Thomas Zink

Cartier Theory of Commutative Formal Groups

in collaboration with Harry Reimann

This is a translation from the German of the book *Cartiertheorie kommutativer formaler Gruppen* by Thomas Zink, printed in 1984 as volume 68 of the "Teubner-Texte zur Mathematik" of Teubner Publishing Company, Leipzig.

The translation was done by Marco Garuti, Michaël Le Barbier Grünewald, Cédric Pépin, and Matthieu Romagny.

The original numbering of chapters, sections and theorems was preserved and a little homogenized. As a general rule, theorems, definitions, remarks (etc.) are given a number of the form $x.y$ and equations are given a number of the form $(x.y.z)$, where x is the chapter number and y is the running number inside a chapter. A small number of exceptions have been tolerated in order to maintain the correspondence with the numbering of the original german text. All equation numbers are displayed in brackets — a rule which in principle has no exception, this time. Each important new term is *emphasized* the first time it appears (usually, in a definition in due form). The page numbers of the original text are indicated in the margins.

The theory of commutative formal groups plays an important role in algebraic number theory and algebraic geometry over a field of characteristic p. The french mathematician P. Cartier found a new approach to this theory which is simpler and more general than others and which has interesting applications to abelian varieties. 2

This book is for students and mathematicians interested in algebraic geometry or number theory and familiar with commutative algebra. It gives a new presentation of the theory based on concepts of deformation theory. Besides the so-called main theorems of the theory, it contains basic facts on isogenies, deformations of p-divisible formal groups and Dieudonné's classification.

Preface

This book has its origin in lectures that I gave during the academic year 1979/1980 at the Humboldt Universität of Berlin. M. H. Reimann elaborated on these lectures and improved a couple of proofs. I rested on his preparatory work in order to complete the manuscript. 3

The book assumes that the reader has a basic knowledge in Commutative Algebra, as one can find in the books [2], [11], [21].

The first chapter is an introduction to the theory of formal groups from an elementary point of view. It is intended in the first place to readers that never had a contact with formal groups. In the second chapter, the technical rudiments of the functorial language are presented. The reader can skip it in a first reading, and look up the relevant definitions when the need appears. This is especially true if he or she is familiar with the contents of the work [20]. The core of the book is composed of Chapters III and IV, that contain all the basic results of Cartier theory. In Chapter V it is shown that formal groups over a base ring of characteristic p are classified up to isogeny by their V-divided Cartier module. In the last paragraph, we compute the universal deformation of a p-divisible formal group. Finally Chapter VI contains the classification of V-divided Cartier modules over an algebraically closed field of characteristic p.

Berlin, March 1984 Thomas Zink

Contents

Chapter I

Formal group laws

In the theory of formal groups, one can choose the point of view of formal power series or the point of view of bigebras and functors. In this book, we will choose the latter. It is closer in spirit to Grothendieck's methods of algebraic geometry. The purpose of the present chapter is to provide a glimpse into what is both the first and the older point of view. It is therefore independent from the rest of the text, up to a few details. 6

§ 1 Definition of formal group laws

In the sequel, we denote by K a commutative ring with unit. We let $K[[X_1, \dots, X_n]]$ denote the ring of power series in n indeterminates over K. We use the short notations $\underline{X} = (X_1, \dots, X_n)$ and $K[[\underline{X}]] = K[[X_1, \dots, X_n]]$.

1.1. Definition: A *formal group law of dimension n over K* is an n-tuple of power series $G = (G_1, \dots, G_n)$, $G_i \in K[[X_1, \dots, X_n, Y_1, \dots, Y_n]] = K[[\underline{X}, \underline{Y}]]$ such that

1) $G_i(\underline{X}, 0) = G_i(0, \underline{X}) = X_i$,

2) $G_i(G(\underline{X}, \underline{Y}), \underline{Z}) = G_i(\underline{X}, G(\underline{Y}, \underline{Z}))$.

A formal group law is called *commutative* when moreover

3) $G_i(\underline{X}, \underline{Y}) = G_i(\underline{Y}, \underline{X})$.

We call $K[[\underline{X}]]$ the *coordinate ring* of G.

1.2. Examples:

1) Let $\mathbb{G}_{\mathrm{a}}$ be the one-dimensional formal group law $\mathbb{G}_{\mathrm{a}}(X, Y) = X + Y$. We call $\mathbb{G}_{\mathrm{a}}$ simply the *additive group*. More generally, one can define the n-dimensional additive group:
$$\mathbb{G}_{\mathrm{a}}(\underline{X}, \underline{Y}) = (X_1 + Y_1, \dots, X_n + Y_n).$$

2) Let $\mathbb{G}_{\mathrm{m}}$ be the one-dimensional formal group law
$$\mathbb{G}_{\mathrm{m}}(X, Y) = X + Y + XY = (1 + X)(1 + Y) - 1.$$
We call $\mathbb{G}_{\mathrm{m}}$ the *multiplicative group*.

3) One obtains an example of a non-commutative formal group law by considering the formal analogue of the full linear group. Let $X_{i,j}$, $i,j = 1,\dots,n$ be indeterminates. We define a formal group law $G = (G_{i,j})$ of dimension n^2 by means of the matrix identity

$$1 + (G_{i,j}) = (1 + (X_{i,j}))(1 + (Y_{i,j})).$$

In this equality, the symbol 1 stands for the unit matrix.

4) Let D be a finite-dimensional algebra over K, that may not contain a unit element. We assume that D is free as a K-module. Let $e_1,\dots,e_n$ be a basis of this module. If we add formally a unit element, in $D \otimes_K K[[\underline{X},\underline{Y}]]$ we have an equality

$$\left(1 + \sum_{i=1}^{n} X_i e_i\right)\left(1 + \sum_{i=1}^{n} Y_i e_i\right) = 1 + \sum_{k=1}^{n}\left(X_k + Y_k + \sum_{i,j} c_{i,j}^k X_i Y_j\right) e_k.$$

Thereby appear some constants $c_{i,j}^k \in K$ that define the multiplicative structure of the K-algebra D. It follows that the power series $G_k(\underline{X},\underline{Y}) = X_k + Y_k + \sum_{i,j} c_{i,j}^k X_i Y_j$, $k = 1,\dots,n$ define a formal group law. We call this the *multiplicative formal group law* $\mathbb{G}_{\mathrm{m}}D$ *of* D.

1.3. Conventions on power series: Let $\underline{i} = (i_1,\dots,i_n) \in \mathbb{N}^n$ be a vector of natural integers (including 0). We set

$$\underline{X}^{\underline{i}} = X_1^{i_1} \dots X_n^{i_n}.$$

The *degree* of the monomial is $|i| = \sum_{k=1}^{n} i_k$. Any $f \in K[[\underline{X}]]$ can be written

$$f = \sum_{\underline{i} \in \mathbb{N}^n} a_{\underline{i}} \underline{X}^{\underline{i}}, \qquad a_{\underline{i}} \in K.$$

When $a_{\underline{i}} = 0$ for $|i| < r$, we shall write $f = 0 \mod \deg r$. From Axiom 1.1.1) follows that

$$G_i(\underline{X},\underline{Y}) = X_i + Y_i \mod \deg 2.$$

Let $(\underline{X})$ be the ideal of $K[[\underline{X}]]$ generated by $X_1,\dots,X_n$. Its powers $(\underline{X})^N$ define a topology on $K[[\underline{X}]]$ for which $K[[\underline{X}]]$ is complete and separated. The graded ring associated to the filtration $(\underline{X})^N$ on $K[[\underline{X}]]$ is the ring of polynomials

$$K[X_1,\dots,X_n] = K[\underline{X}] = \mathrm{gr}\ K[[\underline{X}]] = \bigoplus_N (\underline{X})^N/(\underline{X})^{N+1}.$$

This isomorphism identifies the set of homogeneous polynomials of degree N with

$$\mathrm{gr}^N\ K[[\underline{X}]] = (\underline{X})^N/(\underline{X})^{N+1}.$$

The K-algebra $K[[\underline{X}]]$ is endowed with an augmentation, that is to say a K-algebra homomorphism $\varepsilon : K[[\underline{X}]] \to K$. This maps any power series f to its constant term $f(0)$. A *homomorphism of augmented* K*-algebras* $\varphi : K[[\underline{Y}]] \to K[[\underline{X}]]$ is a homomorphism of K-algebras such that $\varepsilon(\varphi(f)) = \varepsilon(f)$ for all f. This is equivalent to the requirement that $\varphi((\underline{Y})) \subset (\underline{X})$. In this case, we speak simply of a *morphism*. It is obvious that the datum of a

morphism φ is equivalent to the datum of power series $\varphi(Y_i) = \varphi_i(X_1, \ldots, X_n)$, $i = 1, \ldots, m$ such that $\varphi_i(0) = 0$. Let $\varphi' : K[[\underline{Y}']] \to K[[\underline{X}']]$ be a second morphism. Then we define $\varphi \otimes \varphi' : K[[\underline{Y}, \underline{Y}']] \to K[[\underline{X}, \underline{X}']]$ by $\varphi \otimes \varphi'(Y_i) = \varphi(Y_i)$ and $\varphi \otimes \varphi'(Y_i') = \varphi'(Y_i')$.

1.4. Lemma: A morphism $\varphi : K[[Y_1, \ldots, Y_n]] \to K[[X_1, \ldots, X_n]]$ is an isomorphism if and only if the Jacobi matrix $(\partial\varphi_i/\partial X_j)(0) \in M_n(K)$ is invertible. 7/8

Proof: The morphism φ induces a homomorphism $\operatorname{gr}\varphi : K[Y_1, \ldots, Y_n] \to K[X_1, \ldots, X_n]$. It is well-known and easy (see [2] Chap. III § 8) that φ is an isomorphism if and only if $\operatorname{gr}\varphi$ is an isomorphism. From

$$\operatorname{gr}\varphi(Y_i) = \sum_{j=1}^{n} (\partial\varphi_i/\partial X_j)(0).X_j,$$

the claim follows.

1.5. Corollary: Let G be a formal group law. Then, there is a uniquely determined n-tuple of power series $\psi(\underline{X}) = (\psi_1(\underline{X}), \ldots, \psi_n(\underline{X}))$ with

$$G_i(\underline{X}, \psi(\underline{X})) = 0, \qquad i = 1, \ldots, n. \tag{1.5.1}$$

Proof: Let $\alpha : K[[\underline{X}, \underline{Y}]] \to K[[\underline{X}, \underline{Y}]]$ be the morphism defined by $\alpha(X_i) = X_i$ and $\alpha(Y_i) = G_i(\underline{X}, \underline{Y})$. From 1.4, we get that α is an isomorphism. The inverse mapping has the form $X_i \mapsto X_i$ and $Y_i \mapsto \varphi(\underline{X}, \underline{Y})$. Let us write $\varphi(\underline{X}, \underline{Y}) = (\varphi_1(\underline{X}, \underline{Y}), \ldots, \varphi_n(\underline{X}, \underline{Y}))$. Then, we have

$$G_i(\underline{X}, \varphi(\underline{X}, \underline{Y})) = Y_i,$$

and this equality together with $\varphi(0) = 0$ determines φ uniquely. It is visible that $\psi(\underline{X}) = \varphi(\underline{X}, 0)$ is the sought-for n-tuple of power series. It is unique, because for any solution ψ' to (1.5.1) we have

$$G_i(\underline{X}, G(\psi'(\underline{X}), \underline{Y})) = G_i(G(\underline{X}, \psi'(\underline{X})), \underline{Y}) = G_i(0, \underline{Y}) = Y_i$$

and from the uniqueness of φ follows that $\varphi(\underline{X}, \underline{Y}) = G(\psi'(\underline{X}), Y)$. Thus we find that $\psi' = \psi$.

1.6. Remark: Let $\mathscr{N}$ be a *nilpotent* commutative K-algebra, which means that there exists a natural number $r \in \mathbb{N}$ such that any product of r elements of $\mathscr{N}$ equals 0, that is $\mathscr{N}^r = 0$. Let $\mathscr{N}^{(n)}$ be the direct sum of n copies of $\mathscr{N}$. When $\underline{a} = (a_1, \ldots, a_n) \in \mathscr{N}^{(n)}$ is a vector and $f \in K[[\underline{X}]]$ is a power series, the element $f(\underline{a}) \in \mathscr{N}$ has an obvious meaning. Let G be a formal group law. We define an operation on $\mathscr{N}^{(n)}$ by

$$\underline{a} +_G \underline{b} = G(\underline{a}, \underline{b}).$$

Axioms 1.1 and Corollary 1.5 imply that $+_G$ defines a group structure on $\mathscr{N}^{(n)}$.

Let G be a formal group law. The datum of the power series $(G_1, \ldots, G_n)$ is equivalent to that of a morphism

$$\mu : K[[X_1, \ldots, X_n]] \longrightarrow K[[X_1, \ldots, X_n, Y_1, \ldots, Y_n]]. \tag{1.7}$$

We can express the axioms in 1.1 concerning series in the form of commutative diagrams:

8
9

(1.7.1)
$$\begin{array}{ccccc} & & & & K[[\underline{X}]] \\ & \overset{\mathrm{id}}{\nearrow} & & & \uparrow{\scriptstyle 1\otimes\epsilon} \\ K[[\underline{X}]] & & \longrightarrow & & K[[\underline{X},\underline{Y}]] \\ & \underset{\mathrm{id}}{\searrow} & & & \downarrow{\scriptstyle \epsilon\otimes 1} \\ & & & & K[[\underline{X}]] \end{array}$$

(1.7.2)
$$\begin{array}{ccc} K[[\underline{X}]] & \xrightarrow{\mu} & K[[\underline{X},\underline{Y}]] \\ \downarrow{\scriptstyle \mu} & & \downarrow{\scriptstyle \mu\otimes 1} \\ K[[\underline{X},\underline{Y}]] & \xrightarrow{1\otimes\mu} & K[[\underline{X},\underline{Y},\underline{Z}]] \end{array}$$

(1.7.3)
$$\begin{array}{ccc} K[[\underline{X}]] & \xrightarrow{\mu} & K[[\underline{X},\underline{Y}]] \\ & \underset{\mu}{\searrow} & \downarrow{\scriptstyle c} \\ & & K[[\underline{X},\underline{Y}]] \end{array}$$

Here c is the morphism exchanging $\underline{X}$ and $\underline{Y}$.

1.8. Definition: Let G and H be formal group laws of respective dimensions n and m. A *morphism* $\varphi : G \to H$ is a vector of power series

$$\varphi(\underline{X}) = (\varphi_1(X_1,\ldots,X_n),\ldots,\varphi_m(X_1,\ldots,X_n))$$

such that $\varphi(0) = 0$ and

(1.8.1)
$$\varphi(G(\underline{X},\underline{X}')) = H(\varphi(\underline{X}),\varphi(\underline{X}')).$$

The power series $\varphi_1,\ldots,\varphi_n$ define a morphism

$$\begin{aligned} \varphi^* : K[[Y_1,\ldots,Y_m]] &\longrightarrow K[[X_1,\ldots,X_n]] \\ Y_i &\longmapsto \varphi_i. \end{aligned}$$

We call this the *comorphism* of φ. The relation (1.8.1) may again be expressed in terms of a commutative diagram:

(1.8.2)
$$\begin{array}{ccc} K[[\underline{Y}]] & \xrightarrow{\varphi^*} & K[[\underline{X}]] \\ \downarrow{\scriptstyle \nu} & & \downarrow{\scriptstyle \mu} \\ K[[\underline{Y},\underline{Y}']] & \xrightarrow{\varphi^*\otimes\varphi^*} & K[[\underline{X},\underline{X}']] \end{array}$$

Here the morphisms ν and μ correspond to the formal group laws G and H in the sense of (1.7).

1.9. Example: The most popular example of an isomorphism of formal group laws over a $\mathbb{Q}$-algebra K (i.e. $\mathbb{Q} \subset K$) is

$$u : \mathbb{G}_{\mathrm{a}} \longrightarrow \mathbb{G}_{\mathrm{m}}, \qquad u(X) = \sum_{n \geqslant 1} X^n/n! = \exp X - 1.$$

Let $D_1 \to D_2$ be a homomorphism of K-algebras that are free as K-modules. Let $e_1, \ldots, e_n$ and $f_1, \ldots, f_m$ be K-bases for D_1 and D_2. Let $\sum_j a_{i,j} f_j$ be the image of e_i. Then, the m-tuple of power series $\varphi_j = \sum_{i=1}^{n} a_{i,j} X_i$ defines a morphism of formal group laws $\mathbb{G}_{\mathrm{m}} D_1 \to \mathbb{G}_{\mathrm{m}} D_2$.

1.10. Let $\psi : H \to F$ be a morphism of formal group laws. We define the composition with φ: 9 10

$$\psi \circ \varphi(\underline{X}) = \psi(\varphi(\underline{X})).$$

For the comorphisms, we have $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.

Let G and H be formal group laws of dimensions n and m as above. The direct product of G and H is a formal group law of dimension $n + m$:

$$(G \times H)(\underline{X}, \underline{Y}, \underline{X}', \underline{Y}') = (G(\underline{X}, \underline{X}'), H(\underline{Y}, \underline{Y}')).$$

According to (1.7), it corresponds to the morphism $\mu \otimes \nu : K[[\underline{X}, \underline{Y}]] \to K[[\underline{X}, \underline{Y}, \underline{X}', \underline{Y}']]$. The *diagonal* $G \to G \times G$ is defined by the power series $(X_1, \ldots, X_n, X_1, \ldots, X_n)$. It is a morphism. When G is commutative, it is an easy exercise to see that $G(\underline{X}, \underline{Y})$ defines a morphism $G \times G \to G$ and ψ from 1.5 defines a morphism $G \to G$. If $\alpha : G \to G'$ and $\beta : H \to H'$ are two morphisms, then one defines in an obvious fashion the morphism $\alpha \times \beta : G \times H \to G' \times H'$. Its comorphism is $\alpha^* \otimes \beta^*$.

1.11. Base change: Let K' be a K-algebra, also assumed to be commutative and having a unit element. Let G be a formal group law over K. The images of the G_i under the mapping $K[[\underline{X}, \underline{Y}]] \to K'[[\underline{X}, \underline{Y}]]$ are denoted $G_{K',i}$. It is clear that $G_{K'} = (G_{K',1}, \ldots, G_{K',n})$ is a formal group law over K'. We say that $G_{K'}$ is obtained by base change from G. It is visible that the mapping $G \mapsto G_{K'}$ is a functor. By base change from $\mathbb{G}_{\mathrm{a}}$ and $\mathbb{G}_{\mathrm{m}}$, one obtains again $\mathbb{G}_{\mathrm{a}}$ and $\mathbb{G}_{\mathrm{m}}$ but as formal group laws over K'. If we want to emphasize that we are considering $\mathbb{G}_{\mathrm{a}}$ and $\mathbb{G}_{\mathrm{m}}$ over K, then we shall write $\mathbb{G}_{a,K}$ and $\mathbb{G}_{\mathrm{m},K}$. One sees easily, with the notations of 1.2.4), that we have $(\mathbb{G}_{\mathrm{m}} D)_{K'} = \mathbb{G}_{\mathrm{m}}(D \otimes_K K')$.

§ 2 Derivations

1.12. Definition: A *K-derivation* $D : K[[\underline{X}]] \to K[[\underline{X}]]$ is a K-linear mapping such that

$$D(fg) = fDg + gDf, \quad \text{for } f, g \in K[[\underline{X}]]. \tag{1.12.1}$$

Obviously $D(\underline{X})^N \subset (\underline{X})^{N-1}$ holds. Therefore D is continuous in the topology of $K[[\underline{X}]]$. From 1.12.1 and continuity it follows that

(1.13) $$Df = \sum_i (\partial f/\partial X_i) DX_i.$$

The derivations form a $K[[\underline{X}]]$-module. Equality (1.13) means that it is free and that the partial derivatives $f \mapsto (\partial f/\partial X_i)$ constitute a basis.

Let G be a formal group law and $\mu : K[[\underline{Z}]] \to K[[\underline{X}, \underline{Y}]]$ the comorphism attached to it by (1.7).

10 11 **1.14. Definition:** A derivation D is called *invariant* when the following diagram is commutative:

$$\begin{array}{ccc} K[[\underline{Z}]] & \xrightarrow{D} & K[[\underline{Z}]] \\ {\scriptstyle\mu}\downarrow & & \downarrow{\scriptstyle\mu} \\ K[[\underline{X}, \underline{Y}]] & \xrightarrow{1\otimes D} & K[[\underline{X}, \underline{Y}]]. \end{array}$$

According to (1.13), the derivation D may be written in the form $D = \sum_i u_i(\underline{Z})(\partial/\partial X_i)$. The commutativity of the diagram in 1.14 for the function Z_i means, when written in full:

(1.14.1) $$\sum_j u_j(\underline{Y})(\partial G_i/\partial Y_j) = u_i(G(\underline{X}, \underline{Y})).$$

The invariant derivations form a K-module.

1.15. Theorem: The mapping $D \mapsto (u_1(0), \ldots, u_n(0))$ is an isomorphism of the K-module of invariant derivations with K^n.

Proof: First, the mapping is injective, since from $u_i(0) = 0$ and (1.14.1) it follows that $u_i(G(\underline{X}, 0)) = u_i(\underline{X}) = 0$. One finds solutions to (1.14.1) by differentiating the associativity law

$$G_i(G(\underline{X}, \underline{Y}), \underline{Z})) = G_i(\underline{X}, G(\underline{Y}, \underline{Z})).$$

If $D_{2,k}$ denotes the partial derivative with respect to the k-th indeterminate from the second series of variables, we have

$$\frac{\partial G_i}{\partial Z_j}(G(\underline{X}, \underline{Y}), \underline{Z}) = \sum_k D_{2,k} G_i \, \frac{\partial G_k}{\partial Z_j}(\underline{Y}, \underline{Z}).$$

Setting $\underline{Z} = 0$ in this equality, one finds, with $u_{i,j}(\underline{Y}) = (\partial G_i/\partial Z_j)(\underline{Y}, \underline{Z})_{\underline{Y}=0}$:

(1.15.1) $$u_{i,j}(G(\underline{X}, \underline{Y})) = \sum_k \frac{\partial G_i}{\partial Y_k} u_{k,j}(\underline{Y}).$$

For fixed j, we have found a solution to the system of equations (1.14.1). The surjectivity of the mapping follows, since from 1.1.1) we have

$$u_{i,j}(0) = (\partial G_i/\partial Z_j)_{\underline{Y}=\underline{Z}=0} = \delta_{i,j}.$$

1.16. Remark: Let $(J_{i,k}) = J$ be the matrix $(\partial G_i/\partial Y_k)$. Then with obvious notations, one can write Equality (1.15.1) in matrix form:

(1.16.1) $$U(G) = JU(\underline{Y}).$$

The matrix $U(\underline{Y})$ is invertible since $\det U(0) = 1$. Indeed, we have $\det U(\underline{Y}) = 1 - f(\underline{Y})$, $f(0) = 0$ and $(\det U(\underline{Y}))^{-1} = \sum_i f(\underline{Y})^i$. One can deduce from this an expression for the partial derivatives $(\partial/\partial X_i)$ in terms of the invariant derivations $D_j = \sum_k u_{k,j}(\partial/\partial X_k)$. Thus the D_j, $j = 1, \ldots, n$, form a basis of the free $K[[\underline{X}]]$-module of derivations $\mathrm{Der}\, K[[\underline{X}]]$.

§ 3 The module of differential forms

11
12

1.17. Definition: Let $\Omega^1_{K[[\underline{X}]]}$ be the free $K[[\underline{X}]]$-module with basis $dX_1, \ldots, dX_n$. Its elements are called *differential forms*.

One has a K-linear map $d : K[[\underline{X}]] \to \Omega^1_{K[[\underline{X}]]}$, $df = \sum (\partial f/\partial X_i) dX_i$, $f \in K[[\underline{X}]]$. It satisfies:

$$d(fg) = gdf + fdg.$$

Let $\alpha : K[[\underline{X}]] \to K[[\underline{Z}]]$ be a morphism and $\alpha(X_i) = p_i(Z_1, \ldots, Z_m)$, $i = 1, \ldots, n$. Then α induces a mapping

$$\alpha_\bullet : \Omega^1_{K[[\underline{X}]]} \to \Omega^1_{K[[\underline{Z}]]}$$

$$\alpha_\bullet \left(\sum a_i(\underline{X}) dX_i\right) = \sum a_i(\underline{p}(\underline{Z})) dp_i(\underline{Z}).$$

It is characterized by the following properties:

$$\alpha_\bullet(f\omega) = \alpha(f)\alpha_\bullet(\omega), \qquad \alpha_\bullet(df) = d\alpha(f), \qquad f \in K[[\underline{X}]],\ \omega \in \Omega^1_{K[[\underline{X}]]}.$$

When α is the comorphism of a morphism of formal group laws $\varphi : G_1 \to G_2$, we write $\varphi^*\omega$ for $\alpha_\bullet\omega$.

Let G be a formal group law.

1.18. Definition: A differential form $\omega = \sum a_i(\underline{X}) dX_i \in \Omega^1_{K[[\underline{X}]]}$ is called *invariant with respect to* G when

$$\sum_i a_i(G(\underline{X}, \underline{Y})) \frac{\partial G_i}{\partial Y_j}(\underline{X}, \underline{Y}) = a_j(\underline{Y}). \tag{1.18.1}$$

Let $D = \sum u_i(\underline{X})(\partial/\partial X_i) \in \mathrm{Der}\, K[[\underline{X}]]$ be a derivation. Then one defines a bilinear form $(D, \omega) = \sum u_i a_i$:

$$(\ ,\ ) : \mathrm{Der}\, K[[\underline{X}]] \times \Omega^1_{K[[\underline{X}]]} \to K[[\underline{X}]].$$

It is characterized by the equality:

$$(D, gdf) = gDf, \qquad f, g \in K[[\underline{X}]].$$

1.19. Theorem: The mapping $\omega = \sum a_i dX_i \mapsto (a_1(0), \ldots, a_n(0))$ is an isomorphism of the K-module of invariant differential forms with K^n. When ω and D are invariant, then $(D, \omega) \in K$. One obtains in this way a perfect pairing between the K-module of invariant derivations and that of invariant differential forms. If ω is an arbitrary differential form such that $(D, \omega) \in K$ for all invariant derivations D, then ω is invariant.

Proof: Let $\underline{a}$ be the row vector of the a_i. Then the condition of invariance may be written, in matrix form:

$$\underline{a}(G)J = \underline{a}(\underline{Y}). \tag{1.19.1}$$

Since the matrix U is invertible, it follows from (1.16.1) that $U^{-1}(\underline{Y}) = U^{-1}(G)J$. Thus the row vectors of $U^{-1}(\underline{X}) = (a_{i,j})$ are solutions of (1.18.1). We obtain invariant differential forms $\omega_i = \sum_j a_{i,j}dX_j$. If $D_k = \sum_j u_{j,k}(\partial/\partial X_j)$ denotes the basis of the module of invariant derivations constructed before, it follows that

$$(D_k, \omega_i) = \delta_{k,i}.$$

12/13 Since by 1.16 the D_k generate the $K[[\underline{X}]]$-module $\mathrm{Der}\, K[[\underline{X}]]$, a differential form ω vanishes if and only if $(D_k, \omega) = 0$ for $k = 1, \ldots, n$. Let ω be an arbitrary differential form, so that $(D_i, \omega) = c_i \in K$ for $i = 1, \ldots, n$. Then the following holds:

$$(D_j, \omega) = (D_j, \sum c_i\omega_i).$$

Consequently $\omega = \sum c_i\omega_i$ is invariant. Q.E.D.

1.20. Exercise: Let G be a commutative formal group law and μ the morphism associated to it as in (1.7). Consider moreover the morphisms $p_1, p_2 : K[[\underline{Z}]] \to K[[\underline{X}, \underline{Y}]]$, $p_1(Z_i) = X_i$ and $p_2(Z_i) = Y_i$. Show that a differential form ω is invariant if and only if

$$\mu_\bullet\omega = p_{1\bullet}\omega + p_{2\bullet}\omega. \tag{1.20.1}$$

§ 4 Tangent space and curves

1.21. Definition: A *curve* is an n-tuple of power series $\gamma(T) = (\gamma_1(T), \ldots, \gamma_n(T))$, $\gamma_i(T) \in K[[T]]$, $\gamma_i(0) = 0$.

One can conceive a curve as a homomorphism $K[[\underline{X}]] \to K[[T]]$ such that $X_i \mapsto \gamma_i(T)$.

1.22. Definition: The *tangent space of* $K[[\underline{X}]]$ is the K-module

$$\mathrm{Hom}_K((\underline{X})/(\underline{X})^2, K).$$

If G is a formal group law with coordinate ring $K[[\underline{X}]]$, we also call it the *tangent space of* G and denote it by t_G or $\mathrm{Lie}\, G$.

The tangent space has several interpretations. First, to each tangent vector

$$t \in \mathrm{Hom}_K((\underline{X})/(\underline{X})^2, K)$$

corresponds a homomorphism $K[[\underline{X}]] \to K[[T]]/(T)^2$. Conversely, any such homomorphism defines a tangent vector.

Any derivation D defines a homomorphism $K[[\underline{X}]] \to K[[T]]/(T)^2$, $f \mapsto f(0) + Df(0)\cdot T$ and hence a tangent vector. According to 1.15, this mapping defines an isomorphism of the K-module of invariant derivations with the tangent space.

The *tangent vector to a curve* $\gamma : K[[\underline{X}]] \to K[[T]]$ can be defined like this:

$$K[[\underline{X}]] \xrightarrow{\gamma} k[[T]] \longrightarrow K[[T]]/(T)^2.$$

A morphism $\alpha : K[[\underline{X}]] \to K[[\underline{Y}]]$ induces a mapping of tangent spaces

$$\alpha^\bullet : \mathrm{Hom}_K((\underline{Y})/(\underline{Y})^2) \to \mathrm{Hom}_K((\underline{X})/(\underline{X})^2, K).$$

When $\alpha(X_i) = p_i(\underline{Y})$, one can represent $\alpha^\bullet$ by the matrix $(\partial p_i/\partial Y_j)|_{\underline{Y}=0}$. By 1.4, α is an isomorphism if $\alpha^\bullet$ is so. If $\gamma : K[[\underline{Y}]] \to K[[T]]$ is a curve and t is the tangent vector to this curve, then $\alpha^\bullet t$ is the tangent vector to the curve $\alpha^\bullet\gamma = (p_i(\gamma(T)))$. Let α be the comorphism of a morphism of formal group laws φ. Then we denote $\alpha^\bullet$ also by the symbol $\mathrm{Lie}\,\varphi$.

1.23. Theorem: Let K be a $\mathbb{Q}$-algebra. Then for any derivation $D : K[[\underline{X}]] \to K[[\underline{X}]]$, there exists a unique curve $\gamma(T)$ such that for all $f \in K[[\underline{X}]]$ we have 13 14

$$\frac{\partial f(\gamma(T))}{\partial T} = Df(\gamma(T)).$$

The curve γ is called the *integral curve* of D.

Proof: It is clear that it suffices to check the required equality for the functions $f = X_i$. Let $DX_i = u_i(\underline{X})$. We obtain the following system of differential equalities.

$$\frac{\partial \gamma_i(T)}{\partial T} = u_i(\gamma(T)), \quad i = 1, \dots, n. \tag{1.24}$$

It is enough to prove the following.

1.25. Lemma: Let K be a $\mathbb{Q}$-algebra. Let $u_1, \dots, u_n \in K[[\underline{X}]]$ be power series and $a_1, \dots, a_n \in K$. Then there exist unique power series $\gamma_1(Y =, \dots, \gamma_n(T) \in K[[T]]$ such that $\gamma_i(0) = a_i$ and the equalities (1.14) are satisfied.

Proof: We show by induction on r that there exist unique polynomials $\gamma_i^{(r)}(T)$ of degree r such that $\gamma_i^{(r)}(0) = a_i$ and

$$\frac{\partial \gamma_i^{(r)}(T)}{\partial T} = u_i(\gamma_1^{(r)}(T), \dots, \gamma_n^{(r)}(T)) \mod T^r.$$

For $r = 0$, the statement is trivial. Let us write $\gamma_i^{(r+1)}(T) = \gamma_i^{(r)}(T) + c_i T^{r+1}$. Since $u_i(\gamma^{(r+1)}) = u_i(\gamma^{(r)}) \mod T^{r+1}$, we can find c_i from the equality

$$(r+1)c_i T^r = -\frac{\partial \gamma_i^{(r)}}{\partial T} + u_i(\gamma^{(r)}) \mod T^{r+1}.$$

§ 5 The $\mathbb{Q}$-theorem

1.26. Theorem: Let G be a formal group law over a $\mathbb{Q}$-algebra K. Let D be an invariant derivation. Then, the integral curve $\gamma(T)$ of D defines a morphism

$$\mathbb{G}_{\mathrm{a}} \longrightarrow G.$$

Conversely, for any homomorphism $\gamma : \mathbb{G}_{\mathrm{a}} \to G$ there exists a unique invariant derivation D for which the integral curve is γ.

Proof: The curve γ defines a morphism if and only if the following equality is fulfilled:

$$\gamma(T+S) = G(\gamma(T), \gamma(S)). \tag{1.26.1}$$

We consider, over the ring $K[[T]]$, the system of differential equations:

14 15
$$\frac{\partial \alpha_i(S)}{\partial S} = u_i(\alpha(S)). \tag{1.26.2}$$

Here, we let $u_i = DX_i$ and $\alpha(0) = (\alpha_1(0), \ldots, \alpha_n(0)) = \gamma(T)$. By the unicity statement in 1.25, it is enough to show that both sides of (1.26.1) are solutions of the system (1.26.2). For $\alpha(S) = \gamma(T+S)$ this is clear. On the other side, we find:

$$\frac{\partial G_i(\gamma(T), \gamma(S))}{\partial S} = \sum u_j(\gamma(S)) D_{2,j} G_i(\gamma(T), \gamma(S)) = u_i(G(\gamma(T), \gamma(S))).$$

The first equality holds because γ is an integral curve and the second holds by (1.14.1).

Conversely, any curve γ defines a derivation D:

$$Df = \frac{\partial f(G(\underline{X}, \gamma(T)))}{\partial T}|_{T=0}.$$

From the law of associativity follows that D is invariant:

$$(1 \otimes D)\mu f = \frac{\partial f(G(\underline{X}, G(\underline{Y}, \gamma(T))))}{\partial T}|_{T=0} = \frac{\partial f(G(G(\underline{X}, \underline{Y}), \gamma(T)))}{\partial T}|_{T=0} = \mu D f.$$

If γ defines a morphism, then γ is an integral curve of D:

$$\frac{\partial f(\gamma(T))}{\partial T} = \frac{\partial f(\gamma(T+S))}{\partial S}|_{S=0} = \frac{\partial f(G(\gamma(T), \gamma(S)))}{\partial S}|_{S=0} = Df(\gamma(T)).$$

This proves the theorem.

1.27. $\mathbb{Q}$-Theorem: Every commutative formal group law G over a $\mathbb{Q}$-algebra is isomorphic to $\mathbb{G}_{\mathrm{a}}^n$.

Proof: Let $D_1, \ldots, D_n$ be a basis of the K-module of invariant derivations of G. Let $\gamma_1, \ldots, \gamma_n$ be the integral curves of these derivations. Since G is commutative, we obtain a homomorphism

$$\sum_{i=1}^{n} \gamma_i : \mathbb{G}_{\mathrm{a}}^n \longrightarrow G.$$

It induces an isomorphism on the tangent spaces.

For invariant differential forms, we have a fact which is dual to 1.26.

1.28. Theorem: Let ω be an invariant differential form for a commutative formal group law G over a $\mathbb{Q}$-algebra K. Then, there exists a unique morphism $\psi : G \to \mathbb{G}_{\mathrm{a}}$ such that $\omega = \psi^* dT$, where $K[[T]]$ stands for the coordinate ring of $\mathbb{G}_{\mathrm{a}}$.

Proof: Let $f \in K[[\underline{X}]]$ be a power series defining the morphism ψ. Then, we have:

$$f(G(\underline{X}, \underline{Y})) = f(\underline{X}) + f(\underline{Y}), \quad f(0) = 0. \tag{1.28.1}$$

15 16

The equality $\omega = \psi^* dT$ means that $\omega = df$.

Assuming that an f exists such that $\omega = df$ and $f(0) = 0$, from the invariance of ω it follows using 1.20 that

$$df(G(\underline{X}, \underline{Y})) = df(\underline{X}) + df(\underline{Y}). \tag{1.28.2}$$

One verifies easily that over a $\mathbb{Q}$-algebra K, a power series does not depend on X_i when the partial derivative with respect to X_i vanishes. This implies that the second of the above equalities implies the first.

In order to see that the equation $\omega = df$ has a solution, one can restrict oneself to the case $G = \mathbb{G}_{\mathrm{a}}^n$. Then any invariant differential has the form $\sum a_i dX_i$ where $a_i \in K$. The claim follows.

§ 6 Differential operators

Let $\underline{X} = (X_1, \ldots, X_n)$ and $\underline{Z} = (Z_1, \ldots, Z_n)$. We consider a continuous K-linear mapping $D : K[[\underline{X}]] \to K[[\underline{X}]]$. A power series $f \in K[[\underline{X}, \underline{Z}]]$ may be written uniquely in the form $\sum p_{\underline{i}}(\underline{X})\underline{Z}^{\underline{i}}$ where $p_{\underline{i}}(\underline{X}) \in K[[\underline{X}]]$. We define a K-linear mapping

$$\begin{aligned} L_D : \quad & K[[\underline{X}, \underline{Z}]] \longrightarrow K[[\underline{X}]] \\ & \textstyle\sum p_{\underline{i}}(\underline{X})\underline{Z}^{\underline{i}} \longmapsto \sum p_{\underline{i}}(\underline{X}) D\underline{X}^{\underline{i}}. \end{aligned} \tag{1.29}$$

The last sum makes sense since D is continuous. Obviously L_D is continuous and K-linear.

Let $J \subset K[[\underline{X}, \underline{Z}]]$ be the ideal generated by the $X_i - Z_i$.

1.30. Definition: A K-linear continuous mapping $D : K[[\underline{X}]] \to K[[\underline{X}]]$ is called a *differential operator of order N* when $L_D(J^{N+1}) = 0$.

1.31. Remark: A differential operator of order 0 is K-linear. Indeed,

$$D(f(\underline{X})g(\underline{X})) = L_D(f(\underline{Z})g(\underline{Z})) = L_D(f(\underline{X})g(\underline{Z})) = f(\underline{X})Dg(\underline{X}).$$

The middle equality holds since $f(\underline{Z}) - f(\underline{X}) \in J$ and $L_D(J) = 0$. In particular, $Df(\underline{X}) = f(\underline{X}) \cdot D1$ holds. The differential operator D is therefore the multiplication by the function

$D1$. We will occasionnally consider a power series $h \in K[[\underline{X}]]$ as a differential operator of order 0. The reader can check similarly that a differential operator D of order 1 with $D1 = 0$ is a derivation.

The differential operator form a $K[[\underline{X}]]$-module. When we consider a power series f as a differential operator of order 0, we can look at the composition of functions $D \circ f$. We have $(D \circ f)g = D(fg)$, and it follows that $D \circ f$ is a differential operator of the same order as D. Of course, $D \circ f$ and Df have nothing to see with each other, whereas $f \circ D = fD$.

16 17 **1.32. Lemma:** A continuous K-linear mapping $D : K[[\underline{X}]] \to K[[\underline{X}]]$ is a differential operator of order N if and only if for all $f \in K[[\underline{X}]]$, the mapping $f \circ D - D \circ f$ is a differential operator of order $N - 1$.

Proof: Let D be a differential operator of order N. Since $f(\underline{X}) - f(\underline{Z}) \in J$, for all $g(\underline{X}, \underline{Z}) \in J^N$ we have $L_D((f(\underline{X}) - f(\underline{Z}))g(\underline{X}, \underline{Z})) = 0$. This equality is equivalent to

$$L_{f \circ D - D \circ f} g = 0.$$

Conversely, when $f \circ D - D \circ f$ is a differential operator of order $N - 1$ then $L_D((f(\underline{X}) - f(\underline{Z}))g) = 0$ for all $g \in J^N$. Therefore $L_D(J^{N+1}) = 0$.

1.33. Theorem: Let D_1 and D_2 be differential operators of order N_1 and N_2. Then $D_1 \circ D_2$ is a differential operator of order $N_1 + N_2$ and $[D_1, D_2] = D_1 \circ D_2 - D_2 \circ D_1$ is a differential operator of order $N_1 + N_2 - 1$.

Proof: We lead the proof by induction on $N_1 + N_2$. When D_1 or D_2 has order 0, the claim follows from 1.31 and 1.32. Then one obtains the induction step using 1.32 and the following equalities.

$$f\, D_1 \circ D_2 - D_1 \circ D_2 \circ f = (f \circ D_1 - D_1 \circ f) \circ D_2 + D_1 \circ (f \circ D_2 - D_2 \circ f),$$

$$f \circ [D_1, D_2] - [D_1, D_2] \circ f = [f, [D_1, D_2]] = [[D_2, f], D_1] + [[f, D_1], D_2].$$

The last equality is a consequence of the following fact. Let R be a ring (that is associative but not necessarily commutative or with unit element). For $x, y \in R$ let $[x, y] = xy - yx$. Then the *Jacobi identity* holds:

$$[[x, y], z] + [[y, z], x] + [[z, x], y] = 0. \tag{1.34}$$

Let DO be the $K[[\underline{X}]]$-module of all differential operators. According to the last theorem, this is a ring. Let $\mathrm{DO}_N \subset \mathrm{DO}$ be the submodule of differential operators of order N, where $\mathrm{DO}_N = 0$ for $N < 0$. The composition of differential operators defines a map

$$\mathrm{DO}_N \,/\, \mathrm{DO}_{N-1} \times \mathrm{DO}_M \,/\, \mathrm{DO}_{M-1} \longrightarrow \mathrm{DO}_{N+M} \,/\, \mathrm{DO}_{N+M-1}\,.$$

We obtain a graded ring $\mathrm{gr}\,\mathrm{DO} = \bigoplus_N \mathrm{DO}_N \,/\, \mathrm{DO}_{N-1}$. By 1.33, this ring is commutative.

1.35. Theorem: Let $g \in K[[\underline{X}]]$. Then, we have a representation

$$g(\underline{X} + \underline{Y}) = \sum D_{\underline{i}} g(\underline{X}) \underline{Y}^{\underline{i}}. \tag{1.35.1}$$

The mapping $g \mapsto D_{\underline{i}}g$ is a differential operator of order $|\underline{i}| = i_1 + \cdots + i_n$. The $K[[\underline{X}]]$-module DO_N is free with basis $D_{\underline{i}}$, $|\underline{i}| \leqslant N$.

Proof: The map $g \mapsto D_{\underline{i}}g$ is K-linear and continuous. We have: $g(\underline{Z}) = g(\underline{X} + (\underline{Z} - \underline{X})) = \sum D_{\underline{i}}g(\underline{X})(\underline{Z} - \underline{X})^{\underline{i}}$. A differential operator of order N is given by means of a $K[[\underline{X}]]$-linear mapping $L : K[[\underline{X}, \underline{Z}]] \to K[[\underline{X}]]$ such that $L(\underline{Z} - \underline{X})^{\underline{i}} = 0$ for $|\underline{i}| > N$. Since any element $f \in K[[\underline{X}, \underline{Z}]]$ may be represented uniquely in the form 17 18

$$f(\underline{X}, \underline{Z}) = \sum f_{\underline{i}}(\underline{X})(\underline{Z} - \underline{X})^{\underline{i}},$$

the datum of L is equivalent to the datum of $L(\underline{Z} - \underline{X})^{\underline{i}} = a_{\underline{i}}(\underline{X})$. Then it is clear that

$$L(g(\underline{Z})) = \sum a_{\underline{i}}(\underline{X}) D_{\underline{i}}g(\underline{X}).$$

The claim follows.

1.36. Corollary: Let $\partial_{\underline{i}}$ be the differential operator $\partial^{i_1} \dots \partial^{i_n}$. If K is a $\mathbb{Q}$-algebra, every differential operator of order N has a unique representation

$$D = \sum_{|\underline{i}| \leqslant N} a_{\underline{i}}(\underline{X}) \partial_{\underline{i}}.$$

Proof: Indeed, by partial differentiation from (1.35.1) one obtains the Taylor formula

$$i!\, D_{\underline{i}}g = \partial_{\underline{i}}g. \qquad \text{Q.E.D.}$$

1.37. Definition: Let G be a formal group law and $K[[\underline{X}]]$ the coordinate ring of G. A differential operator $D : K[[\underline{X}]] \to K[[\underline{X}]]$ is called *invariant* when the following diagram is commutative (compare with 1.14):

$$\begin{array}{ccc} K[[\underline{X}]] & \xrightarrow{D} & K[[\underline{X}]] \\ {\scriptstyle \mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ K[[\underline{X}, \underline{Y}]] & \xrightarrow{1 \otimes D} & K[[\underline{X}, \underline{Y}]] \end{array}$$

For a derivation, this is just the old definition.

1.38. Theorem: Let $l : K[[\underline{X}]] \to K$ be a K-linear map such that $l((\underline{X})^{N+1}) = 0$. Then there exists a unique invariant differential operator of order N

$$D : K[[\underline{X}]] \longrightarrow K[[\underline{X}]]$$

such that $Df(0) = l(f)$.

Proof: For an invariant D with $Df(0) = l(f)$, we have

$$\begin{aligned} Df(\underline{X}) &= Df(G(\underline{X}, \underline{Y}))|_{\underline{Y}=0} = \mu Df(\underline{X}, \underline{Y})|_{\underline{Y}=0} \\ &= (1 \otimes D)\mu f(\underline{X}, \underline{Y})|_{\underline{Y}=0} = (1 \otimes l)(f(G(\underline{X}, \underline{Y}))). \end{aligned}$$

This proves uniqueness. If one takes the above equality as a definition, then D is continuous and K-linear. By definition, one has $L_D g(\underline{X},\underline{Z}) = (1\otimes l)(g(\underline{X},G(\underline{X},\underline{Y})))$. From $X_i - G_i(\underline{X},\underline{Y}) \in (\underline{Y})K[[\underline{X},\underline{Y}]]$ it follows that $g(\underline{X},G(\underline{X},\underline{Y})) \in (\underline{Y})^{N+1}$ for $g \in J^{N+1}$. From this, it is seen that D is a differential operator of order N. The invariance follows from:

$$\begin{aligned}\mu D f &= (1\otimes 1\otimes l)f(G(G(\underline{X},\underline{Y}),\underline{Z})) = (1\otimes 1\otimes l)f(G(\underline{X},G(\underline{Y},\underline{Z})))\\ &= (1\otimes D)f(G(\underline{X},\underline{Y})) = (1\otimes D)\mu f. \qquad \text{Q.E.D.}\end{aligned}$$

It is immediately clear that one obtains invariant differential operators $H_{\underline{i}}$ in the following way:

18 19 (1.39) $$f(G(\underline{X},\underline{Y})) = \sum H_{\underline{i}} f(\underline{X})\underline{Y}^{\underline{i}}.$$

1.40. Corollary: The invariant differential operators of order N form a free K-module with basis $H_{\underline{i}}$, $|\underline{i}| \leqslant N$.

Proof: An invariant differential operator can be written

$$(1\otimes l)f(G(\underline{X},\underline{Y})) = (1\otimes l)\big(\sum H_{\underline{i}} f\cdot \underline{Y}^{\underline{i}}\big) = \sum l(\underline{Y}^{\underline{i}})H_{\underline{i}} f. \qquad \text{Q.E.D.}$$

The K-algebra of invariant differential operators of the formal group law G will be denoted $\mathbb{H}_G$.

