to that of hyperalgebras.

11. Separable and infinitesimal groups

Let $\bar{k}$ be an algebraic closure of k; we denote $\mathfrak{G}$ the group of k-automorphisms of $\bar{k}$, and we will use the terminology of Galois module for a noncommutative group on which $\mathfrak{G}$ operates such that every point has open stabilizer in $\mathfrak{G}$. Finally, we say that a commutative algebra E of finite rank over k is separable if it is a direct product of separable algebraic extensions of the field k.

Let G be a formal group. We say that G is *separable* if, for every commutative algebra A and every $g \in G_A$, there exists a separable algebra E of finite rank, $h \in G_E$ and a homomorphism $\sigma : E \to A$ such that $g = G(\sigma)\cdot h$. Suppose that G is separable; the group $G_{\bar{k}}$ is thus a Galois module for $\mathfrak{G}$, and the functor associating $G_{\bar{k}}$ to G is an equivalence from the category of separable formal groups to the category of Galois modules for $\mathfrak{G}$. If k is algebraically closed, so that $\bar{k} = k$ and $\mathfrak{G} = (1)$, the groups G_A are determined by $\Gamma = G_k$. In the group algebra of Γ with coefficients of A, we consider the elements of the form $\sum_\gamma e_\gamma \cdot \gamma$ where e_γ are idempotents of A, pairwise orthogonal, zero except for a finite number, summing to 1. Under multiplication in the group algebra of Γ, these elements form a group, which is naturally isomorphic to G_A; in particular, if every idempotent in A is equal to 0 or 1, the group G_A is isomorphic to Γ.

We say that the formal group G is *infinitesimal* if the group $G_{\bar{k}}$ is reduced to its neutral element e; in this case, $\mathcal{O}(G)$ is a local ring whose maximal ideal $\mathfrak{m}$ is the set of functions f such that $f_{\bar{k}}(e) = 0$. We say that G is infinitesimal of finite type if the ideal $\mathfrak{m}$ is generated by a finite number of elements; it is equivalent to suppose that the vector space $\mathfrak{m}/\mathfrak{m}^2$ has finite dimension; if so, the ideals $\mathfrak{m}^n$ form a fundamental system of neighborhoods of 0 in $\mathcal{O}(G)$.

Theorem 2. *Let G be a formal group over a perfect field k.*

a) We can decompose G uniquely as a semidirect product $G^s \times G^i$ by a separable subgroup G^s and an infinitesimal normal subgroup G^i.

b) *Suppose* G *is infinitesimal of finite type and* k *is of characteristic zero. Then the topological algebra* $\mathcal{O}(\mathsf{G})$ *is isomorphic to an algebra of formal power series* $\mathsf{k}[[\mathsf{T}_1, \dots, \mathsf{T}_r]]$.

c) *Suppose* G *is infinitesimal of finite type and* k *is of characteristic* $p \neq 0$. *The topological algebra* $\mathcal{O}(\mathsf{G})$ *is isomorphic to an algebra of truncated formal series* $\mathsf{k}[[\mathsf{T}_1, \dots, \mathsf{T}_{r+s}]]/(\mathsf{T}_{r+1}^{p^{n_1}}, \dots, \mathsf{T}_{r+s}^{p^{n_s}})$ *(with* $r \geq 0$*,* $s \geq 0$*,* $n_i \geq 0$*).*

The proof of a) relies on the classical theorem that an algebra of finite rank over a perfect field is a direct sum of a separable subalgebra and a nilpotent ideal. The assertion b) is a consequence of the structure theorem of the hyperalgebra of an infinitesimal group which will be given in §12; for c), it is proved in quite a laborious manner and uses the technique of Dieudonné for hyperalgebras.

