Lectures on p-divisible groups

September 2023

Contents

1 Schemes and formal schemes **3**

1.1 k-functors . . . 3
1.2 Affine k-schemes . . . 4
1.3 Closed and open subfunctors; schemes . . . 5
1.4 The geometric point of view . . . 6
1.5 Finiteness conditions . . . 7
1.6 The four definitions of formal schemes . . . 7
1.7 Operations on formal schemes . . . 11
1.8 Constant and etale schemes . . . 12
1.9 The Frobenius morphism . . . 13
1.10 Frobenius map and symmetric products . . . 14

2 Group-schemes and Formal Group-schemes **15**

2.1 Group-functors . . . 15
2.2 Constant and etale k-groups . . . 16
2.3 Affine k-groups . . . 16
2.4 k-formal-groups, Catier duality . . . 18
2.5 The Frobenius and the Verschiebung morphisms . . . 19
2.6 The category of affine k-groups . . . 20
2.7 Etale and constant formal-groups . . . 22
2.8 Multiplicative affine groups . . . 24
2.9 Unipotent affine groups. Decomposition of affine groups . . . 25
2.10 Smooth formal-groups . . . 26
2.11 p-divisible groups . . . 29

2.12 Appendix 31

3 Witt Groups and Dieudonne Modules **31**

3.1 The Artin-Hasse exponential series 31

3.2 The Witt rings (over $\mathbb{Z}$) 33

3.3 The Witt rings (over k) 35

3.4 Duality of finite Witt groups 37

3.5 Dieudonne modules (Affine unipotent groups) 38

3.6 Dieudonne modules (p-torsion finite k-groups) 40

3.7 Dieudonne modules (p-divisible groups) 42

3.8 Dieudonne modules (connected formal group of finite type) 44

4 Classification of p-divisible groups **44**

4.1 Isogenies 44

4.2 The category of F-spaces 45

4.3 The F-spaces E^λ, $\lambda \geq 0$ 46

A very useful link: https://ncatlab.org/nlab/show/Demazure%2C+lectures+on+p-divisible+groups.

1 Schemes and formal schemes

1.1 k-functors

Definition 1.1.1. Let k be a ring and $\mathbf{M}_k$ be the category of k-rings (i.e., commutative associated k-algebras with unit, or simply couples (R, φ) where R is a ring and $\varphi : k \to R$ a morphism). Actually, for set-theoretically reasons, one should not take the category of all k-rings, but a smaller one (see [DG70] page XXV-XXVI) but we shall not bother about this point.

A k-functor is by definition a covariant functor from $\mathbf{M}_k$ to the category **Set**. The category of k-functors is denoted by $\mathbf{M}_k\mathrm{E}$.

Example 1. The affine line $\mathbf{O}_k$ is defined by $R \mapsto R$, $R \in \mathbf{M}_k$.

Remark 1.1.2. *If $\varphi : R \to S$ is an arrow of $\boldsymbol{M}_k$, if $X \in \boldsymbol{M}_k\mathrm{E}$, and if $x \in X(R)$, we shall write x_S (or sometimes x) instead of $X(\varphi)(x) \in X(S)$; if $f : X \to Y$ is an arrow of $\boldsymbol{M}_k\mathrm{E}$, if $R \in \boldsymbol{M}_k$ and $x \in X(R)$, we shall write $f(x)$ instead of $f(R)(x) \in Y(R)$; with these notations, the fact that f is a morphism of functors amounts to $f(x)_S = f(x_S)$.*

Proposition 1.1.3. The category $\mathbf{M}_k\mathrm{E}$ has projective limits, for example:

(a) a final object e is defined by $e(R) = \varnothing$, $R \in \mathbf{M}_k$,

(b) if $X, Y \in \mathbf{M}_k\mathrm{E}$, the product $X \times Y$ is defined by $(X \times Y)(R) = X(R) \times Y(R)$,

(c) if $X \xrightarrow{f} Z \xleftarrow{g} Y$ is a diagram of $\mathbf{M}_k\mathrm{E}$, the fibre product $T = X \times_Z Y$ is defined by

$$T(R) = X(R) \times_{Z(R)} Y(R) = \{(x, y) \in X(R) \times Y(R),\ f(x) = g(y)\}$$

more generally, one has $(\lim_{\leftarrow} X_i)(R) = \lim_{\leftarrow} X_i(R)$,

(d) $f : X \to Y$ is a monomorphism if and only if $f(R) : X(R) \to Y(R)$ is injective for each R. We say that X is a subfunctor of Y if $X(R) \subseteq Y(R)$ and $f(R)$ is the inclusion, for all R.

Proposition 1.1.4. Let $k' \in \mathbf{M}_k$; as any k'-algebra can be viewed as a k-algebra, there is an obvious functor $\mathbf{M}_{k'} \to \mathbf{M}_k$ and therefore an obvious functor $\mathbf{M}_k\mathrm{E} \to \mathbf{M}_{k'}\mathrm{E}$; the latter is denoted by $X \mapsto X \otimes_k k'$. So, if R is a k'-ring and $R_{[k]}$ the underlying k-ring, one has

$$(X \otimes_k k')(R) = X(R_{[k]})$$

the functor $X \mapsto X \otimes k'$ is called the base-change functor or scalar-extension functor. It commutes with projective limit, hence is left-exact. For instance, $\mathbf{O}_k \otimes_k k'$ can be (and will be) identified with $\mathbf{O}_{k'}$.

1.2 Affine k-schemes

Definition 1.2.1. Let $A \in \mathbf{M}_k$, the k-functor $\mathrm{Sp}_k A$ (or simply $\mathrm{Sp}A$) is defined by

$$(\mathrm{Sp}_k A)(R) = \mathrm{Mor}_{\mathbf{M}_k}(A, R)$$

$$(\mathrm{Sp}_k A)(\varphi) = \{\psi \mapsto \varphi \circ \psi\} \quad \text{for } \varphi : R \to S$$

if $f : A \to B$ is an arrow of $\mathbf{M}_k$, then $\mathrm{Sp}_k f : \mathrm{Sp}_k B \to \mathrm{Sp}_k A$ is obviously defined. So $A \mapsto \mathrm{Sp}_k A$ is a contravariant functor from $\mathbf{M}_k$ to $\mathbf{M}_k\mathrm{E}$.

An affine k-scheme is a k-functor isomorphic to a $\mathrm{Sp}_k A$. For instance $\mathbf{O}_k$ is an affine k-scheme because

$$(\mathrm{Sp}_k k[T])(R) = \mathrm{Mor}_{\mathbf{M}_k}(k[T], R) \cong R = \mathbf{O}_k(R)$$

Remark 1.2.2. *Let X be a k-functor, and A a k-ring. We have the very simple and very important Yoneda bijection*

$$\mathrm{Mor}_{\boldsymbol{M}_k\mathrm{E}}(\mathrm{Sp}_k A, X) \xrightarrow{\sim} X(A)$$

to $f : \mathrm{Sp}_k A \to X$ is associated $\xi = f(\mathrm{id}_A)[= f(A)(\mathrm{id}_A)] \in X(A)$; conversely, if $\xi \in X(A)$ and $\varphi \in \mathrm{Sp}_k(A)(R) = \mathrm{Mor}_{\boldsymbol{M}_k}(A, R)$, we put $f(\varphi) = X(\varphi)(\xi)$; with our notation, the correspondence between f and ξ is simply $f(\varphi) = \varphi(\xi)$.

As an example, we take $X = \mathrm{Sp}_k B$; then $X(A) = \mathrm{Mor}_{\boldsymbol{M}_k}(B, A)$, and we have a bijection

$$\mathrm{Mor}_{\boldsymbol{M}_k\mathrm{E}}(\mathrm{Sp}_k A, \mathrm{Sp}_k B) \cong \mathrm{Mor}_{\boldsymbol{M}_k}(B, A)$$

it means that $A \mapsto \mathrm{Sp}_k A$ is fully faithful, or equivalently that it induces an anti-equivalence between the category of k-rings and the category of affine k-schemes.

This fundamental equivalence can also be looked at in the following way: Let X be any k-functor; define a functor on X to be a morphism $f : X \to \boldsymbol{O}_k$, i.e., a functorial system of maps $X(R) \to R$. The set of these functions, say $\mathcal{O}(X)$, has an obvious k-ring structure: if $f, g \in \mathcal{O}(X)$, $\lambda \in k$, then

$$(f + g)(x) = f(x) + g(x)$$

$$(fg)(x) = f(x)g(x)$$

$$(\lambda f)(x) = \lambda f(x)$$

for any $R \in \boldsymbol{M}_k$ and any $x \in X(R)$. If $x \in X(R)$ is fixed, then by the very definition of the k-ring structure of $\mathcal{O}(X)$, $f \mapsto f(x)$ is an element $\mathrm{Mor}_{\boldsymbol{M}_k}(\mathcal{O}(X), R) = \mathrm{Sp}\mathcal{O}(X)$; we therefore have a canonical morphism

$$\alpha : X \to \mathrm{Sp}\mathcal{O}(X)$$

It is easily seen that α is universal with respect to morphisms of X into affine k-schemes (any such morphism can be uniquely factorized through α). The definition of affine k-schemes can be rephrased as: X is an affine k-scheme if and only if α is an isomorphism. For instance $\mathcal{O}(\boldsymbol{O}_k)$ is the polynomial algebra $k[T]$ generated by the identity morphism $T : \boldsymbol{O}_k \to \boldsymbol{O}_k$.

The functor $A \mapsto \mathrm{Sp}_k A$ commutes with projective limits and base change: one has the following obvious isomorphisms:

$$\mathrm{Sp}(A) \times_{\mathrm{Sp}(C)} \mathrm{Sp}(B) \cong \mathrm{Sp}(A \otimes_C B)$$

$$\lim_{\leftarrow} \mathrm{Sp}(A_i) \cong \mathrm{Sp}(\lim_{\rightarrow} A_i)$$

$$\mathrm{Sp}_k(A) \otimes_k k' \cong \mathrm{Sp}_k(A \otimes_k k')$$

(the last one explaining the notation $\otimes$ for base change); as a consequence, the full subcategory of affine schemes is stable under projective limits and base-change.

1.3 Closed and open subfunctors; schemes

Definition 1.3.1. Let X be a k-functor and E be a set of functions on X; $E \subseteq \mathcal{O}(X)$. We define two subfunctors $V(E)$ and $D(E)$ of X:

$$V(E)(R) = \{x \in X(R) | f(x) = 0,\ \forall f \in E\}$$

$$D(E)(R) = \{x \in X(R) | f(x) \text{ for } f \in E, \text{ generate the unit ideal of } R\}$$

If $U : Y \to X$ is a morphism of k-functors and $F = \{f \circ u, f \in E\} \subseteq \mathcal{O}(Y)$, then $u^{-1}(V(E)) = V(F)$, $u^{-1}(D(E)) = D(F)$ [if $u : Y \to X$ is a morphism of k-functors and Z is a subfactor of X, then $u^{-1}(Z)$ is defined as the subfactor of Y such that $u^{-1}(Z)(R) = \{y \in Y(R) | u(y) \in Z(R)\}$].

Proposition 1.3.2. If X is an affine k-scheme, then

(1) $V(E)$ is an affine k-scheme with $\mathcal{O}(V(E)) = \mathcal{O}(X)/E(\mathcal{O}(X))$,

(2) if $E = \{f\}$ has only one element, then $D(E)$ is an affine k-scheme with $\mathcal{O}(D(\{f\})) = \mathcal{O}(X)[f^{-1}] = \mathcal{O}(X)[T]/(Tf - 1)$.

Proof. If $X = \mathrm{Sp}A$, and $E \subseteq A = \mathcal{O}(X)$, then for all $R \in \mathbf{M}_k$,

$$V(E)(R) = \{\varphi \in \mathrm{Mor}_{\mathbf{M}_k}(A, R) | \varphi(E) = 0\} \cong \mathrm{Mor}_{\mathbf{M}_k}(A/EA, R)$$

$$D(\{f\})(R) = \{\varphi \in \mathrm{Mor}_{\mathbf{M}_k}(A, R) | \varphi(f) \text{ is invertible}\} \cong \mathrm{Mor}_{\mathbf{M}_k}(A[f^{-1}], R)$$

■

Definition 1.3.3. The subfunctor Y of X is said to be closed (resp. open) if for any morphism $u : T \to X$ where T is an affine scheme, the subfunctor $u^{-1}(Y)$ of T is of the form $V(E)$ (resp. $D(E)$).

For instance, if X is affine, then Y is closed (resp. open) if and only if it is a $V(E)$ (resp. $D(E)$). As a corollary, a closed subfunctor of an affine k-scheme is also an affine k-scheme; this need not be true for open subfunctors: take $X = \mathrm{Sp}k[T, T'] \cong \mathbf{O}_k^2$ and $Y = D(\{T, T'\})$.

Definition 1.3.4. In the functorial setting, the precise definition of a not-necessarily affine k-scheme k-scheme is a bit complicated. Let us give it for the sake of completeness:

The k-functor X is a scheme if:

(1) [X is a sheaf for the Zariski Grothendieck topology on $\mathbf{M}_k^{\mathrm{op}}$] it is a "local" k-functor: for any k-ring R and any "partition of unity" f_i of R (= family of elements of R such that $\sum Rf_i = R$), given elements $x_i \in X(R[f_i^{-1}])$ such that the images of x_i and x_j in $X(R[f_i^{-1}f_j^{-1}])$ coincide for all couples (i, j), then there exists one and only one $x \in X(R)$ which maps on to the x_i.

(2) [X has a cover of Zariski open immersions of affine k-schemes] There exists a family (U_j) of open subfunctors with the following properties: each U_j is an affine k-functor; for any field $K \in \mathbf{M}_k$, $X(K)$ is the union of the $U_j(K)$.

Proposition 1.3.5. (1) An open or closed subfunctor of a k-functor is a k-scheme,

(2) any finite projective limit (e.g. fibre product) of k-schemes is a k-scheme,

(3) if X is a k-scheme, then $X \otimes_k k'$ is a k'-scheme.

Remark 1.3.6. *As an illustration of (1), let $A \in \boldsymbol{M}_k$ and $E \subseteq A(\cong \mathcal{O}(\mathrm{Sp}A))$; then $D(E) \subseteq \mathrm{Sp}A$ is a k-scheme, because it is local and covered by the affine k-schemes $D(\{f\})$, $f \in E$.*

Also note that the limit of a directed projective system of schemes is not generally a scheme.

1.4 The geometric point of view

Definition 1.4.1. Let X be a k-functor; we want to define a geometric space (topological space with a sheaf of local rings) $|X|$ associated to X.

First, the underlying set of X is defined as follows: a point of $|X|$ is an equivalence class of elements of all $X(K)$ where K runs through the fields of $\mathbf{M}_k$, $x \in X(K)$ and $x' \in X(K')$ being equivalent if there exist two morphisms of $\mathbf{M}_k$, say $K \to L$, $K' \to L$, where L is a field with $x_L = x'_L$.

Second, the topology. If Y is a subfunctor of X, then $|Y|$ can be identified with a subset of $|X|$; we define a subset U of $|X|$ to be open if there exists an open subfunctor Y of X, such that $|Y| = U$; moreover, such a Y can be proved to be unique, and we write $Y = X_U$.

Third, the sheaf is the associated sheaf to the presheaf of rings $U \to \mathcal{O}(X_U)$.

Example 2. As an example, take $X = \mathrm{Sp}A$, $A \in \mathbf{M}_k$. Then $|\mathrm{Sp}A|$ is the usual spectrum $\mathrm{Spec}A$ of A; the points of $\mathrm{Spec}A$ are the prime ideals of A; the open sets are the $|D(S)| = \{\mathfrak{p} | S \not\subseteq \mathfrak{p}\}$, $S \subseteq A$, the sheaf is associated to the presheaf $|D(S)| \to A[S^{-1}]$. (One basic theorem asserts that the ring of sections of the sheaf over $|D(\{f\})|$ is $A[f^{-1}]$).

In the general case, for all $A \in \mathbf{M}_k$, and all $\xi \in X(A)$, the Yoneda morphism $\mathrm{Sp}A \to X$ associated to ξ defines a ringed-space morphism $\mathrm{Spec}A \to |X|$ and $|X|$ can be proved to be the inductive limit of the (non-directed) system of the $\mathrm{Spec}A$. ([DG70] I, section 1, n^o4)

Theorem 1.4.2. One has the following comparison theorem ([DG70] I, section 1, 4.4):

$X \mapsto |X|$ induces an equivalence between the category of k-schemes and the category of geometric spaces locally isomorphic to a $\mathrm{Spec}A$, $A \in \mathbf{M}_k$.

Remark 1.4.3. *One can give a quasi-inverse functor: there is a functorial bijection between $X(R)$ and the set of geometric-space-morphisms from $\mathrm{Spec}R$ to $|X|$, as follows from the theorem and Yoneda's isomorphism.*

By this equivalence, one defines geometric objects associated to the k-scheme X: the local ring $\mathcal{O}_{X,x}$ and the residue field $\kappa(x)$, $x \in |X|$; all are k-rings.

1.5 Finiteness conditions

Definition 1.5.1. Let k be a field. A k-scheme X is said to be finite if it is affine and if $\mathcal{O}(X)$ is a finite dimensional vector space; if X is finite, then $[\mathcal{O}(X) : k]$ is called the rank $\mathrm{rk}(X)$ of X. A k-scheme X is locally algebraic (algebraic) if it has a covering (a finite covering) by open subfunctors X_i which are affine k-schemes such that each $\mathcal{O}(X_i)$ is a finitely generated k-algebra.

Proposition 1.5.2. If X is an affine k-scheme, then the following conditions are equivalent:

(1) X is algebraic,

(2) X is locally algebraic,

(3) $\mathcal{O}(X)$ is a finitely generated k-algebra.

([DG70] I,section 3, 1.7)

Proposition 1.5.3. (1) It follows from the Normalization lemma that X is finite if and only if X is algebraic and $|X|$ is finite.

(2) It follows from the Nullstellensatz that if X is locally algebraic and $\neq \varnothing$ (one defines $\varnothing(R) = \varnothing$ for all R, or equivalently $|\varnothing| = \varnothing$), then $X(K) \neq \varnothing$ for some finite extension K of k.

(3) Let X be a (locally) algebraic k-scheme, k algebraically closed; then if U is an open subfunctor of X, $U(k) = \varnothing$ implies $U = \varnothing$. This easily implies that if one views $X(k)$ as the subspace of $|X|$ whose points are the $x \in |X|$ such that $\kappa(x) = k$, the open subsets of $|X|$ and the open subsets of $X(k)$ are in a bijection correspondence (by $|U| \mapsto U(k)$).

It is therefore equivalent to know the k-scheme X, or the k-geometric space $X(k)$ - the only difference between the $X(k)$'s and Serre's algebraic spaces lies in that the latter have no nilpotent elements in their local rings, whereas the former may have. As we shall see late, this is an important difference. Serre's algebraic spaces correspond to "reduced" algebraic k-schemes (i.e., with no nilpotent elements). A similar disscussion can be made in the case of a general field k; one has to replace $X(k)$ by the set of closed points of $|X|$ (by the Nullstellensatz, $x \in |X|$ is closed if and only if $\kappa(x)$ is a finite extension of k).

1.6 The four definitions of formal schemes

From now on, k is assumed to be a field.

Definition 1.6.1. We denote by $\mathbf{Mf}_k$ the full subcategory of $\mathbf{M}_k$ consisting of finite (= finite dimensional) k-rings. A k-formal functor is a covariant functor $F : \mathbf{Mf}_k \to \mathbf{Set}$; the category of k-formal functors is denoted by $\mathbf{Mf}_k\mathrm{E}$; this category has finite projective limits. The inclusion functor $\mathbf{Mf}_k \to \mathbf{M}_k$ gives a canonical functor $\mathbf{M}_k\mathrm{E} \to \mathbf{Mf}_k\mathrm{E}$ called the completion functor: if $X \in \mathbf{M}_k\mathrm{E}$, then $\hat{X} \in \mathbf{Mf}_k\mathrm{E}$ is defined by $\hat{X}(R) = X(R)$ for $R \in \mathbf{Mf}_k$. The completion-functor is obviously left-exact.