1.40.1. Lemma: Let D_i, $i = 1,2$ be invariant differential operators and $l_i(f) = D_i f(0)$. Then the following holds:

$$(D_1\circ D_2)f(0) = (l_1\otimes l_2)f(G(\underline{X},\underline{Y})).$$

Proof: We have:

$$\begin{aligned}D_1\circ D_2 f(\underline{Z}) &= D_1(1\otimes l_2)f(G(\underline{Z},\underline{Y}))\\ &= (1\otimes l_1\otimes 1)(1\otimes 1\otimes l_2)f(G(G(\underline{Z},\underline{X}),\underline{Y}))\\ &= (1\otimes l_1\otimes l_2)f(G(\underline{Z},G(\underline{X},\underline{Y}))).\end{aligned}$$

The claim follows by setting $\underline{Z} = 0$.

Let $\varphi : G \to G'$ be a morphism of formal group laws, and let $\varphi^* : K[[\underline{X}']] \to K[[\underline{X}]]$ be the comorphism. By mapping a linear form $l : K[[\underline{X}]] \to K$ to the linear form $l\circ\varphi^*$, we obtain a map $\varphi_* : \mathbb{H}_G \to \mathbb{H}_{G'}$.

1.41. Theorem: $\varphi_* : \mathbb{H}_G \to \mathbb{H}_{G'}$ is a homomorphism of K-algebras that maps differential operators of order N to differential operators of the same order.

Proof: We only have to show that φ_* respects the multiplication:

$$(\varphi_* D_1 \circ \varphi_* D_2) f = (\varphi_* l_1 \otimes \varphi_* l_2) f(G'(\underline{X}', \underline{Y}')) = (l_1 \otimes l_2) f(G'(\varphi(\underline{X}), \varphi(\underline{Y})))$$

$$= (l_1 \otimes l_2) f(\varphi(G(\underline{X}, \underline{Y}))) = \varphi_*(D_1 \circ D_2) f,$$

for all $f \in K[[\underline{X}']]$. Q.E.D.

1.42. Exercise: Let $H_{\underline{i}} \circ H_{\underline{j}} = \sum_{\underline{k}} a_{\underline{k},\underline{i},\underline{j}} H_{\underline{k}}$, $a_{\underline{k},\underline{i},\underline{j}} \in K$, where we use the notations of 1.40. Prove that $a_{\underline{k},\underline{i},\underline{j}}$ is the coefficient of $\underline{X}^{\underline{i}} \underline{Y}^{\underline{j}}$ in $G(\underline{X}, \underline{Y})^{\underline{k}}$. Describe the algebra $\mathbb{H}_{\mathbb{G}_{\mathrm{a}}^n}$ (the algebra of divided powers of the module K^n).

§ 7 The Lie algebra and its enveloping algebra

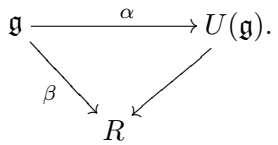
Let G be a formal group law. The K-module of invariant derivations $\operatorname{Lie} G$ is a submodule of $\mathbb{H}_G$. When $D_1, D_2 \in \operatorname{Lie} G$, it follows from 1.33 that $[D_1, D_2] \in \operatorname{Lie} G$. The bracket $[\ ,\ ]$ is K-bilinear on G, satisfies the Jacobi identity (1.34), and $[D, D] = 0$ holds. One makes the abstract definition:

1.43. Definition: A *Lie algebra* $\mathfrak{g}$ is a free K-module with a K-bilinear mapping $[\ ,\ ] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ such that $[x, x] = 0$, $x \in \mathfrak{g}$ and the Jacobi identity holds. A *morphism of Lie algebras* is a morphism $\varphi : \mathfrak{g} \to \mathfrak{g}'$ of K-modules such that $[\varphi(x), \varphi(y)] = \varphi[x, y]$, $x, y \in \mathfrak{g}$. 19 20

Let $\{x_i\}_{i \in I}$ be a basis of $\mathfrak{g}$. We denote by $T\mathfrak{g}$ the free associative K-algebra with generators x_i. Let $\mathfrak{a}$ be the two-sided ideal of $T\mathfrak{g}$ generated by the elements

$$[x_i, x_j] - x_i x_j + x_j x_i,$$

where the brackets are understood in $\mathfrak{g}$. One calls $U(\mathfrak{g}) = T\mathfrak{g}/\mathfrak{a}$ the *universal enveloping algebra of* $\mathfrak{g}$. There is a canonical mapping $\alpha : \mathfrak{g} \to U(\mathfrak{g})$, $x_i \mapsto x_i$, such that $\alpha([x, y]) = \alpha(x)\alpha(y) - \alpha(y)\alpha(x)$. It is easy to observe that $U(\mathfrak{g})$ is characterized by the following universal property. Let $\beta : \mathfrak{g} \to R$ be a map to an associative K-algebra with $\beta([x, y]) = \beta(x)\beta(y) - \beta(y)\beta(x)$. Then there exists a unique factorization



We remark that every morphism of formal group laws $\varphi : G \to G'$ induces a morphism of Lie algebras $\operatorname{Lie} \varphi : \operatorname{Lie} G \to \operatorname{Lie} G'$ and a morphism of their enveloping algebras. This follows from 1.41.

1.44. Exercise: Let G be a formal group law with coordinate ring $K[[\underline{X}]]$. We have an isomorphism $\operatorname{Lie} G = K^n$, $D \mapsto (DX_1(0), \ldots, DX_n(0))$ that induces a bracket on K^n. Let

$$G_i(\underline{X}, \underline{Y}) = X_i + Y_i + \sum_{k,l} c_i^{k,l} X_k Y_l \mod \deg 3.$$

Let $\underline{v}, \underline{w} \in K^n$ and $\underline{u} = [\underline{v}, \underline{w}]$. Show that

$$u_i = \sum_{k,l} c_i^{k,l}(v_k w_l - w_l v_k).$$

Let G be a formal group law and $D_1, \ldots, D_n$ a basis of the K-module $\mathrm{Lie}\, G$. By the universal property of $U(\mathrm{Lie}\, G)$, we find a K-algebra homomorphism

$$U(\mathrm{Lie}\, G) \longrightarrow \mathbb{H}_G. \tag{1.45}$$

We will show that over a $\mathbb{Q}$-algebra K, this is an isomorphism.

1.46. Theorem: Let K be a $\mathbb{Q}$-algebra. Let D be a differential operator of order N. Then D has a unique representation:

$$D = \sum_{|\underline{i}| \leqslant N} a_{\underline{i}}(\underline{X}) D_1^{i_1} \circ \cdots \circ D_n^{i_n}, \qquad a_{\underline{i}}(\underline{X}) \in K[[\underline{X}]].$$

Proof: We show by induction on N that the claimed representation exists. The $K[[\underline{X}]]$-algebra $\mathrm{gr}\,\mathrm{DO}$ is commutative and is generated by the derivations $(\partial/\partial X_i)$, by 1.36. Since these derivations are linear combinations of the D_i (by 1.16), then $D_1, \ldots, D_n$ form also a generating system. It follows that we have:

$$D = \sum_{|\underline{i}| = N} a_{\underline{i}}(\underline{X}) D_1^{i_1} \circ \cdots \circ D_n^{i_n} \mod \mathrm{DO}_{N-1}\,.$$

The existence of the representation follows by induction.

We can formulate what has been proven in the following way. Let L be the free $K[[\underline{X}]]$-module with basis $D_1^{i_1} \circ \cdots \circ D_n^{i_n}$, $|\underline{i}| \leqslant N$. Then the canonical mapping $L \to \mathrm{DO}_N$ is a surjection. Since both modules are free of the same rank (see 1.35), this is an isomorphism. Q.E.D.

1.47. Corollary: With the same assumptions, let D be an invariant differential operator. Then D has a unique representation

$$D = \sum_{|\underline{i}| \leqslant N} a_{\underline{i}}(\underline{X}) D_1^{i_1} \circ \cdots \circ D_n^{i_n}, \qquad a_{\underline{i}} \in K.$$

Proof: Let $D = \sum a_{\underline{i}}(\underline{X}) D_1^{i_1} \circ \cdots \circ D_n^{i_n}$ and $D' = \sum a_{\underline{i}}(0) D_1^{i_1} \circ \cdots \circ D_n^{i_n}$. These two operators are invariant, and $(D - D')f(0) = 0$, $f \in K[[\underline{X}]]$. It follows from 1.38 that $D = D'$.

1.48. Theorem: Let G be a formal group law over a $\mathbb{Q}$-algebra K. Then the canonical map $U(\mathrm{Lie}\, G) \to \mathbb{H}_G$ is an isomorphism.

Proof: It is obviously enough to prove that every element of $U(\mathrm{Lie}\, G)$ has a representation of the form $\sum a_{\underline{i}} D_1^{i_1} \circ \cdots \circ D_n^{i_n}$. Since $D_1, \ldots, D_n$ generate the K-algebra $U(\mathrm{Lie}\, G)$, it is enough

to prove this for elements of the form $D_{j_1} \circ \cdots \circ D_{j_r}$. Let r be minimal such that the desired representation does not exist. One has the relation:

$$\begin{aligned} &D_{j_1} \circ \cdots \circ D_{j_s} \circ D_{j_{s+1}} \circ \cdots \circ D_{j_r} \\ &\quad = D_{j_1} \circ \cdots \circ D_{j_{s+1}} \circ D_{j_s} \circ \cdots \circ D_{j_r} + D_{j_1} \circ \cdots \circ [D_{j_s}, D_{j_{s+1}}] \circ \cdots \circ D_{j_r}. \end{aligned}$$

Since in the right-hand side the second summand has the desired representation by the inductive hypothesis, the first summand cannot have it by assumption. From this follows that $D_{j_{\pi(1)}} \circ \cdots \circ D_{j_{\pi(s)}}$ does not possess the desired representation, for any permutation π. This is a contradiction.

1.49. Remark: Let $\mathfrak{g}$ be a Lie algebra over K with basis $x_1, \ldots, x_n$. The Poincaré-Birkhoff-Witt Theorem states that every element of $U(\mathfrak{g})$ has a unique representation $\sum a_{\underline{i}} x_1^{i_1} \ldots x_n^{i_n}$. We have proven this theorem for $U(\operatorname{Lie} G)$. For the general case, we refer to [22].

§ 8 The bigebra of a formal group law

21
22

By 1.38, we can write $\mathbb{H}_G = \operatorname{Hom}_{K,\mathrm{cont}}(K[[\underline{X}]], K)$, where K is seen with the discrete topology. Two continuous linear forms l_1 and l_2 of $K[[\underline{X}]]$ define a continuous linear form $l_1 \otimes l_2 : K[[\underline{X}, \underline{Y}]] \to K$. We obtain an isomorphism

$$\mathbb{H}_G \otimes_K \mathbb{H}_G = \operatorname{Hom}_{K,\mathrm{cont}}(K[[\underline{X}, \underline{Y}]], K).$$

The multiplication in $\mathbb{H}_G$ defines a map

$$\mu^* : \mathbb{H}_G \otimes_K \mathbb{H}_G \longrightarrow \mathbb{H}_G.$$

By 1.41, we obtain it by application of the functor $\operatorname{Hom}_{k,\mathrm{cont}}(-, K)$ to the map (1.7) $\mu : K[[\underline{X}]] \to K[[\underline{X}, \underline{Y}]]$. We say that μ^* is the *dual map* of μ.

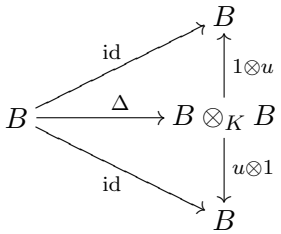
The multiplication $m : K[[\underline{X}, \underline{Y}]] \to K[[\underline{X}]]$, $m(f(\underline{X}, \underline{Y})) = f(\underline{X}, \underline{X})$ is the comorphism of the diagonal $G \to G \times G$, see 1.10. Since the diagonal is a morphism of formal group laws, m induces by dualization an algebra homomorphism

$$m : \mathbb{H}_G \longrightarrow \mathbb{H}_G \otimes_K \mathbb{H}_G.$$

The algebra homomorphism $e : K \to K[[\underline{X}]]$ induces by dualization the augmentation $e^* : \mathbb{H}_G \to K$, $l \mapsto l(0)$.

1.50. Definition: A *bigebra* B over K is a K-algebra B with a unit, an augmentation $u : B \to K$ and a K-algebra homomorphism $\Delta : B \to B \otimes_K B$, such that the following diagrams are commutative (compare with (1.7)):

(1.50.1)



(1.50.2)
$$\begin{array}{ccc} B & \xrightarrow{\Delta} & B \otimes_K B \\ {\scriptstyle\Delta}\downarrow & & \downarrow{\scriptstyle\Delta\otimes 1} \\ B \otimes_K B & \xrightarrow{1\otimes\Delta} & B \otimes_K B \otimes_K B \end{array}$$

A *morphism of bigebras* $\varphi : B \to B'$ is a K-algebra homomorphism such that the following diagrams are commutative:

$$\begin{array}{ccc} B & \xrightarrow{\varphi} & B' \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle u'} \\ K & = & K \end{array} \qquad\qquad \begin{array}{ccc} B & \xrightarrow{\varphi} & B' \\ {\scriptstyle\Delta}\downarrow & & \downarrow{\scriptstyle\Delta'} \\ B \otimes_K B & \xrightarrow{\varphi\otimes\varphi} & B' \otimes_K B'. \end{array}$$

When G is a formal group law, then $\mathbb{H}_G$ is a bigebra.

22
23 The bigebra structure is defined by $\Delta = m^*$ and $u = e^*$. One can obtain the last diagram for example by dualizing the associative law in $K[[\underline{X}]]$.

$$\begin{array}{ccc} K[[\underline{X}]] & \xleftarrow{m} & K[[\underline{X},\underline{Y}]] \\ {\scriptstyle m}\uparrow & & \uparrow{\scriptstyle m\otimes 1} \\ K[[\underline{X},\underline{Y}]] & \xleftarrow{1\otimes m} & K[[\underline{X},\underline{Y},\underline{Z}]]. \end{array}$$

A morphism of formal group laws $\varphi : G \to G'$ induces a morphism of bigebras $\varphi_* : \mathbb{H}_G \to \mathbb{H}_{G'}$. In order to see for instance that φ_* respects the structure map Δ, one dualizes the diagram:

(1.51)
$$\begin{array}{ccc} K[[\underline{X}',\underline{Y}']] & \xrightarrow{\alpha\otimes\alpha} & K[[\underline{X},\underline{Y}]]. \\ {\scriptstyle m'}\downarrow & & \downarrow{\scriptstyle m} \\ K[[\underline{X}']] & \xrightarrow{\alpha} & K[[\underline{X}]] \end{array}$$

Here, α stands for the comorphism.

1.52. Theorem: Let G and G' be formal group laws over K. Then, the map

$$\mathrm{Hom}(G, G') \longrightarrow \mathrm{Hom}_{\mathrm{Bigebras}}(\mathbb{H}_G, \mathbb{H}_{G'})$$

is a bijection.

Proof: Let $\psi : \mathbb{H}_G \to \mathbb{H}_{G'}$ be a morphism of bigebras. By dualizing ψ one obtains a K-linear map $\alpha : K[[\underline{X}']] \to K[[\underline{X}]]$. It is continuous, because the open submodules of $K[[\underline{X}]]$ are the orthogonal complements of the finitely generated submodules of $\mathbb{H}_G$. We must show that α is the comorphism of a morphism of formal group laws. The required properties of α are expressed by commutative diagrams that are obtained by dualizing the corresponding diagrams for $\psi : \mathbb{H}_G \to \mathbb{H}_{G'}$. We content ourselves with giving an example of this procedure

and leave the rest to the reader. The fact that α is a ring homomorphism is expressed by Diagram (1.51). We obtain it by dualizing:

$$\begin{array}{ccc} \mathbb{H}_G \otimes \mathbb{H}_G & \xrightarrow{\psi\otimes\psi} & \mathbb{H}_{G'} \otimes \mathbb{H}_{G'} \\ \downarrow{\scriptstyle m^*} & & \downarrow{\scriptstyle m'^*} \\ \mathbb{H}_G & \xrightarrow{\psi} & \mathbb{H}_{G'}. \end{array}$$

Let $\mathfrak{g}$ be a Lie algebra over K. We define on $U(\mathfrak{g})$ the structure of a bigebra. Let $\Delta : \mathfrak{g} \to U(\mathfrak{g}) \otimes_K U(\mathfrak{g})$ be the homomorphism $\Delta(x) = 1 \otimes x + x \otimes 1$, $x \in \mathfrak{g}$. One verifies immediately that $\Delta[x, y] = \Delta x \Delta y - \Delta y \Delta x$. It follows that Δ factors through a K-algebra homomorphism $U(\mathfrak{g}) \to U(\mathfrak{g}) \otimes_K U(\mathfrak{g})$ that we still denote by Δ. From the definition of $U(\mathfrak{g})$ one obtains an augmentation $u : U(\mathfrak{g}) \to K$, $u(x) = 0$ for $x \in \mathfrak{g}$. The commutativity of the diagrams in 1.50 follows from the universal property. 23 24

The map (1.45) is a morphism of bigebras. In fact, for that it is enough to verify that the following diagrams are commutative:

$$\begin{array}{ccc} U(\operatorname{Lie} G) & \longrightarrow & \mathbb{H}_G \\ \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle e^*} \\ K & = & K \end{array} \qquad \begin{array}{ccc} U(\operatorname{Lie} G) & \longrightarrow & \mathbb{H}_G \\ \downarrow & & \downarrow{\scriptstyle m^*} \\ U(\operatorname{Lie} G) \otimes U(\operatorname{Lie} G) & \longrightarrow & \mathbb{H}_G \otimes \mathbb{H}_G. \end{array}$$

The verification for the first diagram is trivial. By the universal property, it is enough to verify the commutativity of the second diagram for $D \in \operatorname{Lie} G$. Let $l(f) = Df(0)$, $f \in K[[\underline{X}]]$. Then commutativity means that $m^* l(g(\underline{X}, \underline{Y})) = (1 \otimes l + l \otimes 1)(g(\underline{X}, \underline{Y}))$, $g \in K[[\underline{X}, \underline{Y}]]$. Due to the continuity of l, we may assume that $g(\underline{X}, \underline{Y}) = f(\underline{X})h(\underline{Y})$. Then the claimed equality means:

$$D(f(\underline{X})h(\underline{X}))|_{\underline{X}=0} = f(\underline{X})Dh(\underline{X})|_{\underline{X}=0} + h(\underline{X})Df(\underline{X})|_{\underline{X}=0}.$$

This is clear because D is a derivation.

1.53. Exercise: Show that conversely, from $m^* l = 1 \otimes l + l \otimes 1$ it follows that D is a derivation. When K is a $\mathbb{Q}$-algebra, one obtains for $D \in U(\operatorname{Lie} G)$:

$$D \in \operatorname{Lie} G \iff 1 \otimes D + D \otimes 1 = \Delta D.$$

§ 9 The main theorems of Lie theory

1.54. Theorem: Let K be a $\mathbb{Q}$-algebra. Let G and G' be formal group laws over K. Then the map

$$\operatorname{Hom}(G, G') \longrightarrow \operatorname{Hom}(\operatorname{Lie} G, \operatorname{Lie} G')$$

is bijective, where on the right-hand side are Lie algebra homomorphisms.

Proof: Since $U(\operatorname{Lie} G) = \mathbb{H}_G$ and $U(\operatorname{Lie} G') = \mathbb{H}_{G'}$, one has a commutative diagram

$$\begin{array}{ccc} \operatorname{Hom}(G, G') & \longrightarrow & \operatorname{Hom}(\operatorname{Lie} G, \operatorname{Lie} G') \\ & \searrow \quad \swarrow & \\ & \operatorname{Hom}_{\text{Bigebras}}(U(\operatorname{Lie} G), U(\operatorname{Lie} G')). & \end{array}$$

Since the left-hand slanted arrow is bijective by 1.52, it is enough to prove that the right-hand one is injective. But this is clear, since $\operatorname{Lie} G \subset \mathbb{H}_G \simeq U(\operatorname{Lie} G)$.

Using the Poincaré-Birkhoff-Witt Theorem (see 1.49), we show:

1.55. Theorem: Let $\mathfrak{g}$ be a finite-dimensional Lie algebra over a $\mathbb{Q}$-algebra K. Then there exists a formal group law G over K with Lie algebra $\mathfrak{g}$.

24 25

Proof: The bigebra of G must be $U(\mathfrak{g})$. Let $D_1, \dots, D_n$ be a basis of the K-module $\mathfrak{g}$. By 1.49, every $D \in U(\mathfrak{g})$ has a unique representation $D = \sum a_{\underline{i}} D_1^{i_1} \circ \dots \circ D_n^{i_n}$. Let $\underline{i}! = i_1! \dots i_n!$. We define an isomorphism of topological modules:

$$\varphi : K[[\underline{X}]] \longrightarrow \operatorname{Hom}_K(U(\mathfrak{g}), K), \qquad \varphi(\underline{X}^{\underline{i}})(D) = \underline{i}! a_{\underline{i}}.$$

There, the topology on the right-hand side is defined by the orthogonal complements of the finitely generated submodules. The map $\Delta : U(\mathfrak{g}) \to U(\mathfrak{g}) \otimes U(\mathfrak{g})$ induces by dualization the map $m : K[[\underline{X}, \underline{Y}]] \to K[[\underline{X}]]$. Indeed,we must prove that

$$\varphi(m(\underline{X}^{\underline{i}} \underline{Y}^{\underline{j}}))(\underline{D}^{\underline{k}}) = (\varphi(\underline{X}^{\underline{i}}) \otimes \varphi(\underline{Y}^{\underline{j}}))\Delta(\underline{D}^{\underline{k}}),$$

where $\underline{D}^{\underline{k}} = D_1^{k_1} \dots D_n^{k_n}$. This is equivalent to

$$\Delta \underline{D}^{\underline{k}} = \sum_{\underline{i}+\underline{j}=\underline{k}} \frac{\underline{k}!}{\underline{i}!\,\underline{j}!}\, \underline{D}^{\underline{i}} \otimes \underline{D}^{\underline{j}}.$$

For $\underline{D}^{\underline{k}} = D_r^{k_r}$, this is the usual Binomial Theorem. The general case follows since Δ is an algebra homomorphism. The algebra structure map $\alpha : U(\mathfrak{g}) \otimes U(\mathfrak{g}) \to U(\mathfrak{g})$ induces by dualization a morphism $\mu : K[[\underline{X}]] \to K[[\underline{X}, \underline{Y}]]$ of K-modules that respects the augmentation. The fact that μ is a ring homomorphism is obtained by dualizing the following commutative diagram:

$$\begin{array}{ccc} U(\mathfrak{g}) & \xrightarrow{\qquad\Delta\qquad} & U(\mathfrak{g}) \otimes U(\mathfrak{g}) \\ {\scriptstyle\alpha}\uparrow & & \uparrow{\scriptstyle\alpha} \\ U(\mathfrak{g}) \otimes U(\mathfrak{g}) & \xrightarrow{\Delta\otimes\Delta} & U(\mathfrak{g}) \otimes U(\mathfrak{g}) \otimes U(\mathfrak{g}) \otimes U(\mathfrak{g}). \end{array}$$

This expresses the fact that Δ is a ring homomorphism. The reader will check easily that μ is a formal group law (compare with (1.7)).

§ 10 Cartier duality

In the following, we interpret a morphism from a formal group law G to $\mathbb{G}_{\mathrm{m}}$ with the help of the algebra $\mathbb{H}_g$. Let $\varphi : G \to \mathbb{G}_{\mathrm{m}}$ be a morphism and $\varphi^* : K[[T]] \to K[[\underline{X}]]$ its comorphism. The power series $\varphi^*(1+T) \in K[[\underline{X}]]$ defines a K-linear map $\alpha : \mathbb{H}_G \to K$. We now prove that α is a ring homomorphism.

By definition, we have $\varphi^*(1+T) = 1 = \varphi$. Let $l_1, l_2 \in \mathbb{H}_G$. Then

$$\begin{aligned} \alpha(l_1 \cdot l_2) &= (l_1 \cdot l_2)(\varphi^*(1+T)) = (l_1 \otimes l_2)(1 + \varphi G(\underline{X}, \underline{Y})) \\ &= (l_1 \otimes l_2)(1 + \varphi(\underline{X}) + \varphi(\underline{Y}) + \varphi(\underline{X})\varphi(\underline{Y})) \\ &= l_1(\varphi^*(1+T)) l_2(\varphi^*(1+T)) = \alpha(l_1)\alpha(l_2). \end{aligned}$$

Let $\alpha : \mathbb{H}_G \to K$ be an arbitrary K-algebra homomorphism. It is induced by a power series $1 + \varphi \in K[[\underline{X}]]$ with $\varphi(0) = 0$. Thus the above series of equalities hold for all $l_1, l_2 \in \mathbb{H}_G$. We deduce from the third equality that φ induces a morphism $G \to \mathbb{G}_{\mathrm{m}}$. We have obtained the following. 25 26

1.56. Theorem (Cartier duality): Let G be a formal group law over K. Then there is a canonical bijection

$$\mathrm{Hom}_{K\text{-Alg}}(\mathbb{H}_G, K) \longrightarrow \mathrm{Hom}(G, \mathbb{G}_{\mathrm{m}}).$$

Let K' be a commutative K-algebra with unit element. Then, one has $\mathbb{H}_G \otimes_K K' = \mathbb{H}_{G_{K'}} = \mathrm{Hom}_{K,\mathrm{cont}}(K'[[\underline{X}]], K')$. We obtain a bijection

$$\mathrm{Hom}_{K\text{-Alg}}(\mathbb{H}_G, K') = \mathrm{Hom}_{K'\text{-Alg}}(\mathbb{H}_G \otimes K', K') = \mathrm{Hom}(G_{K'}, \mathbb{G}_{\mathrm{m},K'}).$$

Let G be commutative. Then $\mathbb{H}_G$ is also commutative. One can formulate 1.56 in the following way. The functor $K' \mapsto \mathrm{Hom}(G_{K'}, \mathbb{G}_{\mathrm{m},K'})$ from the category of commutative K-algebras is representable by the algebra of invariant differential operators on G.

1.57. Exercise: Let R be a K-algebra and M an R-module. Define the derivations from R to M as follows:

$$\mathrm{Der}_K(R, M) = \big\{\delta \in \mathrm{Hom}_K(R, M) \,|\, \delta(r_1 r_2) = r_1\delta(r_2) + r_2\delta(r_1)\big\}.$$

We consider K as an $\mathbb{H}_G$-module via the augmentation $e^* : \mathbb{H}_G \to K$. Show that

$$\mathrm{Hom}(G, \mathbb{G}_{\mathrm{a}}) = \mathrm{Der}_K(\mathbb{H}_G, K).$$

Let K be a $\mathbb{Q}$-algebra. Then, one has bijections:

$$\begin{aligned}\big\{&\text{invariant differential forms } \omega \,|\, \omega([D, D']) = 0 \text{ for all } D, D' \in \mathrm{Lie}\, G\big\}\\ &\simeq \mathrm{Hom}(\mathrm{Lie}\, G, \mathrm{Lie}\, \mathbb{G}_{\mathrm{a}})\\ &= \mathrm{Der}_K(U(\mathrm{Lie}\, G), K).\end{aligned}$$

§ 11 Lubin-Tate groups

We have seen in the last paragraphs that the theory of formal group laws over a $\mathbb{Q}$-algebra is equivalent to the theory of Lie algebras. Over an arbitrary ring, the situation is considerably more complicated. In the following chapters, we will reduce the theory of commutative formal group laws to the theory of certain modules over the Cartier ring. However, before we begin with the general theory, it is good to have before one's eyes a non-trivial example of a commutative formal group law when K is not a $\mathbb{Q}$-algebra. This is why we give the construction of Lubin-Tate groups, that were the starting point for Cartier Theory and other developments in the theory of formal groups. For the applications to Algebraic Number Theory, we refer the reader to [13] and [25].

26/27 Let K be a discrete valuation ring and π a prime element. Let $K/\pi K$ be a finite field of characteristic p with q' elements. Let $q = p^a$ be a power of q'. Our goal is the construction of one-dimensional group laws $F(X,Y)$ over K. By base change, we obtain from $F(X,Y)$ a formal group law $\overline{F}(X,Y)$ over k. Since the coefficients of $\overline{F}$ are in k, we have

$$\overline{F}(X,Y)^q = \overline{F}(X^q, Y^q).$$

This equality says that the power series $g(X) = X^q$ defines an endomorphism $g : F \to F$. It is called the *Frobenius endomorphism* Fr.

Since F is one-dimensional, $\mathrm{Lie}\, F$ is a free K-module of rank 1. An endomorphism of F induces on $\mathrm{Lie}\, F$ the multiplication by an element of K.

1.58. Definition: A *Lubin-Tate group over K* is a one-dimensional formal group law F over K for which an endomorphism $\varphi : F \to F$ exists such that $\mathrm{Lie}\,\varphi$ is multiplication by π and such that φ induces the Frobenius endomorphism of $\overline{F}$. In other words, the power series satisfies the following conditions:

(1.58.1) $$\varphi(X) = \pi X \mod \deg 2, \qquad \varphi(X) = X^q \mod \pi K.$$

The construction of such formal group laws is based on the following

1.59. Lemma: Let φ and ψ be power series satisfying (1.58.1). Let $L(X_1,\dots,X_n) = \sum a_i X_i$ be a linear polynomial with coefficients in K. Then, there exists a unique power series $F(X_1,\dots,X_n) \in K[[\underline{X}]]$ such that

$$F(X_1,\dots,X_n) = L(X_1,\dots,X_n) \mod \deg 2,$$
$$\varphi(F(X_1,\dots,X_n)) = F(\psi(X_1),\dots,\psi(X_n)).$$

Proof: We prove by induction on r that there exists a unique polynomial $F_r(\underline{X})$ of degree r such that $F(\underline{X}) = L(\underline{X}) \mod \deg 2$ and $\varphi(F_r(\underline{X})) = F_r(\psi(\underline{X}) \mod \deg(r+1)$. Obviously $F_1 = L$. Let us write $F_{r+1} = F_r + \Delta_{r+1}$ where Δ_{r+1} is a homogeneous polynomial of degree $r+1$. One finds the equalities:

$$\varphi(F_{r+1}(\underline{X})) = \varphi(F_r(\underline{X})) + \pi\Delta_{r+1}(\underline{X}) \mod \deg(r+2),$$
$$F_{r+1}(\psi(\underline{X})) = F_r(\psi(\underline{X})) + \pi^{r+1}\Delta_{r+1}(\underline{X}) \mod \deg(r+2).$$

It follows that the left-hand sides are congruent if we can find Δ_{r+1} such that

$$(\pi^{r+1} - \pi)\Delta_{r+1}(\underline{X}) = \varphi(F_r(\underline{X})) - F_r(\psi(\underline{X})) \mod \deg(r+2).$$

Thus existence and uniqueness of Δ_{r+1} will follow if we can show that the coefficients of the left-hand power series are divisible by π. From (1.58.1) it follows immediately that

27/28 $$\varphi(F_r(\underline{X})) - F_r(\psi(\underline{X})) = (F_r(\underline{X}))^q - (F_r(\underline{X}^q)) = 0 \mod \pi.$$

The lemma follows with the power series F for which $F = F_r \mod \deg(r+1)$ for all r.

Applying the lemma for $\varphi = \psi$ and $L = X+Y$, one obtains a power series $F_\varphi(X,Y)$. The power series $F_\varphi(F_\varphi(X,Y),Z)$ and $F_\varphi(X,F_\varphi(Y,Z))$ are solutions of the following equalities for a power series G:

$$G(X,Y,Z) = X+Y+Z \mod \deg 2, \qquad \varphi(G(X,Y,Z) = G(\varphi(X),\varphi(Y),\varphi(Z)).$$

Since by the lemma the solution is unique, it follows that $F_\varphi(F_\varphi(X,Y),Z) = F_\varphi(X,F_\varphi(Y,Z))$. One sees analogously that $F_\varphi(X,0) = F_\varphi(0,X) = X$ and that F_φ is symmetric in X and Y. Thus F_φ is a one-dimensional, commutative formal group law. It is a Lubin-Tate group.

For any $a \in K$ we define the power series $\langle a\rangle_{\varphi,\psi} \in K[[T]]$ as the unique solution to the following equalities:

$$\langle a\rangle_{\varphi,\psi}(T) = aT \mod \deg 2, \qquad \varphi(\langle a\rangle_{\varphi,\psi}(T)) = \langle a\rangle_{\varphi,\psi}(\psi(T)).$$

By the same principle as for the associative law for F, one proves:

1.60. Theorem: Let φ,ψ,χ be power series satisfying the conditions (1.58.1) and $a,b \in K$. Then, the following identities hold:

1) $F_\varphi(\langle a\rangle_{\varphi,\psi}(X),\langle a\rangle_{\varphi,\psi}(Y)) = \langle a\rangle_{\varphi,\psi}(F_\psi(X,Y))$,

2) $\langle a\rangle_{\varphi,\psi}(\langle b\rangle_{\psi,\chi}(T)) = \langle ab\rangle_{\varphi,\chi}(T)$,

3) $\langle a+b\rangle_{\varphi,\psi}(T) = F_\varphi(\langle a\rangle_{\varphi,\chi}(T),\langle b\rangle_{\varphi,\chi}(T))$,

4) $\langle \pi\rangle_{\varphi,\varphi}(T) = \varphi(T)$, $\langle 1\rangle_{\varphi,\varphi}(T) = T$.

The first equality says that $\langle a\rangle_{\varphi,\psi}$ is a homomorphism $F_\psi \to F_\varphi$. The set $\mathrm{Hom}(F_\psi,F_\varphi)$ is an abelian group. Indeed, according to 1.10 one can define the sum of two morphisms α and β in the following way:

$$F_\psi \longrightarrow F_\psi \times F_\psi \xrightarrow{\alpha\times\beta} F_\varphi \times F_\varphi \longrightarrow F_\varphi.$$

The third equality says that $K \to \mathrm{Hom}(F_\psi,F_\varphi)$, $a \mapsto \langle a\rangle_{\varphi,\psi}$ is a homomorphism from the additive group of K to $\mathrm{Hom}(F_\psi,F_\varphi)$. From the second equality, the composition of morphisms corresponds to the multiplication in K. It follows that $\langle 1\rangle_{\varphi,\psi}$ defines an isomorphism of F_ψ to F_φ. The map $K \to \mathrm{Hom}(F_\varphi,F_\varphi)$ is a ring homomorphism. If φ is fixed, then $\langle a\rangle_{\varphi,\psi}$ is also denoted simply $\langle a\rangle$. Therefore, we obtain:

1.61. Theorem: Given K,π and q, there is up to isomorphism a unique Lubin-Tate group F. There exists a ring homomorphism $K \to \mathrm{End}\,F = \mathrm{Hom}(F,F)$, $a \mapsto \langle a\rangle$, such that $\langle a\rangle$ induces the multiplication by a on $\mathrm{Lie}\,F$. The endomorphism $\langle\pi\rangle$ induces the Frobenius endomorphism Frob_q by the base change $K \to k$. 28 29

Let $K = \mathbb{Z}_p$, $\pi = p$ and $q = p^a$. Then using 1.60.3), one finds that

$$\langle p\rangle(T) = F(T,F(\dots,F(T,T))\dots),$$

where T stands p times. It follows by base change that

$$T^q = \overline{F}(T,\overline{F}(\dots,\overline{F}(T,T))\dots).$$

Let $q' \neq q$ and F' be the Lubin-Tate group attached to $\mathbb{Z}_p$, p, q'. Then, there is no nonzero homomorphism $\alpha : \overline{F} \to \overline{F}'$. Indeed, we find the relation $\alpha(T^q) = (\alpha(T))^{q'}$. The reader can check easily that this is not fulfilled over any reduced $\mathbb{F}_p$-algebra B. From this follows that over an $\mathbb{F}_p$-algebra, there are always infinitely many non-isomorphic, one-dimensional formal group laws. In comparison, over a $\mathbb{Q}$-algebra there is only $\mathbb{G}_{\mathrm{a}}$.

Chapter II

Formal groups as functors

30

§ 1 Definition of formal groups

In this chapter and all the following ones, a formal group law will always be assumed to be commutative.

We denote by $\mathrm{Nil_K}$ the category of nilpotent, commutative K-algebras. A formal group law G defines by 1.6 a functor to the category of abelian groups:

$$\begin{aligned} \widetilde{G} : \mathrm{Nil_K} &\longrightarrow \mathrm{Ab} \\ \mathscr{N} &\longmapsto (\mathscr{N}^{(n)}, +_G). \end{aligned}$$

We can see $\widetilde{G}$ as a functor to the category of sets, by forgetting the abelian group structure on $\widetilde{G}(\mathscr{N})$. We denote this set-valued functor by $\mathrm{Var}\,\widetilde{G}$ and call it the *variety* of $\widetilde{G}$. The functor $\mathrm{Var}\,\widetilde{G}$ is just $\mathscr{N} \mapsto \mathscr{N}^{(n)}$.

Conversely, if we are given a functor $\widetilde{G} : \mathrm{Nil_K} \to \mathrm{Ab}$, such that $\mathrm{Var}\,\widetilde{G}\ (\mathscr{N}) = \mathscr{N}^{(n)}$, then $\widetilde{G}$ is defined by a formal group law. Indeed, let $K[[\underline{X}, \underline{Y}]]$ be the ring of powers series in $2n$ indeterminates $X_1, \ldots, X_n, Y_1, \ldots, Y_n$, and $\mathfrak{a} \subset K[[\underline{X}, \underline{Y}]]$ be the ideal which is generated by the indeterminates. Then $\mathfrak{a}/\mathfrak{a}^N$ is an object of $\mathrm{Nil_K}$ for all natural numbers N. Thus $\widetilde{G}(\mathfrak{a}/\mathfrak{a}^N)$ is an abelian group with underlying set $(\mathfrak{a}/\mathfrak{a}^N)^{(n)}$. We construct in this group the sum

$$(X_1, \ldots, X_n) +_G (Y_1, \ldots, Y_n) = (G_1^{(N)}, \ldots, G_n^{(N)}), \quad G_i^{(N)} \in \mathfrak{a}/\mathfrak{a}^N.$$

As $\widetilde{G}(\mathfrak{a}/\mathfrak{a}^{n+1}) \to \widetilde{G}(\mathfrak{a}/\mathfrak{a}^n)$ is a group homomorphism, we have

$$G_i^{(N+1)} = G_i^{(N)} \mod \mathfrak{a}^N.$$

Thereby we find some power series G_i such that $G_i = G_i^{(N)} \mod \deg N$. The fact that the G_i define a formal group law is left to the reader.

The additive and the multiplicative groups are seen as functors in the following way:

$$\begin{aligned} \mathbb{G}_{\mathrm{a}}(\mathscr{N}) &= (\mathscr{N}, +), \\ \mathbb{G}_{\mathrm{m}}(\mathscr{N}) &= (1 + \mathscr{N})^{\times}. \end{aligned}$$

Here $(\mathscr{N},+)$ is the group $\mathscr{N}$ with the usual addition and $(1+\mathscr{N})^\times$ the set of all formal sums $1+u$, $u\in\mathscr{N}$, with the obvious multiplication.

2.1. Remark: Instead of $\mathscr{N}$, we will sometimes consider the augmented K-algebra $A = K\oplus\mathscr{N}$, where the ring structure is as follows:

$$(k_1,u_1)(k_2,u_2) = (k_1k_2, k_1u_2+k_2u_1+u_1u_2),\quad k_i\in K, u_i\in\mathscr{N}.$$

The map $\varepsilon : A\to K$ is the augmentation.

30 31 Conversely, let A be a commutative augmented K-algebra (that is, a K-algebra with unit and a K-algebra homomorphism $\varepsilon : A\to K$) such that $\operatorname{Ker}\varepsilon$ is nilpotent. Then we have

$$A = K\oplus\operatorname{Ker}\varepsilon,\quad \operatorname{Ker}\varepsilon\in\mathrm{Nil_K}\,.$$

We call A an *augmented nilpotent K-algebra* and also denote by A^+ the augmentation ideal $\operatorname{Ker}\varepsilon$. Note that $\mathbb{G}_{\mathrm{m}}(A^+)$ is the subgroup of 1-units of A:

$$\mathbb{G}_{\mathrm{m}}(A^+) = \{x\in A\mid \varepsilon(x)=1\}.$$

2.2. Definition: A *formal group* is an exact functor $G : \mathrm{Nil_K}\to\mathrm{Ab}$ which commutes with infinite direct sums.

In detail, this means the following. For each exact sequence in $\mathrm{Nil_K}$

$$0\longrightarrow\mathscr{N}_1\longrightarrow\mathscr{N}_2\longrightarrow\mathscr{N}_3\longrightarrow 0,$$

the sequence

$$0\longrightarrow G(\mathscr{N}_1)\longrightarrow G(\mathscr{N}_2)\longrightarrow G(\mathscr{N}_3)\longrightarrow 0$$

is exact. For each set of objects $\{\mathscr{N}_i\}_{i\in I}$ of $\mathrm{Nil_K}$, such that $\mathscr{N}_i{}^N = 0$ for some natural number N which is independent from i, the algebra $\oplus_{i\in I}\mathscr{N}_i$ is obviously a nilpotent K-algebra. The injections $\alpha_i : \mathscr{N}_i\to\bigoplus\limits_{i\in I}\mathscr{N}_i$ induce a map

$$\begin{aligned}\bigoplus_{i\in I} G(\mathscr{N}_i) &\longrightarrow G\Big(\bigoplus_{i\in I}\mathscr{N}_i\Big)\\ \oplus\xi_i &\longmapsto \sum G(\alpha_i)\xi_i.\end{aligned}$$

We require that this map be an isomorphism.

2.3. Exercise: An exact functor commutes with finite direct sums. Show that an exact functor commutes with infinite direct sums if and only if the following condition is fulfilled. Let I be a directed set and $\{\mathscr{N}_i\}_{i\in I}$ be a system of subalgebras of a nilpotent algebra $\mathscr{N}$, such that $\mathscr{N}_i\subset\mathscr{N}_j$ for $i\leqslant j$. Assume that $\bigcup\limits_{i\in I}\mathscr{N}_i = \mathscr{N}$. Then we have $\bigcup\limits_{i\in I}G(\mathscr{N}_i) = G(\mathscr{N})$.

2.4. Example: Let S be an augmented algebra and S^+ its augmentation ideal. We define a functor:

$$\mathbb{G}_{\mathrm{m}}S(\mathscr{N}) = (1+S^+\otimes_K\mathscr{N})^\times.$$

If S^+ is a flat K-module, it is a formal group, as tensor products commute with arbitrary direct sums. A particular role is played in Cartier theory by the formal group $\mathbb{G}_{\mathrm{m}}K[t]$, that we also denote by Λ:

$$\Lambda(\mathscr{N}) = \{1 + u_1 t + \ldots + u_r t^r \mid u_i \in \mathscr{N}\}.$$

The multiplication is the usual multiplication of polynomials.

§ 2 Representable and prorepresentable functors

31 32

In this paragraph, we consider functors from $\mathrm{Nil_K}$ to the category of sets Ens. Let A be an augmented nilpotent K-algebra. Then A defines a functor

$$\mathrm{Spf}\, A : \mathrm{Nil_K} \longrightarrow \mathrm{Ens},$$

$$\mathrm{Spf}\, A\,(\mathscr{N}) = \mathrm{Hom}_{K\text{-Alg}}(A^+, \mathscr{N}) = \mathrm{Hom}_{K\text{-Alg}}(A, K \oplus \mathscr{N}).$$

By the first Hom we mean K-algebra homomorphisms and by the second one those which respect the augmentation.

2.5. Definition: A functor $H : \mathrm{Nil_K} \to \mathrm{Ens}$ is said to be *representable* if it is isomorphic to a functor of the form $\mathrm{Spf}\, A$.

Now we introduce the category $\mathrm{Compl_K}$ of complete, augmented K-algebras. Let R be a commutative K-algebra with unit and with an augmentation $\varepsilon : R \to K$. We denote by $\mathfrak{a}_1$ the augmentation ideal $\mathrm{Ker}\,\varepsilon$. Let there be given in R a decreasing sequence of ideals $\mathfrak{a}_m$, $m \in \mathbb{N}$:

$$\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \mathfrak{a}_3 \supset \ldots$$

We say that $(R, \mathfrak{a}_m)$ is a *complete, augmented K-algebra*, when the following conditions are fulfilled:

(2.6.1) $\qquad \mathfrak{a}_1/\mathfrak{a}_m$ is a nilpotent K-algebra,

(2.6.2) $$R = \varprojlim R/\mathfrak{a}_m.$$

The ideals $\mathfrak{a}_m$ define a topology on R. Condition (2.6.2) is equivalent to the fact that R is Hausdorff and complete with respect to this topology. Let $(R', \mathfrak{a}'_m)$ be a second augmented, complete K-algebra. A *morphism* $\alpha : R \to R'$ is a continuous homomorphism of augmented K-algebras, that is, for each natural number M there exists an N such that $\alpha(\mathfrak{a}_N) \subset \mathfrak{a}'_M$. Assume given in R a second sequence of ideals $\mathfrak{b}_m$, $m \in \mathbb{N}$, which satisfies Conditions (2.6.1) and (2.6.2). Then the identity map $(R, \mathfrak{a}_m) \to (R, \mathfrak{b}_m)$ defines an isomorphism of objects in $\mathrm{Compl_K}$ if and only if $\mathfrak{a}_m$ and $\mathfrak{b}_m$ define the same topology.

Let $\mathscr{N} \in \mathrm{Nil_K}$ and $A = K \oplus \mathscr{N}$. One can view A with the sequence $\mathfrak{a}_1 = \mathscr{N}$ and $\mathfrak{a}_m = 0$, $m \geqslant 2$ as an object of $\mathrm{Compl_K}$. We obtain in this way an embedding of categories:

$$\mathrm{Nil_K} \hookrightarrow \mathrm{Compl_K}\,.$$

One can extend a functor $H : \mathrm{Nil}_K \to \mathrm{Ens}$ to the category Compl_K by setting: $H(R) = \varprojlim H(\mathfrak{a}_1/\mathfrak{a}_m)$. We allow ourselves to denote $H(R)$ also by $H(\mathfrak{a}_1)$.

An algebra $R \in \mathrm{Compl}_K$ defines a functor (*formal spectrum*):

32
33

$$\mathrm{Spf}\, R : \mathrm{Nil}_K \longrightarrow \mathrm{Ens},$$

$$\mathrm{Spf}\, R\,(\mathscr{N}) = \mathrm{Hom}_{\mathrm{Compl}_K}(R, K \oplus \mathscr{N}) = \varinjlim \mathrm{Hom}_{K\text{-Alg}}(\mathfrak{a}_1/\mathfrak{a}_m, \mathscr{N}).$$

2.7. Definition: A functor $H : \mathrm{Nil}_K \to \mathrm{Ens}$ is said to be *prorepresentable* if it is isomorphic to a functor of the form $\mathrm{Spf}\, R$.

2.8. Example: Let $G : \mathrm{Nil}_K \to \mathrm{Ab}$ be the functor of a formal group law. Then $\mathrm{Var}\, G$ is prorepresentable by $R = K[[\underline{X}]]$ and $\mathfrak{a}_m = (\underline{X})^m$. Indeed, the elements of $\mathrm{Spf}\, K[[X]]\ (\mathscr{N})$ are in $1-1$ correspondence with the n-tuples $(x_1, \ldots, x_n) \in \mathscr{N}^{(n)}$.

$$K[[X_1, \ldots, X_n]] \longrightarrow K \oplus \mathscr{N}$$
$$X_i \longmapsto x_i.$$

When we extend the functor $\mathrm{Spf}\, R$ to the category Compl_K, then we obtain for $S \in \mathrm{Compl}_K$:

$$\mathrm{Spf}\, R\,(S) = \mathrm{Hom}_{\mathrm{Compl}_K}(R, S).$$

The following lemma shows that the functor $\mathrm{Spf}\, R$ defines the complete, augmented K-algebra R up to unique isomorphism.

