UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Matematica "Tullio Levi-Civita"

Corso di Laurea in Matematica

Tesi di Laurea

Introduction to p-divisible groups

Relatore

Prof. Matteo Longo

Laureando

Ravi Ferigo

Matricola 2061889

20/09/2024

Contents

Introduction **3**

1 Preliminaries **5**
1.1 The categorical framework 5
1.1.1 Basic notions 5
1.1.2 Presheaves categories: the Yoneda Lemma 9
1.1.3 Examples 10
1.1.4 Limits and colimits 11
1.1.5 Abelian categories 16
1.1.6 Grothendieck topologies and sheaves 18
1.2 Algebras, bi-algebras and Höpf algebras 22
1.2.1 Basic notions: rings and modules 23
1.2.2 Algebras and co-algebras 25
1.2.3 Group objects, bi-algebras, Höpf algebras 27

2 Schemes, group schemes and formal schemes **33**
2.1 Schemes and formal schemes 33
2.1.1 Geometrical approach 33
2.1.2 The functorial point of view 40
2.1.3 Formal Schemes 44
2.2 Group schemes and formal group schemes 49
2.2.1 Affine group schemes 49
2.2.2 Examples 53
2.2.3 Connected and étales k-groups 53
2.2.4 formal k-groups and Cartiér dual 55
2.3 Witt vectors and Dieudonné modules 60
2.3.1 The ring of Witt vectors 60
2.3.2 Witt covectors 67
2.3.3 Dieudonné rings and modules 68

3 p-divisible Groups **71**
3.1 Definition of p-divisible groups 71
3.1.1 Notations 71
3.1.2 Serre and Tate 74

3.1.3 Grothendieck definition of *Barsotti-Tate* groups 78
3.2 Examples of p-divisible groups 81
3.2.1 p-adic numers 81
3.2.2 The *Prüfer* group and the *multiplicative* group 82
3.2.3 Abelian schemes 84
3.2.4 Constant and étale schemes 87
3.2.5 Cartier dual of p-divisible group 87
3.3 Formal groups and p-divisible groups 88
3.3.1 p-divisible groups and formal p-groups 88
3.3.2 Formal power series, formal Lie groups 90
3.3.3 Dieudonné modules and p-divisible groups 94
3.4 Tate and Serre main theorem on p-divisible groups 100
3.4.1 The main statement 100
3.4.2 Outline of the proof 101

4 Elliptic Curves **103**
4.1 Definition and main properties 103
4.1.1 Elliptic curves as plane curves 104
4.1.2 The ring of regular functions 105
4.2 Elliptic curves as abelian varieties 108
4.3 The formal group of an elliptic curve 118
4.4 Morphisms between curves 120
4.5 Isogenies 122
4.6 p-divisible group of an elliptic curve 124

Bibliography **129**

Aknowledgements **131**

Abstract

The main aim of this thesis is to introduce a very important algebraic and geometric object: the notion of ***p-divisible group***. p-divisible groups represent a profound intersection between the branch of ***algebraic geometry***, ***number theory*** and ***representation theory***, and provide a deep insight into the structure of algebraic varieties over fields of characteristic p. In order to give the definition of p-divisible groups and to analyze some of their main properties, we first organize a review of the main concepts of modern algebraic geometry, which stands at the base of objects such as p-divisible groups; and we consider other important concepts such as the notions of group schemes, formal group schemes and formal groups in general, using a categorical framework. We proceed by analyzing the notion of p-divisible group given by Serre and Tate and comparing it with the one given later by Grothendieck, who renamed this groups ***Barsotti-Tate groups***. Using important tools such as Witt vectors, Dieudonné modules and Cartiér duals, we show some properties of p-divisible groups and state some significant results. Finally, after introducing ***elliptic curves*** in the context of ableian varieties, we do the specific computations of the p-divisible group of those objects.

Introduction

The main aim of this thesis is the study of very important algebric and geometric objects: p-**divisible groups**.

After the refoundation of **algebraic geometry** operated by André Weil and based on the modern thecniques of commutative algebra, during the late '50 and the '60, Jean-Pierre Serre and Alexandre Grothendieck rebuilt and revolutioned the subjects of algebraic geometry introducing foundamental concepts and new important theories such as **sheaf theory** and **scheme theory** and this led to the study of abelian varieties and their properties. Also in the late '50 and '60 Cartier, Manin and Dieudonné developed their studies on formal groups. Dieudonné module theory, together with the generalization of the concept of p-**adic numers** thanks to Witt, provided important instruments in order to study general properties of formal groups and in particular of p-**divisible groups**. It was the italian mathematician Iacopo Barsotti that first introduced the concept of p-**divisible groups** calling them **"equidimentional hyperdomains"**, successively Serre and Tate got interested in the topic and formalized the foundation theory at the base of those concepts. Finally Grothendieck gave a great contribution on the matter that led to new interesting developements in the context of the **deformation theory**. In those processes also the developement of p-**adic analysis** and **étale cohomology** played a very important role.

The idea at the base of the notion of p-**divisible groups** meant by Barsotti was that of (in the language of modern scheme theory) "subgroup schemes of elements of order $\mathbf{p^n}$ of an **abelian variety**". Serre and Tate formalized this concept and developed the main theorems which provided a description of the properties of the homomorphisms between p-divisible groups, thanks to Dieudonné theory. Lately Grothendieck generalized this concept and used the terminology **Barsotti - Tate groups** meaning *"fppf sheaves of commutative groups over a scheme S that are: p-divisible, p-torsion, and the points G(1) of order p of G are a finite locally free scheme"*.

The journey of this work is motivated by the notion of **p-divisible groups** used by Serre and Tate: a **p-divisible groups** (Barsotti-Tate group using Grothendieck) of heigh h over a scheme S is an inductive system $G = (G_n, i_n), n \geq 0$ where G_n is a finite group scheme over S of order p^{hn} and for each n the sequence $0 \to G_n \to^{i^n} G_{n+1} \to^{p^n} G_{n+1}$ is exact, with the p^n-*arrow* being the multiplication by p^n.

Starting from this, and keeping in mind the emblematic example of $(\mathbb{Q}_p/\mathbb{Z}_p)^h$, we want to analize the main properties of those groups and in particular apply these studies to the **p-divisible groups** of abelian varieties and, more specifically, **elliptic plane curves**.

In order to do this, we organize in **Chapter 1** and **Chapter 2** a review of the main concepts of modern algebraic geometry that stands at the base of the notion of **p-divisible group**, such as the notions of **group schemes**, **formal group schemes** and **formal groups** in general. Along the entire work, the purpose is to use both a geometric approach (with examples clarifying concepts coming from algebraic varieties) together with an algebraic, much more formal, point of view, thanks to the useful tool of modern **Cathegory theory**, that allows us to show, for example, the equivalence between the category of *(commutative) affine k-groups* and *(commutative) formal k-groups* or, lately, thanks to Serre and Tate, the equivalence of categories between the category of *p-divisible, commutative formal Lie groups* (over a scheme S) and the category of *connected p-divisible groups* (over S).

After summarizing the technical instruments needed we proceed, in **Chapter 3** by stating and comparing the different definitions of **p-divisible groups**, using some notions such as: **Witt vectors, Dieudinné modules and Cartiér duals**, in order to describe properties of **p-divisible groups**. Finally we consider important objects such as:

- the Dieudonné module of the k-formal group scheme G_k, for k a field, which is a $W(k)$-module of rank the height of G_k (being $W(k) =$ the ring of Witt vectors over k);
- the Tate module of $G_K = \mathcal{G}(K/k)$, for $k = \text{Quot}(W(k))$ and K its algebraic closure, i.e. $T_p(G_K) := \varprojlim_{n\in\mathbb{N}} G_n(\bar{K})$, which is a free $\mathbb{Z}_p$-module of rank the heigh of G_K with a continuous G_K-action.

Thanks to this we state an important result, due to Serre and Tate, which describes the morphisms between p-divisible groups giving a bijection:

$$Hom(G, H) \to Hom(G_K, H_K) \to Hom_{Gal(\bar{K}/K)}(T_p(G_K), T_p(H_K))$$

which shows that the functor from the category of p-divisible groups over k, to that of p-divisible groups over K, is fully faithful.

Finally, in **Chapter 4**, after introducing **elliptic curves** and their main properties in the context of ableian varieties, we do the specific computations of the **p-divisible group** of those object, distinguishing the different cases (supersingular and ordinary) of curves in a field of characteristic $p > 0$ and we analyze the associated algebra of this group, applying what developed in the previous chapters.

Chapter 1

Preliminaries

In this section we recall some important notions and results coming from *category theory*, that we are going to use along the entire work as our algebraic framework. A very useful result is the *Yoneda lemma*, which will allow us to show the *equivalence* between different categories. We sum up some properties of limits and colimits and finally we give the definitions of *abelian category*, of *Grothendieck topology* and of *sheaves on sites*.

1.1 The categorical framework

1.1.1 Basic notions

We start summing up some basic definitions and properties of *categories* and *functors*.

Definition 1.1 A **category** $\mathcal{C}$ is defined by giving:

- a collection (or class) $\mathtt{Ob}(\mathcal{C})$ of **objects**, denoted with capital letters such as $A, B, C, ..., X, Y$;
- a collection (or class) $\mathtt{Mor}(\mathcal{C})$ of **morphisms** between objects, denoted with $f, g, ...$ or $\psi, \varphi, \chi, ...$;
- for each $A, B \in \mathtt{Ob}(\mathcal{C})$, a class $\mathrm{Hom}_{\mathcal{C}}(A, B) \subseteq \mathtt{Mor}(\mathcal{C})$;
- two functional relations (or simply a functions):

$$\partial_0 : \mathtt{Mor}(\mathcal{C}) \to \mathtt{Ob}(\mathcal{C}) \tag{1.1}$$

$$\partial_1 : \mathtt{Mor}(\mathcal{C}) \to \mathtt{Ob}(\mathcal{C}) \tag{1.2}$$

  respectively called the **domain** and the **target** of a morphism and s.t. for each $\varphi \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ then $\partial_0(\varphi) = A$ and $\partial_1(\varphi) = B$;
- a functional relation (or simply a function) $id_{(-)} : \mathtt{Ob}(\mathcal{C}) \to \mathtt{Mor}(\mathcal{C})$, called the **identity** morphism and s.t. $id_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$;
- a functional relation (or simply a function) $(-) \circ (-) : \mathtt{Mor}(\mathcal{C}) \times \mathtt{Mor}(\mathcal{C}) \to \mathtt{Mor}(\mathcal{C})$:

the **composition map**, s.t. for each $A, B, C \in \mathtt{Ob}(\mathcal{C})$ and $\varphi \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, $\psi \in \mathrm{Hom}_{\mathcal{C}}(B, C)$, then $\psi \circ \varphi \in \mathrm{Hom}_{\mathcal{C}}(A, C)$;

such that:

(i) $id_{\partial_1(f)} \circ f = f \circ id_{\partial_0(f)} = f$ for each $f \in \mathtt{Mor}(\mathcal{C})$;

(ii) $(-) \circ (-)$ is **associative**, i.e. $(f \circ g) \circ h = f \circ (g \circ h)$ for each $f, g, h \in \mathtt{Mor}(\mathcal{C})$ s.t. $\partial_1(g) = \partial_0(f)$ and $\partial_1(h) = \partial_0(g)$.

Remark 1.2 (Set-theoretic issues) In order to avoid *set-theoretic* problems one should specify a-priori the "universe" and the set-axiomatization used. In fact, from categories of "big" size could come some contradictions, for example, while indexing some direct products but also one can get other issues about the cardinality of the objects used. For this reason we assume everything behaving in a good way with the following:

Definition 1.3 A category $\mathcal{C}$ such that the class of its morphisms $\mathtt{Mor}(\mathcal{C})$ is a **set** (and hence $\mathtt{Ob}(\mathcal{C})$ is a set too), is called **small category**. $\mathcal{C}$ is said to be **locally small** if $\mathrm{Hom}_{\mathcal{C}}(A, B)$ is a set for each $A, B \in \mathcal{C}$. In this context the "functional relations" mentioned above are actually functions (between sets).

In order to avoid set-theoretic issues mentioned in [1.2], we will mostly use *(locally) small categories*, in particular in the context of algebraic geometry proofs.

Notations 1.4 Often we use a more simple notation to specify objects and morphism of a category $\mathcal{C}$: we write $A \in \mathcal{C}$ instead of $A \in \mathtt{Ob}(\mathcal{C})$ and $f : A \to B$ instead of $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$.We should also write $\mathrm{Hom}(-,-)$ instead of $\mathrm{Hom}_{\mathcal{C}}(-,-)$, whenever the base category is clear from the context. Finally when writing $f \circ g$ we always mean that $\partial_1(g) = \partial_0(f)$ so that the composition makes sense.

Definition 1.5 Let $\mathcal{C}$ be a category and $f \in \mathrm{Hom}(A, B)$ a morphism, then:

- $f : A \to B$ is a **monomorphism** if for each $X \in \mathcal{C}$ and $g_1, g_2 : X \to A$ such that $f \circ g_1 = f \circ g_2$, then $g_1 = g_2$;
- $f : A \to B$ is a **epimorphism** if for each $X \in \mathcal{C}$ and $g_1, g_2 : B \to X$ such that $g_1 \circ f = g_2 \circ f$, then $g_1 = g_2$;
- $f : A \to B$ is a **split mono** if there exist $g : B \to A$ s.t. $g \circ f = id_A$;
- $f : A \to B$ is a **split epi** if there exist $g : B \to A$ s.t. $f \circ g = id_B$;
- $f : A \to B$ is an **isomorphism** if there exist $g : B \to A$ s.t. $g \circ f = id_B$ and $f \circ g = id_A$ (if and only if it is both split mono and split epi), and we write $f : A \xrightarrow{\sim} B$ or $A \simeq B$.

Proposition 1.6 Let $\mathcal{C}$ be a category and let $f : A \to B$, $g : B \to C$ be morphisms, then:

(i) if f and g are *monomorphisms* (resp. *epimorphisms*/*isomorphisms*) then $g \circ f$ is a *monomorphism* (resp. *epimorphism*/*isomorphism*);

(ii) if $g \circ f$ is a *monomorphism* (resp. *epimorphism*) then f (resp. g) is a *monomorphism* (resp. *epimorphism*);

(iii) f is an *isomorphism* if and only if it is both *split mono* and *split epi*;

(iv) if f is an *isomorphism* then it is both a *monomorphism* and an *epimorphism*;

(v) an *isomorphism* $f : A \xrightarrow{\sim} B$, if it exists, it is unique and we write f^{-1} to denote its inverse;

(vi) the identity $id_{(-)}$ is an *isomprphism*.

Proof. Follows easily from the definitions above; for example let f and g be *monomorphisms*, then consider $h_1, h_2 : C \to D$ s.t. $g \circ f \circ h_1 = g \circ f \circ h_2$. Since g is *mono* $f \circ h_1 = f \circ h_2$ but then since f is *mono* too we get $h_1 = h_2$ as needed. Notice that, for example, $id_X : X \to X$ is such that $id_X^{-1} = id_X^{-1} \circ id_X = id_X$. □

Definition 1.7 A category $\mathcal{C}$ is said to be a **groupoid** if all of its morphisms are isomorphisms.

Definition 1.8 Let $\mathcal{C}$ be a category, for each $X, Y \in \mathcal{C}$, then:

- a category $\mathcal{C}'$ is said to be a **subcategory** of $\mathcal{C}$ if $\mathtt{Ob}(\mathcal{C}') \subseteq \mathtt{Ob}(\mathcal{C})$ and $\mathrm{Hom}_{\mathcal{C}'}(X, Y) \subseteq \mathrm{Hom}_{\mathcal{C}}(X, Y)$; moreover it is said to be a **full** subcategory if $\mathrm{Hom}_{\mathcal{C}'}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(X, Y)$;
- the **opposite category** $\mathcal{C}^{op}$ is the category such that $\mathtt{Ob}(\mathcal{C}^{op}) = \mathtt{Ob}(\mathcal{C})$ and $\mathrm{Hom}_{\mathcal{C}^{op}}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X)$

Definition 1.9 (Functors) A **covariant functor** $F : \mathcal{C} \to \mathcal{D}$ between two categories $\mathcal{C}$ and $\mathcal{D}$, consists of two maps:

$$F_0 : \mathtt{Ob}(\mathcal{C}) \to \mathtt{Ob}(\mathcal{D}) \tag{1.3}$$

$$F_1 : \mathtt{Mor}(\mathcal{C}) \to \mathtt{Mor}(\mathcal{D}) \tag{1.4}$$

such that, for each $X, Y \in \mathcal{C}$ and $f : X \to Y$, then $F_1(f) : F_0(X) \to F_0(Y)$; $F_1(id_X) = id_{F_0(X)}$; and finally $F_1(f \circ g) = F_1(f) \circ F_1(g)$. A **contravariant functor** $F : \mathcal{C} \to \mathcal{D}$ is a covariant functor $\mathcal{C}^{op} \to \mathcal{D}$.

Definition 1.10 One can define the category **Cat** whose objects are *small categories* and whose morphisms are *functors* between them.

Notation 1.11 Whenever it is clear from the context we write F instead of F_i for $i \in \{0, 1\}$. Moreover, when not specified, a functor is always meant to be *covariant*.

Definition 1.12 Let $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{E}$ be functors, then we define the functor $G \circ F : \mathcal{C} \to \mathcal{E}$ to be such that: $(G \circ F)(A) = G(F(A))$ and $(G \circ F)(f) = G(F(f))$ for each $A \in \mathcal{C}$, $f \in \texttt{Mor}(\mathcal{C})$.

Definition 1.13 (Natural transformations) Let $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{C} \to \mathcal{D}$ be functors. A **natural transformation** $\eta : F \to G$ between F and G, is a family of morphisms $\eta_X : F(X) \to G(X)$, for each $X \in \mathcal{C}$, such that for each $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ the following diagram commutes:

$$\begin{array}{ccc} F(X) & \xrightarrow{\eta_X} & G(X) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(Y) & \xrightarrow[\eta_Y]{} & G(Y) \end{array} \tag{1.5}$$

Remark 1.14 A *natural transformation* η between two functors as above is an *isomorphism* if and only if η_X is an isomorphism for each X.

Notations 1.15

- Sometimes natural transformations are also called *morphisms between functors*.
- Let $\mathcal{C}, \mathcal{C}'$ be *(locally) small* categories, we denote $\mathrm{Fnct}(\mathcal{C}, \mathcal{C}')$ the category whose objects are functors and whose morphisms are natural transformations between them.

Definition 1.16 Let $F : \mathcal{C} \to \mathcal{D}$ be a functor and $X, Y \in \mathcal{C}$. Then F is said to be:

- **full** if $\mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{D}}(F(X), F(Y))$ is injective;
- **faithful** if $\mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{D}}(F(X), F(Y))$ is surjective;
- **essentially surjective** if for every $D \in \mathcal{D}$ there exists $C \in \mathcal{C}$ s.t. $F(C) \simeq D$.

Before stating the *Yoneda Lemma*, let us show how it is possible to express different concepts of "congruence" between two categories $\mathcal{C}$ and $\mathcal{D}$, the first of all achieved when the two categories coincide: $\mathcal{C} = \mathcal{D}$.

Definition 1.17 Given two categories $\mathcal{C}$ and $\mathcal{D}$, then we say that they are **isomorphic**, if there exist two functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ such that:

$$F \circ G = \mathbb{I}_{\mathcal{D}} \quad \text{and} \quad G \circ F = \mathbb{I}_{\mathcal{C}} \tag{1.6}$$

as functors. Where $\mathbb{I}_{(-)}$ is the identity functor.

Definition 1.18 Two categories $\mathcal{C}$ and $\mathcal{D}$ are said to be **equivalent** if there exist two functors $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$, and two natural transformations η, ε such that:

$$\eta(F \circ G) = \mathbb{I}_{\mathcal{D}} \quad \text{and} \quad \varepsilon(G \circ F) = \mathbb{I}_{\mathcal{C}} \tag{1.7}$$

i.e. the composition of the functors *isomorphic* to the identity morphism in a natural way.

It is much more common (and easy) to find an equivalence between two categories (i.e. to say that two categories are isomorphic after changing the internal notion of object and morphisms in a natural way) rather than to get an isomorphism of categories.

We state without proving the following:

Theorem 1.19 A functor $F : \mathcal{C} \to \mathcal{D}$ gives an equivalence between two categories if and only if it is fully faithful and essentially surjective.

This is a very useful result, since without an explicit construction of the inverse G and of the natural transformations of Definition [1.18] above, we are able to prove an equivalence between two categories; however notice that there could be many choices for F and that the theorem itself is based on a sufficiently strong version of the axiom of choice.

Definition 1.20 The pair of functors (F, G), with $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$, is said to be an **adjoint pair**, or equivalently we say that F is left adjoint to G or that G is right adjoint to F and we write $F \dashv G$, if for each $X \in \mathcal{C}$ and $Y \in \mathcal{D}$ we have:

$$\mathrm{Hom}_{\mathcal{D}}(F(X), Y) \simeq \mathrm{Hom}_{\mathcal{C}}(X, G(Y)) \tag{1.8}$$

We can restate the theorem:

Theorem 1.21 A functor $F : \mathcal{C} \to \mathcal{D}$ gives an equivalence between two categories if and only if it is fully faithful and F has a right adjoint G.

Remark 1.22 Notice indeed that from Equation (1.8) we have that:

$$\mathrm{Hom}_{\mathcal{D}}(F(G(Y)), Y) \simeq \mathrm{Hom}_{\mathcal{C}}(G(Y), G(Y)) \tag{1.9}$$

$$\mathrm{Hom}_{\mathcal{D}}(F(X), F(X))) \simeq \mathrm{Hom}_{\mathcal{C}}(X, G(F(X)) \tag{1.10}$$

1.1.2 Presheaves categories: the Yoneda Lemma

Definition 1.23 Given a *(locally) small* category $\mathcal{C}$, one can define the **category of presheaves** $\mathrm{Psh}(\mathcal{C})$, also denoted $\mathcal{C}^\wedge$, as:

- $\mathtt{Ob}(\mathcal{C}^\wedge) = \mathbf{Set}^{\mathcal{C}^{op}} := \mathrm{Fnct}(\mathcal{C}^{op}, \mathbf{Set})$
- $\mathtt{Mor}(\mathcal{C}^\wedge) = \mathrm{Hom}_{fnct}(F, G)$

Hence a *presheaf* in $\mathrm{Psh}(\mathcal{C})$, is a *functor* from the opposite category $\mathcal{C}^{op}$ tho the category **Set** of sets and a morphism between two such functors is nothing but a *natural transformation* between them.

Definition 1.24 Let $\mathcal{C}$ be a small category. Consider the functor:

$$h_{(-)} : \mathcal{C} \to \mathcal{C}^\wedge \tag{1.11}$$

$$A \mapsto h_A := \mathrm{Hom}_{\mathcal{C}}(-, A) \tag{1.12}$$

such that, for each $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, then $h_f = f \circ \psi \in h_B$, for each $\psi \in h_A$. The functor $h_{(-)}$ is called **Yoneda embedding**.

Definition 1.25 A functor $F \in \mathcal{C}^\wedge$ of the form $F \simeq h_A$ for $A \in \mathcal{C}$, is called **representable functor**.

Lemma 1.26 (Yoneda) Let $X \in \mathcal{C}^\wedge$ and $A \in \mathcal{C}$. Then there is a *bijection* $\mathrm{Hom}_{\mathcal{C}^\wedge}(h_A, X) \simeq X(A)$, which is functorial in X and A.

Proof. Let $\varphi \in \mathrm{Hom}_{\mathcal{C}^\wedge}(h_A, X)$ and consider $\varphi_A \in \mathrm{Hom}_{set}(h_A(A), X(A))$, where $h_A(A) := \mathrm{Hom}_{set}(A, A)$. Now take $\varphi_A(id_A) \in X(A)$. This gives a map:

$$\mathrm{Hom}_{\mathcal{C}^\wedge}(h_A, X) \ni \varphi \mapsto \varphi_A \mapsto \varphi_A(id_A) \in X(A) \tag{1.13}$$

Conversely, starting from $\mathbf{x} \in X(A)$, for each $B \in \mathcal{C}$ we build a $\psi \in \mathrm{Hom}_{\mathcal{C}^\wedge}(h_A, X)$ such that $\psi_B : \mathrm{Hom}_{\mathcal{C}}(B, A) = h_A(B) \to X(B)$ is given by:

$$\mathrm{Hom}_{\mathcal{C}}(B, A) = h_A(B) \to \mathrm{Hom}_{set}(X(A), X(B)) \to X(B) \tag{1.14}$$

$$f \mapsto X(f) \mapsto X(f)(\mathbf{x}) \tag{1.15}$$

The two maps are clearly one inverse to the other. Morover notice that the bijection is functorial in $A \mapsto h_A$ and X. □

Corollary 1.28 We can define a functor $h^A(-) := \mathrm{Hom}_{\mathcal{C}}(A, -)$ as we did for h_A and repeat the proof of the lemma for this functor as well.

Corollary 1.29 The functor h_A (equiv. h^A) is fully faithfull.

Proof. For $A, B \in \mathcal{C}$ we have $\mathrm{Hom}_{\mathcal{C}^\wedge}(h_A, h_B) \simeq h_B(A) = \mathrm{Hom}_{\mathcal{C}}(A, B)$. □

1.1.3 Examples

Here are some classical examples of common categories:

Example 1.30

- The category **Set**, whose objects are sets and morphisms functions between sets.
- The category **Gps**, whose objects are groups and morphisms are homomorphisms of groups.

- The category **AbGps**, which is the full subcategory of **Gps**, whose objects are abelian groups.
- The category **Rng**, whose objects are rings and morphisms are homomorphisms of rings.
- The category $\mathbf{Mod_k}$, whose objects are k-modules, for a commutative unital ring k, and morphisms are k-linear maps. ([1.59])
- The category $\mathbf{Alg_k}$, whose objects are k-algebras, for a commutative unital ring k (i.e. k-modules with a ring structure; in particular we mean *associative* algebras); and whose morphisms are k-linear homomorphisms. ([1.64])
- The category **Top**, whose objects are topological spaces and morphisms are continuous maps.
- The category $*$ consisting of only one object $*$ and only one morphism.

1.1.4 Limits and colimits

In this section we give some basic notions about limits and colimits using the framework of the categorical language, and we state, without proving them, some useful results. We start with a proposition that shows a construction of projective limits in the category of sets.

Proposition 1.31 Let I be a small category and $\beta : I^{op} \to \mathbf{Set}$ a functor. We define the projective limit (of β) in **Set**, indexed by I, to be:

$$\varprojlim \beta := \{\{x_i\}_i \in \prod_i \beta(i) | \beta(f)(x_j) = x_i \text{ for all } f \in \mathrm{Hom}_{set}(i,j)\} \tag{1.16}$$

As a consequence we have that:

$$\varprojlim_i \mathrm{Hom}_{set}(A, \beta(i)) \simeq \mathrm{Hom}_{set}(A, \varprojlim \beta) \tag{1.17}$$

for each $A \in \mathbf{Set}$.

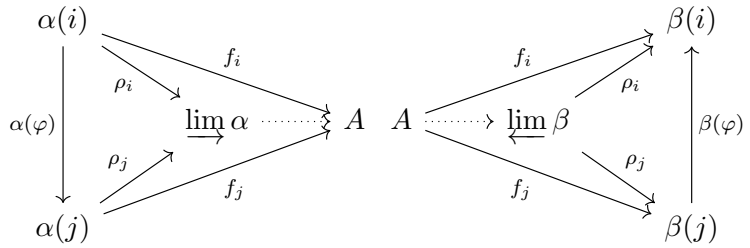
Definition 1.32 Let I be a small category and $\mathcal{C}$ a category. Consider the functors $\beta : I^{op} \to \mathcal{C}$ and $\alpha : I \to \mathcal{C}$. We say that:

- the category $\mathcal{C}$ admits **projective limits** indexed by I if there exist a representative $\varprojlim \beta$ for the functor $A \mapsto \varprojlim \mathrm{Hom}_{\mathcal{C}}(A, \beta(i))$, i.e. $\varprojlim_i \mathrm{Hom}_{\mathcal{C}}(A, \beta(i)) \simeq \mathrm{Hom}_{\mathcal{C}}(A, \varprojlim \beta)$;
- the category $\mathcal{C}$ admits **inductive limits** indexed by I if there exist a representative $\varinjlim \alpha$ for the functor $A \mapsto \varprojlim \mathrm{Hom}_{\mathcal{C}}(\alpha(i), A)$, i.e. $\varinjlim_i \mathrm{Hom}_{\mathcal{C}}(\alpha(i), A) \simeq \mathrm{Hom}_{\mathcal{C}}(\varinjlim \alpha, A)$.

Definition 1.33 (Universal property) Consider the assumptions of the above Definition [1.32], we say equivalently that $\mathcal{C}$ has:

- projective limits indexed by I if there exist an object $\varprojlim \beta$ and a family of morphisms $\rho_i : \varprojlim \beta \to \beta(i)$, s.t. for each $A \in \mathcal{C}$ and family $(f_i)_{i\in I}$ of morphisms that satisfy $f_i = \beta(\varphi) \circ f_j$ for each $\varphi \in \mathrm{Hom}_I(i,j)$, then the f_i's factorize through $\varprojlim \beta$;
- inductive limits indexed by I if there exist an object $\varinjlim \alpha$ and a family of morphisms $\rho_i : \alpha(i) \to \varinjlim \alpha$, s.t. for each $A \in \mathcal{C}$ and family $(f_i)_{i\in I}$ of morphisms that satisfy $f_i = f_j \circ \alpha(\varphi)$ for each $\varphi \in \mathrm{Hom}_I(i,j)$, then the f_i's factorize through $\varinjlim \alpha$;

The universal property defined above can be visualized in the following two diagrams:



(1.18)

where the dotted arrows are the (unique) morphisms given by the property.

Definition 1.34 On the category **Set** of sets we define the **product** of a family of objects $\{X_i\}_i$ indexed by a small set I as:

$$\prod_i X_i := \{(x_i)_i \mid x_i \in X_i \text{ for each } i \in I\} \tag{1.19}$$

and for $f, g : X \rightrightarrows Y$ we denote with:

$$\ker(f,g) := \{x \in X \mid f(x) = g(x)\} \tag{1.20}$$

the **equalizer** or **kernel** of the two maps f and g.

Definition 1.35 Let $\mathcal{C}$ be a (locally) small category and I be a (small) set. Let $\{X_i\}_i$ be a family of objects in $\mathcal{C}$. Then:

(i) the **product** of the X_i's denoted by $\prod_i X_i$ is a representative for the functor:

$$\mathcal{C}^{op} \to \mathbf{Set} \tag{1.21}$$

$$A \mapsto \prod_i \mathrm{Hom}_{\mathcal{C}}(A, X_i) \tag{1.22}$$

i.e. a representable functor:

$$\mathrm{Hom}_{\mathcal{C}}(A, \prod_i X_i) \simeq \prod_i \mathrm{Hom}_{\mathcal{C}}(A, X_i) \tag{1.23}$$

(ii) the **coproduct** of the X_i's denoted by $\coprod_i X_i$ is a representative for the functor:

$$\mathcal{C} \to \mathbf{Set} \tag{1.24}$$

$$A \mapsto \prod_i \mathrm{Hom}_{\mathcal{C}}(X_i, A) \tag{1.25}$$

i.e. a representable functor:

$$\mathrm{Hom}_{\mathcal{C}}(\coprod_i X_i, A) \simeq \prod_i \mathrm{Hom}_{\mathcal{C}}(A, X_i) \tag{1.26}$$

(iii) if $X_i = X$ for all i then we write:

$$\prod_i X_i = X^I \quad \coprod_i X_i = X^{(I)} \tag{1.27}$$

if, moreover $I = \{1, 2\}$ then the product is denoted by $X_1 \times X_2$ and the coproduct is denoted by $X_1 \sqcup X_2$.