If $A \in \mathbf{Mf}_k$, we denote by $\mathrm{Spf}_k A$ or Spf the k-formal functor $R \mapsto \mathrm{Mor}_{\mathbf{Mf}_k}(A, R)$; one has obviously $\widehat{\mathrm{Sp}A} = \mathrm{Spf}A$, and for any $F \in \mathbf{Mf}_k\mathrm{E}$ a Yoneda isomorphism

$$\mathrm{Mor}_{\mathbf{Mf}_k\mathrm{E}}(\mathrm{Spf}A, F) \xrightarrow{\sim} F(A), \quad A \in \mathbf{Mf}_k$$

In particular, the functor $A \mapsto \mathrm{Spf}A$ is fully-faithful, or, what amounts to the same, the functor $X \mapsto \hat{X}$, X a finite k-scheme, is fully faithful. We therefore can view the category of finite k-schemes as a full subcategory of either $\mathbf{M}_k\mathrm{E}$ or $\mathbf{Mf}_k\mathrm{E}$ (we shall say: "the completion does not change the finite k-schemes").

Definition 1.6.2 (The first definition)**.** By definition, a k-formal-scheme is a k-formal functor which is the limit of a directed inductive system of finite k-schemes: F is a k-formal-scheme if there exists a directed projective system (A_i) of finite k-rings and functorial (in R) isomorphisms:

$$F(R) \cong \lim \mathrm{Mor}_{\mathbf{Mf}_k}(A_i, R) = \varinjlim \mathrm{Spf}(A_i)(R)$$

For any k-formal functor G, one has a Yoneda isomorphism

$$\mathrm{Mor}_{\mathbf{Mf}_k\mathrm{E}}(\varinjlim \mathrm{Spf}(A_i), G) = \varprojlim G(A_i)$$

Definition 1.6.3 (The second definition)**.** Let A be a profinite k-ring, i.e., a topological k-ring whose topology has a basis of neighborhoods of zero consisting of ideals of finite codimension; one also can say that A is the inverse limit (as a topological ring) of discrete quotients which are finite k-rings. If $R \in \mathbf{Mf}_k\mathrm{E}$, we define $\mathrm{Spf}(A)(R)$ as the set of all continuous homomorphisms of the topological k-ring A to the discrete k-ring R; if (A_i) is the family of discrete finite quotients of A defining its topology, then obviously $\mathrm{Spf}(A)(R) = \varinjlim \mathrm{Spf}(A_i)(R)$, and $\mathrm{Spf}A$ is a k-formal scheme.

Theorem 1.6.4. If $\varphi : A \to B$ is a morphism of profinite k-rings, then $\mathrm{Spf}\varphi : \mathrm{Spf}B \to \mathrm{Spf}A$ is obviously defined, then we have $A \mapsto \mathrm{Spf}A$ is an anti-equivalence of the category $\mathbf{PM}_k$ of profinite k-rings with the category of k-formal-schemes.

Proof. We first prove that Spf is fully faithful: let A and B be two profinite k-rings and (A_i) be the family of all finite discrete quotients of A. We have isomorphisms

$$\mathrm{Mor}_{\mathbf{Mf}_k\mathrm{E}}(\mathrm{Spf}A, \mathrm{Spf}B) \cong \varprojlim(\mathrm{Spf}B)(A_i) \cong \varprojlim \mathrm{Mor}_{\mathbf{PM}_k}(B, A_i) \cong \mathrm{Mor}_{\mathbf{PM}_k}(B, A)$$

We now prove that any k-formal-scheme F is isomorphic to a $\mathrm{Spf}A$. By definition there is a directed projective system (A_i) of $\mathbf{Mf}_k$ such that F is isomorphic to $\varinjlim \mathrm{Spf}A_i$; let A be the topological k-ring $\varprojlim A_i$; we shall prove that A is a profinite k-ring and that $\varinjlim \mathrm{Spf}A_i \cong \mathrm{Spf}A$.

Let us fix an i; the images of the transition maps $f_{ij} : A_j \to A_i$, $j \geq i$, form a directed decreasing set of sub-k-rings in the finite k-ring A_i (then the set of $f_j(A_j)$ only has chains with finite length); it follows that there is a $j(i) \geq i$ such that

$$f_{ij(i)}(A)(A_{j(i)}) = \bigcap_{j \geq i} A_{ij}$$

it implies that, if we replace each A_i by $A'_i = \bigcap_{j \geq i} A_{ij}$, we change neither the topological k-ring A, nor the functor $\varinjlim \mathrm{Spf}A_i$. We can hence suppose that all transition maps $A_j \to A_i$ are surjective. It is now sufficient to prove that the projections $A \to A_i$ are surjective; this would imply both our assertions.

Let now C_i be the k-vector space dual to A_i; the C_i form a directed inductive system with injective transition maps; call $C = \varinjlim C_i$; each canonical map $C_i \to C$ is injective. Let C^* be

the dual space of C. The dual maps $C^* \to A_i$ are surjective and form a projective system; they factorize through A and the projections $A \to A_i$ are a fortiori surjective. In fact, the canonical map $C^* \to A$ is bijective; if $v \in C^*$ maps to 0 on each A_i; then the linear form v over C vanishes on each C_i, hence is zero; conversely, if $a \in A$, then the projection of a on each A_i is a k-linear form on C_i; these linear forms match together, and define a k-linear form on C, which means that a belongs to the image of C^*. ■

Definition 1.6.5 (The third definition)**.** A k-cogebra is a k-vector space C together with a k-linear map $\Delta : C \to C \otimes_k C$. We say that C is a k-coring if Δ is coassociative, cocommutative, and has a counit ϵ; let us make these three notions precise.

(1) Δ is coassociative if $(\Delta \otimes \mathrm{id}_C) \circ \Delta = (\mathrm{id}_C \otimes \Delta) \circ \Delta$, in the following diagram

$$C \longrightarrow C \otimes C \underset{\Delta \otimes \mathrm{id}_C}{\overset{\mathrm{id}_C \otimes \Delta}{\rightrightarrows}} C \otimes C \otimes C$$

(2) Δ is cocommutative if the image of Δ consists of symmetric tensors; equivalently, if $\sigma \circ \Delta = \Delta$ where $\sigma(x \otimes y) = y \otimes x$.

(3) A counit ϵ to Δ is a k-linear form $\epsilon : C \to k$ such that the two maps

$$C \xrightarrow{\Delta} C \otimes C \xrightarrow{\mathrm{id}_C \otimes \epsilon} C \otimes k \xrightarrow{\sim} C$$

$$C \xrightarrow{\Delta} C \otimes C \xrightarrow{\epsilon \otimes \mathrm{id}_C} k \otimes C \xleftarrow{\sim} C$$

are id_C.

If C is a k-cogebra, then the dual k-vector space C^* has an algebra structure defined by $\langle x \cdot y, u \rangle = \langle x \otimes y, \Delta u \rangle$, $x, y \in C^*, u \in C$. If C is a k-coring, then C^* is a ring.

Conversely, if A is a finite k-algebra, the dual space A^* has a natural cogebra structure, which is a coring structure if A is a ring.

The morphisms of k-corings are defined in an obvious way, and the k-corings form a category.

Lemma 1.6.6. Let A and R be two finite k-rings, and A^* the dual k-coring of A. Linear maps $A \to R$ correspond bijectively to elements of the tensor product $A^* \otimes R$; the k-linear maps Δ_{A^*} and ϵ_{A^*} extend to R-linear maps $A^* \otimes R \to (A^* \otimes R) \otimes (A^* \otimes R)$ and $A^* \otimes R \to R$ which also we denote by Δ and ϵ. We then have the k-linear map $A \to R$ associated to $u \in A^* \otimes R$ is a ring homomorphism if and only if $\Delta u - u \otimes u$ and $\epsilon u = 1$.

We therefore have a functorial isomorphism

$$\mathrm{Sp}A(R) = \{u \in A^* \otimes R | \Delta u = u \otimes u, \epsilon u = 1\}$$

Definition 1.6.7. For any k-coring C, we define the k-formal functor $\mathrm{Sp}^* C$ by $\mathrm{Sp}^* C(R) = \{u \in C \otimes R | \Delta u = u \otimes u, \epsilon u = 1\}$. We thus have a covariant functor Sp^* from the category of k-corings to he category of k-formal functors.

Theorem 1.6.8. The functor Sp^* is an equivalence between the category of k-corings and the category of k-formal-schemes.

Proof. As we have already seen Sp$*$ induces an equivalence between the category of finite k-corings and the category of finite k-schemes by the formula.

$$\mathrm{Spf}A = \mathrm{Sp}^* A^*$$

We have already seen that any k-formal-scheme F is an inductive limit of finite schemes $\mathrm{Spf}(A_i)$ with surjective transition maps $A_j \to A_i$; the inductive limit $C = \lim_{\to} Ai*$ is naturally endowed with a k-coring structure, and, for any $R \in \mathbf{Mf}_k$, we have

$$\mathrm{Sp}^* C(R) \cong \lim_{\to} \mathrm{Sp}^* A_i^*(R) \cong \lim_{\to} \mathrm{Spf} A_i(R) = F(R)$$

The only point that remains to be checked is that any k-coring is a union of finite dimensional ones:

Lemma. If C is a k-coring, and E a finite dimensional subvector space of C, there exists a finite-dimensional subvector space F of C with $E \subseteq F$ and $\Delta F \subseteq F \otimes F$.

We need only prove the lemma for $[E : k] = 1$, say $E = kx$. Let a_i be a k-basis of C and write $\Delta x = \sum x_i \otimes a_i$; put $F = \sum kx_i$; one has $x = (1 \otimes \epsilon)\Delta(x) = \sum x_i \epsilon(a_i) \in F$, and

$$\sum \Delta x_i \otimes a_i = (\Delta \otimes 1)\Delta x = (1 \otimes \Delta)\Delta x = \sum x_i \otimes \Delta a_i$$

if $\Delta a_i = \sum b_{ij} \otimes a_j$, this gives $\Delta x_i = \sum x_i \otimes b_{ji} \in F \otimes C$, hence $\Delta F \subseteq F \otimes C$. Since Δ is cocommutative, we have $\Delta F \subseteq C \otimes F$, hence $\Delta F \subseteq F \otimes F$. ■

Remark 1.6.9. *If C is a k-coring, let C^* be the k-dual space of C with the linear topology defined by the subspaces of C which are orthogonal to the finite-dimensional subcorings of C. Then, what we have proved already in the previous gives: the k-ring C^* is profinite and*

$$\mathrm{Sp}^* C = \mathrm{Spf} C^*$$

Conversely, we can recover C as the set of continuous linear forms on C^*: if A is a profinite k-ring, write A', for the set of continuous linear forms on A, then

$$\mathrm{Spf}A = \mathrm{Sp}^* A'$$

Theorem 1.6.10 (The fourth definition)**.** The fourth definition of k-formal scheme is from a purely functorial point of view:

The k-formal functor $\mathbf{Mf}_k \to E$ is a k-formal scheme if and only if it is a left exact functor.

Recall that a left exact functor is one which commutes with finite projective limits (i.e., which commutes with fibre products and with the final objects). Any $\mathrm{Spf}(A)$, $A \in \mathbf{Mf}_k$ is clearly left exact (this is true in any category, and is the very definition of finite projective limits) hence also any inductive limit of $\mathrm{Spf}(A_i)$, $A_i \in \mathbf{Mf}_k$, i.e., any k-formal-scheme, is left exact.

A proof of the converse can be found in [DG70] V, section 2, 3.1. This fourth definition will not be used in the sequal.

1.7 Operations on formal schemes

Proposition 1.7.1. A finite projective limit of k-formal-schemes is a k-formal-scheme.

For instance let $F_1 \to F \leftarrow F_2$ be a diagram of k-formal-schemes corresponding to a diagram $A_1 \leftarrow A \to A_2$ of profinite k-rings; then $F_1 \times_F F_2$ is a k-formal scheme corresponding to the profinite k-ring $A_1 \widehat{\otimes}_A A_2$, where

$$A_1 \widehat{\otimes}_A A_2 = \lim_{\leftarrow} A_1/I_1 \otimes_A A_2/I_2$$

where I_1 (resp. I_2) runs through the open ideals of A_1 (resp. A_2); $A_1 \widehat{\otimes}_A A_2$ can also be defined as the completed ring of the usual tensor product $A_1 \otimes_A A_2$ for the topology given by the $A_1 \otimes I_2 + I_1 \otimes A_2$.

The description from the coring point of view is a bit more difficult. Let $C_1 \xrightarrow{\varphi_1} C \xleftarrow{\varphi_2} C_2$ be the corresponding coring diagram. Then the k-coring D defining the fibre product is the kernel of the map from $C_1 \otimes C_2$ to C which sends $x_1 \otimes x_2$ to $\varphi_1(x_1)\epsilon_2(x_2) - \epsilon_1(x_1)\varphi_2(x_2)$; the canonical maps $D \to C_1$ and $D \to C_2$ are defined by $x_1 \otimes x_2 \mapsto x_1\epsilon_2(x_2)$ and $x_1 \otimes x_2 \mapsto \epsilon_1(x_1)x_2$.

More particularly $F_1 \times F_2$ corresponds to the profinite k-ring $A_1 \hat{\otimes} A_2$ and to the coring $A_1^* \otimes A_2^*$:

$$\mathrm{Spf} A_1 \times \mathrm{Spf} A_2 = \mathrm{Spf}(A_1 \hat{\otimes} A_2)$$

$$\mathrm{Sp}^* C_1 \times \mathrm{Sp}^* C_2 = \mathrm{Sp}^*(C_1) = \mathrm{Sp}^*(C_1 \otimes C_2)$$

(note that the maps $C_1 \otimes C_2 \to C_i$, $i = 1, 2$, are defined by the counits).

Lemma 1.7.2. Let $f = \mathrm{Spf}\Psi = \mathrm{Sp}^*\varphi$ be a morphism of k-formal schemes. Then

$$f \text{ is a monomorphism} \iff \Psi \text{ is surjective} \iff \varphi \text{ is injective}$$

Proof. Clearly,

$$\varphi \text{ is injective} \Rightarrow \Psi \text{ is surjective} \Rightarrow f \text{ is a monomorphism}$$

Conversely, if $f : X \to Y$ is a monomorphism, then (general nonsense) the diagonal morphism $X \to X \times_Y X$ is an isomorphism. If $\varphi : C \to D$ is the corresponding coring morphism, then the following sequence

$$0 \to C \xrightarrow{u} C \otimes C \xrightarrow{v} D$$

is exact, where $u(x) = x \otimes x$, $v(x \otimes y) = \epsilon_C(x)\varphi(y) - \epsilon_C(y)\varphi(x)$. If $\alpha \in \mathrm{Ker}(\varphi)$, then $\epsilon_C(\alpha) = \epsilon_D(\varphi(\alpha)) = 0$; it follows that for any $x \in C$, one has $v(x \otimes \alpha) = 0$; hence $C \otimes (\mathrm{Ker}\varphi) \subseteq u(C)$. This implies $\mathrm{Ker}(\varphi) = 0$, or $[C : k] = 1, \varphi = 0$; in the latter case, one has $\epsilon_C = \varphi \circ \epsilon_D = 0$, and this implies that $C = 0$ (for instance because $\mathrm{id}_C^* = 0$ implies $C^* = 0$). ■

Proposition 1.7.3. The category of k-formal-schemes has infinite direct sums:

$$\coprod \mathrm{Spf} A_i = \mathrm{Spf} \prod A_i$$

$$\coprod \mathrm{Sp}^* C_i = \mathrm{Sp}^* \sum C_i$$

Definition 1.7.4. A formal scheme F is said to be local if it is isomorphic to a $\mathrm{Spf} A$ where A is a local ring; equivalently, $\mathrm{Card}(F(K))$ must be 1 for all fields $K \in \mathbf{Mf}_k$.

Proposition 1.7.5. Any formal scheme is a direct sum of local formal-schemes: if $A = \lim_{\leftarrow} A/I_i$ is a profinite k-ring, let Ω be the set of all open maximal ideals of A; the Artinian k-ring A/I_i is a product of local rings, which are the localized rings $(A/I_i)_{\mathfrak{m}/I_i}$, where $\mathfrak{m}$ runs through the elements of Ω containing I_i; since $(A/I_i)_{\mathfrak{m}} = (A/I_i)_{\mathfrak{m}/I_i}$, if $\mathfrak{m} \supseteq I_i$ and $\{0\}$ otherwise, we have $A/I_i = \prod_{\mathfrak{m}\in\Omega}(A/I_i)_{\mathfrak{m}}$; defining $A_{\mathfrak{m}}$ as the limit of the $(A/I_i)_{\mathfrak{m}}$, we get

$$A = \prod_{\mathfrak{m}\in\Omega} A_{\mathfrak{m}}$$

(each $A_{\mathfrak{m}}$ being local, as a directed projective limit of local rings).

Definition 1.7.6. Let k' be an extension of k; we define the base change functor by the following formulas

$$(\mathrm{Spf}A) \otimes_k k' = \mathrm{Spf}(A \otimes_k k')$$
$$(\mathrm{Sp}^* C) \otimes_k k' = \mathrm{Sp}^*(C \otimes_k k')$$

If k'/k is finite, then this base-change functor is the obvious one, defined by $(F \otimes_k k')(R) = F(R_{[k]})$.

Remark 1.7.7. *If X is a k-scheme, then its completion $\hat{X}$ is a k-formal scheme: more precisely, $\hat{X}$ is the direct sum of the $\mathrm{Spf}\,\hat{\boldsymbol{O}}_{X,x}$ where x runs through the points of x such that $[\kappa(x) : k] < \infty$, and where $\mathrm{Spf}\,\hat{\boldsymbol{O}}_{X,x}$ is the completion of $\hat{\boldsymbol{O}}_{X,x}$ defined by the ideals of finite codimension. If X is a (locally) algebraic k-scheme, then these x are precisely the closed points of X, and $\hat{\boldsymbol{O}}_{x,x}$ is the completion of $\boldsymbol{O}_{X,x}$ for the usual adic topology. For instance, if $X = \mathrm{Sp}A$, where A is a finitely generated k-ring, then $\hat{X} = \coprod \mathrm{Spf}\hat{A}_{\mathfrak{m}}$, where $\mathfrak{m}$ runs through all maximal ideals of A, and $\widehat{A_{\mathfrak{m}}}$ is the completion of the local ring $A_{\mathfrak{m}}$ for the $\mathfrak{m}$-adic topology. The functor $X \mapsto \hat{X}$ is left exact and commutes with base-change.*

1.8 Constant and etale schemes

For the moment, let us drop the assumption that k is a field.

Definition 1.8.1. Given a set E, we define the constant scheme E_k to be the direct sum (in the category of k-schemes)

$$E_k = (\mathrm{Sp}_k k)^{(E)}$$

equivalently, $|E_k|$ is the direct sum $(\mathrm{Spec}k)^{(E)}$.

For any scheme X, we have canonical bijections

$$\mathrm{Mor}_{\mathbf{M}_k\mathrm{E}}(E_k, X) \cong \mathrm{Mor}_{\mathbf{M}_k\mathrm{E}}(\mathrm{Sp}_k k, X)^{(E)} \cong X(k)^{(E)} = \mathrm{Mor}_{\mathbf{Set}}(E, X(k))$$

so that $E \mapsto E_k$ is the right adjoint functor to $X \mapsto X(k)$. This implies that $E \mapsto E_k$ commutes with finite projective limits.

If $k' \in \mathbf{M}_k$, one has a canonical isomorphism

$$E'_k \cong E_k \otimes_k k'$$

Remark 1.8.2. *If X is a scheme, then $\mathrm{Mor}_{\boldsymbol{M}_k\mathrm{E}}(X, E_k)$ can be identified with the set of continuous (i.e., locally constant) maps of $|X|$ to the discrete space E.*

Proposition 1.8.3. If E is finite, then E_k is affine and $\mathcal{O}_k(E_k)$ is the k-ring k^E.

Definition 1.8.4. Let now k be again a field. We define the constant formal-scheme $\hat{E}_k$ as the completion of E_k, or equivalently, as the direct sum $(\mathrm{Spf})^{(E)}$. Then $\hat{E}_k \cong \mathrm{Spf} k^E$, where k^E has the product topology.

A k-scheme (resp. k-formal-scheme) is called constant if it is isomorphic to an E_k (resp. $\hat{E}_k$). The completion functor induces an equivalence between the category of canstant k-schemes and the category of constant k-formal schemes.