The formal groups studied by Dieudonné are the infinitesimal groups such that $\mathcal{O}(\mathsf{G})$ is isomorphic to an algebra of formal power series in a finite number of variables. Let us choose an isomorphism

$$\eta : \mathsf{k}[[\mathsf{T}_1, \dots, \mathsf{T}_r]] \to \mathcal{O}(\mathsf{G})$$

and let $u_i = \eta(\mathsf{T}_i)$. Then, for every commutative algebra A, the transformation $g \mapsto ((u_1)_A(g), \dots, (u_r)_A(g))$ is a bijection from G_A to the set of vectors in A^r with nilpotent coordinates.

12. Formal groups and Lie algebras

We distinguish two very different cases, depending on whether the characteristic of k is zero or not.

Suppose first that k has characteristic zero. Let G be a formal group; in the set $\mathsf{U}(\mathsf{G})$ of distributions on G, we consider the vector subspace $\mathsf{L}(\mathsf{G})$ formed by T such that

$$\mathsf{P}(\mathsf{T}) = \mathsf{T} \otimes 1 + 1 \otimes \mathsf{T} \tag{17}$$

("primitive elements" in the sense of Hopf algebras). If T and T' are in $\mathsf{L}(\mathsf{G})$, so is $[\mathsf{T}, \mathsf{T}'] = \mathsf{T}\mathsf{T}' - \mathsf{T}'\mathsf{T}$; consequently, $\mathsf{L}(\mathsf{G})$ is a Lie algebra under the bracket above; it is the *Lie algebra of* G. Suppose that G is infinitesimal. We can define a natural isomorphism of vector spaces from $\mathsf{L}(\mathsf{G})$ to the dual of $\mathfrak{m}/\mathfrak{m}^2$ (where $\mathfrak{m}$ is the maximal ideal of $\mathcal{O}(\mathsf{G})$); it follows that G is of finite type if and only if the Lie algebra $\mathsf{L}(\mathsf{G})$ is of finite dimension.

Theorem 3. *Let* k *be a field of characteristic zero.*

a) *If* G *is an infinitesimal group over* k*, the associative algebra* $\mathsf{U}(\mathsf{G})$ *is the universal enveloping algebra*[12] *of the Lie algebra* $\mathsf{L}(\mathsf{G})$*.*

b) *The functor* L *is an equivalence of categories from infinitesimal groups to Lie algebras.*

Theorem 3 a) easily implies Theorem 2 b) by means of the Poincaré-Birkhoff-Witt theorem (cf. N. Bourbaki [Bou60]).

Let $\mathfrak{g}$ be a Lie algebra. We can construct as follows an infinitesimal group G whose Lie algebra is isomorphic to $\mathfrak{g}$. Let A be a commutative algebra and let $\mathfrak{n}(A)$

[12] This signifies that every linear map f from $\mathsf{L}(\mathsf{G})$ to an associative algebra R satisfying $f([x, y]) = f(x)f(y) - f(y)f(x)$ has a unique extension to an algebra homomorphism $\mathsf{U}(\mathsf{G}) \to \mathsf{R}$.

be the ideal of nilpotent elements of A. On the tensor product $\mathfrak{g} \otimes \mathfrak{n}(A)$, we define the structure of a Lie algebra by the formula:

$$[x \otimes a, y \otimes b] = [x, y] \otimes ab. \tag{18}$$

Then, on the Lie algebra $\mathfrak{g} \otimes \mathfrak{n}(A)$, one defines the structure of a group by means of the formula of Campbell-Hausdorff-Dynkin:

$$x \cdot y = \sum \left(\sum_i (p_i + q_i) \right)^{-1} \left(\prod_i (-1)^{p_i+q_i} p_i! q_i! \right)^{-1} \underbrace{[x_1, [\ldots, [x_1,}_{p_1} \underbrace{[x_2, [\ldots, [x_2,}_{q_1} \ldots \underbrace{[x_1, \ldots, [x_1,}_{p_m} x_2] \ldots] \tag{19}$$

the sum being extended over all systems of integers $p_1, \ldots, p_m, q_1, \ldots, q_m$ with general m and with either $q_m = 1$ or $p_m = 1$ and $q_m = 0$. Let G_A be the group defined by the law (19) on the set $\mathfrak{g} \otimes \mathfrak{n}(A)$; if $\sigma : A \to B$ is an algebra homomorphism, the transformation $I \otimes \sigma : \mathfrak{g} \otimes A \to \mathfrak{g} \otimes B$ restricts to a homomorphism of groups $G(\sigma) : G_A \to G_B$ (where I is the identity transformation of $\mathfrak{g}$). This achieves the construction of G.