(iv) Given two parallel morphisms $f, g : A \rightrightarrows B$, the **kernel** of f and g, denoted $\ker(f, g)$, is a representative for the functor:

$$\mathcal{C}^{op} \to \mathbf{Set} \tag{1.28}$$

$$Y \mapsto \ker(\mathrm{Hom}_{\mathcal{C}}(Y, A) \rightrightarrows \mathrm{Hom}_{\mathcal{C}}(Y, B)) \tag{1.29}$$

i.e. a representable functor:

$$\mathrm{Hom}_{\mathcal{C}}(Y, \ker(f, g)) \simeq \ker(\mathrm{Hom}_{\mathcal{C}}(Y, A) \rightrightarrows \mathrm{Hom}_{\mathcal{C}}(Y, B)) \tag{1.30}$$

(v) Given two parallel morphisms $f, g : A \rightrightarrows B$, the **cokernel** of f and g, denoted $\mathrm{coker}(f, g)$, is a representative for the functor:

$$\mathcal{C} \to \mathbf{Set} \tag{1.31}$$

$$Y \mapsto \ker(\mathrm{Hom}_{\mathcal{C}}(B, Y) \rightrightarrows \mathrm{Hom}_{\mathcal{C}}(A, Y)) \tag{1.32}$$

i.e. a representable functor:

$$\mathrm{Hom}_{\mathcal{C}}(\mathrm{coker}(f, g), Y) \simeq \ker(\mathrm{Hom}_{\mathcal{C}}(B, Y) \rightrightarrows \mathrm{Hom}_{\mathcal{C}}(A, Y)) \tag{1.33}$$

(vi) An **initial object** $\perp \in \mathcal{C}$, is an object (if it exists it is unique) such that for each $A \in \mathcal{C}$ there exists a unique morphism $\perp \to A$. A **terminal object** is an object $\top \in \mathcal{C}$ (if it exists it is unique) such that for each object $A \in \mathcal{C}$ there exists a unique morphism $A \to \top$. A 0 object in $\mathcal{C}$, is an object that is both initial and terminal.

(vii) A **cartesian category** $\mathcal{C}$ is a category that admits binary products $A \times B$ for each pair of objects $A, B \in \mathcal{C}$, and that has a terminal object.

(vii) The **kernel of a morphism** denoted with $\ker(f)$ is the kernel of the morphisms $(f, 0)$ for a 0 object in $\mathcal{C}$.

Definition 1.36 Let $\mathcal{C}$ be a category as in the above definition, then the kernel and the cokernel in $\mathcal{C}$ can be defined also through a universal property. Namely, let $f, g : A \rightrightarrows B$, be parallel morphisms, then:

- the **kernel** (or equalizer) of the two maps is given by an object $\ker(f, g) \in \mathcal{C}$ and a map $h : \ker(f, g) \to A$, such that for each map $u : C \to A$ that equalize f, g i.e. $f \circ u = g \circ u$, then there exists a unique $j : C \to \ker(f, g)$ such that $u = h \circ j$, which implies that the kernel is a **monomorphism**;
- the **cokernel** (or coequalizer) of the two maps above, is given by an object $\operatorname{coker}(f, g)$ in $\mathcal{C}$ and a map $k : B \to \operatorname{coker}(f, g)$ such that for each map $u : B \to C$ that coequalize f, g i.e. $u \circ f = u \circ g$, then there exists a unique $j : \operatorname{coker}(f, g) \to C$ such that $u = j \circ k$, which implies that the kernel is an **epimorphism**;

The universal property [1.36] (which is equivalent to definition [1.35]) can be visualized with the following commutative diagrams:

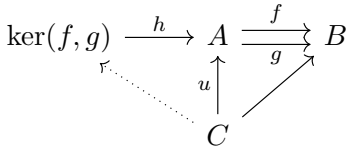


Figure 1.1: kernel-universal property

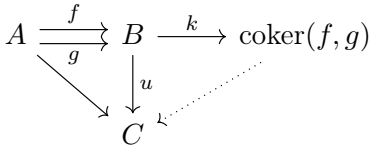


Figure 1.2: cokernel-universal property

Proposition 1.37 Products, copruducts, kernels, cokernels and 0-objects, as previously defined, can be expressed in terms of finite projective or inductive limits. Conversely projective and inductive limits can be defined using those objects.

Proof. We prove $\Rightarrow$. Consider the category $\mathcal{I} := \{\bullet, \square\}$ with two objects and two parallel morphisms $\bullet \rightrightarrows \square$, other than the identities. Then the functor $\mathcal{I} \to \mathcal{C}$ is defined by two parallel arrows $f, g : A \rightrightarrows B$ of $\mathcal{C}$. Inductive (resp. projective) limits indexed by $\mathcal{I}$ are nothing but the kernel (resp. cokernel) of f and g. If $\mathcal{I} = \emptyset$ is the empty category, then the colimit (resp. limit) defined by the functor $\alpha : \mathcal{I} \to \mathcal{C}$ exists if and only if $\mathcal{C}$ admits an initial object $\perp$ (resp. terminal object $\top$) and $\varinjlim \alpha = \perp$ (resp. $\varprojlim \alpha = \top$). With an analogous argoument, if $\mathcal{I}$ is a discrete set, then direct (resp. inverse) limits indexed by $\mathcal{I}$

on $\mathcal{C}$ are nothing but finite coproducts (resp. products). The implication $\Leftarrow$ is similar, see for example ([Sc], II, 2.3.7). $\square$

We state, without proving them, some properties of limits and colimits, for a detailed proof see, for example, ([Sc], II, 2.4).

Definition 1.38 A (small) category I is called **filtrant** if it is not the empty category and if it is such that: for any $i, j \in I$ there exists k and morphisms $i \to k$, $j \to k$, and moreover, for each pair of parallel morphisms $f, g : i \rightrightarrows j$ there exists a morphism $h : j \to k$ such that $h \circ f = h \circ g$. If I is filtrant then I^{op} is said to be **cofiltrant**. A **cofinal** functor $\Phi : I \to J$, with I filtrant, is a fully faithful functor such that for each $i \in I$ there exist $j \in J$ and a morphism $i \to \Phi(j)$.

Proposition 1.39 Let $I \to \mathbf{Set}$ be a functor. If I is a filtrant category then the relation given by:

$$(\bigsqcup_{i \in I} \alpha(i))/\sim \tag{1.34}$$

where $\alpha(i) \ni x \sim y \in \alpha(j)$ if and only if there exist $k \in I$ and maps $\varphi : i \to k$, $\psi : j \to k$ such that $\alpha(\varphi)(x) = \alpha(\psi)(y)$, is an equivalence relation.

Proof. Reflexivity and symmetry are evident, transitivity comes from the definition of filtrant category. See ([Sc], II, 2.5.3) for details. $\square$

Proposition 1.40 Let $\mathcal{C}$ be a category that admits limits and colimits indexed by a (small) category I. Then

(i) for any category $\mathcal{D}$, the presheaves category $\mathrm{Fnct}(\mathcal{D}, \mathcal{C})$ admits projective (resp. inductive) limits, namely if $\beta : I^{op} \to \mathrm{Fnct}(\mathcal{D}, \mathcal{C})$ (resp. $\alpha : I \to \mathrm{Fnct}(\mathcal{D}, \mathcal{C})$) is a functor, its projective (resp. inductive) limit is given by

$$(\varprojlim \beta)(A) = \varprojlim \beta(A) \text{ resp. } (\varinjlim \alpha)(A) = \varinjlim \alpha(A) \tag{1.35}$$

for $A \in \mathcal{D}$, where $\beta(A) : I^{op} \to \mathcal{C}$ (resp. $\alpha(A) : I \to \mathcal{C}$) is a well defined functor giving the projective (resp. inductive) limits on $\mathcal{C}$;

(ii) let J be another small category, then considering the functors $\beta : I^{op} \to \mathrm{Fnct}(J, \mathcal{C})$ and $\alpha : I \to \mathrm{Fnct}(J, \mathcal{C})$, we have that:

$$\varprojlim_I (\varprojlim_J \beta) \simeq \varprojlim_J (\varprojlim_I \beta) \tag{1.36}$$

$$\varinjlim_I (\varinjlim_J \alpha) \simeq \varinjlim_J (\varinjlim_I \alpha) \tag{1.37}$$

(iii) let $F : \mathcal{C} \to \mathcal{D}$ be a functor and $G : \mathcal{D} \to \mathcal{C}$ be its **left** (resp **right**) adjoint ([1.20]), assume moreover that also $\mathcal{D}$ admits projective (resp. inductive) limits indexed by

I and denoted with the functor β (resp. α) as above, then:

$$F(\varprojlim_I \beta) \simeq \varprojlim_I F(\beta) \tag{1.38}$$

$$F(\varprojlim_I \alpha) \simeq \varprojlim_I F(\alpha) \tag{1.39}$$

i.e. F commutes with projective (resp. inductive) limits.

(iv) Let J be a finite category and I be a filtrant one, and consider $J^{op} \to \mathrm{Fnct}(I, \mathcal{C})$. Then:

$$\varprojlim_j (\varinjlim_i \alpha_j(i)) \simeq \varinjlim_i (\varprojlim_j \alpha_j)(i) \tag{1.40}$$

where $j \mapsto \alpha_j$ (as a functor) and $\alpha_j : I \to \mathcal{C}$. This means that the functor:

$$\varinjlim : \mathrm{Fnct}(I, \mathcal{C}) \to \mathcal{C} \tag{1.41}$$

commutes with finite projective limits.

(v) If $\Phi : I \to J$ is a fully faithful functor, I is filtrant and Φ is cofinal, then:

$$\varprojlim \beta \simeq \varprojlim (\beta \circ \Phi) \tag{1.42}$$

$$\varinjlim \alpha \simeq \varinjlim (\alpha \circ \Phi) \tag{1.43}$$

for α and β defined as before.

1.1.5 Abelian categories

We give some useful definitions and properties of additive and abelian categories that we will use proving some results about (affine) schemes. For detailed proofs and observations see for example ([Sc], III and IV).

Definition 1.41 An **additive** category $\mathcal{C}$ is a category that satisfies:

- there exist a zero object, 0, in $\mathcal{C}$;
- $\mathcal{C}$ admits finite products and coproducts;
- for any $A, B \in \mathcal{C}$ then $\mathrm{Hom}_{\mathcal{C}}(A, B)$ is an abelian group, with the multiplication defined as the composition law $(-) \circ (-)$ and with the the zero morphism as neutral element; moreover $(-) \circ (-)$ is bilinear.

Remark 1.42 The first and the second conditions of previous Definition [1.41] are equivalent to ask that $\mathcal{C}$ is a cartesian category and this means that for any $A_1, A_2 \in \mathcal{C}$ there

exists an object C and morphisms $\mathrm{i}_j : A_j \to C$ and $\mathrm{pr}_j : C \to A_i$, for $j \in \{1, 2\}$, such that:

$$\begin{cases} \mathrm{pr}_i \circ \mathrm{i}_j = id_{A_j}, \text{ if } i = j \\ \mathrm{pr}_i \circ \mathrm{i}_j = 0, \text{ if } i \neq j \\ \mathrm{i}_1 \circ \mathrm{pr}_1 + \mathrm{i}_2 \circ \mathrm{pr}_2 \simeq id_C \end{cases} \tag{1.44}$$

so that $C \simeq X \times Y$ (the product) and also $Z \simeq X \sqcup Y$ (the coproduct also denoted by $X \oplus Y$).

Definition 1.43 A category $\mathcal{C}$ is called **abelian** if:

(i) it is an additive category that admits finite kernels and cokernels;

(ii) each morphism $f : A \to B$ admits kernel and cokernel and moreover the natural (canonical) morphism:

$$\widehat{f} : \mathrm{coim}(f) \to \mathrm{im}(f) \tag{1.45}$$

given by the (commutative) diagram:

$$\begin{array}{ccccccc} \ker(f) & \xrightarrow{h} & A & \xrightarrow{f} & B & \xrightarrow{k} & \mathrm{coker}(f) \\ & & \downarrow & \overset{f'}{\nearrow} & \uparrow & & \\ & & \mathrm{coim}(f) := \mathrm{coker}(h) & \xrightarrow{\widehat{f}} & \mathrm{im}(f) & & \end{array} \tag{1.46}$$

is an **isomorphism** (where the dotted arrows exist and are uniqe thanks to the universal properties of kernel and cokernel).

Proposition 1.44 Let $\mathcal{C}$ be an abelian category, then:

(i) the category $\mathrm{Fnct}(\mathcal{D}, \mathcal{C})$ is abelian as well;

(ii) $\mathcal{C}$ admits **finite** inductive and projective limits;

(iii) a morphism $f : A \to B$ is a monomorphism (resp. epimorphism) if and only if $\ker(f) \simeq 0$ (resp. $\mathrm{coker}(f) \simeq 0$) and f is an isomorphism if and only if it is both a monomorphism and an epimorphism.

Definition 1.45 A sequence of morphisms in an abelian category $\mathcal{C}$ of the form:

$$A \xrightarrow{f} B \xrightarrow{g} C \tag{1.47}$$

is said to be an **exact sequence** if $\mathrm{im}(f) \simeq \ker(g)$. A **short exact sequence** is an exact sequence of the form:

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0 \tag{1.48}$$

Proposition 1.46 Let $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be a short exact sequence in the abelian category $\mathcal{C}$ as before, then the following are equivalent:

(i) g admits a right inverse, i.e. there exist h such that $g \circ h = id_C$;

(ii) f admits a left inverse, i.e. there exist k such that $k \circ f = id_A$;

(iii) there exist two isomorphisms, one inverse to the other, $\varphi : B \xrightarrow{\sim} A \oplus C$ and $\varphi^{-1} : A \oplus C \xrightarrow{\sim} B$;

in this case the sequence is said to be **split exact**.

Definition 1.47 Let $F : \mathcal{C} \to \mathcal{C}'$ be a functor between abelian categories. Then F is said to be:

(i) **left exact** if it commutes with finite projective limits;

(ii) **right exact** if it commutes with finite inductive limits;

(iii) **exact** if it is both left and right exact.

Proposition 1.48 Let $F : \mathcal{C} \to \mathcal{C}'$ be a functor between abelian categories. Then:

(i) F is left (resp. right) exact if and only if it commutes with kernels (resp. cokernels) if and only if for any exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$, the sequence $0 \to F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C)$ is exact in $\mathcal{C}'$.

(ii) F is exact if and only if for any exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$, the sequence $0 \to F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \to 0$ is exact in $\mathcal{C}'$.

(iii) If F admits a left (resp. right) adjoint then it is left (resp. right) exact.

(iv) (Mittag-Leffler condition) Let k be a (commutative unital) ring and

$$0 \to A_n \xrightarrow{f_n} B_n \xrightarrow{g_n} C_n \to 0 \tag{1.49}$$

an exact sequence of projective systems of k-modules indexed by $\mathbb{N}$, then, if for each n, the map $A_{n+1} \to A_n$ is surjective, the sequence

$$0 \to \varprojlim A_n \xrightarrow{f} \varprojlim B_n \xrightarrow{g} \varprojlim C_n \to 0 \tag{1.50}$$

is exact too.

Notice that the categories **AbGps** of abelian groups and $\mathbf{Alg_k}$ of k-algebras (for k commutative unital ring) are examples of abelian categories.

1.1.6 Grothendieck topologies and sheaves

We briefly recall what does it mean to endow a category with a Grothendieck topology in order to introduce the notion of sheaf.

Definition 1.49 Given a category $\mathcal{C}$, a **Grothendieck topology** on $\mathcal{C}$ is, for each object $U \in \mathcal{C}$, the assignement of a collection of arrows $\{\mathbf{U_i} \longrightarrow \mathbf{U}\}$, called **coverings** of U, such that:

- if $\{U_i \longrightarrow U\}$ is a covering and $V \longrightarrow U$ any arrow, there exist the fiber product $\{V \times_U U_i\}$ and $\{V \times_U U_i \longrightarrow V\}$ is a covering.
- given $\{U_i \longrightarrow U\}$, if for each i there is a covering $\{V_{ij} \longrightarrow U_i\}$, then $\{V_{ij} \longrightarrow U_i \longrightarrow U\}$ is a covering.
- given an isomorphism $V \longrightarrow U$ then $\{V \longrightarrow U\}$ is a covering.

A category $\mathcal{C}$ endowed with a Grothendieck topology is called **site**

Example 1.50 In the category Op^{op}, of open subsets of a topological space X, with arrows given by the inclusions, we can build a Grothendieck topology considering, for each open $U \in \mathrm{Op}^{op}$, the set of open coverings $\{(U_i)_i \text{ s.t. } \bigcup_i U_i = U\}$, of U, and the fiber product $U_1 \times_U U_2 := U_1 \cap U_2$.

Remark 1.51 The **pull-back** of the morphism $f : X \to Y$ along the morphism $g : Z \to Y$, for X, Y, Z objects in a category $\mathcal{C}$, which admits finite direct products, is given by the map pr_2 (the projection) that makes commutative the diagram:

$$\begin{array}{ccc} X \times_Y Z & \xrightarrow{\mathrm{pr}_1} & X \\ {\scriptstyle \mathrm{pr}_2}\downarrow & & \downarrow{\scriptstyle f} \\ Z & \xrightarrow{g} & Y \end{array} \tag{1.51}$$

where $X \times_Y Z := \{(x, z) \in X \times Z | f(x) = g(z)\}$ is called **fiber product** (of X and Z with base Y). If $F : \mathcal{C} \to \mathcal{D}$ is a functor we also define the **pull-back** of a morphism $f : X \to Y$ to be the morphism $F(f) := f^* : F(X) \to F(Y)$ making commutative the diagram:

$$\begin{array}{ccc} F(X) & \xleftarrow{F} & X \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle f} \\ F(Y) & \xleftarrow{F} & Y \end{array} \tag{1.52}$$

We can consider the Zariski-Grothendieck topology, which will be useful in our discussion of p-divisible groups along Chapter 3.

Definition 1.52

Let k be a commutative unital ring. The (global) **Grothendieck – Zariski** topology on the category (**Aff**)**Sch**$/k$, of (affine) schemes over a fixed scheme $\mathrm{Spec}(k)$, is given considering the coverings $\{U_i \longrightarrow U\}$, which are the assignement of open embeddings, i.e. morphisms that are isomorphisms (of schemes) between the U_i's and an affine open sub-k-scheme of U. (We will define later these objects, for details see [2.13],[2.16] and [2.23]).

Definition 1.53 Given a site $\mathcal{C}$, a functor $F : \mathcal{C}^{op} \longrightarrow$ **Set** (i.e. a presheaf), is said to be:

- **separated** if, given a covering $\{U_i \longrightarrow U\}$ and a couple of sections s and t in $F(U)$, such that their pullback, given by $F(U) \longrightarrow F(U_i)$, coincides for every i (in $F(U_i)$), then this implies that $s = t$.
- a **sheaf** if, given a covering $\{U_i \longrightarrow U\}$, and sections $s_i \in F(U_i)$, and assuming moreover that, for every i and j we have that $\mathrm{pr}_1^*(s_i) = \mathrm{pr}_2 * (s_j) \in F(U_i \times_U U_j)$ (i.e. the pull-back given by the projections $p_1 : U_i \times_U U_j \longrightarrow U_i$ and $p_2 : U_i \times_U U_j \longrightarrow U_j$), then there exist $s \in F(U)$ whose pullback in $F(U_i)$ is equal to s_i for all i.

Proposition 1.54 Given a site $\mathcal{C}$, a functor $F : \mathcal{C}^{op} \longrightarrow \mathbf{Set}$ is a sheaf if and only if the following diagram is an equalizer for every covering $\{U_i \longrightarrow U\}$ in $\mathcal{C}$:

$$F(U) \longrightarrow \prod_i F(U_i) \underset{p_2^*}{\overset{p_1^*}{\rightrightarrows}} \prod_{i,j} F(U_i \times_U U_j) \tag{1.53}$$

Proof. We proceed by steps

Step 1: From the definition of sheaf, let $(s_i)_i$ be sections $\in (F(U_i))_i$ such that

$$\mathrm{pr}_1^*(s_i) = \mathrm{pr}_2^*(s_j) \in F(U_i \times_U U_j) \tag{1.54}$$

for every i, j.

Step 2: Then F is a sheaf if and only if there exist a **unique** $s \in F(U)$ and $s \mapsto s_i \in F(U_i)$, i.e. the diagram above is an equalizer and we get:

$$F(U) = \ker(\prod_i F(U_i) \underset{\mathrm{pr}_2^*}{\overset{\mathrm{pr}_1^*}{\rightrightarrows}} \prod_{i,j} F(U_i \times_U U_j)) \tag{1.55}$$

Step 3: Clearly $\prod_i F(U_i) \ni (s_i)_i \mapsto (\mathrm{pr}_k^*(s_i))_i \in \prod_{i,j} F(U_i \times_U U_j)$ is induced by $F(U_i) \ni s_i \mapsto \mathrm{pr}_k^*(s_i) \in F(U_i \times_U U_j)$ for $k = 1, 2$. □

Now we itroduce also the definition of *fppf* topology, a Grothendieck topology which is "finer" than the Zariski one.

Definition 1.55 Let k be a commutative ring. The category of (affine) schemes over k (**Aff**)**Sch**$/k$ endowed with the **Grothendieck-fppf** topology, is a site where a covering $\{U_i \longrightarrow U\}$ is given by a jointly surjective collection of maps (i.e. such that the set-theoretic union of their images equals the entire U) that are **flat** and **finitely presented** (see [2.20]). This is the true meaning of the name *fppf* which comes from: *"fidèlement plat et de présentation finie"*.

Just to be more precise one can use the given definition [1.49] as the definition of a Grothendieck **pretopology** and then see that, once introduced the notion of *sieve*, two pretopologies inducing the same topology are equivalent in some sense, namely if they

"contain" the same sieves and hence induce the same sheaves. We sum up, without proving them, some constructions, see ([Vi], II) for details.

Construction 1.56

- Let U be an object of a category $\mathcal{C}$, and $F : \mathcal{C}^{op} \longrightarrow \mathbf{Set}$ a presheaf. One can define, for a generic set of arrows $\mathcal{U} = \{U_i \longrightarrow U\}$, the set $F(\mathcal{U})$ as the subset of $\prod_i F(U_i)$, such that the images of its elements in $\prod_{i,j} F(U_i \times_U U_j)$ (given by the pull-backs) coincide. In particular if $\mathcal{C}$ is a site, one can consider as $\mathcal{U}$ the covering $\mathcal{U} = \{U_i \longrightarrow U\}$.
- It is easy to show that if $\mathcal{C}$ is a site, F is a sheaf if and only if the natural map:

$$F(U) \xrightarrow{\sim} F(\mathcal{U}) \tag{1.56}$$

  induced by a covering, namely by the maps $F(U) \longrightarrow F(U_i)$, is a **bijection**.
- Consider the Yoneda embedding: $h_U := \mathrm{Hom}_{\mathcal{C}}(-, U) : \mathcal{C}^{op} \ni X \mapsto \mathrm{Hom}_{\mathcal{C}}(X, U) \in \mathbf{Set}$. Let U be an object of the category $\mathcal{C}$, a **sieve** on U is a subfunctor $\mathcal{S} \subseteq h_U$.
- Given an object $U \in \mathcal{C}$, and a set of arrows $\mathcal{U} = \{U_i \longrightarrow U\}$, we can consider the **sieve** associated with $\mathcal{U}$ as the subfunctor $h_{\mathcal{U}} \subseteq h_U$ such that for every object T, $h_{\mathcal{U}}(T)$ is the set of arrows that factorize throughout U_i for some i: $T \longrightarrow U_i \longrightarrow U$.
- It can be proven that there is a canonical bijection $\mathrm{Hom}(h_{\mathcal{U}}, F) \simeq F(\mathcal{U})$, and that a functor F is a sheaf for the site $\mathcal{C}$ if and only if for any covering $\mathcal{U} = \{U_i \longrightarrow U\}$, there is a bijection:

$$F(U) \simeq \mathrm{Hom}(h_U, F) \xrightarrow{\sim} \mathrm{Hom}(h_{\mathcal{U}}, F) \simeq F(\mathcal{U}) \tag{1.57}$$

- Let $\mathcal{T}$ be a Grothendieck topology on a category $\mathcal{C}$. We say that a sieve $\mathcal{S} \subseteq h_U$ belongs to $\mathcal{T}$, if there exist a covering $\mathcal{U} = \{U_i \longrightarrow U\}$ such that $h_{\mathcal{U}} \subseteq \mathcal{S}$.
- Finally, it is easy to show that a functor $F : \mathcal{C}^{op} \longrightarrow \mathbf{Set}$ is a sheaf for the topology $\mathcal{T}$ of the site $\mathcal{C}$, if and only if for every sieve $\mathcal{S} \in \mathcal{T}$ there is a bijection:

$$F(U) \simeq \mathrm{Hom}(h_U, F) \xrightarrow{\sim} \mathrm{Hom}(S, F) \tag{1.58}$$

Notice that the category of **sheaves** of abelian groups on a site $\mathcal{C}$ (namely the full subcategory of $\mathrm{Fnct}(\mathcal{C}^{op}, \mathbf{AbGps})$ made of those presheaves that are sheaves for the Grothendieck topology on $\mathcal{C}$) is an abelian category. We conclude with a more general and useful result about presheaves. Recall that the category $\mathrm{Fnct}(\mathcal{C}^{op}, \mathbf{Set})$ admits limits and colimits ([1.44]) computed pointwise (since **Set** admits limits and colimits).

Theorem 1.57 Every presheaf $F : \mathcal{C}^{op} \to \mathbf{Set}$ is the inductive limit of (its) representable presheaves (i.e. those presheaves of the form $h_X \subseteq F$ where h_X is the Yoneda embedding [1.24]).

Proof. Consider the Yoneda embedding $X \mapsto \mathrm{Hom}_{\mathcal{C}}(-, X) \in \mathrm{Fnct}(\mathcal{C}^{op}, \mathbf{Set})$. Consider the category $\mathcal{C}/F$ i.e. the category whose obects are the (natural) morphisms $h_X \to F$ for $X \in \mathcal{C}$ and whose morphisms are the commutative diagrams:

$$\begin{array}{ccc} h_X & \xrightarrow{h_f} & h_Y \\ & \searrow \quad \swarrow & \\ & F & \end{array} \tag{1.59}$$

where $f : X \to Y$ is a morphism. Consider the forgetful functor $for : \mathcal{C}/F \to \mathcal{C}$. We want to show that:

$$F \simeq \varinjlim_{(h_X \to F) \in \mathcal{C}/F} (h_{(-)} \circ for) \tag{1.60}$$

Let now $G \in \mathrm{Fnct}(\mathcal{C}^{op}, \mathbf{Set})$, we have that:

$$\mathrm{Hom}_{\mathrm{Fnct}(\mathcal{C}^{op}, \mathbf{Set})}(\varinjlim_{(h_X \to F) \in \mathcal{C}/F} (h_X \circ for), G) \simeq \varprojlim_{(h_X \to F) \in \mathcal{C}/F} \mathrm{Hom}_{\mathrm{Fnct}(\mathcal{C}^{op}, \mathbf{Set})}(h_X, G) \simeq \tag{1.61}$$

$$\simeq \varprojlim_{(h_X \to F) \in \mathcal{C}/F} G(X) \simeq \mathrm{Hom}_{\mathrm{Fnct}((\mathcal{C}/F)^{op}, \mathbf{Set})}(\top, G) \tag{1.62}$$

where we used the Yoneda lemma and the universal property of the inverse limit together with the property of the terminal object; here we also used $\top$ to indicate both the functor $\top :$ object $\mapsto \top$ and the terminal object. Now for each element $\alpha \in \mathrm{Hom}_{\mathrm{Fnct}((\mathcal{C}/F)^{op}, \mathbf{Set})}(\top, G)$ there is a natural isomorphism $\alpha : F \to G$ given by:

$$\mathcal{C}/F \ni (h : h_X \to F) = (h \in F(X)) \mapsto \alpha_X : \top \to G(X) \tag{1.63}$$

functorial in X, which gives the isomorphism:

$$\mathrm{Hom}_{\mathrm{Fnct}((\mathcal{C}/F)^{op}, \mathbf{Set})}(\top, G) \simeq \mathrm{Hom}_{\mathrm{Fnct}(\mathcal{C}^{op}, \mathbf{Set})}(F, G) \tag{1.64}$$

and we can conclude the proof. □

1.2 Algebras, bi-algebras and Höpf algebras

Before dealing with the important notions of *schemes* and *affine schemes* (both in a classical geometrical way and using the categorical-algebraic tools), we shall recall the concept of *algebra* and introduce the related structures of *bi-algebra* and *Höpf algebra*. Starting from this and thanks to the categorical notion of equivalence developed before, it will be much more easier to understand *affine group schemes* and their properties.

Along the whole section let k be a commutative unital ring.

1.2.1 Basic notions: rings and modules

Remark/Definition 1.58 A commutative unital ring k is said to be a **local** ring if it has a unique maximal ideal $\mathcal{M}$. The localization of a ring at a prime ideal $\mathcal{P}$, i.e. $k_{\mathcal{P}} := \{\frac{r}{s} | r \in k, s \in k \setminus \mathcal{P}\}$, is a local ring with unique maximal ideal $\mathcal{P}_{\mathcal{P}}$. The **Krull dimension** of a ring k is the supremum of the different possible lengths of strict inclusions of primes $\mathcal{P}_0 \subseteq ... \subseteq \mathcal{P}_n$.

Remark/Definition 1.59 Recall that for a k-module R we shall mean an abelian group $(R, +)$ together with a map $(-) \cdot (-) : k \times R \to R$ (a "scalar" operation on R namely $a \cdot r = ar \in R$ for $a \in k$) s.t. $1_k \cdot r = r$, $(a + b) \cdot r = a \cdot r + b \cdot r$, $(ab) \cdot r = a \cdot (b \cdot r)$, $a \cdot (r + s) = a \cdot r + a \cdot s$ and in particular $0_k \cdot r = 0_R$, for each $a, b \in k$ and $r, s \in R$. The category of k-modules is denoted with $\mathbf{Mod_k}$ as in [1.30], and morphisms between k-modules are k-linear maps, i.e. $\varphi : R \to S$ s.t. $\varphi(ar + bs) = a\varphi(r) + b\varphi(s)$. (Here S is another k-module).