2.9. Lemma (Yoneda): Let $\mathcal{C}$ be a category. We denote by $\widehat{\mathcal{C}}$ the category of all functors from $\mathcal{C}$ to the category of sets. Each object $R \in \mathcal{C}$ defines a functor $\mathrm{Spf}\, R\,(S) = \mathrm{Hom}_{\mathcal{C}}(R, S)$ of $\widehat{\mathcal{C}}$. If F is a functor on $\widehat{\mathcal{C}}$, then one has a bijection

$$\kappa : \mathrm{Hom}_{\widehat{\mathcal{C}}}(\mathrm{Spf}\, R, F) \longrightarrow F(R).$$

In particular we have $\mathrm{Hom}_{\widehat{\mathcal{C}}}(\mathrm{Spf}\, R, \mathrm{Spf}\, S) = \mathrm{Hom}_{\mathcal{C}}(S, R)$.

Proof: Let $\xi : \mathrm{Spf}\, R \to F$ be a morphism. The image of the identity $\mathrm{id}_R \in \mathrm{Hom}(R, R) = \mathrm{Spf}\, R\,(R)$ by the map $\xi_R : \mathrm{Spf}\, R\,(R) \to F(R)$ is $\kappa(\xi)$. Conversely, let $c \in F(R)$. We define for all $S \in \mathcal{C}$ a map

$$\xi_S : \mathrm{Spf}\, R\,(S) \longrightarrow F(S).$$

Let $\alpha \in \mathrm{Spf}\, R\,(S) = \mathrm{Hom}(R, S)$. Then $\xi_S(\alpha) = F(\alpha)(c)$. The ξ_S clearly define a morphism of functors ξ such that $\kappa(\xi) = c$.

To summarize, we now have the following embeddings of categories:

$$\mathrm{Nil}_K \hookrightarrow \mathrm{Compl}_K \hookrightarrow \mathbf{Functors}(\mathrm{Nil}_K, \mathrm{Ens}).$$

2.10. Base change: Let K' be a commutative K-algebra with unit. Each object of $\mathrm{Nil}_{K'}$ can be viewed as a K-algebra. We obtain a functor

$$b : \mathrm{Nil}_{K'} \longrightarrow \mathrm{Nil}_K\,.$$

If $H : \mathrm{Nil_K} \to \mathrm{Ens}$ is a functor, then we say that $H_{K'} = H \circ b$ is *deduced from H by base change*. Let $(R, \mathfrak{a}_m)$ be a complete, augmented K-algebra, and let $H = \mathrm{Spf}\, R$. We have:

$$H_{K'}(\mathscr{N}') = \varinjlim \mathrm{Hom}_{K\text{-Alg}}(\mathfrak{a}_1/\mathfrak{a}_m, \mathscr{N}') = \varinjlim \mathrm{Hom}_{K'\text{-Alg}}(\mathfrak{a}_1/\mathfrak{a}_m \otimes_K K', \mathscr{N}'). \quad \frac{33}{34}$$

We denote by $R \mathbin{\widehat{\otimes}}_K K'$ the K'-algebra $\varprojlim (R/\mathfrak{a}_m \otimes_K K')$. Let $\mathfrak{a}'_m$ be the kernel of the projection $R \mathbin{\widehat{\otimes}}_K K' \to R/\mathfrak{a}_m \otimes_K K'$. Then $(R \mathbin{\widehat{\otimes}}_K K', \mathfrak{a}'_m)$ is a complete augmented K'-algebra and $H_{K'} = \mathrm{Spf}\, R \mathbin{\widehat{\otimes}}_K K'$. Prorepresentable functors are thus turned into prorepresentable functors by base change. If $H = \mathrm{Spf}\, R$ is representable, so is $H_{K'}$, and we have $R \mathbin{\widehat{\otimes}}_K K' = R \otimes_K K'$.

2.11. In this point, we generalize Example 2.8. Let P be a K-module. We associate to P the following functor:

$$\begin{aligned} h_P : \mathrm{Nil_K} &\longrightarrow \mathrm{Ens} \\ \mathscr{N} &\longmapsto \mathscr{N} \otimes_K P. \end{aligned}$$

We are going to show that the functor h_P is prorepresentable when P is a projective module which admits a countable generating system.

We first consider the case where P is a finitely generated projective K-module. Let $P^* = \mathrm{Hom}_K(P, K)$ be the dual K-module. Then the canonical map

$$P \longrightarrow P^{**}$$

is an isomorphism. This is clear for a finitely generated free module. The general case follows from the fact that P is a direct summand of such a module. The same argument shows that for a K-module M the canonical map

$$M \otimes_K P \longrightarrow \mathrm{Hom}_K(P^*, M)$$

is an isomorphism.

Let M be a K-module. We denote by $S(M)$ the symmetric algebra of M. It is characterized by the following universal property. Let K' be a K-algebra like in 2.10. Then one has a bijection

$$\mathrm{Hom}_K(M, K') = \mathrm{Hom}_{K\text{-Alg}}(S(M), K').$$

Also $S(M)$ is an augmented K-algebra. Let J be its augmentation ideal. Clearly

$$S\hat{}(M) := \varprojlim_N S(M)/J^N$$

is an object of $\mathrm{Compl_K}$. With $A = K \oplus \mathscr{N}$, we find:

$$\mathscr{N} \otimes_K P = \mathrm{Hom}_K(P^*, \mathscr{N}) = \mathrm{Hom}_{K\text{-Alg}}(S(P^*), A) = \mathrm{Hom}_{\mathrm{Compl_K}}(S\hat{}(P^*), A).$$

Consequently the functor h_P is prorepresentable in this case.

We now consider the case where P is not necessarily finitely generated. The reader can first skip these considerations and begin with the next paragraph.

We denote by $U^\perp \subset P^*$ the orthogonal complement of a submodule $U \subset P$. We endow P^* with the topology in which $\{U^\perp\}$ is a system of neighborhoods of 0, where U runs $\frac{34}{35}$

through the finitely generated submodules of P. Let M be a K-module. Then one has a canonical homomorphism

$$M \otimes_K P \longrightarrow \varinjlim \mathrm{Hom}_K(P^*/U^\perp, M) = \mathrm{Hom}_{K,\mathrm{cont}}(P^*, M).$$

We show that it is an isomorphism for a projective module P. First, let P be a free module. Then one already obtains a system of neighborhoods $\{U^\perp\}$ of 0, when we let U run through the finitely generated, free direct summand U of P. We obtain:

$$\varinjlim \mathrm{Hom}_K(P^*/U^\perp, M) = \varinjlim \mathrm{Hom}(U^*, M) = \varinjlim (M \otimes_K U) = M \otimes_K P.$$

In the general case, P is a direct summand of a free module L_1. We find an exact sequence

$$0 \longrightarrow P \longrightarrow L_1 \longrightarrow L_2,$$

in which the cokernel of the middle map is a direct summand of the free module L_2. One obtains from this an exact sequence of continuous homomorphisms

$$L_2^* \longrightarrow L_1^* \longrightarrow P^* \longrightarrow 0.$$

One obtains the claim from the following commutative diagram with exact rows:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_{K,\mathrm{cont}}(P^*, M) & \longrightarrow & \mathrm{Hom}_{K,\mathrm{cont}}(L_1^*, M) & \longrightarrow & \mathrm{Hom}_{K,\mathrm{cont}}(L_2^*, M) \\
 & & \uparrow & & \uparrow & & \uparrow \\
0 & \longrightarrow & M \otimes_K P & \longrightarrow & M \otimes_K L_1 & \longrightarrow & M \otimes_K L_2.
\end{array}$$

Let P be a projective module with a countable generating system $\{e_i\}_{i\in\mathbb{N}}$. Let U_n be the submodule of P generated by $e_1, \ldots, e_n$. We define the *completed symmetric algebra* of the topological module P^*:

$$S^\wedge_{\mathrm{top}}(P^*) = \varprojlim S^\wedge(P^*/U_n^\perp).$$

Let J_n be the augmentation ideal of $S^\wedge(P^*/U_n^\perp)$. We denote by $\mathfrak{a}_n$ the inverse image of J_n^n by the canonical projection:

$$S^\wedge_{\mathrm{top}}(P^*) \longrightarrow S^\wedge(P^*/U_n^\perp).$$

One finds some maps

$$S^\wedge_{\mathrm{top}}(P^*)/\mathfrak{a}_n = S^\wedge(P^*/U_n^\perp)/J_n^n \longrightarrow S^\wedge(P^*/U_i^\perp)/J_i^n, \quad \text{for } i \leqslant n.$$

By taking the limit, one obtains:

$$\varprojlim_n S^\wedge_{\mathrm{top}}(P^*)/\mathfrak{a}_n \longrightarrow S^\wedge(P^*/U_i^\perp),$$
$$\varprojlim_n S^\wedge_{\mathrm{top}}(P^*)/\mathfrak{a}_n \longrightarrow S^\wedge_{\mathrm{top}}(P^*).$$

35 36 The latter morphism comes from the universal property of inverse limits. Consequently, $S^\wedge_{\mathrm{top}}(P^*)$ is an object of $\mathrm{Compl_K}$. For an augmented nilpotent K-algebra R, we have:

$$\begin{aligned}
\mathrm{Hom}_{\mathrm{Compl_K}}(S^\wedge_{\mathrm{top}}(P^*), R) &= \varinjlim \mathrm{Hom}_{\mathrm{Compl_K}}(S^\wedge(P^*/U_n^\perp), R) \\
&= \varinjlim \mathrm{Hom}_K(P^*/U_n^\perp, R^+) \\
&= \mathrm{Hom}_{K,\mathrm{cont}}(P^*, R^+) = R^+ \otimes_K P.
\end{aligned}$$

We have thus proved that $h_P = \mathrm{Spf}\, S^{\widehat{}}_{\mathrm{top}}(P^*)$.

One can calculate $S^{\widehat{}}_{\mathrm{top}}(P^*)$ rather explicitly, when P is a free module with basis $\{e_i\}_{i\in\mathbb{N}}$. Indeed, let $X_i \in P^*$ be such that

$$X_i(e_j) = \delta_{i,j}.$$

Then we have:

$$S^{\widehat{}}(P^*/U_n^{\perp}) = S^{\widehat{}}(U_n^*) = K[[X_1, \ldots, X_n]].$$

The morphism $S^{\widehat{}}(U_n^*) \to S^{\widehat{}}(U_i^*)$ for $i \leqslant n$ is the projection:

$$\begin{aligned} K[[X_1, \ldots, X_n]] &\longrightarrow K[[X_1, \ldots, X_i]] \\ X_j &\longmapsto \begin{cases} X_j & \text{if } j \leqslant i, \\ 0 & \text{if } j > i. \end{cases} \end{aligned}$$

We denote the inverse limit by $K\{X_1, X_2, \ldots\}$. It consists of all power series of the following form. Let $\alpha : \mathbb{N} \to \mathbb{N} \cup \{0\}$ be a function with finite support (that is, $\alpha(n) = 0$ for almost all $n \in \mathbb{N}$). Let $\underline{X}^{\alpha}$ be the monomial $\prod_{n\in\mathbb{N}} X_n^{\alpha(n)}$. Then:

$$K\{X_1, X_2, \ldots\} = \left\{ \sum_{\alpha:\mathbb{N}\to\mathbb{N}\cup\{0\}} c_\alpha \underline{X}^{\alpha} \quad | \quad c_\alpha \in K \right\}.$$

Here α runs through the functions with finite support, and the c_α are arbitrary coefficients.

The ideal $\mathfrak{a}_n$ consists of all power series for which $c_\alpha = 0$ if $\sum_{i\leqslant n} \alpha(i) + \sum_{i>n} n\alpha(i) < n$. It is convenient to use another system of neighborhoods of 0 than that of the $\mathfrak{a}_n$. We define the *weight* of a monomial:

$$w(\underline{X}^{\alpha}) = \sum_{i\in\mathbb{N}} i\alpha(i). \tag{2.12}$$

Let $\mathfrak{a}'_n$ be the ideal generated by all the power series $\sum c_\alpha \underline{X}^{\alpha}$ such that $c_\alpha = 0$ for $w(\underline{X}^{\alpha}) < n$. The $\mathfrak{a}'_n$ obviously define the same topology as the $\mathfrak{a}_n$.

§ 3 Left-exact functors

Let $\varphi_1 : M_1 \to M_3$ and $\varphi_2 : M_2 \to M_3$ be maps of sets. We denote the *fibre product* by $M_1 \times_{M_3} M_2$:

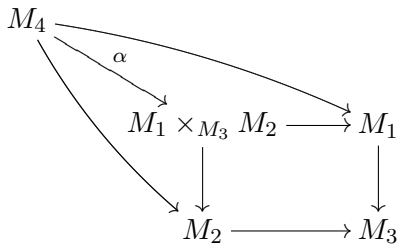
$$M_1 \times_{M_2} M_3 = \{(m_1, m_2) \in M_1 \times M_2 \mid \varphi_1(m_1) = \varphi_2(m_2)\}.$$

This definition extends in an obvious way to other categories (e.g. abelian groups, K-algebras or functors with values in these categories). For example, when the M_i are functors $\mathrm{Nil_K} \to \mathrm{Ens}$, one defines the functor $M_1 \times_{M_3} M_2$ by

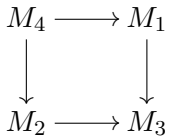
$$(M_1 \times_{M_3} M_2)(\mathscr{N}) = M_1(\mathscr{N}) \times_{M_3(\mathscr{N})} M_2(\mathscr{N}).$$

36 37

The usual universal property is fulfilled: let $\psi_1 : M_4 \to M_1$ and $\psi_2 : M_4 \to M_2$ be morphisms such that $\psi_1\varphi_1 = \psi_2\varphi_2$. Then there exists a uniquely defined morphism $\alpha : M_4 \to M_1 \times_{M_3} M_2$ such that the following diagram is commutative:

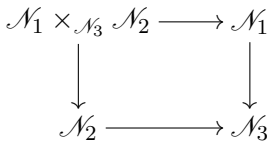


When α is an isomorphism, then we call



a *fibre product diagram*.

We consider a fibre product diagram in $\mathrm{Nil_K}$:



Let $H : \mathrm{Nil_K} \to \mathrm{Ens}$ be a functor. Due to the universality of the fibre product, one obtains a map

$$H(\mathscr{N}_1 \times_{\mathscr{N}_3} \mathscr{N}_2) \longrightarrow H(\mathscr{N}_1) \times_{H(\mathscr{N}_3)} H(\mathscr{N}_2). \tag{2.13}$$

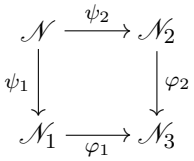
2.14. Definition: A functor is said to be *left-exact* if (2.13) is an isomorphism for all fibre product diagrams and if $H(0) = \{0\}$.

A functor H is said to *commute with finite direct products* if $H(0) = \{0\}$ and (2.13) is an isomorphism for $\mathscr{N}_3 = 0$.

Let $\mathscr{N} \in \mathrm{Nil_K}$ and let $\mathscr{M} \subset \mathscr{N}$ be an ideal, that is, $\mathscr{N} \cdot \mathscr{M} \subset \mathscr{M}$. Then the quotient $\mathscr{N}/\mathscr{M}$ is in a natural way a nilpotent K-algebra.

2.15. Theorem: A functor $H : \mathrm{Nil_K} \to \mathrm{Ens}$ is left-exact if and only if $H(0) = \{0\}$ and H transforms any fibre product diagram

37
38



where φ_1 is a surjection with $\mathscr{N}_1 \operatorname{Ker} \varphi_1 = 0$, into a fibre product diagram. If we assume that H commutes with finite direct products, then it is enough that H respects fibre products of the above form where moreover φ_2 is an isomorphism onto an ideal of $\mathscr{N}_3$.

Proof: The necessity part of the claim is clear. Conversely, let H be a functor which satisfies the sufficient conditions of the claim. We first show that H turns injections into injections. Let $\mathscr{N}_1 \subset \mathscr{N}_2$. One can assume that $\mathscr{N}_1$ is an ideal in $\mathscr{N}_2$. Indeed, each algebra in the following chain is an ideal in its predecessor:

$$\mathscr{N}_2 \supset \mathscr{N}_1 + \mathscr{N}_2\mathscr{N}_1 \supset \mathscr{N}_1 + \mathscr{N}_2\mathscr{N}_1^2 \supset \ldots = \mathscr{N}_1.$$

We assume that $\mathscr{N}_1$ is an ideal in $\mathscr{N}_2$ and we consider the following chain:

$$\mathscr{N}_2 \supset \mathscr{N}_1 + \mathscr{N}_2^2 \supset \mathscr{N}_1 + \mathscr{N}_2^3 \ldots = \mathscr{N}_1 \supset \mathscr{N}_1\mathscr{N}_2 \supset \mathscr{N}_1\mathscr{N}_2^2 \ldots = 0.$$

We denote its terms by $\mathscr{M}_i$:

$$\mathscr{N}_2 = \mathscr{M}_s \supset \mathscr{M}_{s-1} \supset \ldots \supset \mathscr{M}_0 = 0. \tag{2.15.1}$$

Then we have $\mathscr{N}_2\mathscr{M}_i \subset \mathscr{M}_{i-1}$.

We show by induction on s that all the arrows $H(\mathscr{M}_{i-1}) \to H(\mathscr{M}_i)$ are injective. For $i < s$ this holds by the inductive hypothesis. For $i = s$ we consider the fibre product diagram

$$\begin{array}{ccc} H(\mathscr{M}_{s-1}) & \longrightarrow & H(\mathscr{M}_s) \\ \downarrow & & \downarrow \\ H(\mathscr{M}_{s-1}/\mathscr{M}_1) & \longrightarrow & H(\mathscr{M}_s/\mathscr{M}_1). \end{array}$$

As the lower map is injective by the inductive hypothesis, the injectivity of the upper map follows.

We consider a fibre product diagram as in 2.15, where φ_1 is an arbitrary surjection and φ_2 an arbitrary injection. Then H respects such fibre product diagrams. Indeed, as putting fibre product diagrams one after the other produces another such diagram, one can with the above filtrations reduce to the case where $\mathscr{N}_2$ is an ideal in $\mathscr{N}_3$ and $\mathscr{N}_1 \operatorname{Ker} \varphi_1 = 0$.

Assume given a fibre product diagram 2.15, such that φ_2 is injective and φ_1 is arbitrary. We show that it is respected by H. One can assume that $\mathscr{N}_2$ is an ideal in $\mathscr{N}_3$. Then one finds a filtration of $\mathscr{N}_3$ as in (2.15.1), where $\mathscr{N}_2$ appears. We consider the fibre product of this filtration with $\mathscr{N}_1$: 38 39

$$\begin{array}{ccccccccc} & \mathscr{M}'_0 & \subset & \mathscr{M}'_1 & \subset & \cdots & \mathscr{M}'_{s-1} & \subset & \mathscr{M}'_s = \mathscr{N}_1 \\ & \downarrow & & \downarrow & & & \downarrow & & \downarrow \quad \downarrow \\ 0 = & \mathscr{M}_0 & \subset & \mathscr{M}_1 & \subset & \cdots & \mathscr{M}_{s-1} & \subset & \mathscr{M}_s = \mathscr{N}_3. \end{array}$$

We show by induction on s that H turns all the squares into fibre product diagrams. By the inductive hypothesis it is enough to consider the last square. Let $\xi'_s \in H(\mathscr{M}'_s)$, $\xi_{s-1} \in H(\mathscr{M}_{s-1})$ and $\xi_s \in H(\mathscr{M}_s)$ be their common image. We denote by $\overline{\xi}_i$ (resp. $\overline{\xi}'_i$) the images

in $H(\mathscr{M}_i/\mathscr{M}_1)$ (resp. $H(\mathscr{M}'_i/\mathscr{M}'_1)$). By the inductive hypothesis we have a fibre product diagram:

$$\begin{array}{ccc} H(\mathscr{M}'_{s-1}/\mathscr{M}'_1) & \longrightarrow & H(\mathscr{M}'_s/\mathscr{M}'_1) \\ \downarrow & & \downarrow \\ H(\mathscr{M}_{s-1}/\mathscr{M}_1) & \longrightarrow & H(\mathscr{M}_s/\mathscr{M}_1). \end{array}$$

For $s = 2$ we use that H turns injections into injections. We set $\overline{\xi}'_{s-1} = \overline{\xi}_{s-1} \times_{\overline{\xi}_s} \overline{\xi}'_s$. One considers the fibre product diagram

$$\begin{array}{ccc} H(\mathscr{M}'_{s-1}) & \longrightarrow & H(\mathscr{M}'_{s-1}/\mathscr{M}'_1) \\ \downarrow & & \downarrow \\ H(\mathscr{M}'_s) & \longrightarrow & H(\mathscr{M}'_s/\mathscr{M}'_1). \end{array}$$

Let $\xi'_{s-1} = \xi'_s \times_{\overline{\xi}'_s} \overline{\xi}'_{s-1}$. As H respects injections, ξ'_{s-1} is mapped to ξ_{s-1}. It follows that $\xi'_{s-1} = \xi'_s \times_{\xi_s} \xi_{s-1}$ is the desired fibre product.

By considering a chain of the form (2.15.1), one sees by induction on s that $H(\mathscr{N} \times \mathscr{N}_2) \to H(\mathscr{N}) \times H(\mathscr{N}_2)$ is an isomorphism. Indeed, one considers the diagram

$$\begin{array}{ccc} \mathscr{N} \times \mathscr{M}_s & \longrightarrow & \mathscr{N} \times \mathscr{M}_s/\mathscr{M}_0 \\ \downarrow & & \downarrow \\ \mathscr{M}_s & \longrightarrow & \mathscr{M}_s/\mathscr{M}_0. \end{array}$$

Finally, assume given a fibre product diagram as in 2.15, in which φ_1 and φ_2 are arbitrary. Then the following diagram is a fibre product diagram too:

39
40

$$\begin{array}{ccc} \mathscr{N} & \xrightarrow{(\psi_1,\psi_2)} & \mathscr{N}_1 \times \mathscr{N}_2 \\ {\scriptstyle (\psi_1,\psi_2)}\downarrow & & \downarrow \\ \mathscr{N}_1 \times \mathscr{N}_2 & \longrightarrow & \mathscr{N}_1 \times \mathscr{N}_2 \times \mathscr{N}_3 \\ (u_1,u_2) & \longmapsto & (u_1,u_2,\varphi_1(u_1)) \end{array} \qquad \begin{array}{c} (u_1,u_2) \\ \downarrow \\ (u_1,u_2,\varphi_2(u_2)) \end{array}$$

As the arrows in this diagram are injections, H turns it into a fibre product diagram. Because H commutes with finite direct products, it follows easily that H turns also the diagram 2.15 into a fibre product diagram. Thus the theorem is proved.

2.16. Theorem: Let $H : \mathrm{Nil}_K \to \mathrm{Ab}$ be a functor to the category of abelian groups. Then H is left-exact if and only if for each exact sequence in Nil_K:

$$0 \longrightarrow \mathscr{N}_1 \longrightarrow \mathscr{N}_2 \xrightarrow{\pi} \mathscr{N}_3 \longrightarrow 0,$$

the sequence

$$0 \longrightarrow H(\mathscr{N}_1) \longrightarrow H(\mathscr{N}_2) \longrightarrow H(\mathscr{N}_3)$$

is exact.

Proof: If the upper sequence admits a section ($\sigma : \mathscr{N}_3 \to \mathscr{N}_2$, $\pi\sigma = \mathrm{id}$), so does the lower one. It follows that H respects finite direct products. Let

$$\begin{array}{ccc} \mathscr{N} & \longrightarrow & \mathscr{N}_2 \\ \downarrow & & \downarrow \\ \mathscr{N}_1 & \twoheadrightarrow & \mathscr{N}_3 \end{array}$$

be a fibre product diagram, such that $\mathscr{N}_2$ is an ideal of $\mathscr{N}_3$ and that the lower arrow is surjective. Then we have an exact sequence

$$0 \longrightarrow \mathscr{N} \longrightarrow \mathscr{N}_1 \longrightarrow \mathscr{N}_3/\mathscr{N}_2 \longrightarrow 0.$$

We obtain a commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H(\mathscr{N}) & \longrightarrow & H(\mathscr{N}_1) & \longrightarrow & H(\mathscr{N}_3/\mathscr{N}_2) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & H(\mathscr{N}_2) & \longrightarrow & H(\mathscr{N}_3) & \longrightarrow & H(\mathscr{N}_3/\mathscr{N}_2). \end{array}$$

One sees that the first square is a fibre product diagram. Conversely, it is clear that a left-exact functor turns exact sequences into left-exact sequences.

§ 4 Tangent spaces

We can view each K-module M as a nilpotent K-algebra, by setting $M^2 = 0$. One obtains in this way an embedding of the category of K-modules

$$\mathrm{Mod}_K \hookrightarrow \mathrm{Nil_K}\,.$$

2.17. Definition: Let $H : \mathrm{Nil_K} \to \mathrm{Ens}$ be a functor. We call the restriction of H to Mod_K the *tangent functor* t_H.

2.18. Lemma: Let $t : \mathrm{Mod}_K \to \mathrm{Ens}$ be a functor, such that the map $t(M \oplus N) \to t(M) \times t(N)$ is an isomorphism for all $M, N \in \mathrm{Mod}_K$. Then $t(M)$ carries a canonical K-module structure for all M, that is, the functor t factors as

$$t : \mathrm{Mod}_K \longrightarrow \mathrm{Mod}_K \xrightarrow{V} \mathrm{Ens},$$

where V is the functor which maps each module to the underlying set.

Proof: Let $k \in K$. We consider the addition and multiplication-by-k maps:

$$+ : M \oplus M \longrightarrow M, \qquad k : M \longrightarrow M.$$

By applying the functor t, we obtain

$$+ : t(M) \oplus t(M) \longrightarrow t(M), \qquad k : t(M) \longrightarrow t(M).$$

These define a K-module structure on $t(M)$, as is easily seen by expressing the corresponding conditions in terms of commutative diagrams. We remark that the hypothesis implies $t(0) = 0$.

2.19. Remark: Let $t : \mathrm{Mod}_K \to \mathrm{Ab}$ be a functor which satisfies the hypotheses of the lemma. Then we have two additions on $t(M)$: the addition $+$ from the lemma and the addition $+'$ of the abelian group $t(M)$. These both additions coincide. Indeed

$$+ : t(M) \times t(M) \longrightarrow t(M)$$

is a homomorphism of abelian groups. It follows from this that:

$$(a_1 +' a_2) + (b_1 +' b_2) = (a_1 + b_1) +' (a_2 + b_2).$$

We obtain the claim.

Let t be a functor as in 2.18. Each $m \in M$ defines a K-module homomorphism $c_m : K \to M$, $c_m(1) = m$. One obtains a K-module homomorphism:

$$\begin{aligned} M \otimes_K t(K) &\longrightarrow t(M) \\ m \otimes \xi &\longmapsto t(c_m)(\xi). \end{aligned} \tag{2.20}$$

2.21. Theorem: Let $t : \mathrm{Mod}_K \to \mathrm{Mod}_K$ be a right-exact functor which commutes with infinite direct sums. Then (2.20) is an isomorphism.

Proof: The proof is based on a standard trick, with which one compares right-exact functors. Clearly (2.20) is an isomorphism for $M = K$. As the functors on both sides of (2.20) commute with infinite direct sums, we obtain the claim for $M = K^{(I)}$, where I is an index set ($K^{(I)}$ denotes the direct sum of I copies of K). In the general case we find an exact sequence $K^{(I)} \to K^{(J)} \to M \to 0$. One obtains the claim from the following diagram:

41
42

$$\begin{array}{ccccccc} K^{(I)} \otimes_K t(K) & \longrightarrow & K^{(J)} \otimes_K t(K) & \longrightarrow & M \otimes_K t(K) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ t(K^{(I)}) & \longrightarrow & t(K^{(J)}) & \longrightarrow & t(M) & \longrightarrow & 0. \end{array}$$

Let $G : \mathrm{Nil_K} \to \mathrm{Ab}$ be a formal group. Then t_G satisfies the hypotheses of 2.21. Consequently $t_G(K)$ determines the functor t_G.

2.22. Definition: We call $t_G(K)$ the *tangent space* of G.

As t_G is exact, $t_G(K)$ is a flat K-module. If $t_G(K)$ is a finitely generated projective K-module of rank d, we say that G is *finite dimensional of dimension d.*

Let $H : \mathrm{Nil_K} \to \mathrm{Ens}$ be a functor which respects finite direct products. We consider an exact sequence

$$0 \longrightarrow \mathscr{K} \longrightarrow \mathscr{M} \longrightarrow \mathscr{N} \longrightarrow 0$$

such that $\mathscr{M} \cdot \mathscr{K} = 0$. Then the addition defines a morphism in $\mathrm{Nil_K}$:

$$+ : \mathscr{K} \oplus \mathscr{M} \longrightarrow \mathscr{M}.$$

By applying the functor H, we obtain an action of the abelian group $H(\mathscr{K})$ on $H(\mathscr{M})$:

$$H(\mathscr{K}) \times H(\mathscr{M}) \longrightarrow H(\mathscr{M}).$$

When H is a functor to the category of abelian groups, one sees as in 2.19 that this action coincides with the addition in $H(\mathscr{M})$.

We have a fibre product diagram:

$$\begin{array}{ccc} (u,m) & \mathscr{K} \oplus \mathscr{M} & \longrightarrow \mathscr{M} \\ \big\downarrow & \big\downarrow{\scriptstyle \mathrm{pr}} & \big\downarrow{\scriptstyle \pi} \\ m & \mathscr{M} & \xrightarrow{\pi} \mathscr{N}. \end{array}$$

When the functor H is left-exact, we obtain a fibre product diagram

$$\begin{array}{ccc} H(\mathscr{K}) \times H(\mathscr{M}) & \longrightarrow & H(\mathscr{M}) \\ \big\downarrow & & \big\downarrow{\scriptstyle H(\pi)} \\ H(\mathscr{M}) & \longrightarrow & H(\mathscr{N}). \end{array} \tag{2.23}$$

Let $\xi \in H(\mathscr{N})$. We set $H_\xi(\mathscr{M}) = H(\pi)^{-1}(\xi)$. Then (2.23) is a fibre product diagram if and only if for all ξ the following condition is fulfilled.

2.24. Condition: $H(\mathscr{K})$ acts simply transitively on $H_\xi(\mathscr{M})$. That is, for $\xi' \in H_\xi(\mathscr{M})$, the map

$$\begin{aligned} H(\mathscr{K}) &\longrightarrow H_\xi(\mathscr{M}) \\ \eta &\longmapsto \eta + \xi' \end{aligned}$$

is bijective. The set $H_\xi(\mathscr{M})$ can also be empty.

2.25. Exercise: A functor which satisfies Condition 2.24 turns injections into injections. 42 43

2.26. Definition: A functor $H : \mathrm{Nil_K} \to \mathrm{Ens}$ is called *half-exact* if it respects finite direct products and if for all $\xi \in H(\mathscr{N})$, the group $H(\mathscr{K})$ acts transitively on $H_\xi(\mathscr{M})$.

2.27. Exercise: Let $H : \mathrm{Nil_K} \to \mathrm{Ab}$ be a half-exact functor. Let p be a prime number, which is nilpotent in K. Then we have $p^N H(\mathscr{N}) = 0$ for $\mathscr{N} \in \mathrm{Nil_K}$ fixed and N large enough. Thereby we obtain a map $\mathbb{Z}_p \to \mathrm{End}\, H$ to the endomorphism ring of H.

§ 5 Prorepresentability of smooth functors

2.28. Definition: A morphism $H \to G$ of set-valued functors on $\mathrm{Nil_K}$ is called *smooth* if for each surjection $\mathscr{M} \twoheadrightarrow \mathscr{N}$ in $\mathrm{Nil_K}$ the following map is surjective:

$$H(\mathscr{M}) \longrightarrow H(\mathscr{N}) \times_{G(\mathscr{N})} G(\mathscr{M}).$$

For example the canonical morphism $H \to \operatorname{Spf} K$ is smooth if and only if H turns surjections into surjections. In this case we say that H is *smooth*.

We call a surjection $\alpha : \mathscr{M} \twoheadrightarrow \mathscr{N}$ *small* if $\mathscr{M} \cdot \operatorname{Ker} \alpha = 0$. One sees that a morphism is smooth if it satisfies Condition 2.28 for small surjections.

We remark that a smooth functor does not necessarily turn surjections in $\mathrm{Compl_K}$ into surjections.

2.29. Lemma: Let $\varphi : (R, \mathfrak{a}_n) \to (S, \mathfrak{b}_n)$ be a surjection in $\mathrm{Compl_K}$, such that $\varphi(\mathfrak{a}_n)$ is a system of neighborhoods of 0 in S. If H is a smooth, half-exact functor, then $H(\varphi)$ is surjective.

Proof: We need the following property of half-exact functors. Assume given a fibre product diagram:

$$\begin{array}{ccc} \mathscr{N} & \longrightarrow & \mathscr{N}_2 \\ {\scriptstyle\alpha'}\downarrow & & \downarrow{\scriptstyle\alpha} \\ \mathscr{N}_1 & \longrightarrow & \mathscr{N}_3. \end{array}$$

Let the map α be surjective. Then the map $H(\mathscr{N}) \to H(\mathscr{N}_1) \times_{H(\mathscr{N}_3)} H(\mathscr{N}_2)$ is surjective too.

One reduces to the case of a small surjection α. Then α' is a small surjection too, with the same kernel $\mathscr{K}$. Let $\eta \in H(\mathscr{N}_1)$ and $\overline{\eta} \in H(\mathscr{N}_3)$ be its image. We must prove that the following map is surjective:

$$H_\eta(\mathscr{N}) \longrightarrow \eta \times H_{\overline{\eta}}(\mathscr{N}_2) \tag{2.29.1}$$

As H is smooth, we have $H_\eta(\mathscr{N}) \neq \emptyset$. As H is half-exact, $H(\mathscr{K})$ acts transitively on both sets. Hence (2.29.1) is surjective.

43 44 Now we show that $H(\varphi)$ is surjective. Clearly, one can assume that $\varphi(\mathfrak{a}_n) = \mathfrak{b}_n$. Let $\eta \in H(S)$ and let η_n be its image in $H(S/\mathfrak{b}_n)$. We construct by induction on n an inverse image $\xi_n \in H(R/\mathfrak{a}_n)$ of η_n, such that ξ_n is mapped to ξ_{n-1} by $H(R/\mathfrak{a}_n) \to H(R/\mathfrak{a}_{n-1})$. Let $S = R/I$. We consider the diagram

$$\begin{array}{ccc} R/\mathfrak{a}_{n+1} & \longrightarrow & R/I + \mathfrak{a}_{n+1} = S/\mathfrak{b}_{n+1} \\ \downarrow & & \downarrow \\ R/\mathfrak{a}_n & \longrightarrow & R/I + \mathfrak{a}_n = S/\mathfrak{b}_n \end{array}$$

One checks that the map $R/\mathfrak{a}_{n+1} \to R/\mathfrak{a}_n \times_{S/\mathfrak{b}_n} S/\mathfrak{b}_{n+1}$ is surjective. Due to the hypotheses on H, we obtain a surjection $H(R/\mathfrak{a}_{n+1}) \to H(R/\mathfrak{a}_n) \times_{H(S/\mathfrak{b}_n)} H(S/\mathfrak{b}_{n+1})$. We choose for ξ_{n+1} an inverse image of $\xi_n \times_{\eta_n} \eta_{n+1}$. Q.E.D.

The following theorem is a generalization of 1.4.

2.30. Theorem: Let $\alpha : H \to G$ be a morphism of set-valued functors on $\mathrm{Nil_K}$, which induces an isomorphism of the tangent functors $t_H \to t_G$. Then α is an isomorphism if the following conditions are fulfilled:

1) H is half-exact and G is left-exact.

2) H is smooth or α is smooth.

Proof: Let $\mathscr{N} \in \mathrm{Nil_K}$. One finds a sequence of small surjections $\mathscr{N} \twoheadrightarrow \mathscr{M}_1 \twoheadrightarrow \ldots \twoheadrightarrow \mathscr{M}_k = 0$. We prove by induction on k that $H(\mathscr{N}) \to G(\mathscr{N})$ is an isomorphism. Let $\mathscr{N}_1$ be the kernel of $\mathscr{N} \to \mathscr{M}_1$. We consider the diagram

$$\begin{array}{ccc} H(\mathscr{N}) & \longrightarrow & H(\mathscr{M}_1) \\ \downarrow & & \downarrow \wr \ \alpha_{\mathscr{M}_1} \\ G(\mathscr{N}) & \longrightarrow & G(\mathscr{M}_1). \end{array}$$

By the inductive hypothesis, $\alpha_{\mathscr{M}_1}$ is an isomorphism.
Let $\eta \in H(\mathscr{M}_1)$ and ξ be its image in $G(\mathscr{M}_1)$. It is enough to prove that

$$H_\eta(\mathscr{N}) \longrightarrow G_\xi(\mathscr{N})$$

is an isomorphism. By the first condition, the group $H(\mathscr{N}_1) \simeq G(\mathscr{N}_1)$ acts transitively on $H_\eta(\mathscr{N})$ and simply transitively on $G_\xi(\mathscr{N})$. The claim follows from this, except in the case where $H_\eta(\mathscr{N}) = \emptyset$ and $G_\xi(\mathscr{N}) \neq \emptyset$. The second condition excludes this possibility.

2.31. Theorem: Let $H : \mathrm{Nil_K} \to \mathrm{Ens}$ be a functor which satisfies the following conditions.

1) H is left-exact and smooth.

2) t_H commutes with infinite direct sums. [44] [45]

3) $t_H(K)$ is a projective K-module with a countable basis.

Then H is prorepresentable.

Proof: From 2.21 one has an isomorphism

$$t_H(M) = M \otimes_K P = \mathrm{Hom}_{K,\mathrm{cont}}(P^*, M) \tag{2.31.1}$$

where $P = t_H(K)$ and P^* is the dual module of P in the sense of 2.11. With the topology introduced on P^*, $K \oplus P^*$ is an object of $\mathrm{Compl_K}$. By taking inverse limits from (2.31.1), we find a bijection

$$H(K \oplus P^*) = \mathrm{Hom}_{K,\mathrm{cont}}(P^*, P^*).$$

Let $\xi_1 \in H(K \oplus P^*)$ be the element which corresponds to the identity map of P^*. From the Yoneda lemma 2.9, one can view ξ_1 as a morphism:

$$\mathrm{Spf}\ K \oplus P^* \longrightarrow H. \tag{2.31.2}$$

For an $\mathscr{N} \in \mathrm{Nil_K}$ with $\mathscr{N}^2 = 0$, $\xi_{1,\mathscr{N}} : \mathrm{Spf}(K \oplus P^*)(\mathscr{N}) \to H(\mathscr{N})$ is the isomorphism (2.31.1). The map

$$H(S^{\wedge}_{\mathrm{top}}(P^*)) \longrightarrow H(K \oplus P^*)$$

is surjective from 2.29. Let $\xi \in H(S^{\wedge}_{\mathrm{top}}(P^*))$ be an inverse image of ξ_1. It defines a morphism

$$\xi : h_P = \mathrm{Spf}\, S^{\wedge}_{\mathrm{top}}(P^*) \longrightarrow H,$$

which is an isomorphism by 2.30.

2.32. Corollary: Let $H : \mathrm{Nil_K} \to \mathrm{Ab}$ be a formal group. If $H(K)$ is a projective K-module with a countable basis, then H is prorepresentable. If $H(K)$ is a finitely generated, free module, then H is defined by a formal group law.

Proof: The first assertion is clear. If $H(K) = K^n$, then it follows from the proof of 2.31 that $H = h_{K^n}$. One obtains the claim from the considerations at the beginning of this chapter.

2.33. Exercise (Curves lemma): Let $G = \mathrm{Spf}\, K[[X_1, \ldots, X_n]]$ and $H : \mathrm{Nil_K} \to \mathrm{Ens}$ be a functor which commutes with finite, direct sums and which turns injections into injections. Let $\gamma^{(d)}$ be the curve (see 1.21)

$$\gamma_i^{(d)} = T^{c(i)}, \quad \text{where } c(i) = \sum_{k=i-1}^{n-1} d^k.$$

Show that the kernel of the map $\gamma^{(d)} : K[[\underline{X}]] \to K[[T]] \to K[[T]]/(T^{d^{n+1}})$ lies in $(\underline{X})^d$. Conclude to the injectivity of the map

$$H(K[[X]]) \longrightarrow \prod_{\gamma^{(d)}} H(K[[T]]).$$

Thereby one obtains an injection:

$$\mathrm{Hom}(G, H) \longrightarrow \mathrm{Hom}_{\mathrm{Ens}}(G(K[[T]]), H(K[[T]])). \tag{2.33.1}$$

In general this map is injective in the case where $G = h_L$ for a K-module L.

45
46 Let $G : \mathrm{Nil_K} \to \mathrm{Ab}$ be a right-exact functor which commutes with infinite direct sums. Let P be a finitely generated, projective K-module, and $\alpha : P \to t_G(K)$ be a map. Then there exists a morphism $h_P \to G$, which induces α on the tangent spaces. More generally, assume given a family $P_i \xrightarrow{\alpha_i} t_G(K)$, $i \in I$ of such maps. Then there exists a morphism $h_{\oplus P_i} \to G$, which induces α_i on the tangent spaces. Consequently, there is a surjection $h_L \to G$ for an appropriate module L. Therefore (2.33.1) is injective for G.

§ 6 Bigebras

In 1.50, we have associated to each formal group law G a bigebra $\mathbb{H}_G$. The same construction is possible in a more general situation.

Let $H : \mathrm{Nil_K} \to \mathrm{Ab}$ be a functor. We denote by $\underline{H}$ its variety, that is, the underlying set-valued functor. The group structure on $H(\mathscr{N})$ is given by a morphism $(+) : \underline{H} \times \underline{H} \to \underline{H}$.

One can interpret the zero element as a morphism $(0) : \mathrm{Spf}\, K \to \underline{H}$, which maps the unique element of $\mathrm{Spf}\, K$ $(\mathscr{N})$ to the zero element of $H(\mathscr{N})$. Finally, one has the multiplication-by-(-1).

Conversely, let $\underline{H}$ be a set-valued functor which is endowed with morphisms $(+)$, (0) and (-1), such that the following diagrams are commutative:

$$\begin{array}{ccc} \underline{H}\times\underline{H}\times\underline{H} & \xrightarrow{(+)\times\mathrm{id}} & \underline{H}\times\underline{H} \\ {\scriptstyle \mathrm{id}\times(+)}\downarrow & & \downarrow{\scriptstyle (+)} \\ \underline{H}\times\underline{H} & \xrightarrow{(+)} & \underline{H} \end{array} \qquad \begin{array}{ccc} \mathrm{Spf}\, K\times\underline{H} & \xrightarrow{(0)\times\mathrm{id}} & \underline{H}\times\underline{H} \\ & \searrow \quad \swarrow{\scriptstyle (+)} & \\ & \underline{H} & \end{array}$$

$$\begin{array}{ccc} \underline{H} & \xrightarrow{\mathrm{id}\times(-1)} & \underline{H}\times\underline{H} \\ \downarrow & & \downarrow{\scriptstyle (+)} \\ \mathrm{Spf}\, K & \xrightarrow{(0)} & \underline{H} \end{array} \qquad \begin{array}{ccc} \underline{H}\times\underline{H} & \xrightarrow{(+)} & \\ {\scriptstyle p}\downarrow & & \underline{H} \\ \underline{H}\times\underline{H} & \xrightarrow{(+)} & \end{array}$$

Here p denotes the maps that switches the factors. The diagrams express the fact that $\underline{H}(\mathscr{N})$ is an abelian group for the operation $(+)$. Therefore $(\underline{H}, (+), (0), (-1))$ defines a functor $\mathrm{Nil_K} \to \mathrm{Ab}$.

Let $\underline{H} = \mathrm{Spf}\, R$ be prorepresentable. Then we have:

$$\begin{aligned} \underline{H}\times\underline{H}\,(\mathscr{N}) &= \varinjlim(\mathrm{Hom}_{K\text{-Alg}}(R/\mathfrak{a}_n, K\oplus\mathscr{N})\times\mathrm{Hom}_{K\text{-Alg}}(R/\mathfrak{a}_n, K\oplus\mathscr{N})) \\ &= \varinjlim \mathrm{Hom}_{K\text{-Alg}}(R/\mathfrak{a}_n\otimes_K R/\mathfrak{a}_n, K\oplus\mathscr{N}). \end{aligned}$$

The algebra $R\,\widehat{\otimes}_K R = \varprojlim(R/\mathfrak{a}_n\otimes_K R/\mathfrak{a}_n) = \varprojlim R\otimes_K R/\mathfrak{a}_n\otimes R + R\otimes_K \mathfrak{a}_n$ is an object of $\mathrm{Compl_K}$, which prorepresents $\underline{H}\times\underline{H}$. 46 47

The morphisms $(+)$, (0), (-1) define comorphisms

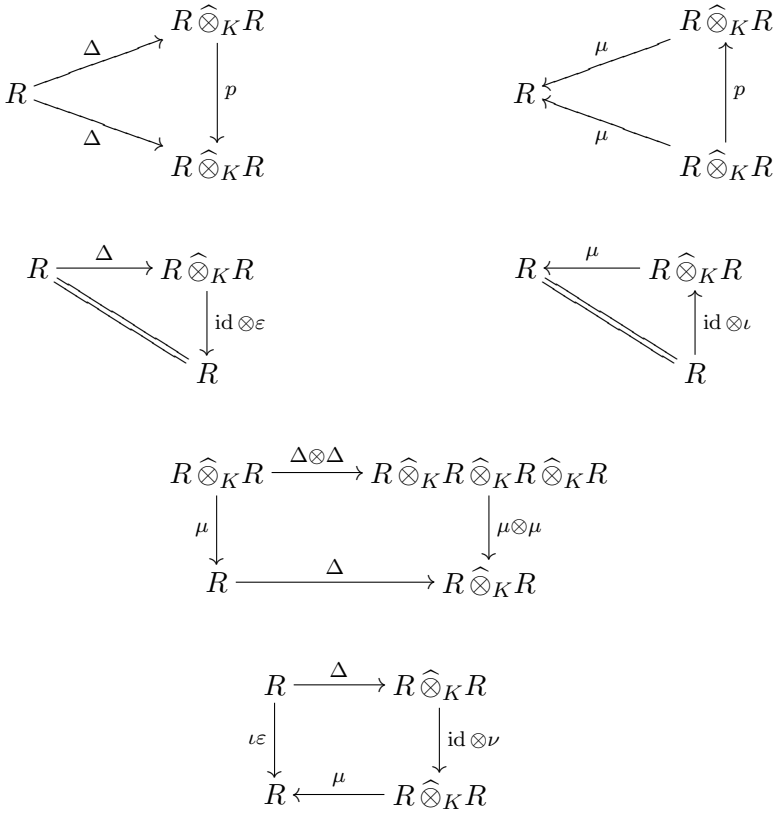
$$\Delta : R \longrightarrow R\,\widehat{\otimes}_K R, \quad \varepsilon : R \longrightarrow K, \quad \nu : R \longrightarrow R.$$

The K-algebra structure on the K-module R is given by the following maps:

$$\mu : R\,\widehat{\otimes}_K R \longrightarrow R, \qquad \iota : K \longrightarrow R.$$

One obtains the following commutative diagrams:

$$\begin{array}{ccc} R & \xrightarrow{\Delta} & R\,\widehat{\otimes}_K R \\ {\scriptstyle \Delta}\downarrow & & \downarrow{\scriptstyle \mathrm{id}\otimes\Delta} \\ R\,\widehat{\otimes}_K R & \xrightarrow{\Delta\otimes\mathrm{id}} & R\,\widehat{\otimes}_K R\,\widehat{\otimes}_K R \end{array} \qquad \begin{array}{ccc} R & \xleftarrow{\mu} & R\,\widehat{\otimes}_K R \\ {\scriptstyle \mu}\uparrow & & \uparrow{\scriptstyle id\otimes\mu} \\ R\,\widehat{\otimes}_K R & \xleftarrow{\mu\otimes\mathrm{id}} & R\,\widehat{\otimes}_K R\,\widehat{\otimes}_K R \end{array}$$



Conversely, let R be a K-module endowed with a filtration by submodules $\mathfrak{a}_n$ such that $R = \varprojlim R/\mathfrak{a}_n$. Assume given morphisms $\Delta, \mu, \varepsilon, \iota, \nu$ such that the above diagrams are commutative. Then $(R, \mathfrak{a}_n)$ with the ring structure μ is an object of $\mathrm{Compl_K}$ and $\mathrm{Spf}\, R$ with the operation $\mathrm{Spf}\, \Delta : \mathrm{Spf}\, R \times \mathrm{Spf}\, R \to \mathrm{Spf}\, R$ is a functor to the category of abelian groups.