We define now an etale k-scheme (resp. an etale k-formal-scheme) to be a direct sum of Sp (resp. Spf) of finite separable extensions of k.

Proposition 1.8.5. Let $\bar{k}$ be an algebraic closure of k, and k_s the subextension consisting of all separable elements of $\bar{k}$. Then for a k-scheme X (resp. a k-formal scheme X), the following conditions are equivalent:

$$X \text{ is etale}, \quad X \otimes_k \bar{k} \text{ is constant}, \quad X \otimes_k k_s \text{ is constant}$$

This proposition is an easy consequence of the following: if A is a k-ring, then A is a finite product of finite separable extensions of k if and only if $A \otimes_k \bar{k}$ is a finite power of $\bar{k}$, or $A \otimes_k k_s$ a finite power of k_s.

Proposition 1.8.6. Let Π be the Galois group of k_s/k; it is a profinite topological group. Let X be an etale k-scheme; then Π operates on the set $X(k_s)$ and the isotropy group of any $x \in X(k_s)$ is open in Π (one calls $X(k_s)$ a Π-set). The fundamental theorem of Galois theory is equivalent to: $X \mapsto X(k_s)$ is an equivalence between the category of etale k-schemes and the category of Π-sets.

Note also that $X \mapsto \hat{X}$ is an equivalence between the categories of etale k-schemes and etale k-formal schemes.

1.9 The Frobenius morphism

Remark 1.9.1. *We suppose now that the characteristic p of the field k is > 0.*

Definition 1.9.2. For any k-ring A, we denote $f_A : A \to A$ the map $x \mapsto x^p$; we denote by $A_{[f]}$ the k-ring deduced from by the scalar restriction $f_k : k \to k$, and $A^{(p)} : A \otimes_{k,f_k} k$ the k-ring obtained by the scalar extension f_k.

Then $f_A : A \to A_{[f]}$ is a k-ring morphism, and defines a k-ring morphism

$$F_A : A^{(p)} \to A, \quad x \otimes \lambda = x^p \lambda$$

If X is a k-functor, we put $X^{(p)} = X \otimes_{k,f} k$, so that

$$X^{(p)}(R) = X(R_{[f]})$$

and we define the Frobenius morphism $F_X : X \to X^{(p)}$ by

$$F_X(R) = X(f_R) : X(R) \to X^{(p)}(R) = X(R_{[f]})$$

For example, if $X = \mathrm{Sp}_k A$, then $X^{(p)} = \mathrm{Sp}_k A^{(p)}$ and $F_X = \mathrm{Sp}_k F_A$. More generally, if X is a k-scheme, $X^{(p)}$ is a k-scheme. If $k = \mathbb{F}_p$, then $X^{(p)} = X$, but $F_X \neq \mathrm{id}_X$ in general. If k' is an extension of k, then $(X \otimes_k k')^{(p)} = X^{(p)} \otimes_k k'$ and $F_{X \otimes_k k'} = F_X \otimes_k k'$ (obviously from the definition).

Analogous definitions can be given for formal-functors and formal-schemes and the completion functor commutes with these constructions.

Proposition 1.9.3. Let X be a k-formal scheme, or a locally algebraic k-scheme; then X is etale if and only if F_X is a monomorphism, or if and only if F_X is an isomorphism.

Proof. Let us give the proof in the case of a locally algebraic k-scheme. We can replace X by $X \otimes_k \bar{k}$, hence suppose that $k = \bar{k}$. If X is constant, then F_X is an isomorphism. Conversely, suppose that F_x is a monomorphism; let $U = \mathrm{Sp}A$ be an algebraic open affine subscheme of X; then F_U is a monomorphism and we have to prove that A is a finite power of k. Let $\mathfrak{m}$ be a maximal ideal of A; write $A/\mathfrak{m}^2 = A/\mathfrak{m} \oplus \mathfrak{m}/\mathfrak{m}^2$ and look at the following maps: the first one is the canonical map $u : A \to A/\mathfrak{m}^2$, the second one is $v : A \to A/\mathfrak{m} \to A/\mathfrak{m} \oplus \mathfrak{m}/\mathfrak{m}^2$. Trivially $u \circ F_A = v \circ F_A$; but by hypothesis F_A is an epimorphism of $\mathbf{M}_k$, and this implies $u = v$, i.e., $\mathfrak{m}/\mathfrak{m}^2 = 0$. For any maximal ideal $\mathfrak{m}$ of A, we therefore have $\mathfrak{m} = \mathfrak{m}^2$, and this in turn implies in a well-known manner that $A \xrightarrow{\sim} k^n$. ■

1.10 Frobenius map and symmetric products

Definition 1.10.1. Suppose again $p \neq 0$. Let V be a k-vector space, $\otimes^p V$ the p-fold tensor product of V, TS^pV the subspace of symmetric tensors and $s : \otimes^p V \to TS^pV$ the symmetrization operator:

$$s(a_1 \otimes \cdots \otimes a_p) = \sum a_{\sigma(1)} \otimes \cdots \otimes a_{\sigma(p)}$$

where σ runs through the symmetric group $\mathfrak{S}_p$. Let $\alpha_V : V^{(p)} \to TS^pV$ be the linear map sending $a \otimes \lambda$ to $\lambda(a \otimes \cdots \otimes a)$.

Lemma 1.10.2. The composite map $V^{(\alpha)} \xrightarrow{\alpha_V} TS^pV \to TS^pV/s(\otimes^p V)$ is bijective.

Definition 1.10.3. Define the canonical map $\lambda_V : TS^pV \to V^{(p)}$ by $\lambda_V \circ s = 0$, $\lambda_V \circ \alpha_V = \mathrm{id}$.

Remark 1.10.4. *If A is a k-ring, then TS^pA is a ring and λ_A a k-ring homomorphism (because $s(\otimes^p A)$ is an ideal in TS^pA by the formula $s(uv) = us(v)$ for u symmetric). If $X = \mathrm{Sp}A$, we denote $\mathrm{Sp}(TS^pA)$ by S^pX (p-fold symmetric power of X). One has then the following commutative diagram:*

$$\begin{array}{ccc} X^p & \xrightarrow{\text{can}} & S^pX \\ \uparrow & & \uparrow{\scriptstyle \mathrm{Sp}\lambda_A} \\ X & \xrightarrow[F_X]{} & X^{(p)} \end{array}$$

which gives another definition for F_X.

Theorem 1.10.5. Let now C be a k-coring, and consider the Frobenius morphism $F : \mathrm{Sp}^*C \to \mathrm{Sp}^*C^{(p)}$ (it is clear that $(\mathrm{Sp}^*C)^{(p)}$, where $C^{(p)} = C \otimes_{k,f} k$). There exists a unique coring map

$V_C : C \to C^{(p)}$ such that $F = \mathrm{Sp}^* V_C$. The pth iterate $\Delta_p : C \to \otimes^p C$ of $\Delta : C \to \otimes^2 C$ (defined inductively by $\Delta_2 = \Delta$, $\Delta_3 = (1 \otimes \Delta) \circ \Delta = (\Delta \otimes 1) \circ \Delta, \cdots$) maps C in $TS^p C$, and we have the theorem $V_C : C \to c^{(p)}$ is the composite map $C \xrightarrow{\Delta_p} TS^p C \xrightarrow{\lambda_C} C^{(p)}$.

Proof. Let A be the (profinite) k-ring C^*; then $A^{(p)} \cong (c^{(p)})^* = (C^*)^{(p)}$. If $a \in A, x \in C$, one has by definition $\langle a \otimes 1, V(x) \rangle = \langle a^p, x \rangle$ where $a \otimes 1 \in (C^*)^{(p)} = C^* \otimes_{k,f} k$ and $V(x) \in C^{(p)}$. By definition of the multiplication of A, one also has $\langle a^p, x \rangle = \langle a \otimes \cdots \otimes a, \Delta_p x \rangle$ in the duality between $\otimes^p A$ and $\otimes^p C$. But $a \otimes \cdots \otimes a$ is symmetric, and $\Delta_p(x) = \alpha_C(y) + s(v)$ for $y = \lambda_C \Delta_p(x)$ and a suitable $v \in \otimes^p C$. Since $\langle a \otimes \cdots \otimes a, s(v) \rangle = 0$, this gives

$$\langle a \otimes 1, V(x) \rangle = \langle a \otimes \cdots \otimes a, \alpha_C(x) \rangle = \langle a \otimes 1, y \rangle$$

and $V(x) = y = \lambda_C \Delta_p(x)$, as claimed above. ■

Corollary 1.10.6. $X = \mathrm{Sp}^* C = \mathrm{Spf} A$ is etale if and only if F_A is surjective (resp. bijective) and if and only if V_C is injective (resp. bijective).

2 Group-schemes and Formal Group-schemes

2.1 Group-functors

Definition 2.1.1. Let k be a ring. A group law on a functor $G \in \mathbf{M}_k$ is a family of group-laws on all the $G(R)$, $R \in \mathbf{M}_k$, such that each functoriality map $G(R) \to G(S)$ is a homomorphism. Equivalently, a group law on G is a morphism

$$\pi : G \times G \to G$$

such that

$$\pi(R) : G(R) \times G(R) \to G(R)$$

is a group law for all R; this condition is equivalent to the axioms:

- (Ass) The two morphisms $\pi \circ (\pi \times \mathrm{id}_G)$ and $\pi \circ (\mathrm{id}_G \times \pi)$ from $G \times G \times G$ to G are equal.
- (Un) There exists an element $1 \in G(k)$ (or equivalently a morphism $eL\mathrm{Sp}k \to G$) such that $\pi \circ (\mathrm{id}_G \times e)$ and $\pi \circ (e \times \mathrm{id}_G)$ are equal to id_G.
- (Inv) There exists a morphism $\sigma : G \to G$ such that the two morphisms $G \xrightarrow{(\mathrm{id}_G, \sigma)} G \times G \xrightarrow{\pi} G$ and $G \xrightarrow{(\sigma, \mathrm{id}_G)} G \times G \xrightarrow{\pi} G$ are equal to id_G.

We are principally interested in commutative group laws, i.e., such that $G(R)$ is commutative for all R, i.e.

- (Com) If $\tau : G \times G \to G \times G$ is the symmetry, then $\tau \circ \pi = \pi$.

A k-group functor is a pair (G, π), where G is a k-functor and π a group-law on G. The k-group functors form a category, a homomorphism $f : G \to H$ being a morphism such that $f(R) : G(R) \to$

$H(R)$ is a group-homomorphism for each R, or equivalently such that $(f \times f) \circ \Delta_G = \Delta_H \circ f$. The category $\mathbf{Gr}_k$ of k-group-functors has projective limits. For instance:

- The final object $e_k = \mathrm{Sp}k$ has a unique group law.

- If $G \to H \leftarrow K$ is a diagram of $\mathbf{Gr}_k$, the fibre product $G \times_H K$ has an obvious group law, for which it is the fibre product in $\mathbf{Gr}_k$.

- In particular, if $f : G \to H$ is a homomorphism, then the kernel $\mathrm{Ker}(f)$ of f is the sub-functor $G \times_H e_k$ of G; equivalently

$$\mathrm{Ker}(f)(R) = \mathrm{Ker}(f(R) : G(R) \to H(R))$$

The homomorphism f is a monomorphism if and only if $\mathrm{Ker}(f) = e_k$.

- The definition of a subgroup functor is clear.

A k-group-scheme or k-group is a k-group functor whose underlying k-functor is a scheme.

The base change functor $\mathbf{Gr}_k \to \mathbf{Gr}_{k'}$, for $k' \in \mathbf{M}_k$ is obviously defined.

2.2 Constant and etale k-groups

Definition 2.2.1. The functor $E \mapsto E_k$ from sets to k-schemes commutes with products and final objects; it follows that E_k has a natural group-law if E is a group. Such a k-group is called a constant k-group.

Proposition 2.2.2. Suppose k is a field and Π the Galois group of k_s/k; the functor $X \mapsto X(k_s)$ from etale k-schemes to Π-sets is an equivalence; it follows then from the definition of a k-groups, and the fact that a product of etale schemes is also etale: The functor $X \mapsto X(k_s)$ is an equivalence between the category of etale k-groups (resp. commutative etale k-groups) and the category of Π-groups (resp. commutative Π-groups = Galois modules over Π).

Moreover, X is an etale k-group if and only if $X \otimes_k k_s$ is a constant k-group.

2.3 Affine k-groups

Definition 2.3.1. Let $G = \mathrm{Sp}_k A$ be an affine k-scheme. The morphism $\pi : G \times G \to G$ are the $\mathrm{Sp}_k \Delta$ where $\Delta : A \to A \otimes_k A$ is a k-ring morphism. Moreover π satisfies Ass, Com, Un if and only if coassocaitive, cocommutative, has a counit. The condition (Inv) is equivalent to (Coinv): there exists $\sigma : A \to A$ such that the composite maps

$$A \xrightarrow{\Delta} A \otimes A \xrightarrow{\mathrm{id}_A \otimes \sigma} A \otimes A \xrightarrow{\text{product}} A$$

$$A \xrightarrow{\Delta} A \otimes A \xrightarrow{\sigma \otimes \mathrm{id}_A} A \otimes A \xrightarrow{\text{product}} A$$

are the composite map $A \xrightarrow{\epsilon} k \to A$. Such a σ is called an involution, or antipodism. If one identifies A with $\mathcal{O}(G)$, $A \otimes A$ with $\mathcal{O}(G \times G)$, then

$$(\Delta f)(x, y) = f(xy), \quad \sigma f(x) = f(x^{-1}), \quad \epsilon f = f(1)$$

for $x, y \in G(R)$, $R \in \mathbf{M}_k$.

We shall be interested in commutative groups. Let us define a k-biring A as a k-module, together with a structure of k-ring and a tructure of k-coring, which are compatible in either of the two equivalent following senses:

- the product $A \otimes A \to A$ is a k-coring morphism.

- the coproduct $A \to A \otimes A$ is a k-ring morphism.

Then, the category of commutative affine k-groups is antiequivalent to the category of k-birings with antipodism by $G \mapsto \mathcal{O}(G)$ and $A \mapsto \mathrm{Sp}A$ (the morphisms of birings are defined in the obvious way).

A very useful remark is the following: let G be an affine k-group and $A = \mathcal{O}(G)$ [then $\mathbf{M}_k(A, R) \cong G(R)$ for any $R \in \mathbf{M}_k$],

(1) in the group $G(A \otimes A) = \mathbf{M}_k(A, A \otimes A)$, Δ_A is the product of the canonical maps $i_1 : a \mapsto 1 \otimes a$ and $i_2 : a \mapsto a \otimes 1$,

(2) in the group $G(A) = \mathbf{M}_k(A, A)$, σ_A is the inverse of id_A,

(3) ϵ_A is the identity of $G(k) = \mathbf{M}_k(A, k)$.

These facts are trivial: for instance (1) says that if H is a group, the map $(x, y) \mapsto xy$ is the product $(x, y) \mapsto x$ and $(x, y) \mapsto y$.

Example 3. The additive group α_k is defined as follows: $\alpha_k(R)$ is the additive group of R; then, by the above remarks:

$$\mathcal{O}(\alpha_k) = k[T]$$

(T is the identity $\alpha_k \to \mathcal{O}_k$), $\Delta T = T \otimes 1 + 1 \otimes T$, $\sigma T = -T$, $\epsilon T = 0$.

Example 4. The multiplicative group μ_k is defined as follows: $\mu_k(R)$ is the multiplicative group of invertible elements of R; hence

$$\mathcal{O}(\mu_k) = k[T, T^{-1}]$$

($T : \mu_k \to \mathcal{O}_k$ is the inclusion), $\Delta T = T \otimes T$, $\sigma T = T^{-1}$, $\epsilon T = 1$.

Example 5. Let $n \geq 1$ be an integer. We define a group homomorphism $\mu_k \xrightarrow{n} \mu_k$ by $x \mapsto x^n$. The kernel of this homomorphism is denoted by ${}_n\mu_k$. Hence

$${}_n\mu_k(R) = \{x \in R,\ x^n = 1\}$$

$$\mathcal{O}({}_n\mu_k) = k[T]/(T^n - 1)$$

with the same formulas as above. Note that if k is a field and n is not 0 in k, ${}_n\mu_k$ is etale (because $T^n - 1$ is a separable polynomial) and ${}_n\mu_k(k_s)$ is the Galois module of nth roots of unity.

Example 6. Let k be a field with characteristic $p \neq 0$. One defines ${}_{p^r}\alpha_k$ as the kernel of the homomorphism $x \mapsto x^{p^r}$ of α_k in itself. Hence

$${}_{p^r}\alpha_k(R) = \{x \in R,\ x^{p^r} = 0\}$$

$$\mathcal{O}({}_{p^r}\alpha_k) = k[T]/T^{p^r}$$

Note that ${}_{p^r}\alpha_k(K) = \{0\}$ for any field K.

Remark 2.3.2. *Remark that* $\alpha_k \otimes_k k' = \alpha_{k'}$, $\mu_k \otimes_k k' = \mu_{k'}, \cdots$

Lemma 2.3.3. The remarks we made about the construction of Δ, ϵ can be generalized in the following way. Let H be any k-group functor, and $G = \mathrm{Sp}_k A$ be an affine k-group. Let $f \in \mathrm{Mor}_{\mathbf{M}_k\mathrm{E}}(G, H) \cong H(A)$; consider the three maps $i_1, i_2, \Delta : A \to A \otimes A$. Then:

The element $f \in H(A)$ is a group homomorphism from G to H if and only if in the group $H(A \otimes A)$, one has $\Delta(f) = i_1(f) i_2(f)$. Because, if $H(A \otimes A)$ is identified with $\mathrm{Mor}_{\mathbf{M}_k\mathrm{E}}(G \times G, H)$, then $\Delta(f), i_1(f)$ and $i_2(f)$ map (x, y) to $f(xy)$, $f(x)$, $f(y)$ respectively.

Example 7.

$$\mathrm{Mor}_{\mathbf{Gr}_k}(G, \alpha_k) = \{x \in A, \Delta x = x \otimes 1 + 1 \otimes x\}$$

$$\mathrm{Mor}_{\mathbf{Gr}_k}(G, {}_{p^r}\alpha_k) = \{x \in A, x^{p^r} = 0, \Delta x = x \otimes 1 + 1 \otimes x\}$$

$$\mathrm{Mor}_{\mathbf{Gr}_k}(G, \mu_k)\{x \in A, \Delta x = x \otimes x, \epsilon x = 1\}$$

Remark 2.3.4. *As for the latter, remark that the lemma gives:* $x \in A = \mathrm{Mor}_{\boldsymbol{M}_k\mathrm{E}}(E, \boldsymbol{O}_k)$ *is a homomorphism from* G *to* μ_k *if and only if* $\Delta x = x \otimes x$, *and* x *is invertible. But this implies* $\epsilon x = 1$ *(because a group homomorphism sends* 1 *to* 1*); conversely, if* $\Delta x = x \otimes x$ *and* $\epsilon x = 1$, *then by (Coinv)* $x\sigma(x) = \epsilon x = 1$

$$\mathrm{Mor}_{\boldsymbol{Gr}_k}(G) = \{x \in A,\ x^n = 1,\ \Delta x = x \otimes x, \epsilon x = 1\}$$

2.4 k-formal-groups, Catier duality

Definition 2.4.1. Suppose now that k is a field. A k-formal group is a k-formal-group-functor whose underlying k-formal-scheme. For k-formal-groups, we can replace tensor products, by completed tensor products: the coproduct maps A to $A\hat{\otimes}A, \cdots$ If G is a k-group, then $\hat{G}$ has a natural structure of a k-formal group. For instance, $G \mapsto \hat{G}$ is an equivalence between constant (resp. etale, resp. finite) k-groups and constant (resp. etale, resp. finite) k-formal groups.