Remark/Definition 1.60 We denote with $(-) \otimes (-) : \mathbf{Mod_k} \times \mathbf{Mod_k} \to \mathbf{Mod_k}$, the **tensor product** defined on the category of k-modules using one of the two following equivalent contructions:

- (universal property): for each $R, S \in \mathbf{Mod_k}$, their tensor product is given by a k-module (that we denote a-priori) $R \otimes S$, together with a k-bi-linear map $\tau : R \times S \to R \otimes S$, such that for each k-module T and k-bi-linear map $\psi : R \times S \to T$ there exist a *unique* k-linear map $\varphi : R \otimes S \to T$ that makes the following diagram commutative:

$$\begin{array}{ccc} R \times S & \xrightarrow{\psi} & T \\ {\scriptstyle\tau}\downarrow & \nearrow_{\exists! \varphi} & \\ R \otimes S & & \end{array}$$

we write $\tau(r, s) =: r \otimes s$ for each $r \in R$ and $s \in S$.

- (quotient construction): consider the map $I \hookrightarrow k^{(I)}$ given by $i \mapsto (0, 0, ..., \overset{\text{i-th}}{1}, ..., 0, ...)$; then identify $R \times S$ with a subset of $k^{(R \times S)}$ (for each $R, S \in \mathbf{Mod_k}$). The tensor product $R \otimes S$ is the k-module given by the quotient $(R \times S)/Q$, where the sub-module Q is the one generated by the relations:

$$\begin{aligned} Q :=< (r + r', s) - (r, s) - (r', s);\ (r, s + s') - (r, s) - (r, s');& \\ (ar, s) - a(r, s);\ (ar, s) - (r, as) >& \end{aligned}$$

for each $r \in R$, $s \in S$ and $a \in k$. We denote $r \otimes s := \overline{(r, s)}$ for each $r \in R$ and $s \in S$.

Remark/Definition 1.61 An exact sequence of k-modules $0 \to M \to N \to P \to 0$ is an exact sequence, as defined in [1.45], in the abelian category of k-modules $\mathbf{Mod_k}$.

We recall some basic notions on k-modules before introducing the definition of algebra and co-algebra. We will state more properties (linked to the notion of tensor products) and then show some important connections with modules and schemes in the next section.

Definition 1.62 A k-module R is said to be:

(i) **finitely generated**: if there exist $r_1, r_2, ..., r_n \in R$ such that for each $r \in R$ we can write $r = \lambda_1 r_1 + ... + \lambda_n r_n$, with $\lambda_i \in k$ for $i = 1, ..., n$;

(ii) **free**: if it admits a *basis*, i.e. if there exists a set S of elements of R such that each $r \in R$ is written as a linear combination of finite elements of S and the elements of S are linearly independent; namely each $r \in R$ is such that there exist $s_1, ..., s_n \in S$ and $r = \lambda_1 s_1 + ... + \lambda_n s_n$, and moreover if $\lambda_1 s_1 + ... + \lambda_n s_n = 0_R$ then $(\lambda_1, ..., \lambda_n) = (0, ..., 0) \in k^n$.

(iii) **projective**: if for every surjective module homomorphism $N \twoheadrightarrow M$ and for any k-module homomorphism $R \to M$, there exists a k-module homomorphism $R \to N$ that makes commutative the diagram:

$$\begin{array}{ccc} & & N \\ & \nearrow & \downarrow \\ R & \longrightarrow & M \end{array} \tag{1.65}$$

(iv) **flat**: if for every injective k-module homomorphism $L \hookrightarrow K$, then taking the tensor product with R preserves injectivity, i.e. the map $R \otimes_k L \hookrightarrow R \otimes_k K$ is injective too;

(v) **locally free**: if the localization of R at every prime ideal, i.e. $R_{\mathfrak{p}}$, is a free k-module over the corresponding localization $k_{\mathfrak{p}}$;

(vi) **torsion free**: if its torsion sub-module contains only the zero element, i.e. 0_R is the only element annihilated by a non-zero divisor;

(vii) **of finite lenght**: if the largest length of any chain of submodules contained in R, i.e. $(0) = R_0 \subseteq R_1 \subseteq ... \subseteq R_n = R$, is finite; we write length$(R) = n$ (if n is finite it is the same value for every reduced chain of submodules);

(viii) **noetherian**: if every ascending chain of submodules of R, namely $(0) = R_0 \subseteq R_1 \subseteq ... \subseteq R_n \subseteq ...$, stabilizes, i.e. equivalently if every submodule of R is finitely generated;

(ix) **artinian**: if every descending chain of submodules of R, namely $R = R_0 \supseteq R_1 \supseteq ... \supseteq R_n \supseteq ...$, stabilizes;

(x) **finitely presented**: if it is finitely generated and morover there exists an exact sequence of k-modules: $k^m \to k^n \to R \to 0$.

Remark 1.63 We state some useful implications about the previous definitions:

- if a commutative unital ring k is noetherian, then the k-module R is noetherian if and only if it is finitely generated;
- a k-module R is both a noetherian and an artinian k-module if and only if it has finite length;
- the following implications are true: R is free $\Rightarrow$ R is projective $\Rightarrow$ R is locally free $\Rightarrow$ R is flat $\Rightarrow$ R is torsion free;
- if R is finitely presented then: R is flat $\Leftrightarrow$ R is projective;
- if k is noetherian then to be finitely presented and to be finitely generated are equivalent properties for R;
- if R is finitely generated over a noetherian ring k, then: R is locally free $\Leftrightarrow$ R is projective.

1.2.2 Algebras and co-algebras

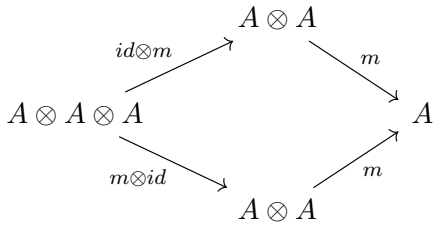
Definition 1.64 A k-**algebra** is a k-module A together with a *ring structure* given by two k-linear maps:

$$m : A \otimes A \to A \tag{1.66}$$

$$e : k \to A \tag{1.67}$$

such that:

- the following diagram commutes (*associativity*):



and moreover:

- the following maps are nothing but the *identity* map $id_A : A \to A$ on A:

$$A \simeq k \otimes A \xrightarrow{e \otimes id} A \otimes A \xrightarrow{m} A$$

$$A \simeq A \otimes k \xrightarrow{id \otimes e} A \otimes A \xrightarrow{m} A$$

(where $A \simeq k \otimes A$ is given by $a \mapsto 1_k \otimes a$ for each $a \in A$).

The definition above is clearly equivalent to the classical construction of an algebra structure on a set.

Proposition 1.65 Let k be a commutative unital ring as above. The above and the following two alternative definition of k-algebra are equivalent.

(i) a k-algebra A is a *ring* A together with a ring *homomorphism* $e' : k \to A$;

(ii) A is a k-module and there exist a map $(-)\cdot(-) : A \times A \to A$ satisfying the bilinearity relations defined in the construction of Q (in the above Definition of tensor ptoduct [1.60]), and satisfying also associativity and identity. Namely $\lambda(a \cdot b) = \lambda a \cdot b = a \cdot \lambda b$, $(a+b)\cdot c = a \cdot c + b \cdot c$, $a \cdot (b+c) = a \cdot b + a \cdot c$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ and $\exists\ 1_A$ s.t. $1_A \cdot a = a \cdot 1_A = a$, for each $a, b, c \in A$, $\lambda \in k$.

Proof. Clearly *(ii)* $\Leftrightarrow$ there exist maps m and e as in the above Definition [1.64], thanks to the definition of tensor product, in particular considering the diagram:

$$\begin{array}{ccc} A \times A & \xrightarrow{(-)\cdot(-)} & A \\ {\scriptstyle\tau}\downarrow & \nearrow_{\exists! m} & \\ A \otimes A & & \end{array}$$

For *(ii)* $\Leftrightarrow$ *(i)* observe that, since A is a ring, there exist an internal multiplication which is associative and distributive with respect to the sum operator, and clearly it satisfies the bilinearity relations above. Moreover $e'(1_k) := 1_A$ is the identity element of A. □

Now we want to "reverse" in some sense the maps above and build a new structure with similar operations.

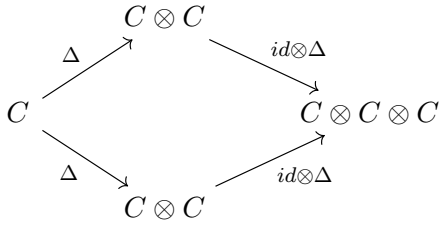
Definition 1.66 A k-**co-algebra** that is co-associative and with co-identity is a k-module C together with two k-linear maps:

$$\Delta : C \to C \otimes C \tag{1.68}$$

$$\epsilon : C \to k \tag{1.69}$$

such that:

- the following diagram commutes (*co-associativity*):



and moreover:

- the following maps are nothing but the *identity* map $id_C : C \to C$ on C (*co-identity*):

$$C \xrightarrow{\Delta} C \otimes C \xrightarrow{\epsilon \otimes id} k \otimes C \simeq C$$
$$C \xrightarrow{\Delta} C \otimes C \xrightarrow{id \otimes \epsilon} C \otimes k \simeq C$$

(where $C \simeq k \otimes C$ is given by $c \mapsto 1_k \otimes c$ for each $c \in C$).

Definition 1.67 Let R be a k-module, then we define the **dual** k-module R^* to be the set of k-modules homomorphisms (i.e. k-linear maps) from R to k, namely $R^* := \mathrm{Hom}_{k-mod}(R, k)$, with an obvious k-module structure. Clearly $R^* \simeq R^* \otimes k = \mathrm{Hom}_{k-mod}(R, k)$, and by extension of scalars (by definition of tensor pruducts) $R^* \otimes_k S = \mathrm{Hom}_{k-mod}(R, S)$.

Proposition 1.68

(i) Let (C, Δ, ϵ) be a k-co-algebra, then C^* is an associative k-algebra;

(ii) let (A, m, e) be a k-algebra, then if A is projective and finitely generated A^* is a k-co-algebra.

Proof. See for example ([Mi1], ch. II). □

Definition 1.69 A **homomorphism** between two co-algebras C and D is a k-linear map $f : C \to D$ such that the following diagrams commute:

$$\begin{array}{ccc} C \otimes C & \xrightarrow{f \otimes f} & D \otimes D \\ \uparrow{\scriptstyle \Delta} & & \Delta \uparrow \\ C & \xrightarrow[f]{} & D \end{array} \qquad \begin{array}{ccc} C & \xrightarrow{f} & D \\ \downarrow{\scriptstyle \epsilon} & \swarrow_{\epsilon} & \\ k & & \end{array} \tag{1.70}$$

1.2.3 Group objects, bi-algebras, Höpf algebras

Let us now introduce the notion of *bi-algebra* and then that of *Höpf algebra*. Finally we conclude with an important characterization.

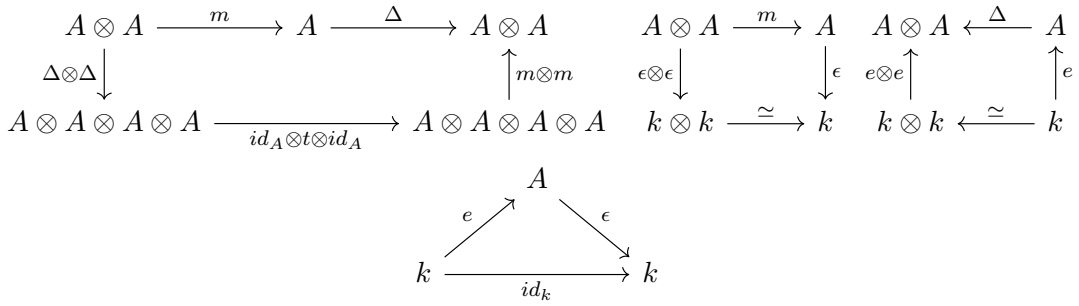
Definition 1.70 A **bi-algebra** over k, or a k-bi-algebra, is given by $(A, m, e, \Delta, \epsilon)$, where A is a k-module and:

- (A, m, e) is a k-algebra (associative with identity e);
- (A, Δ, ϵ) is a k-co-algebra (co-associative with co-identity ϵ);
- $\Delta : A \to A \otimes A$ is a homomorphism of k-algebras;
- $\epsilon : A \to k$ is a homomorphism of k-algebras.

Proposition 1.71 The last two conditions of the previous definition, (i.e. to require that Δ and ϵ are k-algebra homomorphisms) are equivalent to:

- m and e are k-co-algebra homomorphisms

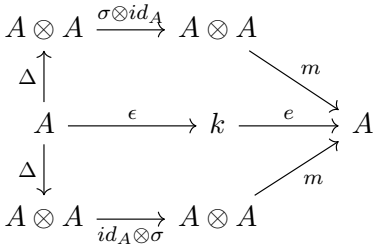
Proof. The conditions stated are both equivalent to the commutativity of the following diagrams:



where the map $t : A \otimes A \to A \otimes A$ is such that $t(a \otimes b) := b \otimes a$.

□

Definition 1.72 An **inverision** map for a bi-algebra A over k, which is also called **antipode**, is a k-linear map $\sigma : A \to A$, such that the following diagram commutes:



Definition 1.73 A k-algebra A can be seen as a category, where objects are the elements $a \in A$ and morphisms $a \to b$ are given by the product law $a \cdot b$ that makes A a k-algebra. Clearly A^{op} is given by substituting ab with ba. The same construction can be applied to a k-co-algebra C (with the co-multiplication Δ).

Proposition 1.74 The antipode $\sigma : A \to A$ is an *anti-isomorphism* of k-(co)algebras, i.e. maps A to A^{op} both as an algebra and as a co-algebra; in particular $\sigma(ab) = \sigma(b)\sigma(a)$ and $\sigma(1_A) = 1_A$. (This is obvious if A is commutative and descends from the Definition [1.73] above).

Proof. Using a notation called *Sweedler notation*, we consider

$$\Delta(a) := \sum_i a'_i \otimes a''_i =: a_{(1)} \otimes a_{(2)} \tag{1.71}$$

and we use the property of the tensor product $A \otimes A$ such that each $a \in A \otimes A$ can be written as linear combination of elements of the form $a' \otimes a''$ (and those elements can be viewed as equivalence classes $\overline{(a', a'')}$, as in the construction of tensors). Then we "forget" about the summation symbol. Now from the diagram of the above Definition [1.72] and

using the notation introduced, we have that:

$$\sigma(a_{(1)})a_{(2)} = a_{(1)}\sigma(a_{(2)}) = (e \circ \epsilon)(a) = \epsilon(a)1_A \textbf{ 1st property} \tag{1.72}$$

$$a = a_{(1)}\epsilon(a_{(2)}) = \epsilon(a_{(1)})a_{(2)} \textbf{ 2nd property} \tag{1.73}$$

$$\sigma(a) = \sigma(a_{(1)})\epsilon(a_{(2)})1_A \textbf{ 3rd property} \tag{1.74}$$

where we used, respectively, the definition of σ and the properties of e and ϵ. Then we have that:

$$\sigma(ab) \overset{\text{3rd-prop.}}{=} \sigma(ab_{(1)}) \cdot \epsilon(a_{(2)})1_A \cdot \epsilon(b_{(2)})1_A \overset{\text{1st-prop.}}{=} \tag{1.75}$$

$$= \sigma(a_{(1)}b_{(1)}) \cdot \sigma(a_{(2)})a_{(3)} \cdot \epsilon(b_{(2)})1_A \overset{\text{def } \sigma \text{ + commut}}{=} \tag{1.76}$$

$$= \sigma(a_{(1)}b_{(1)}) \cdot a_{(2)} \cdot \epsilon(b_{(2)})1_A \cdot \sigma(a_{(3)}) \overset{\text{1st-prop.}}{=} \tag{1.77}$$

$$= \sigma(a_{(1)}b_{(1)}) \cdot a_{(2)}b_{(2)} \cdot \sigma(b_{(3)})\sigma(a_{(3)}) \overset{\text{1st-prop.}}{=} \tag{1.78}$$

$$= \epsilon(a_{(1)}b_{(1)})1_A \cdot \sigma(b_{(3)})\sigma(a_{(3)}) \overset{\text{commut}}{=} \tag{1.79}$$

$$= \epsilon(b_{(1)})1_A\sigma(b_{(3)}) \cdot \epsilon(a_{(1)})1_A\sigma(a_{(3)}) \overset{\text{3rd-prop}}{=} \tag{1.80}$$

$$\sigma(b)\sigma(a) \tag{1.81}$$

We omitted the operator $(-) \cdot (-)$ whenever clear from the context. Recall that $\epsilon(-) \in k$ and that the map $(e \circ \epsilon)(-)$ commutes with all elements of A by definition. The proof for k-co-algebras is analogous. □

Definition 1.75 Let H be a k-bi-algebra, then if H admits an inversion map it is said to be a **Höpf algebra**. Clearly a **homomorphism** between Höpf algebras is given by a homomorphism between the underlying bi-algebras.

Notice that thanks to Definition [1.70] and to Proposition [1.71] above, the notion of *bi-algebra* is self-dual, and hence also the notion of *Höpf algebra* is self-dual (meaning that H is again a bi-algebra/Höpf algebra in the category $\mathbf{Mod_k}^{op}$); moreover, if H is a Höpf algebra that is finitely generated and projective as k-module, then H^* (the dual module) is again a Höpf algebra thanks to the Proposition [1.68].

Definition 1.76 A k-bi-algebra A is said to be:

- **commutative** if its underlying k-algebra is commutative;
- **co-commutative** if its underlying k-co-algebra is co-commutative, i.e. if the following diagram commutes:

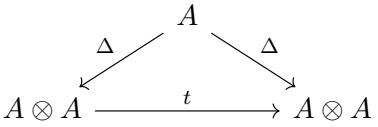


Figure 1.3: co-commutativity

- **finitely generated (finitely presented)** if its underlying k-module is finitely generated (resp. finitely presented).
- If a k-algebra is finitely generated as k-algebra (and not as k-module) we say it is of **finite type**.

We conclude with an important result which allow us to show the deep connection between *Höpf algebras* and *affine group schemes* in Section 2.2. We first recall an important definition coming from category theory.

Definition 1.77 Let $\mathcal{C}$ be a category that admits *finite products* (i.e. binary cartesian products between objects, and a terminal object $\top$). A **group object** G in $\mathcal{C}$, is given by a quadruple (G, m, e, i), where $m : G \times G \to G$, $e : \top \to G$ and $i : G \to G$ are morphisms such that the following diagrams commute:

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{id_G \times m} & G \times G \\ {\scriptstyle m \times id_G}\downarrow & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow[m]{} & G \end{array} \qquad \begin{array}{ccc} \top \times G & \xrightarrow{e \times id_G} & G \times G \\ {\scriptstyle id_G \times e}\downarrow & \overset{\simeq}{\searrow} & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow[m]{} & G \end{array} \tag{1.82}$$

$$\begin{array}{ccc} G & \xrightarrow{(\mathrm{i}, id_G)} & G \times G \\ {\scriptstyle (id_G, \mathrm{i})}\downarrow & \overset{e \circ \top}{\searrow} & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow[m]{} & G \end{array} \tag{1.83}$$

where $\top$ is the unique morphism $top : G \to \top$.

Theorem 1.78 A Höpf algebra H is a *group object* in the category $\mathbf{Alg_k}^{op}$ of k-algebras.

Proof. Clearly $\mathbf{Alg_k}^{op}$ admits binary products (between k-algebras), and k is a terminal object. Given a k-algebra A one can also define a co-product $A \oplus A$ such that

$$A \hookrightarrow A \oplus A \hookleftarrow A \tag{1.84}$$

as in Remark [1.42], and one can see that this definition coincides with that of tensor product $A \otimes A$. (We already observed that the category $\mathbf{Alg_k}^{op}$ is an abelian category, see ([Sc], ch. IV) for details).

($\Rightarrow$): Given a Höpf algebra H, consider an object $G := h^H$ in the category of presheaves as in Corollary [1.28]; since H is, in particular, a bi-algebra, then from the k-algebra homomorphisms $\Delta : H \to H \otimes H$ and $\epsilon : H \to k$, we know that the diagrams of Definitions [1.64] and [1.66] and of Proposition [1.71] commute. We have that the functor $H \mapsto h^H$ given by the Yoneda Lemma [1.26], is fully faithful, and sends tensor products (that are *comproducts* of k-algebras) to products, namely $\mathrm{Hom}(h^H \times h^H, h^H) \simeq \mathrm{Hom}(H, H \otimes H)$. As a consequence (of the commutativity of the diagrams of [1.66]) the diagrams of the above Definition [1.77] (of group object - namely eq. (1.82)), letting $G := h^H$, commute too. Moreover, if $\sigma : H \to H$ is the inversion map, then from Definition [1.72], this implies

that the diagram of eq. (1.83) - about the inverse of G - commutes too. (Thanks again to Yoneda lemma, and considering $h^\sigma : h^H \to h^H$).

($\Leftarrow$): Conversely, to give a group object H in the category $\mathbf{Alg_k}^{op}$, means that the diagrams of Definition [1.77] above (again equations (1.82) and (1.83)), when applied to H, commute, and hence h^H is a group object in the category of presheaves. This implies that the diagrams of Definitions [1.66] and [1.72] above, commute too (thanks again to Yoneda). In particular there exist maps Δ, ϵ, σ such that $(H, m, e, \Delta, \epsilon, \sigma)$ is a Höpf algebra with inversion. $\square$

Chapter 2

Schemes, group schemes and formal schemes

2.1 Schemes and formal schemes

In this section we introduce the concept of **(affine) scheme** using both the classical approach coming from algebraic geometry (and strictly connected to the notion of affine variety) and as well the more formal algebraic-categorical aspect. The first one uses tools such as the **spectrum of a ring** or objects such as **locally ringed spaces**, and takes advantage of the underlying topological structure of those objects; while the latter introduces schemes and affine schemes as functors of a presheaves category. We will see that there is an equivalence between these two points of view.

After giving some characterizations we deal with the **group objects** of the category of (affine) schemes and finally we build the notion of **formal scheme** using topological rings.

2.1.1 Geometrical approach

Let k be a commutative unital ring (our base ring). Let K be an algebraically closed field. Denote by $\mathbf{Alg_k}$, as before, the category of k-algebras (that are associative, commutative and with a natural ring structure).

We start by introducing the notions we need in order to give a complete definition of *affine scheme* as a topological space, in the classical geometrical sense.

Definition 2.1 A **ringed space** X, is a topological space X together with:

- a **structure sheaf** of k-algebras (see Definition [1.53] and Remark [2.4]), i.e. $\mathcal{O}_X \in \mathrm{Fnct}(\mathrm{Op}^{op}, \mathbf{Alg_k})$;
- restriction maps $\rho_{V,U} : \mathcal{O}_X(V) \to \mathcal{O}_X(U)$, for every $U \subseteq V \in \mathrm{Op}^{op}$;

where Op^{op} is the category consisting of the open subsets of X with morphisms given by the inclusions (i.e. $U \to V$ if and only if $U \subseteq V$), while $\mathrm{Fnct}(\mathrm{Op}^{op}, \mathbf{Alg_k})$ is the presheaves

category of contravariant functors $\mathrm{Op}^{op} \to \mathbf{Alg_k}$; (one can see that this definition agree with Definition [1.53] and Example [1.50]). See [Sc], ch. V, for details.

Definition 2.2 A **locally ringed space** X, is a ringed space such that, for every $\mathbf{x} \in X$, all the **stalks**

$$\mathcal{O}_{X,\mathbf{x}} := \varinjlim_{U \ni \mathbf{x}} \mathcal{O}_X(U), \tag{2.1}$$

are **local rings**.

Remark 2.3 The definition of ringed space can be given requiring the structure sheaf to be simply a sheaf of *rings*, i.e. $\mathrm{Op}^{op} \to \mathbf{Rng}$. Here we wanted to give a much more general notion, observing that all k-algebras are indeed rings and that all commutative unital rings can be seen as $\mathbb{Z}$-algebras. We will clarify this in definition [2.17].

Remark 2.4 The sheaf $\mathrm{Op}^{op} \to \mathbf{Rng}$ can be defined using the Grothendieck topology of the open subsets of X (see Example [1.50]). From Definition [1.53] (of sheaf), keeping in mind the conditions a sheaf must satisfy, we have that:

- $\mathcal{O}_X(\emptyset) = 0$;
- $\rho_{U,U} = \mathrm{id}_U$, the identity map on U;
- $\rho_{V,U} \circ \rho_{W,V} = \rho_{W,U}$, for all $U \subseteq V \subseteq W \in \mathrm{Op}^{op}$;
- $\mathcal{O}_X$ satisfies the gluing property (of [1.53]):

  for each open $U \subseteq X$, each open covering $\{U_i\}_i$ of U, and sections $\varphi_i \in \mathcal{O}_X(U_i)$ s.t. $\varphi_i|_{U_i \cap U_j} = \varphi_j|_{U_i \cap U_j}$, then there exist a unique $\varphi \in \mathcal{O}_X(U)$ s.t. $\varphi|_{U_i} = \varphi_i$.

Definition 2.5 A **morphism** between ringed spaces X and Y, is given by:

- a continuous map between the underlying topological spaces, $f : X \to Y$;
- a family of k-algebras homomorphisms (or ring-homomorphisms as well),

$$\varphi_V : \mathcal{O}_Y(V) \to \mathcal{O}_X(f^{-1}(V)) \tag{2.2}$$

  for each open $V \subseteq Y$, such that the following diagram commutes (i.e. the maps are compatible with the restrictions):

$$\begin{array}{ccc} \mathcal{O}_Y(V_2) & \xrightarrow{\varphi_{V_2}} & \mathcal{O}_X(f^{-1}(V_2)) \\ {\scriptstyle \rho_{V_2,V_1}}\downarrow & & \downarrow{\scriptstyle \rho_{f^{-1}(V_2),f^{-1}(V_2)}} \\ \mathcal{O}_Y(V_1) & \xrightarrow[\varphi_{V_1}]{} & \mathcal{O}_X(f^{-1}(V_1)) \end{array} \tag{2.3}$$

  for every $V_1 \subseteq V_2 \in Y$.

- If, moreover, X and Y are *locally* ringed spaces, then for each $\mathbf{x} \in X$, the map between the local rings $\varphi_{\mathbf{x}} : \mathcal{O}_{X,\mathbf{x}} \to \mathcal{O}_{Y,f(\mathbf{x})}$, must preserve maximality, i.e. sends the maximal ideal of $\mathcal{O}_{X,\mathbf{x}}$ to the maximal ideal of $\mathcal{O}_{Y,f(\mathbf{x})}$.

Definition 2.6 Let k be our base ring as always. The **spectrum** of k is the set

$$\mathrm{Spec}(k) := \{\mathcal{P} \subseteq k | \mathcal{P} \text{ prime ideal of } k\} \tag{2.4}$$

of all **prime ideals** of k.

Remark/Definition 2.7 Recall that an **affine variety** over an algebraically closed field K, say $X \subseteq \mathbb{A}^n_K$, is defined as $X := V(\mathcal{S}) = \{x \in \mathbb{A}^n_K | f(x) = 0 \text{ for all } f \in \mathcal{S}\}$, where $\mathcal{S} \subseteq K[X_1, ..., X_n]$ is a **finite set** of polynomials (see Warning [W1]). $K[X_1, ..., X_n]$ is the coordinate polynomial ring of the n-dimensional affine space $\mathbb{A}^n_K$.

Warning! Notice that, as we are going to see in [2.15], in the above Definition [2.7] it is actually the same thing to consider either the set $V(\mathcal{S})$ or the set $V(\mathcal{I})$, where $\mathcal{I}$ is the ideal generated by $\mathcal{S}$ in $K[X_1, ..., X_n]$. So that $f(x) = 0$ for $f \in \mathcal{S}$ if and only if $f(x) = 0$ for $f \in \mathcal{I}$. Since K is a field, then $K[X_1, ..., X_n]$ is noetherian and $\mathcal{I}$ is finitely generated. Also notice that $f^n(x) = 0 \Rightarrow f(x) = 0$, and this means that $f^n \in \mathcal{I} \Rightarrow f \in \mathcal{I}$ and so that a variety must always be **reduced** (see Warning [W3] after Definition [2.20]).

We can define *functions* on $\mathrm{Spec}(k)$ and see that those functions can be viewed as the elements of the base ring k itself. This will be more clear in the following definition, keeping in mind the case of the coordinate ring $A(X)$ of an affine variety X, which is given by $A(X) := k[X_1, ..., X_n]/\mathcal{I}$, where $\mathcal{I}$ is the ideal generated by the set $\mathcal{S}$ defining the varierty X.

Definition 2.8 Let $\mathcal{P} \in \mathrm{Spec}(k)$ be a prime ideal of k,

- the **residue field** of $\mathrm{Spec}(k)$ at $\mathcal{P}$ is the field

$$K(\mathcal{P}) := \mathrm{Quot}(k/\mathcal{P}) \tag{2.5}$$

  i.e. the quotient field of the domain $k/\mathcal{P}$.

- let $f \in k$, then f can be viewed as a **function** on $\mathrm{Spec}(k)$ and its value at $\mathcal{P}$ is given by:

$$k \twoheadrightarrow k/\mathcal{P} \hookrightarrow K(\mathcal{P}) \tag{2.6}$$

$$f \mapsto \overline{f} \ (\mathrm{mod.}\ \mathcal{P}) \mapsto \frac{\overline{f}}{1} =: f(\mathcal{P}) \tag{2.7}$$

We can endow the spectrum of a ring with a topology, called the *Zariski topology*. It is much more simple to define this topology by declaring what are its closed subsets rather then its opens.

Definition 2.9 The **Zariski topology** on $\mathrm{Spec}(k)$ is defined specifying the **closed subsets** to be all the sets of the form:

$$V(I) := \{\mathcal{P} \text{ prime ideal} \in \mathrm{Spec}(k) | \mathcal{P} \supseteq I\} \tag{2.8}$$

for every ideal I of k. Or equivalently:

$$V(\mathcal{S}) := \{\mathcal{P} \text{ prime ideal} \in \mathrm{Spec}(k) | \mathcal{P} \supseteq \mathcal{S}\} \tag{2.9}$$

for every $\mathcal{S} \subseteq \mathrm{Spec}(k)$, since $V(\mathcal{S}) = V(< \mathcal{S} >)$. (Being $< \mathcal{S} >$ the ideal generated by the set $\mathcal{S}$).