13.

Now we study the case when k has characteristic $p \neq 0$. Let G be a formal group. We define the Lie algebra $L(G)$ as in §12; but, for $T \in L(G)$, one also has $T^p \in L(G)$, so that $L(G)$ is a p-Lie algebra in the sense of Jacobson [Jac37]. When G is commutative, one can relate this p-operation in $L(G)$ to the homomorphism $V : G^\varphi \to G$; indeed, one can identify $L(G^\varphi)$ with the Lie algebra $L(G)^\varphi$; and the Lie algebra homomorphism $\eta : L(G)^\varphi \to L(G)$ induced by V is given by the formula

$$\eta(x \otimes T) = x \cdot T^p \qquad (x \in k, T \in L(G)) \tag{20}$$

Moreover, Theorem 3 has the following analogue here:

Theorem 4. *Let k be a field of characteristic $p \neq 0$.*

a) Let G be a formal group over k. For G to be infinitesimal, it is necessary and sufficient that for every algebra A, the group G_A is the union of the kernels of the homomorphisms $F^n_A : G_A \to G_A^{\varphi^n}$.
b) Let G be a formal group such that the homomorphism F is trivial. Then the associative algebra $U(G)$ is the universal enveloping algebra [13] of the p-Lie algebra $L(G)$.
c) The functor L is an equivalence from the category of formal groups where the Frobenius homomorphism is trivial and the category of p-Lie algebras.

For the moment, we do not know how to generalize b) and c) to the formal groups where F^n is trivial. The question is linked to a non-commutative generalization of Theorem 1, by means of the theory of duality.

[13] Cf. 12 but it suffices to impose on f the extra relation $f(x^p) = f(x)^p$.

14. Duality between algebraic groups and formal groups

We consider the category C of commutative algebraic groups and the category F of commutative formal groups. First of all, given a group G from C and a group H from F, we say a *coupling* of G and H is a family of bilinear transformations:

$$u_A : G_A \times H_A \to (\mathbb{G}_m)_A$$

(for every commutative algebra A) verifying the commutation relations:

$$u_B(G(\sigma) \cdot g, H(\sigma) \cdot h) = \sigma \cdot u_A(g, h) \tag{21}$$

for every algebra homomorphism $\sigma : A \to B$, $g \in G_A$ and $h \in H_A$. The set of couplings of G and H is a commutative group denoted $\mathrm{Acc}(G, H)$; it is a contravariant bifunctor in G and H.

We can thus construct two contravariant functors:

$$D : C \to F \qquad D' : F \to C$$

whose description matters little, except for that it is characterised by the following assertion a).

a) *There exist isomorphisms from* $\mathrm{Acc}(G, H)$ *to* $\mathrm{Hom}(G, D'(H))$ *and to* $\mathrm{Hom}(H, D(G))$*, functorial in* G *and* H*.*
b) *Every commutative algebraic group* G *is isomorphic to* $D'(D(G))$ *by means of a certain canonical homomorphism; just the same, every commutative formal group* H *is isomorphic to* $D(D'(H))$*.*
c) *The functors* D *and* D' *are dualities.*

We say that the formal group $D(G)$ is the *dual* of the commutative algebraic group G; we quote assertion b) by the name of the biduality theorem. It follows from the explicit construction of $D(G)$ that we have:

$$D(G)_k = \mathrm{Hom}(G, \mathbb{G}_m). \tag{22}$$

By means of the duality, we easily translate between properties of algebraic groups and properties of formal groups. For example, for the commutative algebraic group G to be reductive (resp. unipotent), it is necessary and sufficient that the commutative formal group $D(G)$ to be separable (resp. infinitesimal).