Let R be an object of $\mathrm{Compl_K}$, such that for all n, $R/\mathfrak{a}_n$ is a finitely generated projective K-module. Let

$$R^* = \mathrm{Hom}_{K,\mathrm{cont}}(R, K) = \varinjlim \mathrm{Hom}_K(R/\mathfrak{a}_n, K).$$

Then we have:

47 48
$$(R \widehat{\otimes}_K R)^* = \varinjlim \mathrm{Hom}_K(R/\mathfrak{a}_n \otimes_K R/\mathfrak{a}_n, K) = \varinjlim((R/\mathfrak{a}_n)^* \otimes_K (R/\mathfrak{a}_n)^*) = R^* \otimes_K R^*.$$

One obtains a bigebra structure on R^*, which is moreover provided with the additional structure $\nu^* : R^* \to R^*$.

2.34. Remark: Let R be an augmented nilpotent K-algebra. Then we have $R \widehat{\otimes}_K R = R \otimes_K R$. The above diagrams are then self-dual, that is, if one replaces R by R^*, Δ by μ^*, μ by Δ^*, ε by ι^*, ι by ε^* and ν by ν^*, then one obtains the same diagrams as when applying the functor $*$. If the augmentation ideal of R^* is nilpotent again, then $\mathrm{Spf}\, R^*$ defines a functor $\mathrm{Nil_K} \to \mathrm{Ab}$ again, that one calls the *Cartier dual* of $H = \mathrm{Spf}\, R$. The fact that R^* is not necessarily nilpotent can be checked by the reader with the following example.

Let K be a ring of characteristic p, that is, $pK = 0$. The functor

$$\mu_p(\mathscr{N}) = \{x \in (1 + \mathscr{N})^\times \mid x^p = 1\}$$

is represented by the augmented K-algebra $R = K[T]/(T^p - 1)$, where the augmentation is defined by $\varepsilon(T) = 1$. One shows that R^* does not contain any nilpotent element. On the contrary, the following functor admits a Cartier dual in the above sense:

$$\alpha_p(\mathscr{N}) = \{x \in \mathscr{N} \mid x^p = 0\} \subset \mathbb{G}_{\mathrm{a}}(\mathscr{N}).$$

One checks that the dual functor is α_p again. For a treatment of Cartier duality in a more general setting, we refer to Mumford [16].

2.35. Theorem: Let $H : \mathrm{Nil_K} \to \mathrm{Ab}$ be a functor, which is prorepresentable by a complete, augmented K-algebra $(R, \mathfrak{a}_n)$. We assume that the $R/\mathfrak{a}_n$ are finitely generated, projective K-modules. Then one has a canonical exact sequence of functors $\mathrm{Nil_K} \to \mathrm{Ab}$ (see 2.4):

$$0 \longrightarrow H \longrightarrow \mathbb{G}_{\mathrm{m}}R^* \longrightarrow \mathbb{G}_{\mathrm{m}}R^* \otimes_K R^*.$$

Proof: Let A be an augmented nilpotent K-algebra. We have an embedding:

$$H(A^+) = \mathrm{Hom}_{\mathrm{Compl_K}}(R, A) \subset \mathrm{Hom}_{K,\mathrm{cont}}(R, A) = R^* \otimes_K A.$$

Two homomorphisms $\varphi_1, \varphi_2 : R \to A$ can be added when viewed in the group $H(A^+)$ as follows:

$$\varphi_1 +_H \varphi_2 = \mu_A \circ (\varphi_1 \otimes \varphi_2) \circ \Delta : R \longrightarrow R \mathbin{\widehat{\otimes}_K} R \longrightarrow A \mathbin{\widehat{\otimes}_K} A \longrightarrow A.$$

This composition law extends to $\mathrm{Hom}_{K,\mathrm{cont}}(R, A)$ and defines on $R^* \otimes_K A$ the usual multiplication. Indeed, as the composition law is bilinear, one can assume that the φ_i are of the form:

$$\varphi_i(r) = r_i^*(r)a_i, \quad r \in R,\ r_i \in R,\ a_i \in A,\ i = 1, 2.$$

Then we have:

$$\big(\mu_A(\varphi_1 \otimes \varphi_2)\Delta\big)(r) = \langle r_1^* \otimes r_2^*, \Delta(r)\rangle a_1 a_2 = \langle \Delta^*(r_1^* \otimes r_2^*), r\rangle a_1 a_2 = r_1^* r_2^*(r) a_1 a_2 \qquad \begin{matrix}48\\49\end{matrix}$$

where $\langle\ ,\ \rangle$ denotes the canonical pairing $R^* \otimes R \to K$. Thereby we obtain an embedding in the group of units of the K-algebra $R^* \otimes_K A$:

$$H(A^+) \subset (R^* \otimes_K A)^\times.$$

As a $\varphi \in \mathrm{Hom}_{\mathrm{Compl_K}}(R, A)$ respects the augmentation, we have $\varphi = \mathrm{id}_K + \varphi^+ : K \oplus R^+ \to K \oplus A^+$. Thereby we find:

$$H(A^+) \subset (1 + (R^*)^+ \otimes_K A^+)^\times = \mathbb{G}_{\mathrm{m}}R^*(A^+).$$

We want to characterize the elements of $(R^* \otimes_K A)^\times$ which define K-algebra homomorphisms $\varphi : R \to A$, that is, for which the following diagram is commutative:

(2.35.1)
$$\begin{array}{ccc} R & \longrightarrow & A \\ {\scriptstyle\mu}\uparrow & & \uparrow{\scriptstyle\mu_A} \\ R \otimes_K R & \longrightarrow & A \otimes_K A \end{array}$$

We consider the following maps:

$$c_1 = \mu^* \otimes \mathrm{id}_A : R^* \otimes_K A \longrightarrow R^* \otimes_K R^* \otimes_K A,$$

$$\begin{array}{rcl} c_2 : R^* \otimes_K A & \longrightarrow & R^* \otimes_K A \otimes_K R^* \otimes_K A \longrightarrow R^* \otimes_K R^* \otimes_K A \\ x & \longmapsto & x \otimes x. \end{array}$$

When φ corresponds to the element x, then the commutativity of (2.35.1) is equivalent to $c_1(x) = c_2(x)$. The maps c_1, c_2 define homomorphisms of the groups of units of the algebras. This is clear for c_2, and for c_1 this follows from the fact that μ^* is an algebra homomorphism. As c_1 and c_2 turn elements with augmentation 1 into such ones, we obtain an exact sequence

$$0 \longrightarrow H(A^+) \longrightarrow \mathbb{G}_{\mathrm{m}} R^*(A^+) \xrightarrow{c_1 - c_2} \mathbb{G}_{\mathrm{m}} R^* \otimes_K R^*(A^+).$$

2.36. Remark: R^* is flat, as it is the direct limit of the projective modules $(R/\mathfrak{a}_n)^*$. Thereby $\mathbb{G}_{\mathrm{m}} R^*$ and $\mathbb{G}_{\mathrm{m}} R^* \otimes_K R^*$ are formal groups.

Chapter III

The main theorems of Cartier theory

50

§ 1 Elementary symmetric functions

Let us recall the main theorem in the theory of elementary symmetric functions. Let t be an indeterminate over the polynomial ring $\mathbb{Z}[T_1, \ldots, T_n]$. The *elementary symmetric functions* $\sigma_i(T_1, \ldots, T_n) \in \mathbb{Z}[T_1, \ldots, T_n]$ are defined by the following identity:

$$\prod_{i=1}^{n} (1 - T_i t) = 1 - \sigma_1 t + \cdots + (-1)^n \sigma_n t^n. \tag{3.1}$$

Let G denote the permutation group of the set $\{1, \ldots, n\}$. Then G operates as a group of automorphisms on the polynomial ring $\mathbb{Z}[T_1, \ldots, T_n]$:

$$(gf)(T_1, \ldots, T_n) = f(T_{g^{-1}(1)}, \ldots, T_{g^{-1}(n)}), \quad g \in G.$$

The functions σ_i are obviously left-invariant under the operation of G, *i.e.* $g\sigma_i = \sigma_i$.

Let N be an abelian group. We set $N[T_1, \ldots, T_n] = N \otimes_{\mathbb{Z}} \mathbb{Z}[T_1, \ldots, T_n]$. The group G then operates on $N[T_1, \ldots, T_n]$ through the second factor. We denote by $N[T_1, \ldots, T_n]^G$ the subgroup of invariants for this operation.

3.2. Theorem: Let $X_1, \ldots, X_n$ be indeterminates. There is an isomorphism of abelian groups

$$\begin{aligned} N[X_1, \ldots, X_n] &\longrightarrow N[T_1, \ldots, T_n]^G, \\ x_i &\longmapsto \sigma_i. \end{aligned}$$

We defined in (2.12) the weight of a monomial $\underline{X}^\alpha$. Let $N[X_1, \ldots, X_n]_{(m)}$ be the subgroup of $N[\underline{X}]$ spanned by the monomials of weight m and $N[T_1, \ldots, T_n]_m$ the subgroup of $N[\underline{T}]$ consisting of degree m homogeneous polynomials. This yields the graduations:

$$\begin{aligned} N[\underline{X}] &= \sum_{m \geqslant 0} N[\underline{X}]_{(m)}, \\ N[\underline{T}] &= \sum_{m \geqslant 0} N[\underline{T}]_m. \end{aligned}$$

Since the operation of G defined in 3.2 is compatible with these graduations, we have

$$N[\underline{X}]_{(m)} = N[\underline{T}]_m^G.$$

Set $\mathfrak{c}_{(m)} = \sum_{k \geqslant m} N[\underline{X}]_{(k)}$ and $\mathfrak{c}_m = \sum_{k \geqslant m} N[\underline{T}]_m$. We have then an isomorphism

$$N[\underline{X}]/\mathfrak{c}_{(m)} = (N[\underline{T}]/\mathfrak{c}_m)^G. \tag{3.2.1}$$

Let $N[[X_1, \dots, X_n]]$ be the abelian group of power series with coefficients in N. It is easy to see that

50 51
$$N[[\underline{X}]] = N[[\underline{T}]]^G \tag{3.2.2}$$

Let A be an augmented K-algebra whose augmentation ideal is nilpotent. Then $A[[\underline{X}]] = \varprojlim A[\underline{X}]/\mathfrak{c}_m$ is an object in Compl_K. Also, whenever $(R, \mathfrak{a}_m)$ is an object of Compl_K then so is $R[[\underline{X}]]$. Indeed, let $\mathfrak{a}'_m$ be the kernel of the projection

$$R[[\underline{X}]] \longrightarrow (R/\mathfrak{a}_m)[\underline{X}]/(\mathfrak{c}_m).$$

Then $\mathfrak{a}'_m$ is a system of neighbourhoods of 0 in $R[[\underline{X}]]$. Obviously we have $R[[\underline{X}]][[\underline{Y}]] = R[[\underline{X}, \underline{Y}]]$. Let $F : \mathrm{Nil}_K \to \mathrm{Ens}$ be a functor. Since projective limits commute together, we have

$$F(R[[\underline{X}]]) = \varprojlim F((R/\mathfrak{a}_m)[[\underline{X}]]).$$

Let $F : \mathrm{Nil}_K \to \mathrm{Ens}$ be a functor and A an augmented nilpotent K-algebra. We have then a canonical morphism

$$F(A[[\underline{X}]]) \longrightarrow F(A[[\underline{T}]])^G. \tag{3.3}$$

3.4. Condition: For all A, (3.3) is an isomorphism.

By the previous remarks, if this condition holds, it also holds for $A \in \mathrm{Compl}_K$. Condition 3.4 is satisfied, for instance, in the following situations.

3.4.1. Every left-exact functor satisfies Condition 3.4. Indeed, let us consider the following commutative diagram:

$$\begin{array}{ccc} A[\underline{X}]/\mathfrak{c}_{(m)} & \longrightarrow & A[\underline{T}]/\mathfrak{c}_m \\ \downarrow & & \downarrow \Delta \\ A[\underline{T}]/\mathfrak{c}_m & \xrightarrow{\varphi} & \prod_{g \in G} A[\underline{T}]/\mathfrak{c}_m \end{array}$$

where $\Delta(f) = (\dots, f, \dots)$ is the diagonal and $\varphi(f) = (\dots, gf, \dots)$. According to (3.2.1) this is a fibre product diagram. Therefore, an application of the functor F yields

$$F(A[\underline{X}]/\mathfrak{c}_{(m)}) = F(A[\underline{T}]/\mathfrak{c}_m)^G.$$

The conclusion follows by taking limits.

3.4.2. Let M be a K-module. Then 3.4 is satisfied by the functor h_M (*cf* 2.11). Indeed, since $h_M(A[[\underline{X}]]) = (M \otimes_K A)[[\underline{X}]]^+$, the conclusion follows from (3.3).

3.4.3. Exercise: Let $H : \mathrm{Nil}_K \to \mathrm{Ab}$ be a functor that takes an exact sequence $0 \to \mathscr{N}_1 \to \mathscr{N}_2 \to \mathscr{N}_3 \to 0$ where $\mathscr{N}_3^2 = 0$ and $\mathscr{N}_3$ is a free finitely generated K-module, to an exact sequence $0 \to H(\mathscr{N}_1) \to H(\mathscr{N}_2) \to H(\mathscr{N}_3) \to 0$. Show that H satisfies Condition 3.4.

Let $H : \mathrm{Nil}_K \to \mathrm{Ab}$ be a functor satisfying Condition 3.4. We consider the morphisms of algebras

$$u_i^n : K[[X]] \longrightarrow K[[T_1, \ldots, T_n]], \qquad u_i^n(X) = T_i.$$

We obtain a map 51 52

$$u_H^n = \sum H(u_i^n) : H(K[[X]]) \longrightarrow H(K[[\underline{T}]])^G = H(K[[\underline{X}]]).$$

We compute this map for the functor $H = \Lambda$ and the element $1 - Xt \in \Lambda(K[[X]])$ (see chapterII, § 2.1). We have $\Lambda(u_i^n)(1 - Xt) = (1 - T_i t)$ and

$$u_\Lambda^n(1 - Xt) = \prod(1 - T_i t) = 1 - X_1 t + \cdots + (-1)^n X_n t^n.$$

§ 2 The first main theorem of Cartier Theory

3.5. Theorem: Let $H : \mathrm{Nil}_K \to \mathrm{Ab}$ be a functor satisfying Condition 3.4. Then, we have an isomorphism of abelian groups

$$\begin{aligned} \lambda_H : \mathrm{Hom}(\Lambda, H) &\xrightarrow{\sim} H(K[[\underline{X}]]) \\ \Phi &\longmapsto \Phi_{K[[X]]}(1 - Xt). \end{aligned}$$

Proof: It is obvious that λ_H is a group homomorphism. We prove first its injectivity. Let $A = K \oplus \mathscr{N}$ be an augmented nilpotent K-algebra. Let $f \in \Lambda(A) = \Lambda(\mathscr{N})$, $f = 1 + a_1 t + \cdots + a_n t^n$, $a_i \in \mathscr{N}$. We consider the morphisms

$$\begin{aligned} \rho_n^f : K[[X_1, \ldots, X_n]] &\longrightarrow A \\ X_i &\longmapsto (-1)^i a_i. \end{aligned}$$

For each $\Phi : \Lambda \to H$ we get a commutative diagram

$$\begin{array}{ccccc} \Lambda(K[[X]]) & \xrightarrow{u_\Lambda^n} & \Lambda(K[[\underline{X}]]) & \xrightarrow{\Lambda(\rho_n^f)} & \Lambda(A) \\ \downarrow{\scriptstyle \Phi_{K[[X]]}} & & \downarrow{\scriptstyle \Phi_{K[[\underline{X}]]}} & & \downarrow{\scriptstyle \Phi_A} \\ H(K[[X]]) & \xrightarrow{u_H^n} & H(K[[\underline{X}]]) & \xrightarrow{H(\rho_n^f)} & H(A) \end{array}$$

The identity $\Lambda(\rho_n^f) u_\Lambda^n(1 - Xt) = f$ holds. If $\Phi \in \mathrm{Ker}\, \lambda_H$ then $\Phi_{K[[X]]}(1 - Xt) = 0$ and the commutativity yields $\Phi_A(f) = 0$. This proves the injectivity.

Conversely, let $\theta \in H(K[[X]])$. We put $\theta_n = u_H^n(\theta)$ for $n \in \mathbb{N}$. Let $\Phi_A(f) = H(\rho_n^f)(\theta_n)$. The number n is not determined by f, for we did not rule out $a_n = 0$. Let us show the independence of $\Phi_A(f)$ from the chosen value of n.

We consider the commutative diagram:

$$\begin{array}{ccc} K[[X_1,\dots,X_n]] & \xrightarrow{\pi_n} & K[[T_1,\dots,T_{n-1}]] \\ \downarrow & & \downarrow \\ K[[T_1,\dots,T_n]] & \xrightarrow{\pi_n} & K[[T_1,\dots,T_{n-1}]] \end{array}$$

There we have $\pi_n(X_i) = X_i$ for $i < n$ and $\pi_n(X_n) = 0$, the same holds for the T_i. We get

$$\begin{aligned} H(\pi_n)(\theta_n) = H(\pi_n)\left(\sum_{i=1}^{n} H(u_i^n)(\theta)\right) &= \sum_{i=1}^{n} H(\theta_n u_i^n)(\theta) \\ &= \sum_{i=1}^{n-1} H(u_i^{n-1})(\theta) = \theta_{n-1}. \end{aligned}$$

52 53 Hence Φ_A is well-defined and obviously is a morphism of functors. We still have to prove that Φ_A is a morphism of groups.

We now consider the case where $A = K[[\underline{X},\underline{Y}]]$. Let $\xi_n', \xi_n'' \in \Lambda(K[[\underline{X},\underline{Y}]])$ be the elements

$$\xi_n' = 1 - X_1 t + \cdots + (-1)^n X_n t^n, \qquad \xi_n'' = 1 - Y_1 t + \cdots + (-1)^n Y_n t^n.$$

We show that

$$\Phi_K[[\underline{X},\underline{Y}]](\xi_n' + \xi_n'') = \Phi_K[[\underline{X},\underline{Y}]](\xi_n') + \Phi_K[[\underline{X},\underline{Y}]](\xi_n''). \tag{3.5.1}$$

Let $K[[\underline{X},\underline{Y}]] \to K[[\underline{T},\underline{U}]]$ be the morphism given by $X_i \mapsto \sigma_i(T_1,\dots,T_n)$ and $Y_i \mapsto \sigma_i(U_1,\dots,U_n)$. The group $G \times G$ operates on $K[[\underline{T},\underline{U}]]$ by letting the first factor permute the X_i and the second factor the Y_i. We get

$$\begin{aligned} K[[\underline{T},\underline{U}]]^{G\times G} = (K[[\underline{T}]][[\underline{U}]]^{1\times G})^{G\times 1} = K[[\underline{T}]][[\underline{Y}]]^{G\times 1} = K[[\underline{X},\underline{Y}]], \\ H(K[[\underline{X},\underline{Y}]]) = H(K[[\underline{T},\underline{U}]])^{G\times G} \subset H(K[[\underline{T},\underline{U}]]). \end{aligned}$$

It is therefore enough to show that (3.5.1) holds in $K[[\underline{T},\underline{U}]]$.

Let $u_n', u_n'' : K[[\underline{X}]] \to K[[\underline{T},\underline{U}]]$ be the maps $u_i'(X) = T_i$ and $u_i''(X) = U_i$. We get $\Phi_K[[\underline{X},\underline{Y}]](\xi_n') = \sum H(u_i')(\theta)$. Since a similar relation holds for ξ_n'', the right-hand side of (3.5.1) becomes

$$\sum H(u_i')(\theta) + \sum H(u_i'')(\theta) = u_H^{2n}(\theta) = \theta_{2n}.$$

On the other hand the equality $\xi_n' + \xi_n'' = u^{2n}(1 - Xt)$ holds. Thus

$$\Phi_K[[\underline{T},\underline{U}]]u^{2n}(1 - Xt) = u_H^{2n}\Phi_{K[[X]]}(1 - Xt) = u_H^{2n} = \theta_{2n}.$$

and this proves (3.5.1).

Let A be an arbitrary nilpotent augmented K-algebra. We consider two elements $f' = 1 + a'_1 t + \cdots + a'_n t^n$ and $f'' = 1 + a''_1 t + \cdots + a''_n t^n$ of $\Lambda(A)$. Let $\rho : K[[\underline{X}, \underline{Y}]] \to A$ be the morphism defined by $\rho(X_i) = (-1)^i a'_i$, $\rho(Y_i) = (-1)^i a''_i$. Then we have

$$\Phi_A(f') = H(\rho)\Phi_K[[\underline{X}, \underline{Y}]](\xi'_n),$$
$$\Phi_A(f'') = H(\rho)\Phi_K[[\underline{X}, \underline{Y}]](\xi''_n),$$
$$\Phi_A(f' + f'') = H(\rho)\Phi_K[[\underline{X}, \underline{Y}]](\xi'_n + \xi''_n).$$

With (3.5.1), this yields immediately $\Phi_A(f' + f'') = \Phi_A(f') + \Phi_A(f'')$.

§ 3 The Cartier ring

For any ring R, we denote by R^{op} the opposite ring of R. As an abelian group, it is the same as R, but the multiplication is processed the other way around.

3.6. Definition Let $\mathbb{E}_K = (\mathrm{End}\,\Lambda)^{\mathrm{op}}$ be the opposite ring to the endomorphism ring of the functor Λ. We call it the *Cartier ring* of K and denote it shortly by $\mathbb{E}$. According to the first main theorem 3.5, we have a bijection

$$\lambda_\Lambda : \mathbb{E}_K \longrightarrow \Lambda(K[[\underline{X}]]).$$

We consider a base change morphism $K \to K'$ (*cf* 2.9). The correspondence $K \to \mathbb{E}_K$ is functorial. More precisely, we have a commutative diagram

$$\begin{array}{ccc} \mathbb{E}_K & \longrightarrow & \Lambda_K(K[[X]]) \\ \downarrow & & \downarrow \\ \mathbb{E}_{K'} & \longrightarrow & \Lambda_{K'}(K'[[X]]). \end{array}$$

We define the following elements of $\mathbb{E}_K$:

$$V_n = \lambda_\Lambda^{-1}(1 - X^n t), \quad F_n = \lambda_\Lambda^{-1}(1 - Xt^n), \quad \text{for } n \in \mathbb{N}, \tag{3.7}$$
$$[c] = \lambda_\Lambda^{-1}(1 - cXt), \quad \text{for } c \in K.$$

For each functor $H : \mathrm{Nil}_K \to \mathrm{Ab}$ the group $\mathrm{Hom}(\Lambda, H)$ is a right $\mathrm{End}(\Lambda)$-module and a left $\mathbb{E}$-module. When Condition 3.4 is satisfied, we consider on $H(K[[X]])$ the left E-module structure given by λ_H. We denote this module by M_H.

We now consider the following endomorphisms of $K[[X]]$:

$$\phi_n : K[[X]] \longrightarrow K[[X]], \quad n \in \mathbb{N}, \qquad X \longmapsto X^n$$
$$\psi_c : K[[X]] \longrightarrow K[[X]], \quad c \in K. \qquad X \longmapsto cX$$

3.8. Lemma: Let $H : \mathrm{Nil}_K \to \mathrm{Ab}$ be a functor satisfying Condition 3.4. Then the following holds:

$$V_n\gamma = H(\phi_n)\gamma, \qquad [c]\gamma = H(\psi_c)\gamma, \quad \gamma \in H(K[[\underline{X}]]).$$

In particular $V_n[c]F_m = \lambda_\Lambda^{-1}(1 - cX^n t^m)$ holds in the Cartier ring.

Proof: The first main theorem yields a $\Phi \in \mathrm{Hom}(\Lambda, H)$ such that $\Phi_{K[[X]]}(1 - Xt) = \gamma$. Then:

$$\begin{aligned} V_n\gamma &= \Phi_{K[[X]]}(1 - X^n t) = \Phi_{K[[X]]}\Lambda(\phi_n)(1 - Xt) \\ &= H(\phi_n)\Phi_{K[[X]]}(1 - Xt) = H(\phi_n)\gamma \end{aligned}$$

and

$$[c]\gamma = \Phi_{K[[X]]}(1 - cXt) = \Phi_{K[[X]]}\Lambda(\psi_c)(1 - Xt) = H(\psi_c)\gamma.$$

We now consider $H : \mathrm{Nil}_K \to \mathrm{Ab}$ an exact functor. We consider on M_H the descending filtration given by

$$M_H^n = \mathrm{Im}\left(H(X^n K[[X]]) \longrightarrow H(XK[[X]])\right).$$

From the exactness follows the existence of isomorphisms

$$M_H^n/M_H^{n+1} \simeq H\left((X^n K[[X]])/(X^{n+1}K[[X]])\right).$$

3.9. Definition: A *V-reduced Cartier module M* is a left $\mathbb{E}$-module equipped with a filtration by abelian groups

$$\cdots \subset M^n \subset \cdots \subset M^1 = M$$

such that the following conditions hold:

1) $V_m[c]M^n \subset M^{mn}$ for all $m, n \in \mathbb{N}$ and $c \in K$.

1') For all m, n there is a r such that $F_m M^r \subset M^n$.

54 55 2) $V_m : M/M^2 \to M^m/M^{m+1}$ is a bijection.

3) $M = \varprojlim_n M/M^n$.

We see M as a topological module, where M^n is a system of neighborhoods of the origin.

3.10. Example: Let $H : \mathrm{Nil}_K \to \mathrm{Ab}$ be an exact functor. Then M_H is a V-reduced Cartier module. Conditions 1)–3) are obviously fulfilled. We show that Condition 1') holds. For this, we introduce a suitable notation. Let $0 \to \mathscr{N}_1 \to \mathscr{N} \to \mathscr{N}_2 \to 0$ be an exact sequence in Nil_K and $\xi \in H(\mathscr{N})$. We write $\xi = 0 \mod \mathscr{N}_1$ when the image of ξ in $H(\mathscr{N}_2)$ is zero. Let $\theta \in H(K[[X]]^+) = M_H$. Then $\theta = 0 \mod X^r$ means $\theta \in M_H^r$. Let $\rho : K[[X_1, \ldots, X_n]] \to K[[X]]$ be the morphism defined by $\rho(X_i) = 0$ for $i < n$ and $\rho(X_n) = (-1)^{n+1}X$. Let $\Phi : \Lambda \to H$ be the morphism associated to θ by 3.5. By the definition of Φ, we have

$$F_n\theta = \Phi(1 - Xt^n) = H(\rho)u_H^n(\theta).$$

Assume $\theta = 0 \mod X^{mn}$. It is enough to prove that $F_n\theta = 0 \mod X^m$. Let $\tau_{(mn)}$ be the ideal of $K[[\underline{X}]]$ generated by all monomials whose weight is greater than or equal to mn (*cf* 3.2). We see easily that $u_H^n(\theta) = 0 \mod \tau_{(mn)}$. Since ρ induces a morphism $K[[\underline{X}]]/\tau_{(mn)} \to K[[\underline{X}]]/(X^m)$, we have $H(\rho)u_H^n(\theta) = 0 \mod X^m$.

Let M be a V-reduced Cartier module. We consider a system of representatives $\{x_\alpha\}_{\alpha\in M/M^2}$ for M/M^2 in M, *i.e.* $\alpha = x_\alpha \mod M^2$. Since M is complete, each sum similar to $\sum_{n=1}^{\infty} V_n x_{\alpha_n}$ converges.

3.11. Lemma: Each element $x \in M$ admits a unique representation

$$x = \sum_{n=1}^{\infty} V_n x_{\alpha_n}.$$

Proof: We construct iteratively the x_α such that $x - \sum_{n=1}^{m-1} V_n x_{\alpha_n} = y_m \in M^m$. According to 3.9.2)we have a unique representation $y_m = V_m x_{\alpha_m} + y_{m+1}$ with $y_{m+1} \in M^{m+1}$.

We are allowed by 3.5 to identify $\mathbb{E}$ and M_Λ. We put $\mathbb{E}_n = M_\Lambda^n$. Every sum of the following form is convergent:

$$\sum_{n=1}^{\infty} V_n \xi_n, \qquad \xi_n \in \mathbb{E}_n.$$

3.12. Theorem: Each $\xi \in \mathbb{E}$ has a unique representation

$$\xi = \sum_{n,m\geqslant 1} V_n [a_{n,m}] F_m, \qquad a_{n,m} \in K,$$

where for fixed n almost all $a_{n,m}$ vanish. 55 56

Proof: In $\Lambda(XK[[\underline{X}]]/(X^2))$ the identity

$$1 - \sum_{m=1}^{N} a_m X t^m = \prod_{m=1}^{N} (1 - a_m X t^m)$$

holds. Therefore $\{\sum [a_m] F_m \mid a_m \in K\}$ is a system of representatives of M_Λ/M_Λ^2. The claim then follows from 3.11.

In particular, we have:

$$\mathbb{E}_n = \left\{ \sum_{r\geqslant n, s\geqslant 1} V_r [a_{r,s}] F_s \mid a_{r,s} \in K, \quad a_{r,s} = 0 \text{ for } s \gg 0 \text{ and fixed } r \right\}$$

3.13. Theorem: The following identities hold in $\mathbb{E}$:

a) $V_1 = F_1 = 1$,

b) $[c] V_n = V_n [c^n]$ for all $c \in K$,

c) $V_m V_n = V_{mn}$,

d) $[c_1][c_2] = [c_1 c_2]$,

e) $F_n V_n = n$,

f) $F_n[c] = [c^n]F_n$ for all $c \in K$,

g) $F_nF_m = F_{nm}$,

h) $F_nV_m = V_mF_n$ whenever $(n, m) = 1$,

i) there exist polynomials $a_n(X_1, X_2) \in \mathbb{Z}[X_1, X_2]$ such that $[c_1 + c_2] = [c_1] + [c_2] + \sum_{n=2}^{\infty} V_n[a_n(c_1, c_2)]F_n$ for all $c_1, c_2 \in K$.

Proof: Properties a)–d) are a direct consequence of 3.8. In order to prove e)–h), we introduce the morphism $\phi : \mathbb{Z}[X] \to K$, $X \mapsto c$. It induces a morphism of Cartier rings $\mathbb{E}_{\mathbb{Z}[X]} \to \mathbb{E}_K$, $\sum V_n[c_{n,m}]F_m \mapsto \sum V_n\phi[c_{n,m}]F_m$. It is therefore enough to check the relations in $\mathbb{E}_{\mathbb{Z}[X]}$. If we choose an embedding $\mathbb{Z}[X] \to \mathbb{C}$, we see that we can assume that $K = \mathbb{C}$. Let $\zeta_n = e^{2\pi i/n}$. Then we have $(1 - X^nt^n) = \prod_{i=0}^{n-1}(1 - \zeta_n^i Xt)$, that is, $V_nF_n = \sum_{i=0}^{n-1}[\zeta_n^i]$. Furthermore

$$V_nF_nV_n = \sum_{i=0}^{n-1}[\zeta_n^i]V_n = \sum_{i=0}^{n-1}V_n[\zeta_n^{in}] = \sum_{i=0}^{n-1}V_n = nV_n.$$

Since V_n operates injectively in $\mathbb{E}_K = \Lambda(K[[\underline{X}]]^+)$, we get e). But according to d), $[c]$ and $\sum[\zeta_n^i]$ can be permuted, so that

$$V_nF_n[c] = [c]V_nF_n = V_n[c^n]F_n.$$

We thus get f). Relation g) follows from

$$\begin{aligned} V_{mn}F_nF_m &= V_m\sum_{i=0}^{n-1}[\zeta_n^i]F_m = V_mF_m\sum_{i=0}^{n-1}[\zeta_{nm}^i] \\ &= \sum_{k=0}^{m-1}[\zeta_n^k]\sum_{i=0}^{n-1}[\zeta_{nm}^i] = \sum_{r=0}^{mn-1}[\zeta_{mn}^r] \\ &= V_{mn}F_{nm}. \end{aligned}$$

For h) note that if $(n, m) = 1$ then

56 57
$$V_nF_nV_m = \sum_{i=0}^{n-1}[\zeta_n^i]V_m = \sum_{i=0}^{n-1}[\zeta_n^{im}] = \sum_{i=0}^{n-1}V_m[\zeta_n^i] = V_mV_nF_n = V_nV_mF_n.$$

We still need to prove i). By introducing the morphism $\mathbb{Z}[X_1, X_2] \to K$, $X_i \mapsto c_i$, we may assume that $K = \mathbb{Z}[X_1, X_2]$ and $X_i = c_i$. One shows directly that any series $1 + \sum_{i\geqslant 1} a_iT^i \in K[[T]]$ admits a unique decomposition $1 + \sum a_iT^i = \prod(1 - u_iT^i)$, $u_i \in K$. The element $[c_1 + c_2] - [c_1] - [c_2] \in \mathbb{E}$ corresponds to $(1 - (c_1 + c_2)Xt)(1 - c_1Xt)^{-1}(1 - c_2Xt)^{-1}$. It admits a decomposition $\prod_{i\geqslant 2}(1 - a_i(Xt)^i)$ and the $a_i \in \mathbb{Z}[X_1, X_2]$ are the required polynomials.

3.14. Remark: Let Φ_n be the minimal polynomial in $\mathbb{Z}[X]$ of $e^{2\pi i/n}$. We say that K *contains a primitive n-th root of unity* if there is $\zeta_n \in K$ such that $\Phi_n(\zeta_n) = 0$. Then the relation $1 - T^n = \prod_{i\in\mathbb{Z}/n\mathbb{Z}}(1 - \zeta_n^i)$ holds in $K[T]$. Indeed, there is a morphism $\mathbb{Z}[X]/\Phi_n(X) \to K$, $X \mapsto \zeta_n$.

Since we can embed $\mathbb{Z}[X]/\Phi_n(X)$ in $\mathbb{C}$, it is enough, as in the proof of 3.13, to show the relation for $K = \mathbb{C}$. In this case, it is clear that the polynomials on both sides have the same roots.

In the Cartier ring $\mathbb{E}$, this relation is written as

$$\sum_{i=0}^{n-1} [\zeta_n^i] = V_n F_n.$$

We can obviously embed any ring K in a ring K' containing a primitive n-th root of unity. If K has characteristic p, then 1 is a primitive p-th root of unity and in this case we have $V_p F_p = F_p V_p = p$.

3.15. Exercise: a) Let $\mathscr{N} \in \mathrm{Nil}_K$. The Cartier ring $\mathbb{E}$ operates on the right on $\Lambda(\mathscr{N})$. Show that every element of $\Lambda(\mathscr{N})$ has a unique representation

$$\sum_{i=1}^{n}(1 - c_i t^i) = \sum_{i=1}^{n} F_i$$

where the sums are taken in $\Lambda(\mathscr{N})$.

b) Let $\xi = \sum V_s[x_s]$, $F_s \in \mathbb{E}$. Show that ξ is a unit precisely when all the sums $\sum_{sm=1} s x_s^m$ are units in K. For this, compute the operation of ξ on $\Lambda(\mathscr{N})$ when $\mathscr{N}^2 = 0$ and conclude with 2.30.

c) Let M be a V-reduced Cartier module. Show that the multiplication by $[c]$, $c \in K$ defines on M/M^2 a K-module structure. Assume that M/M^2 is a free K-module and let $\{m_i\}_{i\in I}$ be a set of elements of M whose residues modulo M^2 form a basis of M/M^2. We call $\{m_i\}_{i\in I}$ a *V-basis*. Show that each element $m \in M$ has a unique representation 57 58

$$m = \sum_{\substack{r\geqslant 1\\ i\in I}} V_r[c_{r,i}]m_i.$$

d) In the case where K contains all primitive n-th roots of unity, Condition 1') in 3.9 is a consequence of the remaining ones.

§ 4 The reduced tensor product

Let N be a V-reduced Cartier module. From 3.9.1) and 3.9.3) follows that $\mathbb{E}_n M \subset M^n$. We denote by $\overline{\mathbb{E}_n M}$ the topological closure.

3.16. Lemma: We have $\overline{\mathbb{E}_n M} = M^n$ and if M is a finitely generated $\mathbb{E}$-module, we have $\mathbb{E}_n M = M^n$.

Proof: By 3.9.2), each $m_n \in M^n$ has a unique representation $m_n = V_n x_n + m_{n+1}$ with $x_n \in M$ and $m_{n+1} \in M^{n+1}$. We find $m_n = \sum_{r\geqslant n} V_r x_r \in \overline{\mathbb{E}_n M}$. Let $u_1, \ldots, u_n$ be generators of M. We then have $m_n = \sum_j V_n \xi_{n,j} u_j + m_{n+1}$, where $\xi_{n,j} \in \mathbb{E}$, which yields $m_n = \sum_j (\sum_r V_r \xi_{r,j}) u_j \in \mathbb{E}_n M$.

3.17. Remark: The proof also shows that for a finitely generated $\mathbb{E}$-module M, Condition 3.9.1') follows from the three other conditions in 3.9.

Let R be a right $\mathbb{E}$-module. Let $R_s = \{r \in R \mid r\mathbb{E}_s = 0\}$. We denote by $R_s \circ M^s$ the image of $R_s \otimes_{\mathbb{Z}} M^s \to R \otimes_{\mathbb{E}} M$. We then have $R_n \circ M^n \subset R_{n+1} \circ M^{n+1}$. Indeed, using the same notations as in 3.16, we have:

$$r_n \otimes m_n = r_n \otimes (V_n x_n + m_{n+1}) = r_n \otimes m_{n+1}. \tag{3.19}$$

We put $(R \otimes_{\mathbb{E}} M)_\infty = \bigcup_n R_n \circ M^n$.

3.20. Definition: We call *reduced tensor product* the abelian group

$$R \,\overline{\otimes}_{\mathbb{E}}\, M = R \otimes_{\mathbb{E}} M/(R \otimes_{\mathbb{E}} M)_\infty.$$

According to 3.16, we have $R \,\overline{\otimes}_{\mathbb{E}}\, M = R \otimes_{\mathbb{E}} M$ for finitely generated abelian groups. We call R a *torsion right module* when $R_s = R$.

3.21. Theorem: Let $R_1 \to R_2 \to R_3 \to 0$ be an exact sequence of torsion right modules. Then

$$R_1 \,\overline{\otimes}_{\mathbb{E}}\, M \longrightarrow R_2 \,\overline{\otimes}_{\mathbb{E}}\, M \longrightarrow R_3 \,\overline{\otimes}_{\mathbb{E}}\, M \longrightarrow 0$$

is exact again.

Proof: The usual tensor product is right-exact, it is therefore enough to show the surjectivity of the map $(R_2 \otimes_{\mathbb{E}} M)_\infty \to (R_3 \otimes_{\mathbb{E}} M)_\infty$. We take $r_n \otimes m_n \in R_{3,n} \circ M^n$. Then r_n lifts to an element $u_1 \in R_{2,l}$ for some $l \geqslant n$. But 3.19 allows us to assume that $m_n \in M^l$ and the conclusion follows.

58
59

3.22. Theorem: Let $\mathscr{N} \in \mathrm{Nil}_K$. Then $\Lambda(\mathscr{N})$ is a torsion right $\mathbb{E}$-module.

Proof: We choose some s such that $\mathscr{N}^s = 0$. Let $f = 1 + a_1 t + \cdots + a_n t^n \in \Lambda(\mathscr{N})$. By 3.5 an endomorphism $\Phi \in \mathrm{End}\,\Lambda$ corresponds to a polynomial $\theta = 1 + \sum u_i t^i$, where $u_i \in K[[X]]$. The endomorphism Φ belongs to $\mathbb{E}_m$ precisely when $u_i = 0 \mod X^m$. With the same notations as in the proof of 3.5, we have

$$\Phi_{\mathscr{N}}(1 + a_1 t + \cdots a_n t^n) = \Lambda(\rho_n^f) u^n(\theta) = \Lambda(\rho_n^f)\left(\prod_{i=1}^n \theta(T_i)\right).$$

Put $\prod_{i=1}^n \theta(T_i) = 1 + p_1(T_1, \ldots, T_n)t + \cdots + p_N(T_1, \ldots, T_n)t^N$. The p_i are symmetric power series in the T_i. If $\Phi \in \mathbb{E}_m$ then the monomials occurring in the p_i have a degree greater than m. According to (3.2.2) we can also see the p_i as power series in the X_i. Monomials in the X_i occurring in the p_i have a weight greater than m and a degree greater than m/n. It follows that $\rho_n^f(p_i) = 0$ for $m > ns$. We get $\Phi_{\mathscr{N}}(1 + a_1 t^1 + \cdots + a_n t^n) = 0$ for $m \geqslant ns$.

Each V-reduced Cartier module M therefore defines a right-exact functor $\mathrm{Nil}_K \to \mathrm{Ab}$, $\mathscr{N} \mapsto \Lambda(\mathscr{N}) \,\overline{\otimes}_{\mathbb{E}}\, M$. We will determine in the sequel which modules M yield a formal group.

3.23. Examples of reduced tensor products:

a) $\mathbb{E}/\mathbb{E}_n \overline{\otimes}_{\mathbb{E}} M = M/M^n$. Indeed, M^n is obviously contained in the kernel of the surjection $M \to \mathbb{E}/\mathbb{E}_n \overline{\otimes}_{\mathbb{E}} M$, $m \mapsto 1 \otimes m$. By definition, this kernel is generated by all the em such that $e\mathbb{E}_s \subset \mathbb{E}_n$ and $m \in M^s$. We must show that $em \in M^n$. Since $\mathbb{E}_s M$ is dense in M^s, it is enough to show that the operation $e\mathbb{E}_s M \subset M^n$ is continuous, which is obvious.

b) Let $\mathbb{E}^{(I)}$ be a direct sum of some copies of $\mathbb{E}$ and e_i the standard basis of $\mathbb{E}^{(I)}$. When I is infinite, the module $\mathbb{E}^{(I)}$ with the filtration $\mathbb{E}_n^{(I)}$ is not a V-reduced Cartier module, because 3.9.3) is not satisfied. We get a V-reduced Cartier module by taking the completion

$$\widehat{\mathbb{E}^{(I)}} = \varprojlim \mathbb{E}^{(I)}/\mathbb{E}_n^{(I)}.$$

Then $\widehat{\mathbb{E}^{(I)}}$ consists of all sums $\sum_{i\in I} \xi_i e_i$ where $\xi_i \in \mathbb{E}$, such that for each fixed n, almost all of the ξ_i belong to $\mathbb{E}_n$. For each torsion right module we have an isomorphism:

$$\begin{aligned} R \overline{\otimes}_{\mathbb{E}} \widehat{\mathbb{E}^{(I)}} &\xrightarrow{\sim} R^{(I)} \\ \sum r_i \overline{\otimes} e_i &\longleftarrow\!\shortmid (r_i) \\ r \overline{\otimes} \sum \xi_i e_i &\longmapsto (r\xi_i). \end{aligned}$$

59
60

In order to prove that these maps are mutual inverses, it is enough to show that

$$r \overline{\otimes} \sum \xi_i e_i = \sum r\xi_i \overline{\otimes} e_i, \qquad r \in R_n.$$

This equality is clearly true when almost all ξ_i are 0 or when $\xi_i \in \mathbb{E}_n$. Indeed, in the latter case we have $\sum \xi_i e_i \in \widehat{\mathbb{E}_n^{(I)}}$. By the definition of the reduced tensor product, the two sides of the equality are zero. The general case follows.

c) According to a) we have:

$$M/M^2 \simeq \Lambda(XK[[\underline{X}]]/X^2) \overline{\otimes}_{\mathbb{E}} M.$$

Let $\mathscr{N} \in \mathrm{Nil}_K$ with $\mathscr{N}^2 = 0$. If we apply 2.21 to the functor $\mathscr{N} \mapsto \Lambda(\mathscr{N}) \overline{\otimes}_{\mathbb{E}} M$, we obtain a canonical isomorphism

$$\mathscr{N} \otimes_K M/M^2 \xrightarrow{\sim} \Lambda(\mathscr{N}) \overline{\otimes}_{\mathbb{E}} M.$$

In the sequel, we define reduced Tor groups by analogy with the usual Tor groups.

A *morphism of V-reduced $\mathbb{E}$-modules* is a morphism $\phi : N \to M$ of $\mathbb{E}$-modules such that $\phi(M^n) \subset M^n$.

3.24. Lemma: The following conditions for ϕ are equivalent:

(i) ϕ is onto.

(ii) $\phi(N^n) = M^n$.

(iii) $\phi : N/N^2 \to M/M^2$ is onto.

Let L be the kernel of L, with the filtration $L^n = L \cap N^n$. Then L is a V-reduced Cartier module.

Proof: The equivalence of the three conditions follows directly from 3.11. We show that L satisfies Condition 3.9.2), the remaining ones being trivial. We have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L^n/L^{n+1} & \longrightarrow & N^n/N^{n+1} & \longrightarrow & M^n/M^{n+1} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle V_n} & & \downarrow{\scriptstyle V_n} & & \downarrow{\scriptstyle V_n} & & \\ 0 & \longrightarrow & L/L^2 & \longrightarrow & N/N^2 & \longrightarrow & M/M^2 & \longrightarrow & 0 \end{array}$$

The bijectivity of $V_n : L/L^2 \to L^n/L^{n+1}$ follows.

Let M be a V-reduced $\mathbb{E}$-module. We then have a bijection

$$\begin{aligned} \mathrm{Hom}_{\mathbb{E}}(\mathbb{E}^{(I)}, M) &= M^I \\ \phi &\longmapsto \prod_{i \in I} \phi(e_i) \end{aligned}$$

60 61 where M^I stands for the direct product of I copies of M.

We see easily that every V-reduced Cartier module M admits a resolution

$$\cdots \longrightarrow P_r \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0,$$

where $P_i = \widehat{\mathbb{E}^{(I_i)}}$. By a standard result in homological algebra (see [26]) any two resolutions are homotopically equivalent. The following definition is therefore independent of the chosen resolution:

3.25. Definition: Let R be a torsion right $\mathbb{E}$-module and M a V-reduced Cartier module. We define the *reduced* Tor *groups*:

$$\overline{\mathrm{Tor}}_i^{\mathbb{E}}(R, M) = H_i(R \,\overline{\otimes}_{\mathbb{E}}\, P_\bullet).$$

We say that an algebra $\mathscr{N} \in \mathrm{Nil}_K$ is *flat* if it admits a filtration $0 = \mathscr{N}_1 \subset \cdots \subset \mathscr{N}_r = \mathscr{N}$ such that $\mathscr{N}_{i+1}^2 \subset \mathscr{N}_i$ and $\mathscr{N}_{i+1}/\mathscr{N}_i$ is a flat K-module.