Notice that from Definition [2.8] we have that:

$$V(\mathcal{S}) := \{\mathcal{P} \text{ prime ideal} \in \mathrm{Spec}(k) | \mathcal{P} \supseteq \mathcal{S}\} = \{\mathcal{P} \in \mathrm{Spec}(k) | f(\mathcal{P}) = 0 \text{ for all } f \in \mathcal{S}\} \tag{2.10}$$

Definition 2.10 One can also define a **basis** for the Zariski topology of $\mathrm{Spec}(k)$, declaring what the open sets are:

- a **distinguished open set** of $f \in k$ in $\mathrm{Spec}(k)$ is a set of the form

$$D(f) := \mathrm{Spec}(k) \setminus V(f) = \{\mathcal{P} \in \mathrm{Spec}(k) | f \notin \mathcal{P}\} \tag{2.11}$$

- distinguished opens form a **basis** for the Zariski topology i.e. each open $U \subseteq \mathrm{Spec}(k)$ is of the form:

$$U = \mathrm{Spec}(k) \setminus V(\mathcal{S}) = \mathrm{Spec}(k) \setminus \bigcap_{f \in \mathcal{S}} V(f) = \bigcup_{f \in \mathcal{S}} (\mathrm{Spec}(k) \setminus V(f)) = \bigcup_{f \in \mathcal{S}} D(f) \tag{2.12}$$

Definition 2.11 We can define the **sheaf of regular functions** on $\mathrm{Spec}(k)$, denoted $\mathcal{O}_{\mathrm{Spec}(k)}$, as the sheaf $\mathrm{Op}^{op} \to \mathbf{Rng}$, such that a regular function $\varphi \in \mathcal{O}_{\mathrm{Spec}(k)}(U)$ is given by a family of functions $(\varphi_{\mathcal{P}})_{\mathcal{P} \in U}$, each $\varphi_{\mathcal{P}} = \frac{f}{g}$ being an element of the localization $k_{\mathcal{P}}$. These functions must satisfy the property that, for all primes $\mathcal{P} \in U$ and for all $\mathcal{Q} \in V \subseteq U$ with $\mathcal{P} \in V$ (V open), then there exist f', g' such that:

$$\varphi_{\mathcal{Q}} := \frac{f'}{g'} \in k_{\mathcal{Q}} \tag{2.13}$$

for $f', g' \in k$ s.t. $g'(\mathcal{Q}) \neq 0$. It can be proven that $\mathcal{O}_{\mathrm{Spec}(k)}$ defined in this way is clearly a sheaf: it sufficies to show the gluing properties (of [1.53]) on the functions φ, which are trivially satisfyed thanks to the condition above. The sheaf $\mathcal{O}_{\mathrm{Spec}(k)}$ is called the **structure sheaf** of $\mathrm{Spec}(k)$. For each open U, the set $\mathcal{O}_{\mathrm{Spec}(k)}(U)$ has an obvious ring structure given by pointwise addition and multiplication.

Following Definition [2.8], and since $k_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}} \simeq K(\mathcal{P})$ for each prime $\mathcal{P} \in U$ open, an element $\varphi \in \mathcal{O}_{\mathrm{Spec}(k)}(U)$ can be thought as a function $\varphi : U \to K(\mathcal{P})$, namely the function

such that $\varphi(\mathcal{P}) := \overline{\varphi_{\mathcal{P}}} \in k_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}}$.

Warning! One must be careful that in general, for a ring k with nilpotents, a regular function $\varphi \in \mathcal{O}_{\mathrm{Spec}(k)}(U)$, for U open of $\mathrm{Spec}(k)$, is not completely determined by its values $\varphi(\mathcal{P}) \in k_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}}$. For example, all the regular functions φ of $\mathrm{Spec}(k[X]/(X^2))$ are of the form $\varphi = a + bX$, $(a, b) \in k$; but when computed con the unique prime

$$\mathcal{P} = (X) \in \mathrm{Spec}(k[X]/(X^2)) \tag{2.14}$$

they give $\varphi((X)) = (a + bX) \equiv a \ \mathrm{mod}.(X) \in k(\simeq \frac{k[X]/(X^2)}{(X)/(X^2)})$. For more explicit considerations see [2.20] and the following [W3].

Proposition 2.12 We have that $\mathcal{O}_{\mathrm{Spec}(k)}(\mathrm{Spec}(k)) \simeq k$. Moreover, $\mathrm{Spec}(k)$ endowed with the Zariski topology is a *locally ringed space*.

Proof. We will prove this in the general case of affine k-schemes in Proposition [2.28]. For a detailed proof based on the fact that, for each distinguished open $D(f)$, we have that $\mathcal{O}_{\mathrm{Spec}(k)}(D(f)) \simeq k_f$ (the localization of k at f) see for example [Ga], 12.19. For the second part of the statement, notice that $\mathrm{Spec}(k)$ with the Zariski topology is a topological space and thanks to the previous definitions it can be endowed with a structure sheaf of rings, the sheaf of regular functions $\mathcal{O}_{\mathrm{Spec}(k)}$, becoming a ringed space. Moreover one has that:

$$\mathcal{O}_{\mathrm{Spec}(k),\mathcal{P}} := \varinjlim_{U \ni \mathcal{P}} \mathcal{O}_{\mathrm{Spec}(k)}(U) = k_{\mathcal{P}} \tag{2.15}$$

by definition of regular functions and of local rings. (For a detailed proof see [Ga], ch. 12).

□

Now let us define the central object of this section using the concepts just introduced.

Definition 2.13 Let R be a commutative unital ring. An **affine scheme** X is a **locally ringed space** that is isomorphic to the space $\mathrm{Spec}(R)$, endowed with the Zariski topology. The structure sheaf $\mathcal{O}_{\mathrm{Spec}(k)}$ is the sheaf of regular functions defined in [2.11] (it can be extended to a sheaf of k-algebras as we will point out in [2.17]). A **morphism** between affine schemes $X \to Y$ is a morphism between the underlying locally ringed spaces. Affine schemes together with morphisms between them form a category that we denote with **AffSch**.

Remark 2.14 Notice that $\mathrm{Spec}(k)$ is itself an affine scheme: indeed it is a locally ringed space thanks to Proposition [2.12]. It is the affine scheme associated to the ring k. Observe also that a morphism between affine schemes $\mathrm{Spec}(k) \to \mathrm{Spec}(k')$ corresponds thanks to Definition [2.5] to a morphism between the associated rings of functions, i.e. $\mathcal{O}_{\mathrm{Spec}(k')}(\mathrm{Spec}(k')) \to \mathcal{O}_{\mathrm{Spec}(k)}(\mathrm{Spec}(k))$, and hence it gives a morphisms between the base rings $k' \to k$.

Proposition 2.15 Let X be an affine variety over an algebraically closed field K as before. Then $X := V(\mathcal{S})$ can be thought as an affine scheme $X \simeq \mathrm{Spec(R)}$, where R is the finitely generated k-algebra (i.e. $R \simeq k[X_1, ..., X_n]/\mathcal{I}$ for $\mathcal{I}$ the ideal generated by the set $\mathcal{S}$), which represent the sheaf of *regular functions* (the - also called - coordinate ring $A(X) = R$ of X).

Proof. Let $X := V(\mathcal{S})$ so that $R := A(X) = k[X_1, ..., X_n]/\mathcal{I}$ with $\mathcal{I} =< \mathcal{S} >$ (and $\mathcal{S}$ can be thought as a finite set of polynomials $f_1, ..., f_m$ in $k[X_1, ..., X_n]$; which is the definition of finitely generated algebra). One has a bijection:

$$\{x \in X\} \longleftrightarrow \{\mathcal{M} \in \mathrm{Spec(R)} | \mathcal{M} \text{ is maximal}\} \longleftrightarrow \{k[X_1, ..., X_n] \ni \text{maximal ideals } \supseteq \mathcal{I}\}$$

thanks to the classical Hilbert's Nullstellensaz (for details see for example [Ga], ch. 12). Now $A(X)$ is the quotient of a noetherian ring with a principal ideal domain $\mathcal{I}$ and hence it is artinian, so that each prime is maximal and so $X \simeq \mathrm{Spec(R)}$. Finally $\mathcal{O}_{\mathrm{Spec(R)}}(X) \simeq R = k[X_1, ..., X_n]/\mathcal{I}$.

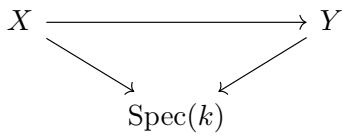
□

As a consequence of this, there is a bijection between **affine varieties** over (an algebraically closed field) k and **reduced affine schemes of finite type** over k that are also **separated** (an affine variety is always separated - see [2.20] and [W3]).

Definition 2.16 A **scheme** X is given by a locally ringed space that has an open covering $(U_i)_i$ of affine schemes, i.e. $U_i \simeq \mathrm{Spec}(R_i)$ for $R_i \in \mathbf{Rng}$. Clearly the structure sheaf of rings $\mathcal{O}_X$ given by Definition [2.1] must satisfy contitions of Remark [2.4] and, in particular, $\mathcal{O}_X(U)$ can be viewed as the **ring of regular functions** on $U \in \mathrm{Op}^{op}$, satisfying the gluing properties previously mentioned. One has the obvious $\mathcal{O}_X(U_i) \simeq R_i$, for each open affine $U_i \simeq \mathrm{Spec}(R_i)$. The schemes form a category that we denote **Sch**, and whose morphisms are the morphisms between schemes, i.e. between the underlying locally ringed spaces.

Using a more functorial point of view, that we are going to develop later, we will see that the (sheaf)-conditions of previous Definition [2.16], mean that a scheme is a presheaf of $\mathrm{Fnct}(\mathbf{Alg_k}, \mathbf{Set})$ that is a sheaf for the Grothendieck-Zariski topology [1.52]. However, since in our definition of locally ringed space we considered the structure sheaf of rings in a very general way, namely as a sheaf of k-algebras $\mathrm{Op}^{op} \to \mathbf{Alg_k}$, instead of a sheaf of rings $\mathrm{Op}^{op} \to \mathbf{Rng}$, we must clarify this difference with the following definition.

Definition 2.17 We define the category of **affine schemes over** k, which is also called the category of affine schemes over the base scheme $S := \mathrm{Spec}(k)$, and we denote it $\mathbf{AffSch}/k$, as the category whose objects are the morphisms $X \to \mathrm{Spec}(k)$, and whose morphisms are the morphisms $X \to Y$ between affine schemes, such that the following diagram commutes:



for all $X \simeq \mathrm{Spec}(R)$, $Y \simeq \mathrm{Spec}(S)$ and R, S commutative unital rings. In an analogous way we can define the category $\mathbf{Sch}/k$ of schemes over k.

Remark 2.18 Notice that, thanks to the above Definition [2.17] and to Remark [2.14], an affine scheme $X \simeq \mathrm{Spec}(R)$ over k gives automatically a ring homomorphism $k \to R$ that turns R into an associative k-algebra (cfr. [2.22]). Hence following Definition [2.1], the structure sheaf $\mathcal{O}_X$ gives, for each open $U \subseteq X$, a morphism $k \to R = \mathcal{O}_X(X) \to \mathcal{O}_X(U)$ that turns $\mathcal{O}_X$ into a sheaf of k-algebras as wanted. The same thing applies to all schemes over k.

We conclude with some useful properties of (affine) schemes. We state a list of properties characterizing the structure morphism of (affine) schemes over k (a commutative unital ring); however, those properties can actually be extended to generic moorphisms between schemes (not over k). Then we give some properties for a generic morphism $X \to Y$ between schemes. We say that a (affine) scheme X over k satisfies one of this properties if the base morphism $X \to \mathrm{Spec}(k)$ satisfies it.

Definition 2.19 A (affine) scheme X over k is said to be:

(i) **finite** if the induced morphism $k \to \mathcal{O}_X(X)$ turns $\mathcal{O}_X(X)$ into a finitely generated k-module;

(ii) **of finite type** if the induced morphism $k \to \mathcal{O}_X(X)$ turns $\mathcal{O}_X(X)$ into a finitely generated k-algebra;

(iii) of **finite presentation** if the induced morphism $k \to \mathcal{O}_X(X)$ turns $\mathcal{O}_X(X)$ into a finitely presented k-algebra.

Definition 2.20 A morphism of schemes $f : X \to Y$ is said to be:

(i) **affine** if $f^{-1}(V)$ is an open affine for each open $V \subseteq Y$;

(ii) **quasi-compact** if $f^{-1}(V)$ is a quasi-compact set for each open quasi-compact $V \subseteq Y$;

(iii) **(faithfully) flat** if for every $U \subseteq X$ and $V \subseteq Y$ such that $f(U) \subseteq V$ then $\mathcal{O}_Y(V)$ is a flat module over $\mathcal{O}_X(U)$ (and f is surjective);

(iv) **flat/locally free/projective/free** if for every $U \subseteq X$ and $V \subseteq Y$ such that $f(U) \subseteq V$ then $\mathcal{O}_Y(V)$ is a flat/locally free/ptojective/free module over $\mathcal{O}_X(U)$;

(v) **a closed immersion** if $f(X)$ is a closed subscheme of Y and the map $\mathcal{O}_Y \to f_*\mathcal{O}_X$, given by $V \mapsto (\mathcal{O}_Y(V) \to f_*\mathcal{O}_X(V) := \mathcal{O}_X(f^{-1}(V)))$ for each open $V \subseteq Y$, is surjective;

(vi) **universally closed** if for every scheme Z (over k) and morphism $g : Z \to Y$, the **pull-back morphism** of f (through g) defined as the morphism $X \times_Y Z \to Z$, is a closed map (for the underlying topological spaces);

(vii) **separated** if considering the diagonal morphism $\Delta : X \to X \times_Y X$, then $\Delta(X)$ is a closed subset of $X \times_Y X$.

Warning! To be more precise, in the modern definition of scheme one should add to Definition [2.17] the fact that a scheme X must be **reduced**, meaning that its associated algebra has no non-zero nilpotent elements; using this definition one call a **pre-scheme** what we defined as a scheme. It can be proven the following statement, i.e. if the affine scheme X is reduced then:

"a regular function is completely determined by its values at each point"

which can be translated into:

"if $f \in \mathcal{O}_X(X)$ is such that $f_{\mathcal{P}} \in \mathcal{M}_{\mathcal{P}} \subseteq \mathcal{O}_{X,\mathcal{P}}(X)$ for each $\mathcal{P} \in X$, then $f \equiv 0$"

and it is certainly true from the fact that the intesection of all prime ideals gives the nilpotent ideal of X which is (0) thanks to the reducedness. (See also [Ga] for details).

2.1.2 The functorial point of view

In this section we give a ctegorical construction of (affine) schemes which actually coincide with the first geometrical definition given in the previous subsection.

Along the whole subsection let k be, as before, a commutative unital ring and consider again the category of k-algebras $\mathbf{Alg_k}$ (suppose we are working with *small categories* as pointed out in [1.2] and [1.3]).

Definition 2.21 A **k-functor** is an element of the presheaves category $\mathrm{Fnct}(\mathbf{Alg_k}, \mathbf{Set})$, i.e. a covariant functor between the category of k-algebras and the category of sets. A k-subfunctor U of X is a k-functor such that $U(R) \subseteq X(R)$ for all k-algebras R; and we write $U \subseteq X$. The (presheaves) category of k-subfunctors admits projective limits.

Definition 2.22 We can define a contravariant functor $\mathrm{Sp}_k : \mathbf{Alg_k}^{op} \to \mathrm{Fnct}(\mathbf{Alg_k}, \mathbf{Set})$ from the category of k-algebras $\mathbf{Alg_k}$ to the category of k-functors in the following way:

- let $A \in \mathbf{Alg_k}^{op}$, then $\mathrm{Sp}_k A := \mathrm{Hom}_{k-alg}(A, -)$, i.e. $\mathrm{Sp}_k A(R) := \mathrm{Hom}_{k-alg}(A, R)$ for each $R \in \mathbf{Alg_k}$. For each $f \in \mathrm{Hom}_{k-alg}(R, S)$, then $\mathrm{Sp}_k A(f) : \mathrm{Hom}_{k-alg}(A, R) \to \mathrm{Hom}_{k-alg}(A, S)$, is such that $\psi \mapsto f \circ \psi$, for each $R, S \in \mathbf{Alg_k}$ and $\psi \in \mathrm{Hom}_{k-alg}(A, R)$;
- let $\varphi : A \to B$ for $A, B \in \mathbf{Alg_k}^{op}$, then $\mathrm{Sp}_k(f) := \mathrm{Sp}_k B(R) \to \mathrm{Sp}_k A(R)$ is given by $\varphi \mapsto \varphi \circ f$, for each $R \in \mathbf{Alg_k}$.

The functor Sp_k commutes with projective limits.

Recall that k-functors defined in this way, i.e. of the form $\mathrm{Hom}_{k-alg}(A, -)$, are called *representable* functors of $\mathrm{Fnct}(\mathbf{Alg_k}, \mathbf{Set})$. (See [1.25]).

We can now introduce the notion of affine scheme using this categorical framework.

Definition 2.23 Let $A \in \mathbf{Alg_k}$, an **affine k-scheme** is a k-functor isomorphic to $\mathrm{Sp}_k A$ i.e. a representable functor of $\mathrm{Fnct}(\mathbf{Alg_k}, \mathbf{Set})$. Affine k-schemes form a category, denoted with $\mathbf{AffSch}/k$, that is a full subcategory of the category of k-functors.

Proposition/Example 2.24 The **affine line**, defined as the k-functor $\mathbb{O}_a(-)$ such that $\mathbb{O}_a(R) = R$ (as a set) for each $R \in \mathbf{Alg_k}$, is an affine k-scheme.

Proof. Clearly $\mathbb{O}_a(R) = R \simeq \mathrm{Hom}_{k-alg}(k[x], R)$ as a set but also as $k[x]$-module, as a k-module and as a ring. As a consequence of this the isomoprhism holds also as a k-algebra morphism. Therefore $\mathbb{O}_a(-) \simeq \mathrm{Sp}_k k[x]$ is a representable functor (and moreover we will see that its ring of functions is given by $\mathcal{O}_X(\mathbb{O}_a) = k[x]$). □

Remark 2.25 Notice that $\mathbb{O}_a(R) = R$ as a set, but we will se later that this is true also considering $\mathbb{O}_a(R) = R = (R, +)$ as an additive group, which will turn the affine line into a *group scheme* i.e. a k-functor of groups for each R. This is why we will use the notation $\mathbb{G}_a$ instead of $\mathbb{O}_a$, meaning the *additive group scheme*.

Proposition 2.26 The functor $A \mapsto \mathrm{Sp}_k A$, for $A \in \mathbf{Alg_k}^{op}$, is fully faithful and essentially surjective, i.e. it induces an antiequivalence of categories between the category of k-algebras and the category of affine k-schemes.

Proof. Let $A \in \mathbf{Alg_k}^{op}$ and let $\mathrm{Sp}_k A$ be the associated affine k-scheme as before. Thanks to the Yoneda embedding (see [1.24] and [1.26]), we have that, for a k-functor $X \in \mathrm{Fnct}(\mathbf{Alg_k}, \mathbf{Set})$:

$$\mathrm{Hom}_{k-fnct}(\mathrm{Sp}_k A, X) \simeq X(A) \tag{2.16}$$

In particular, if $X = \mathrm{Sp}_k B$, for $B \in \mathbf{Alg_k}^{op}$, then we have that:

$$\mathrm{Hom}_{k-fnct}(\mathrm{Sp}_k A, \mathrm{Sp}_k B) \simeq \mathrm{Sp}_k B(A) = \mathrm{Hom}_{k-alg}(B, A) \tag{2.17}$$

The essentially surjective part is obvious and follows from the definition of affine k-scheme.

□

We defined the ring of *regular functions* for affine varieties or for affine schemes in the geometrical constructions of [2.11] and [2.16]. We can give an analogous notion for a generic k-functor X.

Definition 2.27 Let $X \in \mathrm{Fnct}(\mathbf{Alg_k}, \mathbf{Set})$. Consider the set of elements $f : X \to \mathbb{O}_a$, such that for each $R \in \mathbf{Alg_k}$ we get a functorial system of maps $f_R : X(R) \to R$, i.e. we are considering the set of natural transformations f between the two k-functors. We denote this set:

$$\mathcal{O}(X) := \mathrm{Hom}_{k-fnct}(X, \mathbb{O}_a) \tag{2.18}$$

and we call it the set of **regular functions** on X; notice that $\mathcal{O}(X)$ has a natural k-algebra structure given by pointwise addition and multiplication (as in [2.11]). Namely let $f, g \in \mathcal{O}(X)$, for any $R \in \mathbf{Alg_k}, \lambda \in k$ and $x \in X(R)$:

$$(f+g)_R(x) = f_R(x) + g_R(x),\ (f \cdot g)_R(x) = f_R(x) \cdot g_R(x),\ (\lambda f)_R(x) = \lambda \cdot f_R(x) \tag{2.19}$$

Proposition 2.28 Let $A \in \mathbf{Alg_k}^{op}$ and $X = \mathrm{Sp}_k A$ be an affine k-scheme. Then:

$$\mathcal{O}(X) \simeq A \tag{2.20}$$

as k-algebras.

Proof. Indeed we have:

$$\mathcal{O}(X) := \mathrm{Hom}_{k-fnct}(X, \mathbb{O}_a) = \tag{2.21}$$

$$\mathrm{Hom}_{k-fnct}(\mathrm{Sp}_k A, \mathbb{O}_a) = \mathrm{Hom}_{k-fnct}(\mathrm{Hom}_{k-alg}(A, -), \mathbb{O}_a(-)) \simeq \mathbb{O}_a(A) = A \tag{2.22}$$

were the last equality is thanks to Yoneda Lemma [1.26]. □

We can see the equivalence proved in Proposition [2.26] with another perspective:

Proposition 2.29 A k-functor X is an affine k-scheme if and only if the natural morphism given by:

$$\alpha : X \to \mathrm{Sp}_k \mathcal{O}(X) \tag{2.23}$$

$$X(R) \ni \mathbf{x} \mapsto (f_R \mapsto f_R(\mathbf{x}) \in R) \tag{2.24}$$

is an isomorphism.

Proof. Clearly if α is an isomorphism it follows by definition that $X \simeq \mathrm{Sp}_k \mathcal{O}(X)$ is an affine k-scheme. Conversely let $X = \mathrm{Sp}_k A$ for $A \in \mathbf{Alg_k}^{op}$. Then $\mathcal{O}(X) = \mathcal{O}(\mathrm{Sp}_k A) \simeq A$ thanks to eq. (2.20). Hence, since $\mathrm{Hom}_{k-alg}(A, \mathcal{O}(X)) = \mathrm{Hom}_{k-fnct}(\mathrm{Sp}_k \mathcal{O}(X), \mathrm{Sp}_k A)$, α is an isomorphism too. □

Whenever clear from the context we shall always write $\mathcal{O}(X)$ meaning the ring of regular functions on X over X. If we need to precisate the base scheme, we write $\mathcal{O}_X(U)$, meaning, for example, the ring of regular functions on U over X, which is the restriction of the functor $\mathcal{O}(-)$ to a subfunctor U of X.

Definition 2.30 Let X be a k-functor and let $E \subseteq \mathcal{O}(X)$ be a subset of the ring of regular functions on X. We can define two k-subfunctors of X in the following way, functorially in $R \in \mathbf{Alg_k}$:

- $V(E)(R) := \{x \in X(R) | f_R(x) = 0 \text{ for all } f \in E\}$;
- $D(E)(R) := \{x \in X(R) | f_R(x) \text{ generate the unit ideal of } R\}$.

Proposition 2.31 If $\varphi : Y \to X$ is a natural morphism of k-functors, then:

$$F := \{f \circ \varphi | f \in E\} \subseteq \mathcal{O}(Y) \tag{2.25}$$

$$\varphi^{-1}(V(E)) = V(F) \tag{2.26}$$

$$\varphi^{-1}(D(E)) = D(F) \tag{2.27}$$

Moreover, if X is affine:

- $V(E)$ is an affine k-scheme with $\mathcal{O}(V(E)) = \mathcal{O}(X)/E\mathcal{O}(X)$;
- if $E := \{f\}$, then $D(E)$ is an affine k-scheme with $\mathcal{O}(D(\{f\})) = \mathcal{O}(X)[f^{-1}] \simeq \mathcal{O}(X)[t]/(tf - 1)$.

Proof. The proof follows from the definitions, for details see for example [De], I, 3. □

Definition 2.32 A k-subfunctor U of X is said to be **closed (resp. open)** if for every k-functors morphism $\varphi : T \to X$, with T an affine k-scheme, then $\varphi^{-1}(U)$ is of the form $V(E)$ (resp. $D(E)$), for $E \subseteq \mathcal{O}(X)$.

Definition 2.33 A k-functor X is said to be a k-scheme if it satisfies the following two properties:

(i) for any k-algebra R and any family of elements $(f_i)_{i \in I} \in R$ such that $\sum_{i \in I} f_i R = R$, given the elements $x_i \in X(R[f_i^{-1}])$, such that for every $i, j \in I$ the images of x_i and x_j coincides in $X(R[f_i^{-1}, f_j^{-1}])$, then there exist a unique $x \in X(R)$ which is mapped to x_i thanks to the morphism $R \to R[f_i^{-1}]$, for each $i \in I$;

(ii) there exist a family $(U_i)_{i \in I}$ of open k-subfunctors of X such that each U_i is affine and $X(K) = \bigcup_{i \in I} U_i(K)$, for any field K.

Notice that the k-schemes as just defined form the category $\mathbf{Sch}/k$ whose morphisms are morphisms between k-schemes as k-functors. Moreover if we endow this category with a Grothendieck topology (Definition [1.49]) then the above conditions a k-functor must satisfy in order to be a k-scheme, are exactly the conditions that turn it into a sheaf (see [1.53]).

Proposition 2.34 Any open or closed k-subfunctor of a k-scheme is a k-scheme too. Moreover, a finite projective limit of a k-scheme is again a k-scheme. A closed k-subfunctor of an affine k-scheme is again an affine k-scheme.

Finally we state a result which gives an equivalence between the two different approaches developed in the previous subsections and allows us to translate the geometrical approach into the functorial one and viceversa. For a proof of this and of the previous proposition see for example some references that can be found in [De], I, 3.

Theorem 2.35 There exists a morphism that induces an equivalence between the category of k-schemes and the category of topological locally ringed spaces that are schemes over k in the sense of Definition [2.17], i.e. they are locally isomorphic to $\mathrm{Spec}(R)$ for a k-algebra R.

Proof. Just to give an idea of the proof, the equivalence of the statement is given by the morphism:

$$X \to |X| \tag{2.28}$$

where $|X|$ denotes the underlying topological space of X given by considering, as points, the equivalence classes of elements $x \in X(K)$, for K running through all the possible k-fields, where $x' \in X(K')$ is such that $x \sim x'$ if and only if there exist a field L and morphisms $K \to L$, $K' \to L$ such that the image of x and x' in $X(L)$ coincides. The topology of $|X|$ is given by letting all the opens to be of the form $|U|$ for all the open subfunctors U of X. The sheaf $\mathcal{O}(-) \in \mathrm{Fnct}(\mathrm{Op}^{op}, \mathbf{Rng})$ is given by $|U| \mapsto \mathcal{O}_X(U)$, using the ring of regular functions defined on the k-functor X. □

Remark 2.36 Finally notice that Proposition [2.29] is still true for the affine k-subfunctors of a k-scheme X, i.e. it gives an isomorphism $U \simeq \mathrm{Sp}_k\mathcal{O}_X(U)$, whenever U is a generic affine k-subscheme of X.

2.1.3 Formal Schemes

Before we introduce the notion of k-formal functor so that we can proceed by stating the main definitions and results for this section, we recall some basic notions abut *topological rings*.

Definition 2.37 Let k be a commutative ring with unity that is also a **topological** ring, we recall that:

(i) k is said to be **linearly topologised** if there exists a basis of neighbourhood of 0 consisting of ideals (and hence opens);

(ii) the ring $\hat{k} := \varprojlim_{\mathcal{I} \in \Omega_k} (k/\mathcal{I})$, where Ω_k is the set of open ideals of k and each quotient is equipped with the discrete topology, is the **completion** of k (it is of course linearly topologised);

(iii) a topologic k-module R (for k linearly topologised) is said to be **linearly topologised** if there exists a basis of neighbourhood of 0 consisting of submodules (and hence opens);

(iv) the module $\hat{R} := \varprojlim_{S \in \Lambda_R} (R/S)$, where Λ_R is the set of open submodules of R and each quotient is equipped with the discrete topology, is the **completion** of R (it is of course linearly topologised);

(v) a linearly topologised ring k, that is separated and complete, is said to be **pseudo-compact** if $k/\mathcal{I}$ is artinian for each $\mathcal{I} \in \Omega_k$;

(vi) for a pseudo-compact ring k, a linearly topologised separated and complete k-module R, is said to be **pro-artinian** if R/S is artinian for each $S \in \Lambda_R$;

(vii) for a pseudo-compact ring k, a linearly topologised separated and complete k-module R, is said to be **profinite** if R/S is of finite length for each $S \in \Lambda_R$;

(viii) for a pseudo-compact ring k, a linearly topologised separated and complete k-module R, is said to be **finite** if it is profinite and of finite length;

(ix) a k-algebra R is linearly topologised/pro-artinian/profinite/finite, if it is linearly topologised/pro-artinian/profinite/finite as a k-module.

Definition 2.38 We define:

(i) AM_k the category of pro-artinian k-algebras with morphisms the continuous homomorphisms of k-algebras;

(ii) PM_k the full subcategory of AM_k consisting of profinite k-algebras.

(iii) FM_k the full subcategory of PM_k consisting of finite k-algebras.

We recall, without proving it, that the category AM_k (and hence PM_k) of pro-artinian k-algebras is *abelian*, and hence there exists the projective limit of a filtrant system $(R_j)_j$ of pro-artinian k-modules and it is again a pro-artinian k-module. (See [Fo] for details).

Starting from now, and for the whole section, let k be a commutative unital pseudo-compact ring.

Definition 2.39 A k-**formal functor** $\hat{X}$ is a functor:

$$\hat{X} : FM_k \to \mathbf{Set} \tag{2.29}$$

from the category of finite k-algebras to the category of sets. We denote with $\mathrm{Fnct}(FM_k, \mathbf{Set})$ the category of such functors.

Proposition 2.40 A k-formal functor F, defined as above, can be extended to the category of profinite k-algebras:

$$\hat{X} : PM_k \to \mathbf{Set} \tag{2.30}$$

and moreover it commutes with filtrant projective limits.

Proof. Let R be a profinite k-algebra then we set:

$$\hat{X}(R) = \varprojlim_{\mathcal{I}\in\Omega_R} \hat{X}(R/\mathcal{I}) \tag{2.31}$$

For the second part we give an idea of the proof (that can be found for example in [Fo]). Let $(R_i)_{i\in I}$ be a firltrant projective systems of finite k-algebras and let $i \leq j \in I$. Consider the respective maps $f_{ij} : R_j \to R_i$; let $R'_i := \bigcap_{j\geq i} f_{ij}(R_j)$ then, since the R_j's are finite k-algebras, there exist j_i s.t. $R'_i = f_{ij_i}(R_{j_i})$. But then this mean that we can replace R_i with R'_i and this does not change the computation of the projective limit $\varprojlim \hat{X}(R_i) = \varprojlim \hat{X}(R'_i)$. As a consequence we can suppose that the f_{ij}'s are all surjective and therefore we obtain a surjective map $R = \varprojlim R_i \to R'_i$ as well. Hence the ideals $\mathcal{I}_i \simeq R/R'_i$ form a set which is cofinal [1] with respect to the set of all ideals of R, and we conclude that:

$$\hat{X}(R) = \varprojlim_{\mathcal{I}\in\Omega_R} \hat{X}(R/\mathcal{I}) = \varprojlim_{i} \hat{X}(R'_i) \tag{2.32}$$

□

From now on a k-formal functor can be considered as a functor from the category of profinite k-algebras to that of sets, such that it commutes with filtrant projective limits.