Suppose that k has characteristic $p \neq 0$. We identify the formal groups $D(G^\varphi)$ and $D(G)^\varphi$; this being done, the sequence of homomorphisms:

$$G \xrightarrow{F} G^\varphi \xrightarrow{V} G$$

is transformed by the contravariant functor D to the sequence:

$$D(G) \xleftarrow{V} D(G)^\varphi \xleftarrow{F} D(G)$$

This property gives a very natural construction of the homomorphism $V : G^\varphi \to G$ by means of the Frobenius homomorphism of formal groups and the duality.

If we take into account Theorems 1 and 4, we obtain the structure theorem for infinitesimal commutative groups.

Theorem 5. *For every formal commutative group* G*, set:*

$$V'_n(G) = \mathrm{Hom}(D(W_n), G)$$

The functor V'_n *is an equivalence between the category of commutative formal groups where* F^n *is zero and the category of left modules for the ring* E_n*.*

By means of passing to the limit in n, the previous theorem easily recovers the fundamental theorem of DIEUDONNÉ [Die55] on the structure of commutative infinitesimal groups.

Examples:

1) The dual of $\mathbb{G}_m$ is the separable formal group associated to the group of integers on which the Galois group $\mathfrak{G}$ of $\bar{k}$ over k acts trivially.
2) Let G be a reductive commutative algebraic group. The dual $D(G)$ is the separable formal group associated to the Galois module $X(G)$ defined in §5.
3) Let $r \geq 2$ be an integer; we denote by μ_r the kernel of the homomorphism $r \cdot \delta_{\mathbb{G}_m} : \mathbb{G}_m \to \mathbb{G}_m$. It is a reductive algebraic group, and the dual is a separable formal group associated to the additive group of integers modulo r on which the Galois group $\mathfrak{G}$ of $\bar{k}$ over k acts trivially.
4) Let W be the formal group dual to $\mathbb{G}_a$. For every commutative algebra A, the group W_A is the multiplicative group of polynomials $P(T)$ with coefficients in A verifying

$$P(T + T') = P(T) \cdot P(T') \tag{23}$$

("multiplicative polynomials"). When k is of characteristic zero, these polynomials are e^{aT} where $a \in A$ is nilpotent; we can identify W_A with the additive group of nilpotent elements in A. When k is of characteristic $p \neq 0$, the general form of multiplicative polynomials is the following:

$$P(T) = \prod_{i \geq 0} \exp(a_i T^{p^i}) \tag{24}$$

where all but finitely many a_i are zero and all pth powers are zero, so that the exponential series written above make sense. One can identify W_A with the additive group of Witt vectors $(a_0, a_1, \dots)$ with infinite length where all the coordinates verify $a_i^p = 0$ and are zero except for a finite number of entries.
5) By means of the Hasse-Witt exponentail, we can define a coupling of $W_{n,r}$ with $W_{r,n}$ which defines an isomorphism of each of these groups with the dual of the other ($W_{n,r}$ is both an algebraic group and a formal group).

15. Relations between algebraic groups and formal groups

They are of two kinds. First of all, to every algebraic group G, we can associate a formal group $\hat{G}$ called the *completion* of G; the group $\hat{G}_A$ is the subgroup of G_A formed by g for which there exists a commutative algebra E of finite rank, $h \in G_E$ and a homomorphism $\alpha : E \to A$ such that $g = G(\alpha) \cdot h$; moreover, for every algebra homomorphism $\sigma : A \to B$, the homomorphism $\hat{G}(\sigma)$ is the restriction of $G(\sigma)$ to $\hat{G}_A$. We can relate this operation of completion to the operation of completion to a topological ring; to simplify, we suppose that G is of finite type and that k is algebraically closed. We can define the notion of a function on an algebraic group as in the case of formal groups; the functions on G form an algebra $\mathcal{O}(G)$, and for every point $x \in G_k$, the functions f on G where $f_k(x) = 0$ form a maximal ideal $\mathfrak{m}_x$ of the algebra $\mathcal{O}(G)$; moreover, the algebra $\mathcal{O}(G)$ has a finite number of generators, and the Hilbert Nullstellensatz implies that the correspondence $x \mapsto \mathfrak{m}_x$ is a bijection from G_k to the set of maximal ideals of $\mathcal{O}(G)$. Then, *the algebra $\mathcal{O}(\hat{G})$ of functions on the formal group $\hat{G}$ is isomorphic to the product of completed local rings of $\mathcal{O}(G)$ at the prime ideals $\mathfrak{m}_x$ (x running over G_k).*