3.26. Theorem: Let $\mathscr{N} \in \mathrm{Nil}_K$ and M be a V-reduced Cartier module. If $\mathscr{N}$ is flat or if M/M^2 is a flat K-module, then

$$\overline{\mathrm{Tor}}_i^{\mathbb{E}}(\Lambda(\mathscr{N}), M) = 0 \quad \text{for } i > 0.$$

Proof: We consider an exact sequence of V-reduced Cartier modules

$$0 \longrightarrow L \longrightarrow P \longrightarrow M \longrightarrow 0$$

where $P = \widehat{\mathbb{E}^{(I)}}$. Assume now that $\mathscr{N}^2 = 0$. If we construct the reduced tensor product with $\Lambda(\mathscr{N})$, we obtain by 3.23.c) an exact sequence

$$\mathscr{N} \otimes_K L/L^2 \longrightarrow \mathscr{N} \otimes_K P/P^2 \longrightarrow \mathscr{N} \otimes_K M/M^2 \longrightarrow 0$$

which is also exact on the left if $\mathscr{N}$ is flat or M/M^2 is flat. In theses cases the long homology sequence yields

$$\overline{\mathrm{Tor}}_1^{\mathbb{E}}(\Lambda(\mathscr{N}), M) = 0, \quad \overline{\mathrm{Tor}}_i^{\mathbb{E}}(\Lambda(\mathscr{N}), M) = \overline{\mathrm{Tor}}_{i+1}^{\mathbb{E}}(\Lambda(\mathscr{N}), M)$$

for $i > 1$. If M/M^2 is flat, so is L/L^2 and an induction yields $\overline{\mathrm{Tor}}_i^{\mathbb{E}}(\Lambda(\mathscr{N}), M) = 0$ for $i > 0$.

In the general case, we use a filtration $0 = \mathscr{N}_1 \subset \cdots \subset \mathscr{N}_r = \mathscr{N}$ such that $\mathscr{N}_s^2 \subset \mathscr{N}_{s-1}$. If $\mathscr{N}$ is flat, we may also assume that $\mathscr{N}_s/\mathscr{N}_{s-1}$ is flat. We consider the sequence

$$0 \longrightarrow \Lambda(\mathscr{N}_{s-1}) \longrightarrow \Lambda(\mathscr{N}_s) \longrightarrow \Lambda(\mathscr{N}_s/\mathscr{N}_{s-1}) \longrightarrow 0.$$

After tensoring by M, we get the exact equence

$$\overline{\mathrm{Tor}}_i^{\mathbb{E}}\left(\Lambda(\mathscr{N}_{s-1}), M\right) \longrightarrow \overline{\mathrm{Tor}}_i^{\mathbb{E}}\left(\Lambda(\mathscr{N}_s), M\right) \longrightarrow \overline{\mathrm{Tor}}_i^{\mathbb{E}}\left(\Lambda(\mathscr{N}_s/\mathscr{N}_{s-1}), M\right).$$

By induction, we may assume that the outer terms are 0, and the claim follows.

§ 5 The second main theorem of Cartier theory

3.27. Definition We say that a V-reduced Cartier module M is *V-flat* if M/M^2 is a flat K-module. If M/M^2 is projective and admits a countable system of generators, we say that M is *reduced*. 61 62

3.28. Theorem (second main theorem): A functor $H : \mathrm{Nil}_K \to \mathrm{Ab}$ is isomorphic to a functor of the form $\Lambda(\mathscr{N}) \mathbin{\overline{\otimes}}_{\mathbb{E}} M$ for some V-flat Cartier module M if and only if H is a formal group. If H_1 and H_2 are formal groups and M_1 and M_2 their Cartier modules (see 3.10), then there is a natural bijection

$$\mathrm{Hom}(H_1, H_2) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{E}}(M_1, M_2).$$

Proof: A functor of the form $\mathscr{N} \to \Lambda(\mathscr{N}) \mathbin{\overline{\otimes}}_{\mathbb{E}} M$ commutes to infinite direct sums and is exact by 3.26. It is then a formal group.

Conversely, let H be a formal group. We then have a canonical morphism

$$\Lambda(\mathscr{N}) \otimes_{\mathbb{E}} M_H \longrightarrow H(\mathscr{N}). \tag{3.28.1}$$

Indeed let $f \in \Lambda(\mathscr{N})$ and $m \in M_H$. By 3.5, m defines a morphism $\Phi_m : \Lambda \to H$. The correspondence $f \times m \to \Phi_m(f) \in H(\mathscr{N})$ is $\mathbb{E}$-bilinear since if $e \in \mathbb{E}$ and $\Phi_e : \Lambda \to \Lambda$ is the corresponding morphism, we have by definition $\Phi_m(fe) = \Phi_m \circ \Phi_e(f) = \Phi_{em}(f)$. This yields a map $\Lambda(\mathscr{N}) \otimes_{\mathbb{E}} M_H \to H(\mathscr{N})$. We will now show that it factors through the reduced tensor product, that is, that $f \otimes m$ lies in the kernel of this map when $f \cdot \mathbb{E}_s = 0$ and $m \in M_H^s$.

Indeed, $f \otimes \mathbb{E}_s M_H$ lies obviously in the kernel. Since $\mathbb{E}_s M_H$ is dense in M_H^s, it is enough to show that $f \otimes M_H^r$ is in the kernel for large enough r. Let $f = 1 + a_1 t + \cdots + a_n t^n \in \Lambda(\mathscr{N})$. By definition $\Phi_m(f) = H(\rho_n^f)(u_H^n(m))$ (*cf* 3.5). With the notations of 3.10, for large r the map ρ_n^f factors through

$$K[[X_1, \ldots, X_n]]/\tau_{(r)} \longrightarrow K \oplus \mathscr{N}.$$

If $M = 0 \mod X^r$ then $u_H^n(m) = 0 \mod \tau_r$. We obtain $H(\rho_n^f)(u_H^n(m)) = 0$. Hence (3.28.1) is well-defined.

If $\mathscr{N}^2 = 0$ then (3.28.1) is an isomorphism according to 2.21 and 3.23.c). From the exactness of H follows that M_H/M_H^2 is a flat K-module. Hence the functor on the left-hand side of (3.28.1) is a formal group. With 3.20, we see that (3.28.1) is an isomorphism. The last statement in the theorem is trivial.

The theorem shows that the category of V-flat Cartier modules is equivalent to the category of formal groups.

3.29. Exercise: A functor $H : \mathrm{Nil}_K \to \mathrm{Ab}$ is of the form $\mathscr{N} \mapsto \Lambda(\mathscr{N}) \mathbin{\overline{\otimes}}_E EM$ for some V-reduced Cartier module if and only if it satisfies the following conditions: 62 63

a) H is right-exact and commutes with infinite direct sums.

b) For each exact sequence $0 \longrightarrow \mathscr{N}_1 \longrightarrow \mathscr{N}_2 \longrightarrow \mathscr{N}_3 \longrightarrow 0$ where $\mathscr{N}_3^2 = 0$ and $\mathscr{N}_3$ is a free K-module, $0 \longrightarrow H(\mathscr{N}_1) \longrightarrow H(\mathscr{N}_2) \longrightarrow H(\mathscr{N}_3) \longrightarrow 0$ is exact (*cf* 3.4.3).

Let G be a formal group such that $G(XK[[\underline{X}]]/X^2)$ is a free K-module. Let $m_i \in M_G = G(K[[\underline{X}]]),\ i \in I$ be curves whose residues modulo X^2 form a basis of $M_G/M_G^2 = G(XK[[\underline{X}]]/X^2)$, that is, the m_i form a V-basis of M_G. We can consider m_i as a morphism $m_i : \mathrm{Spf}\, K[[\underline{X}]] \to G$. By 2.30 we get an isomorphism:

$$\begin{aligned} \bigoplus_{i\in I} \mathrm{Spf}\, K[[\underline{X}]] &\longrightarrow G \\ \oplus n_i &\longmapsto \sum m_i(n_i). \end{aligned} \tag{3.30}$$

The functor on the left-hand side of (3.30) is obviously isomorphic to $h_{K^{(I)}}$. Let $p_j : h_{K^{(I)}} \to h_K$ be the canonical projection on the j-th summand. The isomorphism (3.30) can then be written as

$$\sum_{j\in I} m_j p_j : h_{K^{(I)}} \longrightarrow G. \tag{3.30.1}$$

3.31. Definition: We call (3.30.1) the *curvilinear coordinate system relative to the m_i on G*. If we identify the set-valued functor underlying $\mathrm{Var}\, G$ with $h_{K^{(I)}}$, we get

$$\sum m_j p_j = \mathrm{id}_G\,.$$

Chapter IV

Local Cartier theory

64

§ 1 Cartier theory over a $\mathbb{Q}$-algebra

4.1. Theorem: Let K be a $\mathbb{Q}$-algebra. Then there is an isomorphism

$$\Lambda \simeq \bigoplus_{i=1}^{\infty} \mathbb{G}_{\mathrm{a}}.$$

Proof: Let S be a $\mathbb{Q}$-algebra and $x \in S$ a nilpotent element. Define then

$$\exp x = \sum_{i=0}^{\infty} \frac{x^i}{i!}\,, \qquad \log(1-x) = -\sum_{i=1}^{\infty} \frac{x^i}{i}.$$

We consider the algebra $S = K[t] \otimes_K (K \oplus \mathscr{N})$, for $\mathscr{N} \in \mathrm{Nil}_K$. Then $\exp$ and $\log$ define inverse maps

$$(1 \oplus t\,\mathscr{N})^{\times} \underset{\exp}{\overset{\log}{\rightleftarrows}} (t\,\mathscr{N})^{+}\,. \tag{4.1.1}$$

The ring $\mathbb{E}$ acts to the right on the functor Λ. This action extends to $\bigoplus_{i=1}^{\infty} \mathbb{G}_{\mathrm{a}}$. Let $x \in \bigoplus_{i=1}^{\infty} \mathbb{G}_{\mathrm{a}}(\mathscr{N}) = \bigoplus_{i=1}^{\infty} \mathscr{N}$. We denote the i-th component by x_i.

4.2. Corollary: The action of $\mathbb{E}$ on $\bigoplus \mathbb{G}_{\mathrm{a}}$ is as follows:

$$(xV_n)_m = nx_{nm}, \quad (x[c])_m = x_m c^m, \quad (xF_n)_m = \begin{cases} x_{\frac{m}{n}} & \text{if } n \mid m \ (n \text{ divides } m), \\ 0 & \text{otherwise.} \end{cases}$$

Proof: Identifying $\bigoplus \mathbb{G}_{\mathrm{a}}(\mathscr{N})$ with $t\,\mathscr{N}[t]$, represent x as the element $\sum x_i t^i$. Let us prove the first identity. By the first main theorem 3.5, it suffices to verify that

$$\log((1-Xt)V_n) = (\log(1-Xt))V_n.$$

But

$$\log((1-Xt)V_n) = \log(1-X^nt) = -\sum X^{nm}t^m/m$$

and

$$(\log(1-Xt))V_n = \left(-\sum X^m \frac{t^m}{m}\right) V_n = -\sum X^{nm}t^m/m.$$

The remaining verifications are left to the reader.

One sees immediately that $\frac{1}{n}V_nF_n : \bigoplus_{i=1}^{\infty} \mathbb{G}_{\mathrm{a}} \to \bigoplus_{i=1}^{\infty} \mathbb{G}_{\mathrm{a}}$ is the projection onto the summands whose indices are divisible by n.

$$\left(x\,\frac{1}{n}V_nF_n\right)_m = \begin{cases} x_m & \text{if } n \mid m, \\ 0 & \text{if } n \nmid m. \end{cases}$$

The product $\prod \left(1 - \frac{1}{\ell}V_\ell F_\ell\right) = P$ over all prime numbers ℓ converges in the Cartier ring $\mathbb{E}$. It acts on $\bigoplus \mathbb{G}_{\mathrm{a}}$ as projection onto the first factor. We have:

$$\left(x\,\tfrac{1}{n}V_nPF_n\right)_m = \begin{cases} x_n & \text{if } n = m, \\ 0 & \text{otherwise.} \end{cases} \tag{4.3}$$

64
65 **4.4. Definition:** Let M be a left $\mathbb{E}$-module. The elements of the subgroup $PM \subset M$ will be called *typical elements* of M.

An element $m \in M$ is typical precisely when $F_nm = 0$ for $n > 1$. Indeed, let $m \in PM$. For every prime number ℓ, we find that $F_\ell\left(1 - \frac{1}{\ell}V_\ell F_\ell\right) = 0$ and therefore $F_\ell P = 0$. Hence $F_nm = 0$ for $n > 1$. On the other hand, assume that $F_nm = 0$ for $n > 1$. Since P has the form $1 + \sum_{n>1} a_nV_nF_n$, for suitable $a_n \in \mathbb{Z}$, we conclude that $Pm = m$.

From 3.13 it follows that, for $c_1, c_2 \in K$ and $m \in PM$,

$$[c_1]\,m + [c_2]\,m = [c_1 + c_2]\,m.$$

Therefore PM is a K-module.

4.5. Lemma: Let M be a V-reduced $\mathbb{E}$-module. The inclusion $PM \subset M$ induces an isomorphism of K-modules:

$$PM \longrightarrow M/M^2.$$

Proof: We show that M^2 lies in the kernel of the projection $P : M \to PM$. An element $m \in M^2$ can be written in the form $\sum_{n>1} V_nm_n$. Since M is stable under the action of $\mathbb{E}$, it suffices to show that $PV_n = 0$. We are easily reduced to the case where $n = \ell$ is a prime number. Then we get $\left(1 - \frac{1}{\ell}V_\ell F_\ell\right) V_\ell = 0$, hence $PV_\ell = 0$. Clearly $P : M/M^2 \to PM$ is an inverse map.

4.6. Theorem: Let M be a V-reduced $\mathbb{E}$-module. Then every element $m \in M$ has a unique representation

$$m = \sum_{n>0} V_nm_n, \qquad m_n \in PM.$$

Let M_1 and M_2 be V-reduced $\mathbb{E}$-modules and $\overline{\alpha} : M_1/M_1^2 \to M_2/M_2^2$ a K-linear map. Then there is a uniquely determined $\mathbb{E}$-module homomorphism $\alpha : M_1 \to M_2$ inducing $\overline{\alpha}$.

Proof: By 4.3 we have the identity $\sum_{n>0} \frac{1}{n} V_n P F_n = 1$, from which the existence and uniqueness of the desired representation follow. By 4.5 a map induces a K-linear map $\alpha : PM_1 \to PM_2$. Clearly, the required $\mathbb{E}$-module homomorphism is given by $\sum V_n m_n \mapsto \sum V_n \alpha(m_n)$.

4.7. Corollary: Let K be a $\mathbb{Q}$-algebra. The functor $H \mapsto t_H(K)$ is an equivalence of categories between the category of formal groups with the category of flat K-modules. If $t_H(K)$ is a free K-module, then H is isomorphic to a direct sum of copies of $\mathbb{G}_{\mathrm{a}}$.

4.8. Corollary: Let K be a field of characteristic 0. Then every prorepresentable functor $H : \mathrm{Nil}_K \to \mathrm{Ab}$ satisfying the conditions of 2.35 is isomorphic to a direct sum of copies of $\mathbb{G}_{\mathrm{a}}$.

Proof: We have an exact sequence

$$0 \longrightarrow H \longrightarrow H_1 \longrightarrow H_2, \qquad \begin{matrix}65\\66\end{matrix}$$

where H_1 and H_2 are formal groups. By 4.7, the functor H_i is isomorphic to to the functor $\mathscr{N} \mapsto \mathscr{N} \otimes_K t_{H_i}(K)$ and $H_1 \to H_2$ is induced by a homomorphism $t_{H_1}(K) \to t_{H_2}(K)$. Denoting by M the kernel of this homomorphism, we obtain an isomorphism $\mathscr{N} \otimes_K M = H(\mathscr{N})$.

4.9. Exercise: Let $H : \mathrm{Nil}_K \to \mathrm{Ab}$ be a functor satisfying the conditions of 3.29. Then H is isomorphic to a functor of the form $\mathscr{N} \mapsto \mathscr{N} \otimes_K M$, where M is a K-module.

4.10. Exercise: Let H be a formal group and M_H its Cartier module. Show that there is an isomorphism

$$\begin{aligned} \mathrm{Hom}(\mathbb{G}_{\mathrm{a}}, H) &\longrightarrow PM_H = M_H/M_H^2. \\ \Phi &\longmapsto \Phi_{K[[X]]}(X) \end{aligned}$$

For a formal group law H, this is 1.26.

§ 2 p-typical elements

We have seen that the V-reduced Cartier modules over a $\mathbb{Q}$-algebra are rather simple, since in the Cartier ring there are many projectors 4.3. The rest of this chapter is devoted to the following more complicated case, in which however we will still have plenty of projectors. Let $\mathbb{Z}_{(p)}$ be the localization of the integers at the prime ideal $p\mathbb{Z}$. From now on, we assume that K is a $\mathbb{Z}_{(p)}$-algebra.

Let H be a formal group. From 2.30 it follows that the multiplication $n : H \to H$ by an integer prime to p is an isomorphism. Taking $H = \Lambda$, we get that n is a unit in the Cartier ring. Let $\varepsilon_1 = \prod(1 - \frac{1}{\ell} V_\ell F_\ell) \in \mathbb{E}$, where the product runs over all prime numbers $\ell \neq p$. For a prime-to-p integer n, let $\varepsilon_n = \frac{1}{n} V_n \varepsilon_1 F_n \in \mathbb{E}$.

4.11. Lemma: The elements ε_n satisfy the relations $\varepsilon_n^2 = \varepsilon_n$, $\varepsilon_n \varepsilon_m = 0$ for $n \neq m$, and $\sum_{(n,p)=1} \varepsilon_n = 1$.

Proof: Clearly one can reduce to the case $K = \mathbb{Z}_{(p)}$. Since $E_{\mathbb{Z}_{(p)}} \subset E_{\mathbb{Q}}$, we are further reduced to the case $K = \mathbb{Q}$. With notations as in 4.2 we have:

$$(x\varepsilon_n)_m = \begin{cases} x_m & \text{if } m = np^k, \\ 0 & \text{otherwise.} \end{cases} \tag{4.11.1}$$

From this one deduces all the claims of the Lemma.

For any $\mathscr{N} \in \mathrm{Nil}_K$, we get a decomposition

$$\Lambda(\mathscr{N}) = \bigoplus_n \Lambda(\mathscr{N})\varepsilon_n$$

66 67 Indeed, for any $\xi \in \Lambda(\mathscr{N})$ we have $\xi\varepsilon_n = 0$ for large n, since $\Lambda(\mathscr{N})$ is a torsion module. Hence the functor $\Lambda_n(\mathscr{N}) = \Lambda(\mathscr{N})\varepsilon_n$ is a formal group. For Λ_1 we will also use the notation $\widehat{W}$ and call it the *formal group of Witt vectors*.

4.12. Lemma: Left multiplication by V_n induces an isomorphism

$$\begin{aligned} \Lambda_n(\mathscr{N}) &\longrightarrow \widehat{W}(\mathscr{N}) \\ x &\longmapsto xV_n. \end{aligned}$$

Proof: Let $x = y\varepsilon_n$. Then we have

$$y\varepsilon_n V_n = y\frac{1}{n}V_n\varepsilon_1 F_n V_n = yV_n\varepsilon_1 \in \widehat{W}(\mathscr{N}).$$

The inverse map is given by $z \mapsto z\frac{1}{n}F_n$.

We have thus found an isomorphism

$$\Lambda \simeq \bigoplus_{(n,p)=1} \widehat{W}. \tag{4.13}$$

The identity 4.13 transfers to all $\mathbb{E}$-modules.

4.14. Definition and Theorem: Let M be a reduced $\mathbb{E}$-module. The elements of the subgroup $\varepsilon_1 M \subset M$ are called *p-typical*. An element $m \in M$ is p-typical precisely when $F_n m = 0$ for $(n, p) = 1$ and $n > 1$. Every $m \in M$ has a unique decomposition

$$m = \sum_{(n,p)=1} V_n m_n, \qquad \text{where } m_n \text{ is } p\text{-typical.}$$

Proof: Let $\ell \neq p$ be a prime number. Since $F_\ell(1 - \frac{1}{\ell}V_\ell F_\ell) = 0$, it follows that $F_\ell\,\varepsilon_1 = 0$. As a consequence, $F_n m = 0$ for every p-typical element m. Conversely, assume $F_\ell m = 0$. Then $(1 - \frac{1}{\ell}V_\ell F_\ell)m = m$, so $\varepsilon_1 m = m$. The decomposition is obtained by taking $m_n = \frac{1}{n}\varepsilon_1 F_n m$.

§ 3 Local version of the first main theorem

Let H be a formal group. The p-typical elements of $M_H = H(K[[X]])$ will also be called *p-typical curves*. Let $\gamma = (1 - Xt)\varepsilon_1 \in \widehat{W}(K[[X]])$, i.e. γ is the curve corresponding to ε_1 by the first main theorem. Then by definition $\varepsilon_1\gamma = \gamma$.

4.15. Theorem: Let H be a functor for which the first main theorem holds. Then there is an isomorphism

$$\begin{aligned} \operatorname{Hom}(\widehat{W}, H) &\xrightarrow{\sim} \varepsilon_1 H(K[[X]]). \\ \Phi &\longmapsto \Phi_{K[[X]]} \end{aligned}$$

Proof: This follows immediately from the isomorphism

$$\operatorname{Hom}(\Lambda\varepsilon_1, H) \simeq \varepsilon_1 \operatorname{Hom}(\Lambda, H).$$

4.16. Corollary: The endomorphism ring of $\widehat{W}$ is $\varepsilon_1\mathbb{E}\,\varepsilon_1$. Every element of $\varepsilon_1\mathbb{E}\,\varepsilon_1$ admits a unique decomposition

$$\varepsilon_1 \sum_{r,s\geqslant 0} V_{p^r}[x_{r,s}]F_{p^s} = \sum_{r,s\geqslant 0} V_{p^r}[x_{r,s}]F_{p^s}\varepsilon_1 \qquad x_{r,s} \in K, \qquad \frac{67}{68}$$

where for any fixed r almost all $x_{r,s}$ vanish.

Proof: The first statement is trivial. According to 3.13, ε_1 commutes with V_{p^r}, F_{p^s} and $[x]$ for $x \in K$. When n is not a p-power, we have $\varepsilon_1 V_n = F_n\varepsilon_1 = 0$. The existence of the required decomposition follows from 3.12. We show the uniqueness. Let $\xi = \sum V_{p^r}[x_{r,s}]F_{p^s}$. We have to show that $\varepsilon_1\xi = 0$ implies $\xi = 0$. Since the action of V_p on $\mathbb{E}$ is injective, we may assume $\xi \notin M^2$. On the other hand, it follows from $\varepsilon_1\xi = 0$ that

$$\xi = \sum_{\substack{(n,p)=1 \\ n>1}} \varepsilon_n\xi = \sum V_n \frac{1}{n}\varepsilon_1 F_n \in M^2.$$

This contradiction completes the proof.

4.17. Definition and Theorem: We call $\varepsilon_1\mathbb{E}\,\varepsilon_1 =: \mathbb{E}_p$ the *local Cartier ring* corresponding to the prime number p. Set $V = \varepsilon_1 V_p = V_p\,\varepsilon_1$, $F = \varepsilon_1 F_p = F_p\,\varepsilon_1$, $[x]_p = \varepsilon_1[x] = [x]\varepsilon_1$. Then every element in $\mathbb{E}_p$ has a unique decomposition

$$\sum_{r,s\geqslant 0} V^r[x_{r,s}]F^s \qquad x_{r,s} \in K,$$

where for fixed r almost all $x_{r,s}$ vanish. The following relations hold:

$$\begin{aligned} &[1]_p = 1 && FV = p \\ &[x]_pV = V[x^p]_p && F[x]_p = [x^p]_pF \\ &[x]_p[y]_p = [xy]_p && [x+y]_p = [x]_p + [y]_p + \textstyle\sum_{n\geqslant 1} V^n\,[a_{p^n}(x,y)]_p\,F^n \end{aligned}$$

where the a_{p^n} are the polynomials defined by 3.13. When K is a ring of characteristic p, then $VF = FV = p$.

All the claims follow from 3.13. When there is no risk of confusion, we will simply write $[x]$ instead of $[x]_p$.

4.18. Lemma: Let M be a V-reduced Cartier module. Then there is a canonical isomorphism

$$\varepsilon_1 M/V\varepsilon_1 M = M/M^2.$$

Proof: The map $\varepsilon_1 M \to M/M^2$ is surjective, since $\varepsilon_1 m = m \bmod M^2$. Let $\varepsilon_1 m \in M^2$. Then we have a representation

$$\varepsilon_1 m = \sum_{r \geqslant 2} V_r m_r$$

Multiplying this identity by ε_1 we get

$$\varepsilon_1 m = \sum_{n \geqslant 1} V_{p^n} \varepsilon_1 m_{p^n} \in V\varepsilon_1 M.$$

68
69 **4.19. Lemma:** Let $\{m_i\}_{i\in I}$, $m_i \in \varepsilon_1 M$, be a complete set of representatives for $\varepsilon_1 M/V\varepsilon_1 M$. Then every element $m \in \varepsilon_1 M$ has a unique representation

$$m = \sum_{n \geqslant 0} V^n m_{i(n)}.$$

This follows immediately from 3.11 and 4.18.

4.20. Definition: We shall say that an $\mathbb{E}_p$-module M_p is *V-reduced* when

a) $V : M_p \to M_p$ is injective,

b) $M_p = \varprojlim M_p/V^n M_p$.

§ 4 Local version of the second main theorem

4.21. Theorem: Let M be a V-reduced $\mathbb{E}$-module. There is a canonical isomorphism

$$\widehat{W}(\mathscr{N}) \otimes_{\varepsilon_1 \mathbb{E} \varepsilon_1} \varepsilon_1 M \xrightarrow{\sim} \Lambda(\mathscr{N}) \overline{\otimes}_{\mathbb{E}} M.$$

Proof: We shall define a map $\beta : \Lambda(\mathscr{N}) \otimes_{\mathbb{Z}} M \to \widehat{W}(\mathscr{N}) \otimes_{\varepsilon_1 \mathbb{E} \varepsilon_1} \varepsilon_1 M$. According to 4.14, we have a unique decomposition

$$m = \sum_{(n,p)=1} V_n m_n, \qquad m_n \in \varepsilon_1 M.$$

Let $\beta(a \otimes m) = \sum_{(n,p)=1} aV_n\varepsilon_1 \otimes m_n$. The last sum is finite, as $\Lambda(\mathscr{N})$ is a torsion module.

This map vanishes when $a\mathbb{E}_s = 0$ and $m \in M^s$. Indeed $\varepsilon_n\mathbb{E}_s \subset \mathbb{E}_s$ implies that $\varepsilon_n m = V_n m_n \in M^s$. Let r be the smallest integer greater or equal than s/n. Then we have $m_n \in M^r$. From 4.19 we get a representation

$$m_n = \sum_{p^a \geqslant s/n} V_{p^a} m_{n,a} = V_{p^b} m'_n, \qquad p^b \geqslant s/n, \quad m'_n \in \varepsilon_1 M.$$

Therefore $\beta(a \otimes m) = \sum aV_nV_{p^b}\varepsilon_1 \otimes m'_n = 0$.

We prove that β is bilinear. It suffices to show that $\beta(a\xi \otimes V_n m_n) = \beta(a \otimes \xi V_n m_n)$, because for a given ξ and large n both sides vanish. One is easily reduced to the cases $\xi = V_r$, $\xi = [x]$ and $\xi = F_r$. The first two cases are obvious. For the last one we remark that one always has $F_r\varepsilon_1 = \varepsilon_1 F_r \varepsilon_1$. First, let $(r,n) = 1$. Then,

$$\begin{aligned}\beta(aF_r \otimes V_n m_n) &= aF_rV_n\varepsilon_1 \otimes m_n = aV_n\varepsilon_1 F_r\varepsilon_1 \otimes m_n \\ &= aV_n\varepsilon_1 \otimes \varepsilon_1 F_r \varepsilon_1 m_n = \beta(a \otimes V_n F_r m_n) = \beta(a \otimes F_r V_n m_n).\end{aligned}$$

Let r be a divisor of n. We have:

$$\begin{aligned}\beta(aF_r \otimes V_n m_n) &= arV_{n/r}\varepsilon_1 \otimes m_n = aV_{n/r}\varepsilon_1 r\varepsilon_1 \otimes m_n \\ &= aV_{n/r}\varepsilon_1 \otimes rm_n = \beta\left(a \otimes V_{n/r} r m_n\right) = \beta(a \otimes F_r V_n m_n).\end{aligned}$$

69
70

All in all, β defines a map $\overline{\beta} : \Lambda(\mathscr{N}) \overline{\otimes}_{\mathbb{E}} M \to \widehat{W}(\mathscr{N}) \otimes_{\varepsilon_1\mathbb{E}\varepsilon_1} \varepsilon_1 M$. This map is obviously an inverse to the one in the theorem.

4.22. Theorem: The functor $M \mapsto \varepsilon_1 M$ is an equivalence between the category of V-reduced $\mathbb{E}$-modules with the category of V-reduced $\mathbb{E}_p$-modules.

Proof: We shall construct from any V-reduced $\mathbb{E}_p$-module M_p a V-reduced $\mathbb{E}$-module M such that $\varepsilon_1 M = M_p$. To this end, we consider the $\mathbb{E}$-module $\mathbb{E}\varepsilon_1 \otimes_{\varepsilon_1\mathbb{E}\varepsilon_1} M_p$ and equip it with the topology defined by the submodules $\mathbb{E}_n\varepsilon_1 \otimes_{\varepsilon_1\mathbb{E}\varepsilon_1} M_p$. The completion of this module will be denoted by M. Clearly, every element in M can be written uniquely as a convergent series

$$\sum_{(n,p)=1} V_n\varepsilon_1 \otimes m_n, \qquad m_n \in M_p.$$

Let $\{m_i\}_{i\in I}$, $m_i \in M_p$ be a set of representatives for M_p/VM_p. Then any element in M has a unique representation:

$$\sum_r V_r\varepsilon_1 \otimes m_{i(r)} = \sum_{(n,p)=1} V_n\varepsilon_1 \otimes \left(\sum_{s=0}^{\infty} V_{p^s} m_{i(np^s)}\right)$$

From this it follows that M is a V-reduced $\mathbb{E}$-module.

4.23. Theorem: Let $H : \mathrm{Nil}_K \to \mathrm{Ab}$ be a formal group. The p-typical curves $\varepsilon_1 H(K[[X]])$ constitute a V-reduced $\mathbb{E}_p$-module $M_{p,H}$. There is a canonical isomorphism

$$\widehat{W}(\mathscr{N}) \otimes_{\mathbb{E}_p} M_{p,H} \longrightarrow H(\mathscr{N})$$

The functor $H \mapsto M_{p,H}$ is an equivalence between the category of of formal groups with the category of V-reduced $\mathbb{E}_p$-modules such that M_p/VM_p is a flat K-module. The tangent space to H identifies with $M_{p,H}/VM_{p,H}$.

In the following, when working over a $\mathbb{Z}_{(p)}$-algebra K, we shall simply write M_H instead of $M_{p,H}$.

§ 5 The formal group of Witt vectors $\widehat{W}$

We give an alternative description of $\widehat{W}(\mathscr{N})$.

4.24. Lemma: Every element of $\Lambda(\mathscr{N})$ has a unique representation $\prod_{i=1}^{N}\left(1-x_it^i\right)$. Every element of $\widehat{W}(\mathscr{N})$ has a unique representation $\prod_{n=0}^{N}\left(1-y_nt^{p^n}\right)\varepsilon_1$, for $x_i, y_n \in \mathscr{N}$.

70 71 **Proof:** We have the following morphism of set-valued functors on Nil_K:

$$\bigoplus_{i=1}^{\infty}\mathscr{N} \longrightarrow \Lambda(\mathscr{N}), \qquad \oplus n_i \longmapsto \prod\left(1-n_it^i\right).$$

When $\mathscr{N}^2=0$, we have $\prod\left(1-n_it^i\right)=1-\sum n_it^i$. Hence in this case, the morphism is an isomorphism. The general case follows from 2.30. For the proof of the second claim, we may for the same reasons assume that $\mathscr{N}^2=0$. Every element of $\widehat{W}(\mathscr{N})$ can be written as

$$\prod\left(1-x_it^i\right)\varepsilon_1=\prod\left(1-x_it\right)F_i\varepsilon_1=\prod\left(1-x_{p^n}t\right)F_{p^n}\varepsilon_1$$

Let $\prod\left(1-y_nt^{p^n}\right)\varepsilon_1=1$. Since $y_n^2=0$, it follows that $(1-y_nt)F_{p^n}V_m=(1-y_nt)V_mF_{p^n}=(1-y_n^mt)F_{p^n}=1$ for $(m,p)=1$, $m>1$. Therefore $\left(1-y_nt^{p^n}\right)\varepsilon_m=1$. Since $\sum\varepsilon_m=1$, we conclude that $\prod\left(1-y_nt^{p^n}\right)=1$, whence $y_n=0$.

One calls (x_i) (resp. (y_n)) the *Witt vector* corresponding to the element of $\Lambda(\mathscr{N})$ (resp. of $\widehat{W}(\mathscr{N})$).

We define the following *Witt polynomials*:

$$u_m(X_1,\dots,X_m)=\sum_{r|m}\frac{m}{r}X_{m/r}^r, \qquad w_n(X_0,\dots,X_n)=\sum_{s=0}^{n}p^{n-s}X_{n-s}^{p^s}=u_{p^n}.$$

4.25. Theorem: The polynomials u_m and w_n define homomorphisms of functors

$$\begin{aligned}\Lambda(\mathscr{N}) &\longrightarrow \bigoplus_{m=1}^{\infty}\mathbb{G}_{\mathrm{a}}(\mathscr{N}).\\ \prod\left(1-x_it^i\right) &\longmapsto u_m(x_1,\dots,x_m)\end{aligned} \tag{4.25.1}$$

$$\begin{aligned}\widehat{W}(\mathscr{N}) &\longrightarrow \bigoplus_{m=1}^{\infty}\mathbb{G}_{\mathrm{a}}(\mathscr{N}).\\ \prod\left(1-y_nt^{p^n}\right)\varepsilon_1 &\longmapsto w_n(y_0,\dots,y_n)\end{aligned} \tag{4.25.2}$$

Proof: First, we consider the case where K is a $\mathbb{Q}$-algebra. Then the first morphism is a slight modification of (4.1.1). Indeed:

$$\log \prod \left(1 - x_i t^i\right) = \sum_i \left(1 - x_i t^i\right) = -\sum_i \sum_r \frac{x_i^r t^{ir}}{r} = -\sum_m \sum_{r|m} \frac{x_{m/r}^r t^m}{r}.$$

This shows that (4.25.1) is a group homomorphism. According to (4.11.1), ε_1 induces on the right-hand side of (4.25.1) the projection onto those summands whose index is a p-power. From this, it follows that (4.25.2) is a group homomorphism. For the general case, let us consider the ring $\mathbb{Z}[X_n]_{n\in\mathscr{N}}$ with the canonical augmentation ideal $\mathfrak{a}$. For large r, we have a surjection $\mathfrak{a}/\mathfrak{a}^r \to \mathscr{N}$. In this way, one may reduce to the case where $K = \mathbb{Z}$ and $\mathscr{N}$ is torsion-free, i.e. $\mathscr{N} \subset \mathscr{N} \otimes \mathbb{Q}$. From this last inclusion, one can immediately reduce to the case $K = \mathbb{Q}$. 71 72

4.26. Remark: Over a $\mathbb{Q}$-algebra, (4.25.1) and (4.25.2) are isomorphisms of functors. The fact that these are group homomorphisms commuting with base change determines uniquely the group structure on $\Lambda(\mathscr{N})$ and $\widehat{W}(\mathscr{N})$. The $\mathbb{E}$- (resp. $\mathbb{E}_p$-)module structure on $\Lambda(\mathscr{N})$ (resp. $\widehat{W}(\mathscr{N})$) is similarly determined, due to the following theorem.

4.27. Theorem: Let $\xi \in \Lambda(\mathscr{N})$ (resp. $\xi \in \widehat{W}(\mathscr{N})$) and $x = (x_i)$ (resp. $y = (y_n)$) the corresponding Witt vector. Denoting the Witt vector corresponding to ξe, for $e \in \mathbb{E}$ (resp. $e \in \mathbb{E}_p$), by xe (resp. ye), the following relations hold:

$$u_m(x[c]) = u_m(x)c^m, \qquad w_m(y[c]) = w_m(y)c^{p^m},$$
$$u_m(xV_n) = u_{mn}(x), \qquad w_m(yV) = w_{m+1}(y),$$
$$u_m(xF_n) = \begin{cases} pu_{m/n}(x) \text{ if } n \mid m \\ 0 \qquad\quad \text{otherwise,} \end{cases} \qquad w_m(yF) = pw_{m-1}(y),$$

where $c \in K$ and $w_{-1} = 0$. Furthermore

$$(y_0, \dots, y_n, \dots)[c] = (y_0 c, \dots, y_n c^{p^n}, \dots)$$
$$(y_0, \dots, y_n, \dots)F = (0, y_0, \dots, y_n, \dots)$$

and, if the ring K has characteristic p,

$$(y_0, \dots, y_n, \dots)V = (y_0^p, \dots, y_n^p, \dots).$$

Proof: To prove the relations for the u_m, one is quickly reduced to the case where K is a $\mathbb{Q}$-algebra. Then the relations follow immediately from 4.2. The relations for the w_m follow immediately from the following commutative diagram:

$$\begin{array}{ccc} \Lambda(\mathscr{N}) & \xrightarrow{u} & \bigoplus \mathbb{G}_{\mathrm{a}}(\mathscr{N}) \\ \downarrow & & \downarrow{\scriptstyle \varepsilon_1} \\ \widehat{W}(\mathscr{N}) & \xrightarrow{w} & \bigoplus \mathbb{G}_{\mathrm{a}}(\mathscr{N}) \end{array}$$

Here the ε_1 to the right is the projection onto those summands whose index is a p-power.

We prove now the last three identities. For the first two, we may again assume that K is a $\mathbb{Q}$-algebra. As (4.25.2) is an isomorphism, it suffices to check that

72 73
$$w_m(yF) = w_m(0, y_0, \dots, y_n, \dots), \qquad w_m(y[c]) = w_m\left(y_0 c, \dots, y_n c^{p^n}, \dots\right).$$

This is trivial. In order to prove the last identity, consider the ring of polynomials $\mathbb{Z}[Y_0, \dots, Y_n, \dots]$. Let $\mathfrak{a}$ be ideal generated by the Y_i. For a sufficiently large integer M we have a homomorphism $\mathfrak{a}/\mathfrak{a}^M \to \mathscr{N}$, $Y_n \mapsto y_n$. Let

$$(Y_0, \dots, Y_n, \dots)\, V = (P_0, \dots, P_n, \dots), \qquad P_n \in \mathfrak{a}/\mathfrak{a}^M.$$

We must prove that $P_i = Y_i^p \bmod p$. Assume that this is proved for $i < m$. Then for $i < m$ we get that

$$p^i P_i^{p^{m-i}} = p^i Y_i^{p^{m-i+1}} \mod p^{m+1}.$$

The relation $w_m(YV) = w_{m+1}(Y)$ yields

$$(Y_0^{p^{m+1}} + pY_1^{p^m} + \dots) + p^m Y_m^p + p^{m+1} Y_{m+1} = (P_0^{p^m} + pP_1^{p^{m-1}} + \dots) + p^m P_m$$

Since the terms in brackets are equal modulo p^{m+1}, the claim follows.

§ 6 The Witt ring

We use remark 4.26 to define Witt vectors $W(K)$ for an arbitrary ring K. Analogous considerations could be made for the functor Λ.

4.28. Definition and Theorem: There exists a functor from the category of commutative rings to itself $W : \mathrm{Rings} \to \mathrm{Rings}$ uniquely characterised by the following properties.

a) There is an isomorphism as set-valued functors

$$W(K) = \bigoplus_{n=0}^{\infty} K.$$

In this way one can describe elements in $W(K)$ as vectors (a_n), $a_n \in K$.

b) The following map is a ring homomorphism:

$$\begin{aligned} W(K) &\longrightarrow \bigoplus_{n=0}^{\infty} K. \\ (a_n) &\longmapsto (w_n(a_0, \dots, a_n)) \end{aligned}$$

4.29. Remark: From the definition of the w_n it is clear that, over the ring $\mathbb{Z}[1/p]$, the X_n can be written as polynomials in the w_n. Thus, over a $\mathbb{Z}[1/p]$-algebra K, the map in b) above an isomorphism. The existence and uniqueness of $W(K)$ is therefore clear in this case. For

later applications, it is useful to compute the first components of the vectors $(a_n) + (b_n)$ and $(a_n)(b_n)$ on the basis of these considerations.

The proof of the Theorem rests on the following lemma:

4.30. Lemma: Let $\Phi \in \mathbb{Z}[X, Y]$ be a polynomial. Then there exist uniquely determined polynomials 73 74

$$\varphi_0(X_0, X_0'), \ldots, \varphi_n(X_0, \ldots, X_n, X_0', \ldots, X_n'), \ldots \in \mathbb{Z}[X_0, X_0', X_1, X_1', \ldots]$$

such that

$$\Phi\left(w_n(X_0, \ldots, X_n), w_n(X_0', \ldots, X_n')\right) = w_n\left(\varphi_0(X_0, X_0'), \ldots, \varphi_n(X_0, \ldots, X_n, X_0', \ldots, X_n')\right).$$

Proof: Denote by φ the vector $(\varphi_0, \ldots, \varphi_n, \ldots)$, by φ^p the vector $(\varphi_0^p, \ldots, \varphi_n^p, \ldots)$ and so on. We have

$$\Phi\left(w_n(\underline{X}), w_n(\underline{X}')\right) = w_n(\varphi) = p^n\varphi_n + w_{n-1}(\varphi^p).$$

Therefore, over the ring $\mathbb{Z}[1/p]$, the following recursive formula holds:

$$\varphi_n = \frac{1}{p^n}\left(\Phi\left(w_n(\underline{X}), w_n(\underline{X}')\right) - w_{n-1}(\varphi^p)\right).$$

This proves the uniqueness of the φ_n. It only remains to check that their coefficients are integers, namely:

$$\Phi\left(w_n(\underline{X}), w_n(\underline{X}')\right) = w_{n-1}(\varphi^p) \mod p^n.$$

Since $w_n(\underline{X}) = p^n X_n + w_{n-1}(\underline{X}^p) \mod p^n$, the last congruence is equivalent to

$$\Phi\left(w_{n-1}(\underline{X}^p), w_n(\underline{X}'^p)\right) = w_{n-1}(\varphi^p) \mod p^n.$$

Since we may assume by induction hypothesis that $\varphi_i(\underline{X}, \underline{X}')$ has integer coefficients for $i < n$, it follows that

$$\varphi_i(\underline{X}^p, \underline{X}'^p) = \varphi_i^p(\underline{X}, \underline{X}') \mod p.$$

From the form of the Witt polynomials, it follows immediately that

$$w_{n-1}(\varphi^p) = w_{n-1}\left(\varphi(\underline{X}^p, \underline{X}'^p)\right) \mod p^n.$$

The right-hand side of this identity is by construction

$$\Phi\left(w_{n-1}(\underline{X}^p), w_n(\underline{X}'^p)\right). \qquad \text{Q.E.D.}$$

Proof of 4.28: Applying 4.30 to $\Phi = X + Y$ and $\Phi = XY$ yields polynomials

$$S_0(X_0, X_0'), \ldots, S_n(X_0, \ldots, X_n, X_0', \ldots, X_n'), \ldots$$

and

$$P_0(X_0, X_0'), \ldots, P_n(X_0, \ldots, X_n, X_0', \ldots, X_n'), \ldots$$

The addition and multiplication of two vectors in $W(K)$ are defined as follows:

$$(a_n) + (a'_n) = \big(S_0(a_0, a'_0), \dots, S_n(a_0, \dots, a_n, a'_0, \dots, a'_n), \dots\big)$$
$$(a_n)(a'_n) = \big(P_0(a_0, a'_0), \dots, P_n(a_0, \dots, a_n, a'_0, \dots, a'_n), \dots\big)\,.$$

As in the proof of 4.26, we see that every ring K is a homomorphic image of a torsion-free ring K'. Thus, in order to check that the definitions above define a ring structure, it suffices to do so in the case where K is a $\mathbb{Q}$-algebra. Since in this case the map defined by 4.28.a) is an isomorphism, the claim follows. The same kind of argument can be used to prove the uniqueness.

4.31. Exercise: Let A be a ring without zero-divisors and $\pi \in A$ an element such that $A/\pi = \mathbb{F}_q$ is the finite field with $q = p^a$ elements. By analogy with the polynomials w_n, define

$$\begin{aligned}
\omega_0 &= X_0 \\
\omega_1 &= X_0^q + \pi X_1 \\
&\vdots \\
\omega_n &= X_0^{q^n} + \pi X_1^{q^{n-1}} + \dots + \pi^n X_n.
\end{aligned}$$

One shows that for any polynomial $\Phi \in A[X, Y]$, a result analogous to Lemma 4.30 holds. Consequently, there exists a functor from the category of A-algebras to itself $W_{A,\pi} : A\text{-Alg} \to A\text{-Alg}$ such that $W_{A,\pi}(K) = \prod_{n=0}^{\infty} K$ as a set-valued functor and such that the ω_n define a ring homomorphism $W_{A,\pi}(K) \to \prod_{n=0}^{\infty} K$.

4.32. Corollary: The map

$$\begin{aligned}
\widehat{W}(\mathscr{N}) &\longrightarrow W(\mathscr{N}) \\
\prod_{n=0}^{N} \left(1 - c_n t^{p^n}\right) \varepsilon_1 &\longmapsto (c_0, \dots, c_N, \dots)
\end{aligned}$$

is a homomorphism of abelian groups.

Proof: When $\mathscr{N}$ is a $\mathbb{Z}[1/p]$-algebra, via the w_n, we may identify this map with

$$\bigoplus \mathscr{N} \longrightarrow \prod \mathscr{N}.$$

The general case follows as in 4.25.

4.33. Corollary: The set of all elements of the form $\sum V^n[a_n]F^n$, $a_n \in K$, defines a subring of the Cartier ring $\mathbb{E}_p$. The map

$$\begin{aligned}
W(K) &\longrightarrow \mathbb{E}_p \\
(a_0, \dots, a_n, \dots) &\longmapsto \sum V^n[a_n]F^n
\end{aligned}$$

is an isomorphism onto this subring.

Proof: The first claim follows immediately from 4.17. We get an action of $\mathbb{E}_p$ on the tangent space to W:

$$W\left(XK[[X]]/X^2\right) = \mathbb{E}_p/V\mathbb{E}_p.$$

An element of this tangent space has a unique representation $\sum[c_i]F^i$. We compute this action:

$$\begin{aligned}\left(\sum[c_i]F^i\right)\left(\sum V^n[a_n]F^n\right) &= \sum_i \sum_{n\leqslant i}[c_i]p^nF^{i-n}[a_n]F^n \\ &= \sum_i \left[c_i\left(\sum p^n a^{p^{i-n}}\right)\right]F^i \\ &= \sum_i \left[c_i w_i(a_0,\dots,a_i)\right]F^i \mod V\mathbb{E}_p.\end{aligned}$$

75 76

From this it follows that the map $\sum V^n[a_n]F^n \mapsto (w_0(a_0),\dots,w_i(a_0,\dots,a_i),\dots)$ is a homomorphism to the ring $\prod_{n=0}^{\infty} K$. The claim now follows by functoriality and from 4.28.

§ 7 The universality of Witt vectors

Originally, the Witt polynomials were introduced in order to describe unramified extensions of $\mathbb{Z}_p$. We would like to quickly survey this theme, although it will not be needed in the sequel.

Let K be a ring of characteristic p. The Frobenius Frob_K is the ring homomorphism $c \mapsto c^p$, $c \in K$. When Frob_K is an isomorphism, the ring K is said to be *perfect*.