Definition 2.41 Let $A \in PM_k$ be a profinite k-algebra, we define a contravariant k-formal functor $\mathrm{Spf}_k : PM_k^{op} \to \mathrm{Fnct}(FM_k, \mathbf{Set})$, such that $A \mapsto \mathrm{Spf}_k A$, which satisfies:

- $\mathrm{Spf}_k A(R) := \mathrm{Hom}_{k-alg,cont.}(A, R)$, for all finite k-algebras R (where for "Hom" we mean moprhisms of profinite k-algebras, i.e. continuous homomorphisms);
- $\mathrm{Spf}_k(\varphi) : \mathrm{Hom}_{k-alg,cont.}(A, R) \to \mathrm{Hom}_{k-alg,cont.}(A, S)$ is such that $\psi \mapsto \varphi \circ \psi$ for all $R, S \in FM_k$, $\varphi : R \to S$.
- for each $B \in FM_k$, then we have:

  $$\mathrm{Hom}_{k-f.fct}(\mathrm{Spf}_k B, \mathrm{Spf}_k A) \simeq \mathrm{Spf}_k A(B) \simeq \mathrm{Hom}_{k-alg,cont.}(A, B) \tag{2.33}$$

  thanks to the Yoneda Lemma.

Proposition 2.42 The k-formal functor $\mathrm{Spf}_k A$, if $A \in FM_k^{op}$ is **finite**, is nothing but a *representable* functor of $\mathrm{Fnct}(FM_k, \mathbf{Set})$, moreover it can be extended also as a functor belonging to $\mathrm{Fnct}(PM_k, \mathbf{Set})$. For $R \in PM_k$ we have that:

$$\mathrm{Spf}_k A(R) = \mathrm{Hom}_{k-alg,cont.}(A, R) = \tag{2.34}$$

$$= \mathrm{Hom}_{k-alg,cont.}(A, \varprojlim_{\mathcal{A}\in\Omega_R} R/\mathcal{A}) = \varprojlim_{\mathcal{A}\in\Omega_R} \mathrm{Hom}_{k-alg,cont.}(A, R/\mathcal{A}) \tag{2.35}$$

[1] For A, B ordered sets, $A \subseteq B$ is cofinal if for every $b \in B$ there exist $a \in A$ s.t. $b \leq a$.

If $A \in PM_k^{op}$ is profinite, then $\mathrm{Spf}_k A$ is the **inductive limit** of *representables* functors of $\mathrm{Fnct}(FM_k, \mathbf{Set})$, as shown by the following:

Proposition 2.43 Let R be a finite k-algebra. Notice that if $(A_i)_i$ is the family of (discrete) quotiens of A defining its topology (i.e. each $A_i = A/\mathcal{A}_i$ is a finite k-algebra for a $\mathcal{A}_i \in \Omega_A$, and $A = \varprojlim A_i$), then:

$$\mathrm{Spf}_k A(R) := \mathrm{Hom}_{k-alg,cont.}(A, R) = \mathrm{Hom}_{k-alg,cont.}(\varprojlim_i A_i, R) = \tag{2.36}$$

$$= \varinjlim_i \mathrm{Hom}_{k-alg,cont.}(A_i, R) \tag{2.37}$$

where R can be considered also as a profinite k-algebra.

Proof. The proof of the above propositions is trivially contained in the statement and using the properties of limits and colimits. Namely equations (2.34) and (2.36). □

Remark 2.44 What we have just proven is still true whenever $A = \varprojlim A'_i$, for $(A'_i)_i$ is a filtrant projective sistem of finite k-algebra, and in order to show this it is sufficient to reply the construction of Proposition [2.43] above. However, it is not true in general that if R is *profinite* (but not finite) then $\mathrm{Spf}_k A(R)$ is equal to $\varinjlim_i \mathrm{Spf}_k A_i(R)$, for a generic $A = \varprojlim_i A_i$. The reason of $\mathrm{Spf}_k A(R) = \varinjlim_i \varprojlim_{\mathcal{A} \in \Omega_R} (A_i, R/\mathcal{A})$, is that inductive limits of *filtrant systems* commutes with finite projective limits.

Definition 2.45 (Formal k-scheme) A k-formal functor $\hat{X} : PM_k \to \mathbf{Set}$ is called **formal k-scheme** if there exists a profinite k-algebra A such that $\hat{X} \simeq \mathrm{Spf}_k A$. The category of k-formal schemes adimts finite projective limits and has infinite direct sums $\coprod_i \mathrm{Spf}_k A_i \simeq \mathrm{Spf}_k \prod_i A_i$. (See also [De], I, 7).

Remark 2.46 Thanks to Propositions [2.42] and [2.43], to be a formal k-scheme is equivalent to be the filtrant inductive limit of representable k-formal functors.

Theorem 2.47 The functor $A \mapsto \mathrm{Spf}_k A$, for $A \in PM_k^{op}$, is **fully faithful** (and essentially surjective by definition), i.e. it induces an antiequivalence of categories between the csategory of profinite k-algebras and the category of formal k-schemes.

Proof. Thanks to Yoneda, for each k-formal functor $\hat{X}$ we have:

$$\mathrm{Hom}_{k-f.fnct}(\mathrm{Sp}_k A, \hat{X}) \simeq \varprojlim_i \hat{X}(A_i) \tag{2.38}$$

In particular, if $\hat{X} = \mathrm{Spf}_k B$, for $B \in PM_k^{op}$, then we have that:

$$\mathrm{Hom}_{k-f.fnct}(\mathrm{Spf}_k A, \mathrm{Spf}_k B) \simeq \varprojlim_i \mathrm{Spf}_k B(A_i) = \tag{2.39}$$

$$= \varprojlim_i \mathrm{Hom}_{k-alg,cont}(B, A_i) = \mathrm{Hom}_{k-alg,cont}(B, A) \tag{2.40}$$

□

Proposition 2.48 Let X be a k-functor, then it induces a k-formal functor $\hat{X}$ called the **completion** of X:

Proof. From the inclusion of finite (resp. profinite) k-aslgebras $FM_k \hookrightarrow \mathbf{Alg_k}$ (resp. $PM_k \hookrightarrow \mathbf{Alg_k}$) we get: $\hat{X}(R) := X(R)$ for each $R \in FM_k$ (resp. PM_k).

□

Example 2.49 The formal completion of the **affine line** $\mathbb{O}_a(-)$ is $\widehat{\mathbb{O}_a}$ s.t. $\widehat{\mathbb{O}_a}(R) = R$ for each $R \in PM_k$.

As we did for the k-functors we shall define an *affine algebra* associated to a k-formal functor $\hat{X}$.

Definition 2.50 Let $\hat{X} \in \mathrm{Fnct}(PM_k, \mathbf{Set})$. We denote by $\mathcal{O}^f(\hat{X})$ the set of elements $f : \hat{X} \to \widehat{\mathbb{O}}_a$. Meaning the set of all morphisms $f_R : \hat{X}(R) \to R$, functorially in R for all $R \in PM_k$. The k-algebra structure is given again by pointwise addition and multiplication (as in [2.27]). The topology on $\mathcal{O}^f(\hat{X})$ is the greatest topology such that each

$$\varphi_{x,R} : \mathcal{O}^f(\hat{X}) \to R \tag{2.41}$$

given by $\varphi_{x,R}(f) = f_R(x)$ (for each $x \in \hat{X}(R)$) is a continuous map.

Proposition 2.51 The ring $\mathcal{O}^f(\hat{X})$, defined above, is a profinite k-algebra.

Proof. With the topology given by Definition [2.50], $\mathcal{O}^f(\hat{X})$ is clearly a linearly topologised ring with open ideals given by arbitrary unions of finite intersections of $\ker \varphi_{x,R}$ (which is a system of neighbourhoods of 0); hence each quotient $\mathcal{O}^f(\hat{X})/\ker \varphi_{x,R}$ is a finite k-algebra, so that $\mathcal{O}^f(\hat{X})$ is a (completed separated) profinite k-algebra. □

Proposition 2.52 Let $\hat{X} = \mathrm{Spf}_k A$, for $A \in PM_k^{op}$, be a formal k-scheme. Then:

$$\mathcal{O}^f(\hat{X}) \simeq A \tag{2.42}$$

as k-algebras.

Proof. Indeed we have:

$$\mathcal{O}^f(\hat{X}) := \mathrm{Hom}_{k-f.fnct}(\hat{X}, \widehat{\mathbb{O}_a}) = \tag{2.43}$$

$$\mathrm{Hom}_{k-f.fnct}(\mathrm{Spf}_k A, \widehat{\mathbb{O}_a}) = \varprojlim_i \widehat{\mathbb{O}_a(A_i)} = \varprojlim_i A_i = A \tag{2.44}$$

were the third equality is given thanks to Yoneda Lemma. □

Proposition 2.53 The k-functor $\hat{X}$ is a formal k-scheme if and only if the *canonical morphism* given by

$$\hat{\alpha} : \hat{X} \to \mathrm{Spf}_k \mathcal{O}^f(\hat{X}) \tag{2.45}$$

is an *isomorphism.*

Proof. One can repeat the proof we did for affine k-schemes (see [2.29]) using the result from previous Proposition [2.52]. □

Notice that, if X is an affine k-scheme, then we can consider the quotient $A/\mathcal{A}$, for A the affine algebra associated to X, and $\mathcal{A}$ the ideals of A such that each quotient $A/\mathcal{A}$ endowed with the discrete topology is a finite k-algebra. Then $\mathcal{O}^f(\hat{X}) = \hat{A} := \varprojlim A/\mathcal{A}$. We call $\hat{A}$ the profinite completion of $A \in \mathbf{Alg_k}$.

Definition 2.54 We say that a formal k-scheme $\hat{X}$ is a **finite** k-scheme, if its associated algebra is a finite k-algebra. (I.e. if $\hat{X}$ is *representable* as presheaf of finite k-algebras, [2.42]).

We conclude the section stating another important characterization.

Proposition 2.55 A k-formal functor $\hat{X}$ is a formal k-scheme if and only if it is left exact.

Proof. Clearly $\hat{X} = \mathrm{Spf}_k A$ for $A \in PM_k^{op}$ commutes with finite ptojective limits. For a complete proof of the converse see ([De], II.6). □

2.2 Group schemes and formal group schemes

In this section we use the notions of Höpf algebras, of (affine) scheme and of formal scheme previously introduced, in order to give a definition of (affine) group scheme and formal group scheme. After that, we proceed with some characterizations of those objects.

2.2.1 Affine group schemes

Recall that for an **abstract** group we mean a set G together with an associative group law

$$(-)\cdot(-) : G \times G \to G \tag{2.46}$$

an element 1_G (the identity of G, such that $g \cdot 1_G = 1_G \cdot g = g$ for all $g \in G$), and an inverse map $i : G \to G$ (such that $i(g) \cdot g = g \cdot i(g) = 1_G$ for all $g \in G$).

Definition 2.56 (Affine k-group scheme) Let, as always, k be a commutative unital ring. Let $G = \mathrm{Sp}_k A$ be an affine k-scheme, then G is called **affine k-group scheme** or simply **affine k-group**, if it can be viewed as a k-functor :

$$G : \mathbf{Alg_k} \to \mathbf{Gps} \tag{2.47}$$

such that $G(R)$ is a (abstract) group for each $R \in \mathbf{Alg_k}$. Moreover G is said to be **commutative** if $G(R)$ is an abelian group for each R, i.e.

$$G : \mathbf{Alg_k} \to \mathbf{AbGps} \tag{2.48}$$

Notice that the definition above means that: to give an affine k-group G is nothing but to give a representable k-functor that factors through the forgethful functor for:

$$\mathbf{Alg_k} \xrightarrow{G} \mathbf{Gps} \xrightarrow{for} \mathbf{Set} \tag{2.49}$$

and hence such that $for \circ G$ is the corresponding underlying affine k-scheme. This leads to the following alternative and equivalent definition.

Definition 2.57 (Alternative definition)

- A **k-functor of groups** is a group object in the presheaves category of k-functors $\mathrm{Fnct}(\mathbf{Alg_k}, \mathbf{Set})$;
- an **affine k-group scheme** is a k-functor of groups whose underlying k-fnctor is representable (i.e. it is an affine k-scheme);
- k-functors of groups form a category, the category $\mathrm{Fnct}(\mathbf{Alg_k}, \mathbf{Gps})$, whose morphisms are k-functor morphisms $\varphi : G \to H$, such that $G(R) \to H(R)$ is a group homomorphism for each R, functorially in R. It is a full sub-category of the (presheaves) category of k-functors.

Proposition 2.58 The two definitions given above are equivalent.

Proof. A k-functor of groups (i.e. a group object in $\mathrm{Fnct}(\mathbf{Alg_k}, \mathbf{Set})$) is a (covariant) functor between the category of k-algebras and the category of groups, i.e. a k-functor that factors as in the first definition. Indeed to give a group object $G \in \mathrm{Fnct}(\mathbf{Alg_k}, \mathbf{Set})$ means to give morphisms of k-functors: $m : G \times G \to G$, $e : \mathrm{Sp}_k k \to G$ and $i : G \to G$ (as in Definition [1.77]) such that the diagrams of equations (1.82) and (1.83) commute. This

means that there exist, functorially in R, for each $R \in \mathbf{Alg_k}$, group homomorphisms:

$$m_R : G(R) \times G(R) \to G(R) \tag{2.50}$$

$$e_R : \{1\} \to G(R) \tag{2.51}$$

$$i_R : G(R) \to G(R) \tag{2.52}$$

that turn each $G(R)$ into a (abstract) group; the k-functor of group is commutative if $G(R)$ is an abelian group for each R. (As observed in the next proposition $\mathrm{Sp}_k k$ is a *terminal object* in the category of k-functors). □

Proposition 2.59 Let $G = \mathrm{Sp}_k A$ be an affine k-scheme, then the following are equivalent:

(i) G is a (commutative) affine k-group;

(ii) G is a (commutative) group object in the category of affine k-schemes **AffSch**/k;

(iii) (A, Δ, ε) is a (commutative) Höpf algebra with antipodism.

Proof. (i) ⇔ (ii): G is a (commutative) affine k-group if and only if $G(R)$ is a (abelian, abstract) group for each $R \in \mathbf{Alg_k}$. Then let $m_R : G(R) \times G(R) \to G(R)$, $e_R : \{1\} \to G(R)$ and $i_R : G(R) \to G(R)$ be respectively the multiplication, the identity and the inverse maps (defining the group laws) on $G(R)$ for each R (namely, we are considering each *abstract group* as a group object in the category **Set** of sets, so that m_R is the binary operation of $G(R)$, e_R maps a singleton to the identity 1_G and i_R maps each element to its inverse). From those maps clearly arise three maps $m : G \times G \to G$, $e : \mathrm{Sp}_k k \to G$ and $i : G \to G$ functorially in R which gives to G a group-object structure in **AffSch**/k. Conversely starting from the three maps defining a group object in **AffSch**/k, we get the correspondent group laws on each $G(R)$ (functorially in R) thanks to the commutativity, once again, of Diagrams (1.82), (1.83) given in the definition of group object. Observe that $\mathrm{Sp}_k k(R) := \{1\}$ since there exist only one ring homomorphism $k \to R$ the one defining the k-algebra R, hence $\mathrm{Sp}_k k$ is the terminal object of **AffSch**/k (and $\{1\}$, i.e. a point, is the terminal object of **Set**).

(ii) ⇔ (iii): let $G = \mathrm{Sp}_k A$. Clearly, using that $A \simeq \mathcal{O}(G)$, then G is a (commutative) group object in **AffSch**/k if and only if the map $\Delta : A \to A \otimes A$, that corresponds, thanks to Yoneda Lemma, to the multiplication $m : \mathrm{Sp}_k A \times \mathrm{Sp}_k A \to \mathrm{Sp}_k A$, is a (co-commutative) co-multiplication, endowing A with k-bi-algebra structure, with co-identity ($\epsilon : A \to k$) and inversion ($\sigma : A \to A$). Indeed:

$$\mathrm{Sp}_k A \times \mathrm{Sp}_k A = \mathrm{Hom}(A, -) \times \mathrm{Hom}(A, -) \simeq \mathrm{Hom}(A \otimes A, -) \tag{2.53}$$

and using that $A \otimes A$, as k-algebra is the coproduct of A and itself, but then:

$$\mathrm{Hom}(\mathrm{Sp}_k A \times \mathrm{Sp}_k A, \mathrm{Sp}_k A) \simeq \mathrm{Hom}(A, A \otimes A) \tag{2.54}$$

and analogously for the inversion and the co-identity. Therefore the Diagrams (1.82) and (1.83) that make G a group object of **AffSch**/k commute if and only if the diagrams of Definition [1.66] (of co-algebra) and [1.72] (of antipode) commute, and clearly G is commutative (i.e. the map m commutes after transposing $m(x,y) = m(y,x)$) if and only if A is co-commutative, i.e. diagram of Definition [1.76] commutes. □

The theorem is still true when dealing with a generic k-group scheme G, with associated k-algebra $\mathcal{O}(G)$, with the difference that it corresponds to a group object in the category of k-schemes $\mathbf{Sch}/k$. (We will discuss some details in Chapter 4, dealing with elliptic curves).

Corollary 2.60 We observe some important properties of affine k-groups:

(i) writing $\mathcal{O}(G)$, we mean the affine algebra associated to the affine k-scheme G as in the definitions given in the previous section. Being $A \simeq \mathcal{O}(G)$ with $G = \mathrm{Sp}_k A$, then $\Delta : \mathcal{O}(G) \to \mathcal{O}(G) \otimes \mathcal{O}(G)$ is such that if we consider the maps $x, y : \mathcal{O}(G) \to R$, then (from the properties of tensor products and thanks to the previous propositions):

$$\mathcal{O}(G) \xrightarrow{\Delta} \mathcal{O}(G) \otimes \mathcal{O}(G) \xrightarrow{x \otimes y} R \otimes R \xrightarrow{(-)\cdot(-)} R \tag{2.55}$$

where the last arrow is the multiplication of the ring R; and $\mathcal{O}(G) \otimes \mathcal{O}(G)$ is the associated affine algebra of $G \times G$;

(ii) the category of k-functors of groups admits (finite) projective limits.

Corollary 2.61 There is an antiequivalence between the category **Höpf**, of Höpf algebras, and the category of affine k-group schemes, given by the functor $A \mapsto G := \mathrm{Sp}_k A$. A *quasi-inverse* for this functor is given by the functor $G \mapsto \mathcal{O}(G)$.

Corollary 2.62 An affine k-group can be viewed as a *group object* also in the category $\mathbf{Alg_k}^{op}$. (See [1.78]).

Lemma 2.63 Let G be an affine k-group, i.e. $G = \mathrm{Sp}_k A$ for a Höpf algebra A, then for each k-functor of groups H, a homomorphism of k-functor of groups f is an element $f \in \mathrm{Hom}_{k-gp.fnct}(G, H) \simeq H(A)$ (thanks to Yoneda Lemma), and such that:

$$H(\Delta) : H(A) \to H(A \otimes A) \tag{2.56}$$

$$f \mapsto m_H(H(i_1)(f), H(i_2)(f)) \tag{2.57}$$

where $m_H : H \times H \to H$ is the multiplication law given on H and $i_1, i_2 : A \to A \otimes A$ are such that $i_1(f) = f \otimes 1$ and $i_2(f) = 1 \otimes f$.

Proof. The proof follows easily from the characterization of the co-algebra structure morphisms, for details see for example [De], II.3. □

Theorem 2.64 The category of all *commutative* affine k-groups is abelian.

Proof. For a proof see [De], II.6. □

2.2.2 Examples

Before we proceed with our discussion about k-groups and k-formal groups, we give some classical and useful examples of affine k-groups.

Example 2.65

(1) The **additive group** $\mathbb{G}_a$ is defined by $\mathbb{G}_a(R) := (R, +)$, i.e. it is the identity of R viewed as an additive group. As previously seen in [2.24] and [2.25], the associated algebra of $\mathbb{G}_a$ is given by $\mathcal{O}(\mathbb{G}_a) \simeq k[X]$, with k-co-algebra structure morphisms given by $\Delta : X \mapsto X \otimes 1 + 1 \otimes X$, $\epsilon : X \mapsto -X$ and $i : X \mapsto 0_R$.

(2) The **multiplicative group** $\mathbb{G}_m$ is defined by $\mathbb{G}_m(R) := R^\times$, i.e. it is the group of invertible elements of R, hence the affine algebra associated to $\mathbb{G}_m$ is given by $k[X, X^{-1}]$, with k-co-algebra structure morphisms given by $\Delta : X \mapsto X \otimes X$, $\epsilon : X \mapsto X^{-1}$ and $i : X \mapsto 1_R$.

(3) Consider an integer $n \geq 1$ and the k-group scheme morphism $[n] : \mathbb{G}_m \to \mathbb{G}_m$ given by $\mathbb{G}_m(R) \ni x \mapsto x^n \in \mathbb{G}_m(R)$, for each k-algebra R. Then the kernel:

$$\mu_n(R) := \ker([n])(R) = \{x \in \mathbb{G}_m(R) | x^n = 1_R\} \tag{2.58}$$

defines a k-group scheme with associated algebra:

$$\mathcal{O}(\mu_n) \simeq k[X]/(X^n - 1) \tag{2.59}$$

2.2.3 Connected and étales k-groups

In this subsection we briefly sum up the definitions of *connected* and *étales* k-group schemes and we give (without proving it) a standard decomposition for a k-group scheme G into connected and étales components.

Definition 2.66 We define the following objects:

(i) given a set E, let k be a field, then the **constant scheme** E_k is given by the direct sum (in the category of k-schemes):

$$E_k := (\mathrm{Sp}_k k)^{(E)} \tag{2.60}$$

A k-scheme X is constant if it is isomorphic to the scheme E_k. If E is finite, then E_k is affine with associated k-algebra $\mathcal{O}(E_k) = k^E$. A **formal constant** k-scheme is a scheme isomorphic to the completion of E_k i.e.

$$\widehat{E_k} := (\mathrm{Spf}_k k)^{(E)} \simeq \mathrm{Spf}_k k^E \tag{2.61}$$

where k^E is endowed with the discrete topology.

(ii) We define an **étale k-scheme (resp. formal étale k-scheme**) to be a k-scheme X such that:

$$X \otimes_k \overline{k}, \text{ resp. } \widehat{X} \otimes_k \overline{k} \tag{2.62}$$

is constant or equivalently

$$X \otimes_k k_s, \text{ resp. } \widehat{X} \otimes_k k_s \tag{2.63}$$

is constant, where $\overline{k}$ (resp. k_s) is an algebraic closure (resp. separable closure) of k.

(iii) let $\pi := \mathcal{G}(k_s/k)$ be the Galois group of k_s/k (k_s separable closure of k), then a π-set is given by the set $X(k_s)$ on which π, endowed with the profinite topology, acts continuously;

(iv) from Proposition ([2.67], *(iv)*) below, it follows that if E is a group, then E_k is the **constant k-group scheme**.

We sum up some properties of constant and étale (formal) k-schemes.

Proposition 2.67 Let k be a field and k_s its separable closure. Then:

(i) for a k-scheme X, there are canonical bijections:

$$\mathrm{Hom}_{k-fnct}(E_k, X) \simeq (\mathrm{Hom}_{k-fnct}(\mathrm{Sp}_k k, X))^E \simeq X(k)^E \simeq \mathrm{Hom}_{set}(E, X(k)) \tag{2.64}$$

hence the functor $E \mapsto E_k$ is the right adjoint to the functor $X \mapsto X(k)$ and therefore it commutes with projective limits;

(ii) if $\pi := \mathcal{G}(k_s/k)$ is the Galois group of k_s/k, then there is an equivalence between the category of étale k-schemes and the category of π-sets, induced by the action of the group π on $X(k_s)$, where π is endowed with the profinite topology;

(iii) there is an equivalence between the category of constant (resp. étale) k-schemes and the category of constant (resp. étale) formal k-schemes;

(iv) the functor $E \mapsto E_k$ (from the category of sets to the category of constant k-schemes) commutes with products and with 0-objects;

(v) the functor $X \mapsto X(k_s)$ induces an equivalence between the category of étale (commutative) k-group schemes and the category of (commutative) π-groups, where π is the Galois group of k_s/k, as above, and the π-groups are nothing but the π-sets that are also groups (notice that the product of two étale k-schemes is again an étale k-scheme thanks to the definition of étale scheme);

(vi) for each (affine) k-group scheme there exists a canonical decomposition, i.e. there exist two (affine) k-group scheme G^0 and $G_{\acute{e}t}$, such that G^0 is the connected component of G, $G_{\acute{e}t}$ is an étale k-group given by $G_{\acute{e}t} = G(\bar{k})$ for an algebraic closure $\bar{k}$ of

k, and the following sequence:

$$0 \to G^0 \to G \to G_{\acute{e}t} \to 0 \tag{2.65}$$

is exact, i.e. $G_{\acute{e}t} \simeq G/G^0$.

For a detailed proof see [De], I.8; II. 2. □

2.2.4 formal k-groups and Cartiér dual

Let k be a *pseudo-compact* commutative unital (topological) ring.

Definition 2.68

- A (commutative) k-**formal functor of groups** is a (commutative) group object in the category of k-formal functors, hence a (commutative) object $\widehat{G} \in \mathrm{Fnct}(PM_k, \mathbf{Set})$. This mean that, following the constructions of the previous sections, a (commutative) k-formal functor of groups can be seen as a covariant functor:

$$\widehat{G} : FM_k \to (\mathbf{Ab})\mathbf{Gps} \tag{2.66}$$

or extended as a functor:

$$\widehat{G} : PM_k \to (\mathbf{Ab})\mathbf{Gps} \tag{2.67}$$

that commutes with filtrant projective limits.

- A **formal k-group scheme**, or simply **formal k-group**, or again **formal group (scheme)** over k, is a k-formal functor of groups such that the underlying k-formal functor is a formal k-scheme, i.e. $\widehat{G} = \mathrm{Spf}_k A$, for $A \in PM_k^{op}$;

- given two profinite k-algebras $R, S \in PM_k$, then $R\widehat{\otimes}S$ is the separated completion of the topological ring $R \otimes S$, meaning that:

$$R\widehat{\otimes}S = \varprojlim (S/\mathcal{S} \otimes_{k/\mathcal{A}} R/\mathcal{R}) \tag{2.68}$$

where $\mathcal{A} \in \Omega_k$, $\mathcal{S} \in \Omega_S$ and $\mathcal{R} \in \Omega_R$.

- A (co-commutative) **formal bi-algebra** over k is given by a profinite k-algebra $A \in PM_k$ and a profinite k-algebras morphism $\widehat{\Delta} : A \to A\widehat{\otimes}A$ that makes the diagrams below commutative:

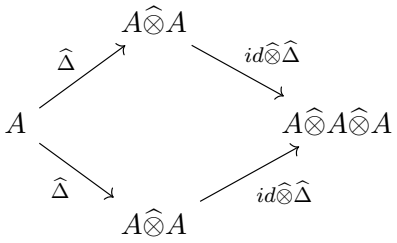


Figure 2.1: co-associativity

$$A \xrightarrow{\widehat{\Delta}} A\widehat{\otimes}A \xrightarrow{\epsilon\widehat{\otimes}id} k\widehat{\otimes}A \simeq A$$
$$A \xrightarrow{\widehat{\Delta}} A\widehat{\otimes}A \xrightarrow{id\widehat{\otimes}\epsilon} A\widehat{\otimes}k \simeq A$$

Figure 2.2: co-identity

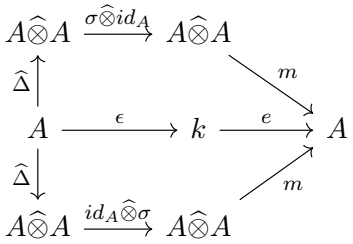
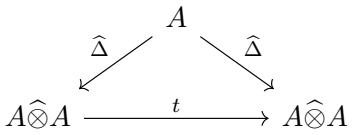


Figure 2.3: inversion

Recall that co-commutativity means, once again, that the following diagram commutes:



Remark 2.69 Clearly the category of k-formal functor of groups is a full sub-category of the category of k-formal functors, and $A \mapsto \mathrm{Spf}_k A$ induces an antiequivalence between this category and the category of formal bi-algebras over k, with $\mathcal{O}^f$ as a quasi-inverse.

Definition 2.70 A profinite k-module R is said **topologically free** if it is isomorphic (as a module) to the k-module k^I endowed with the product topology, where I is a set. Instead R is called **topologically flat** if it is projective as k-module, which is equivalent, in this case, to the functor $S \mapsto S\widehat{\otimes}R$ being exact. (For $S \in PM_k$).

Definition 2.71 A formal bi-algebra over k is said **topologically flat** if it is flat as a k-module. A formal k-group is said to be **topologically flat** if its underlying formal bi-algebra is topologically flat.

Lemma 2.72 Let k be an *artinian* commutative unital pseudo-compact ring (or a *field*). The functor:

$$(-)^* : R \mapsto R^* = \mathrm{Hom}_{k-mod,cont}(R, k) \tag{2.69}$$

induces an antiequivalence between the category of *profinite projective* (resp. *profinite topologically free*) k-modules and the category of *projective* (resp. *free*) k-modules, with a quasi-inverse the functor:

$$(-)^{\#} : S \mapsto S^{\#} := \mathrm{Hom}_{k-mod,cont}(S, k) \tag{2.70}$$

Where S is a k-module (without topology) and $\mathrm{Hom}_{k-mod,cont}(S,k)$ is the topological module of continuous k-linear maps $S \to k$, with the topology given by the simple convergence topology.

Proof. We only give an outline of the proof (for details see [Fo], I.3). Clearly we have that $\mathrm{Hom}(\mathrm{Hom}(A,-),\mathrm{Hom}(B,-)) = \mathrm{Hom}(B,A)$ thanks to the Yoneda Lemma, and this implies that $(-)^*$ is fully faithful. Let S be a projective k-module and consider

$$(S^{\#})^* := \mathrm{Hom}_{k-mod,cont}(\mathrm{Hom}_{k-mod,cont}(S,k),k) \tag{2.71}$$

where the topology for the continuity of the k-linear maps is given by the simple ("pointwise") convergence. Then as k-modules (without topology) $S \simeq (S^{\#})^*$ in a canonical way, namely $S \ni s \mapsto (f \mapsto f(s))$ for $f \in \mathrm{Hom}_{k-mod,cont}(S,k)$. Therefore each S can be viewed as a $(R)^*$, for $R := S^{\#}$ and finally $(-)^{\#}$ is a quasi-inverse. □

Notice that in the specific case in which k is a field, then clearly $V^* \otimes W^* \simeq (V \otimes W)^*$ for V, W finite-dimensional k-vector spaces. We do an analogue computation (that can also be found in [Fo]), for the case of dual k-algebras/co-algebras.