Suppose that k has characteristic zero. By using the decomposition of $\hat{\mathsf{G}}$ as a semidirect product of a separable group $\hat{\mathsf{G}}^s$ and an infinitesimal group $\hat{\mathsf{G}}^{\mathsf{i}}$, we see that all the complete local rings earlier are isomorphic to $\mathcal{O}(\hat{\mathsf{G}}^{\mathsf{i}})$; but, $\hat{\mathsf{G}}^{\mathsf{i}}$ is a infinitesimal group of finite type, and so by Theorem 2 b), the ring $\mathcal{O}(\hat{\mathsf{G}}^{\mathsf{i}})$ is isomorphic to a ring of formal power series, therefore without nilpotent elements. Since $\mathcal{O}(\mathsf{G})$ is a subring of $\mathcal{O}(\hat{\mathsf{G}})$, it follows easily that *the ring* $\mathcal{O}(\mathsf{G})$ *has no nonzero nilpotent elements*[14].

16.

For a functor from algebras to groups to be a finite algebraic group, it is necessary and sufficient that it verifies the axioms (G2) and (G3), which is to say that it is both a formal group and an algebraic group.

The theory of duality thus furnishes an autoduality on the category of finite commutative algebraic groups; in this case, we have $\mathsf{D}(\mathsf{G}) = \mathsf{D}'(\mathsf{G})$, so that G is isomorphic to $\mathsf{D}(\mathsf{D}(\mathsf{G}))$; what's more, we can define a natural isomorphism of algebras from $\mathsf{U}(\mathsf{G})$ to $\mathcal{O}(\mathsf{D}(\mathsf{G}))$ and from $\mathcal{O}(\mathsf{G})$ to $\mathsf{U}(\mathsf{D}(\mathsf{G}))$[15].

If k is of characteristic zero, the finite algebraic groups are all separable and correspond to finite Galois modules. If k is perfect of characteristic $\mathsf{p} \neq 0$, every finite *commutative* algebraic group is written in a unique manner in the form

$$\mathsf{G} = \mathsf{G}^{sr} \times \mathsf{G}^{su} \times \mathsf{G}^{ir} \times \mathsf{G}^{iu}$$

G^{sr} separable and reductive

G^{su} separable and unipotent

G^{ir} infinitesimal and reductive

G^{iu} infinitesimal and unipotent

Moreover, G^{sr} corresponds to a finite Galois module of order prime to p, G^{su} to a finite Galois module of order a power of p, G^{ir} the dual of a formal group corresponding to a finite Galois module of order a power of p; finally, G^{iu} is a piece not reducible to the usual Galois theory, but, by Theorem 5, we can make it correspond to a module of finite length over a ring derived from the E_n by passage to the limit. We refer to the study of P. Gabriel [Gab60].

Without entering into the theory of abelian varieties, we mention only that the kernel of an isogeny $\alpha : \mathsf{A} \to \mathsf{B}$ of abelian varieties is a finite commutative algebraic group N. If ${}^t\alpha : \mathrm{Pic}(\mathsf{B}) \to \mathrm{Pic}(\mathsf{A})$ is the dual isogeny to α, we can show that the kernel of ${}^t\alpha$ is isomorphic to $\mathsf{D}(\mathsf{N})$ in a natural way.