Let A be a commutative ring with unity and let $\mathfrak{a}$ be an ideal of A such that the residue class ring $A/\mathfrak{a} = K$ is perfect. We assume that there exists an integer n such that, for all $a \in \mathfrak{a}$ and $0 \leqslant i \leqslant n$

$$p^i a^{p^{n-i}} = 0.$$

We shall define a multiplicative map $t : K \to A$, i.e. $t(c_1t(c_2 = t(c_1c_2$. Since K is perfect, any element $c \in K$ can be seen as a p^n-th root. Let $x^{p^n} = c$ and $u \in A$ a lifting of x, i.e. $x = u \mod \mathfrak{a}$. Then u^{p^n} is independent of the choice of x. Indeed, let u' be another lift of x. One sees by induction on m that

$$u^{p^m} = u'^{p^m} \mod \mathfrak{a}_m,$$

where $\mathfrak{a}_m$ is the ideal generated by all elements of the type $p^i a^{p^{m-i}}$, for $a \in \mathfrak{a}$, $0 \leqslant i \leqslant m$. We may therefore define $t(c) = u^{p^n}$. The multiplicativity is straightforward.

4.34. Lemma: There exists a uniquely determined multiplicative map $t : K \to A$ such that $t(c) = c \mod \mathfrak{a}$.

4.35. Theorem (Universality of Witt vectors): Under the assumptions above, there exists a uniquely determined homomorphism $\phi : W(K) \to A$ making the following diagram commute:

$$\begin{array}{ccc} W(K) & \xrightarrow{\ \phi\ } & A \\ & \searrow^{w_0} & \downarrow \\ & & K = A/\mathfrak{a} \end{array}$$

Proof: The map $w_n : W(A) \to A$ is a ring homomorphism. By assumption, when a Witt vector $a = (a_0,\dots,a_n,\dots)$ has its components in $\mathfrak{a}$, we have $w_n(a) = 0$. Therefore we get a

factorization:

76
77

$$\begin{array}{ccc} W(A) & \xrightarrow{w_n} & A \\ & \searrow & \uparrow{\scriptstyle \alpha_n} \\ & & W(K) \end{array}$$

We have $w_0(c)^{p^n} = \alpha_n(c) \bmod \mathfrak{a}$. Let Frob_K^{-n} be the inverse of the isomorphism Frob_K^n and $\phi = \alpha_n W(\mathrm{Frob}_K^{-n}) : W(K) \to W(K) \to A$. Then we have $w_0(c) = \phi(c) \bmod \mathfrak{a}$. Thus we have proved the existence.

Clearly $c \mapsto \phi([c])$, for $c \in K$, is a multiplicative map from K to A. Therefore $\phi([c]) = t(c)$. Let $\sum V^n[c_n]F^n \in W(K)$. Since K is perfect, we find

$$\xi = \sum V^n[c_n]F^n = \sum V^n F^n[c_n^{p^{-n}}] = \sum p^n[c_n^{p^{-n}}].$$

Therefore $\phi(\xi) = \sum p^n t(c_n^{p^{-n}})$. This concludes the proof of the theorem.

4.36. Exercise: Let A be a p-torsion-free ring ($pa = 0 \Rightarrow a = 0$), such that $A = \varprojlim A/p^n$. Assume that $K = A/pA$ is a perfect ring. Then A is isomorphic to the Witt ring $W(K)$. In particular, $W(\mathbb{F}_p) = \mathbb{Z}_p$.

§ 8 The structure equations of a Cartier module

4.37. Lemma: Every closed submodule of a V-reduced $\mathbb{E}_p$-module is V-reduced. Let $M_1 \to M_2$ be a homomorphism of V-reduced $\mathbb{E}_p$-modules such that $M_1/VM_1 \to M_2/VM_2$ is injective. Then $M_1 \to M_2$ is injective and $M = M_2/M_1$ is a V-reduced $\mathbb{E}_p$-module.

Proof: The first statement is trivial. Furthermore, it is clear that $M_1 \to M_2$ is injective. From the snake lemma, it follows that $V : M \to M$ is injective. By taking projective limits in the exact sequence $0 \to M_1/V^nM_1 \to M_2/V^nM_2 \to M/V^nM \to 0$, we get that M is V-separated and complete. Q.E.D.

Let I be an index set. We denote by $\widehat{\mathbb{E}_p^{(I)}}$ the completion with respect to the V-adic topology of a direct sum of I copies of $\mathbb{E}_p$. Thus $\widehat{\mathbb{E}_p^{(I)}}$ is the module of p-typical curves of $\widehat{W}^{(I)}$.

Let M be a V-reduced Cartier module such that M/VM is a free K-module. Let $\{m_i\}_{i\in I}$ be a family of elements of M whose residue classes mod VM form a basis of the K-module M/VM. Then a complete system of representatives for M/VM is given by the elements $\sum_{i\in I}[c_i]\, m_i$, where $c_i = 0$ for almost all i. According to 4.19, every element of M has a unique representation $\sum V^n[c_{n,i}]\, m_i$, where $c_{n,i} = 0$ for fixed n and almost all i. We call the m_i a *V-basis* of M (compare 3.15). In particular, we find the identities

77
78 (4.38)
$$Fm_i = \sum_{\substack{n\geqslant 0 \\ j\in I}} V^n[c_{n,i,j}]\, m_j, \qquad i \in I,\ c_{n,i,j} \in K.$$

We call these identities the *structure equations* for M.

These equations can be expressed by an exact sequence. Let $L = \widehat{\mathbb{E}_p^{(I)}}$ and e_i, $i \in I$ the standard basis.

$$L = \left\{ \sum_{i \in I} \xi_i e_i \mid \xi_{i \in \mathbb{E}_p} \text{ and } \xi_i \in V^n \mathbb{E}_p \text{ for almost all } i \text{ and given } n \right\}$$

Let $L \to L$ be the map $e_i \mapsto Fe_i - \sum V^n[c_{n,i,j}]\, e_j$. By 4.38 there is a sequence

$$\begin{array}{ccccccc} L & \longrightarrow & L & \longrightarrow & M & \longrightarrow & 0. \\ e_i & \longmapsto & m_i & & & & \end{array}$$

4.39. Theorem: Let $\alpha_{n,i,j}$, $i, j \in I$, $n \in \mathbb{N}$ be elements of $W(K) \subset \mathbb{E}_p$ such that for fixed n and i almost all $\alpha_{n,i,j}$ vanish. Let $\varphi : L \to L$ be the map $e_i \mapsto Fe_i - \sum_{n,j} V^n \alpha_{n,i,j} e_j$. Then the cokernel of φ is a V-reduced Cartier module M. The images of the e_i in M form a V-basis of M. There is an exact sequence

$$0 \longrightarrow L \xrightarrow{\varphi} L \longrightarrow M \longrightarrow 0.$$

Conversely, every V-reduced Cartier module such that M/VM is a free K-module can be obtained by this construction.

Proof: By 4.37 it suffices to prove that the map $L/VL \to L/VL$ is injective and that its cokernel is freely generated by the images of the e_i. We have $\sum_{n,j} V^n \alpha_{n,i,j} e_j = \sum_j [a_{i,j}]\, e_j \mod VL$, where $a_{i,j} = w_0(\alpha_{0,i,j}$. Since the elements $F^n e_i$, for $n \in \mathbb{N}$ and $i \in I$ form a V-basis of L, it follows that the elements

$$\varphi(F^n e_i) = F^n \left(Fe_i - \sum_{n,j} V^n \alpha_{n,i,j} e_j \right) = F^{n+1} e_i - \sum_{r \leqslant n, j} \left[b_{i,j}^{(r)} \right] F^r e_j \mod VL$$

are linearly independent in L/VL. They span a subspace that is complementary to the module $\bigoplus_{i \in I} Ke_i$. Therefore the images of the e_i form a basis of M/VM. The last claim follows from 4.38.

4.40. Exercise: Let R be a commutative ring. The polynomials $S_0, \ldots, S_{n-1}$ from the proof of 4.28 define an abelian group structure on the vectors $(a_0, \ldots, a_{n-1})$, $a_i \in K$. We denote it by $W_n(K)$ and call its elements the *Witt vectors of length* n. The restriction of the functors W_n to $\mathrm{Nil_K}$ will be denoted by $\widehat{W}_n$. It is a formal group of dimension n. The Cartier module of W_n has the following structure equations:

$$Fm_i = m_{i+1}, \quad \text{for } 1 \leqslant i < n, \quad Fm_n = 0.$$

We take m_0 to be the curve corresponding to the canonical projection $\widehat{W} \to \widehat{W}_n$. 78 79

§ 9 Base change

4.41. Theorem: Let M be a V-reduced $\mathbb{E}_p$-module. When $\mathscr{N}$ is flat or when M/VM is a flat K-module, then:

$$\mathrm{Tor}_i^{\mathbb{E}_p}\left(\widehat{W}(\mathscr{N}), M\right) = 0, \quad \text{for } i > 0.$$

Proof: As in the proof of 3.26, one can restrict to the case $\mathscr{N}^2 = 0$. According to 2.21, we have an isomorphism

$$\widehat{W}(\mathscr{N}) \otimes_{\mathbb{E}_p} M = \mathscr{N} \otimes_K M/VN.$$

Consider the exact sequence

$$0 \longrightarrow N \longrightarrow L \longrightarrow M \longrightarrow 0.$$

where L is a free $\mathbb{E}_p$-module. Tensoring with $\widehat{W}(\mathscr{N})$ we get the sequence

$$0 \longrightarrow \mathscr{N} \otimes_K N/VN \longrightarrow \mathscr{N} \otimes_K L/VL \longrightarrow \mathscr{N} \otimes_K M/VM \longrightarrow 0.$$

It is exact when either $\mathscr{N}$ or M/VM is flat. The claim follows as in 4.23.

From 4.41 we obtain a new proof of 4.23.

4.42. Exercise: a) Generalize 4.21 to Tor groups.
b) Let K be a reduced $\mathbb{Z}_{(p)}$-algebra and $H : \mathrm{Nil_K} \to \mathrm{Ab}$ a functor which is representable by a finitely generated projective K-algebra R. Then there exists an $\mathbb{E}_p$-module N and an isomorphism of functors

$$H(\mathscr{N}) \simeq \mathrm{Tor}_1^{\mathbb{E}_p}\left(\widehat{W}(\mathscr{N}), N\right).$$

In keeping with 3.27, we shall say that a V-reduced $\mathbb{E}_p$-module is *V-flat* when M/VM is a flat K-module.

4.43. Theorem: Let $\rho : K \to K'$ be a homomorphism. Let M be a V-flat $\mathbb{E}_{K,p}$-module. Let $M' = \mathbb{E}_{K',p} \mathbin{\widehat{\otimes}}_{\mathbb{E}_{K,p}} M$ be the completion of $\mathbb{E}_{K',p} \otimes_{\mathbb{E}_{K,p}} M$ for the V-adic topology. Then M' is a V-flat $\mathbb{E}_{K',p}$-module and we have

$$\widehat{W}(\mathscr{N}) \otimes_{\mathbb{E}_{K,p}} M = \widehat{W}(\mathscr{N}) \otimes_{\mathbb{E}_{K',p}} M', \qquad \mathscr{N} \in \mathrm{Nil_K}\,.$$

If M has a V-basis m_i, $i \in I$, and $Fm_i = \sum V^n \alpha_{n,i,j} m_j$, with $\alpha_{n,i,j} \in W(K)$, are the structure equations of M, then the structure equations of M' are $Fm'_i = \sum V^n \alpha'_{n,i,j} m'_j$, where the $\alpha'_{n,i,j}$ are the images of the $\alpha_{n,i,j}$ under the map $W(K) \to W(K')$.

If H is a formal group whose module of p-typical curves is M, then M' is the module of p-typical curves of $H_{K'}$.

79
80 **Proof:** Set $\mathbb{E}_p = \mathbb{E}_{K,p}$ and $\mathbb{E}'_p = \mathbb{E}_{K',p}$. Tensoring by M the exact sequence $\mathbb{E}'_p \xrightarrow{V} \mathbb{E}'_p \longrightarrow \mathbb{E}'_p/V\mathbb{E}'_p$ and applying 4.41 we get that $V : \mathbb{E}'_p \otimes_{\mathbb{E}_p} M \to \mathbb{E}'_p \otimes_{\mathbb{E}_p} M$ is injective. Thus V is also injective on M'. We conclude that M' is V-reduced.

We have a map

$$\widehat{W}(\mathscr{N}) \otimes_{\mathbb{E}_p} M = \widehat{W}(\mathscr{N}) \otimes_{\mathbb{E}'_p} \left(\mathbb{E}'_p \otimes_{\mathbb{E}_p} M\right) \longrightarrow \widehat{W}(\mathscr{N}) \otimes_{\mathbb{E}'_p} \left(\mathbb{E}'_p \mathbin{\widehat{\otimes}}_{\mathbb{E}_p} M\right).$$

There is an inverse map. Indeed, let $a \otimes m' \in \widehat{W}(\mathscr{N}) \otimes_{\mathbb{E}'_p} M'$. For large n, we have $aV^n = 0$. By definition, m' has a representation $m' = m_1 + V^n m'_2$, where $m_1 \in \mathbb{E}'_p \otimes_{\mathbb{E}_p} M \subset M'$ and $m'_2 \in M'$. Define $a \otimes m_1$ as the image of the inverse map. The remark on the structure equations follows by taking the exact sequence given by 4.39

$$0 \longrightarrow L \longrightarrow L \longrightarrow M \longrightarrow 0,$$

tensoring it by $\mathbb{E}'_p$ and completing. The last claim in the theorem is trivial.

4.44. Lemma: Let M be a V-reduced Cartier module. Assume that there is an exact sequence

$$P_2 \xrightarrow{\alpha} P_1 \xrightarrow{\beta} M/VM \longrightarrow 0, \tag{4.44.1}$$

where P_1 and P_2 are free K-modules. Then there exists an exact sequence of V-reduced Cartier modules

$$L_2 \longrightarrow L_1 \longrightarrow M \longrightarrow 0$$

such that $L/VL_2 \longrightarrow L/VL_1 \longrightarrow M/VM \longrightarrow 0$ is isomorphic to Sequence (4.44.1).

Proof: Let e_i, $i \in I$ be a basis of P_1. Pick $m_i \in M$ lifting the $\beta(e_i)$. We find expressions $Fm_i = \sum V^n[c_{n,i,j}]\, m_j$. Let L_1 be the V-reduced $\mathbb{E}_p$-module defined by these structure equations. The reduction mod V of the obvious map $\widetilde{\beta} : L_1 \to M$ can be identified with β. Let $K = \operatorname{Ker} \widetilde{\beta}$. Then K is a V-reduced $\mathbb{E}_p$-module nd $K/VK = \operatorname{Im} \alpha$. Applying the same procedure to K and $P_2 \to \operatorname{Im} \alpha$, one gets the desired exact sequence.

4.45. Theorem: Let M be a V-flat $\mathbb{E}_p$-module such that the K-module M/VM is of finite presentation, i.e. there is an exact sequence $P_2 \to P_1 \to M/VM \to 0$ where the P_i are free K-modules with a finite basis. Let $K \to K'$ be a ring homomorphism. Then the map

$$\mathbb{E}_{K',p} \otimes_{\mathbb{E}_{K,p}} M \longrightarrow \mathbb{E}_{K',p} \widehat{\otimes}_{\mathbb{E}_{K,p}} M$$

is an isomorphism.

Proof: Assume first that M/VM is a free K-module with a finite basis. By 4.39, we have an exact sequence 80 81

$$0 \longrightarrow \mathbb{E}^n_{K,p} \longrightarrow \mathbb{E}^n_{K,p} \longrightarrow M \longrightarrow 0.$$

The claim follows, since $\mathbb{E}_{K',p} \otimes_{\mathbb{E}_{K,p}} \mathbb{E}^n_p = \mathbb{E}^n_{K',p}$ is separated and complete with respect to the V-adic topology.
In the general case, 4.44 provides an exact sequence $L_2 \to L_1 \to M \to 0$. We get a commutative diagram with exact rows

$$\begin{array}{ccccccc}
\mathbb{E}_{K',p} \otimes_{\mathbb{E}_{K,p}} L_2 & \longrightarrow & \mathbb{E}_{K',p} \otimes_{\mathbb{E}_{K,p}} L_1 & \longrightarrow & \mathbb{E}_{K',p} \otimes_{\mathbb{E}_{K,p}} M & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
\mathbb{E}_{K',p} \widehat{\otimes}_{\mathbb{E}_{K,p}} L_2 & \longrightarrow & \mathbb{E}_{K',p} \widehat{\otimes}_{\mathbb{E}_{K,p}} L_1 & \longrightarrow & \mathbb{E}_{K',p} \widehat{\otimes}_{\mathbb{E}_{K,p}} M & \longrightarrow & 0.
\end{array}$$

Since we have shown that the first two vertical maps are isomorphism, the claim follows.

4.46. Theorem: Let $K \to K'$ be a surjection of rings. Let H' be a formal group over K' whose tangent space $t_{H'}$ is a free K'-module. Then there exists a formal group H over K such that t_H is a free K-module and $H_{K'} = H'$. One says that *the formal group H' can be lifted*.

Proof: Let M' be the module of p-typical curves of H'. We have structure equations for M':

$$Fm_i = \sum_{n,j} V^n[c'_{n,i,j}]\, m_j, \qquad c'_{n,i,j} \in K'.$$

Let $c_{n,i,j} \in K$ be pre-images of the $c'_{n,i,j}$, such that $c_{n,i,j} = 0$ whenever $c'_{n,i,j} = 0$. The structure equations

$$Fm_i = \sum V^n[c_{n,i,j}]\, m_j$$

define a V-reduced $\mathbb{E}_{K,p}$-module whose associate formal group has the desired properties.

The question whether a homomorphism of formal groups can be lifted is rather more complicated.

4.47. Theorem: Let $\mathfrak{a}$ be an ideal of K such that $p\mathfrak{a} = \mathfrak{a}^p = 0$ and $K' = K/\mathfrak{a}$. Let G_1 and G_2 be formal groups over K and $\varphi' : G_{1,K'} \to G_{2,K'}$ a homomorphism. Then there exists a homomorphism $\psi : G_1 \to G_2$ such that $p\varphi' = \psi_{K'}$. Let $\varphi_1, \varphi_2 : G_1 \to G_2$ be two homomorphisms such that $\varphi_{1,K'} = \varphi_{2,K'}$. Then $p\varphi_1 = p\varphi_2$.

Proof: We have an exact sequence

$$0 \longrightarrow \mathbb{E}_p(\mathfrak{a}) \longrightarrow \mathbb{E}_{K,p} \longrightarrow \mathbb{E}_{K',p} \longrightarrow 0.$$

If M is a V-flat $\mathbb{E}_{K,p}$-module, we get an exact sequence

81
82
$$0 \longrightarrow \mathbb{E}_p(\mathfrak{a}) \mathbin{\widehat{\otimes}}_{\mathbb{E}_{K,p}} M \longrightarrow M \longrightarrow \mathbb{E}_{K',p} \mathbin{\widehat{\otimes}}_{\mathbb{E}_{K,p}} M \longrightarrow 0.$$

Put $\mathbb{E}_{K',p} \mathbin{\widehat{\otimes}}_{\mathbb{E}_{K,p}} M = M_{K'}$. Thus the kernel of the map $M \to M_{K'}$ consists of elements of the form $\alpha = \sum V^n[a_{n,i}]\, m_i$, with $a_{n,i} \in \mathfrak{a}$. Clearly, $p\alpha = \left([p] + \sum_{n\geqslant 1} V^n[c_n]F^n\right)\alpha = 0$. Therefore the multiplication by p factors as $p : M \longrightarrow M_{K'} \xrightarrow{\rho} M$.

Let M_1 and M_2 be the modules of p-typical curves of G_1 and G_2. Then we define ψ as the composite map

$$M_1 \longrightarrow M_{1,K'} \xrightarrow{\varphi'} M_{2,K'} \xrightarrow{\rho} M_2.$$

If φ is any lifting of φ', then $p\varphi = \psi$, from which the last claim follows.

Chapter V

Isogenies of formal groups

§ 1 Homomorphisms of formal groups over a perfect field

5.1. Theorem: Let $M' \subset M$ be an inclusion of reduced $\mathbb{E}_p$-modules over a perfect field K. We assume that $V^N M \cap M' \subset VM'$ for large enough integers N. Then there exists a V-basis $\{m_i\}_{i\in I}$ of M, a subset $J \subset I$ and natural integers n_j, $j \in J$, such that $\{V^{n_j} m_j\}_{j\in J}$ is a V-basis of M'. The assumption $V^N M \cap M' \subset VM'$ is fulfilled if M/VM or M'/VM' is a finite-dimensional K-vector space.

Proof: Let $\mathrm{gr}^n M = V^n M/V^{n+1}M$. The field K acts via the operators $[c]$ on $V^n M/V^{n+1}M$. In this way, one obtains a structure of K-vector space on $V^n M/V^{n+1}M$. Let us consider the K-vector subspace $(V^n M \cap M')/(V^{n+1}M \cap M') = G_n$. The bijection $V : \mathrm{gr}^n M \to \mathrm{gr}^{n+1} M$ maps G_n onto a K-vector subspace VG_n of G_{n+1}. Indeed, if $m = Vm_1 \in VG_n$ and $c \in K$, we have $[c]m = [c]Vm_1 = V[c^p]m_1 \in VG_n$. Let U_{n+1} be a K-vector subspace of G_{n+1} complementary to VG_n. Then one has a direct sum decomposition of K-vector spaces

$$G_n = \bigoplus_{0\leqslant i\leqslant n} V^i U_{n-i}. \tag{5.1.1}$$

We choose a basis $\{\overline{u}_j\}_{j\in J_n}$ of the K-vector space U_n. Let $u_j \in V^n M \cap M'$ be representatives, and let $m_j = V^{-n} u_j \in M$. Let $J = \cup_n J_n$. Then the $\{m_j\}_{j\in J}$ are linearly independent modulo VM. Indeed, assume $\sum [c_j] m_j \in VM$. If we multiply by V^n for large enough n, we obtain a relation

$$\sum \left[c_j^{p^n}\right] V^{n-n_j} u_j \in V^{n+1} M \cap M', \quad u_j \in U_{n_j}.$$

From the direct sum decomposition 5.1.1 follows that $c_j = 0$. It remains to prove that the u_j are a V-basis of M'. With the help of the decomposition 5.1.1, it follows easily that every element $m' \in M'$ may be written as a convergent sum:

$$\sum_n \sum_{j\in J_n} V^m \left[a_{m,j,n}\right] u_j. \tag{5.1.2}$$

Here, for all fixed m and n, we have $a_{m,j,n} = 0$ for almost all j. If $V^N M \cap M' \subset VM'$, we find $U_n = 0$ for $n \geqslant N$. The claim follows immediately. If M/VM or M'/VM' is finite-

dimensional, the dimension of G_n is bounded independently of n. From 5.1.1 then follows that $U_n = 0$ for large n. The theorem is therefore proved.

83 84 **5.2. Theorem:** Let $f : G \to H$ be a homomorphism of formal groups of finite dimension over a perfect field K of characteristic p. Let $e = \dim H$ and $d = \dim G$. Then there are isomorphisms of functors

$$H \simeq \operatorname{Spf} K[[Y_1, \ldots, Y_e]], \quad G \simeq \operatorname{Spf} K[[X_1, \ldots, X_d]],$$

such that the comorphism f^* of f has the following expression:

$$f^*(X_i) = Y_i^{p^{n_i}}, \quad \text{for } i \leqslant r \text{ and } f^*(X_i) = 0 \text{ for } i > r.$$

Here $0 \leqslant r \leqslant \min(e, d)$ and $n_1, \ldots, n_r$ are natural integers.

Proof: Let N and M be the Cartier modules of H and G. Then f induces a mapping $N \to M$. The image $M' \subset M$ is a V-reduced Cartier module that corresponds to a finite-dimensional group G'. Let us now consider the case when $H = G'$. Let $m_1, \ldots, m_d$ be a V-basis of G and $u_i = V^{n_i} m_i$, $i = 1, \ldots, e$ be a V-basis of H 5.1. In the curvilinear coordinates 3.31, we obtain a map

$$f : \operatorname{Spf} K[[\underline{Y}]] \longrightarrow \operatorname{Spf} K[[\underline{X}]].$$

We identify the varieties of H and G with $\operatorname{Spf} K[[\underline{Y}]]$ and $\operatorname{Spf} K[[\underline{X}]]$. Let $q_i : H \to \operatorname{Spf} K[[X]]$ and $p_i : G \to \operatorname{Spf} K[[X]]$ be the projections $q_i^*(X) = Y_i$ and $p_i^*(X) = X_i$. Let $g : H \to G$ be the map $g^*(X_i) = Y_i^{p^{n_i}}$, $i \leqslant e$, $g^*(X_i) = 0$, $i > e$. One finds immediately $m_i p_i g = f u_i q_i$ for $i = 1, \ldots, e$ and $m_i p_i g = 0$ for $i > e$. From the definition of the curvilinear coordinate system, it follows that $g = \sum_{i=1}^{d} m_i p_i q = \sum_{i=1}^{e} f u_i q_i = f$. In the general case, we consider the surjection $\alpha : N \to M'$. Let $u_1, \ldots, u_r$ be a V-basis of M'. One finds a V-basis $v_1, \ldots, v_e$ of N such that $\alpha(v_i) = u_i$ for $i \leqslant r$ and $\alpha(v_i) = 0$ for $i > r$. In the curvilinear coordinates, the map takes the form

$$\operatorname{Spf} K[[Y_1, \ldots, Y_e]] \longrightarrow \operatorname{Spf} K[[X_1, \ldots, X_r]], \quad \alpha^*(X_i) = Y_i.$$

The theorem follows.

5.3. Theorem: Let K be a perfect field of characteristic p and let $H : \mathrm{Nil}_K \to \mathrm{Ab}$ be a functor that is represented by a finite K-algebra R. Then R is isomorphic to

$$K[[X_1, \ldots, X_r]] / \left(X_1^{p^{n_1}}, \ldots, X_r^{p^{n_r}}\right).$$

Proof: This is a direct consequence of 2.35 and 5.2.

One calls $\sum n_i = \log_p \dim_K R$ the *height* of H.

84 85 § 2 Definition of isogenies

5.4. Definition: A morphism $\varphi : G_1 \to G_2$ of formal groups of the same finite dimension is called an *isogeny* if the kernel of φ is representable.

Explicitly, this definition means the following. Let $G_i = \operatorname{Spf} R_i$, $i = 1, 2$ and let $\mathfrak{a}_i$ be the augmentation ideals. Since by assumption the tangent spaces $t_{G_i}(K)$ are finitely generated, projective K-modules, the ideals $\mathfrak{a}_i$ are finitely generated, and $\mathfrak{a}_i^N$ is a system of neighbourhoods of 0 in R_i.

5.5. Lemma: The morphism φ is an isogeny if and only if $\mathfrak{a}_1$ is nilpotent in $R_1/\mathfrak{a}_2 R_1$.

Proof: The kernel of φ is prorepresented by

$$R_1 \mathbin{\widehat{\otimes}}_{R_2} R_2/\mathfrak{a}_2 = \varprojlim (R_1/\mathfrak{a}_1^N \otimes_{R_2} R_2/\mathfrak{a}_2) = R_1/(\bigcap_N \mathfrak{a}_1^N + \mathfrak{a}_2 R_1).$$

Here, $\mathfrak{a}_1^N + \mathfrak{a}_2 R_1$ is a system of neighbourhoods of 0. The last ring is a nilpotent, augmented K-algebra if

$$\mathfrak{a}_1^N + \mathfrak{a}_2 R_1 = \mathfrak{a}_1^{N+1} + \mathfrak{a}_2 R1 = \ldots, \quad \text{for large } N.$$

Let $\mathfrak{b}$ be the image of the latter ideal in $R_1/\mathfrak{a}_2 R_1$ and $\overline{\mathfrak{a}}_1$ be the image of $\mathfrak{a}_1$. Since R_1 is complete, the elements of $1 + \mathfrak{a}_1$ and $1 + \overline{\mathfrak{a}}_1$ are units. It follows that $\overline{\mathfrak{a}}_1$ lies in the radical of $R_1/\mathfrak{a}_2 R_1$. Since $\mathfrak{a}_1 \mathfrak{b} = \mathfrak{b}$ and $\mathfrak{b}$ is finitely generated, it follows from Nakayama's lemma that $\mathfrak{b} = 0$.

5.6. Remark: The property that φ is an isogeny is preserved by base change. Indeed, if $K \to K'$ is a ring homomorphism, then $\ker(\varphi_{K'}) = (\ker \varphi)_{K'}$.

Let K be a field of characteristic p and R a finite K-algebra that represents $\ker \varphi$. Let K' be a perfect field extension of K. Then, according to 5.3 there exists a natural number h such that $\dim_K R = \dim_{K'} R \otimes_K K'$. One calls h the *height* of the isogeny φ.

An isogeny over a $\mathbb{Q}$-algebra is an isomorphism 4.7.

The notion of isogeny is local in the following sense. Let $f_1, \ldots, f_m$ be elements of K that generate the unit ideal. Then φ is an isogeny if $\varphi_{K_{f_i}}$ is an isogeny for $i = 1, \ldots, m$. Indeed, let $(R, \mathfrak{a}_n)$ be a complete augmented K-algebra that prorepresents $\ker \varphi$. Then $\ker \varphi_{K_{f_i}}$ is represented by $R \mathbin{\widehat{\otimes}}_K K_{f_i} = \varprojlim R/\mathfrak{a}_n \otimes_K K_{f_i}$. If $\ker \varphi_{K_{f_i}}$ is representable, then it follows that for large n we have $\mathfrak{a}_n \otimes_K K_{f_i} = \mathfrak{a}_{n+1} \otimes_K K_{f_i}$. From this, one gets $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \cdots = 0$.

5.7. Lemma: If φ is an isogeny, then the comorphism $R_2 \to R_1$ is finite. 85 86

Proof: Since $\mathfrak{a}_1$ is finitely generated and nilpotent in $R_1/\mathfrak{a}_2 R_1$, the latter ring is a finite K-module. Let $f_1, \ldots, f_s$ be elements that modulo $\mathfrak{a}_2$ form a generating system of this module. One considers the map:

(5.7.1)
$$\begin{aligned} \bigoplus_{i=1}^{s} R_2 &\longrightarrow R_1 \\ \oplus r_i &\longmapsto \sum r_i f_i. \end{aligned}$$

We equip $\oplus_{i=1}^s R_2$ with the filtration by the $\oplus \mathfrak{a}_2^N$, and R_1 with the filtration by the $R_1 \mathfrak{a}_2^N$. Then the map (5.7.1) is a map of complete, filtered modules such that the associated map of graded modules is surjective. The lemma follows.

§ 3 The Weierstrass preparation theorem

5.8. Theorem: Let K be a commutative ring with unit element. Let $p_1, \dots, p_n \in K[[X_1, \dots, X_n]]$ be power series such that X_i is nilpotent in $K[[X_1, \dots, X_n]]/(p_1, \dots, p_n)$ for $i = 1, \dots, n$. Consider the mapping

$$K[[Y_1, \dots, Y_n]] \longrightarrow K[[X_1, \dots, X_n]] \tag{5.8.1}$$
$$Y_i \longmapsto p_i.$$

Then $K[[\underline{X}]]$ is a finite projective $K[[\underline{Y}]]$-module. The morphism (5.8.1) is a faithfully flat ring homomorphism.

Proof: The proof is pure commutative algebra, which is not necessary for the understanding of the sequel. It can therefore be skipped on a first reading. We prove a series of claims.

Claim 1: $K[[\underline{X}]]$ is a finite projective $K[[\underline{Y}]]$-module if and only if for all N, the module $K[[\underline{X}]]/(\underline{Y})^N K[[\underline{X}]]$ is a projective $K[[\underline{Y}]]/(\underline{Y})^N$-module.

Actually, we proved the finiteness already. Let P be the finite projective K-module $K[[\underline{X}]]/(\underline{Y})K[[\underline{X}]]$. It is clear that $P[[\underline{Y}]]$ is a projective $K[[\underline{Y}]]$-module. Therefore the map of $K[[\underline{Y}]]$-modules $P \simeq K[[\underline{X}]]/(\underline{Y})K[[\underline{X}]]$ lifts to a map $P[[\underline{Y}]] \to K[[\underline{X}]]$. We must show that this is an isomorphism. Since both modules are complete and separated in the $(\underline{Y})$-adic topology, it is enough to prove that $P[[\underline{Y}]]/(\underline{Y})^N \to K[[\underline{X}]]/(\underline{Y})^N K[[\underline{X}]]$ is an isomorphism for all N. By 5.7 this map is surjective. We obtain:

$$0 \longrightarrow C \longrightarrow P[[\underline{Y}]]/(\underline{Y})^N \longrightarrow K[[\underline{X}]]/(\underline{Y})^N K[[\underline{X}]] \longrightarrow 0$$

$$0 \longrightarrow C \otimes_{K[[\underline{Y}]]/(\underline{Y})^N} K \longrightarrow P \longrightarrow K[[\underline{X}]]/(\underline{Y})K[[\underline{X}]] \longrightarrow 0.$$

86 87

The second sequence is exact since by assumption $K[[\underline{X}]]/(\underline{Y})^N K[[\underline{X}]]$ is a projective $K[[\underline{Y}]]/(\underline{Y})^N$-module. We obtain $(\underline{Y})C = C$ and since $(\underline{Y})$ is nilpotent in $K[[\underline{Y}]]/(\underline{Y})^N$, then $C = 0$.

Before we continue, let us remark that $P = K \oplus P'$ and hence $P[[\underline{Y}]] = K[[\underline{Y}]] \oplus P'[[\underline{Y}]]$. Using this, the last claim of the theorem follows from the others.

Claim 2: one can assume that the p_i are polynomials. Indeed $(\underline{X})^N$ is 0 in $K[[\underline{X}]]/(\underline{p})$ if and only if $(\underline{X})^N \subset (\underline{p}) + (\underline{X})^{N+1}$. This inclusion implies that

$$(\underline{p}) + (\underline{X})^N = (\underline{p}) + (\underline{X})^{N+1} = \dots.$$

Using this we can conclude like in 5.5. Let p_i' be polynomials such that

$$p_i' = p_i \mod \deg M \quad \text{for} \quad M > N.$$

Then we find $(\underline{p}') \subset (\underline{p}) + (\underline{X})^N = (\underline{p})$ and $(\underline{X})^N \subset (\underline{p}) + (\underline{X})^{N+1} = (\underline{p}') + (\underline{X})^{N+1}$. By symmetry we find $(\underline{p}) = (\underline{p}')$. We consider the map

$$K[[\underline{Y}]]/(\underline{Y})^s \longrightarrow K[[\underline{X}]]/(\underline{p})^s = K[[\underline{X}]]/(\underline{p}')^s$$
$$Y_i \longmapsto p_i.$$

Since $(\underline{p})^s$ contains a power of $(\underline{X})$, we can choose the polynomials p_i' in such a way that $p_i' = p_i \mod (\underline{p})^s$. Then we obtain the claim.

Claim 3: We may assume that K is noetherian.

Let $p_1, \ldots, p_n$ be polynomials and let $K_0 \subset K$ be the subring generated by their coefficients. Then K_0 is noetherian. Let $\mathfrak{p}_0 \subset K_0[[\underline{X}]]$ and $\mathfrak{p} \subset K[[\underline{X}]]$ be the ideals generated by $p_1, \ldots, p_s$. If we assume that the theorem is proved for noetherian rings, then $K_0[[\underline{X}]]/\mathfrak{p}_0^s \otimes_{K_0} K$ is a finite projective $K_0[[\underline{Y}]]/(\underline{Y})^s \otimes_{K_0} K$-module. In fact, by adjoining finitely many coefficients to K_0, we can arrange that the inclusion $(\underline{X})^N \subset \mathfrak{p}_0 + (\underline{X})^{N+1}$ holds. But then $(\underline{X})$ is nilpotent in $K_0[[\underline{X}]]/\mathfrak{p}_0$. Let $\mathfrak{a} = \mathfrak{p}_0^s \cap K_0[\underline{X}]$. Since $(\underline{X})^N \subset \mathfrak{p}_0^s$ for large enough N, we find

$$\begin{aligned} K_0[[\underline{X}]]/\mathfrak{p}_0^s \otimes_{K_0} K &= K_0[\underline{X}]/\mathfrak{a} \otimes_{K_0} K = K[\underline{X}]/\mathfrak{a}K[\underline{X}] \\ &= K[[\underline{X}]]/\mathfrak{a}K[[\underline{X}]] = K[[\underline{X}]]/\mathfrak{p}^s K[[\underline{X}]] \end{aligned}$$

and $K_0[[\underline{Y}]]/(\underline{Y})^s \otimes_{K_0} K = K[[\underline{Y}]]/(\underline{Y})^s$. The claim follows.

Claim 4: One can assume that K is a complete noetherian local ring.

According to Claim 1, is is enough to show that $K[[\underline{X}]]/(\underline{p})^s$ is a projective $K[[\underline{Y}]]/(\underline{Y})^s$-module. A finitely generated module over a noetherian ring is projective if and onyl if its localizations at maximal ideals are free modules. The maximal ideals of $K[[\underline{Y}]]/(\underline{Y})^s$ are of the form $\mathfrak{m} + (\underline{Y})$, where $\mathfrak{m}$ is a maximal ideal of K. Hence is is enough to prove that $K_\mathfrak{m}[[\underline{X}]]/(\underline{p})^s$ is a free $K_\mathfrak{m}[[\underline{Y}]]/(\underline{Y})^s$-module. Since a module over a local noetherian ring is free if and only if its base change to the completion is free, we can finally assume that K is complete. 87 88

Claim 5: One can assume that K is a field.

Let K be a complete local noetherian ring with maximal ideal $\mathfrak{m}$. Let $f_1, \ldots, f_h \in K[[\underline{X}]]$ be power series whose residue classes form a basis of the $K/\mathfrak{m}$-vector space $K/\mathfrak{m}[[\underline{X}]]/(\underline{p})$. The elements f_i define a map

$$K[[\underline{Y}]]^h \longrightarrow K[[\underline{X}]]. \tag{5.8.2}$$

Since the theorem is taken for granted for a field, the map

$$K/\mathfrak{m}[[\underline{Y}]]^h \longrightarrow K/\mathfrak{m}[[\underline{X}]] \tag{5.8.3}$$

is an isomorphism. Now we consider the modules in (5.8.2) equipped with the filtrations $(\mathfrak{m}^i[[\underline{Y}]])^h$ and $\mathfrak{m}[[\underline{X}]]$. The map on graded objects $(\mathfrak{m}^i/\mathfrak{m}^{i+1}[[\underline{Y}]])^h \to \mathfrak{m}^i/\mathfrak{m}^{i+1}[[\underline{X}]]$ is obtained by applying the tensor product $\mathfrak{m}^i/\mathfrak{m}^{i+1} \otimes_{K/\mathfrak{m}}$ in (5.8.3). Therefore, the graded objects are isomorphic. Since the filtrations are complete and separated, it follows that (5.8.2) is also an isomorphism.

When K is a field, the result is well-known and is a consequence of the follwing general result of Commutative Algebra. Let $A \to B$ be a morphism of regular local rings of the same dimension such that B is finite over A. Then B is a free A-module (*cf* [21]).

§ 4 The fibre criterion for isogenies

Let K be a $\mathbb{Z}_{(p)}$-algebra and $\varphi : G_1 \to G_2$ be an isogeny. Let $\mathfrak{p}$ be a prime ideal of K and $\kappa(\mathfrak{p}) = K_{\mathfrak{p}}/\mathfrak{p}K_{\mathfrak{p}}$ the residue field. By 5.8, the kernel of φ is represented by a finitely generated projective K-algebra R. According to Remark 5.6, we have $\dim_{\kappa(\mathfrak{p})} R \otimes_K \kappa(\mathfrak{p}) = p^{h(\mathfrak{p})}$ where $h(\mathfrak{p})$ is a natural integer. The function $h(\mathfrak{p})$ is a locally constant function on $\operatorname{Spec} K$ (*cf* [2]). If K contains no idempotent elements other than 0 and 1, then $\operatorname{Spec} K$ is connected and hence $h(\mathfrak{p}) = h$ is a constant function.

5.9. Definition: We say that φ *is an isogeny of height* h if $h(\mathfrak{p}) = h$ for all primes $\mathfrak{p} \in \operatorname{Spec} K$.

Let for a moment K be a ring of characteristic p. We look at the multiplication by p on the multiplicative group:

88
89
$$\begin{aligned} p : \mathbb{G}_{\mathrm{m}}(\mathscr{N}) &\longrightarrow \mathbb{G}_{\mathrm{m}}(\mathscr{N}) \\ 1 + n &\longmapsto (1+n)^p = 1 + n^p. \end{aligned}$$

Obviously, the kernel is represented by $K[T]/T^p$. It follows that the multiplication-by-p map is an isogeny of height 1.

If φ is an isogeny of height h, we say also that *the height of* φ *is defined* and we write $\operatorname{height} \varphi = h$.

5.10. Theorem: Let $\varphi_1 : G_1 \to G_2$ and $\varphi_2 : G_2 \to G_3$ be morphisms of formal groups of the same dimension. Then $\varphi_2 \circ \varphi_1$ is an isogeny if and only if φ_1 and φ_2 are isogenies. Moreover, we have

$$\operatorname{height} \varphi_1 + \operatorname{height} \varphi_2 = \operatorname{height} \varphi_2 \circ \varphi_1$$

if two of the heights are defined.

Proof: By Remark 5.6, one can assume that $G_1 = \operatorname{Spf} K[[\underline{X}]]$, $G_2 = \operatorname{Spf} K[[\underline{Y}]]$, $G_3 = \operatorname{Spf} K[[\underline{Z}]]$. We show that φ_2 is an isogeny if $\varphi_2 \circ \varphi_1$ is one. The remaining implications are trivial. We must show that the multiplication-by-Y_i^N map vanishes for large enough N:

$$K[[\underline{Y}]]/(\underline{Z})K[[\underline{Y}]] \xrightarrow{Y_i^N} K[[\underline{Y}]]/(\underline{Z})K[[\underline{Y}]].$$

If we tensor with $\otimes_{K[[\underline{Y}]]} K[[\underline{X}]]$, we obtain

$$K[[\underline{X}]]/(\underline{Z})K[[\underline{X}]] \xrightarrow{Y_i^N} K[[\underline{X}]]/(\underline{Z})K[[\underline{X}]].$$

Since by assumption $(\underline{X})$ is nilpotent in this ring, it follows that the mapping is 0 for large enough N. Since we already know by 5.5 that φ_1 is an isogeny, the morphism $K[[\underline{Y}]] \to K[[\underline{X}]]$ is faithfully flat. Therefore the morphism was already 0 before tensoring. For the last claim, it suffices to observe that $K[[\underline{X}]]$ is a free $K[[\underline{Y}]]$-module of rank $p^{\operatorname{height} \varphi_1}$ etc.

5.11. Lemma: Let $\mathfrak{a}$ be an ideal of K consisting of nilpotent elements and $K' = K/\mathfrak{a}$. Let $p_1, \ldots, p_n \in K[[X_1, \ldots, X_n]]$ be power series. If $(\underline{X})$ is nilpotent in $K'[[\underline{X}]]/(p) \cdot K'[[\underline{X}]]$, then $(\underline{X})$ is nilpotent in $K[[\underline{X}]]/(\underline{p})$ also.

Proof: By assumption, for large enough natural integers N we have:

$$(\underline{X})^N \subset \mathfrak{a}[[\underline{X}]] + (\underline{p}) + (\underline{X})^{N+1}.$$

Obviously, there exists a finitely generated ideal $\mathfrak{a}' \subset \mathfrak{a}$ such that

$$(\underline{X})^N \subset \mathfrak{a}'[[\underline{X}]] + (\underline{p}) + (\underline{X})^{N+1}.$$

From Nakayama's lemma it follows like in 5.5 that $(\underline{X})^N \subset \mathfrak{a}'[[\underline{X}]] + (\underline{p})$. Since $\mathfrak{a}'$ is finitely generated, it follows that $\mathfrak{a}'[[\underline{X}]]^M = 0$ for large M and hence $(\underline{X})^{NM} \subset (\underline{p})$.

5.12. Corollary: Let $\varphi : G_1 \to G_2$ be a morphism of formal groups over K. Let $K \to K'$ be as in Lemma 5.11. If $\varphi_{K'}$ is an isogeny, then φ is an isogeny. 89 90

5.13. Lemma: Let $K \to K'$ be a faithfully flat ring extension. Let $p_1, \ldots, p_n$ be power series in $K[[X_1, \ldots, \underline{X}_n]]$. If $(\underline{X})$ is nilpotent in $K'[[\underline{X}]]/(\underline{p})K'[[\underline{X}]]$, then $(\underline{X})$ is nilpotent in $K[[\underline{X}]]/(\underline{p})K[[\underline{X}]]$.

Proof: One has an isomorphism:

$$K[[\underline{X}]]/(\underline{p}) + (\underline{X})^N \otimes_K K' = K'[[\underline{X}]]/(\underline{p}) + (\underline{X})^N. \tag{5.13.1}$$

Indeed, in order to see this one may assume that the p_i are polynomials. Then, we have:

$$K[[\underline{X}]]/(\underline{p}) + (\underline{X})^N \otimes_K K' = K[\underline{X}]/(\underline{p}) + (\underline{X})^N \otimes_K K'.$$

Since $K[\underline{X}] \otimes_K K' = K'[\underline{X}]$, one obtains the isomorphism (5.13.1). By assumption, the multiplication by $\underline{X}^{\underline{\alpha}}$ on $K'[[\underline{X}]]/(\underline{p}) + (\underline{X})^N$, $|\underline{\alpha}| = N - 1$, is 0 for large enough N. Since K' is a faithfully flat extension, it follows from (5.13.1) that $\underline{X}^{\underline{\alpha}}$ vanishes in $K[[\underline{X}]]/(\underline{p}) + (\underline{X})^N$.

5.14. Corollary: Let $\varphi : G_1 \to G_2$ be a morphism of formal groups over K. Let $K \to K'$ be as in Lemma 5.13. If $\varphi_{K'}$ is an isogeny, then φ is an isogeny.

5.15. Theorem: Let $\varphi : G_1 \to G_2$ be a morphism of formal groups of the same dimension over K. Assume that for every prime ideal $\mathfrak{p} \subset K$, the morphism $\varphi_{\kappa(\mathfrak{p})}$ is an isogeny whose height we denote by $h(\mathfrak{p})$. Then $h(\mathfrak{p}) \geqslant h(\mathfrak{q})$ holds for $\mathfrak{p} \supseteq \mathfrak{q}$. If $h(\mathfrak{p}) = h$ is independent of $\mathfrak{p}$ and K has only finitely many minimal prime ideals, then φ is an isogeny.

The Theorem follows from:

5.16. Lemma: Let $p_1, \ldots, p_n$ be power series in $K[[X_1, \ldots, X_n]]$. Assume that for every prime ideal $\mathfrak{p}$ of K, the ideal $(\underline{X})$ is nilpotent in $\kappa(\mathfrak{p})[[\underline{X}]]/(\underline{p})$, and let $r(\mathfrak{p}) = \dim_{\kappa(\mathfrak{p})} \kappa(\mathfrak{p})[[\underline{X}]]/(\underline{p})$. Then $h(\mathfrak{p}) \geqslant h(\mathfrak{q})$ holds for $\mathfrak{p} \supseteq \mathfrak{q}$. If $r(\mathfrak{p}) = r$ is independent of $\mathfrak{p}$ and K has only finitely many minimal prime ideals, then $(\underline{X})$ is nilpotent in $K[[\underline{X}]]/(\underline{p})$.