A DISCUSSION:

Recall that if k is an artinian ring and R is an arinian k-module, then R is also noetherian and hence it is finitely generated (see the Hopkins-Levitzki theorem, that can be found for example in [Cohn P.M., *Basic Algebra: Groups, Rings and Fields*, 2003]). So, given a pseudo-compact artinian ring k, let R be a profinite projective k-module. Then $R = \varprojlim R/\mathcal{A}$ for $\mathcal{A} \in \Omega_R$ and each $R/\mathcal{A}$ is artinian and hence finitely generated. If, moreover, R is projective, then (as we stated in Proposition [1.68]) we have that $(R/\mathcal{A})^* \otimes (R/\mathcal{A})^* \simeq ((R/\mathcal{A}) \otimes (R/\mathcal{A}))^*$ (this actually mean that we can give to R^* a co-algebra structure if R is a k-algebra). Finally it is sufficient to consider $R^* \simeq \mathrm{Hom}(R,k) = \varinjlim_{\mathcal{A} \in \Omega_R} \mathrm{Hom}(R/\mathcal{A},k) = \varinjlim_{\mathcal{A} \in \Omega_R} (R/\mathcal{A})^*$. Let us do more explicitly this computation.

Consider now the functor $(-)^*$ defined in the above theorem, when applyed to a formal k-bi-algebra A that is topologically flat (i.e. projective). We have $A \mapsto A^* = \mathrm{Hom}_{k-mod,cont}(A,k)$, which is a projective (and hence flat) k-module. From the antiequivalence above, the co-product $\widehat{\Delta} : A \to A\widehat{\otimes}A$ induces a map $\widehat{\Delta}^* : A^* \otimes A^* \simeq (A\widehat{\otimes}A)^* \to A^*$ (the isomorphism is thanks, again, to Proposition [1.68], however in this case it is sufficient to consider the monomorphism/injective k-linear map $A^* \otimes A^* \hookrightarrow (A\widehat{\otimes}A)^*$). But then A^* is a k-algebra with multiplication $\widehat{\Delta}^*$. It is also a k-co-algebra thanks to the co-product defined by $\widehat{m_A}^* : A^* \to (A\widehat{\otimes}A)^* \simeq A^* \otimes A^*$, which is induced by the map $\widehat{m_A} : A\widehat{\otimes}A \to A$ such that $\widehat{m_A}(a\widehat{\otimes}b) = m_A(a,b) = a \cdot b$, where $m_A := (-) \cdot (-)$ is the multiplication law defined on the k-algebra $A \in PM_k \subset \mathbf{Alg_k}$.

Remark 2.73 With abuse of notation sometimes we will use R^* both to indicate the dual module of a k-module R, and the k-module $\mathrm{Hom}_{k-mod,cont}(R,k)$ when the module R is a *topological* (profinite) k-module given by the functor $(-)^*$. It is clear from the context whenever we mean one of these two meanings.

We are now ready to introduce the definition of *Cartiér dual* for affine k-groups and formal k-groups.

Definition 2.74 We define a contravariant functor $\mathtt{D}$ from the category of formal k-groups (topologically flat) to the category of affine k-groups as the functor:

$$G \mapsto \mathtt{D}(G) \tag{2.72}$$

such that if $G := \mathrm{Spf}_k A$ for $A \in PM_k^{op}$, then $\mathtt{D}(G) := \mathrm{Sp}_k A^*$. (Heare A^* is the k-bi-algebra given by the functor of previous lemma). The affine k-group (scheme) $\mathtt{D}(G)$ is called **Cartiér dual** of G. Clearly if A is a topologically flat profinite k-bi-algebra then A^* is a flat (as a module) k-algebra.

Let now B be a (flat - as k-module) k-bi-algebra, then using the above functor $(-)^{\#}$ and thanks to the antiequivalence we proved, we get a formal k-bi-algebra $B^{\#}$ (that is topologically flat). To show that $B^{\#}$ is a formal k-bi-algebra one can use analogue considerations as we did for the functor $(-)^*$ before, starting from the structure morphisms of a formal k-bi-algebra (with inversion) $(B, \Delta, \epsilon, m, e, \sigma)$.

Definition 2.75 We define a contravariant functor $\widehat{\mathtt{D}}$ from the category of affine and flat k-groups (heare flatness/projectivity is necessary, see previous paragraphs and recall that k is artinian), to the category of topologically flat formal k-groups, as the functor:

$$G \mapsto \widehat{\mathtt{D}}(G) \tag{2.73}$$

such that if $G := \mathrm{Sp}_k B$ for $B \in \mathbf{Alg_k}^{op}$, then $\widehat{\mathtt{D}}(G) := \mathrm{Spf}_k B^{\#}$. The formal k-group (scheme) $\widehat{\mathtt{D}}(G)$ is called **Cartiér dual** of G.

Thanks to the above constructions we have already proven the following:

Theorem 2.76 The Cartiér dual given by the functor $G \mapsto \mathtt{D}(G)$ induces an antiequivalence between the category of topologically flat formal k-groups and the category of affine flat k-groups, with quasi-inverse the functor $G \mapsto \widehat{\mathtt{D}}(G)$.

Corollary 2.77 If k is a field then the above equivalence is between the category of formal k-groups and the category of affine k-groups.

Let now k be noetherian (commutative unital ring), in this case, a k-module R is *finitely generated* if and only if it is *finitely presented* ([1.76]), and hence a finitely generated k-module R is projective if and only if it is flat if and only if it is locally free. Moreover R^*,

the dual module of R, is again a flat k-module. Recall also that from Definition [1.76] we defined as *finite* a finitely generated k-module. Whenever R is also a k-algebra we say that it is of *finite type* if it is finitely generated as k-algebra.

Definition/Remark 2.78 A **finite (affine) k-group (scheme)** is a group scheme over k such that its associated algebra A is finitely generated as k-module (i.e. a finite k-module). If k is pseudo-compact topological ring, recall that there is a different definition of "finiteness" for a linearly topologised separated complete k-module: such a module is said to be finite if it is profinite and of finite length. Hence a **finite formal k-group** is a k-formal functor of groups such that its associated profinite k-algebra $\hat{A}$ is a finite *topological* k-module. (One can show that for profinite k-algebras the two notions coincide).

Definition 2.79 We call again the **Cartiér dual** of G the functor $G \mapsto \mathtt{D}(G)$ that gives an antiequivalence between the category of finite flat (affine) k-groups into itself, i.e. the functor such that if $G := \mathrm{Sp}_k A$ then $\mathtt{D}(G) = \mathrm{Sp}_k A^*$ (using the *dual module* A^* of A which is again a k-algebra). From previous remark this is actually a functor from the category of finite flat (affine) k-groups and finite (topologically) flat formal k-groups, hence if k is a topological pseudo-compact artinian ring the two definitions we gave (of Cartiér dual) coincide.

Proposition 2.80 Let k be a noetherian ring as before. There is a (canonical) identification $G \simeq \mathtt{D}(\mathtt{D}(G))$.

Proof. See ([De], II, 4-5). □

Following the above definition of Cartiér dual, we can prove an important result.

Theorem 2.81 Let k be a noetherian commutative unital ring, then the functor defining the Cartiér dual, $G \mapsto \mathtt{D}(G)$, is a (commutative) k-functor of groups such that, for each $R \in \mathbf{Alg_k}$, we have:

$$\mathtt{D}(G)(R) \simeq \mathrm{Hom}_{k-fnct,gps}(G \otimes R, \mu_R) \tag{2.74}$$

where μ_R is the multiplicative group (scheme) extended to R, i.e. given an (associative) R-algebra S (equiv. a ring homomorphism $R \to S$), then $\mu_R(S) := (S^\times, \cdot)$. μ_R is the affine R-group scheme with associated algebra $R[X, X^{-1}]$.

Proof. Let $G := \mathrm{Sp}_k A$ and let A^* be the dual k-module (k-algebra) of A. Recall that $\mathrm{Hom}_{k-mod}(A^*, R)$ is canonically isomorphic to $(A^*)^* \otimes R \simeq A \otimes R$. Hence, since $\mathtt{D}(G)(R) = \mathrm{Sp}_k A^*(R) = \mathrm{Hom}_{k-alg}(A^*, R)$ (as k-algebras morphisms), then it is clearly a sub-set of $\mathrm{Hom}_{k-mod}(A^*, R) \simeq A \otimes R$ (as k-modules morphisms). To be more precise, if $f : A^* \to R \in \mathtt{D}(G)(R)$, then it can be viewed as $f \in A \otimes R$, and so $\Delta_R : (A \otimes R) \otimes (A \otimes R) \to (A \otimes R)$ must be such that:

$$f \mapsto \Delta_R(f) = f \otimes f \tag{2.75}$$

thanks to the multiplication law defined on G and to the fact that $f \in \mathtt{D}(G)(R)$ i.e. $f = \mathtt{D}(g)$ for $g \in G(R)$. Moreover $\epsilon_R : (A \otimes R) \to k \otimes R \simeq R$ must be such that:

$$\epsilon_R(f) = 1_R \tag{2.76}$$

again thanks to the unit $k \to A$ defining the unit in $G(R)$. So we have shown that:

$$f \in \{x \in A \otimes R | x \otimes x = 1,\ \epsilon(x) = 1_R\} \tag{2.77}$$

which is nothing but the (definition of co-multiplication and co-unit of the) multiplicative group $(A \otimes R)^\times$. Therefore, thanks to Lemma [2.63], in particular using equations (2.56), this means that f must be a *group homomorphism*, namely:

$$f \in \mathrm{Hom}_{k-fnct,gps}(G \otimes R, \mu_R) \simeq \mu_R(A \otimes R) = (A \otimes R)^\times \tag{2.78}$$

For the first part we used again Yoneda Lemma, namely:

$$\mathrm{Hom}_{k-fnct,gps}(G \otimes R, \mu_R) = \mathrm{Hom}_{k-fnct,gps}(\mathrm{Sp}_k A \otimes R, \mu_R) = \mathrm{Hom}_{k-fnct,gps}(\mathrm{Sp}_R A, \mu_R) = \mu_R(A \otimes R) = A^\times \tag{2.79}$$

as an R-algebra. □

2.3 Witt vectors and Dieudonné modules

In this section we introduce the important notions of *Wing vectors* and *Dieudonné modules*.

2.3.1 The ring of Witt vectors

Let's start considering the ring $\mathcal{B} := \mathbb{Z}[X_0, X_1, X_2, ..., X_n, ...]$ for $(X_n)_{n \in \mathbb{N}}$ a family of variables. Denote with $\mathcal{B}_\mathbb{Q}$ the corresponding ring $\mathbb{Q}[X_0, X_1, X_2, ..., X_n, ...] = \mathcal{B} \otimes_\mathbb{Z} \mathbb{Q}$.

Definition 2.82 Let $X = (X_n)_{n \in \mathbb{N}}$ and, for each $n \in \mathbb{N}$, define the polynomials:

$$X^{(n)} = \Phi_n(X) := X_0^{p^n} + pX_1^{p^{n-1}} + ... + p^n X_n \tag{2.80}$$

which are called n^{th}-**ghost components**.

Notice that $X_0 = X^{(0)}$ and hence $X_1 = \frac{1}{p}(X^{(1)} - X^{(0)p})$, more in general we have that:

$$X_n = \Psi_n(X^{(0)}, X^{(1)}, ..., X^{(n)}) \in \mathbb{Z}\left[\frac{1}{p}\right] \tag{2.81}$$

hence we have that:

$$\mathcal{B}_\mathbb{Q} = \mathbb{Q}[X^{(0)}, X^{(1)}, ..., X^{(n)}, ...] \tag{2.82}$$

Definition 2.83 Consider the category $\mathbf{Alg}_{\mathbb{Z}}$ of $\mathbb{Z}$-algebras (i.e. rings) and define the *affine $\mathbb{Z}$-scheme*:

$$W := \mathrm{Sp}_{\mathbb{Z}}\mathcal{B} \tag{2.83}$$

such that:

$$W(R) = \mathrm{Hom}_{\mathbb{Z}}(\mathcal{B}, R) \tag{2.84}$$

for each ring $R \in \mathbf{Alg}_{\mathbb{Z}}$.

Remark 2.84 Observe that for each ring R, an element $x \in W(R)$ is completely defined by its **components**:

$$x_i := x(X_i) \in R \tag{2.85}$$

so that $W(R) = R^{\mathbb{N}}$ as a *set* (or equivalently $W \simeq (\mathrm{Sp}_{\mathbb{Z}}k[t])^{\mathbb{N}}$ as $\mathbb{Z}$-functor) and $W(R) \ni x = (x_i)_{i\in\mathbb{N}}$. However we want to endow $W(R)$ with a *ring* structure (for each R, in a functorial way).

Notice that if R is a $\mathbb{Q}$-algebra, then $x \in W_{\mathbb{Q}}(R) = \mathrm{Hom}_{\mathbb{Q}}(\mathcal{B}_{\mathbb{Q}}, R)$ is completely defined (thanks to equation (2.82)) by $x^{(i)} := x(X^{(i)})$, i.e. the **ghost components** of x. Moreover, $W_{\mathbb{Q}}(R) \simeq R^{\mathbb{N}}$ as *rings*, with sum and multiplication given by:

$$(x+y)^{(i)} = x^{(i)} + y^{(i)}$$
$$(xy)^{(i)} = x^{(i)}y^{(i)}$$

More explicitly, the operations defined above on the $\mathbb{Q}$-scheme $\mathrm{Sp}_{\mathbb{Q}}\mathcal{B}_{\mathbb{Q}} = W_{\mathbb{Q}}$ for each R, come from the maps:

$$\mathbf{S} : \mathcal{B}_{\mathbb{Q}} \to \mathcal{B}_{\mathbb{Q}} \otimes \mathcal{B}_{\mathbb{Q}} \quad \text{and} \quad \mathbf{P} : \mathcal{B}_{\mathbb{Q}} \to \mathcal{B}_{\mathbb{Q}} \otimes \mathcal{B}_{\mathbb{Q}} \tag{2.86}$$

$$X^{(i)} \mapsto X^{(i)} \otimes 1 + 1 \otimes X^{(i)} \quad \text{and} \quad X^{(i)} \mapsto X^{(i)} \otimes X^{(i)} \tag{2.87}$$

and are such that, for $x, y \in W_{\mathbb{Q}}(R)$:

$$x + y := \mu_R \circ (x \otimes y) \circ \mathbf{S} \quad \text{and} \quad x \cdot y := \mu_R \circ (x \otimes y) \circ \mathbf{P} \tag{2.88}$$

where $\mu_R : W_{\mathbb{Q}}(R) \otimes W_{\mathbb{Q}}(R) \to W_{\mathbb{Q}}(R)$ is the multiplication map.

In order to extend those operations also for $W(R)$, we need to verify that once computed on the X_i, $\mathbf{S}(X_i)$ and $\mathbf{P}(X_i)$ are polynomials (in the $(X_n)_{n\in\mathbb{N}}$) with coefficients in $\mathbb{Z}$. In order to do this we need a "preparation" lemma.

Definition 2.85 Consider the morphism of $\mathbb{Z}$-schemes:

$$F_R : W(R) \to W(R) \tag{2.89}$$

defined starting from the endomorphism $\mathcal{B} \to \mathcal{B}$ given by $X_n \mapsto X_n^p$ for each $n = 0, 1, ...$, such that:

$$(F_R(x))_i := x_i^p \tag{2.90}$$

i.e. $(x_0, x_1, ...) \mapsto (x_0^p, x_1^p, ...)$. Such a morphism is called the **Frobenius endomorphism of W**. We only write F whenever R is clear from the context.

Lemma 2.86 Let $\underline{X} \in W_{\mathbb{Q}}(\mathcal{B}_{\mathbb{Q}})$ given by $\mathcal{B} \to \mathcal{B}_{\mathbb{Q}}$ s.t. $(X_0, X_1, ...) \mapsto (X_0, X_1, ...) =: \underline{X}$. Then:

$$(\underline{X})^{(n)} = (F(\underline{X}))^{(n-1)} + p^n X_n \tag{2.91}$$

Proof.

$$(\underline{X})^{(n)} = \sum_{i=0}^{n} p^i X_i^{p^{n-i}} = \sum_{i=0}^{n-1} p^i X_i^{p^{n-i}} + p^n X_n =$$
$$= \sum_{i=0}^{n} p^i (X_i^p)^{p^{(n-1)-i}} + p^n X_n = (F(\underline{X}))^{(n-1)} + p^n X_n$$

□

Lemma 2.87 Let $n > 0$ and $m \geq 0$. Consider $u, v \in W_{\mathbb{Q}}(\mathcal{B}_{\mathbb{Q}})$. Then the following are equivalent:

(i) $u_i = v_i$ mod. $p^n\mathcal{B}$ for every $i \leq m$

(ii) $u^{(i)} = v^{(i)}$ mod. $p^{n+1}\mathcal{B}$ for every $i \leq m$

Proof.

Observe that, since $a \equiv b$ mod. $p^n\mathcal{B}$ implies $a^p \equiv b^p$ mod. $p^{n+1}\mathcal{B}$, then $u_i = v_i$ mod. $p^n\mathcal{B}$ gives $F(u)_i = F(v)_i$ mod. $p^{n+1}\mathcal{B}$.

Let's prove $((i) \Rightarrow (ii))$: by induction on i, we have that $u_0 = u^{(0)}$ and $v_0 = v^{(0)}$. Suppose that this holds for each $0 \leq j < i$, then in particular:

$$F(u)^{(i-1)} = F(u)^{(i-1)} \text{mod.} p^{n+1}\mathcal{B}$$

but then from Equation (2.91) of the previous lemma:

$$u^{(i)} = F(u)^{(i-1)} - p^i u_i$$
$$v^{(i)} = F(v)^{(i-1)} - p^i v_i$$

For $((ii) \Rightarrow (i))$ consider, from the definition of the X_i's, that:

$$u_i = \frac{1}{p^i}(u^{(i)} - \sum_{j=0}^{i-1} p^j u_j^{p^{i-j}})$$
$$v_i = \frac{1}{p^i}(v^{(i)} - \sum_{j=0}^{i-1} p^j v_j^{p^{i-j}})$$

and again by induction on i, we get $u_j = v_j$ mod. $p^n\mathcal{B} \Rightarrow u_i^{p^{i-j}} = v_i^{p^{i-j}}$ mod. $p^{n+i-j}\mathcal{B}$ for each $0 \leq j < i$, hence the thesis holds. □

We are ready to show what we need to make W as functor of *rings*.

Theorem 2.88 The polinomials $\mathbf{S}(X_i)$ and $\mathbf{P}(X_i)$ (defined in Equation (2.86)), for $i \in \mathbb{N}$, are polynomials (in the $(X_n)_{n\in\mathbb{N}}$) with coefficients in $\mathbb{Z}$.

Proof.

- step **1**: observe that from equations (2.81) and (2.88) we have that:

$$\mathbf{S}(X_n) = \Psi_n(X^{(0)} \otimes 1 + 1 \otimes X^{(0)}, ..., X^{(n)} \otimes 1 + 1 \otimes X^{(n)}) \tag{2.92}$$
$$\mathbf{P}(X_n) = \Psi_n(X^{(0)} \otimes X^{(0)}, ..., X^{(n)} \otimes X^{(n)}) \tag{2.93}$$

- step **2**: from $\mathcal{B}_\mathbb{Q} \otimes_\mathbb{Q} \mathcal{B}_\mathbb{Q} \xrightarrow{\sim} \mathbb{Q}[\underline{X}, \underline{Y}]$ given by $X^{(i)} \otimes 1 \mapsto \underline{X}_i$ and $1 \otimes X^{(i)} \mapsto \underline{Y}_i$ we get:

$$\mathbf{S}_n(\underline{X}, \underline{Y}) = \mathbf{S}(X_n) = \Psi_n(\Phi_0(\underline{X}_0) + \Phi_0(\underline{Y}_0), ..., \Phi_n(\underline{X}_n) + \Phi_n(\underline{Y}_n)) \tag{2.94}$$
$$\mathbf{P}_n(\underline{X}, \underline{Y}) = \mathbf{P}(X_n) = \Psi_n(\Phi_0(\underline{X}_0)\Phi_0(\underline{Y}_0), ..., \Phi_n(\underline{X}_n)\Phi_n(\underline{Y}_n)) \tag{2.95}$$

where $\underline{X} := (\underline{X}_0, ...)$ and $\underline{Y} = (\underline{Y}_0, ...)$.

- step **3**: now we proceed by induction on n, for $n = 0$:

$$\mathbf{S}_0(\underline{X}, \underline{Y}) = \mathbf{S}(X_0) = \Psi_0(\underline{X}^{(0)} + \underline{Y}^{(0)}) = \underline{X}_0 + \underline{Y}_0 \in \mathbb{Z}[\underline{X}_0, ...; \underline{Y}_0, ...] \tag{2.96}$$

- step **4**: now suppose that $\mathbf{S}_j(\underline{X}, \underline{Y}) \in \mathbb{Z}[\underline{X}, \underline{Y}]$ for each $0 \leq j < n-1$ and consider:

$$(\underline{x}_0, ...),\ (\underline{y}_0, ...) \in W(\mathbb{Q}[\underline{X}, \underline{Y}])$$

then, recalling that $\underline{x} + \underline{y} = \mu_{\mathbb{Q}[\underline{X},\underline{Y}]} \circ (\underline{x} \otimes \underline{y}) \circ \mathbf{S}$, we have that:

$$F(\underline{x} + \underline{y})_j := (\underline{x} + \underline{y})_j^p = (\mu_{\mathbb{Q}[\underline{X},\underline{Y}]} \circ (\underline{x} \otimes \underline{y}) \circ \mathbf{S}_j(\underline{X}, \underline{Y}))^p \equiv \tag{2.97}$$
$$\equiv (\mu_{\mathbb{Q}[\underline{X},\underline{Y}]} \circ (\underline{x} \otimes \underline{y}) \circ \mathbf{S}_j(\underline{X}, \underline{Y})^p) \text{ mod. } p\mathbb{Z}[\underline{X}, \underline{Y}] \equiv \tag{2.98}$$
$$\equiv (\mu_{\mathbb{Q}[\underline{X},\underline{Y}]} \circ (\underline{x} \otimes \underline{y}) \circ \mathbf{S}_j(\underline{X}^p, \underline{Y}^p)) \text{ mod. } p\mathbb{Z}[\underline{X}, \underline{Y}] \equiv \tag{2.99}$$
$$\equiv (F(\underline{x}) + F(\underline{y}))_j \text{ mod. } p\mathbb{Z}[\underline{X}, \underline{Y}] \tag{2.100}$$

for every $0 \leq j < n$; from this and from previous Lemma [2.87] we get:

$$F(\underline{x}+\underline{y})^{(n-1)} = F((\underline{x})+F(\underline{y}))^{(n-1)} = F(\underline{x})^{(n-1)} + F(\underline{y})^{(n-1)} \text{ mod. } p^n\mathbb{Z}[\underline{X},\underline{Y}] \quad (2.101)$$

hence using Equation (2.101) together with (2.91) of Lemma [2.86] we get:

$$F(\underline{x}+\underline{y})^{(n-1)} = (\underline{x})^{(n-1)} + (\underline{y})^{(n-1)} \text{ mod. } p^n\mathbb{Z}[\underline{X},\underline{Y}] \quad (2.102)$$

but now again Equation (2.91) applyed to $\underline{x}+\underline{y}$ gives:

$$p^n(\underline{x}+\underline{y})_n = (\underline{x}+\underline{y})^{(n)} - (F(\underline{x}+\underline{y}))^{(n-1)} = \quad (2.103)$$

$$= (\underline{x})^{(n)} + (\underline{y})^{(n)} - (F(\underline{x}+\underline{y}))^{(n-1)} \equiv 0 \text{ mod. } p^n\mathbb{Z}[\underline{X},\underline{Y}] \quad (2.104)$$

and finally this implies $(\underline{x}+\underline{y})_n \in \mathbb{Z}[\underline{X},\underline{Y}]$ (that is $S_n(\underline{X},\underline{Y}) \in \mathbb{Z}[\underline{X},\underline{Y}]$).

• step **5**: doing the same computations for the product we can conclude that also $P_n(\underline{X},\underline{Y}) \in \mathbb{Z}[\underline{X},\underline{Y}]$. □

Definition/Corollary 89 For each ring R, the *set* $W(R)$ endowed with the operations of addition and multiplication defined as above is a **ring** with unit $1_{W(R)} = (1,0,0,...)$ and $0_{W(R)} = (0,0,0,...)$; it is called the **ring of Witt vectors over** $\mathbb{Z}$.

Remark 2.90 From the theorem it is clear that the operations **S** and **P** gives to $R \mapsto W(R)$ a structure of $\mathbb{Z}$-functor with values on the category of ($\mathbb{Z}$-)*rings*.

After this hard computations we can define the more general ring of Witt vectors over a commutative unital ring k. Then proceed summing up some of the main properties of Witt vectors and covectors and defining the Dieudonné rings and modules.

Definition 2.91 Let k be commutative unital ring, the k-scheme:

$$W_k := \mathrm{Sp}_k(\mathbb{Z} \otimes_{\mathbb{Z}} k)[X_0,...] = \mathrm{Sp}_k k[X_0,...] \quad (2.105)$$

is called (the k-scheme of) ring of **Witt vectors over** k.

Example 2.92 Let $k = \mathbb{F}_p$ and R a ring with characteristic equal to p, then:

$$W_{\mathbb{F}_p}(R) = W(R) = \{x = (x_n)_n | x_n \in R\} \quad (2.106)$$

and the polinomials defining $(x+y)_i$ and $(xy)_i$ are: $\overline{\mathbf{S}}_i(\underline{X},\underline{Y}), \overline{\mathbf{P}}_i(\underline{X},\underline{Y}) \in \mathbb{F}_p[\underline{X},\underline{Y}]$. Notice that in this case $x^{(i)} = x_0^{p^i}$, and this gives a concrete meaning to the terminology "ghost components".

Definition 2.93 Let W be the ring of Witt vectors over k as before. Then we define:

- the k-scheme of rings W_m, also called **truncated Witt ring of length** m, s.t. $W_m(R) = \{(x_0, ..., x_{m-1}) | x_i \in R\}$ for each k-algebra R;
- a functor $(\mathbf{m}) : W \to W_m$ such that $x \mapsto (x_0, ..., x_m)$ for each R and $x \in W(R)$;
- a functor $V : W \to W$ such that for each R and $x \in R$ then $(x_0, x_1, ..., x_n, ...) \mapsto (0, x_0, x_1, ..., x_{n-1}, ...)$, that is called the **Verschiebung morphism** of W;
- a functor $V_m : W_m \to W_{m+1}$ s.t. $V_m(x_0, x_1, ..., x_{m-1}) = (0, x_0, x_1, ..., x_{m-1})$ for each R and $x \in R$.

Proposition 2.94 Let W be the ring of Witt vectors over k. Then:

$$W = \varprojlim_n (W_n) = \varprojlim (W_1 \leftarrow W_2 \leftarrow W_3 ...) \tag{2.107}$$

Proof. It is clear from the sequence given by the canonical ring-homomorphisms:

$$\mathbb{Z}[X_0, X_1, ...] = \varinjlim (\mathbb{Z}[X_0] \to \mathbb{Z}[X_0, X_1] \to ...) \tag{2.108}$$

□

Proposition/Remark 2.95 Notice that as a consequence $W(R) = \varprojlim_n W_n(R)$ is a *linearly topologized* ring that is *separated* and *complete*.

Proposition 2.96 (Properties of V and F) Let $F : W \to W$ and $V : W \to W$ be respectively the Frobenius and the Verschiebung morphism (of the k-functor of Witt rings), let $\underline{x} = (\underline{x}_0, ...)$ and $\underline{y} = (\underline{y}_0, ...)$ be Witt vectors in $W(\mathbb{Z}[\underline{X}, \underline{Y}])$; then:

(i) $(\underline{x})^{(n)} = (F(\underline{x}))^{(n-1)} + p^n x_n$ (that is equation (2.91) of Lemma [2.86]);

(ii) $(V\underline{x})^{(n)} = p(\underline{x})^{(n-1)}$;

(iii) $V(\underline{x} + \underline{x}) = (V(\underline{x})) + (V(\underline{y}))$;

(iv) $V_m((\mathbf{m})(\underline{x} + \underline{y})) = (V_m((\mathbf{m})(\underline{x}))) + (V_m((\mathbf{m})(\underline{y})))$;

(v) $F(V(\underline{x})) = V(F(\underline{x}))$;

(vi) $V_m((\mathbf{m})(\underline{x})) = (\mathbf{m})(V(\underline{x}))$;

(vii) $F_m((\mathbf{m})(\underline{x})) = (\mathbf{m})(F(\underline{x}))$;

(viii) $F(V(\underline{x}))_n = (p\underline{x})_n \mod p\mathbb{Z}[X_0, X_1, ...]$;

where $F_m : W_m \to W_m$ is F restricted to W_m, and $(\mathbf{m}) : W \to W_m$ is the functor defined in [2.93].

Proof. All the properties are an almost immediate consequence thanks to the definition of the three functors. We give a proof of the last statement, which will be useful for the next proposition.

From the definition of F and V observe that $F(V(\underline{x})) = (0, \underline{x_0}^p, \underline{x}_1^p, ...)$, if $\underline{x} = (\underline{x_0}, \underline{x}_1, ...)$. Then $(F(V\underline{x}))_j = \underline{x}_{j-1}^p$ and from *(i)*:

$$(p\underline{x})^{(j)} = p(\underline{x})^{(j)} = p(F\underline{x})^{j-1} + p^{j+1}\underline{x}_j \tag{2.109}$$

and so using *(ii)*:

$$(p\underline{x})^{(j)} = (V(F\underline{x}))^{(j)} \text{ mod.} p^{j+1}\mathcal{B} \tag{2.110}$$

and using Lemma [2.87] we get:

$$(p\underline{x})_j = (V(F\underline{x}))_j \text{ mod.} p\mathcal{B} \tag{2.111}$$

□

Theorem 2.97 Let R be a ring such that char(R)=p, then:

$$p = (0, 1, 0, ...) \in W(R) \tag{2.112}$$

Moreover, if R is perfect then:

$$W(R) = \varprojlim_n W(R)/p^m W(R) \tag{2.113}$$

Proof. The proof is based on the fact that from Proposition ([2.96],*(viii)*) we have that $V(Fx) = F(Vx) = px = (0, x_0^p, x_1^p, ...)$ mod. $p\mathcal{B}$ for each $x \in W(R)$. Notice that here we can omit mod. $p\mathcal{B}$ since we are working in char p. As a consequence of this, for $x = 1_{W(R)} = (1, 0, 0, ...)$ clearly we get:

$$p \cdot 1_{W(R)} = p = (0, 1, 0, ...) \in W(R) \tag{2.114}$$

Let now R be perfect, then $p^m(W(R)) = (V \circ F)^m(W(R)) = V^m(W(R))$ since the Frobenius gives $W(R)^p \simeq W(R)$. From this we deduce:

$$W_m(R) \simeq W(R)/p^m W(R) \tag{2.115}$$

and hence

$$W(R) = \varprojlim_n W(R)/p^m W(R) \tag{2.116}$$

and the proof is concluded. □

Remark 2.98 Let $\sigma : R \to R$ be the absolute Frobenius (i.e. $\sigma(r) = r^p$), then sometimes we also denote with σ (with abuse of notation) the Frobenius $W(R) \to W(R)$. Notice also that, from the previous theorem, $W(R) = \varprojlim_n W(R)/p^m W(R)$ is *separated* and *completed* for the p-adic topology.

Since the case of most interest for us is to consider W_k for k a perfect field of characteristic p, we conclude the section on Witt vectors stating, without a proof, a useful result.