Remark 2.4.2. *It is more interesting to look at formal-groups from the point of view of* k*-corings. Let* $G = \mathrm{Sp}^* C$ *be a* k*-formal-scheme; to give a morphism* $\pi : G \times G \to G$ *is equivalent to give a* k*-coring map* $C \otimes C \to C$, *i.e., an algebra structure on* C *compatible with the coring structure; moreover,* π *is a group law (resp. a commutative group law) if and only if this algebra structure is associative, has a unit element and an antipodism (same axiom as (Coinv)) (resp. and is commutative). In particular, is an equivalence between* k*-birings mith antipodism and commutative* k*-formal-groups. It follows that* $\mathrm{Sp}C \to \mathrm{Sp}^* C$ *is an anti-equivalence between commutative affine* k*-groups and commutative* k*-formal-groups. This can also be explained as follows:*

For any commutative k*-group-functor* G, *we define the Cartier dual of* G *as the commutative* k*-group-functor* $D(G)$ *such that, for* $R \in \boldsymbol{M}_k$,

$$D(G)(R) = \mathrm{Mor}_{\boldsymbol{Gr}_R}(G \otimes_k R, \mu_R)$$

if G *and* H *are two commutative* k*-group-functors, then it is equivalent either to give a homomorphism* $G \to D(H)$, *or a homomorphism* $H \to D(G)$, *or a "bilinear" morphism* $G \times H \to \mu_k$. *In particular, there is a canonical biduality homomorphism*

$$\alpha_G : G \to D(D(G))$$

If $k' \in \boldsymbol{M}_k$, then $D(G \otimes_k k') = D(G) \otimes_k k'$, and $\alpha_{G\otimes_k k'} = \alpha_G \otimes_k k'$.

Theorem 2.4.3. (1) If G is an affine commutative k-group, $\widehat{D(G)}$ is a commutative k-formal group. More precisely, if $G = \mathrm{Sp}A$, where A is a k-biring with antipodism, then $\widehat{D(G)} = \mathrm{Sp}^* A$. The functor $G \mapsto \widehat{D(G)}$ is an anti-equivalence between affine commutative k-groups and commutative k-formal-groups.

(2) If G is a finite commutative k-group, then $D(G)$ also is; α_G is an isomorphism, and $G \mapsto D(G)$ induces a duality in the category of finite commutative groups. Moreover, $\mathrm{rk}(G) = \mathrm{rk}(D(G))$.

Proof. Let $G = \mathrm{Sp}A$, where A is a k-biring with involution. Then, for $R \in \mathbf{Mf}_k$,

$$\widehat{D(G)}(R) = \mathrm{Mor}_{\mathbf{Gr}_R}(G \otimes_k R, \mu_R) = \{x \in A \otimes_k R, \Delta x = x \otimes x, \epsilon x = 1\} = \mathrm{Sp}^* A(R)$$

to prove (1); it remains only to show that the multiplication in A giving the group structure of $D(G)$ is the given one; this verification is straightforward. The proof of (2) is similar. ■

Example 8. (1) $D(\mathbb{Z}/n\mathbb{Z})_k =_n \mu_k$ and conversely.

(2) (char $(k) = p \neq 0$) There is a canonical bilinear morphism

$$f : {}_p\alpha_k \times {}_p\alpha_k \to \mu_k$$

given by $f(x, y) = \exp(xy) = 1 + xy + \cdots + (xy)^{p-1}/(p-1)!$. It defines an isomorphism $D({}_p\alpha_k) \cong_p \alpha_k$.

(3) $D(\mu_k) = \mathbb{Z}_k$, hence $\widehat{D(\mu_k)} = \widehat{\mathbb{Z}_k}$.

2.5 The Frobenius and the Verschiebung morphisms

Remark 2.5.1. *Suppose* char $(k) = p \neq 0$. *The functor $G \mapsto G^{(p)}$ and the morphism $F_G : G \to G^{(p)}$ commutes with products. This implies that, if G is a k-group-functor, then $G^{(p)}$ has a natural structure of a k-group-functor, and F_G is a homomorphism. The same is true for k-formal-group-functors.*

Proposition 2.5.2. We define $G^{(p^n)}$ by $G^{(p^n)} = (G^{(p^{n-1})})^{(p)}$, and $F^n_G : G \to G^{(p^n)}$ by $F^n_G = F^{n-1}_{G^{(p)}} \circ F_G$. Let G be a commutative affine k-group, we have $D(G^{(p)}) = D(G)^{(p)}$. By Cartier duality, there is therefore a unique homomorphism (the Verschiebung morphism)

$$V_G : G^{(p)} \to G$$

such that $\widehat{D(V_G)} = F_{\widehat{D(G)}}$. If $G = \mathrm{Sp}A$, then $\widehat{D(G)} = \mathrm{Sp}^* A$, and we see that $V_G = \mathrm{Sp}V_A$.

In the same way, we define the Verschibung homomorphism for commutative k-formal groups. One defines also $V^n_G : G^{(p^n)} \to G$ in the same way as F^n_G.

Proposition 2.5.3. If $f : G \to H$ is a homomorphism of commutative affine k-groups (or k-formal groups), then the following diagram is clearly commutative:

$$\begin{array}{ccccc} G^{(p)} & \xrightarrow{V_G} & G & \xrightarrow{F_G} & G^{(p)} \\ \downarrow{\scriptstyle f^{(p)}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f^{(p)}} \\ H^{(p)} & \xrightarrow{V_H} & H & \xrightarrow{F_H} & H^{(p)} \end{array}$$

Proposition 2.5.4. If G is an affine commutative k-group (resp. a commutative k-formal group), then

$$V_G \circ F_G = p\mathrm{id}_G, \quad F_G \circ V_G = p\mathrm{id}_{G^{(p)}}$$

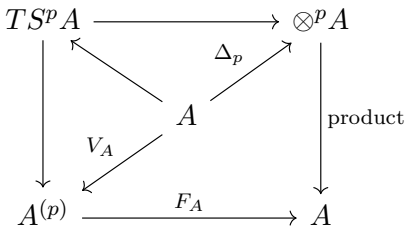
Equivalently, $V_G(F_G(x)) = px$, $F_G(V_G(x)) = px$ (additive notation).

Proof. It is sufficient to prove this for the affine case, because the formal case follows by Cartier duality. Moreover, the first formula (for any G) implies the second one; by the functorial of F and Y, one has a commutative diagram,

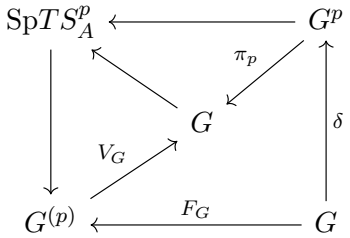
$$\begin{array}{ccc} G & \xleftarrow{V_G} & G^{(p)} \\ {\scriptstyle F_G}\downarrow & & \downarrow{\scriptstyle F_{G^{(p)}}} \\ G^{(p)} & \xleftarrow[V_{G^{(p)}}]{} & G^{(p^2)} \end{array}$$

and $F_G \circ V_G = V_{G^{(p)}} \circ F_{G^{(p)}}$.

To prove $V_G \circ F_G = p\mathrm{id}_G$, one has a commutative diagram (where $A = \mathcal{O}(G)$):



or



with $\delta(g) = (g, \cdots, g)$, and $\pi_p(g_1, \cdots, g_p) = g_1 + \cdots + g_p$. Then $V_G \circ F_G = \pi_p \circ \delta = p\mathrm{id}_G$. ■

Remark 2.5.5. *The above diagram gives a direct definition of V_G.*

Example 9. $V : \mu_k \to \mu_k$ is the identity, $V : \alpha_k \to \alpha_k$ is zero. This follows from the fact that F is an epimorphism for α_k and μ_k and that $p\mathrm{id}_{\mu_k} = F_{\mu_k}$, $p\mathrm{id}_{\alpha_k} = 0$.

2.6 The category of affine k-groups

Definition 2.6.1. Recall that k is supposed to be a field. Let $\mathbf{AC}_k$ be the category of all affine commutative k-groups

Theorem 2.6.2 (Grothendieck)**.** The category $\mathbf{AC}_k$ is Abelian.

(a) $\mathbf{AC}_k$ is an additive category; clear.

(b) Any morphism $f : G \to H$ of $\mathbf{AC}_k$ has a kernel: one has

$$\mathrm{Ker}(f) = G \times_H e, \quad \mathcal{O}(\mathrm{Ker}(f)) = \mathcal{O}(G)/\mathfrak{m}(H)\mathcal{O}(G)$$

($\mathfrak{m}(H) = \mathrm{Ker}\epsilon_H : \mathcal{O}(H) \to k$). Remark that $\mathcal{O}(G) \to \mathcal{O}(\mathrm{Ker}(f))$ is surjective.

(c) Any morphism $f : G \to H$ of $\mathbf{AC}_k$ has a cokernel; One takes $\mathrm{Coker}f$ such that

$$\begin{aligned}\mathcal{O}(\mathrm{Coker}f) = \mathcal{O}(H)^G &= \{f \in \mathcal{O}(H), f(g+h) = f(h),\ \forall g \in G(R), h \in H(R)\} \\ &= \{f \in \mathcal{O}(H), (1 \otimes \mathcal{O}(f))\Delta_H(f) = f \otimes 1\}\end{aligned}$$

Remark that $\mathcal{O}(\mathrm{Coker}f) \to \mathcal{O}(H)$ is injective.

(d) There is only one thing more, and this is the fundamental fact, that any monomorphism is a kernel, and any epimorphism is a cokernel.

More precisely

Theorem 2.6.3. Let $f : G \to H$ be a morphism of $\mathbf{AC}_k$.

(1) The following conditions are equivalent:

- f is a monomorphism,
- $\mathcal{O}(f)$ is surjective (i.e., G is a closed subgroup of H),
- f is a kernel.

(2) The following conditions are equivalent:

- f is an epimorphism,
- $\mathcal{O}(f)$ is injective,
- $\mathcal{O}(f) : \mathcal{O}(H) \to \mathcal{O}(G)$ makes a faithfully flat $\mathcal{O}(H)$-module,
- $\mathcal{O}(f)$ is a cokernel.

For a proof see [DG70] III, 3.7.4. The main point is (f mono)⇒(f kernel) or equivalently (f mono)⇒($f = \mathrm{Ker}(\mathrm{Coker}f)$).

Corollary 2.6.4. If k' is an extension of k, then $G \mapsto G \otimes_k k'$ is an exact functor.

Corollary 2.6.5. Let $0 \to K \to G \to H \to 0$ be an exact sequence, then the $\mathcal{O}(G)$-algebra $\mathcal{O}(G) \otimes_{\mathcal{O}(H)} \mathcal{O}(G)$ is isomorphic to $\mathcal{O}(G) \otimes \mathcal{O}(K)$.

Clear, the morphism $(g, k) \mapsto (g, gk)$ of $G \times K \to G \times_H G$ is an isomorphism.

Corollary 2.6.6. If $0 \to K \to G \to H \to 0$ is an exact sequence with K algebraic (resp. finite of rank r); then $\mathcal{O}(G)$ is a finitely presented $\mathcal{O}(H)$-ring (resp. a finitely generated projective $\mathcal{O}(H)$-module of rank r).

As $\mathcal{O}(G) \to \mathcal{O}(H)$ is faithfully flat, this also follows from that $\mathcal{O}(G) \otimes_{\mathcal{O}(H)} \mathcal{O}(G) \cong \mathcal{O}(G) \otimes \mathcal{O}(K)$ as $\mathcal{O}(G)$-algebras.

Corollary 2.6.7. If $0 \to K \to G \to H \to 0$ is an exact sequence, then G is algebraic (resp. finite) if and only if H and K are. In the finite case, one has $\mathrm{rk}(G) = \mathrm{rk}(K)\mathrm{rk}(H)$.

If $\mathcal{O}(G)$ is finitely generated or finite, so is the subalgebra $\mathcal{O}(H)$ and the quotient $\mathcal{O}(K)$. The converse and the last assertion follow from the above corollary.

Corollary 2.6.8. If $f : G \to H$ is an epimorphism (resp. and if $\mathrm{Ker} f$ is algebraic, resp. finite) and if $R \in \mathbf{M}_k$, and $h \in H(R)$, there exists an R-ring S faithfully flat (resp. and finitely presented, resp. finite and projective) and a $g \in G(S)$ such that $f(g) = h_S$.

Corollary 2.6.9. If $f : G \to H$ is an epimorphism with $\mathrm{Ker} f$ algebraic, if $L \in \mathbf{M}_k$ is a field, and $h \in H(L)$, there exists a finite extension L' of L and a $g \in G(L')$ with $f(g) = h_{L'}$.

Remark 2.6.10. *If f is an epimorphism (without any hypothesis on $\mathrm{Ker}(f)$), then $f(L)$ is surjective for any algebraically closed field L.*

Remark 2.6.11. *By Cartier duality the category of commutative k-formal groups also is Abelian, and $\mathrm{Spf}(\varphi)$ is a monomorphism (resp. an epimorphism) if and only if φ is surjective (resp. injective).*

Theorem 2.6.12. (a) The Abelian category $\mathbf{AC}_k$ satisfies the axiom: it has directed projective limits, and a directed projective limit of epimorphisms is an epimorphism.

(b) The Artinian objects of $\mathbf{AC}_k$ are the algebraic groups. Any object of $\mathbf{AC}_k$ is the directed projective limit of its algebraic quotients.

Proof. (a) is clear from 2.6.3: One has $\lim_{\leftarrow} \mathrm{Sp}\varphi_i = \mathrm{Sp} \lim_{\rightarrow} \varphi_i$ and a directed inductive limit of injective maps is injective.

For (b), see [DG70] II, 2.3.7. ■

By Cartier duality, the dual statements hold for the category of commutative k-formal-groups.

Remark 2.6.13. *From now on we shall mainly speak about commutative groups. We say group instead of commutative group unless otherwise states. From now on also, k is a field, p denotes the characteristic of k, and $\Pi = \mathrm{Gal}(k_s/k)$. Our main interest will be the case $p \neq 0$. As we shall see, the case $p = 0$ is rather trivial.*

2.7 Etale and constant formal-groups

Remark 2.7.1. *We already defined and studied etale affine (resp. formal) groups. They are equivalent to finite (resp. all) Galois modules by*

$$E \mapsto (E \otimes_k k_s)(k_s) = \bigcup_{K/k \text{ sep finite}} E(K)$$

If $p \neq 0$, then G is etale iff $\mathrm{Ker} F_G = e$, and this implies that F is an isomorphism. It follows that subgroups, quotients and extensions (direct limits in the formal case) of etale groups also are etale. The same statement is true if $p = 0$.

Recall, that the formal-group $G = \mathrm{Spf}A$ is local (We shall also say connected) if A is local or equivalently if $G(K) = \{0\}$ for any field K. A morphism from a connected group to an etale group is zero.

Proposition 2.7.2. Let G be a formal-group.

(a) There is an exact sequence (unique up to isomorphism)

$$0 \to G^0 \to G \to \pi_0(G) \to 0$$

where G^0 is connected, and $\pi_0(G)$ etale. If $R \in \mathbf{Mf}_k$ and $\mathfrak{n}$ is the nilradical of R then $G^0(R) = \mathrm{Ker}(G(R) \to G(R/\mathfrak{n}))$. If $p \neq 0$, then G^0 is the limit of the $\mathrm{Ker}(F_G^n : G \to G^{p^n})$, $n \geq 0$. If $k \to k'$ is an extension then $(G \otimes_k k')^0 = G^0 \otimes_k k'$, $\pi_0(G \otimes_k k') = \pi_0(G) \otimes_k k'$.

(b) If k is perfect, there is a unique isomorphism $G \cong G^0 \times \pi_0(G)$.

Proof. Write $G = \mathrm{Spf}A = \coprod \mathrm{Spf}A_{\mathfrak{m}}$. Let A^0 be the local factor $A_{\mathfrak{m}_0}$ corresponding to the ideal $\mathfrak{m}_0 = \mathrm{Ker}(\epsilon : A \to k)$. Call $G^0 = \mathrm{Spf}A^0$; by construction, $G^0(R) = \mathrm{Ker}(G(R) \to G(R/\mathfrak{n}))$ for $R \in \mathbf{M}_k$; it follows that G^0 is a subgroup of G. If $k \to k'$ is an extension, then $A^0 \otimes_k k'$ is local, because the residue field of A^0 is k; it follows that $(G \otimes_k k')^0 = G^0 \otimes_k k'$. Suppose $p \neq 0$, then $\mathrm{Ker}F_G^n = \mathrm{Spf}A/\mathfrak{m}_0^{p^n}$, where $\mathfrak{m}_0^{p^n}$ is the closed ideal of A generated by the x^{p^n}, $x \in \mathfrak{m}_0$; hence $\bigcup_n \mathrm{Ker}F_G^n = \mathrm{Spf}(\lim_{\leftarrow} A/\mathfrak{m}_0^{p^n}) = \mathrm{Spf}A_0 = G^0$. To prove (a), it only remains to show that G/G^0 is etale.

Remark first that G is etale if and only if $G^0 = e$: replacing k by $\bar{k}$ to be algebraically closed; if $G^0 = e$ then $A^0 = k$; but then all the $A_{\mathfrak{m}}$ are isomorphic (by translation); hence $A \cong k^E$ and G is etale. To prove G/G^0 is etale is therefore equivalent to prove $(G/G^0)^0 = e$; if H is the inverse image of $(G/G^0)^0$ in G, then H is an extension of two connected groups; this implies that H is connected (for any field K in $\mathbf{Mf}_k$ then $0 \to G^0(K) \to H(K) \to (G/G^0)(K)$ is an exact sequence, hence $H(K) = \{0\}$) hence $H \subseteq G^0$, i.e., $H = G^0$ and $(G/G^0)^0 = e$.

Suppose now k is perfect. Let $k_{\mathfrak{m}}$ be the residue field of $A_{\mathfrak{m}}$, and $B = \prod k_{\mathfrak{m}}$. Then $\mathrm{Spf}B$ is etale and is a subgroup of G (because B is quotient biring of A); put $G^e = \mathrm{Spf}B$. Then $(G \otimes_k \bar{k})^e = G^e \otimes_k \bar{k}$ as is readily checked, and G is the product of G^0 and G^e, because this becomes true by going to $\bar{k}$. ■

Definition 2.7.3. An affine group G is said to be infinitesimal if it is finite and local, equivalently, if G is algebraic and $G(\bar{k}) = e$. By the preceding proposition, we see that a finite group is an extension of an etale group by an infinitesimal group and this extension splits if k is perfect.

Definition 2.7.4. A (not-necessarily commutative) connected formal group $G = \mathrm{Spf}A$ is said to be of finite type if A is Noetherian; the dimension of G is by definition the Krull dimension of A.

Let $\mathfrak{m}$ be the maximal ideal of A; it is well-known that A is Noetherian if and only if $[\mathfrak{m}/\mathfrak{m}^2 : k] < \infty$, and that $\dim G \leq [\mathfrak{m}/\mathfrak{m}^2 : k]$.

Lemma 2.7.5. A connected formal group G is of finite type if and only if $\mathrm{Ker}F_G$ is finite. If G is of finite type, then $\mathrm{Ker}(F_G^n)$ is finite for all n.

Proof. If $\mathrm{Ker}F_G$ is finite, then $[A/\mathfrak{m}^{(p)}] \leq \infty$, hence $[\mathfrak{m}/\mathfrak{m}^2 : k] < \infty$. Conversely, if $\mathfrak{m}/\mathfrak{m}^2$ is generated by the classes of $x_1, \cdots, x_n$, then A is a quotient of $k[[x_1, \cdots, x_n]]$, and $A/\mathfrak{m}^{(p^n)}$ is a quotient of the finite k-ring $A[[x_1, \cdots, x_n]]/(x_1, \cdots, x_n)^{(p^n)}$. ■

Remark 2.7.6. *It follows that if $p \neq 0$ a connected formal group of finite type is an inductive limit of finite type ($G = \lim_{\to} \mathrm{Ker}F_G^n$).*

Proposition 2.7.7. If G is an algebraic group-scheme, then the "connected completion" $\hat{G}^0$ is of finite type:

$$\hat{G}^0 = \mathrm{Spf}\hat{\mathcal{O}}_{G,e}[= \lim_{\to} \mathrm{Ker}F_G^0 \text{ if } p \neq 0]$$

2.8 Multiplicative affine groups

Lemma 2.8.1. Let G be a k-group-functor. Then the following conditions are equivalent:

(i) G is the Cartier dual of a constant group.

(ii) G is an affine k-group and the k-ring $\mathcal{O}(G)$ is generated by the characters of G (i.e., homomorphisms from G to μ_k).

Such a group is called diagonalizable.