References

[Bar56] Barsotti, I. "Abelian varieties over fields of positive characteristic". In: *Rend. Circ. Mat. Palermo (2)* 5 (1956), pp. 145–169. DOI: 10.1007/BF02854352. MR: 83181

[14] Similar reasoning proves that a group scheme of finite type over a field of characteristic zero is *reduced*.

[15] We thus recover the definition of dual due to Gabriel [Gab60].

[Bou60] Bourbaki, N. *Éléments de mathématique. XXVI. Groupes et algèbres de Lie. Chapitre 1: Algèbres de Lie.* Vol. No. 1285. Actualités Scientifiques et Industrielles [Current Scientific and Industrial Topics]. Hermann, Paris, 1960. MR: 132805

[Car56a] Cartier, P. "Dualité de Tannaka des groupes et des algèbres de Lie". In: *C. R. Acad. Sci. Paris* 242 (1956), pp. 322–325. MR: 75536

[Car56b] Cartier, P. "Hyperalgèbres et groupes formels". In: *Séminaire "Sophus Lie".* Vol. 2. talk 2. Secrétariat Mathématique, 1955-1956. MR: 87895

[Car59] Cartier, P. "Isogénies des variétés de groupes". In: *Bull. Soc. Math. France* 87 (1959), pp. 191–220. DOI: 10.24033/bsmf.1518. MR: 116018

[Che46] Chevalley, C. *Theory of Lie groups. I.* Princeton University Press, Princeton, NJ, 1946. MR: 82628

[Che51] Chevalley, C. *Théorie des groupes de Lie. Tome II. Groupes algébriques.* Actualités Scientifiques et Industrielles [Current Scientific and Industrial Topics], No. 1152. Hermann & Cie, Paris, 1951. MR: 51242

[Die55] Dieudonné, J. "Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$. IV". In: *Amer. J. Math.* 77 (1955), pp. 429–452. DOI: 10.2307/2372633. MR: 71718

[Die56] Dieudonné, J. "Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$. V". In: *Bull. Soc. Math. France* 84 (1956), pp. 207–239. DOI: 10.24033/bsmf.1470. MR: 94412

[Gab60] Gabriel, P. *Sur les catégories abéliennes localement noethériennes et leurs applications aux algèbres étudiées par Dieudonné.* mimeographed. 1960. Translator's Note: Gabriel published "Des catégories abeliénnes" on this topic in 1962. DOI: 10.24033/bsmf.1583.

[GD71] Grothendieck, A. and Dieudonné, J. A. *Éléments de géométrie algébrique. I.* Vol. 166. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer, 1971. MR: 3075000

[Gro57] Grothendieck, A. "Sur quelques points d'algèbre homologique". In: *Tohoku Math. J. (2)* 9 (1957), pp. 119–221. DOI: 10.2748/tmj/1178244839. MR: 102537

[Jac37] Jacobson, N. "Abstract derivation and Lie algebras". In: *Trans. Amer. Math. Soc.* 42.2 (1937), pp. 206–224. DOI: 10.2307/1989656. MR: 1501922

[Ore33] Ore, O. "Theory of non-commutative polynomials". In: *Ann. of Math. (2)* 34.3 (1933), pp. 480–508. DOI: 10.2307/1968173. MR: 1503119

[Ser59] Serre, J.-P. *Groupes algébriques et corps de classes.* Publications de l'Institut de Mathématique de l'Université de Nancago, VII. Hermann, Paris, 1959. MR: 103191

[Ser60] Serre, J.-P. "Groupes proalgébriques". In: *Inst. Hautes Études Sci. Publ. Math.* 7 (1960). DOI: 10.1007/BF02699186. MR: 118722

[Wei53] Weil, A. "Théorie des points proches sur les variétés différentiables". In: *Géométrie différentielle. Colloques Internationaux du Centre National de la Recherche Scientifique, Strasbourg, 1953.* CNRS, Paris, 1953, pp. 111–117. MR: 61455

Translated by JOSHUA MUNDINGER