Proof: By 5.11 one can assume that K is reduced. We show that one may assume that K is an integral domain. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the minimal prime ideals of K. If the Lemma holds for an integral domain and $r(\mathfrak{p}) = r$ is independent of $\mathfrak{p}$, then we have for large enough N:

$$(\underline{X})^N \subset (\underline{p}) + \mathfrak{p}_i[[\underline{X}]].$$

From this follows:

$$(\underline{X})^{Nr} \subset \prod((\underline{p}) + \mathfrak{p}_i[[\underline{X}]]) \subset (\underline{p}) + \prod \mathfrak{p}_i[[\underline{X}]] \subset (\underline{p}).$$

Since $K \to \prod K_{\mathfrak{p}}$, where $\mathfrak{p}$ runs through the minimal prime ideals of K, is a faithfully flat ring extension, one can moreover assume that K is a local ring with maximal ideal $\mathfrak{m}$. 90 91

We can assume that the p_i are polynomials. Indeed, we can find an integer N independent of $\mathfrak{p}$ such that

$$(\underline{X})^N \subset (\underline{p}) + (\underline{X})^{N+1} \text{ in } \kappa(\mathfrak{p})[[\underline{X}]]/(\underline{p}).$$

Let p_i' be polynomials such that $p_i' = p_i \mod (\underline{X})^{N+1}$. If the theorem is proved for polynomials, it follows that $(\underline{X})^s \subset (\underline{p}')$ for large s. Let L be the field of fractions of K. Then, the following holds:

$$K[[\underline{X}]]/(\underline{p}') \subset K[[\underline{X}]]/(\underline{p}') \otimes_K L = L[[\underline{X}]]/(\underline{p}') \quad (cf \text{ (5.13.1)}).$$

From this we get $(\underline{X})^N \subset (\underline{p}')$. Then we have $(\underline{p}) + (\underline{X})^N = (\underline{p}) + (\underline{X})^{N+1} = (\underline{p}')$ and consequently $(\underline{X})^N \subset (\underline{p})$.

We now consider the subring $K'' \subset K$ generated by the coefficients of the p_i. Let $K' = K''_{\mathfrak{m}\cap K''} \subset K$. Then K' is a noetherian local ring. Let $\mathfrak{q}$ be a prime ideal of K and $\mathfrak{q}' = \mathfrak{q} \cap K'$. Since $\kappa(\mathfrak{q}') \to \kappa(\mathfrak{q})$ is faithfully flat, the ideal $(\underline{X})$ is nilpotent in $\kappa(\mathfrak{q}')[[\underline{X}]]/(\underline{p})\kappa(\mathfrak{q}')[[\underline{X}]]$ and we have $r(\mathfrak{q}') = r(\mathfrak{q})$. Therefore 5.16 follows from the following:

5.17. Lemma: Let K be a noetherian local ring with maximal ideal $\mathfrak{m}$. Let $p_1, \ldots, p_n \in K[[X_1, \ldots, X_n]]$ be power series such that $(\underline{X})$ is nilpotent in $\kappa(\mathfrak{p})[[\underline{X}]]/(\underline{p})$ if $\mathfrak{p} = \mathfrak{m}$ or if $\mathfrak{p}$ is a minimal prime ideal of K. Then $r(\mathfrak{p}) \leqslant r(\mathfrak{m})$ for all minimal prime ideals $\mathfrak{p}$. If $r(\mathfrak{p}) = r(\mathfrak{m})$ for all minimal prime ideals $\mathfrak{p}$, then $(\underline{X})$ is nilpotent in $K[[\underline{X}]]/(\underline{p})$.

Proof: Let $\widehat{K}$ be the completion of K. Since the minimal primes of $\widehat{K}$ lie over minimal primes of K, the assumptions are fulfilled by $\widehat{K}$. Since $\widehat{K}$ is faithfully flat over K, we may by 5.13 assume that $\widehat{K} = K$. One sees as above that one can also assume that K is an integral domain. Let L be the field of fractions of K and $k = K/\mathfrak{m}$.

We choose a k-basis $\overline{e}_1, \ldots, \overline{e}_s$ of $k[[\underline{X}]]/(\underline{p})$. Let $e_i \in K[[\underline{X}]]/(\underline{p})$ be liftings of the $\overline{e}_i$. Consider the mapping

$$\alpha : \bigoplus_{m=1}^{s} K[[\underline{Y}]] \longrightarrow K[[\underline{X}]] \quad (cf \text{ (5.7.1)}).$$
$$\oplus r_i \longmapsto \sum r_i e_i$$

By the preparation Theorem 5.8, this is an isomorphism if we replace K by $K/\mathfrak{m}^n$. It follows that α itself is an isomorphism. The map

$$K[[\underline{X}]]/(\underline{p}) \otimes_K L \longrightarrow L[[\underline{X}]]/(\underline{p})L[[\underline{X}]]$$

is surjective, since $(\underline{X})$ is nilpotent in the right-hand ring. Therefore

$$s \geqslant \dim_L L[[\underline{X}]]/(\underline{p})L[[\underline{X}]].$$

Now assume that we have equality, then the above map is an isomorphism. Since $K[[\underline{X}]]/(\underline{p}) \subset K[[\underline{X}]]/(\underline{p}) \otimes_K L$, the desired claim follows. 91 92

Theorem 5.15 is now completely proved. We call it also the *fibre criterion for isogenies*.

§ 5 The V-divided Cartier module

In this paragraph K is a ring of characteristic p. An important example of isogeny is the Frobenius homomorphism.

We consider the ring homomorphism

$$\begin{aligned} \mathrm{Frob} : K &\longrightarrow K \\ c &\longmapsto c^p. \end{aligned}$$

Clearly Frob defines a functor $\mathrm{Nil}_K \to \mathrm{Nil}_K$, $\mathscr{N} \mapsto \mathscr{N}^{(p)}$. As functors $\mathscr{N}$ and $\mathscr{N}^{(p)}$ are isomorphic, but the K-algebra structure on $\mathscr{N}^{(p)}$ is the following:

$$c \cdot n = c^p n.$$

If one goes to the m-th power Frob^m, one obtains $\mathscr{N}^{(p^m)}$.

Let $G : \mathrm{Nil}_K \to \mathrm{Ens}$ be a functor and $G^{(p^m)} = \mathrm{Frob}^m G$ be the functor obtained by base change. By definition, one has

$$G^{(p^m)}(\mathscr{N}) = G(\mathscr{N}^{(p^m)}).$$

The map $\mathscr{N} \mapsto \mathscr{N}^{(p^m)}$, $n \mapsto n^{p^m}$ is a K-algebra homomorphism. Applying the functor G one obtains

$$G(\mathscr{N}) \longrightarrow G(\mathscr{N}^{(p^m)}) = G^{(p^m)}(\mathscr{N}).$$

The resulting morphism of functors is called the *Frobenius*:

$$\mathrm{Fr}_G^m : G \to G^{(p^m)}.$$

We set $\mathrm{Fr}_G = \mathrm{Fr}_G^1$. Then $\mathrm{Fr}_G^m = \mathrm{Fr}_{G^{(p^{m-1}}} \circ \mathrm{Fr}_{G^{(p^{m-2}}} \circ \cdots \circ \mathrm{Fr}_G$. The rule $G \mapsto G^{(p^m)}$ is a functor. If $\alpha : H \to G$ is a morphism, one has a commutative diagram

$$\begin{array}{ccc} H & \xrightarrow{\alpha} & G \\ {\scriptstyle \mathrm{Fr}_H^m}\downarrow & & \downarrow{\scriptstyle \mathrm{Fr}_G^m} \\ H^{(p^m)} & \xrightarrow{\alpha^{(p^m)}} & G^{(p^m)}. \end{array}$$

Similar statements hold for functors $G : \mathrm{Nil}_K \to \mathrm{Ab}$.

Let $R \in \mathrm{Compl}_K$ and $R' = R \mathbin{\widehat{\otimes}}_{K,\mathrm{Frob}^m} K = \varprojlim R/\mathfrak{a}_n \otimes_{K,\mathrm{Frob}^m} K$. We consider R' as a K-algebra via the K-action on the second factor. By definition of the tensor product, one has the relation

$$rc_1 \mathbin{\widehat{\otimes}} c_2 = r \mathbin{\widehat{\otimes}} c_1^{p^m} c_2, \quad r \in R, \quad c_1, c_2 \in K. \qquad \begin{matrix} \mathbf{92} \\ \mathbf{93} \end{matrix}$$

We have $(\mathrm{Spf}\, R)^{p^m} = \mathrm{Spf}\, R'$. The comorphism of Fr^m is

$$\begin{aligned} R \mathbin{\widehat{\otimes}}_{K,\mathrm{Frob}^m} K &\longrightarrow R \\ r \mathbin{\widehat{\otimes}} c &\longmapsto r^{p^m} c, \quad r \in R, \quad c \in K. \end{aligned}$$

Let $R = K[[\underline{X}]]$. Then we have $R' = K[[\underline{X}]]$. The comorphism of Fr^m is

$$K[[\underline{X}]] \longrightarrow K[[\underline{X}]]$$
$$X_i \longmapsto X_i^{p^m}.$$

The kernel of Fr^m is represented by $K[[\underline{X}]]/(X_1^{p^m}, \ldots, X_n^{p^m})$. This is a free K-module with basis $X_1^{e_1} \ldots X_n^{e_n}$, $0 \leqslant e_i < p^m$ of rank p^{nm}. We find:

5.18. Lemma: Let G be a formal group of dimension n. Then Fr^m is an isogeny of height nm.

For the formal group of Witt vectors, one has $\widehat{W} \simeq \widehat{W}^{(p^m)}$. By 4.27, the map $\mathrm{Fr}^m : \widehat{W}(\mathscr{N}) \to \widehat{W}(\mathscr{N})$ is left multiplication by V^m. We now compute the effect of Frobenius on the Cartier module.

The homomorphism $\mathrm{Frob}^m : K \to K$ induces an endomorphism of the Cartier ring $\mathbb{E}_p \to \mathbb{E}_p$, $\xi \mapsto \xi^{F^m}$. If $\xi = \sum V^r [c_{r,s}]\, F^s$, then $\xi^{F^m} = \sum V^r [c_{r,s}^{p^m}]\, F^s$. One has the relations

$$\xi V = V \xi^F, \quad F\xi = \xi^F F.$$

Let G be a formal group and M its Cartier module. According to 4.43, we find

$$M_{G^{(p^m)}} = \mathbb{E}_p \,{}_{F^m, \mathbb{E}_p} \widehat{\otimes}\, M.$$

In the tensor product, the relation $\xi_1 \mathbin{\widehat{\otimes}} \xi_2 u = \xi_1 \xi_2^{F^m} \mathbin{\widehat{\otimes}} u$, $\xi_1, \xi_2 \in \mathbb{E}_p$, $u \in M$ holds. One has a map of Cartier modules

$$\mathrm{fr}^m : M \longrightarrow \mathbb{E}_p \,{}_{F^m, \mathbb{E}_p} \widehat{\otimes}\, M$$
$$u \longmapsto V^m \mathbin{\widehat{\otimes}} u.$$

This map is $\mathbb{E}_p$-linear:

$$\mathrm{fr}^m(\xi u) = V^m \mathbin{\widehat{\otimes}} \xi u = V^m \xi^{F^m} \mathbin{\widehat{\otimes}} u = \xi V^m \mathbin{\widehat{\otimes}} u = \xi\, \mathrm{fr}^m\, u.$$

5.19. Lemma: The Frobenius $\mathrm{Fr}_G^m : G \to G^{(p^m)}$ induces fr^m on the Cartier modules.

Proof: We remarked already that $\widehat{W}(\mathscr{N}^{(p^m)}) = \widehat{W}(\mathscr{N})$ as abelian groups. One obtains
93 94 $\widehat{W}(\mathscr{N}^{(p^m)})$ from $\widehat{W}(\mathscr{N})$ as right $\mathbb{E}_p$-module by the following definition:

$$w \cdot \xi = w \xi^{F^m}, \quad \text{where } w \in \widehat{W}(\mathscr{N}),\ \xi \in \mathbb{E}_p.$$

This follows immediately from 4.27. Therefore

$$G(\mathscr{N}^{(p^m)}) = \widehat{W}(\mathscr{N}^{(p^m)}) \otimes_{\mathbb{E}_p} M = \widehat{W}(\mathscr{N}) \otimes_{F^m, \mathbb{E}_p} M.$$

Since we have seen already that Fr^m acting on $\widehat{W}(\mathscr{N})$ is right multiplication by V^m, the claim follows.

Let G be a formal group. Consider the inductive system

$$G \xrightarrow{\mathrm{Fr}} G^{(p)} \xrightarrow{\mathrm{Fr}} G^{(p^2)} \xrightarrow{\mathrm{Fr}} \ldots$$

From this we obtain an inductive system of $\mathbb{E}_p$-modules $M_{G^{(p^m)}}$.

5.20. Definition: $\widetilde{M}_G = \varinjlim M_{G^{(p^m)}}$ is called the *V-divided Cartier module* of G.

If K is reduced, the map $K[[\underline{X}]]^{(p^m)} \to K[[\underline{X}]]^{(p^{m+1})}$ as well as the map $M_{G^{(p^m)}} \to M_{G^{(p^{m+1})}}$ are injective. In this case $\widetilde{M}_G$ is the union of the submodules $M_{G^{(p^m)}}$. The maps $\mathbb{E}_{pF^m,\mathbb{E}_p} \otimes M_G \to \mathbb{E}_{pF^{m+1},\mathbb{E}_p} M_G$, $\xi \otimes u \mapsto \xi^F \otimes u$ induce a map $\widetilde{M}_G \to \widetilde{M}_G$ that we denote by V^{-1}. One checks easily the relations

$$V^{-1}\xi u = \xi^F V^{-1} u, \quad VV^{-1} = V^{-1}V = \mathrm{id}_{\widetilde{M}_G}, \quad u \in \widetilde{M}_G,\ \xi \in \mathbb{E}_p.$$

The V-divided Cartier module $\widetilde{\mathbb{E}}_p$ can be described in the following way. One considers the set of all symbols ξV^{-a}, $\xi \in \mathbb{E}_p$, $a \in \mathbb{N}$. Call ξV^{-a} and ηV^{-b} *equivalent* if there exists $r \geqslant a, b$ such that $\xi V^{r-a} = \eta V^{r-b}$ in $\mathbb{E}_p$. The set of equivalence classes of such symbols can be identified with $\widetilde{\mathbb{E}}_p$. A ring structure is defined on $\widetilde{\mathbb{E}}_p$:

$$\xi V^{-a} + \eta V^{-b} = (\xi V^b + \eta V^a) V^{-(a+b)}, \qquad \xi V^{-a} \eta V^{-b} = \xi \eta^{F^a} V^{-(a+b)}.$$

Obviously $\widetilde{\mathbb{E}}_p$ acts on $\widetilde{M}_G$.

5.21. Remark: Let M be a flat $\mathbb{E}_p$-module. such that M/VM is a K-module of finite presentation. The maps

$$\begin{aligned} \mathbb{E}_{pF^m,\mathbb{E}_p} \otimes M &\longrightarrow \widetilde{\mathbb{E}}_p \otimes_{\mathbb{E}_p} M \\ \xi \otimes u &\longmapsto \xi V^{-a} \otimes u \end{aligned}$$

define an isomorphism (*cf* 4.45)

$$\widetilde{M} = \widetilde{\mathbb{E}}_p \otimes_{\mathbb{E}_p} M. \qquad \begin{matrix} 94 \\ 95 \end{matrix}$$

Let M be a V-reduced Cartier module with a V-basis m_i, $i \in I$. Then $m'_i = 1 \otimes m_i$, $i \in I$ form a V-basis of $M^{(p)} = \mathbb{E}_{pF,\mathbb{E}_p} \otimes M$. Let $Fm_i = \sum V^n \alpha_{n,i,j} m_j$ be the structure equations of M (*cf* 4.39). Then $Fm'_i = \sum V^n \alpha^F_{n,i,j} m'_j$ are the structure equations of M. The Frobenius $\mathrm{fr} : M \to M^{(p)}$ has the following expression:

$$\sum V^n [c_{n,i}] m_i \longmapsto \sum V^{n+1} [c^p_{n,i}] m'_i.$$

Let G be a formal group and M its Cartier module. The map $\mathbb{E}_{pF,\mathbb{E}_p} \mathbin{\widehat{\otimes}} M \to M$, $\xi \mathbin{\widehat{\otimes}} u \mapsto \xi F u$ defines a morphism $V_G : G^{(p)} \to G$ that we call the *Verschiebung*. We have

$$\mathrm{Fr}_G V_G = V_G \mathrm{Fr}_G = p.$$

§ 6 The surjectivity of isogenies

In this paragraph, we will show that the V-divided Cartier module classifies formal groups up to isogeny. For this, we need a few elementary techniques of faithfully flat descent.

5.22. Lemma: Let $K \to K'$ be a faithfully flat ring extension and M a K-module. Then, one has a fibre product diagram

$$\begin{array}{ccc} M & \longrightarrow & M \otimes_K K' \\ \downarrow & & \downarrow{\scriptstyle p_1} \\ M \otimes_K K' & \xrightarrow{p_2} & M \otimes_K K' \otimes_K K', \end{array}$$

where $p_1(m \otimes k') = m \otimes k' \otimes 1$ and $p_2(m \otimes k') = m \otimes 1 \otimes k'$.

Proof: The lemma claims that the following sequence is exact:

$$\begin{array}{ccccc} 0 \longrightarrow M & \xrightarrow{d_0} & M \otimes_K K' & \xrightarrow{d_1 = p_1 - p_2} & M \otimes_K K' \otimes_K K' \\ & m \longmapsto & m \otimes 1 & & \end{array}$$

Since K' is faithfully flat over K, it is enough to prove exactness of the following sequence:

$$0 \longrightarrow M \otimes K' \xrightarrow{d_0 \otimes K'} M \otimes K' \otimes K' \xrightarrow{d_1 \otimes K'} M \otimes_K K' \otimes K' \otimes K'. \tag{5.22.1}$$

We define maps

$$s_1 : M \otimes K' \otimes K' \otimes K' \to M \otimes K' \otimes K', \quad m \otimes k'_0 \otimes k'_1 \otimes k'_2 \mapsto m \otimes k'_0 \otimes k'_1 k'_2$$

and

$$s_0 : M \otimes K' \otimes K' \to M \otimes K', \quad m \otimes k'_0 \otimes k'_1 \mapsto m \otimes k'_0 k'_1.$$

One verifies immediately that

$$s_1 \circ (d_1 \otimes K') + (d_0 \otimes K') \circ s_0 = \mathrm{id}_{M \otimes K' \otimes K'} .$$

The claim follows immediately.

95
96 Let $\alpha : K \to K'$ be a faithfully flat ring extension. We consider left-exact functors $G_1, G_2 : \mathrm{Nil}_K \to \mathrm{Ens}$ and a morphism $\varphi' : G_{1,K'} \to G_{2,K'}$. If p_1, p_2 have the same meaning as in 5.22, then one has a commutative diagram

$$K \xrightarrow{\alpha} K' \underset{p_2}{\overset{p_1}{\rightrightarrows}} K' \otimes_K K'.$$

Then, we have:

$$p_{1*} G_{i,K'} = (p_1 \alpha)_* G_i = (p_2 \alpha)_* G_i = p_{2*} G_{i,K'} = G_{i,K' \otimes K'}$$

for $i = 1, 2$. By base change, one derives from φ' two morphisms

$$\varphi'_1, \varphi'_2 : G_{1,K' \otimes K'} \longrightarrow G_{2,K' \otimes K'}$$

where $\varphi'_i = p_{i*}\varphi'$. The equality $\varphi'_1 = \varphi'_2$ means the following. Let $\mathscr{M}$ be a $K' \otimes K'$-module. Then, the map $\varphi' : G_{1,K'}(\mathscr{M}) \to G_{2,K'}(\mathscr{M})$ is independent of whether we look at $\mathscr{M}$ as a K'-module via the first or the second factor. If a morphism $\varphi : G_1 \to G_2$ such that $\varphi' = \varphi_{K'}$ exists, then obviously $\varphi'_1 = \varphi'_2$ holds.

5.23. Lemma: If $\varphi'_1 = \varphi'_2$, then there exists a uniquely determined morphism $\varphi : G_1 \to G_2$ such that $\varphi_{K'} = \varphi$.

Proof: Let $\mathscr{N} \in \mathrm{Nil}_K$. From the fibre product diagram

$$\begin{array}{ccc} \mathscr{N} & \longrightarrow & \mathscr{N} \otimes K' \\ \downarrow & & \downarrow \\ \mathscr{N} \otimes K' & \longrightarrow & \mathscr{N} \otimes K' \otimes K' \end{array}$$

one derives a commutative diagram with exact rows

$$\begin{array}{ccccc} G_1(\mathscr{N}) & \longrightarrow & G_1(\mathscr{N} \otimes K') & \overset{p_1}{\underset{p_2}{\rightrightarrows}} & G_1(\mathscr{N} \otimes K' \otimes K') \\ & & \downarrow{\scriptstyle \varphi'} & & \downarrow{\scriptstyle \varphi'_1 = \varphi'_2} \\ G_2(\mathscr{N}) & \longrightarrow & G_2(\mathscr{N} \otimes K') & \overset{p_1}{\underset{p_2}{\rightrightarrows}} & G_2(\mathscr{N} \otimes K' \otimes K'). \end{array}$$

Hence we obtain a morphism $\varphi : G_1(\mathscr{N}) \to G_2(\mathscr{N})$. One sees easily that $\varphi_{K'} = \varphi'$.

5.24. Theorem: Let $\varphi : G_1 \to G_2$ be an isogeny of formals groups and N its kernel. Let $\psi : G_1 \to H$ be a morphism to a left-exact functor $H : \mathrm{Nil}_K \to \mathrm{Ab}$ such that $\psi|_N = 0$. Then there exists a uniquely determined morphism $\chi : G_2 \to H$ such that the following diagram is commutative:

$$\begin{array}{ccccccc} 0 & \longrightarrow & N & \longrightarrow & G_1 & \xrightarrow{\varphi} & G_2 \\ & & & & {\scriptstyle \psi}\downarrow & \swarrow{\scriptstyle \chi} & \\ & & & & H & & \end{array}$$

Proof: Let A be a nilpotent augmented K-algebra with augmentation ideal A^+. Let $\xi \in G_2(A^+)$. We define $\chi(\xi) \in H(A^+)$. Using 5.23, one can reduce easily to the case where $G_2 = \mathrm{Spf}\, K[[\underline{X}]]$ and $G_1 = \mathrm{Spf}\, K[[\underline{Y}]]$. Indeed, if we have constructed χ' over a faithfully flat extension K' of K, it follows from uniqueness that $\chi'_1 = \chi'_2$. We then obtain the desired morphism χ with 5.23. 96 97

Let $K[[\underline{X}]] \to K[[\underline{Y}]]$ be the comorphism of φ. Then to ξ corresponds a homomorphism $K[[\underline{X}]] \to A$. Let $A' = A \otimes_{K[[\underline{X}]]} K[[\underline{Y}]]$. This is a nilpotent augmented K-algebra which according to 5.8 is faithfully flat over A. By Lemma 5.22, one derives an exact sequence

$$0 \longrightarrow G_1(A^+) \longrightarrow G_1((A')^+) \xrightarrow{G_1(p_1) - G_1(p_2)} G_1((A' \otimes_A A')^+).$$

The map $K[[\underline{Y}]] \to A'$ defines a point $\xi' \in G_1((A')^+)$. One sees easily that the image of ξ' in $G_1((A' \otimes_A A')^+)$ lies in $N((A' \otimes_A A')^+)$. Since N lies in the kernel of the map ψ, we have

$$(H(p_1) - H(p_2))(\psi(\xi')) = 0.$$

Thanks to the exact sequence

$$0 \longrightarrow H(A^+) \longrightarrow H((A')^+) \xrightarrow{H(p_1)-H(p_2)} H((A' \otimes_A A')^+)$$

one finds a uniquely determined point $\chi(\xi) \in H(A^+)$ that maps to $\psi(\xi')$. Uniqueness follows, since the morphism $K[[\underline{X}]] \to K[[\underline{Y}]]$ is injective.

§ 7 Isogenies over a ring of characteristic p

5.25. Theorem: Let $\varphi : G_1 \to G_2$ be a morphism of formal groups of the same dimension over a ring of characteristic p. Then, the following conditions are equivalent.

(i) φ is an isogeny.

(ii) There exists a morphism $\psi : G_2 \to G_1^{(p^m)}$ such that $\psi \circ \varphi = \mathrm{Fr}^m_{G_1}$.

(iii) φ induces an isomorphism of the V-divided Cartier modules.

Proof: Let φ be an isogeny and N its kernel. We show that (ii) is fulfilled. Indeed, let $N = \mathrm{Spf}\, R$. The comorphism of the Frobenius has the following expression:

$$\begin{aligned} R \otimes_{K,\mathrm{Frob}^m} K &\longrightarrow R \\ r \otimes k &\longmapsto r^{p^m} k. \end{aligned}$$

For large enough m, we have $(R^+)^{p^m} = 0$. Then this map factors through the augmentation ε of R:

$$\begin{aligned} R \otimes_{K,\mathrm{Frob}^m} K &\longrightarrow K \longrightarrow R \\ r \otimes k &\longmapsto \varepsilon(r) p^m k. \end{aligned}$$

97 98 Therefore Fr^m_N is the zero mapping. We find a commutative diagram

$$\begin{array}{ccccc} N & \longrightarrow & G_1 & \xrightarrow{\varphi} & G_2 \\ {\scriptstyle 0}\downarrow & & \downarrow{\scriptstyle \mathrm{Fr}^m} & \swarrow_{\psi} & \\ N^{(p^m)} & \longrightarrow & G_1^{(p^m)} & & \end{array}$$

The existence of ψ thus follows from 5.24.

By 5.10, the condition (i) follows conversely from (ii). We show that an isogeny induces an isomorphism of V-divided Cartier modules. Indeed, the maps φ and ψ induce maps of V-divided Cartier modules $\varphi_* : \widetilde{M}_1 \to \widetilde{M}_2$ and $\psi_* : \widetilde{M}_2 \to \widetilde{M}_1$ such that $\psi_*\varphi_* = \mathrm{id}_{\widetilde{M}_1}$. It follows that φ_* is injective. Since ψ is likewise an isogeny, we obtain that ψ_* is injective. From this follows that φ_* is bijective. The last implication (iii) $\Rightarrow$ (i) is obtained from the following:

5.26. Theorem: Let G_1 and G_2 be finite-dimensional formal groups over a ring of characteristic p. Let $\alpha : \widetilde{M}_1 \to \widetilde{M}_2$ be an isomorphism of their V-divided Cartier modules. Then there

exists an isogeny $\varphi : G_1 \to G_2^{(p^m)}$, for suitable m, that induces α. Moreover, there exists an isogeny $\psi : G_2^{(p^m)} \to G_1^{(p^m)}$ such that $\psi \circ \varphi = \mathrm{Fr}^r_{G_1}$. If $\varphi : G_1 \to G_2$ is a morphism inducing α, then φ is an isogeny.

Proof: We first consider the case where M_1 and M_2 possess a V-basis. Let $u_1, \ldots, u_s$ be a V-basis for M_1. Then $\alpha(u_1), \ldots, \alpha(u_s)$ are in the image of $M_2^{(p^m)} \to \widetilde{M}_2$ for suitable m. Let $v_1, \ldots, v_r \in M_2^{(p^m)}$ be preimages. We wish to show that $u_i \mapsto v_i$ defines a morphism $M_1 \to M_2^{(p^m)}$. Let $Fu_i = \sum V^n[a_{n,i,j}]\, u_j$ be the structure equations of M_1. It is enough to show that these equalities are also fulfilled by the v_i. Obviously $\rho_i = Fv_i - \sum V^n[a_{n,i,j}]\, v_j$ lies in the kernel of $M_2^{(p^m)} \to \widetilde{M}_2$. It follows that we can find an m' such that the ρ_i are mapped to 0 under the Frobenius $M_2^{(p^m)} \to M_2^{(p^{m'})}$. From this we obtain a map $M_1 \to M_2^{(p^{m'})}$ that induces α. This proves the existence of φ. The map φ is unique in the following sense. Given another map $M_1 \to M_2^{(p^{m''})}$ inducing α, there exists a $t \geqslant m'$ such that the following diagram is commutative:

$$\begin{array}{ccc} M_1 & \longrightarrow & M_2^{(p^{m'})} \\ \downarrow & & \downarrow \\ M_2^{(p^{m'})} & \longrightarrow & M_2^{(p^t)} \end{array}$$

98
99

One constructs the map ψ in a similar way. The equality $\psi \circ \varphi = \mathrm{Fr}^r_{G_1}$ follows from uniqueness.

We consider the comorphisms:

$$\begin{array}{ccc} K[[\underline{Y}]] & \xleftarrow{\varphi^\sharp} & K[[\underline{X}]] \\ & {\scriptstyle (\mathrm{Fr}^r)^\sharp} \nwarrow \quad \nearrow {\scriptstyle \psi^\sharp} & \\ & K[[\underline{Y}]] & \end{array}$$

It follows that $(\underline{Y})$ is nilpotent in $K[[\underline{Y}]]/(\underline{X})K[[\underline{Y}]]$. Therefore the kernel of φ is representable. It follows like in 5.7 that $K[[\underline{Y}]]$ is a finite $K[[\underline{X}]]$-algebra. In order to prove that G_1 and G_2 have the same dimension, we may assume that K is a field. Then, we find:

$$\dim G_1 = \mathrm{Krulldim}\, K[[\underline{Y}]] \leqslant \mathrm{Krulldim}\, K[[\underline{X}]] = \dim G_2.$$

By reasons of symmetry, it follows that $\dim G_1 = \dim G_2$. Thus φ and ψ are isogenies. The last assertion of the theorem is clear.

5.27. Exercise: Let K be a field of characteristic p. Let $\varphi : G_1 \to G_2$ be a morphism of formal groups of the same finite dimension and $K[[\underline{X}]] \to K[[\underline{Y}]]$ the comorphism. Then the following conditions are equivalent.

(i) φ is an isogeny.

(ii) φ induces an injection of the Cartier modules $M_1 \to M_2$.

(iii) The comorphism $K[[\underline{X}]] \to K[[\underline{Y}]]$ is injective.

(iv) The comorphism $K[[\underline{X}]] \to K[[\underline{Y}]]$ is finite.

We remark that for the proof, one can reduce to the case of a perfect field.

§ 8 p-divisible and unipotent formal groups

5.28. Definition: A formal group G over a $\mathbb{Z}_{(p)}$-algebra K is called *p-divisible* if the multiplication by $p : G \to G$ is an isogeny. If p is an isogeny of height h, one says that G *has height h*.

5.29. Theorem: Let G_1, G_2 be formal p-divisible groups of heights h_1 and h_2. If there is an isogeny $\varphi : G_1 \to G_2$, then $h_1 = h_2$.

Proof: One considers the commutative diagram

$$\begin{array}{ccc} G_1 & \xrightarrow{\varphi} & G_2 \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p} \\ G_1 & \xrightarrow{\varphi} & G_2 \end{array}$$

99 / 100 and applies 5.10 .

5.30. Theorem (Rigidity): Let K be a $\mathbb{Z}_{(p)}$-algebra. Let $\mathfrak{a} \subset K$ be a nilpotent ideal and $K' = K/\mathfrak{a}$ the quotient ring. Let G_1 and G_2 be formal groups over K, and assume that G_1 is p-divisible. Let $\varphi_1, \varphi_2 : G_1 \to G_2$ be morphisms such that $\varphi_{1,K'} = \varphi_{2,K'}$. Then $\varphi_1 = \varphi_2$.

Proof: One can obviously assume that $\mathfrak{a}^p = 0$. According to 4.47, we have $\varphi_1 p = \varphi_2 p$. From the uniqueness statement in 5.24, the claim follows.

5.31. Corollary: The group $\mathrm{Hom}(G_1, G_2)$ is torsion-free and we have:

$$\mathrm{Hom}(G_1, G_2) \otimes \mathbb{Q} = \mathrm{Hom}(G_{1,K'}, G_{2,K'}) \otimes \mathbb{Q}.$$

Proof: By 5.24 the group $\mathrm{Hom}(G_1, G_2)$ has no p-torsion. A prime ℓ different from p induces an isomorphism on the tangent space of G_1 and hence an isomorphism of G_1. Thus $\mathrm{Hom}(G_1, G_2)$ is torsion-free. The last claim follows from 4.47 and 5.30.

5.32. Lemma: Let G be a finite-dimensional formal group over a field of characteristic p. Then G is p-divisible if and only if $F : M_G \to M_G$ is injective.

Proof: This follows from 5.27 and the equality $p = VF$.

Let G be a 1-dimensional formal group over a field of characteristic p. Let $\gamma \in M_G$ be a V-basis and $F\gamma = \sum_{m=h-1}^{\infty} V^m[a_m]\,\gamma$, $a_{h-1} \neq 0$, the structure equation. Then G is p-divisible of height h when $h \neq \infty$ and isomorphic to the additive group when $h = \infty$. In fact, one can

write the structure equation in the form $p\gamma = V^h\gamma'$, where γ' is a V-basis of M_G. It follows that in suitable coordinates, the multiplication by p has the form $K[[X]] \to K[[Y]]$, $X \mapsto Y^{p^h}$.

5.33. Theorem: Two 1-dimensional p-divisible formal groups over a separably closed field of characteristic p are isomorphic if and only if their heights are equal.

Proof: Let G be such a group and M its Cartier module. We must show that there exists an element $\gamma \in M$ such that $F\gamma = V^s\gamma$. Let $F\gamma_0 = \sum_{m=s}^{\infty} V^m[a_m]\,\gamma_0$, $a_s \neq 0$. Let $x \in K$. Then we have:

$$F[x]\gamma_0 = [x^p]\sum_{m=s}^{\infty} V^m[a_m]\,\gamma_0 = \sum_{m=s}^{\infty} V^m[a_m x^{p^{m+1}-1}]\,[x]\,\gamma_0.$$

We can choose x in such a way that

$$a_s x^{p^{s+1}-1} = 1.$$

Therefore, we may assume besides that $a_s = 1$.

We show by induction on r the existence of a γ_r such that 100 101

$$F\gamma_r = V^s\gamma_r \mod V^{s+r+1}M.$$

Assume that γ_{r-1} is already constructed. Then we have $F\gamma_{r-1} = V^s\gamma_{r-1} + V^{s+r}[c]\gamma_{r-1} \mod V^{s+r+1}M$. We look for γ_r of the form $\gamma_r = \gamma_{r-1} + V^r[x_r]\gamma_{r-1}$. Then, we have $\gamma_{r-1} = \gamma_r - V^r[x_r]\gamma_r \mod V^{r+1}$. We find:

$$\begin{aligned} F\gamma_r &= F\gamma_{r-1} + V^r\,[x_r^p]\;F\gamma_{r-1} \\ &= V^s\gamma_{r-1} + V^{s+r}[c]\gamma_{r-1} + V^{s+r}\left[x_r^{p^{s+1}}\right]\;\gamma_{r-1} \\ &= V^s\gamma_{r-1} + V^{s+r}[c + x_r^{p^{s+1}}]\gamma_{r-1} \\ &= V^s\gamma_r + V^{s+r}\left[-x_r + c + x_r^{p^{s+1}}\right]\;\gamma_r \mod V^{s+r+1}M. \end{aligned}$$

Since K is separably closed, we can choose x_r so that $-x_r + c + x_r^{p^{s+1}} = 0$. Then γ_r satisfies the equation $F\gamma_r = V^s\gamma_r \mod V^{s+r+1}M$. The element $\gamma = \lim \gamma_r$ fulfills our wishes.

5.34. Exercise: Show that the structure equation $F\gamma = V^{h-1}\gamma$ defines a Lubin-Tate group over $\mathbb{Z}_{(p)}$. We denote it by G. Let $G = \operatorname{Spf}\mathbb{Z}_{(p)}[[\underline{X}]]$ be the curvilinear coordinate system corresponding to the curve γ. Show that the power series $L(X) = \sum_{j=0}^{\infty} X^{p^{hj}}/p^j$ defines a homomorphism $G \to \mathbb{G}_{\mathrm{a}}$. This means $L(G(X,Y)) = L(X) + L(Y)$, or $G(X,Y) = L^{-1}(L(X), L(Y))$, where $L^{-1}(L(X)) = X$.

Show that $G(X,Y)$ is a power series with coefficients in $\mathbb{Z}$. Find the invariant differential of G.

The objects opposite to p-divisible formal groups are the unipotent formal groups.

5.35. Definition: A formal group G is called *unipotent* when F acts as a nilpotent operator on M_G.

5.36. Theorem: Let G be a finite-dimensional formal group over a field K of characteristic p. Then, there exists an exact sequence of functors

$$0 \longrightarrow G^{\mathrm{u}} \longrightarrow G \longrightarrow G^{\mathrm{bt}} \longrightarrow 0,$$

where G^{u} is a unipotent group and G^{bt} is a p-divisible group. Moreover there exists an isogeny $G^{\mathrm{u}} \times G^{\mathrm{bt}} \to G$.

Proof: Let $M' = \{m \in M_G \,|\, p^N m = 0 \text{ for some } N \gg 0\}$. Then M' is a Cartier submodule of M such that $VM \cap M' = VM'$. Therefore, $M/M' = M''$ is a V-reduced Cartier module over which p operates injectively. The exact sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

provides the desired sequence of formal groups.

From the fact that M' is finitely generated, it follows that $p^{N_0} M' = 0$ for some large enough N_0. Thus p^{N_0} defines an injection $M'' \to M$. We obtain an injection $M' \oplus M'' \to M$ which according to 5.27 defines an isogeny.

5.37. Theorem: Let G be a unipotent formal group over a field K of characteristic p. Then there exists an increasing sequence of subgroups $0 = G_0 \subset G_1 \subset \cdots \subset G_r = G$ and exact sequences of functors

$$0 \longrightarrow G_i \longrightarrow G_{i+1} \longrightarrow \mathbb{G}_{\mathrm{a}} \longrightarrow 0.$$

Proof: Let M be the Cartier module of G. Consider an increasing sequence of $\widetilde{\mathbb{E}}_{(p)}$-submodules of the V-divided Cartier module

$$0 = \widetilde{M_0} \subset \cdots \subset \widetilde{M_r} = \widetilde{M}.$$

Then $M_i = \widetilde{M_i} \cap M$ is a V-reduced Cartier module such that $VM_i = M_i \cap VM = M_i \cap V_{i+1}$. It follows that M_{i+1}/M_i is a V-reduced Cartier module. We find $r \leqslant \sum \dim M_{i+1}/M_i = \dim G$. Now assume that r is chosen maximal. Then M_{i+1}/M_i possesses no proper $\mathbb{E}_p$-submodule. By assumption there exists a nonzero element $m \in M_{i+1}/M_i$ such that $Fm = 0$. Since m is a generating element, it follows that $F(M_{i+1}/M_i) = 0$. Thus M_{i+1}/M_i is isomorphic to the Cartier module of the additive group $\mathbb{G}_{\mathrm{a}}$. The claim follows.

In 4.40, we defined the Witt vectors of length n and we determined their structure equations. The group $\widehat{W}_n$ is visibly unipotent.

5.38. Theorem: Let K be a perfect field of characteristic p. Then any finite-dimensional unipotent formal group over K is isogenous to a direct product of groups $\widehat{W}_n$.

Proof: Let M be the V-divided Cartier module of such a group. For each $m \in M$ let e_m be the smallest natural integer such that $F^{e_m} M = 0$. We consider a generating system $m_1, \ldots, m_r$ of the $\mathbb{E}_p$-module M such that $\sum e_{m_i}$ is minimal. We set $e_i = e_{m_i}$ and we index in such a way that $e_1 \leqslant \ldots \leqslant e_r$. We shall show that the elements $F^{f_i} m_i$, $0 \leqslant f_i < e_i$ generate a V-reduced $\mathbb{E}_p$-module M'. It is clear that every element of M' has a representation

$$\sum V^n [a_{n,i,f_i}]\, F^{f_i} m_i. \tag{5.38.1}$$

Assume that such an expression is 0 with coefficients different from 0. Applying a suitable power of F to (5.38.1), we obtain an expression of the form

$$\sum_{n=0}^{\infty} \sum_{i=1}^{l} V^n [c_{n,i}] F^{e_i - 1} m_i = 0,$$

where a certain $c_{0,l}$ does not vanish. Then $\sum_n V^n[c_{n,l}]$ is a unit in $\mathbb{E}_p$. Consequently 102 103

$$F^{e_l-1}m_l = \sum_{i=1}^{l-1} \eta_i F^{e_i-1}m_i = \sum_{i=1}^{l-1} F^{e_i-1}\eta_i^{F^{-e_i+1}}m_i.$$

Let $m_l' = \sum_{i=1}^{l-1} \eta_i^{F^{-e_i+1}} F^{e_i-e_l}m_i - m_l$. Then $m_1, \ldots, m_l', \ldots, m_r$ is a generating system of M with $e_{m_l'} < e_1$. This contradicts the minimality of $\sum e_i$.

Thus M' is a V-reduced $\mathbb{E}_p$-module and M is its V-divided module. It is obvious that the formal group of M is a direct product of groups $\widehat{W}_n$.

§ 9 Deformations of p-divisible groups

Let K be a $\mathbb{Z}_{(p)}$-algebra. Let $A = K \oplus \mathcal{N}$ be a nilpotent, augmented K-algebra and $\varepsilon : A \to K$ the augmentation morphism. Let G be a formal group over K.

5.39. Definition: A *deformation* $(\widetilde{G}, \iota)$ of G is a formal group $\widetilde{G}$ over A together with an isomorphism $\iota : G \to \varepsilon_*\widetilde{G} = \widetilde{G}_K$. Two deformations G_1 and G_2 of G are called *isomorphic* if there exists an isomorphism $\alpha : G_1 \to G_2$ such that the following diagram is commutative:

$$\begin{array}{ccc} & G & \\ {\scriptstyle \iota_1}\swarrow & & \searrow{\scriptstyle \iota_2} \\ \varepsilon_*G_1 & \xrightarrow{\varepsilon_*\alpha} & \varepsilon_*G_2. \end{array}$$

Let G be a p-divisible group. Then according to 5.12 any deformation of G is again p-divisible. From the Rigidity Theorem 5.30 follows that the unique automorphism of a deformation of G is the identity.

Let $\mathcal{N} \in \mathrm{Nil}_K$. We denote by $\mathrm{Def}_G(\mathcal{N})$ the set of isomorphism classes of deformations of G over $K \oplus \mathcal{N}$. This is a set-valued functor on Nil_K.

5.40. Theorem: Let G be a p-divisible formal group over K. Then Def_G is a smooth functor that commutes with fibre products.

Proof: From 4.46 follows that Def_G is smooth. For the proof of the second assertion, we consider a fibre product diagram of nilpotent augmented K-algebras

$$\begin{array}{ccc} B & \xrightarrow{\sigma_1} & A_1 \\ {\scriptstyle \sigma_2}\downarrow & & \downarrow{\scriptstyle \pi_1} \\ A_2 & \xrightarrow{\pi_2} & A. \end{array}$$

By 2.15, we may assume that π_1 is surjective.

Let G_1 and G_2 be deformations of G over A_1 and A_2, and let $\pi_{1*}G_1 \simeq \pi_{2*}G_2$ be an isomorphism of deformations. Since this isomorphism is uniquely determined, we may identify the latter two groups. We denote them by G_3. Let G_0 be a deformation over B that 103 104

induces G_1 and G_2 by base change. For each $\mathscr{N} \in \mathrm{Nil}_K$ that is projective as a B-module, we have a fibre product diagram

$$\begin{array}{ccc} \mathscr{N} & \longrightarrow & \mathscr{N} \otimes_B A_1 \\ \downarrow & & \downarrow \\ \mathscr{N} \otimes_B A_2 & \longrightarrow & \mathscr{N} \otimes_B A. \end{array}$$

We derive from this an exact sequence

$$0 \longrightarrow G_0(\mathscr{N}) \longrightarrow G_1(\mathscr{N} \otimes_B A_1) \oplus G_2(\mathscr{N} \otimes_B A_2) \longrightarrow G_3(\mathscr{N} \otimes_B A).$$

In particular, one has an exact sequence of Cartier modules:

$$\begin{aligned} 0 \longrightarrow N \longrightarrow M_1 \oplus M_2 &\xrightarrow{\alpha} M_3 \\ m_1 \oplus m_2 &\longmapsto m_1 - m_2. \end{aligned}$$

It follows that the deformation G_0 is uniquely determined. Its existence will follow if we prove that $N = \ker \alpha$ is a reduced $\mathbb{E}_{p,A}$-module (*cf* 3.27). It is clear that N is V-reduced. It remains to prove that N/VN is a projective B-module. Since we assumed that π_1 is surjective, then α is surjective also. We obtain an exact sequence

$$0 \longrightarrow N/VN \longrightarrow M_1/VM_1 \oplus M_2/VM_2 \longrightarrow M_3/VM_3 \longrightarrow 0.$$

By localization, one can reduce to the case where the modules M_i/VM_i are free. Let $e_{2,i}$ be a basis of the A_2-module M_2/VM_2. Since $M_3/VM_3 = M_2/VM_2 \otimes_{A_2} A$, this basis specializes to a a basis $e_{3,i}$ of M_3/VM_3. Since $A_1 \to A$ is a surjection with nilpotent kernel, the $e_{3,i}$ lift to a basis $e_{1,i}$ of M_1/VM_1. It is now clear that $e_{1,i} \times_{e_{3,i}} e_{2,i}$ is a basis of N/VN.

5.41. Theorem: Let R be a perfect ring of characteristic p and $\mathfrak{a} \in \mathrm{Nil}_K$ such that $\mathfrak{a}^2 = 0$. Let G be a p-divisible formal group over K and M its Cartier module. The deformations of G over $K' = K \oplus \mathfrak{a}$ are in bijection with the K-linear mappings

$$\alpha : VM/pM \longrightarrow \mathfrak{a} \otimes_K M/VM.$$

Proof: (*cf* [18]) Let $\mathbb{E}_p$ and $\mathbb{E}'_p$ be the Cartier rings of K and K'. Let M' be the Cartier module of a p-divisible formal group over K' and $M = \mathbb{E}_p \otimes_{\mathbb{E}'_p} M'$. One has exact sequences:

$$0 \longrightarrow \mathbb{E}_p(\mathfrak{a}) \longrightarrow \mathbb{E}'_p \longrightarrow \mathbb{E}_p \longrightarrow 0$$

104 105
$$0 \longrightarrow \mathbb{E}_p(\mathfrak{a}) \otimes_{\mathbb{E}'_p} M' \longrightarrow M' \longrightarrow M \longrightarrow 0.$$

Obviously, we have $\mathbb{E}_p(\mathfrak{a})^2 = 0$. Therefore $\mathbb{E}_p(\mathfrak{a})$ is an $\mathbb{E}_p$-module and $\mathbb{E}'_p = \mathbb{E}_p \oplus \mathbb{E}_p(\mathfrak{a})$. We notice that $a + b = [a] + [b]$ for $a, b \in \mathfrak{a}$ since this equality obviously holds in $\mathbb{E}' = \Lambda(K'[[X]])$.

Let $V^i[\mathfrak{a}]M'$ be the subgroup generated by all elements of the form $\sum_{s=1}^{r} V^i[a_s]m_s$, $a_s \in \mathfrak{a}$. One finds isomorphisms

$$C = \mathbb{E}_p(\mathfrak{a}) \otimes_{\mathbb{E}'_p} M' \simeq \prod V^i[\mathfrak{a}]M' \simeq \prod \mathfrak{a} \otimes_K M/VM.$$

Here, the right-hand side is an $\mathbb{E}_p$-module in an obvious way. It follows that one has an exact sequence of the form

$$0 \longrightarrow \prod \mathfrak{a} \otimes_K M/VM \longrightarrow M' \longrightarrow M \longrightarrow 0.$$

We remark that FM' is mapped isomorphically onto FM since $FC = 0$.

Let $N \subset M'$ be the subgroup of all elements $m' \in M'$ for which there exists $k \in \mathbb{N}$ such that

$$V^k m' \in FM' + \sum_{i=0}^{k-1} V^i[\mathfrak{a}]M'. \tag{5.41.1}$$

We claim that the canonical projection $N \to M$ has a reciprocal mapping. In order to show this, we shall prove first that V acts as a nilpotent operator on M/FM. Actually, since K is perfect, FM is a V-reduced Cartier module and the inclusion $FM \subset M$ corresponds to the Verschiebung (*cf* 5.21). This induces an isomorphism of V-divided Cartier modules $\widetilde{FM} \simeq \widetilde{M}$.The nilpotency of V follows. Let $m \in M$. We can find $k \in \mathbb{N}$ such that $V^k m = Fm_1$. Let m' and $m'_1 \in M'$ be liftings of m and m_1. Then, we have:

$$V^k m' - Fm'_1 \in \prod_i V^i[\mathfrak{a}]M'.$$

Obviously, one can change m' to ensure that $m' \in N$. In this way the reciprocal mapping is defined.