Proof. If $G = D(\Gamma_k)$, then $D(R) = \mathrm{Mor}_{\mathbf{Gr}_R}(\Gamma_R, \mu_R) = \mathrm{Hom}(\Gamma, R^*) = \mathrm{Mor}_{\mathbf{M}_k}(k[\Gamma], R)$, hence $G = \mathrm{Sp}k[\Gamma]$, where $k[\Gamma]$ is the algebra of the group Γ (note that $\Delta\gamma = \gamma \otimes \gamma$, $\epsilon\gamma = 1$, $\sigma\gamma = \gamma^{-1}$, $\gamma \in \Gamma$), and each $\gamma \in \Gamma \subseteq k[\Gamma]$ is a character of G.

Conversely, if G is affine and $\mathcal{O}(G)$ generated by characters, let Γ be the group of all characters of G; then the canonical map $k[\Gamma] \to \mathcal{O}(G)$ is surjective. But it is always injective (Dedekind's lemma on linear independence of characters), hence $k[\Gamma] \cong \mathcal{O}(G)$. ■

Theorem 2.8.2. Let G be a k-group. Then the following conditions are equivalent:

(i) $G \otimes_k k_s$ is diagonalizable.

(ii) $G \otimes_k K$ is diagonalizable for a field $K \in \mathbf{M}_k$.

(iii) G is the Cartier dual of an etale k-group.

(iv) $\widehat{D(G)}$ is an etale k-formal group.

(v) $\mathrm{Mor}_{\mathbf{Gr}_k}(G, \alpha_k) = 0$.

(vi) (If $p \neq 0$), $V_G : G^{(p)} \to G$ is an epimorphism.

(vii) (If $p \neq 0$), $V_G : G^{(p)} \to G$ is an isomorphism.

Such a group is called multiplicative.

(vi) and (vii) are the dual version for that G is etale iff F_G is injective iff F_G is an isomorphism.

Proof. The implications (i) $\Longleftrightarrow$ (iv) $\Longleftrightarrow$ (vii) $\Longleftrightarrow$ (vi) are clear.

Proof of (v) $\Longleftrightarrow$ (iv). We know that $\mathbf{Gr}_k(G, \alpha_k)$ is the set of primitive elements of $\mathcal{O}(G)$; let $A = \mathcal{O}(G)$ and let A' be the ring of $\hat{D}(G)$ (i.e. the topological dual of the coring A). By duality,

a primitive element of A corresponds to an algebra morphism

$$A' \to k[t]/t^2$$

compatible with the augmentations of A' and $k[t]/t^2$. All primitive elements are zero if and only if A'^0 has no quotients isomorphic to $k[t]/t^2$, which means that $A'^0 = k$, i.e. $\hat{D}(G)^0 = e$, i.e. $\hat{D}(G)$ is etale.

End of the proof. If k' is an extension of k, then condition (v) for G is equivalent to condition (v) for $G \otimes k'$. This implies the equivalence of all conditions except (iii). It is clear that (iii)⇒(i) (definition); conversely, if $\hat{D}(G)$ is etale, then let E be the etale k-group such that $\hat{E} = \hat{D}(G)$; we claim that $D(E) \cong G$. This is easy if $k = k_s$, because E is constant; the general case is proved by going to k_s (see [DG70] IV, 1.3.2). ■

Remark 2.8.3. *The multiplicative groups correspond by duality to etale formal groups; they form a thick subcategory (= stable by subgroups, quotients, extensions) stable for* $\lim_{\leftarrow}$*, of* $\boldsymbol{AC}_k$*, called* $\boldsymbol{ACm}_k$*, and anti-equivalent to the category of Galois-modules: to* $G \in \boldsymbol{ACm}_k$ *corresponds the Galois-module* $X(G) = \hat{D}(G \otimes_k k_s)(k_s) = \mathrm{Mor}_{\boldsymbol{Gr}_{k_s}}(G \otimes_k k_s, \mu_{k_s})$.

Remark 2.8.4. *If* E *is an etale* k*-group, then* $D(E)$ *is multiplicative and* $\hat{D}(D(E)) = \hat{E}$*; in fact, one already has* $D(D(E)) = E$ *([DG70], loc. cit.). It implies that the antiequivalence between multiplicative groups and etale groups can also be given (without speaking about formal-groups at all) by* $E \mapsto D(E)$, $G \mapsto D(G)$.

2.9 Unipotent affine groups. Decomposition of affine groups

Theorem 2.9.1. Let G be an affine k-group. The following conditions are equivalent:

(i) $\widehat{D(G)}$ is a connected formal group.

(ii) Any multiplicative subgroup of G is zero.

(iii) For any subgroup H of G, $H \neq 0$, we have $\mathrm{Mor}_{\mathbf{Gr}_k}(H, \alpha_k) \neq 0$.

(iv) Any algebraic quotient of G is an extension of subgroups of α_k.

(v) (If $p \neq 0$), $\bigcap \mathrm{Im} V_G^n = e$.

Such a group is called unipotent.

The last condition is the dual version for that $G = \lim_{\to} \mathrm{Ker} F_G^n$ if G is connected and of finite type.

Proof. The equivalence of (i) and (ii) is clear (the formal group H is connected, iff $\pi_0(H) = e$, i.e., iff it has no etale quotients). The equivalence of (ii) and (iii) follows from the theorem in the above subsection. The equivalence of (iii) and (iv) is clear because algebraic groups are Artinian. Suppose $p \neq 0$. If G satisfies (iv), then for any algebraic quotient H of G, one has $V_H^n = 0$ for large n (recall that $V_{\alpha_k} = 0$). It follows that $\bigcap \mathrm{Im} V_G^n$ has no algebraic quotients, hence is e. Conversely, if (v) is true for G, G cannot contain a non-zero multiplicative subgroup H, for $V_H^n : H^{(p^n)} \to H$ is an epimorphism for all n. ■

Remark 2.9.2. *The unipotent groups correspond by duality to connected formal groups. They form a thick subcategory, stable for* $\lim_{\leftarrow}$*, of* $\boldsymbol{ACu}_k$*, called* $\boldsymbol{ACu}_k$*.*

Theorem 2.9.3. By duality, the local-etale exact sequence gives that an affine group is in a unique way of a unipotent group by a multiplicative group. This extension splits if k is perfect.

Remark 2.9.4. *In particular, if* k *is perfect, any finite group is uniquely the product of four subgroups which are respectively etale multiplicative, etale unipotent, infinitesimal multiplicative and infinitesimal unipotent. Therefore the category* $\boldsymbol{F}_k$ *of finite (commutative)* k*-groups splits as a product of four subcategories, called* $\boldsymbol{Fem}_k$*,* $\boldsymbol{Feu}_k$*,* $\boldsymbol{Fim}_k$*,* $\boldsymbol{Fiu}_k$*. The categories* $\boldsymbol{Feu}_k$ *and* $\boldsymbol{Fim}_k$ *are dual to each other, the categories* $\boldsymbol{Fem}_k$ *and* $\boldsymbol{Fim}_k$ *are autodual.*

Proposition 2.9.5. (1) Let $p = 0$. Then $\mathbf{F}_k = \mathbf{Fem}_k$: any finite (commutative) k-group is etale and multiplicative.

(2) Let $p \neq 0$ and k be algebraically closed. Any (commutative) finite k-group is an extension of copies of ${}_p\alpha_k$, ${}_p\mu_k$ and $(\mathbb{Z}/r\mathbb{Z})_k$, r prime.

Proof. (1) By duality, it suffices to prove that any finite unipotent group is 0. Such a group is a product of an etale unipotent group and an infinitesimal unipotent group; by the first theorem, these two groups are extensions respectively of etale subgroups of α_k and infinitesimal subgroups of α_k. Any etale subgroup of α_k must be 0, because $\alpha_k(\bar{k}) = \bar{k}$ has no finite subgroups; an infinitesimal subgroup of α_k is of the form $\mathrm{Sp}k[T]/T^n$ where n must be such that $\Delta T^n \subseteq (T^n)\otimes k[T] + k[T]\otimes(T^n)$, this means $(T+T')^n = \alpha T^n + \beta T'^n$ and implies $n = 1$.

(2) Let $G \in \mathbf{F}_k$. If G is etale, then $G = \Gamma_k$, where Γ is a finite group; but Γ is an extension of groups $\mathbb{Z}/r\mathbb{Z}$, r prime, and G is an extension of $(\mathbb{Z}/r\mathbb{Z})_k$. If G is infinitesimal and multiplicative, then $G = D(\Gamma_k)$, where Γ_k is finite and $\mathbf{Gr}(\Gamma, \bar{k}^*) = 0$; this implies Γ is p-torsion, and G is an extension of copies of $D((\mathbb{Z}/p\mathbb{Z})_k) = {}_p\mu_k$. If G is infinitesimal and unipotent, then G is an extension of infinitesimal subgroups of α_k. These are the ${}_{p^r}\alpha_k$, because $(T+T')^n = \alpha T^n + \beta T'^n$ implies $n = p^r$; but ${}_{p^r}\alpha_k$ is a p-fold extension of ${}_p\alpha_k$ (remark that ${}_{p^r}\alpha_k/{}_p\alpha_k = {}_{p^{r-1}}\alpha_k$). ■

Corollary 2.9.6. If m is a prime, and G a finite (commutative) k-group, then $m^\alpha \mathrm{id}_G = 0$ for large α if and only if $\mathrm{rk}(G)$ is a power of m.

It follows from the multiplicativity of the rank, the fact that $\mathrm{rk}(G \otimes_k \bar{k}) = \mathrm{rk}(G)$ and the obvious formulas:

$$\mathrm{rk}((\mathbb{Z}/r\mathbb{Z})_k) = r,\ \mathrm{rk}({}_p\alpha_k) = \mathrm{rk}({}_p\mu_k) = p$$

In particular, if $p^\alpha \mathrm{id}_G = 0$, then $\mathrm{rk}(G) = p^{\mathrm{length}(G\otimes_k \bar{k})}$, where $\mathrm{length}(G)$ is the length of a Jordan-Holder series of G.

2.10 Smooth formal-groups

Definition 2.10.1. A (not-necessarily commutative) connected formal group $G = \mathrm{Spf}A$ is said to be smooth if A is a power-series algebra $k[[x_1, \cdots, x_n]]$. In that case, the coproduct $\Delta : A \to A\hat{\otimes}A$ is given by a set of formal power series:

$$\Phi(X, Y) = (\Phi_i(x_1, \cdots, x_n, y_1, \cdots, y_n)), \quad i = 1, 2, \cdots, n$$

Δ is given by a set of homomorphisms

$$\Delta(R) : (\mathrm{Spf}A\hat{\otimes}A)(R) \to \mathrm{Spf}A$$

which are precisely

$$\Delta(R) : \mathrm{Hom}^{\mathrm{cts}}_{k-\mathrm{alg}}(k[x_1, \cdots, x_n, y_1, \cdots, y_n], R) \to \mathrm{Hom}^{\mathrm{cts}}_{k-\mathrm{alg}}(k[x_1, \cdots, x_n], R)$$

Since any $f \in \mathrm{Hom}^{\mathrm{cts}}_{k-\mathrm{alg}}(k[x_1, \cdots, x_n], R)$ only depends on the values of $x_1, \cdots, x_n$, and $f(x_i)$ takes values in $\mathrm{Ker}(\epsilon)$, where $\epsilon : R \to k$ the structure homomorphism, then $\mathrm{Hom}^{\mathrm{cts}}_{k-\mathrm{alg}}(k[x_1, \cdots, x_n], R) \cong (\mathrm{Ker}(\epsilon))^n$. Thus, $\Delta(R)$ induces a morphism

$$\Phi : (\mathrm{Ker}\epsilon)^{2n} \to (\mathrm{Ker}\epsilon)^n$$

$$(X, Y) \mapsto (\Phi_i(x_1, \cdots, x_n, y_1, \cdots, y_n))$$

between k-algebras.

and the axioms (Ass) and (Un) give

- (Ass) $\Phi(X, \Phi(Y, Z)) = \Phi(\Phi(x, Y), Z)$.
- (Un) $\Phi(0, Y) = \Phi(X, 0) = 0$.

It is easily proved, using the implicit function theorem, that the existence of an antipodism is a consequence of (Ass) and (Un). The axiom (Com) can be written.

- (Com) $\Phi(X, Y) = \Phi(Y, X)$.

Such a set $\{\Phi_i\}$ is a formal-group-law in the sense of Dieudonne.

Theorem 2.10.2. Let $G = \mathrm{Spf}A$ be a (not-necessarily commutative) connected formal group if finite type.

(1) If $p = 0$, then G is smooth.

(2) If $p \neq 0$, the following conditions are equivalent:

  (a) G is smooth,

  (b) $A \otimes_k k^{p^{-1}}$ is reduced.

  (c) $F_G : G \to G^{(p)}$ is an epimorphism.

Proof. Remark first that in (2) we have (a)⇒(b); moreover (c) is equivalent to $F_A : A^{(p)} \to A$ being injective, or to $A^{(p)} \cong A \otimes_k k^{p^{-1}}$ being reduced. We then have to prove that if, either $p = 0$, or $p \neq 0$ and $A \otimes_k k^{p^{-1}}$ is reduced, then $A \cong k[[x_1, \cdots, x_n]]$.

Let first $\mathfrak{m}$ be $\mathrm{Ker}(\epsilon : A \to k)$ and $\delta : \mathfrak{m}/\mathfrak{m}^2 \to k$ be a linear form. We claim that there exists a continuous k-derivation D of A such that for $a \in \mathfrak{m}$, one has $\epsilon D(a) = \delta(a \bmod \mathfrak{m}^2)$. Define first $\bar{\delta}(a) = \delta((a - \epsilon a) \bmod \mathfrak{m}^2)$; then $\bar{\delta}(ab) = \epsilon(a)\bar{\delta}(b) + \epsilon(b)\bar{\delta}(a)$; put $D = (1 \otimes \bar{\delta}) \circ \Delta$: if $\Delta a = \sum a_i \otimes b_i$,

then $Da = \sum a_i \bar{\delta} b_i$. One has $\epsilon Da = \sum \epsilon(a_i)\bar{\delta}(b_i) = \bar{\delta}(\sum \epsilon(a_i)b_i) = \bar{\delta}a$; it remains to dhow that D is derivation:

$$D(ab) = (1 \otimes \delta)\Delta(ab) = (1 \otimes \bar{\delta})(\Delta a \Delta b) = (1 \otimes \epsilon)\Delta a (1 \otimes \bar{\delta})\Delta b + (1 \otimes \epsilon)\Delta b (1 \otimes \bar{\delta})\Delta a = aDb + bDa$$

Let now ζ_i be elements of $\mathfrak{m}$ such that their classes modulo $\mathfrak{m}^2$ form a basis of $\mathfrak{m}/\mathfrak{m}^2$. The canonical map

$$f : k[[x_1, \cdots, x_n]] \to A, \quad f(x_i) = \zeta_i$$

is surjective. Suppose it is not injective. Let $\Phi \in \mathrm{Ker}(f)$, $\Phi \neq 0$, with minimal valuation; certainly $v(\Phi) > 0$ (because $\Phi(0) = \epsilon f(\Phi) = 0$). By the above remark, there exists continuous derivations D_i of A with $D_i(\zeta_j) \equiv \delta_{ij} (\mathrm{mod}\ \mathfrak{m})$. Clearly $0 = D_i f(\Phi) = \sum f\left(\dfrac{\partial \Phi}{\partial x_j}\right) D_i(\zeta_j)$. But the matrix $(D_i(\zeta_j))$ is congruent mod $\mathfrak{m}$ to the identity matrix, hence is invertible. It follows that $\dfrac{\partial \Phi}{\partial x_j} = 0$.

If $p = 0$, then Φ must be 0, and f is injective. If $p \neq 0$, then there exists $\Psi \in k^{1/p}[[x_1, \cdots, x_n]]$ with $\Phi = \Psi^p$; extend f to $f' : k^{1/p}[[x_1, \cdots, x_n]] \to A \otimes_k k^{1/p}$; then $f'(\Psi)^p = f(\Phi) = 0$. Because $A \otimes_k k^{1/p}$ is reduced, this implies that $f'(\Psi) = 0$. But Φ was supposed of minimal valuation, hence $\Psi = 0$ (if not, decompose Ψ as a sum $\sum \lambda_i \psi_i$, $\lambda_i \in k^{1/p}$, $\psi_i \in \mathrm{Ker}(f)$, $\psi_i \neq 0$, and note that $v(\Psi) \geq \inf v(\psi_i)$) and $\Phi = 0$. ■

Remark 2.10.3. *The preceding theorem can be strengthened:*

(1) (Cartier). If $p = 0$ and $G = \mathrm{Sp}^* C$ is a connected (not necessarily commutative) formal-group, then C is the universal enveloping algebra of the Lie algebra $\mathfrak{g}$ of G. This implies that the category of all connected formal-groups is equivalent to the category of all Lie algebras over k. By the Poincare-Birkhoff-Witt theorem, this also implies that, if $\mathfrak{g}$ is finite dimensional, then G is smooth. Moreover, if G is commutative, then $\mathfrak{g}$ is abelian, hence $G \cong (\mathfrak{g}^0)^{(I)}$; by duality, any unipotent (commutative) k-group is a power of the additive group.

(2) (Dieudonne-Cartier-Gabriel). If $p \neq 0$, k is perfect, G is any (not-necessarily commutative) connected formal group of finite type, H a subgroup, and $G/H = \mathrm{Spf} A$, then is of the form $k[[x_1, \cdots, x_n]][y_1, \cdots, y_d]/(y_1^{p^{r_1}}, \cdots, y_d^{p^{r_d}})$. This implies for instance to $A = \hat{\boldsymbol{O}}_{G,e}$, G an algebraic k-group.

Corollary 2.10.4. Suppose $p \neq 0$, and let G be a connected formal group of finite type.

(1) If k is perfect, there exists a unique exact sequence of connected groups

$$0 \to G_{\mathrm{red}} \to G \to G/G_{\mathrm{red}} \to 0$$

with G_{red} smooth, and G/G_{red} infinitesimal (= finite).

(2) For large r, the group $G/\mathrm{Ker}(F_G^r) = \mathrm{Im}(G \to G^{(p^r)})$ is smooth.

Proof. (1) The uniqueness is clear, because any homomorphism from a smooth group to an infinitesimal group is 0 (look at the algebras). Let $G = \mathrm{Spf} A$, and $G_{\mathrm{red}} = \mathrm{Spf} A_{\mathrm{red}}$, where A_{red} is the quotient of A by its nilideal.

Because $A_{\mathrm{red}} \hat{\otimes}_k A_{\mathrm{red}}$ is reduced (see the Appendix)

$$\Delta n \subseteq A \hat{\otimes} n + n \hat{\otimes} A$$

and G_{red} is a subgroup of G, smooth by the theorem. Moreover $G/G_{\mathrm{red}} = \mathrm{Spf}B$, where

$$B = \{x \in A, \Delta x - x \otimes 1 \in A \otimes n\}$$

If $x \in B$, $\epsilon(x) = 0$, then $x = \epsilon \otimes 1(\Delta x - x \otimes 1) \in n$. It implies $B \subseteq k + n$, and B is Artinian, hence finite.

(2) It is clear that $H = G/F_G^n$ is smooth if and only if $H \otimes_k \bar{k}$ is. Replacing k by $\bar{k}$, we can suppose k perfect and apply (1). There exists an i with $F^i(G/G_{\mathrm{red}}) = 0$; but $F^i(G_{\mathrm{red}}) = G_{\mathrm{red}}^{(p^i)}$ because G_{red} is smooth. Hence $F^iG = F^i(G_{\mathrm{red}}) = G_{\mathrm{red}}^{(p^i)}$ and F^iG is smooth. ■

Corollary 2.10.5. Let G be a connected formal group of finite type, and $n = \dim G$. Then $\mathrm{rk}(\mathrm{Coker}F_G^i)$ is bounded and

$$\mathrm{rk}(\mathrm{Ker}(F_G^i)) = p^{ni}\mathrm{rk}(\mathrm{Coker}F_G^i)$$

Proof. If G is smooth, then F_G is an epimorphism, and $\mathrm{Ker}F_G^i \cong \mathrm{Spf}k[[x_1, \cdots, x_n]]/(x_1, \cdots, x_n)^{p^r}$, hence $\mathrm{rk}(\mathrm{Ker}F_G^i) = p^{ni}$. In the general case, let r be such that $H = F^rG$ is smooth, let $K = \mathrm{Ker}(F_G^r)$; we have exact sequences:

$$0 \to \mathrm{Ker}(F_K^i) \to \mathrm{Ker}(F_G^i) \to \mathrm{Ker}(F_H^i) \to \mathrm{Coker}(F_K^i) \to \mathrm{Coker}(F_G^i) \to 0$$

$$0 \to \mathrm{Ker}(F_K^i) \to K \to K^{(p^i)} \to \mathrm{Coker}(F_K^i) \to 0$$

The second sequence gives $\mathrm{rk}(\mathrm{Coker}(F_K^i)) = \mathrm{rk}(\mathrm{Ker}(F_K^i)) \leq \mathrm{rk}(K) < \infty$, the first one gives the claimed formula. ■

Corollary 2.10.6. (1) Let $0 \to G' \to G \to G'' \to 0$ be an exact sequence of connected formal-groups. Then $\dim(G) = \dim(G') + \dim(G'')$.