Proposition 2.99 Let R be a ring s.t. $\text{char}(R) = p$, then:

(i) $W_m(R)$ is a ring s.t. $\text{char}W_m(R) = p^m$;

(ii) $W(R)$ is a ring s.t. $\text{char}W(R) = 0$;

(iii) $x \in W(R)$ is invertible if and only if x_0 is invertible in R;

(iv) if R is a domain then $W(R)$ is a domain too.

Remark 2.100 In general we consider k as a commutative unital ring and R as an associative k-algebra (k-module with ring structure), and from the definition of R, i.e. from the morphism of rings $k \to R$ we also get the morphism of rings $W(k) \to W(R)$ (heare $W = W_k$). As a consequence $W(R)$ can be viewed as a $W(k)$-algebra and as a topologic ring so that $W(R) = \varprojlim_n W_n(R)$ also as $W(k)$-modules.

2.3.2 Witt covectors

Starting from the definition of the k-functor of Witt rings on k given before ([2.91]) and considering the functor between succesive truncated Witt rings given by:

$$V_m : W_m(R) \to W_{m+1}(R) \tag{2.117}$$

$$(x_0, ..., x_m) \mapsto (0, x_0, ..., x_m) \tag{2.118}$$

for each $x = (x_0, ...) \in W(R)$ and each k-algebra R, we observe that V_m is compatible with the addition operator $\mathbf{S}$ defined on W and restricted on W_m, i.e. we have:

$$V_m((x_0, ..., x_m) + (y_0, ..., y_m)) = V_m((x_0, ..., x_m)) + V_m((y_0, ..., y_m)) \tag{2.119}$$

thanks to Proposition [2.96] of previous section. Hence we are now ready to define:

Definition 2.101 (unipotent Witt covectors) Let k be a commutative unital ring and $R \in \mathbf{Alg_k}$, then the k-functor defined by:

$$CW^u(R) := \varinjlim_n W_n(R) \tag{2.120}$$

with the above operation $(-) + (-)$, is called **group of unipotent Witt covectors**.

Remark 2.102 Notice that an element $x \in \varinjlim_n W_n(R)$ can be viewed as a *covector* $(..., x_{-n}, ..., x_{-1}, x_0)$ such that x_{-n} are 0 for all but a finite number of n. So that $(x+y)_{-n} = \mathbf{S}(x_{-m-n}, ..., x_{-n}; y_{-m-n}, ..., y_{-n})$ for $m >> 0$.

We can now define a new k-functor CW and then state, without proving it, an important result giving to $CW(R)$ an abelian group structure for each k-algebra R. For a detailed proof of this we suggest to read [Fo], II.

Definition 2.103 Consider the k-functor CW such that, for each R, an element $x \in CW(R)$ is of the form $(..., x_{-n}, ..., x_{-1}, x_0)$ and the x_{-n}'s verfy the condition:

there exist an $r \geq 0$ s.t. the ideal $\mathcal{N}_r$ of R generated by the x_{-n}, for $n \geq r$, is nilpotent

it is called the k-functor of **Witt covectors**.

Proposition 2.104 Let $R \in \mathbf{Alg_k}$ and $x = (..., x_{-n}, ..., x_{-1}, x_0), y = (..., y_{-n}, ..., x_{-1}, y_0)$ in $CW(R)$, then:

(i) for each $n \geq 0$ the sum operator $\mathbf{S}_m(x_{-m-n}, ..., x_{-n}; y_{-m-n}, ..., y_{-n})$ is stationary for $m \to \infty$;

(ii) the element $s := (..., s_{-n}, ..., s_{-1}, s_0)$ belongs to $CW(R)$, where for each $n \geq 0$, $s_{-n} := \lim_{m \to \infty} \mathbf{S}_m$;

Theorem 2.105 The operation $(-) + (-)$ given by $x + y := s := (..., s_{-n}, ..., s_{-1}, s_0)$ for $x, y \in CW(R)$ and s_{-n} as before, gives to $CW(R)$ an abelian group structure for each R.

Definition 2.106 Let $\mathcal{N}_R$ be the set of all *nilpotents* ideals of $R \in \mathbf{Alg_k}$. Then for $\mathtt{n} \in \mathcal{N}_R$ and $r \geq 0$ denote with $CW(R, \mathtt{n}, r)$ the subgroup of $CW(R)$ given by all the elements $x = (..., x_{-n}, ..., x_{-1}, x_0)$ such that $x_{-n} \in \mathtt{n}$ for $n \geq r$.

Observe that we can endow $CW(R, \mathtt{n}, r) \simeq R^r \times \mathtt{n}^{\mathbb{N}}$ (as groups) with the product topology obtained equipping each component with the discrete topology. Hence, since:

$$CW(R) = \varinjlim_{\mathtt{n} \in \mathcal{N}_R} \varinjlim_{r} CW(R, \mathtt{n}, r) \tag{2.121}$$

then $CW(R)$ is a topological group separated and complete (for each R) and $CW^u(R)$ is a subgroup of $CW(R)$.

2.3.3 Dieudonné rings and modules

We can now give the definition of a very important object, that we will use in order to show some properties of our main subject, i.e. p-divisible groups, and that we will also use to classify them through some equivalence of categories as well.

Definition 2.107 (Dieudonné ring) Let k be a commutative unital ring, $R \in \mathbf{Alg_k}$ and $W_k(R)$ the ring of Witt vectors with a $W_k(k)$-module structure for each R. Then we denote by D_k the (non-commutative) ring generated by $W_k(k)$ and adding two elements

F and V satisfying the following:

$$Fx = x^p F \quad x^p V = Vx \quad FV = VF = p \tag{2.122}$$

Such a D_k is called **Dieudonné ring**.

Remark 2.108 Notice that if k is such that char.$k = p$ and R a k-algebra, D_k can be equipped with the p-adic topology and viewed as a topological ring. ([Fo]).

Proposition 2.109 Endowed with the p-adic topology, $CW_k(R)$ can be viewed as a topological D_k-module.

Definition 2.110 (Dieudonné module) A D_k-module as above is called a **Dieudonné module**.

Chapter 3

p-divisible Groups

In this section we introduce the central object of this work, **p-divisible groups**. We first start with a definition which strictly follows the one given by Serre and Tate in their works, as pioneers of the field. In order to give a characterisation of those objects and to emphasize their main properties, we compare the first definition with the one given later by Grothendieck (which is basically the actual modern definition of p-divisible group), who called those groups **Barsotti-Tate groups**[2]. Then we underline the main aspects of these different but equivalent points of views.

After showing basic properties of p-divisible groups, we give some examples, focusing in particular on the important role they play in the context of **abelian varieties** (such as elliptic curves); we also show the relation between p-divisible groups and finite flat **étales** schemes. Very important is the connection with **formal groups** and **formal Lie groups**, that will allow us to review the definition given by Grothendieck in a more general context. An important role in the characterisation of p-divisible groups as p-formal groups is played, in particular, by Dieudonné modules and Witt vectors.

Finally we go through an important result (due to Serre and Tate) on p-divisible groups and morphisms between them.

3.1 Definition of p-divisible groups

We start by recalling some of the main aspects of the objects we introduced in the previous chapter, which we are going to use in this section.

3.1.1 Notations

Along the whole section we use the following notations:

- unless otherwise specified k is a commutative unital **ring** (our base ring);

[2] I. Barsotti and J. Tate were indeed the forefathers of this field; Barsotti was the first who introduced those objects calling them *equidimensional hyperdomains*.

- with R or $(R_i)_i$ we shall always mean associative and commutative k-**algebras**, i.e. objects of $\mathbf{Alg_k}$ (k-modules with the obvious ring structure).

Remark 3.1 Recall from Theorem [2.35], that we can consider an **affine scheme** $X = \mathrm{Spec}(B)$ over the base scheme $S = \mathrm{Spec}(k)$ as a representable k-functor (we also say that it is an affine scheme over k or an affine k-scheme) i.e.:

$$X : \mathbf{Alg_k} \to \mathbf{Set} \tag{3.1}$$

such that $X = \mathrm{Sp}_k(B)$, for $B \in \mathbf{Alg_k}$. We have $X(A) = \mathrm{Sp}_k(B)(A) := \mathrm{Hom}_{k-alg}(B, A)$, for every $A \in \mathbf{Alg_k}$. From the antiequivalence between the categories $\mathbf{Alg_k}$ and $\mathbf{AffSch}/k$ given by [2.26], X is also a functor (of points):

$$X : \mathbf{AffSch}/k \to \mathbf{Set} \tag{3.2}$$

s.t. for $T = \mathrm{Sp}_k(A)$, $X(T) = \mathrm{Hom}_{k-fnct}(T, X) = \mathrm{Hom}_{k-alg}(B, A)$ (thanks to Yoneda [1.26]). We also recall that an **affine k-group scheme** G is a group object in $\mathbf{AffSch}/k$ as well as a group object of $\mathbf{Alg_k}$ (see [2.59], [1.78]) i.e. a k-functor:

$$G : \mathbf{Alg_k} \to \mathbf{Gps} \tag{3.3}$$

which composed with the forgetful functor $for : \mathbf{Gps} \to \mathbf{Set}$, becomes a representable functor (the underlying affine k-scheme) and that satisfies the group object conditions [1.77]. Keeping in mind the two equivalent different notions given for affine k-schemes (namely [2.17] and [2.23]), we recall that the same applies to a **scheme** X over k. It can be viewed as a k-functor $\mathbf{Alg_k} \to \mathbf{Set}$, that must have an open covering of affine k-schemes and must be a sheaf $\mathrm{Op}^{op} \to \mathbf{Alg_k}$ (for the Grothendieck-Zariski topology -see [1.49]-), as well as it can be considered a locally ringed space: the underlying topological space of X is given by the union of a covering $\mathrm{Spec}(R_i)$ [2.16]. We have, again, that $X(A) = \mathrm{Hom}_{k-fnct}(\mathrm{Sp}_k(A), X)$, for every $A \in \mathbf{Alg_k}$. From what observed, also recall that we can consider the ring of **regular functions** on a (affine) k-scheme X:

$$\mathcal{O}_X(X) := \mathrm{Hom}_{k-fnct}(X, \mathbb{O}_a) \tag{3.4}$$

where $\mathbb{O}_a$ is the affine line ([2.24]) and can be viewed also as the additive k-group scheme $\mathbb{G}_a(R) = (R, +) \simeq \mathrm{Hom}_{k-alg}(k[x], R)$. If $X = \mathrm{Sp}_k(A)$ clearly $\mathcal{O}_X(X) \simeq A$ as a k-algebra. Finally using the locally-ringed-spaces point of view, the morphism of schemes $f : X \to \mathrm{Spec}(k)$, induces a morphism of sheaves $\mathcal{O}_{\mathrm{Spec}(k)} \to f_*\mathcal{O}_X$ making $f_*\mathcal{O}_X$ a sheaf of $\mathcal{O}_{\mathrm{Spec}(k)}$-algebras, which is in particular a sheaf of k-algebras thanks to (see [2.18]):

$$k = \mathcal{O}_{\mathrm{Spec}(k)}(\mathrm{Spec}(k)) \to \mathcal{O}_{\mathrm{Spec}(k)}(V) \to f_*\mathcal{O}_X(U) \tag{3.5}$$

for each open $U \subseteq X$, and V s.t. $f(U) \subseteq V$.

As we already did in the above remark we shall use the same notation (**Aff**)**Sch**/k to indicate both the category of topological (affine) schemes over k as defined in [2.17] and the category of (affine) k-schemes viewed as k-functors ([2.23] and [2.33]); they are indeed equivalent thanks to Theorem [2.35].

Notations 3.2 From now on in order to differentiate the geometrical and the functorial definition of schemes we write, following notations already introduced in [2.33]:

$$X := \text{a } k\text{-functor } \mathbf{Alg_k} \to \mathbf{Set} = \begin{cases} -\mathrm{Sp}_k(A), \text{ if } X \text{ affine} \\ -\text{a sheaf for the Grothendieck-Zariski topology,} \\ \text{otherwise} \end{cases} \tag{3.6}$$

for $A \in \mathbf{Alg_k}$, when considering X as a k-functor ([2.23] and [2.33]). While we write:

$$|X| := \text{underlying locally ringed space of X} = \begin{cases} \mathrm{Spec}(A), \text{ if } X \text{ affine} \\ \bigcup_i \mathrm{Spec}(R_i), \text{ otherwise} \end{cases} \tag{3.7}$$

where U_i is an open covering (for the Zariski topology) of X, viewed as a topological locally ringed space ([2.16]). We precise better the reletionship between the two notions with the following:

Proposition 3.3 Using notations of previous remark [3.1] recall that there is a fully faithful functor from the category of schemes over k to the (presheaves) category of all k-functors:

$$\mathbf{Sch}/k \to \mathrm{Fnct}(\mathbf{Alg_k}, \mathbf{Set}) \tag{3.8}$$

as a consequence:

(i) since every scheme X over k, viewed as a topological space $|X|$, is completely defined by its affine subsets, in particular by a cover of open affines, i.e. $(U_i)_i$ s.t. $|U_i| = \mathrm{Spec}(R_i)$ and $\bigcup_i U_i = |X|$, then X as a k-functor is completely defined by the (U_i) whenever they are viewed as open k-subfunctors;

(ii) a scheme X over k is completely defined by a sheaf of k-algebras, namely X is completely defined by the value of $f_*\mathcal{O}_X(-)$ (defined in previous eq. (3.5)) on his affines.

Proof. By Definition [2.16], $|X|$, viewed as a topological space, admits a cover of open affines as in the statement. If X is viewed as a k-functor, we can also write:

$$X = \varinjlim_{\substack{U_i \subseteq X \\ U_i \text{ affine}}} U_i \tag{3.9}$$

where each U_i can be seen as a k-subfunctor of X, and this is true in general thanks to theorem [1.57]: a presheaf can always be seen as the projective limit of its representable

sub-presheaves. In this case we are using the cover $|U_i|$ of open affine subschemes (k-subfunctors U_i) which thanks to the Grothendieck-Zariski topology [1.52], form a basis for the open affine subsets of X and turn X into a sheaf (U_i must satisfy conditions in [1.53] which translates the gluing properties of [2.4]). Clearly *(i)* $\Rightarrow$ *(ii)*, indeed by definition let V_j open affine of $\mathrm{Spec}(k)$, and for each $|U_j| := f^{-1}(|V_j|) = \mathrm{Spec}(R_j)$ open affine of $|X|$ consider $i : U_j := \mathrm{Sp}_k(R_j) \hookrightarrow X$. Hence $f_*\mathcal{O}_X(V_j) = \mathcal{O}_X(U_j) = i_*\mathcal{O}_{U_j}(U_j) = \mathcal{O}_{U_j}(U_j) \simeq R_j \in \mathbf{Alg_k}$. Finally $X \simeq \varinjlim_j(\mathrm{Sp}_k(R_j))$. □

The category $\mathbf{Sch}/k$ is hence the full subcategory of k-functors corresponding to those presheaves that are sheaves for the Grothendieck-Zariski topology, and this conclude our discussion on the formal definition of a scheme X over k,

3.1.2 Serre and Tate

Before introducing the definition of *p-divisible group*, that strictly follows the works of J. Tate and J.-P. Serre, let us make some observations recalling [2.20].

Remark/Definition 3.4 Let G be a (affine) k-group scheme as before, then:

- G is said to be a **finite** and **locally free (resp. flat/projective/free)** k-group scheme of order m, if the base morphism $f : G \to \mathrm{Spec}(k)$ is finite of rank m and locally free (resp. flat/projective/free) which means that -see also [2.19] and [2.20]- (f is affine and) the sheaf $f_*\mathcal{O}_X$ is a finite and locally free (resp. flat/projective/free) $\mathcal{O}_{\mathrm{Spec}(k)}$-module. Therefore $\mathcal{O}_G(U)$ is a finitely generated k-algebra that is a locally free (resp. flat/projective/free) k-module for each open $U \subseteq G$, in particular this is true for the associated algebra $\mathcal{O}_G(G)$ which is a finitely generated k-module of rank m.

- Being G a group object of (**Aff**)**Sch**/k, then on the (each of the) associated algebra(s), namely on $A = \mathcal{O}_G(G)$ if G is affine or on $\mathcal{O}_G(U)$ for each open $U \subseteq G$, there must be k-algebra homomorphisms $\Delta : A \to A \otimes A$, $i : A \to A$ and $\varepsilon : A \to k$ (resp. $\Delta : \mathcal{O}_G(U) \to \mathcal{O}_G(U) \otimes \mathcal{O}_G(U)$, $i : \mathcal{O}_G(U) \to \mathcal{O}_G(U)$ and $\varepsilon : \mathcal{O}_G(U) \to k$) that endow each $G(R)$ with a multiplicative (abelian) group structure; or equivalently that make the associated algebra(s) an (a sheaf of) Höpf algebra(s) with inversion, as proved in [2.59].

Notice that if k is a **noetherian** ring, for a **finite** k-module M it is equivalent being either locally free, projective or flat. If moreover k is a **local** ring, this is equivalent also to require M being a **free** k-module.

Definition 3.5 (Serre-Tate) Let p be a prime number and $h \geq 0$. A **p-divisible group over k of heigh h** is an **inductive system** of commutative k-group schemes:

$$G = (G_n, i_n)_{n \geq 0} \tag{3.10}$$

where, for each $n \geq 0$:

(i) G_n is a finite and locally free group scheme over k of rank p^{nh};

(ii) $i_n : G_n \to G_{n+1}$ is a homomorphism of group schemes;

(iii) the sequence

$$0 \to G_n \xrightarrow{i_n} G_{n+1} \xrightarrow{[p^n]} G_{n+1} \tag{3.11}$$

is **exact**, where $[p^n]$ is the multiplication-by-p^n map. We write

$$G = \varinjlim_n G_n \tag{3.12}$$

and consider G as the "collection" of G_n for all n.

Let us be more precise and make some observations in order to better understand the definition above. First of all notice that a p-divisible group G is not itself a k-scheme but it is rather an inductive limit of group schemes:

$$G_1 \xrightarrow{i_1} G_2 \xrightarrow{i_2} G_3 \xrightarrow{i_3} ... \xrightarrow{i_n} G_{n+1} \xrightarrow{i_{n+1}} ... \tag{3.13}$$

To be more precise G can be considered as a formal k-scheme as we will point out in section 3.3. Moreover, a p-divisible group G can be viewed as a **functor of points** i.e. a k-functor in the sense of [3.1]):

$$\mathbf{AffSch}/k \ni T \mapsto G(T) = \varinjlim_n G_n(T) \tag{3.14}$$

this make sense if we consider the scheme G as a sheaf for the *fppf* topology (defined in [1.55], which is finer than the Zariski-Grothendieck topology) as proven by the following:

Proposition 3.6 Let G be p-divisible group and consider the defining inductive system $(G_n)_n$ viewed as a system of sheaves of groups $G_n : (\mathbf{Aff})\mathbf{Sch}/k \to \mathbf{Gps}$ or equivalently (thanks to [3.3]) as a system of sheaves $\mathcal{O}_{G_n} : \mathrm{Op}^{op} \to \mathbf{Alg_k}$ for the *fppf* topology. Then the (limit) presheaf G s.t. $(\mathbf{Aff})\mathbf{Sch}/k \ni T \mapsto G(T) = \varinjlim_n G_n(T)$ is again a sheaf for the *fppf* topology.

Proof. Consider the base space $\mathrm{Spec}(k)$ endowed with the *fppf* topology. Then each open covering V_i has a refinement V_{ij} such that $j \in J$ for a finite index set J. We can consider the inductive limit of the definition as the direct limit of sheaves G_n for the *fppf* topology and therefore, this limit (which is a presheaf) thanks to finiteness of J and to proposition [3.3] is indeed a sheaf, namely:

$$\varinjlim_n (G_n(T)) =: (\varinjlim_n G_n)(T) \tag{3.15}$$

so that $G : \mathbf{Sch}/k \to \mathbf{Gps}$ is a sheaf of groups for the *fppf* topology. □

Proposition 3.7 The collection of k-group homomorphisms $(i_n)_n$ is a collection of closed immersions ([2.20], v) of k-group schemes $G_n \to G_{n+1}$. Moreover thanks to the exactness of the sequence in part *(iii)* of definition [3.5], for each $n \geq 0$, G_n can be identified, through these closed immersion maps with the **kernel** of the multiplication-by-p^n map $[p^n] : G_{n+1} \to G_{n+1}$.

Proof. Consider the sequence coming from definition [3.5],

$$0 \to G_n \xrightarrow{i_n} G_{n+1} \xrightarrow{[p^n]} G_{n+1}$$

we denote $G_{n+1}[p^n] := \ker(G_{n+1} \xrightarrow{[p^n]} G_{n+1})$. From the exactness of the sequence we have that $i_n(G_n) \simeq G_{n+1}[p^n]$. For simplicity let $G_{n+1} = \mathrm{Sp}_k(A)$ be an affine k-group, then the kernel of the multiplication-by-p^n map is a closed subscheme since $\ker(G_{n+1} \xrightarrow{[p^n]} G_{n+1}) = \{\mathcal{P} \in \mathrm{Spec}(A) | p^n \cdot \mathcal{P} = 0\} = \{\mathcal{P} \in \mathrm{Spec}(A) | f(\mathcal{P}) = 0 \text{ for all } f \in A/p^nA \subseteq A\} = V(A/p^nA)$, following [2.8] and [2.9]. The general case follows by considering the restriction of the kernel to an open covering of G_{n+1}. The surjectivity part of the definition of closed immersion follows from the injectivity of the i_n. □

Proposition 3.8 Let $n \geq 0$, then for each $m \geq 1$ the group scheme G_n can be identified with $G_{n+m}[p^n]$ (i.e. the kernel of the multiplication-by-p^n map: $[p^n] : G_{n+m} \to G_{n+m}$).

Proof. Starting from the closed immersion $i_n : G_n \to G_{n+1}$ given by proposition [3.7], and iterating the process, we get for each $m \geq 1$, closed immersions:

$$i_{n,m} : G_n \to G_{n+m} \tag{3.16}$$

where $i_{n,m} = i_{n+m} \circ i_{n+m-1} \circ ... \circ i_n$. Now we proceed by induction on m:

- for $m = 1$ we get the statement *(ii)* of def. [3.5];

- let $m > 1$ and suppose $G_n \simeq G_{m+n}[p^n]$, then:

$$G_n \overset{hp}{=} G_{n+m}[p^n] \overset{*}{=} G_{n+m} \cap G_{n+m+1}[p^n] \overset{def}{=} \tag{3.17}$$

$$\overset{def}{=} G_{n+m+1}[p^{n+m}] \cap G_{n+m+1}[p^n] \overset{**}{=} G_{m+n+1}[p^n] \tag{3.18}$$

where $*$ is given by the diagram:

$$\begin{array}{ccc} G_{n+m} & \xrightarrow{[p^n]} & G_{n+m} \\ \downarrow{\scriptstyle i_{n+m}} & & \downarrow{\scriptstyle i_{n+m}} \\ G_{n+m+1} & \xrightarrow[[p^n]]{} & G_{n+m+1} \end{array} \tag{3.19}$$

and $**$ is becouse $G_{m+n+1}[p^n] \subseteq G_{m+n+1}[p^{n+m}]$. □

Definition 3.9 A **homomorphism of p-divisible groups** $f : G \to H$, where $G = (G_n, i_n)$, $H = (G_n, i_n)$ are as in definition [3.5], is the datum of a system of (k-group schemes) homomorphisms $f = (f_n)_n$, such that the following diagram commutes for each $n \geq 0$:

$$\begin{array}{ccc} G_n & \xrightarrow{f_n} & H_n \\ \downarrow{\scriptstyle i_n} & & \downarrow{\scriptstyle i_n} \\ G_{n+1} & \xrightarrow[f_{n+1}]{} & H_{n+1} \end{array} \tag{3.20}$$

This is equivalent to give a collection of $g_n = i_{n+m} \circ f_n$ for each n (with $f_n : G_n \to H_n$ a k-group homomorphism) that makes each possible diagram $G_n \to H_{n+m}$ commutative, and hence

$$\mathrm{Hom}_{p\text{-div}}(G, H) := \mathrm{Hom}(\varinjlim_n G_n, \varinjlim_{t_n} H_{t_n}) = \varprojlim_n \varinjlim_{t_n} \mathrm{Hom}(G_n, H_{t_n}) = \varprojlim_n (G_n, H_n) \tag{3.21}$$

where the last equation is thanks to the fact that t_n is varying through all the possible $n+m$ that make commutative the diagrams above, hence the limit simplifies. (Notice that heare we are considering inductive limits of *fppf* sheaves as in proposition [3.6], however this will be true also working with formal k-groups in the next section).

Proposition 3.10 Let $G = (G_n, i_n)$ be a p-divisible group. The sequence:

$$0 \to G_m \xrightarrow{i_{m,n}} G_{n+m} \xrightarrow{j_{m,n}} G_n \to 0$$

where the $j_{m,n}$ maps come from the universal property of the kernel, namely:

$$\begin{array}{ccccc} G_{m+n} & \xrightarrow{[p^m]} & G_{m+n} & \xrightarrow{[p^n]} & G_{m+n} \\ & \overset{\exists!\ j_{m,n}}{\searrow} & \uparrow{\scriptstyle i_{n,m}} & & \\ & & G_n = G_{n+m}[p^n] & & \end{array} \tag{3.22}$$

is exact.

Proof. From the above diagram observe that, since G_{n+m} identifies with the kernel of $[p^{m+n}] : G_{n+m+1} \to G_{n+m+1}$, then the morphism $[p^n] \circ [p^m] : G_{n+m} \to G_{n+m}$ is the zero morphism. Therefore the maps $j_{m,n}$ are well defined (from the universal property of the kernel [1.36]) and each $j_{m,n}$ is the unique homomorphism such that $i_{n,m} \circ j_{m,n} = [p^m]$. Consider now the sequence of the statement, it is left exact since the map $i_{m,n}$ is injective being the immersion of the (p^n-torsion) subgroup $G_{n+m}[p^m]$. So passing to the quotient, we have another injection:

$$j'_{m,n} : G_{n+m}/i_{m,n}(G_m) \hookrightarrow G_n \tag{3.23}$$

For simplicity let k be a noetherian commutative ring and, for each n, let A_n be the algebra associated to each G_n, which is a locally free finitely generated k-module of rank p^{hn}. Without loss of generality A_n can be considered the associated algebra to $G_{n+m}/i_{m,n}(G_m)$ as well, since both G_n and $G_{n+m}/i_{m,n}(G_m)$ finite locally free k-group schemes of the same

order p^{hn}. Let now $\phi_{m,n} : A_n \twoheadrightarrow A_n$ the surjective homomorphism induced by $j'_{m,n}$. Since k is noetherian the increasing sequence of submodules given by $M_i := \ker(\phi^i_{m,n})$, stabilises. Hence there exist a $h >> 0$ s.t. $M_l = M_{l+1}$ for $l \geq h$ and so $\phi^h : M_h \to M_h$ is surjective but ϕ^h coincide also with the 0-map, hence $M_h = (0)$ and $\phi_{m,n}$ is also injective, from this descend the surjectivity of $j'_{m,n}$ and in conclusion the exactness of the sequence holds. (Heare ϕ^h means the h^{th}-composition of ϕ). □

Proposition 3.11 Let $G = (G_n, i_n)$ be a p-divisible group, then each G_n can be viewed as a sheaf of (flat) $\mathbb{Z}/p^n\mathbb{Z}$-modules.

Proof. Each G_n is a finite locally free k-group scheme of order p^{hn}, and its associated affine k-algebra A_n is a locally free (hence flat) finitely generated k-module of rank p^{hn}. Let $f_n : G \to \mathrm{Spec}(k)$ be the base morphism of each G_n, then the sheaf $(f_n)_*\mathcal{O}_{G_n} : \mathrm{Op}^{op} \to \mathbf{Alg_k}$ of regular functions on G_n, is a sheaf of k-algebras as observed in [3.4]. Now G_1 can be thought as a (sheaf of flat) $\mathbb{Z}/p\mathbb{Z}$-module(s) with h generators, meaning that A_1 can be seen as a locally free (hence flat) $\mathbb{Z}$-module of order p^h (since thanks to the fact that $\mathbb{Z}$ is an initial object in $\mathbf{Alg}_k$ a k-module A is also a $\mathbb{Z}$-module, namely one has $\mathbb{Z} \to k \to A$). Since G_1 is killed by $[p]$, as observed in the first part of proof of proposition [3.10], then there is an induced surjection $A_n \twoheadrightarrow A_n/pA_n$ for each n (as we did in the proof of proposition [3.7]). As a consequence the p-torsion group $G_1 = G_n[p]$ is a locally free $\mathbb{Z}/p\mathbb{Z}$-module (thanks to $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$) with h generators. Inductively we can see that since $A_n/pA_n \simeq A_1$ (thanks to the characterisation of the p^n-torsion groups G_n, namely definition [3.5], *(iii)*), we get that A_n is a $\mathbb{Z}/p^n\mathbb{Z}$-module. Notice that this is a generalisation of proposition [3.6]. □

3.1.3 Grothendieck definition of *Barsotti-Tate* groups

Let us state the *modern* definition of p-divisible group given by Grothendieck and show that it is equivalent to the previous one, meaning that the first can be easily translated into the second one and viceversa.

In this section a k-group scheme $f : G \to \mathrm{Spec}(k) \in \mathbf{Sch}/k$ is considered as *fppf* sheaf of abelian groups $f : \mathbf{Sch}/k \to \mathbf{AbGps}$, we know this is possible thanks to proposition [3.6] (we are using the Grothendieck *fppf* topology - see [1.55] - instead of the Zariski topology on a scheme G [2.16]).

Definition 3.12 A **p-divisible group** G over k, is a **fppf** sheaf of abelian groups on $\mathbf{Sch}/k$ such that:

(i) the morphism

$$[p] : G \to G \tag{3.24}$$

given by the multiplication-by-p map, is an **epimorphism** (in this sense G is said to be **p-divisible**);

(ii) G is p-**torsion**, meaning that:

$$G \simeq \varinjlim_{n} G(n) \tag{3.25}$$

where $G(n) := G[p^n] = \ker(G \xrightarrow{[p^n]} G)$;

(iii) each sub-sheaf $G[p^n]$ is representable by a **finite locally free** group scheme over k.

Proposition 3.13 Part *(iii)* of the definition above can be rephrased inductively: in fact, it is sufficient the datum of $G(1)$ and the fact that, for each $n \geq 1$, $G(n)$ is such that $G(n)/pG(n) \simeq G(1)$.

Before proving this proposition we recall the notion of connected k-scheme.

Remark 3.14 A scheme X is said to be **connected** if it is connected as topological space $|X|$; this is equivalent to require that the only **idempotent** elements of the associated algebra $\mathcal{O}_X(X)$ are 0 and 1. Clearly if K is a field $\mathrm{Spec}(K)$ is connected.