The Witt ring $W(K)$ and F act on N. Moreover, we have $VN \subset N + [\mathfrak{a}]M'$. Indeed, from (5.41.1) one obtains:

$$V^{k-1}(Vm' - m'_1) \in FM' + \sum_{i=0}^{k-2} V^i[\mathfrak{a}]M', \quad m'_1 \in [\mathfrak{a}]M'.$$

Therefore V defines a map

$$\alpha : N \longrightarrow \mathfrak{a} \otimes_K M/VM.$$

Since FN lies in the kernel of this map and $N = M$, we obtain

$$\overline{\alpha} : M/FM \longrightarrow \mathfrak{a} \otimes_K M/VM.$$

Conversely, one can reconstruct the module M' from $\overline{\alpha}$. Indeed, we have a decomposition $M' = M \oplus C = N \oplus C$ which is compatible with the action of $W(K)$ and F. We define

$$V(m, c) = (Vm, \alpha(m) + Vc), \quad m \in M, c \in C.$$

The operation of $\mathbb{E}_p(\mathfrak{a})$ on M' is visibly:

$$[a](m, 0) = (0, [a]m), \quad a \in \mathfrak{a},\ m \in M. \tag{105 106}$$

Thus the liftings M' are in bijection with the maps $\overline{\alpha}$. The datum of $\overline{\alpha}$ is equivalent to that of a linear map

$$\overline{\alpha}V^{-1} : VM/pM \longrightarrow \mathfrak{a} \otimes_K M/VM.$$

5.42. Theorem: Let G be a p-divisible group over a perfect ring K of characteristic p. Then $\mathrm{Def}_G : \mathrm{Nil}_K \to \mathrm{Ens}$ is a prorepresentable functor. For each $\mathscr{N} \in \mathrm{Nil}_K$, one has a bijection between $\mathrm{Def}_G(\mathscr{N})$ and the set of K-linear mappings

$$VM/pM \longrightarrow \mathscr{N} \otimes_K M/VM.$$

Proof: From the proof of the preceding theorem follows that VM/pM is killed by a power of V. Since K is perfect, the K-module $V^iM/V^{i+1}M$ is finitely generated for all i. From this follows that VM/pM is also a finitely generated K-module. If $\mathscr{N}^2 = 0$, then by 5.41 the following holds:

$$\mathrm{Def}_G(\mathscr{N}) = \mathrm{Hom}_K(VM/pM \otimes_K (M/VM)^*, \mathscr{N}),$$

where $(M/VM)^* = \mathrm{Hom}_K(M/VM, K)$ is the dual module.

Since Def_G is an exact functor on $\mathrm{Mod}_K \subset \mathrm{Nil}_K$, the K-module VM/pM is finitely generated and projective. From this and 2.31 follows that Def_G is prorepresented by

$$\mathrm{Spf}\, S^\wedge(VM/pM \otimes_K (M/VM)^*).$$

The theorem follows.

Remark: the correspondence of 5.41 between deformations of G and K-linear maps is visibly functorial. For the correspondence in 5.42, this fact is in general not true.

5.43. Corollary: M/pM is a finitely generated projective K-module whose rank is equal to the height of G.

Proof: Let $\mathfrak{m}$ be a maximal ideal of K. Then $K/\mathfrak{m} = K'$ is a perfect field. Let $M_{K'}$ be the Cartier module of $G_{K'}$. Then by 4.43 and 4.45, we have:

$$M_{K'}/pM_{K'} = \mathbb{E}_{K',p} \otimes_{\mathbb{E}_{K,p}} M/pM.$$

We have an isomorphism:

$$\begin{aligned} \mathbb{E}_{K',p} \otimes_{\mathbb{E}_{K,p}} M/pM &= K' \otimes_K M/pM \\ [k'] \otimes m &\longmapsto k' \otimes m \\ \textstyle\sum V^s[c'_{s,r}]F^r \otimes m &\longmapsto \textstyle\sum c'^{\,p^{-s}}_{s,r} \otimes V^sF^rm. \end{aligned}$$

The last sum is finite since V is nilpotent on M/pM. Since we already know that M/pM is a finitely generated projective K-module, it is enough to prove the claim for a perfect field.
106 107 Using 5.1, one finds V-bases $m_1, \ldots, m_n$ and $m'_1, \ldots, m'_n$ of M such that

$$pm'_i = V^{h_i}m_i, \quad i = 1, \ldots, n.$$

From 5.2 we see that $\mathrm{height}\, p = \mathrm{height}\, G = \sum h_i$. On the other hand, it is clear that $\dim_K M/pM = \sum h_i$.

5.44. Exercise: a) Let $\psi : G_1 \to G_2$ be an isogeny of formal groups over a perfect field. Show that M_{G_1}/M_{G_2} is a $W(K)$-module of length $\mathrm{height}\, \psi$.

b) Let G be a formal group over a $\mathbb{Z}_{(p)}$-algebra K. Let $\overline{G}$ be a lifting of G to $K[\varepsilon]/\varepsilon^2$. One has an exact sequence of Cartier modules

$$0 \longrightarrow C \longrightarrow \overline{M} \longrightarrow M \longrightarrow 0.$$

We assume that M has a V-basis $m_1, \ldots, m_n$. Then one has structure equations

$$Fm_i = \sum V^t[c_{t,i,j}]m_j, \quad c_{t,i,j} \in K.$$

We choose liftings $\overline{m}_i \in \overline{M}$ of m_i. The structure equations for $\overline{M}$ read

$$Fm_i = \sum V^t[c_{t,i,j}]m_j + \sum V^t[\varepsilon a_{t,i,j}]\overline{m}_j. \tag{5.44.1}$$

We assign to this deformation the Cartier module M' over K with the following structure equations:

$$\begin{aligned} Fm'_i &= \sum V^t[c_{t,i,j}]m'_j + \sum V^t[a_{t,i,j}]u_j \\ Fu_i &= 0, \qquad i = 1, \ldots, n. \end{aligned} \tag{5.44.2}$$

These structure equations define an extension of G by the additive group $\mathbb{G}_{\mathrm{a}}^n$:

$$\begin{aligned} E: \ 0 \longrightarrow M_{\mathbb{G}_{\mathrm{a}}^n} &\longrightarrow M' \longrightarrow M \longrightarrow 0. \\ m'_i &\longmapsto m_i \\ u_i &\longmapsto 0 \end{aligned} \tag{5.44.3}$$

Show that this extension is independent of the choice of the lifings $\overline{m}_i$. One obtains in this way a bijection between the extension of G by $\mathbb{G}_{\mathrm{a}}^n$ and the deformation of G over $K[\varepsilon]/\varepsilon^2$.

5.45. Remark: Let L be a K-module and $\underline{L}^+ : \mathrm{Nil}_K \to \mathrm{Ab}$ the functor $\mathscr{N} \mapsto (L \otimes_K \mathscr{N})^+$. We remark that K acts on $\underline{L}^+$, giving a map $K \to \mathrm{End}\,\underline{L}^+$. It follows that we obtain an action of K on the Cartier module N_L of $\underline{L}^+$ (*cf* 3.29).

Assume that p is nilpotent in K. Let G be a p-divisible group over K with Cartier module M. The group $\mathrm{Ext}^1_{\mathbb{E}_p}(M, N_L)$ is a K-module via the action of K on the second factor. According to Messing [15], the functor $L \mapsto \mathrm{Ext}^1_{\mathbb{E}_p}(M, N_L)$ is representable by a projective K-module V:

$$\mathrm{Hom}_K(V, L) = \mathrm{Ext}^1_{\mathbb{E}_p}(M, N_L). \tag{107 / 108}$$

The identity mapping id_V corresponds to the universal extension

$$0 \longrightarrow N_V \longrightarrow M' \longrightarrow M \longrightarrow 0$$

or

$$0 \longrightarrow \underline{V}^+ \longrightarrow G' \longrightarrow G \longrightarrow 0.$$

From the result of Messing, it follows that Def_G is representable. As an exercise, the reader can prove the result of Messing over a perfect ring.

Chapter VI

Isogeny classes of p-divisible formal groups over a perfect field

§ 1 Crystals and isocrystals

Let K be a perfect field of characteristic p. The Witt ring $W = W(K)$ is a discrete valuation ring with residue field K, with maximal ideal generated by p. The Frobenius $\mathrm{Frob}\, x = x^p$ induces an endomorphism $\sigma = W(\mathrm{Frob}) : W \to W$ that we call the *Frobenius of* W.

Let G be a p-divisible formal group over K and M its Cartier module. According to 5.43, the module M/pM is a finite-dimensional K-vector space, whose dimension equals the height of G. Since M is complete and separated in the p-adic topology, it is a finitely generated W-module, and since the multiplication by p is injective on M, it is free.

6.1. Definition: Let us fix an integer $a \neq 0$. A *σ^a-crystal* (M, V) is a finitely generated free W-module together with a σ^a-linear map

$$V : M \to M, \qquad Vwm = w^{\sigma^a} Vm, \qquad w \in W,\ m \in M.$$

The Cartier module M of a p-divisible, formal group G is a σ^{-1}-crystal. Conversely, we have:

6.2. Lemma: Let (M, V) be a σ^{-1}-crystal such that

a) $pM \subset VM$,

b) V is nilpotent on M/pM.

Then (M, V) is the crystal of a p-divisible formal group G.

Proof: Let $F = pV^{-1}$. It is clear that the ring $W[V, F]$ with relations $FV = VF = p$, $wV = Vw^\sigma$, $Fw = w^\sigma F$ acts on M. Since V is nilpotent on M/pM, the sums of the following form are convergent in the p-adic topology:

$$\sum_{r \geqslant 0} V^r w_r m, \qquad w_r \in W,\ m \in M.$$

Thus M turns into a V-reduced Cartier module.

The category of p-divisible formal groups is therefore equivalent with the category of crystals enjoying the properties a) and b). When one classifies the formal groups up to isogeny, one is led to the notion of isocrystal. Let $\mathcal{K}$ be the fraction field of W.

6.3. Definition: A *σ^a-isocrystal* (N, V) is a finite-dimensional $\mathcal{K}$-vector space N together with a σ^a-linear map $V : N \to N$.

109
110

A finitely generated W-submodule $M \subset N$ is called a *lattice* if the elements of M generate the $\mathcal{K}$-vector space N. In other words, M has a basis as W-module that is at the same time a basis of N as $\mathcal{K}$-vector space.

Let $M' \subset N$ be a second lattice. Then we have $p^s M' \subset M$ for large enough natural integers s. It is clear that $M/p^s M'$ is a W-module of finite length. We define

$$[M : M'] = \text{length}\, M/p^s M' - \text{length}\, M'/p^s M'.$$

If M'' is a third lattice, we have:

$$[M : M''] = [M : M'] + [M' : M''].$$

6.4. Definition: Let (N, V) be an isocrystal. We call the dimension of the $\mathcal{K}$-vector space N the *height* of N. The number $[M : VM]$ is independent of the choice of a lattice $M \subset N$. We call it the *dimension* of N.

Indeed, for a second lattice M' we find:

$$[M' : VM'] = [M' : M] + [M : VM] + [VM : VM'].$$

Since obviously $[VM : VM'] = [M : M'] = -[M' : M]$, we obtain $[M' : VM'] = [M : VM]$.

Let G be a p-divisible formal group and M its Cartier module. Since p induces an isomorphism of the p-divided Cartier module $\widetilde{M}$, then $\widetilde{M}$ is a $\mathcal{K}$-vector space. From the equality

$$V^{-r} m = p^{-r} F^r m, \quad m \in M$$

follows that M is a lattice in $\widetilde{M}$. We have

$$\text{height}\, G = \dim_K M/pM = \text{rank}_W M = \dim_{\mathcal{K}} \widetilde{M}.$$

If G has dimension d and height h, it follows that $(\widetilde{M}, V)$ is an isocrystal of height h and dimension d. It determines G up to isogeny.

6.5. Exercise: Let K be a perfect field of characteristic p. Let $H : \text{Nil}_K \to \text{Ab}$ be a functor which is representable by a finite nilpotent K-algebra. It follows from 2.35 that H is the kernel of an isogeny of formal groups $G_1 \to G_2$:

$$0 \longrightarrow H \longrightarrow G_1 \longrightarrow G_2. \tag{6.5.1}$$

Let M_1 and M_2 be the Cartier modules of G_1 and G_2. One obtains an exact sequence

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M \longrightarrow 0.$$

There is an isomorphism of functors $H(\mathscr{N}) = \mathrm{Tor}_1^{\mathbb{E}_p}(\widehat{W}(\mathscr{N}), M)$. The $\mathbb{E}_p$-module M is of finite length and V is nilpotent on it.

Conversely, let M be an $\mathbb{E}_p$-module with these properties. Then, the functor $\mathscr{N} \mapsto \mathrm{Tor}_1^{\mathbb{E}_p}(\widehat{W}(\mathscr{N}), M)$ is representable by a finite nilpotent K-algebra. One obtains an equivalence of categories $H \mapsto M$. One calls M the *covariant Dieudonné module* of H. The length of M is equal to the height of H. Compute the covariant Dieudonné modules of α_p and μ_p (*cf* 2.34). 110 111

That M is independent of the chosen representation (6.5.1) is proven in the following way. One tensors the sequence

$$0 \longrightarrow \mathbb{E}_p \xrightarrow{V^N} \mathbb{E}_p \longrightarrow \mathbb{E}_p/V^N\mathbb{E}_p \longrightarrow 0$$

with M. Then one obtains for large N an isomorphism

$$M \simeq \mathrm{Tor}_1^{\mathbb{E}_p}(\mathbb{E}_p/V^N\mathbb{E}_p, M).$$

§ 2 The first Newton slope of an isocrystal

6.6. Definition: Let (N, V) be an isocrystal, $M \subset N$ a lattice and $m \in M$. We define:

$$\mathrm{ord}_M V = \max\{\, k \in \mathbb{Z}, VM \subset p^k M \,\},$$
$$\mathrm{ord}_M m = \max\{\, k \in \mathbb{Z}, m \in p^k M \,\}.$$

6.7. Lemma: Let M and M' be lattices in an isocrystal (N, V). Let c and c' be integers such that $p^c M \subset M'$ and $p^{c'} M' \subset M$. Then, one has:

$$|\mathrm{ord}_M V - \mathrm{ord}_{M'} V| \leqslant c + c', \qquad |\mathrm{ord}_M m - \mathrm{ord}_{M'} m| \leqslant \max(c, c').$$

Proof: Let $x = \mathrm{ord}_M m$ and $y = \mathrm{ord}_M V$. Then, we have $m \in p^x M \subset p^{x-c} M'$ and $VM' \subset p^{-c'} VM \subset p^{y-c'} M \subset p^{y-c-c'} M'$. We obtain $\mathrm{ord}_{M'} m \leqslant \mathrm{ord}_M m - c$ and $\mathrm{ord}_{M'} V \leqslant \mathrm{ord}_M V - c' - c$. The claim follows if one switches the roles of M and M'.

6.8. Lemma: Let (N, V) be an isocrystal of dimension d and height h. Then for all lattices $M \subset N$ and all natural numbers $n \neq 0$, we have

$$\mathrm{ord}_M V \leqslant (1/n)\,\mathrm{ord}_M V^n \leqslant d/h.$$

If there exists n such that $\mathrm{ord}_M V \neq (1/n)\,\mathrm{ord}_M V^n$, then

$$\mathrm{ord}_M V + (1/h) \leqslant (1/h)\,\mathrm{ord}_M V^h.$$

Proof: From the inclusion $VM \subset p^x M$ we obtain $V^n M \subset p^{nx} M$, and from $V^n M \subset p^y M$ we obtain

$$nd = n[M : VM] = [M : V^n M] \geqslant [M : p^y M] = y[M : pM] = yh.$$

Thus we have proved that $\operatorname{ord}_M V \leqslant (1/n)\operatorname{ord}_M V^n \leqslant d/h$.

Let $x = \operatorname{ord}_M V$ and $V^n M \subset p^{nx+1}M$ for some $n > 1$. We set $M_i = \{\, m \in M \mid V^i m \in p^{ix+1}M \,\}$. From $VM \subset p^x M$ it follows that:

$$pM = M_0 \subset M_1 \subset \cdots \subset M_n = M.$$

One checks easily that if $M_i = M_{i+1}$ then also $M_i = M_j$ for all $j \geqslant i$. Since $\dim_K M/pM = h$, 111 112 we get $M_h = M$. We obtain the desired inequality.

6.9. Definition: Let (N, V) be an isocrystal. If there exists a lattice $M \subset N$ such that $VM \subset M$, we call (N, V) *effective*.

6.10. Lemma: Let (N, V) be an isocrystal of height h and M a lattice of N such that $V^{h+1}M \subset p^{-1}M$. Then (N, V) is effective.

Proof: Consider the lattice

$$M' = \sum_{j=0}^{h} V^j M.$$

We have: $\sum_{j=0}^{h+1} V^j M' = \sum_{j=0}^{2h+1} V^j M = M' + \sum_{j=0}^{h} V^j(V^{h+1}M) \subset p^{-1}M'$. We consider the increasing chain

$$M' \subset M' + VM' \subset \cdots \subset \sum_{j=0}^{h+1} V^j M' \subset p^{-1}M'.$$

Since $\dim_K p^{-1}M' = h$, we find an n such that

$$\sum_{j=0}^{n} V^j M' = \sum_{j=0}^{n+1} V^j M' = M''.$$

Then obviously $VM'' \subset M''$. Q.E.D.

6.11. Definition: For an isocrystal (N, V), we call

$$\operatorname{Newton}(N, V) = \sup\{\, (1/n)\operatorname{ord}_M V^n \mid n \in \mathbb{N} \setminus \{0\}, M \subset N \text{ a lattice} \,\}$$

the *first Newton slope of* (N, V).

6.12. Lemma: Let (N, V) be an isocrystal and $M \subset N$ a lattice. Then one has:

$$\operatorname{Newton}(N, V) = \lim_{n\to\infty} (1/n)\operatorname{ord}_M V^n,$$

$$\operatorname{Newton}(N, p^s V^r) = r \operatorname{Newton}(N, V) + s.$$

Proof: Let λ be the first Newton slope of (N, V). We consider an arbitrary lattice $M' \subset N$. Let $x = \operatorname{ord}_{M'} V^n$ for some $n \in \mathbb{N} \setminus \{0\}$. We can find integers c and c' such that $p^c M \subset M'$ and $p^{c'} M' \subset M$. Then by 6.7 we have:

$$\begin{aligned}\sup_m (1/m)\operatorname{ord}_M V^m &\geqslant \sup_k (1/kn)\operatorname{ord}_M V^{kn} \geqslant \sup_k (1/kn)(\operatorname{ord}_{M'} V^{kn} - c - c') \\ &\geqslant \sup_k (x/n) - (c + c')/kn = x/n.\end{aligned}$$

From this we derive $\lambda = \sup_m (1/m) \operatorname{ord}_M V^m$.

Let $\varepsilon > 0$ and $x = \lambda - \varepsilon/2$. By definition we can find an m such that $\operatorname{ord}_M V^m > mx$. Let $r, s \in \mathbb{N}$ be such that $0 \leqslant s < m$. Then we have: $\operatorname{ord}_M V^{mr+s} > mrx + s \operatorname{ord}_M V$. We choose r_0 in such a way that for $r \geqslant r_0$ and $0 \leqslant s < m$:

$$s(\operatorname{ord}_M V - x)/(mr + s) > -\varepsilon/2.$$

Then for $n > mr_0$, we have $n = mr + s$ with $r \geqslant r_0$ and $0 \leqslant s < m$. We find:

$$\lambda \geqslant (1/n) \operatorname{ord}_M V^n > x + s(\operatorname{ord}_M V - x)/(mr + s) > x - \varepsilon/2 = \lambda - \varepsilon.$$

From this follows that $\lambda = \lim_{n\to\infty} (1/n) \operatorname{ord}_M V^n$. The last claim of the lemma is obvious. 112 113

6.13. Lemma: Let (N, V) be an isocrystal. Let $r, s \in \mathbb{Z}$, $r > 0$, be such that $\operatorname{Newton}(N, V) \geqslant s/r$. Then there exists a lattice $M \subset N$ such that $V^r M \subset p^s M$.

Proof: Let h be the height of (N, V). Let $V' = p^{1-s(h+1)} V^{r(h+1)}$. Then (N, V') is an isocrystal with $\operatorname{Newton}(N, V') \geqslant 1$. We can find a lattice $M \subset N$ such that $V'^n M \subset M$ for some $n \geqslant 1$. Let $M' = M + \cdots + V'^{n-1} M$. Then $V' M' \subset M'$ and consequently $(p^{-s} V^r)^{(h+1)} M' \subset p^{-1} M'$. Using 6.10, we find a lattice M'' with $p^{-s} V^r M'' \subset M''$. Q.E.D.

6.14. Lemma: Let $x \in \mathbb{R}$ and $R \geqslant 2$ an integer. Then there exist $r, s \in \mathbb{Z}$ with $1 \leqslant r \leqslant R - 1$ such that $|x - (s/r)| \leqslant 1/(Rr)$.

Proof: For each $r \in \mathbb{Z}$, there exists $t_r \in \mathbb{R}$ such that $rx - t_r \in \mathbb{Z}$ and $-1/R \leqslant t_r < 1 - (1/R)$. We must prove that $t_r \leqslant 1/R$ for some $r = 1, \ldots, R - 1$. Assume that $t_r > 1/R$ for $r = 1, \ldots, R - 1$. Then one finds $r_1 > r_2$ such that $|t_{r_1} - t_{r_2}| \leqslant 1/R$. It follows that $(r_1 - r_2)x - (t_{r_1} - t_{r_2}) \in \mathbb{Z}$ and $-1/R \leqslant t_{r_1} - t_{r_2} \leqslant 1/R$. This contradiction shows the claim.

6.15. Theorem: Let (N, V) be an isocrystal of height h and dimension d. Let $\lambda = \operatorname{Newton}(N, V)$. Then there exist integers r, s and a lattice $M \subset N$ such that $\lambda = s/r$, $0 < r \leqslant h$, $s \leqslant d$, $\operatorname{ord}_M V^r = s$.

Proof: According to 6.14, we can find integers s, r, $1 \leqslant r \leqslant h$, such that

$$|\lambda - (s/r)| \leqslant 1/(r(h + 1)).$$

Let $V' = p^{-s} V^r$ and $\lambda' = \operatorname{Newton}(N, V')$. Then we have $|\lambda'| = |r\lambda - s| \leqslant 1/(h + 1)$. Using 6.13, we find a lattice $M' \subset N$ such that $V'^{h+1} M' \subset p^{-1} M'$. By 6.10, we obtain that (N, V') is effective. We now consider a lattice $M \subset N$ such that $V' M \subset M$. We get:

$$\operatorname{ord}_M V' \geqslant 0 > \lambda' - 1/h \geqslant (1/h) \operatorname{ord}_M V'^h - 1/h.$$

Using 6.8, we obtain $\operatorname{ord}_M V' = (1/n) \operatorname{ord}_M V'^n$ for $n \geqslant 1$. Also $\lambda' = \operatorname{ord}_M V' \in \mathbb{Z}$ and therefore $\lambda' = 0$. We find $\lambda = s/r$ and $\operatorname{ord}_M V^r = s$. Since according to 6.8 and 6.12 we have $\lambda \leqslant d/h$, then $s \leqslant dr/h \leqslant d$.

§ 3 Decomposition of iscrystals over perfect fields

6.16. Lemma: Let (M, V) be a crystal. Then, there is a decomposition

$$(M, V) = (M_{\text{ét}}, V) \oplus (M_l, V)$$

such that $V : M_{\text{ét}} \to M_{\text{ét}}$ is bijective and $V^n M_l \subset pM_l$ for large enough n.

Proof: The map V induces a map $V : M/p^nM \to M/p^nM$. Since M/p^nM is a W-module of finite length, then

$$M_{n,l} := \bigcup_s \ker V^s = \ker V^r, \quad M_{n,\text{ét}} := \bigcap_s \operatorname{Im} V^s = \operatorname{Im} V^r$$

113 114 for large enough r. Obviously V is nilpotent on $M_{n,l}$ and surjective on $M_{n,\text{ét}}$. Since $M_{n,\text{ét}}$ has finite length, one sees easily that $V : M_{n,\text{ét}} \to M_{n,\text{ét}}$ is bijective. Therefore $M_{n,\text{ét}} \cap M_{n,l} = 0$. Let $m \in M/p^nM$. Then $V^r m = V^{2r} m'$ for some m' and thus $m - V^r m' \in M_{n,l}$. In this way we have a direct sum decomposition $M/p^nM = M_{n,\text{ét}} \oplus M_{n,l}$. The claim follows by taking projective limits.

6.17. Definition: An isocrystal (N, V) is called *isoclinic* (one finds also the terms *isocline* and *pure*) if

$$\operatorname{Newton}(N, V) = \frac{\dim(N, V)}{\operatorname{height}(N, V)}.$$

6.18. Lemma: For an isocrystal (N, V) of height h and dimension d, the following conditions are equivalent:

(i) (N, V) is isoclinic.

(ii) There exists a lattice $M \subset N$ such that $V^h M = p^d M$.

(iii) There exist integers r, s with $r > 0$ and a lattice $M \subset N$ such that $V^r M = p^s M$.

(iv) Let $M \subset N$ be a lattice. Then $\operatorname{Newton}(N, V) = \lim_{n\to\infty} (1/n) \operatorname{ord}_M V^n m$ for all $m \in N \backslash \{0\}$.

Proof: The implication (ii) $\Rightarrow$ (iii) is trivial. We show that (i) $\Rightarrow$ (ii). In fact, by 6.15 we can find a lattice M such that $V^h M \subset p^d M$. Then:

$$[p^d M : V^h M] = [M : V^h M] - [M : p^d M] = h[M : VM] - dh = 0.$$

We obtain $V^h M = p^d M$.

(iii) $\Rightarrow$ (i): We have $0 = [p^s M : V^r M] = rd - sh$. Therefore we find $d/h = s/r = (1/r) \operatorname{ord}_M V^r \leqslant \lambda \leqslant d/h$ and thereby $\lambda = \operatorname{Newton}(N, V)$. The claim follows. At this stage, the first three conditions are equivalent.

(ii) $\Rightarrow$ (iv): by 6.7, the limit is independent of the choice of the lattice M. Let $V^h M = p^d M$. Then, for all $m \in \mathbb{N} \setminus \{0\}$ we have:

$$\operatorname{ord}_M V^{hn} m = nd + \operatorname{ord}_M m.$$

Now we choose c such that $|\operatorname{ord}_M V^a m| \leqslant c$ for $0 \leqslant a < h$. We derive:

$$|(1/(hn+a))\operatorname{ord}_M V^{hn+a}m - nd/(hn+a)| \leqslant c/(hn+a).$$

The claim follows by taking limits when $n \to \infty$.

(iv) $\Rightarrow$ (iii): Let $\lambda = s/r$, $s, r \in \mathbb{Z}$ be the first Newton slope of N. By 6.13, we can find a lattice $M \subset N$ with $V^r M \subset p^s M$. Let $V' = p^{-s}V^r$. Then (M, V') is a crystal. We consider the decomposition of 6.16:

$$(M, V') = (M_{\text{ét}}, V') \oplus (M_l, V').$$

By the definition of M_l, there exists $k > 0$ such that $V'^k M_l \subset pM_l$. Assume that there exists a nonzero element $m \in M_l$. Then $\operatorname{ord}_M V'^{kn} m \geqslant n$ holds for all $n \in \mathbb{N}$. We have:

$$(1/rkn)\operatorname{ord}_M V^{rkn}m \geqslant (n/rkn) + (skn/rkn) = 1/(rk) + \lambda.$$

By taking limits when $n \to \infty$ we obtain a contradiction. Thus $M = M_{\text{ét}}$ is an isoclinic isocrystal. 114 115

The isocrystals constitute a category in an obvious way. A morphism $f : (N_1, V_1) \to (N_2, V_2)$ is a $\mathcal{K}$-linear mapping $f : N_1 \to N_2$ such that the following diagram is commutative:

$$\begin{array}{ccc} N_1 & \xrightarrow{f} & N_2 \\ {\scriptstyle V_1}\downarrow & & \downarrow{\scriptstyle V_2} \\ N_1 & \xrightarrow{f} & N_2. \end{array}$$

6.19. Lemma: Let (N, V) be an isocrystal. Let $0 \neq (N_1, V_1) \subset (N, V)$ be a subobject and $(N, V) \to (N_2, V_2)$ a quotient object. Then, the following holds:

$$\operatorname{Newton}(N, V) \leqslant \operatorname{Newton}(N_i, V_i), \quad i = 1, 2.$$

If (N, V) is isoclinic, then equality holds.

Proof: Let $s/r = \operatorname{Newton}(N, V)$. We can find a lattice $M \subset N$ with $V^r M \subset p^s M$. Let $M_1 = N_1 \cap M$ and M_2 the image of M by the map $N \to N_2$. Then we have $V_i^r M_i \subset p^s M_i$, $i = 1, 2$. If $V^r M = p^s M$, one has $V_i^r M_i = p^s M_i$. Q.E.D.

6.20. Corollary: Let (N, V) be an isoclinic isocrystal and (N_1, V_1) an isocrystal with

$$\operatorname{Newton}(N_1, V_1) > \operatorname{Newton}(N, V).$$

Then:

$$\operatorname{Hom}((N, V), (N_1, V_1)) = \operatorname{Hom}((N_1, V_1), (N, V)) = 0.$$

Proof: Let $(N, V) \to (N_1, V_1)$ be a nonzero homomorphism and (N', V') its image. Then we have, in contradiction with the assumption:

$$\operatorname{Newton}(N, V) = \operatorname{Newton}(N', V') \geqslant \operatorname{Newton}(N_1, V_1).$$

The second claim of the corollary follows similarly.

6.21. Lemma: Let (N,V) be an isocrystal with first Newton slope λ. Then (N,V) has a unique decompostion

$$(N,V) = (N_1,V_1) \oplus (N_2,V_2),$$

where (N_1,V_1) is isoclinic with first Newton slope λ and $\mathrm{Newton}(N_2,V_2) > \lambda$.

Proof: We consider a lattice $M \subset N$ with $V^r M \subset p^s M$, where $\lambda = s/r$. Let $V' = p^{-s}V^r$. One has a decomposition as in 6.16: $(M,V) = (M_{\text{ét}},V') \oplus (M_l,V')$. Tensoring with $\mathcal{K}$, we obtain a decomposition of the isocrystal

$$(N,V') = (N_{\text{ét}},V') \oplus (N_l,V'),$$

where $(N_{\text{ét}},V')$ is isoclinic with slope 0 and $\mathrm{Newton}(N_l,V') > 0$. It follows from 6.20 that a
115 decomposition with these properties is unique if it exists. Therefore the above decomposi-
116 tion coincides with $(N,V') = (VN_{\text{ét}},V') \oplus (VN_l,V')$, that is, $VN_{\text{ét}} = N_{\text{ét}}$, $VN_l = N_l$. The decomposition

$$(N,V) = (N_{\text{ét}},V) \oplus (N_l,V)$$

is the desired one, and is obviously unique.

6.22. Theorem: Let (N,V) be an isocrystal with first Newton slope λ. Then, there exist uniquely determined subcrystals (N_i,V_i) with $\mathrm{Newton}(N_i,V_i) = \lambda_i$ such that

$$(N,V) = \bigoplus_{i=1}^{r} (N_i,V_i) \quad \text{and}$$

$$\lambda = \lambda_1 < \lambda_2 < \cdots < \lambda_r. \tag{6.22.1}$$

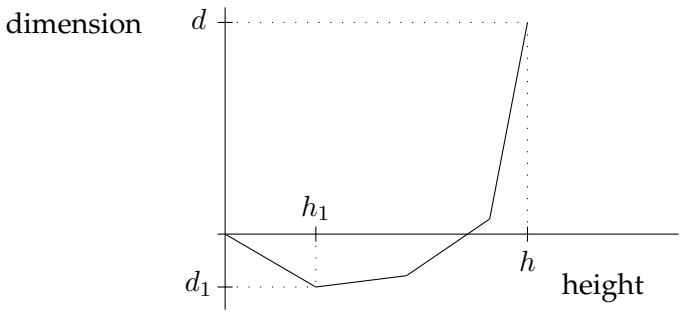
This follows by successive applications of 6.21. We call λ_i the *Newton slopes* of (N,V). Let d_i be the dimension of (N_i,V_i) and h_i its height. The height of (N,V) is $h = \sum_{i=1}^r h_i$, and its dimension is $d = \sum_{i=1}^r d_i$. According to 6.17, we have $\lambda_i = d_i/h_i$. One obtains the sequence of Newton slopes, in which each λ_i from the sequence (6.22.1) is repeated h_i times:

$$(\mu_1,\ldots,\mu_h) = (\underbrace{\lambda_1,\ldots,\lambda_1}_{h_1 \text{ times}},\lambda_2,\ldots,\underbrace{\lambda_r,\ldots,\lambda_r}_{h_r \text{ times}}).$$

Let $\mathrm{Newton}_{(N,V)}(i) = \sum_{j=1}^{i} \mu_j$, $1 \leqslant i \leqslant h$. Then, we have:

$$\mathrm{Newton}(N,V) = \mathrm{Newton}_{(N,V)}(1), \quad d = \mathrm{Newton}_{(N,V)}(h).$$

The graph of the function $i \mapsto \mathrm{Newton}_{(N,V)}(i)$ is called the *Newton polygon* of the isocrystal (N,V). It looks like this:



6.23. Theorem: Let (N, V) be a σ^{-1}-isocrystal (*cf* 6.3), and let $\lambda_1 < \cdots < \lambda_r$ be its Newton slopes. Then (N, V) is the isocrystal of a formal group if and only if $0 < \lambda_1 < \cdots < \lambda_r \leqslant 1$.

Proof: Let (N, V) be the isocrystal of a formal group. Then there exists a lattice M such that

$$VM \subset M, \qquad pV^{-1}M \subset M \quad (\textit{cf} \text{ comment preceding 6.2}).$$ 116 117

Therefore $\lambda_1 = \mathrm{Newton}(N, V) \geqslant 0$, $1 - \lambda_r = \mathrm{Newton}(N, pV^{-1}) \geqslant 0$. Since V is nilpotent on M/pM, it follows that $\lambda_1 > 0$.

Conversely, let (N, V) be an isocrystal whose slopes lie between 0 and 1. Then there exists a lattice $M \subset N$ with $pV^{-1}M \subset M$. Since $\lim_{n\to\infty}(1/n)\,\mathrm{ord}_M\, V^n > 0$, there exists r such that $V^r M \subset pM$. Obviously the lattice $M + \cdots + V^{r-1}M$ fulfills the assumptions of 6.2.

We call a formal p-divisible group *isoclinic* when its isocrystal is isoclinic.

6.24. Corollary: Each p-divisible formal group is isogenous to a direct product of isoclinic formal groups.

§ 4 Classification of isocystals over an algebraically closed field

6.25. Lemma: Let K be an algebraically closed field of characteristic p and $q = p^a$, $a > 0$. Let V be a nonzero K-vector space and $\varphi : V \to V$ a $\mathbb{Z}$-linear isomorphism such that $\varphi(kv) = k^q\varphi(v)$, $k \in K$, $v \in V$. Then there exists a basis $e_1, \ldots, e_n$ of V such that $\varphi(e_i) = e_i$.

Proof: We show that V contains a nonzero φ-invariant vector. Let $v \in V$, $v \neq 0$. Let r be the greatest integer such that the vectors

$$v, \varphi(v), \ldots, \varphi^{r-1}(v)$$

are linearly independent. Then one has a relation

$$\varphi^r(v) = \sum_{i=0}^{r-1} k_i\varphi^i(v), \quad k_i \in K.$$

We look for a vector $w = \sum_{i=0}^{r-1} x_i\varphi^i(v)$ such that $\varphi(w) = w$. The latter equation gives:

$$\varphi(w) = \sum_{i=0}^{r-2} x_i^q\varphi^{i+1}(v) + \sum_{i=0}^{r-1} x_{r-1}^q k_i\varphi^i(v) = \sum_{i=0}^{r-1} x_i\varphi^i(v).$$

We obtain a system of equations for the x_i:

$$\begin{aligned} x_0 &= k_0 x_{r-1}^q \\ x_1 &= x_0^q + k_1 x_{r-1}^q \\ &\vdots \\ x_{r-1} &= x_{r-2}^q + k_{r-1} x_{r-1}^q. \end{aligned}$$

By successive substitutions, we find

$$x_{r-1} = k_0^{q^{r-1}} x_{r-1}^{q^r} + \cdots + k_{r-1} x_{r-1}^q.$$

117 118 Since not all the k_i vanish, this equation has a nonzero solution. This proves the existence of an invariant vector.

Let $e_1, \ldots, e_r$ be a maximal system of linearly independent φ-invariant vectors. Let W be the subspace generated by $e_1, \ldots, e_r$. Assume that $W \neq V$. We have proved that there exists a vector $\overline{e}_{r+1} \in V/W$ such that $\varphi(\overline{e}_{r+1}) = \overline{e}_{r+1}$ and $\overline{e}_{r+1} \neq 0$. Let $e_{r+1} \in V$ be a lifting of $\overline{e}_{r+1}$. We have:

$$\varphi(e_{r+1}) = e_{r+1} + \sum_{i=1}^{r} c_i e_i, \quad c_i \in K.$$

We look for an $e'_{r+1} = e_{r+1} + \sum_{i=1}^r y_i e_i$ such that $\varphi(e'_{r+1}) = e'_{r+1}$, that is to say,

$$\varphi(e'_{r+1}) = e_{r+1} + \sum_{i=1}^{r} (c_i + y_i^q) e_i = e'_{r+1} + \sum_{i=1}^{r} (c_i - y_i + y_i^q) e_i.$$

Obviously, one can choose the y_i so that the brackets vanish.

6.26. Theorem: Let (M, V) be a crystal over an algebraically closed field K such that $VM = M$. Then there exists a basis $e_1, \ldots, e_r$ of M such that $Ve_i = e_i$.

Proof: We can assume that V is σ^a-linear for some $a > 0$. Otherwise, we replace (M, V) be (M, V^{-1}).

We construct by induction on n a basis $e_1^{(n)}, \ldots, e_r^{(n)}$ such that

$$Ve_i^{(n)} = e_i^{(n)} \mod p^n, \quad e_i^{(n)} = e_i^{(n-1)} \mod p^{n-1}.$$

The claim will follow by taking limits when $n \to \infty$.

The initial step of the induction is obtained by 6.25. Let $e_i^{(n)} = f_i$ be previously constructed. Then, we have:

$$Vf_i - f_i = p^n \sum_{j=1}^{r} a_{i,j} f_j, \quad a_{i,j} \in W.$$

Let us look for $e_i^{(n+1)} = h_i$ in the form $h_i = f_i + p^n \sum_{j=1}^r x_{i,j} f_j$. Then, we have:

$$Vh_i - h_i = p^n \sum_{j=1}^{r} (a_{i,j} + x_{i,j}^a - x_{i,j}) f_j.$$

Let $\overline{a}_{i,j}$ and $\overline{x}_{i,j} \in K$ be the residue classes mod p. Obviously, one can choose $x_{i,j}$ in such a way that

$$\overline{a}_{i,j} + \overline{x}^a_{i,j} - \overline{x}_{i,j} = 0$$

and therefore

$$a_{i,j} + x^a_{i,j} - x_{i,j} = 0 \mod p.$$

Then $Vh_i - h_i = 0 \mod p^{n+1}$. Q.E.D.

Let $r, s \in \mathbb{Z}$ with $r > 0$ and $(r, s) = 1$. We consider a $\mathcal{K}$-vector space $N_{s,r}$ with a basis $e_1, \ldots, e_r$. We define on $N_{s,r}$ a structure of σ^a-isocrystal by 118 119

$$Ve_i = \begin{cases} e_{i+1}, & i < r, \\ p^s e_1, & i = r. \end{cases}$$

6.27. Lemma: $N_{s,r}$ is an isoclinic isocrystal of slope s/r that contains no proper subcrystal.

Proof: It is clear that $N_{s,r}$ is isoclinic of slope s/r. Let (N, V) be a subcrystal of $N_{s,r}$ of dimension d and height $h < r$. By 6.20 and 6.22 we get that (N, V) is isoclinic of the same slope as $N_{s,r}$, i.e. $d/h = s/r$. Since s and r are coprime, we obtain that r divides h. Thus $h = 0$ and $N = 0$.

6.28. Theorem: Let (N, V) be an isoclinic isocrystal of slope s/r where $r, s \in \mathbb{Z}$, $r > 0$ and $(s, r) = 1$. Then (N, V) is a direct sum of copies of $N_{s,r}$.

Proof: We choose a lattice M in N such that $V^r M = p^s M$. By 6.26, we can find a basis $m_1, \ldots, m_h$ of M such that $V^r m_i = p^s m_i$ for $i = 1, \ldots, h$. Let $N_i = \sum_{j=1}^{r-1} V^j m_j$. The surjection $N_{s,r} \to N_i$, $e_j \mapsto V^j m_j$ is a homomorphism of isocrystals. From 6.27 follows that this is an isomorphism. Therefore,

$$(N, V) = \sum_{j=1}^{h} (N_i, V), \quad (N_i, V) \simeq N_{s,r}.$$

Leaving aside some summands, one can work it so that

$$(N, V) = \sum_{j=1}^{t} (N'_i, V),$$

where $N'_i \not\subset \sum_{j \neq i} N'_j$ and $(N'_j, V) \simeq N_{s,r}$. From 6.27 we obtain $N'_i \cap \sum_{j \neq i} N'_j = 0$. Thus the sum is direct.

6.29. Theorem: Let (N, V) be an isocrystal over K. Then there exists a direct sum decomposition

$$(N, V) = \bigoplus_{i=1}^{u} N^{t_i}_{s_i, r_i},$$

where $u, s_i, r_i, t_i \in \mathbb{Z}$, $u, t_i, r_i > 0$, $(s_i, r_i) = 1$ and $s_1/r_1 < \cdots < s_u/r_u$. The numbers u, s_i, r_i, t_i are uniquely determined by (N, V).

Proof: This follows immediately from 6.22 and 6.28. The theorem says that over an algebraically closed field, an isocrystal is determined up to isomorphism by its Newton polygon.

Let us consider the case of σ^{-1}-crystals. Let G be a p-divisible formal group over K and
119 120 (N, V) its isocrystal. By the *Newton polygon of* G we mean that of (N, V). It determines G up to isogeny by 6.29.

By 6.23, we know that for $0 < s/r \leqslant 1$, $N_{s,r}$ is the isocrystal of a p-divisible formal group G. The structure equations of such a group take the form:

$$Fm_i = m_{i+1},\ i = 1, \ldots, s-1, \quad Fm_s = V^{r-s}m_1.$$

We denote these groups by $G_{s,r}$. One sees easily that there is an exact sequence of functors

$$0 \longrightarrow W \xrightarrow{F^s - V^{r-s}} W \longrightarrow G_{s,r} \longrightarrow 0.$$

We can formulate 6.29 for formal groups in the following way.

6.30. Theorem: Every p-divisible formal group over K is isogenous to a direct product of groups $G_{s,r}$.

Bibliography

[1] BERTHELOT, P., *Généralités sur les λ-anneaux*, exposé V du Séminaire de Géométrie Algébrique du Bois-Marie 1966–1967 (SGA 6), *Théorie des intersections et théorème de Riemann-Roch*, dirigé par P. Berthelot, A. Grothendieck et L. Illusie, Lecture Notes in Mathematics, No. 225, Springer-Verlag, 1971.

[2] BOURBAKI, N., *Algèbre commutative*, Hermann, 1961.

[3] CARTIER, P., *Relèvements des groupes formels commutatifs*, Séminaire Bourbaki No. 11 (1968-1969), Exposé No. 359.

[4] CARTIER, P., *Groupes formels associés aux anneaux de Witt généralisés*, C. R. Acad. Sci. Paris Sér. A-B 265, 1967, A49–A52.

[5] CARTIER, P., *Modules associés un groupe formel commutatif. Courbes typiques*, C. R. Acad. Sci. Paris Sér. A-B 265, 1967, A129–A132.

[6] DEMAZURE, M., *Lectures on p-divisible groups*, Lecture Notes in Mathematics, No. 302, Springer-Verlag, 1972.

[7] DRINFELD, W.G., *Coverings of p-adic symmetric domains*, Funkcional. Anal. i Priložen. 10 (1976), no. 2, 29–40.

[8] FONTAINE, J.-M., *Groupes p-divisibles sur les corps locaux*, Astérisque, No. 47-48. Société Mathématique de France, 1977.

[9] GROTHENDIECK, A., *Groupes de Barsotti-Tate et cristaux de Dieudonné*, Séminaire de Mathématiques Supérieures, No. 45, Presses de l'Université de Montréal, 1974.

[10] KATZ, N., *Slope filtration of F-crystals*, Journées de Géométrie Algébrique de Rennes, Vol. I, 113–163, Astérisque, No. 63, Soc. Math. France, 1979.

[11] KURKE, H., PFISTER, G., ROCZEN, M., *Henselsche Ringe und algebraische Geometrie*, Mathematische Monographien, Band II. VEB Deutscher Verlag der Wissenschaften, 1975.

[12] LAZARD, M., *Commutative formal groups*, Lecture Notes in Mathematics, No. 443, Springer-Verlag, 1975.

[13] LUBIN, J., TATE, J., *Formal complex multiplication in local fields*, Ann. of Math. (2) 81, 1965, 380–387.

[14] MANIN, YU., *Theory of commutative formal groups over fields of finite characteristic*, Uspehi Mat. Nauk 18, 1963, No. 6 (114), 3–90.

[15] MESSING, W., *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*, Lecture Notes in Mathematics, No. 264, Springer-Verlag, 1972.

[16] MUMFORD, D., *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Oxford University Press, 1970.

[17] MUMFORD, D., *Lectures on curves on an algebraic surface*, Annals of Mathematics Studies, No. 59, Princeton University Press, 1966.

[18] NORMAN, P., *An algorithm for computing local moduli of abelian varieties*, Ann. Math. (2) 101, 1975, 499–509.

[19] RAYNAUD, M., *"p-torsion" du schéma de Picard*, Journées de Géométrie Algébrique de Rennes, Vol. II, 87–148, Astérisque, No. 64, Soc. Math. France, 1979.

[20] SCHLESSINGER, M., *Functors of Artin rings*, Trans. Amer. Math. Soc. 130, 1968, 208–222.

121
122 [21] SERRE, J.-P., *Algèbre locale. Multiplicités*, Cours au Collège de France, 1957–1958, Lecture Notes in Mathematics, No. 11, Springer-Verlag, 1965.

[22] SERRE, J.-P., *Lie algebras and Lie groups*, Lectures given at Harvard University, 1964, W. A. Benjamin, 1965.

[23] ZINK, TH., *Isogenien formaler Gruppen über einem lokal noetherschen Schema*, Math. Nachr. 99, 1980, 273–283.

[24] HAZEWINKEL, M., *Formal groups and applications*, Pure and Applied Mathematics, 78, Academic Press, 1978.

[25] CASSELS, J.W.S., FRÖHLICH, A., *Algebraic Number Theory*, Proc. Instructional Conf., Brighton, London Math. Society, 1965.

[26] GODEMENT, R., *Topologie algébrique et théorie des faisceaux*, Hermann, 1958.

Index of symbols

123

Let C be an object in an additive category. Let I be an index set. We denote the direct sum of I copies of C by $C^{(I)}$ and the direct product by C^I. The invariants under the action of a group G are denoted C^G. If y is the image of x under a map, we write $x \mapsto y$. For a K-module P, we write P^* the dual module $P^* = \mathrm{Hom}_K(P, K)$.

Index of terms

124