(2) If $f : G' \to G$ is a homomorphism of connected formal group, with G smooth, and $\dim G = \dim G'$, then f is an epimorphism if and only if $\mathrm{Ker}(f)$ is finite.

Proof. (1) follows from the snake diagram and the preceding corollary.

(2) We have the equivalence $(\mathrm{Ker}(f)$ finite$) \iff (\dim(\mathrm{Ker}(f)) = 0) \iff (\dim f(G') = \dim G') \iff (\dim f(G') = \dim G)$. But $\dim(f(G')) = \dim G$ gives

$$\mathrm{rkKer}(F_{f(G')}^i) \geq p^{i \dim G} = \mathrm{rk}(\mathrm{Ker}(F_G^i))$$

hence $\mathrm{Ker}(F_{f(G')}^i) = \mathrm{Ker}(F_G^i)$ and $G = \bigcup \mathrm{Ker}(F_G^i) = \bigcup \mathrm{Ker}(F_{f(G')}^i) = f(G')$. ■

2.11 p-divisible groups

Definition 2.11.1. Suppose $p \neq 0$. A (commutative) formal group G is called p-divisible (or a Barsotti-Tate group) if it satisfies the three following conditions:

(1) $p \cdot \mathrm{id}_G : G \to G$ is an epimorphism,

(2) G is a p-torsion group: $G = \bigcup_j \mathrm{Ker}(p^j \mathrm{id}_G)$,

(3) $\mathrm{Ker}(p\mathrm{id}_G)$ is finite.

We know that $\mathrm{rk}(\mathrm{Ker}(p\mathrm{id}_G)) = p^h$, $h \in \mathbb{N}$. This h is called the height height (G) of G. Using (1), this gives

$$\mathrm{rk}(\mathrm{Ker}(p^j\mathrm{id}_G)) = p^{j\mathrm{height}\ (G)}$$

The multiplicativity of the rank gives the exactness of the sequences

$$0 \to \mathrm{Ker}p^j \hookrightarrow \mathrm{Ker}p^{j+k} \xrightarrow{p^j} \mathrm{Ker}p^k \to 0$$

Conversely, if we have a diagram

$$G_1 \xrightarrow{i_1} G_2 \xrightarrow{i_2} G_3 \to \cdots$$

where the G_i are finite k-groups with the following properties

(a) $\mathrm{rk}(G_j) = p^{hj}$, h a fixed integer,

(b) the sequence $0 \to G_j \xrightarrow{i_j} G_{j+1} \xrightarrow{p^j} G_{j+1}$ are exact,

then $\lim_{\to}(G_n, i_n)$ is a p-divisible formal group, of height h, and $\mathrm{Ker}(p^n\mathrm{id}_G : G \to G) \cong G_n$.

This gives an alternative definition of p-divisible groups.

The Serre dual of a p-divisible group G is the p-divisible group G' defined as follows:

Let $G_j = \mathrm{Ker}(p^j\mathrm{id}_G)$, and let $p_j : G_{j+1} \to G_j$ be induced by $p\mathrm{id}_G$. Put $G'_j = D(G_j)$, and $i'_j = D(p_j) : G'_j \to G'_{j+1}$, then $G' = \lim_{\to}(G'_j, i'_j)$ is a p-divisible formal group, with height (G') = height (G); it is clear that $p'_j = D(i_j)$, so that $(G')'$ can be identified with G.

Example 10. (1) The constant formal group $(\mathbb{Q}_p/\mathbb{Z}_p)$; conversely, any constant p-divisible group of height h is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^h_k$.

(2) Let A be a (commutative) algebraic k-group, such that $p\mathrm{id}_G : A \to A$ is an epimorphism. Then it can be shown that $\mathrm{Ker}(p\mathrm{id}_A)$ is finite; define

$$A(p) = \bigcup \mathrm{Ker}(p^j\mathrm{id}_A)$$

Then $A(p)$ is a p-divisible group, containing $\hat{A}^0 = \bigcup_j \mathrm{Ker}(F^jG)$. For instance, for $A = \mu_k$, one finds $A(p) = \bigcup_j {}_pj\mu_k = (\mathbb{Q}_p/\mathbb{Z}_p)'_k$.

If A is an Abelian variety of dimension g, one knows that $p\mathrm{id}_A$ is an epimorphism, with $\mathrm{rk}(\mathrm{Ker}p\mathrm{id}_G) = p^{2g}$. It follows that $A(p)$ is a p-divisible group of height $2g$.

Proposition 2.11.2. Let G be a k-formal group. Then G is p-divisible if and only if the following conditions are satisfied.

(1) $\pi_0(G)(\bar{k}) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r$, r finite.

(2) G^0 is of finite type, smooth, and $\mathrm{Ker}(V : G^{0(p)} \to G^0)$ is finite.

Proof. If G is p-divisible, then G^0 and $\pi_0(G)$ are, and conversely (replace k by $\bar{k}$, then G is the product of G^0 and $\pi_0(G)$). We already know that the etale group E is p-divisible iff $E(\bar{k}) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r$.

Now suppose that G is connected, $\mathrm{Ker}(F_G) \subseteq \mathrm{Ker}(V_G \circ F_G) = \mathrm{Ker}(p\mathrm{id}_G)$, hence G is of finite type;m on the other hand $G^{(p)}$ also is p-divisible, hence $\mathrm{Ker}(V_G) \subseteq \mathrm{Ker}(F_G \circ V_G) = \mathrm{Ker}(p\mathrm{id}_{G^{(p)}})$ is finite, and F_G is an epimorphism, because $p\mathrm{id}_G(V) = F_G \circ V_G$ is.

Conversely, if G is smooth and $\mathrm{Ker}V_G$ finite, F_G and V_G are epimorphism, hence also $p\mathrm{id}_G = V_G \circ F_G$; this implies also an exact sequence

$$0 \to \mathrm{Ker}(F_G) \to \mathrm{Ker}(p\mathrm{id}_G) \to \mathrm{Ker}(V_G) \to 0$$

and $\mathrm{Ker}(p\mathrm{id}_G)$ also is finite. Finally $\bigcup \mathrm{Ker}(p^j \mathrm{id}_G) \supseteq \bigcup \mathrm{Ker}(F_G^j) = 0$. ■

Example 11. If A is an algebraic unipotent k-group, then $\hat{A}^0$ is never p-divisible, unless A is finite. (Recall that G is unipotent iff $\bigcap \mathrm{Im} V_G^n = e$).

Remark 2.11.3. *The above exact sequence for any p-divisible group G the formula* height $(G) = \dim(G) + \dim(G')$.

Proposition 2.11.4. Let G be a connected, of finite type, smooth formal group. There exist two subgroups $H, K \subseteq G$ with H p-divisible, $p^n K$ for large n, $H \cap K$ finite, and $G = H + K$.

Proof. Let $p^n G = \mathrm{Im}(p^n \mathrm{id}_G : G \to G)$; the subgroups $p^n G$ of G are smooth (quotients of G) and form a decreasing sequence. There exists an n such that $p^n G \cap \mathrm{Ker} F_G = p^{2n} G \cap \mathrm{Ker} F_G$ ($\mathrm{Ker} F_G$ is finite, hence Artinian), then $F_{p^n G/p^{2n} G}$ is a monomorphism. This implies $p^n G = p^{2n} G$, because $p^n G/p^{2n} G$ is connected, smooth with monomorphism Frobenius (or dimension 0). Put $H = p^n G$, $K = \mathrm{Ker}(p^n \mathrm{id}_G)$. Then $G = H + K$, $p\mathrm{id}_H$ is epimorphic, and $p^n K = 0$. Therefore $\mathrm{Ker}(p\mathrm{id}_H)$ is finite, hence H is p-divisible, and $H \cap K \subseteq \mathrm{Ker}(p^n \mathrm{id}_H)$ is finite. ■

2.12 Appendix

Theorem 2.12.1. Let k be perfect field with characteristic $p \neq 0$, A and B two complete Noetherian k-rings with residue field k. If A and B are reduced, so is $A \widehat{\otimes}_k B$.

Proof. To be added. ■

3 Witt Groups and Dieudonne Modules

Let p be a fixed prime number.

3.1 The Artin-Hasse exponential series

Definition 3.1.1. Let k be a ring. We denote by $\bigwedge_k$ the affine k-group which associates with $R \in \mathbf{M}_k$ the multiplicative group $1 + tR[[t]]$ of formal power-series in R which constant term 1 (as a functor, $\bigwedge_k$ is obviously isomorphic to $\mathbf{O}_k^N$). For $n \geq 1$, let $\bigwedge_k^{(n)}$ be the closed subgroup such that

$$\bigwedge_k^{(n)}(R) = 1 + t^n R[[t]]$$

one has obvious exact sequences

$$0 \to \bigwedge_k^{(n+1)} \to \bigwedge_k^{(n)} \to \alpha_k \to 0$$

where the first morphism is the inclusion, the second one being $(1 + a_n t^n + \cdots) \mapsto a_n$. The k-group $\bigwedge_k$ hence appears as the inverse limit of the $\bigwedge_k / \bigwedge_k^{(n+1)}$, each $\bigwedge_k / \bigwedge_k^{(n+1)}$ being an n-fold extension of the additive group. (If k is a field, then $\bigwedge_k$ is a unipotent group).

Let $F = 1 - t + \cdots$ be a fixed element of $\Lambda(k) = 1 + yk[[t]]$. Then we have an isomorphism of k-schemes

$$\varphi : \mathbf{O}_k^{\mathbb{N}_+} \to \bigwedge_k$$

by $\varphi((a_n)) = \prod F(a_n t^n)$.

If $k = \mathbb{Q}$, then take $F(t) = \exp(-t)$; one has $F(at)F(bt) = F((a+b)t)$, so that φ is an isomorphism of k-groups from $\alpha_k^{\mathbb{N}_+}$ to $\bigwedge_k$. If k is a field with characteristic p, it is not possible to find $F \in 1 + tk[[t]]$ with

$$F(t) = 1 - t + \cdots ; \ F(at)F(bt) = F(ct)$$

We find first $F(T) = 1 - t + \cdots + (-t)^{p-1}/(p-1)! + \cdots$ and for the coefficient of T^p we fine $0 = 1$ and the computation fails. But remark that for any F one certainly has a formula

$$F(at)F(bt) = \prod_{i>0} F(\lambda_i(a,b)t^i)$$

where $\lambda_i \in k[X, Y]$.

The idea is to find an F such that most of the λ_i vanish. Actually we shall find F with $\lambda_i = 0$ if i is not a power of p.

Proposition 3.1.2. Let μ be the Mobius function, then there is a classic formula

$$\exp(-t) = \prod_n (1 - t^n)^{\mu(n)/n}$$

Proof. Recall first that $\mu_n = 0$ if n is divisible by the square of a prime, $\mu(p_1 \cdots p_k) = (-1)^k$ if $p_1, \cdots, p_k$ are distinct primes and $\mu(1) = 1$. For $n > 1$, one has

$$\sum_{d|n} \mu(d) = 0$$

It follows that

$$-t = \sum_{n \geq 1} -\frac{1}{n} t^n \sum_{d|n} \mu(d) = \sum_{d \geq 1} \frac{\mu(d)}{d} \sum_m -\frac{1}{m} t^{dm} = \sum_{d \geq 1} \frac{\mu(d)}{d} \log(1 - t^d)$$

■

Definition 3.1.3. If char $k = p > 0$, let

$$F(t) = \prod_{(n,p)=1} (1 - t^n)^{\mu(n)/n} = 1 - t + \cdots ;$$

if $\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q}, (p, b) = 1\}$, then

$$F(t) \in \Lambda(\mathbb{Z}_{(p)})$$

If $\mu(n) \neq 0$, then either $(n, p) = 1$, or $n = pn'$, $(n', p) = 1$.

Proposition 3.1.4. We have $\exp(-t) = F(t)/F(t^p)^{1/p}$, then

$$F(t) = \exp(-t)F(t^p)^{1/p} = \exp(-t - \frac{t^p}{p})F(p^2)^{1/p^2} = \cdots$$

so that

$$\begin{cases} F(t) = \exp L(t), \text{ with} \\ L(t) = -t - \dfrac{t^p}{p} - \dfrac{t^{p^2}}{p^2} - \cdots - \dfrac{t^{p^i}}{p^i} - \cdots - \cdots \end{cases}$$

Remark 3.1.5. *The formula $F(at)F(bt) = \prod(F(\lambda_i(a,b))t^i)$ then can be written as $L(at)+L(bt) = \sum L(\lambda_i(a,b)t^i)$ where $\lambda_i \in \mathbb{Z}_{(p)}[X,Y]$. Going to $\mathbb{Q}$, it follows immediately that $\lambda_i = 0$ if λ is not a power of p, which give a formula*

$$F(at)F(bt) = \prod_{i\geq 0} F(\Psi_i(a,b)t^{p^i})$$

Definition 3.1.6. The Artin-Hasse exponential is defined as the morphism

$$E : \mathbf{O}^{\mathbb{N}}_{\mathbb{Z}_{(p)}} \to \Lambda_{\mathbb{Z}_{(p)}}$$

such that

$$E((a_0, \cdots), t) = \prod_{n\geq 0} F(a_n t^{p^n})$$

From the above remark, it follows easily that there exists formula

$$E((a_i)\cdot t)\cdot E((b_i)\cdot t) = E(S_i(a_0, \cdots, a_i, b_0, \cdots, b_i), t)$$

where $S_i \in \mathbb{Z}_{(p)}[x_0, \cdots, x_i, y_0, \cdots, y_i]$. Moreover, any $P \in \bigwedge(R)$, $R \in \mathbf{M}_{\mathbb{Z}_{(p)}}$, can be uniquely written

$$P(t) = \prod_{(n,p)=1} E((a_n), t^n)$$

with $(a_n) \in R^{\mathbb{N}}$.

Proposition 3.1.7. The $\mathbb{Z}_{(p)}$-group $\Lambda_{\mathbb{Z}_{(p)}}$ is isomorphic to the $\{n : (n,p) = 1\}$-power of the subgroup image of E.

Remark 3.1.8. *By base change a similar statement applies to $\Lambda_{\mathbb{F}_p}$; it shows that the Artin-Hasse exponential plays over $\mathbb{F}_p$ a somewhat similar role as the usual exponential over $\mathbb{Q}$.*

3.2 The Witt rings (over $\mathbb{Z}$)

Remark 3.2.1. *By 3.1.4 we can write*

$$E((a_n), t) = \exp\left(-\sum_{n\geq 0} \frac{t^{p^n}\Phi_n}{p^n}\right)$$

with

$$\Phi_n(a_0, \cdots) = a_0^{p^n} + pa_1^{p^{n-1}} + \cdots + p^n a_n$$

And we have

$$\Phi_n(a_0, \cdots, a_n) + \Phi_n(b_0, \cdots, b_n) = \Phi_n(S_0, \cdots, S_n)$$

Lemma 3.2.2. We have $S_n \in \mathbb{Z}[x_0, \cdots, x_n]$.

Proof. We already know that the coefficients of S_i lie in $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$. On the other hand, it is clear from the above remark that they lie in $\mathbb{Z}[p^{-1}]$. Then the result follows by the truth $\mathbb{Z}_{(p)} \cap \mathbb{Z}[p^{-1}] = \mathbb{Z}$. ■

Theorem 3.2.3. There exists a unique commutative group law on $\mathbf{O}_{\mathbb{Z}}^{\mathbb{N}}$ with the following equivalent properties:

(i) $E : \mathbf{O}_{\mathbb{Z}}^{\mathbb{N}} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)} \to \bigwedge_{\mathbb{Z}_{(p)}}$ is a homomorphism.

(ii) Each $\Phi_n : \mathbf{O}_{\mathbb{Z}}^{\mathbb{N}} \to \alpha_{\mathbb{Z}}$ is a homomorphism.

Proof. Each (i), (ii) is equivalent to the fact that (with + for the law we are constructing)

$$(a_n) + (b_n) = (S_n(a_0, \cdots, a_n, b_0, \cdots, b_n))$$

Hence the uniqueness; it remains to be shown that the law defined above is a commutative group law with unit element $(0, 0, \cdots)$. The associativity, commutativity and unit element axioms can be expresses by polynomials identities, with coefficients in $\mathbb{Z}$, in the coefficients of the S_i. These identities are satisfied after going from $\mathbb{Z}$ to $\mathbb{Z}[p^{-1}]$, because the $\phi_n \otimes_{\mathbb{Z}} \mathbb{Z}[p^{-1}]$ defines an isomorphism $\mathbf{O}^N_{\mathbb{Z}[p^{-1}]} \to \mathbf{O}^N_{\mathbb{Z}[p^{-1}]}$. Because $\mathbb{Z} \subseteq \mathbb{Z}[p^{-1}]$, we are done. The existence of an inverse element can be proved if $p \neq 2$ by the remark that $\varphi(-x_0, -x_1, \cdots) = -\varphi_n(x_0, x_1, \cdots)$; in the general case, the antipodism over $\mathbb{Z}[p^{-1}]$ is given by polynomials with coefficients in $\mathbb{Z}[p^{-1}]$; but these coefficients are also in $\mathbb{Z}_{(p)}$, hence are in $\mathbb{Z}$. ■

Definition 3.2.4. The $\mathbb{Z}$-scheme $\mathbf{O}_{\mathbb{Z}}^{\mathbb{N}}$, together with the above law, is called the $\mathbb{Z}$-group of Witt vectors of infinite length relative to p and denoted by W.

If $w = (a_n) \in W(R) = R^{\mathbb{N}}$, a_n is the nth-component of w and $\Phi_n(w)$ the nth-phantom-component of w. The phantom components define a group isomorphism from $W \otimes_{\mathbb{Z}} \mathbb{Z}[p^{-1}]$ to $\alpha^{\mathbb{N}}_{\mathbb{Z}[p^{-1}]}$.

Let $T : W \to W$ be the monomorphism defined by

$$T((a_0, \cdots, a_n, \cdots)) = (0, a_0, a_1, \cdots)$$

Then $\Phi_0(Tw) = 0$, $\Phi_n(Tw) = p\Phi_{n-1}(w)$, $n \geq 1$; it follows that T is group-homomorphism, called the translation. We define the group W_n of Witt0vectors of length n by the exact sequence of group functors

$$0 \to W \xrightarrow{T^n} W \xrightarrow{R_n} W \to 0$$

(i.e. by $W_n(R) = \mathrm{Coker} T^n(R)$ for each R). By the definition of the group law, it is clear that $(a_0, a_1, \cdots) = (a_0, \cdots, a_{n-1}, 0, \cdots) + T^n(a_n, a_{n+1}, \cdots)$, which means that as a scheme, W_n is $\mathbf{O}_k^n$, the projective morphism $W \to W_n$ being $(a_0, \cdots) \mapsto (a_0, \cdots, a_{n-1})$. The group law on W_n is $(a_0, \cdots, a_{n-1}) + (b_0, \cdots, b_{n-1}) = (S_0(a_0, b_0), \cdots, S_{n-1}(a_0, \cdots, a_{n-1}, b_0, \cdots, b_{n-1}))$ in particular $W_1 = \alpha$. The snake diagram gives from the above exact sequence translation homomorphism $T : W_n \to W_{n+1}$, such that $T(a_0, \cdots, a_{n-1}) = (0, a_0, \cdots, a_{n-1})$, projection homomorphism $R : W_{n+1} \to W_n$ such that $R(a_0, \cdots, a_n) = (a_0, \cdots, a_{n-1})$ and exact sequence

$$0 \to W_m \xrightarrow{T^n} W_{n+m} \xrightarrow{R^m} W_n \to 0$$

Moreover, the projections $W \to W_n$ give rise to an isomorphism

$$W \cong \lim_{\leftarrow} W_n$$

Let $\tau : \mathbf{O}_{\mathbb{Z}} \to W$ be the morphism $a \mapsto (a, 0, \cdots)$. We have $\Phi_n(\tau(a)) = a^{p^n}$, $E(\tau(a), t) = F(at)$.

Theorem 3.2.5. There exists a unique ring-structure on the $\mathbb{Z}$-group W such that each of the two following condition is satisfied.

(i) each $\Phi_n : W \to \mathbf{O}_{\mathbb{Z}}$ is a ring-homomorphism.

(ii) $\tau(ab) = \tau(a)\tau(b)$, $a, b \in R \in \mathbf{M}_{\mathbb{Z}}$.

Proof. We first replace $\mathbb{Z}$ by $P = \mathbb{Z}[p^{-1}]$. Then $(\Phi_n) : W_P \to \alpha_P^N$ is an isomorphism, hence the existence and uniqueness of a ring structure on W_P satisfying (i); moreover, because $(\Phi_n(\tau(a)) = (a^{p^n}))$, this ring-structure satisfies (ii); conversely, consider a ring structure on the P-group α_P^N such that $(a^{p^n}) \cdot (b^{p^n}) = ((ab)^{p^n})$; the multiplication is given by polynomials of the form $(x_n) \cdot (y_n) = (\sum a_{ij}^{(n)} x_i y_j)$, with $\sum a_{ij}^{(n)} a^{p^i} b^{p^j} = (ab)^{p^n}$; this gives $a_{ij}^{(n)} = 0$ except with $i = j = n$, and $(x_n)(y_n) = (x_n y_n)$. This ends the proof for P.

The multiplication in W_P we just found is given by polynomials

$$M_n(x_0, \cdots, x_n, y_0, \cdots, y_n) \in \mathbb{Z}[p^{-1}][x_0, \cdots, x_n, y_0, \cdots, y_n]$$

$$(a_0, \cdots) \times (b_0, \cdots) = (M_n(a_0, \cdots, b_0, \cdots))$$

By definition, $\Phi_i((M_n)) = \Phi_i((x_n)) \cdot \Phi_i((y_n))$, $i = 1, 2, \cdots$. We can prove that $M_n \in \mathbb{Z}[x_0, \cdots, y_0, \cdots]$ ([DG70] V, section 1.2); the above formula defines then a $\mathbb{Z}$-morphism $W \times W \to W$. The fact that it gives a ring structure satisfying (i) and (ii), with unit element $\tau(1) = (1, 0, \cdots)$ can be expressed by identities between polynomials with coefficients in $\mathbb{Z}$; these identities are true over $P = \mathbb{Z}[p^{-1}]$ and $\mathbb{Z} \to P$ is injective. ■

Definition 3.2.6. The $\mathbb{Z}$-ring W is called the Witt ring, each W_n is a quotient ring of W, the canonical morphisms $R : W \to W_n$ and $R : W_{n+1} \to W_n$ are ring-homomorphism (but not T!).

3.3 The Witt rings (over k)

Definition 3.3.1. From now on, k is a field with characteristic p. We denote by W_k, W_{nk}, the k-rings $W \otimes_{\mathbb{Z}} k$, $W_n \otimes_{\mathbb{Z}} k$; remark that the phantom-components $W_K \to \alpha_k$ are now $(a_n) \mapsto a_0^{p^n}$.

Because $W_k = W_{\mathbb{F}_p} \otimes_{\mathbb{F}_p} k$, we can identify $W_k^{(p)}$ and W_k and the Frobenius morphism $F : W_k \to W_k$ is given by

$$F(a_0, \cdots, a_n, \cdots) = (a_0^p, \cdots, a_n^p, \cdots)$$

It is a ring-homomorphism (because F commutes with products). Similar statements are true for $\bigwedge_k$ and the W_{nk}.

Proposition 3.3.2. (a) The Verschiebung morphism of $\bigwedge_k$ is $\varphi_t \mapsto \varphi(t^p)$, the Verschiebung morphism of W_k is T, the Verschiebung morphism of W_{nk} is $R \circ T = T \circ R$.

(b) If $x, y \in W_k(R)$, $R \in \mathbf{M}_k$, then $V((Fx) \cdot y) = x \cdot (Vy)$.

Proof. (a) If $\varphi = 1 + \sum c_n t^n \in \bigwedge(R)$, then $F\varphi = 1 + \sum c_n^p t^n$, and $(F\varphi)(t^p) = 1 + \sum c_n^p t^{np} = \varphi^p = V(F\varphi)$. But F is an epimorphism (k is perfect?), hence $V\psi = \psi(t^p)$, for all ψ.

On the other hand, the definition of E and T shows that

$$E(Tx, t) = E(x, t^p)$$

But $E(x, t^p) = VE(x, t) = E(Vx, t)$ and E is monomorphism, hence $Vx = Tx$. Projecting this formula on W_{nk}, we find $V_{W_{nk}} = R \circ T = T \circ R$.

(b) Because $F : W_k \to W_k$ is an epimorphism, we can now suppose $y = Fz$, then $V((Fx) \cdot y) = V((Fx) \cdot (Fz)) = VF(xz) = pxz = x \cdot pz = x \cdot VFz = x \cdot Vy$. ■

Corollary 3.3.3. If $x, y \in W_k(R)$, then

$$E(x \cdot Vy, t) = E(Fx \cdot y, t^p)$$

Corollary 3.3.4. If $x = (a_0, \cdots, a_n, \cdots) \in W_k(R)$, then $px = (0, a_0^p, \cdots, a_n^p, \cdots)$.

Corollary 3.3.5. Suppose k is perfect; then $W(k)$ is a discrete valuation ring, complete, and $W(k)/pW(k) = k$.

Proof. One has $FW(k) = W(k)$ because k is perfect, hence $p^n W(k) = T^n F^n W(k) = T^n W(k)$ and $W(k) = \lim_{\leftarrow} W(k)/p^n W(k)$. Moreover, $W(k)/pW(k) = W_1(k) = \alpha(k) = k$. ■

Proposition 3.3.6 (Witt)**.** Let k be perfect, and let A be complete Noetherian local with residue field k. Let $\pi : A \to k$ be the canonical projection. There exists a unique ring-homomorphism

$$u : W(k) \to A$$

compatible with the projections $W(k) \to k$ and π. If moreover A is a discrete valuation ring with $p \cdot 1_A \neq 0$, then A is a free finite $W(k)$-module of rank $[A/pA : k]$; in particular, if $pA = A$, then u is an isomorphism.

Proof. (After Cartier). Consider the ring-morphisms given by the phantom components $\Phi_n : W_{n+1}(A) \to A$. If $\mathfrak{m}$ is the maximal ideal of A, then $\Phi_n((x_n)) \in \mathfrak{m}^{n+1}$ if $x_i \in \mathfrak{m}$; this gives a commutative square

$$\begin{array}{ccc} W_{n+1}(A) & \xrightarrow{\Phi_n} & A \\ {\scriptstyle W_{n+1}(\pi)}\downarrow & & \downarrow{\scriptstyle \text{can}} \\ W_{n+1}(k) & \xrightarrow{\Phi_n} & A/\mathfrak{m}^{n+1} \end{array}$$

Let $\sigma : k \to k$ be given by $\sigma(\lambda) = \lambda^{1/p}$ and put $u_n = \Phi_n \circ W_{n+1}(\sigma^n)$; then, if $a_0, \cdots, a_n \in A$

$$u_n(\pi(a_0^{p^n}), \cdots, \pi(a_n^{p^n})) = a_0^{p^n} + pa_1^{p^{n-1}} + \cdots + p^n a_n (\text{mod } \mathfrak{m}^{n+1})$$

Let

$$u = \lim_{\leftarrow} u_n : W(k) \to A$$

Then u is a ring-morphism and $\pi u(\alpha_0, \cdots, \alpha_n) = \alpha_0$. This gives the existence of u. Let $u' : W(k) \to A$ be another such homomorphism; then $\tau' = u'\tau : k \to A$ is compatible with

multiplication and such that $\pi\tau' = \mathrm{id}$; such a τ' is unique, as is well-known (because $\tau'(\alpha)$ must be in $\bigcap(\pi^{-1}(\alpha^{p^{-n}}))^{p^n}$ which has only one element (Cauchy)); on the other hand, any $x \in W(k)$ can be written

$$x = (\alpha_0, \alpha_1, \cdots) = (\alpha_0, 0, \cdots) + (0, \alpha_1, 0, \cdots) + \cdots = \tau(\alpha_0) + p\tau(\alpha^{1/p}) + p^2\tau(\alpha_2^{1/p^2}) + \cdots$$

and $u'(x)$ must be $\tau'(\alpha_0) + p\tau'(\alpha^{1/p}) + \cdots$, hence the unicity of u.

The last statement follows from the fact that if $a_1, \cdots, a_e \in A$ are a basis of A modulo pA, then they generate the $W(k)$-modulo A. Therefore A is finitely generated as $W(k)$-module, without torsion because $p^n \cdot 1_A \neq 0$, hence free of rank $[A/pA : k]$. ■

3.4 Duality of finite Witt groups

Definition 3.4.1. For $m, n \geq 1$, we put

$$ {}_mW_n : \mathrm{Ker}(F^m : W_{nk} \to W_{nk})$$

Between these finite k-groups, we have homomorphisms

$$\begin{array}{ccc} {}_mW_n & \xrightarrow{t} & {}_mW_{n+1} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle r} \\ {}_{m-1}W_n & \xrightarrow{i} & {}_mW_n \end{array}$$

where i is the canonical inclusion, and f, t, r are induced by F, T, R. Clearly, i and t are monomorphisms, f and r are epimorphisms, and for the group ${}_mW_n$, we have $F = i \circ f$, $V = r \circ t$.

Remark 3.4.2. *For any $R \in \boldsymbol{M}_k$, let $W'(R)$ be the set of all $(a_0, a_1, \cdots) \in W_k(R)$ such that $a_n = 0$ for large n, and a_n nilpotent for all n. It is easy to check $W'(R)$ is an ideal in $W_k(R)$ and that $E(w, t)$ is a polynomial for $w \in W'(R)$; in particular, $E(w, 1)$ is defined for $w \in W'(R)$, and we have a group-homomorphism*

$$\tilde{E} : W' \to \mu_k$$

given by $w \mapsto E(w, 1)$. If $x \in W_k(R)$, $y \in W'(R)$, then $xy \in W'(R)$ and $E(xy, 1) \in R^*$; moreover, one has

$$E(T^n x \cdot y, 1) = E(T^n(x \cdot F^n y), 1) = E(x \cdot F^n y, 1)$$

The morphism $(x, y) \mapsto E(xy, 1)$ from $W_k \times W'$ to μ_k is bilinear, hence gives a group-homomorphism $W' \to D(W_k)$ (this can be shown to be an isomorphism).

Remark 3.4.3. *Let $\sigma_n : W_{nk} \to W_k$ be the section of $R_n : W_k \to W_{nk}$ define by $\sigma_n(a_0, \cdots, a_{n-1}) = (a_0, \cdots, a_{n-1}, 0, \cdots)$ (σ_n is not a group homomorphism); it is clear that σ_n sends ${}_mW_n$ in W'.*

Theorem 3.4.4. For $x \in {}_mW_n(R)$, $y \in {}_nW_m(R)$, define

$$\langle x, y \rangle = E(\sigma_n(x)\sigma_m(y), 1)$$

Then $\langle x, y \rangle$ is bilinear, gives an isomorphism

$$ {}_mW_n \cong D({}_nW_m)$$

and satisfies

$$\langle x, ty\rangle = \langle fx, y\rangle$$

$$\langle x, ry\rangle = \langle ix, y\rangle$$

Proof. Let $x, x' \in {}_mW_n(R)$, $y \in {}_nW_m(R)$; then $\sigma_n(x+x') - \sigma_n(x) - \sigma_n(x')$ is in $\mathrm{Ker}(R_n) = \mathrm{Im}T^n$, hence

$$\sigma_n(x+x') = \sigma_n(x) + \sigma_n(x') + T^n(u)$$

where $u \in W'(R)$. This implies

$$\langle x+x', y\rangle = \langle x, y\rangle + \langle x', y\rangle + E(T^n(u)\cdot\sigma_m(y), 1) = E(u\cdot F^n\sigma_m(y), 1) = E(u\cdot\sigma_m(F^n y), 1) = 0$$

This proves the bilinearity of $\langle \bullet, \bullet\rangle$.

On the other hand, $\sigma_n(fx) = F\sigma_n(x)$, $\sigma_{m+1}(ty) = T\sigma_m(y)$, hence $\langle fx, y\rangle = \langle x, ty\rangle$; also $\sigma_n(ix) = \sigma_n(x)$, then for $x \in {}_{m-1}W_n, y \in {}_nW_m$, note that $ry - y \in \mathrm{Ker}(R_{m-1}) = \mathrm{Im}(T^{m-1})$, thus $ry - y = T^{m-1}u$ for some $u \in W'(R)$ and

$$\begin{aligned}
&\langle x, ry\rangle - \langle ix, y\rangle \\
=&E(\sigma_n(ix)\sigma_{m-1}(y), 1) - E(\sigma_n(x)\sigma_m(y), 1) \\
=&E(\sigma_n(x)\cdot T^{m-1}u, 1) \\
=&E((F^{m-1}\sigma_n(x))\cdot u, 1) \\
=&E(\sigma_n(F^{n-1}x)\cdot u, 1) = 0
\end{aligned}$$

Hence $\langle x, ry\rangle = \langle ix, y\rangle$.

It remains to prove that $\langle \bullet, \bullet\rangle$ gives an isomorphism between ${}_mW_n$ and $D({}_nW_m)$; but, because of the exact sequences

$$0 \to {}_mW_n \xrightarrow{i^q} {}_{m+q}W_n \xrightarrow{f^m} {}_qW_n \to 0$$

and

$$0 \to {}_nW_m \xrightarrow{t^q} {}_nW_{m+q} \xrightarrow{r^m} {}_nW_q \to 0$$

and the adjointness of t and f and i, we are reduced by induction on m and n to the case $m = n = 1$. In that case ${}_1W_1 = {}_p\alpha_k$, and $\langle \bullet, \bullet\rangle$ is not zero, hence the given homomorphism ${}_p\alpha_k \to D({}_p\alpha_k)$ is not zero; but, because ${}_p\alpha_k$ is simple, it is an isomorphism, and the proof is complete. ■

3.5 Dieudonne modules (Affine unipotent groups)

Remark 3.5.1. *From now on, the field k is supposed to be perfect.*

Obviously $W_i = \mathrm{Spf}(\mathbb{Z}[x_0, \cdots, x_{i-1}])$ as k-functors, then W_{ik} is affine, and further is unipotent since $\bigcap \mathrm{Im}V^n_{W_i} = e$.

Definition 3.5.2. Let $\underrightarrow{W}$ be the inductive system of $\mathbf{ACu}_k$:

$$\underrightarrow{W} : W_{1k} \xrightarrow{T} W_{2k} \xrightarrow{T} W_{3k} \xrightarrow{T} \cdots$$

($\underrightarrow{W}$ can be seen as the set of finite vectors with the first coordinate is not zero.)

The ring $W(k)$ operates on $\underrightarrow{W}$ as follows. First, we denote by $\sigma : a \mapsto a^{(p)}$ the Frobenius homomorphism $W(k) \to W(k)$, and by $a \mapsto a^{(p^n)}$ its nth power, $n \in \mathbb{Z}$ ($a \mapsto a^{(p)}$ is bijective, because k is perfect.) Let $a \in W(k)$ and $w \in W_n(R)$, $R \in \mathbf{M}_k$; then we define

$$a * w = a_R^{(p^{1-n})} \cdot w$$

where $a_R^{(p^{1-n})}$ is the image of $a^{(p^{1-n})}$ in $W(R)$, and $b \cdot w \in W_n(R)$ the product of $b \in W(R)$ and $w \in W_n(R) = W(R)/T^n W(R)$. By this definition, $W_n(R)$ becomes a $W(k)$-module, and $T : W_n(R) \to W_{n+1}(R)$ is a homomorphism of $W(k)$-module, because

$$T(a * w) = T(a_R^{(p^{1-n})} \cdot w) = T(F(a_R^{p^{-n}}) \cdot w) = a^{p^{-n}} \cdot Tw = a * (Tw)$$

Definition 3.5.3. For any $G \in \mathbf{ACu}_k$, we define the Dieudonne module $M(G)$ to be the $W(k)$-module

$$M(G) = \varinjlim \mathrm{Mor}_{ACu_k}(G, W_{nk})$$

(equivalently $M(G) = \mathrm{Ind}_{\mathbf{ACu}_k}(G, \underrightarrow{W})$). Of course, $G \mapsto M(G)$ is a contravariant functor from $\mathbf{ACu}_k$ to category Mod$W(k)$ of all $W(k)$-modules. This construction obviously commutes with automorphisms $k \cong k$, in particular with $f_k : K \to k$. If M is a $W(k)$-module, let $M^{(p)} = M \otimes_{W(k),\sigma} W(k)$: as a group $M^{(p)} = M$, but the external law is $(w, m) \mapsto w^{(p^{-1})}m$; if $f \in \mathrm{Mor}_{\mathbf{ACu}_k}(G, W_{nk})$, then $f^{(p)}$ is a homomorphism from $G^{(p)}$ to $W_{nk}^{(p)} = W_{nk}$. Hence a map $f \mapsto f^{(p)}$ from $M(G)$ to $M(G^{(p)})$; it is clear that $(wf)^{(p)} = w^{(p)}f^{(p)}$ for $w \in W(k)$, and this induces an isomorphism

$$M(G)^{(p)} \xrightarrow{\sim} M(G^{(p)})$$

by means of which we always identify $M(G^p)$ with $M(G)^{(p)}$.

The two morphisms F_G and V_G define two morphisms $F = M(F_G) : M(G)^{(p)} \to M(G)$, and $V = M(V_G) : M(G) \to M(G)^{(p)}$, or equivalently, group homomorphisms $F, V : M(G) \to M(G)$ with $F(am) = a^{(p)}Fm$, $V(a^{(p)}m) = aVm$, $a \in W(k)$, $m \in M(G)$. By construction, if $\bar{m} \in \mathrm{Mor}_{\mathbf{ACu}_k}(G, W_{nk})$ represents $m \in M(G)$, Fm and Vm are represented by $F_{W_{nk}} \circ \bar{m}$ and $V_{W_{nk}} \circ \bar{m}$.

Remark 3.5.4. *The morphism $T : W_{nk} \to W_{(n+1)k}$ being a monomorphism, the maps $\mathrm{Mor}_{\boldsymbol{ACu}_k}(G, W_{nk}) \to \mathrm{Mor}_{\boldsymbol{ACu}_k}(G, W_{(n+1)k})$ are injective, and $\mathrm{Mor}_{\boldsymbol{ACu}_k}(G, W_{nk})$ can be identified with a submodule of $M(G)$; more precisely*

$$\mathrm{Mor}_{\boldsymbol{ACu}_k}(G, W_{nk}) = \{m \in M(G) | V^n m = 0\}$$

It follows that any element of $M(G)$ is killed by a power of V.

Definition 3.5.5. Let D_k be the (non-commutative) ring generated by $W(k)$ and two elements F and V subject to the relations

$$Fw = w^{(p)}F,\ w^{(p)}V = Vw,\ FV = VF = p$$

It can be easily seen that any element can be written uniquely as a finite sum

$$\sum_{i>0} a_{-i}V^i + a_0 + \sum_{i>0} a_i F^i$$

If $G \in \mathbf{ACu}_k$, then $M(G)$ has a canonical structure of a left D_k-module; if K is a perfect extension of k, there is a canonical map of D_k-modules

$$W(K) \otimes_{W(k)} M(G) \to M(G \otimes_k K)$$

(remark that $D_K \cong W(K) \otimes_{W(k)} D_k$, and that the left hand side can also be written $D_K \otimes_{D_k} M(G)$).

Theorem 3.5.6. The functor M induces an anti-equivalence between $\mathbf{ACu}_k$ and the category of all D_k-modules of V-torsion. For any perfect extension K of k, the morphism $W(K)\otimes_{W(k)}M(G)\to M(G\otimes_k K)$ is an isomorphism. Moreover,

$$G \text{ is algebraic } \iff M(G) \text{ is a finitely generated } D_k\text{-module}$$

$$G \text{ is finite } \iff M(G) \text{ is a } W(k)\text{-module of finite length}$$

3.6 Dieudonne modules (p-torsion finite k-groups)

Proposition 3.6.1. The functor $G\mapsto M(G)$ induces an anti-equivalence between $\mathbf{Feu}_k$ (resp. $\mathbf{Fiu}_k$) and the category of D_k-modules, which are $W(k)$-modules of finite length, killed by a power of V and on which F is bijective (resp. and killed by a power of F).

This follows from the above theorem, and the fact that if G is finite, then G is etale (resp. infinitesimal) if and only if F_G is an isomorphism (resp. $F_G^n=0$ for large n).

Example 12. If $G=(\mathbb{Z}/p\mathbb{Z})_k\in\mathbf{Feu}_k$, then $M(G)=k$ with $F=1,V=0$; if $G={}_p\alpha_k\in\mathbf{Fiu}_k$, then $M(G)=0$ with $F=0,V=0$.

Corollary 3.6.2. For $G\in\mathbf{Feu}_k$ or $\mathbf{Fim}_k$, we have

$$\mathrm{rk}(G)=p^{\mathrm{length}(M(G))}$$

Definition 3.6.3. Let m,n be two positive integers; consider the canonical injection ${}_mW_n\to W_n$; it defines an element $u\in M({}_mW_n)$, clearly $V^nu=F^mu=0$, hence a map of D-modules ($D=D_k$):

$$\lambda_{m,n}: D/(DF^m+DV^n)\to M({}_mW_n)$$

Proposition 3.6.4. $\lambda_{m,n}$ is bijective.

Proof. Using the exact sequence connecting the ${}_mW_n$, we are already reduced to the case $m=n=1$; but $D/(DF+DV)\cong k$ and $M({}_1W_1)=M({}_p\alpha_k)=k$. ∎

Corollary 3.6.5. Take $m=n$. Any element in $D/(DF^n+DV^n)$ can be written in a unique way $x=w_{1-n}V^{n-1}+\cdots+w_{-1}V+w_0+w_1F+\cdots+w_{n-1}F^{n-1}$ where $w_i\in W_{n-|i|}(k)$; we therefore have a canonical $W(k)$-linear projection

$$\pi_n: M_n({}_nW_n)\to W_n(k)$$

defined by $\pi_n(\lambda_n(x))=w_0$.

Definition 3.6.6. Let Q be the quotient field of $W(k)$, and W_∞ be the $W(k)$-module $Q/W(k)$; it can be identified with the direct limit of the system

$$W(k)/pW(k)\xrightarrow{p}W(k)/p^2W(k)\to\cdots$$

but this system is also

$$W_1(k)\xrightarrow{T}W_2(k)\xrightarrow{T}W_3(k)\to\cdots$$

Hence $W_\infty=\lim_{\to}W_n(k)=\underrightarrow{W}(k)$.

Definition 3.6.7. For any D_k-module M, we denote by M^* the following D_k-module: as $W(k)$-module, $M^* = \mathrm{Mor}_{\mathrm{Mod}W(k)}(M, W_\infty)$; if $f \in M^*$, then $(Ff)(m) = f(Vm)^{(p)}$, $(Vf)(m) = f(Fm)^{(p^{-1})}$. It is clear (duality of finite length modules over a principal ideal ring) that $M \mapsto M^*$ induces a duality in the category of D_k-modules which are of finite length over $W(k)$.

Proposition 3.6.8. Let now $G \in \mathbf{Fiu}_k$, then there exists n such that $V_G^n = 0$, $F_G^n = 0$; it follows that $M(G) = \mathrm{Mor}_{\mathbf{Fiu}_k}(G, {}_nW_n)$; moreover $V_{D(G)}^n = 0$, $F_{D(G)}^n = 0$, and $M(D(G)) = \mathrm{Mor}_{\mathbf{Fiu}_k}(D(G), {}_nW_n)$. Let $m : D(G) \to {}_nW_n$ be an element of $M(D(G))$; let $ah_n : {}_nW_n \to D({}_nW_n)$ be the isomorphism, and look at the composed homomorphism

$$ {}_nW_n \xrightarrow{ah_n} D({}_nW_n) \xrightarrow{D(m)} D(D(G)) \cong G $$

this gives a D-linear map $\varphi_m : M(G) \to M({}_nW_n)$; composing this with $\pi_n : M({}_nW_n) \to W_n(k)$ and the canonical injection $W_n(k) \to W_\infty$, we get a $W(k)$-linear map $M(G) \to W_\infty$, i.e. an element of $M(G)^*$. Hence a map

$$ M(D(G)) \to M(G)^* $$

This map is independent of the choice of the integer n: if we replace $m : D(G) \to {}_nW_n$ by $m' = itm = tim : D(G) \to {}_{n+1}W_{n+1}$, then $D(M)ah_n$ is replaced by $\varphi_{m'} = M(D(m)ah_nfv) = M(fv)M(D(m)ah_n) = M(fv)\varphi_m$. But $M(fv) : D/(DF^n + DV^n) \to D/(DF^{n+1} + V^{n+1})$ is of course $x \mapsto FVx = px$, and $\pi_{n+1}M(fv) = \pi_{n+1}p = \pi_n$.

The $W(k)$-linear map

$$ M(D(G)) \to M(G)^* $$

is actually an isomorphism of D_k-modules.

In short, the autoduality $G \mapsto D(G)$ of $\mathbf{Fiu}_k$ corresponds, via the Dieudonne functor, to the autoduality $M \mapsto M^*$ in the category of D_k-module of finite length killed by a power of V and F.

Definition 3.6.9. Let now $G \in \mathbf{Fim}_k$ ($D(G) \in \mathbf{Feu}_k$), we define the Dieudonne module $M(G)$ by

$$ M(G) = M(D(G))^* $$

It follows from the Cartier duality between $\mathbf{Fim}_k$ and $\mathbf{Feu}_k$ that the functor $G \mapsto M(G)$ just defined induces an antiequivalence between $\mathbf{Fim}_k$ and the category of all D_k-modules of finite length on which F is nilpotent and V is bijective.

Remark 3.6.10. *We can describe $M(G)$ as follows. Suppose first G is diagonalisable: $G = D(\Gamma_k)$. Then $D(G) \cong \Gamma_k$, and $M(D(G)) = \varinjlim \mathrm{Mor}_{\boldsymbol{ACu}_k}(\Gamma_k, W_{nk}) = \varinjlim \mathrm{Hom}(\Gamma, W_n(k)) = \mathrm{Hom}(\Gamma, W_\infty) = \mathrm{Mor}_{\mathrm{Mod}W(k)}(W(k) \otimes_{\mathbb{Z}} \Gamma, W_\infty)$, hence*

$$ M(G) \cong W(k) \otimes_{\mathbb{Z}} \Gamma $$

In general, G is defined by a Galois module Γ and $M(G)$ is the set of invariants under the Galois group Π of $M(G \otimes_k \bar{k})$; hence

$$ M(G) \cong (W(\bar{k} \otimes_{\mathbb{Z}} \Gamma))^{\Pi} $$

Moreover, F and V are easily described by duality

$$ F(\lambda \otimes \chi) = \lambda^{(p)} $$

$$ V(\lambda \otimes \chi) = \lambda^{p^{-1}} \otimes \chi $$

Proposition 3.6.11. Let $\mathbf{F}_{p^k}$ be the category of all finite k-groups of p-torsion. Any G in $\mathbf{F}_{p^k}$ decomposes uniquely as $H \times K$, with $H \in \mathbf{Fiu}_k \times \mathbf{Feu}_k$, $K \in \mathbf{Fim}_k$ and we define $M(G)$ as $M(H) \times M(K)$.

Theorem 3.6.12. (a) The functor $G \mapsto M(G)$ is an antiequivalence between the category $\mathbf{F}_{p^k} = \mathbf{Fiu}_k \times \mathbf{Feu}_k \times \mathbf{Fim}_k$ of all finite k-groups of p-torsion, and the category of all triples (M, F_M, V_M) where M is a finite length $W(k)$-module and F_M and V_M two group endomorphism of M such that

$$F_m(\lambda m) = \lambda^{(p)} F_M(m)$$
$$V_M(\lambda^{(p)} m) = \lambda V_M(m)$$
$$F_M V_M = V_M F_M = p \cdot \mathrm{id}_M$$

(b) G is etale, infinitesimal, unipotent or multiplicative according as F_M is isomorphic, F_M nilpotent, V_M nilpotent, or V_M isomorphic.

(c) For any $G \in \mathbf{F}_{p^k}$, one has $\mathrm{rk}(G) = p^{\mathrm{length} M(G)}$.

(d) If K is a perfect extension of k, there exists a functorial isomorphism

$$M(G \otimes_k K) \cong W(K) \otimes_{W(k)} M(G)$$

(e) There exists a functorial isomorphism

$$M(D(G)) = M(G)^*$$

3.7 Dieudonne modules (p-divisible groups)

Lemma 3.7.1. Let $\cdots \to M_{n+1} \xrightarrow{\pi_n} M_n \to \cdots \to M_1$ be a system of $W(k)$-modules with the following properties.

(1) The sequence $M_{n+1} \xrightarrow{p^n} M_{n+1} \xrightarrow{\pi_n} M_n \to 0$ is exact for all n.

(2) M_n is of finite length for all n.

Let $M = \lim_{\leftarrow} M_n$. Then M is a finitely generated $W(k)$-module and the canonical map $M \to M_n$ identifies M_n with $M/p^n M$, for all n.

Proof. It follows from (1) that

$$M_{n+m} \xrightarrow{p^n} M_{n+m} \xrightarrow{\pi} M_n \to 0$$

is exact for all n and m (where $\pi = \pi_n \circ \pi_{n+1} \circ \cdots \circ \pi_{m-1}$). Taking the inverse limit over m, we find an exact sequence

$$M \xrightarrow{p^n} M \xrightarrow{\lambda_n} M_n \to 0$$

(the $\lim_{\leftarrow}$ functor is exact for finite length modules) where λ_n is the canonical projection, hence the last assertion. Let now $m_1, \cdots, m_r$ be elements in M generating $M/pM = M_1$; consider the $W(k)$-module homomorphism $\varphi : W(k)^r \to M$ such that $\varphi(a_1, \cdots, a_r) = a_1 m_1 + \cdots + a_r m_r$. It induces surjective maps $W(k)^r/p^n W(k)^r \to M/p^n M$ for all n hence is surjective as an inverse limit of surjective maps of finite length modules. ∎

Definition 3.7.2. We say that a formal group G is of p-torsion if

(1) $G = \bigcup(\mathrm{Ker} p^n \mathrm{id}_G)$.

(2) $\mathrm{Ker}(p\mathrm{id}_G)$ is finite.

We have exact sequence

$$0 \to \mathrm{Ker}(p^n) \to \mathrm{Ker}(p^{n+1}) \xrightarrow{p^n} \mathrm{Ker}(p^{n+1})$$

$$0 \to \mathrm{Ker}(p^n) \to \mathrm{Ker}(p^{m+n}) \xrightarrow{p^n} \mathrm{Ker}(p^m)$$

the latter show by induction that $\mathrm{Ker}(p^n)$ is finite for all n. Define $M(G) = \lim_{\to} M(\mathrm{Ker}(p^n))$.

Theorem 3.7.3. $G \mapsto M(G)$ is an antiequivalence between the category of p-torsion formal groups and the category of tuples (M, F_M, V_M) where M is a finitely generated $W(k)$-module and F_M, V_M two group endomorphisms of M with

$$F_M(wm) = w^{(p)} F_M(m)$$

$$V_M(w^{(p)} m) = w V_M(m)$$

$$F_M V_M = V_M F_M = p\mathrm{id}_M$$

Proof. It follows from the lemma that $M(G)$ is finitely generated and that $M_n \cong M(G)/p^n M(G)$. Conversely, if M is as before, then we define G as $\lim_{\to} G_n$ where $M(G_n) = M/p^n M$. ■

Remark 3.7.4. *From the definitions and what was already proved follow immediately:*

(1) G is finite if and only if $M(G)$ is of finite length.

(2) G is p-divisible if and only if $M(G)$ is torsion-free (= free), and

$$\text{height } (G) = \dim M(G)$$

(3) For any perfect extension K/k, there is a functorial isomorphism

$$M(G \otimes_k K) \cong W(K) \otimes_{W(k)} M(G)$$

(4) If G is p-divisible, with Serre dual G', then

$$M(G') = \mathrm{Mor}_{\mathrm{Mod}W(k)}(M(G), W(k))$$

with $(F_{M(G')} f)(m) = f(V_M m)^{(p)}$, $(V_{M(G')} f)(m) = f(F_M m)^{(p^{-1})}$.

Indeed, let $M(G) = M$; then $M = \lim_{\leftarrow} M/p^n M$, and $M/p^n M = M(\mathrm{Ker}(p^n \mathrm{id}_G))$; but G' is defined as $\lim_{\to} D(\mathrm{Ker}(p^n \mathrm{id}_G))$, hence

$$\begin{aligned} M(G') &= \lim_{\leftarrow} M(D(\mathrm{Ker}(p^n \mathrm{id}_G))) \\ &= \lim_{\leftarrow} (M/p^n M)^* \\ &= \lim_{\leftarrow} \mathrm{Mor}_{\mathrm{Mod}W(k)}(M/p^n M, W(k)/p^n W(k)) \\ &= \mathrm{Mor}_{\mathrm{Mod}W(k)}(M, W(k)) \end{aligned}$$

3.8 Dieudonne modules (connected formal group of finite type)

Definition 3.8.1. By a similar discussion (replacing p by F), we have the following results: if G is a connected finite type formal group, define $M(G) = \lim_{\leftarrow} M(\mathrm{Ker}(F_G^n))$; it is a module over the F-completion $\hat{D}_k$ of D_k.

Theorem 3.8.2. $G \mapsto M(G)$ is an antiequivalence between the category of connected formal groups of finite type and the category of finite types $\hat{D}_k$-modules M such that M/FM has finite length. Moreover

(1) G is finite $\iff$ $M(G)$ has finite length $\iff$ $F^n M(G) = 0$ for n large.

(2) G is smooth $\iff$ $F : M(G) \to M(G)$ is injective; in that case, $\dim(G) = \mathrm{length}(M(G)/F(M(G)))$.

4 Classification of p-divisible groups

Remark 4.0.1. *k is a perfect field (unless otherwise stated),* char $(k) \neq 0$*; we denote by $B(k)$ the quotient field of $W(k)$, and extend $x \mapsto x^{(p)}$ in $W(k)$ (resp. $B(k)$) is $W(\mathbb{F}_p) = \mathbb{Z}_p$ (resp. $B(\mathbb{F}_p) = \mathbb{Q}_p$).*

4.1 Isogenies

Definition 4.1.1. A F-lattice (resp. F-space) over k is a free $W(k)$-module (resp. a $B(k)$-vector space), of finite rank, together with an injective (resp. injective=bijective) group endomorphism F such that $F(\lambda x) = \lambda^{(p)} F x$. If M is a F-lattice, then $M \otimes_{W(k)} B(k)$ has a natural F-space structure.

Proposition 4.1.2. To each p-divisible group G, we associate the F-lattice $M(G)$, and the F-space $E(G) = B(k) \otimes_{W(k)} M(G)$; the functor $G \mapsto M(G)$ is an antiequivalence between p-divisible groups and those F-lattices M for which for which $FM \supseteq pM$.

Definition 4.1.3. If K is a perfect extension of k, and M a F-lattice over k, we define M_K as $W(k) \otimes_{W(k)} M$, similar for F-spaces.

Lemma 4.1.4. Let G and H be two p-divisible groups of the same height and $f : G \to H$ be a homomorphism. The following conditions are equivalent:

(a) $\mathrm{Ker}(f)$ is finite,

(b) f is an epimorphism,

(c) $M(f) : M(H) \to M(G)$ is injective,

(d) $\mathrm{Coker} M(f)$ is finite,

(e) $E(f) : E(H) \to E(G)$ is an isomorphism.

Such an f is called an isogeny.

Proposition 4.1.5. Let G and H be two p-divisible groups. Then $E(G)$ and $E(H)$ are isomorphic if and only if there exists an isogeny $f : G \to H$.

Two such groups are called isogenous. The classification of p-divisible groups isogeny is therefore equivalent to classification of F-spaces of the form $E(G)$.

Proof. Let $\varphi : E(H) \to E(G)$ be an isomorphism; there exists m such that $\varphi(M(H)) \subseteq p^{-m}M(G)$, then $p^m\varphi : M(H) \to M(G)$ corresponds to an isogeny f. The converse is clear. ■

Definition 4.1.6. A F-space E is called effective if it contains a lattice (i.e. a $W(k)$-submodule M such that $E = B(k) \otimes_{W(k)} M$) stale by F, i.e., if it comes from an F-lattice. It comes from a p-divisible group if and only if it contains a lattice stable by F and pF^{-1}.

4.2 The category of F-spaces

Proposition 4.2.1. This is a $\mathbb{Q}_p$-linear category: an Abelian category, such that $\mathrm{Hom}(E_1, E_2)$ has a natural (finite dimension; in fact) $\mathbb{Q}_p$-vector space structure, the composite map $(f, g) \to g \circ f$ being $\mathbb{Q}_p$-bilinear (note that $\mathbb{Q}_p$ is the center of $B(k)$).

It has tensor products and internal Hom: if E_1, E_2 are F-spaces, then $E_1 \otimes E_2$ and $\mathrm{Hom}(E_1, E_2)$ are the usual $\otimes$ and Hom of $B(k)$-vector spaces and $F(x \otimes y) = Fx \otimes Fy, (Fu)(x) = u(F^{-1}x)^{(p)}$, $x \in E_1, y \in E_2$, $u \in \mathrm{Hom}(E_1, E_2)$.

We denote by $\square$ the F-space $(B(k), x \mapsto x^{(p)})$, by $\square(n)$ the F-space $(B(k), x \mapsto p^{-n}x^{(p)})$. The dual $\check{E}$ of E is $\mathrm{Hom}(E, \square)$, the nth twist $E(n)$ of E is $E \otimes \square(n)$.

We have the usual canonical isomorphisms

$$\mathrm{Hom}(A, \mathrm{Hom}(B, C)) = \mathrm{Hom}(A \otimes B, C)$$

$$\mathrm{Hom}(\square, A) = A$$

$$\mathrm{Hom}(A, B) = \mathrm{Hom}(\square, \mathrm{Hom}(A, B))$$

$$A \otimes (B \otimes C) = (A \otimes B) \otimes C$$

In particular

$$E(m)(n) = E(m + n)$$

$$\widetilde{E(m)} = \check{E}(-m)$$

If G is a p-divisible group and G' its Serre dual, then

$$E(G') = \mathrm{Hom}(E(G), \square(-1)) = \widetilde{E(G)}(-1)$$

(because Serre duality sends F to $V = pF^{-1}$).

These conditions commute with the base-extension functor $E \mapsto E_k = E \otimes_{B(k)} B(K)$ (K/k a perfect extension).

4.3 The F-spaces E^λ, $\lambda \geq 0$

Definition 4.3.1. Let $\lambda \geq 0$ be a rational number; write $\lambda = \frac{s}{r}$, with $r, s \in \mathbb{N}$, $r > 0$, $(r, s) = 1$. We define the F-lattice M^λ over $\mathbb{F}_p$ by

$$M^\lambda = \mathbb{Z}_p[T]/(T^r - p^s)$$

F acting by multiplication by T, and similarly, the F-space E^λ over $\mathbb{F}_p$ by

$$E^\lambda = \mathbb{Q}_p[T]/(T^r - p^s)$$

If $0 \leq \lambda \leq 1$, then $r \geq s$; define $\bar{M}^\lambda = \mathbb{Z}_p[F]/(F^{r-s} - V^s)$, then $\bar{M}^\lambda$ is a lattice in E^λ and a Dieudonne module; actually, let G^λ be the p-divisible group over $\mathbb{F}_p$ defined by the exact sequence

$$0 \to G^\lambda \to W(p)$$

References

[DG70] Michel Demazure and Peter Gabriel. *Groupes algébriques*, volume 1. Elsevier Science & Technology, 1970.