Proof. (of proposition [3.13]) Let G be a p-divisible group following definition [3.12], then if $\mathrm{Spec}(k)$ is *connected*, since $G(1)$ is a locally free finite k-group scheme killed by $[p]$ (thanks, to definition [3.12], *(ii)*), it follows that the order of G is p^h for $h > 0$ (see [3.10]). As a consequence, by induction, $G(n)$ is finite locally free of order p^{hn}. In general, for a non-connected base scheme, we can define the **heigh**, h, of G as the **locally constant function** $h : \mathrm{Spec}(k) \to \mathbb{N}$ such that $\mathcal{P} \mapsto h(G(\mathcal{P}))$, where, with abuse of notation, $G(\mathcal{P}) := \mathrm{Hom}_{k-fnct}(\mathrm{Sp}_k(K(\mathcal{P})), G)$ (using Yoneda [1.26] and denoting as always $K(\mathcal{P})$ the quotient field of [2.8]). □

Proposition 3.15 (Equivalence of the two Definitions) A p-divisible group G in the sense of Serre-Tate-definition [3.5] is equivalent to a p-divisible group G as in Grothendieck-definition [3.12].

Proof. ($\Rightarrow$) Let $(G_n)_{n\in\mathbb{N}}$ be an inductive system of k-group schemes as in definition [3.4], and set $G(n) := G_n$, for each $n \geq 0$. Then it is sufficient to consider the limit:

$$G := \varinjlim_{n} G(n) = \varinjlim_{n} G_n \tag{3.26}$$

Thanks to propositions [3.7],[3.8] and [3.10], we have that $G[p^n] = G(n)$, moreover G is p-torsion by definition, considering equation 3.26 above. Furthermore always thanks to [3.4], each $G(n)$ is finite locally free of order p^{hn}. Finally the map $[p] : G \to G$ is surjective thanks to proposition [3.10] considering that the map

$$j_{1,n} : G_{n+1} \to G_n \tag{3.27}$$

is surjective, finite (and faithfully flat morphism of fppf sheaves) of degree p^h thanks to [3.11].

($\Leftarrow$) Conversely consider a p-divisible group G sastisfying the conditions of definition [3.12]. For each $n \geq 0$, let $G_n := G(n) = G[p^n]$ with the natural closed immersion (of kernels) $i_n : G(n) \hookrightarrow G(n+1)$. Observe that since $[p]$ is surjective it is clear that

$$0 \to G(n) \xrightarrow{i_n} G(n+1) \xrightarrow{[p^n]} G(n+1) \tag{3.28}$$

is exact. From [3.11] it is also clear that each G_n is a finite locally free commutative k-group scheme of order $p^{n \cdot h(\mathcal{P})}$. □

Proposition 3.16 Let G be a p-divisible group in the sense of definition [3.12]. Then $G = \varinjlim_n G(n)$, viewed as direct limit of abelian sheaves of $\mathbb{Z}/p^n\mathbb{Z}$-modules has a natural structure of a sheaf of $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$-module (see [3.20], for a detailed definition of $\mathbb{Z}_p$).

Proof. Each $G(n)$ can be seen as a *fppf* sheaf of (finite locally free) $\mathbb{Z}/p^n\mathbb{Z}$-modules thanks to [3.11]. Let $(x_1, x_2, ..., x_n, ...) \in \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$. Consider the multiplication-by-x_n map, this induces a well defined action on $G(n)$, namely $\mathbb{Z}/p^n\mathbb{Z} \times G(n) \to G(n)$ given by $(x_n, g) \mapsto x_n \cdot g$, where for each $T \in (\mathbf{Aff})\mathbf{Sch}/k$ then $x_n \cdot g_T \in G(n)(T)$ is given by $g_T \circ ... \circ g_T$ composed x_n-times. The well-definitedness of the action comes from the commutativity of the following diagram:

$$\begin{array}{ccc} G(n) & \xrightarrow{[x_n]} & G(n) \\ \downarrow{\scriptstyle i_n} & & \downarrow{\scriptstyle i_{n+m}} \\ G(n+1) & \xrightarrow[[x_{n+1}]]{} & G(n+1) \end{array} \tag{3.29}$$

since $x_{n+1} \equiv x_n \mod p^n$. As a consequence there is an induced well defined action of $\mathbb{Z}_p$ on each $G(n)$, again given by the multiplication-by-x_n map. Now we can repeat construction of the proof of proposition [3.11], using the fact that there is an induced surjection $A \to \varprojlim_n A/p^nA$, where A is the associated algebra of G, and it is given by de diagram:

$$\begin{array}{ccc} A_{n+1} & \xrightarrow{[x_{n+1}]} & A_{n+1} \\ \downarrow & & \downarrow \\ A_n & \xrightarrow[[x_n]]{} & G_n \end{array} \tag{3.30}$$

(with A_n associated algebra of each $G(n)$), which is commutative as a consequence of previous diagram 3.29. Since $\varprojlim_n A/p^nA$ has naturally a $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$-module structure ($\mathbb{Z} \to k \to A$ is a $\mathbb{Z}$-module), we deduce the $\mathbb{Z}_p$-module structure on G. □

Proposition 3.17 Part *(i)* of definition [3.5] can be reprased as follows:

*G_n is a finite and **flat** group scheme over k of rank p^{nh}*

Proof. Let $G = (G_n, i_n)$ be a p-divisible group from definition [3.5]. We have seen from [3.15] and [3.11] that it can be seen as an *fppf* sheaf of *flat* $\mathbb{Z}/p^n\mathbb{Z}$-modules. Consider now the multiplication map $[p^n]$, then we have that $\ker[p^m] = \mathrm{im}[p^{n-m}]$ for each $0 \leq m \leq n$. Indeed consider the exact sequence:

$$\mathbb{Z}/p^n\mathbb{Z} \xrightarrow{[p^{n-m}]} \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{[p^m]} \mathbb{Z}/p^n\mathbb{Z} \tag{3.31}$$

and since each $G_n(= G(n))$ is *flat* (as sheaf of modules, see [3.11] and [2.20] for flatness definition), then this mean that $- \otimes G_n$ preserves the exact sequence giving:

$$G_n \xrightarrow{[p^{n-m}]} G_n \xrightarrow{[p^m]} G_n \tag{3.32}$$

and the thesis holds.

Definition 3.18 An **isogeny** is a map $f : G \to H$ between p-divisible groups, such that f is faithfully flat (in particular surjective) and $\ker(f)$ is finite.

Let G be a p-divisible group. Notice that, a consequence of proposition [3.10] or by definition as in [3.12], the multiplication map $[p] : G \to G$ is an **epimorphism** s.t. $\ker[p]$ (is finite flat and) has order p^h, i.e. $[p]$ is an **isogeny**, in particular it is surjective. This is the real reason to call those objects p-divisible groups. However a p-divisible group has to satisfy stronger conditions than the only "being divisible by p" (i.e. $[p]$ surjective), that's also why Grothendieck called them **Barsotti-Tate groups**.

Definition 3.19 The category $\mathbf{BT}_p(k)$, is the category whose objects are p-divisible groups (over k) and whose morphisms are homorphisms between them in the sense of [3.9]. Those morphisms can either be considered as morphisms between inductive systems or between *fppf* abelian sheaves from what observed in [3.11] and [3.16].

3.2 Examples of p-divisible groups

In this section we give some concrete examples of (classical constructions for) p-divisible groups which will be useful in relation to p-divisible groups of elliptic curver that we will see in next chapter. We start recalling some preliminary notions on the ring of p-adic numbers.

3.2.1 p-adic numers

Definition 3.20 The **field** of **p-adic numbers** $\mathbb{Q}_p$ is the completion of the field $\mathbb{Q}$ with respect to the p-adic absolute value

$$|\cdot|_p : \mathbb{Q} \longrightarrow \mathbb{R}_{\geq 0} \tag{3.33}$$

where

$$|r|_p = p^{-\nu_p(r)} \tag{3.34}$$

and $\nu_p(r)$ is the p-adic **valuation**:

$$\begin{cases} \nu_p(n) = \{\max\, k \in \mathbb{N},\ p^k | n\}, \text{ if } n \neq 0 \\ \nu_p(n) = \infty, \text{ otherwise} \end{cases} \tag{3.35}$$

and it can be extended on $\mathbb{Q}$ in the following way: if $r = \frac{m}{n}$, $\nu_p(r) = \nu_p(m) - \nu_p(n)$.

Definition/Proposition 3.21

- a p-**adic number** can be identified with a normalized p-adic series i.e. $\sum_{i=n}^{\infty} a_i p^i$, with $n, a_i \in \mathbb{Z}$, $0 \leq a_i < p$, $a_n \neq 0$;
- p-**adic integers** are p-adic numbers with $n \geq 0$ and form the commutative ring $\mathbb{Z}_p$;
- $\mathbb{Z}_p$ can be seen as $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$;
- $\mathbb{Q}_\mathbf{p}/\mathbb{Z}_\mathbf{p} \simeq \varinjlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}(p^\infty)$ is called the **Prüfer group**.

For a detailed discussion of this see for example [Neu], pp ...

3.2.2 The *Prüfer* group and the *multiplicative* group

Example 3.22 For the first and simplest example of p-divisible group, consider the Prüfer group $G := \mathbb{Q}_\mathbf{p}/\mathbb{Z}_\mathbf{p}$, already introduced in [3.21]. According to definition [3.5] (or [3.12]) it is a p-divisible group of heigh $h = 1$. Indeed G can be seen as the direct limit:

$$\mathbb{Q}_\mathbf{p}/\mathbb{Z}_\mathbf{p} \simeq \varinjlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}(p^\infty)$$

were the inductive system of groups G_n is given by the system of **constant** (cfr. [2.66]) k-group schemes:

$$\mathbb{Z}/p\mathbb{Z} \xrightarrow{\text{mod}p} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\text{mod}p^2} ... \tag{3.36}$$

Recall that this group can indeed be considered as a topological space endowed with the discrete topology, if we put on each $G_n := \mathbb{Z}/p^n\mathbb{Z}$ the discrete topology too.

More in general, for each $n \geq 0$, let $G_n := (\mathbb{Z}/p^n\mathbb{Z})^h$ (endowed again with the discrete topology). Each G_n is the finite (constant) k-group scheme of order p^{nh}: then $G = \varinjlim_n G_n \simeq (\mathbb{Q}_\mathbf{p}/\mathbb{Z}_\mathbf{p})^h$ is the corresponding p-divisible group of heigh h.

Viceversa, let $(G_n, i_n)_{n\in\mathbb{N}}$ be a p-divisible group according to [3.5] and, moreover, let each G_n be **discrete** when seen as an abstract group, meaning that each $G_n(R)$ is endowed with the discrete topology, if considered as a topological (abstract) group. Since from the definition (or inductively) $G_n/pG_n \simeq G_1$ for each n, then G_n is a finite discrete group with cardinality p^{hn} killed by $[p^n]$, and hence it is **free** when viewed as a $\mathbb{Z}/p^n\mathbb{Z}$-module

of rank h. Therefore we have that $G = \varinjlim_n G_n$ is isomorphic in the sense of [3.9] to $\varinjlim_n (\mathbb{Z}/p^n\mathbb{Z})^h \simeq (\mathbb{Q}_{\mathbf{p}}/\mathbb{Z}_{\mathbf{p}})^h$.

Example 3.23 A very important and significative example of p-divisible group, which shows the deep connection of this notion with abelian group schemes (or varieties), i.e. geometric objects cfr. [3.24], is the p-divisible group obtained from the **multiplicative** group scheme $\mathbb{G}_m$.

Recall that $\mathbb{G}_m$ can be seen as a k-functor of (abelian) groups: $(\mathbf{Aff})\mathbf{Sch}/S \to (\mathbf{Ab})\mathbf{Gps}$ such that $\mathbb{G}_m(T) = \mathcal{O}_T^\times(T) := (\mathcal{O}_T^\times(T),\ \cdot\ )$ as the multiplicative group of units. It is representable by:

$$\mathbb{G}_m(T) = \mathrm{Sp}_k(k[x, x^{-1}])$$

with the associated Höpf algebra given by the co-multiplication law:

$$k[x, x^{-1}] \to k[x, x^{-1}] \otimes k[x, x^{-1}], \quad x \mapsto x \otimes x$$

as we saw in [2.65]. Equivalently $\mathbb{G}_m$ is the k-functor of groups $\mathbf{Alg_k} \to (\mathbf{Ab})\mathbf{Gps}$ such that $\mathbb{G}_m(R) = R^\times$ as the multiplicative group of units.

Let now, for each $n \geq 0$, $\mu_{p^n} := \mathbb{G}_m[p^n]$ be the kernel of the p^n-power map that we write with abuse of notation as $[p^n] : \mathbb{G}_m \to \mathbb{G}_m$. Then for each $R \in \mathbf{Alg_k}$ we get the group of p^n-th roots of 1:

$$\mathbb{G}_m[p^n](R) = \mu_{p^n}(R) := \{x \in R^\times \ s.t.\ x^{p^n} = 1\}$$

or, viewing $\mathbb{G}_m$ as a k-functor from $\mathbf{Sch}/S$:

$$\mathbb{G}_m[p^n](T) := \mu_{p^n}(T) = \{f \in \mathcal{O}_T^\times(T) \ s.t.\ f^{p^n} = 1\}$$

for any scheme T over k. Clearly $\mathbb{G}_m$ is representable by:

$$\mu_{p^n}(T) = \mathrm{Sp}_k(k[x]/(x^{p^n} - 1))$$

with Höpf algebra co-multiplication:

$$k[x]/(x^{p^n} - 1) \to k[x]/(x^{p^n} - 1) \otimes k[x]/(x^{p^n} - 1), \quad x \mapsto x \otimes x$$

Finally we consider the inductive system consisting of the groups $(\mu_{p^n})_n$, with natural inclusions $i_n : \mu_{p^n} \hookrightarrow \mu_{p^{n+1}}$. Observing that, from the definition of μ_n, the conditions stated in definition [3.5] are satisfyed, we get the p-divisible group:

$$\mu_{p^\infty} = \mathbb{G}_m[p^\infty] := \varinjlim_n \mu_{p^n}$$

3.2.3 Abelian schemes

For the next example we apply a construction similar to what we did in example [3.23], to a generic abelian (group) scheme A over k. It is a very useful starting point for what will be the main discussion of the entire Chapter 4. Let us give some preliminary notions:

Definition 3.24 Let k be a field. Let A be a k-(group) scheme, viewed as a (geometrical) group scheme (cfr. [2.17]). Then:

- a **geometric point** of A (which is different from taking a point of the underlying topological space $|A|$) is a section map $\mathbf{x} : \mathrm{Spec}(K) \to \mathrm{Spec}(k)$ induced by the inclusion moprphism $k \hookrightarrow K$, for K an algebraic/separable closure of k;

- the **geometric fiber** over a geometric point $\mathbf{x}$ as before is given by the pull-back $A \times_k \mathrm{Spec}(K)$ (cfr. [2.20]) of $A \to \mathrm{Spec}(k)$ through $\mathbf{x} : \mathrm{Spec}(K) \to \mathrm{Spec}(k)$;

- a geometric fiber of A is said to be **connected** if its underlying topologycal space is connected;

- a geometric fiber of A of the form $A_K := A \times_k \mathrm{Spec}(K)$, is said to be **regular** if the stalk of the structure sheaf at each point of A_K, i.e. $\mathcal{O}_{A_K,\mathcal{P}}$, is a regular local ring, i.e. letting $\mathcal{M}$ be its unique maximal ideal, the dimension of $\mathcal{M}/\mathcal{M}^2$ as a $\mathcal{O}_{A_K,\mathcal{P}}/\mathcal{M}$-vector space is equal to the Krull dimension of $\mathcal{O}_{A_K,\mathcal{P}}$.

Definition 3.25 Let now, again, k be a commutative unital (noetherian if needed) **ring**. Let A be a k-(group) scheme, then A is said to be an **abelian scheme** over k of dimension g, if viewed as a (geometrical) group scheme (cfr. [2.13]) it is:

- **proper** over k, i.e. $A \to \mathrm{Spec}(k)$ is separated, of finite type and universally closed (cfr. [2.20]);

- **smooth**, i.e. locally of finite presentation, flat and for every geometric point $\mathrm{Spec}(K) \to \mathrm{Spec}(K(\mathcal{P}))$, the fiber $A_K := A \times_k \mathrm{Spec}(K)$ is regular (heare K is an algebraic/separable closure of the quotient field $K(\mathcal{P})$ of a prime $\mathcal{P} \in \mathrm{Spec}(A)$ cfr. [2.8]);

- the geometric fibers are **connected** of dimension g (the dimension of the local rings mentioned above [3.24]).

We showed that, whenever k is a field, varieties over k can be viewed as affine (reduced and separated) k-schemes of finite type with associated algebra the coordinate ring of the variety (cfr. [2.15]). Now thanks to [3.24] and [3.25], geometric fibers of an abelian scheme are *abelian varieties*, so that an abelian scheme can be thought as a "family" of abelian varieties "parametrized" by k. Notice that there are weakest contitions than those given in definition [3.25] in order to give to a scheme an abelian scheme structure.

Proposition/Example 3.26 Let A be an **abelian group scheme** over k of dimension g and consider, for each $n \geq 0$, the kernel of the multiplication-by-p^n map $[p^n]$:

$$A_{p^n} := A[p^n], \quad [p^n] : A \to A \tag{3.37}$$

The inductive system $(A_{p^n})_n$ form a p-divisible group of heigh $2g$ over k.

Proof. We only give an outline of the proof. For simplicity we assume that the base ring k is *noetherian*, which is the case of our interest (cfr. [3.4]). Recall that, since A is an abelian group scheme, the multiplication law defined on A is commutative. We want to show briefly that, for each n:

- A_{p^n} is a locally free group scheme of order p^{2gn}
- $[p^n]$ is an isogeny (in particular surjective and with finite dimensional kernel cfr. [3.18])

Step 1: Notice that the multiplication-by-n map for an abelian variety A, is always an isogeny. For a rigorous proof of this see for example [*J.S. Milne*, Abelian Varieties, 2022, pp. 12-14] where it is used the notion of ample sheaf. We only state the theorem in [Th1].

Step 2: Observe that $A \to \mathrm{Spec}(k)$ is a smooth (morphism of schemes cfr. [3.25]) and so it is flat. But this mean that the multiplication map $[p^n]_K : A_K \to A_K$, restricted at the level of (geometrical) fibers $A_K := A \times_k \mathrm{Spec}(K)$ (that are abelian varieties), is a flat morphism (thanks to step 1, $[p^n]$ is an isogeny and hence a finite, flat, and surjective morphism). Therefore we use flatness criterion on fibers (see [Th2], or for example [EGA, IV, 11.3.10.1]), which states that a morphism of k-schemes, with k noetherian, is flat if and only if it is flat on all its geometrical fibers. Hence we have that $[p^n] : A \to A$ is a flat morphism too, and so the kernel $A[p^n]$ is a flat scheme.

Step 3: Again from [3.25] we know that A is a proper k-scheme and so $[p^n] : A \to A$ is a proper morphism. From what observed in step 2, beeing $[p^n] : A \to A$ fiberwise an isogeny and hence a finite morphism, we have that $[p^n]$ is quasi-finite. Quasi-finiteness together with properness implies that $[p^n]$ is a finite morphism and $A[p^n]$ is a finite scheme. (We are using the following result stated in [Th3]: a morphism of schemes is finite if and only if it is quasi-finite and proper; see [EGA, IV, 3] for a detailed proof).

Step 4: We proved that $A[p^n]$ is a finite flat group scheme (moreover since A is finitely presented, it is finitely presented too) and hence it is a (projective and so) locally free group scheme over k.

Step 5: The map $[p^n]$ is fiberwise surjective, always thanks of the fact that $[p^n]_s$ is an isogeny, and hence $[p^n]$ surjective too. We can conclude that $[p^n]$ is an isogeny ([3.18]).

Step 6: About the dimension of $A[p^n]$ (being the kernel of $[p^n]$) we can say that: since fiberwise the map $[p^n]$ is such that $A[p^n]_K = \ker([p^n]_K)$ is a finite group scheme of dimension $(p^n)^{2\cdot \dim A}$ (again thanks to the analogous theorem for abelian varieties), then we can conclude that $A[p^n]$ is a locally free group scheme of order $p^{n\cdot 2g}$.

Step 7: In conclusion

$$A(p) := \varinjlim_n A_{p^n} = \varinjlim_n A[p^n] \tag{3.38}$$

is the p-divisible group of heigh $2g$ associated to A. □

In order to give a more complete description we write down, without proving them, the statements mentioned in the intermediate steps of the previous proof.

Isogeny Theorem (for varieties): Let A be an abelian variety of dimension g, and let n > 0 be an integer. Then $[n]$ is an isogeny of degree n^{2g}.

Fibral criterion of flatness (base version): Let $\sigma : R \to A$ and $\rho : A \to B$ (local) homomorphisms between local noetherian rings and let $M \neq 0$ be a B-module of finite type. Let k be the residue field of R, then the following are equivalent:

- the R-module M is flat and the $A \otimes_R k$-module $M \otimes_R k$-module is flat;
- the A-module M is flat and the R-module A is flat.

Quasi-finiteness theorem (and definition): A **quasi-finite** morphism of schemes $f : X \to \mathrm{Spec}(k)$ (i.e. of finite type and such that every geometrical fiber $X \times_k \mathrm{Spec}(K)$ is a finite discrete set) which is also proper then is finite. Also the converse is true.

Example 3.27 In order to complete the discussion we made about p-divisible groups associated to abelian schemes, we can be more explicit when dealing with an *abelian variety* A over an algebraically closed field k, of dimension: $\dim A = g$. In particular it can be shown that:

- if $\mathrm{char}(k) \neq p \;\Rightarrow\; A(k)[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^{2\cdot g}$,
- if $\mathrm{char}(k) = p \;\Rightarrow\; A(k)[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^r$ for $0 \leq r \leq g$

where by $A(k)$ we mean the functor of points: $\mathrm{Hom}_{k-funct}(\mathrm{Spec}(k), A)$, or equivalently, if A is such that $\mathrm{Spec}(\mathcal{O}_A(A)) = \mathrm{Spec}(k[X_1, ..., X_n]/\mathcal{I})$, then $A(k) := \{\underline{x} \in k^n | f(\underline{x}) = 0 \text{ for all } f \in \mathcal{I}\}$. (cfr. [2.7], [2.15]).

As a consequence the respective (associated) p-divisible groups become:

- $\varinjlim_n A(k)[p^n] \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{2g}$
- $\varinjlim_n A(k)[p^n] \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^r$

We will treat this in detail discussing different cases for 1-dimensional abelian varieties, i.e. **elliptic curves**.

3.2.4 Constant and étale schemes

We conclude with an example that will be more clear in the context of k-formal schemes that we are going to introduce in the next section. Along this subsetion let k be a **field**. We briefly recall some important notions coming from previous chapter.

Remark 3.28 Recall that:

- a **constant** (affine) k-scheme is a k-scheme X such that $X \simeq \mathrm{Spec}(k)^{|X|}$; (cfr. [2.66])
- an **étale** (affine) k-scheme is a k-scheme X such that $X \times_k \bar{k}$ (or k^s) is constant; (cfr. [2.66])
- there exist an equivalence between the category of **étale k-schemes** and that of **π-sets**, being $\pi = \mathrm{Gal}(k^s/k)$ the Galois group of a separable extension of k; (cfr. [2.66])
- there exist an equivalence between the category of **étale k-group schemes** and that of **π-groups**; (cfr. [2.66])
- there exist a canonical exact sequence: $0 \to G^0 \to G \to G_{\acute{e}t} \to 0$, where G^0 is the connected component of G, and $G_{\acute{e}t} := \pi_0(G) = G/G^0$ is the étale fundamental group, such that $G_{\acute{e}t} = G(\bar{k})$.

Example 3.29 Let $G = (G_n)_n$ be a p-divisible group. Then there exist an exact sequence of p-divisible groups:

$$G^0 = \varinjlim_n G_n^0 \to G \to G_{\acute{e}t} = \varinjlim_n G_{\acute{e}t,n} \tag{3.39}$$

obtained from an inductive system of exact sequences, passing to the limit thanks to an argument analogous to [3.7].

3.2.5 Cartier dual of p-divisible group

We apply what we introduced in section 2.2.4, in order to deduce the *Cartiér dual* of a p-divisible groups.

Example 3.30 Let (G_n, i_n) be a p-divisible group and consider the Cartiér dual of each group G_n, i.e. $\mathtt{D}(G_n)$. Then thanks to the diagram:

$$\begin{array}{ccccccccccc} & & & & & & G_1 & & & & \\ & & & & & \overset{j_{n,1}}{\nearrow} & & \overset{i_{1,n}}{\searrow} & & & \\ 0 & \longrightarrow & G_n & \xrightarrow{i_n} & G_{n+1} & & \xrightarrow{[p^n]} & & G_{n+1} & \xrightarrow{j_{1,n}} & G_n & \longrightarrow & 0 \end{array} \tag{3.40}$$

(where $i_{1,n}$ is surjective and $j_{n,1}$ is injective) we have immersions $\mathtt{D}(j_{1,n}) : \mathtt{D}(G_n) \to \mathtt{D}(G_{n+1})$, so that the system $(\mathtt{D}(G_n), \mathtt{D}(j_{1,n}))$ is again a p-divisible group (of the same

heigth).

As an example consider the constant p-divisible group of heigth 1, i.e. the p-divisible group $(\mathbb{Z}_p/\mathbb{Q}_p)$. Then its natural Cartiér dual is given, thanks to the above diagram, considering the torsion subgroups of each $\mathbb{Z}/p^n\mathbb{Z}$, which is the n-th element of the inductive system of Example [3.22], so that we get:

$$\varinjlim_n \mathtt{D}(\mathbb{Z}/p^n\mathbb{Z}) \simeq \varinjlim_n \mathbb{G}_m[p^n] \simeq \varinjlim_n \mu_{p^n} = \mu_\infty \tag{3.41}$$

3.3 Formal groups and p-divisible groups

In this section our main purpose is to show some relations between k-formal group (schemes) introduced in the previous Chapter 2, and p-divisible groups. In order to do this let k be a noetherian (local when needed) pseudocompact ring or a (topological pseudocompact) field of characteristic $p \neq 0$. Whenever k is a field, let $\pi = \mathcal{G}(k_s/k)$ be the Galois group of k_s/k (for a finite separable field extension k_s of k).

Frist of all recall that a formal k-scheme X is a functor $PM_k \to \mathbf{Set}$ that commutes with filtrant projective limits and such that $X \simeq \mathrm{Spf}_k A$, where A is a profinite k-algebra (in this case k can be considered as a general artinian pseudocompact ring). X can be equivalently considered as the inductive limit $\varinjlim_i \mathrm{Spf}_k A_i$ where A_i are **finite** topological k-algebras. Hence thanks to the observations made in Theorem [2.72] and in the discussion that follows it (i.e. the equivalence between topological projective k-modules and projective k-modules without topology), a formal k-scheme can be viewed as the inductive limit of a system of **finite** k-algebras $\varinjlim_i \mathrm{Sp}_k A_i^{\#}$.

3.3.1 p-divisible groups and formal p-groups

We first start with a classical definition of (formal) p-divisible groups (that can be found for example in Demazure [De]) and then we show that this is actually the definition given by Grothendieck ([3.12]). This will clarify what already said about the fact that a p-divisible group is a "limit" of group schemes rather than a group scheme itself.

Definition 3.31 A (commutative) k-formal group G, is said to be p-**divisible**, or it is said to be a **Barsotti-Tate** group, if it satisfy:

(i) the (multiplication-by-p) map $[p] : G \to G$, is an epimorphism;

(ii) G is a p-torsion group, i.e. $G \simeq \varinjlim_n G[p^n] := \varinjlim_n \ker(G \xrightarrow{[p^n]} G)$;

(iii) $\ker(G \xrightarrow{[p]} G)$ is finite (and locally free) as k-scheme.

Proposition 3.32 The Definition [3.31] above is equivalent to the datum of an inductive system:

$$G_1 \xrightarrow{i_1} G_2 \xrightarrow{i_2} G_3 \xrightarrow{i_3} ... \tag{3.42}$$

where the G_i are finite (locally free) k-groups (schemes), such that:

- rank(G_i)=$p^{h\cdot i}$, for $h \in \mathbb{N}$;
- there is an exact sequence $0 \to G_n \xrightarrow{i_n} G_{n+1} \xrightarrow{[p^n]} G_{n+1}$.

Proof.

First of all notice that in this case the main difference from the definitions given in the previous subsections is that we are starting from k-formal schemes, i.e. inductive limits of representable formal k-functors $FM_k \to \mathbf{Gps}$. However, thanks to the remarks made previously, to give a formal k-group (scheme) that is p-torsion, i.e. $G \simeq \varinjlim_n G[p^n]$, and s.t. the $G[p^n]$'s are finite, means to give a k-formal group scheme $G \simeq \varinjlim_n \mathrm{Spf}_k A_n$, where A_n is the associated finite (formal) k-(bi)algebra of each $G[p^n]$; and this is equivalent to have an inductive system of finite affine k-schemes $G_n := (G[p^n])^{\#}$ of rank(G_n) =rank[ker$(G \xrightarrow{[p^n]} G)] = p^{h\cdot n}$; the latter thanks to the fact that $[p]$ is an epimorphism and so $G[p]$ must have order p^h for some $h \in \mathbb{N}$. If k is a pseudocompact artinian ($\Rightarrow$ noetherian) ring instead of a field, then we have to add the property that the k-group schemes are *projective*, which is the same of asking that they are *locally free/flat.*

□

We have seen that p-divisible groups can be considered as formal k-groups that satisfy some properties. Now let us go a bit backforeward and show in detail some constructions behind this equivalence. Firstly we give another definition of the Frobenius and the Verschiebung morphisms, when considered as functors between k-group schemes.

Definition 3.33 The **Frobenius** morphism on a k-group scheme G, is defined as the morphism of group schemes $F_G : G \to G^{(p)}$, induced by the map between the associated algebras $\mathcal{O}(G) \to \mathcal{O}(G)$, given by $f : x \mapsto x^p$. The group $G^{(p)}$ is given for each $R \in \mathbf{Alg_k}$, by $G^{(p)}(R) := G(R_{[f]})$ where $R_{[f]}$ is the k-algebra obtained by the scalar restriction of k induced by f: $k \ni x \mapsto x^p \in k^p$ (notice that this construction is possible since the functor F defined on k-schemes commutes with products so that it preserves the k-groups structure). Let G be commutative, so that $\mathtt{D}(G^{(p)}) = \mathtt{D}(G)^{(p)}$, then the **Verschiebung** morphism is the unique morphism $V_G : G^{(p)} \to G$ such that $\widehat{\mathtt{D}(V_G)} = F_{\widehat{\mathtt{D}(G)}}$. (Were the wedge symbol denote the completion we defined for a k-scheme in Proposition [2.48]).

Definition 3.34 A **connected** (or local) formal k-group is a formal group $G := \mathrm{Spf}_k A$ such that $G(K) = 0$ for every field K; equivalently its associated k-formal algebra A is a **local** (noetherian topological profinite) ring; this is clear since:

$$\mathrm{Hom}_{ring}(A, K) = \mathrm{Hom}_{ring}(A_{\mathfrak{M}}, K_{\mathfrak{M}} = 0) \tag{3.43}$$

Moreover G is connected if and only if $G = G^0 = \varinjlim_n(\ker F_G^n)$ where $F_G^n : G \to G^{(p^n)}$ is the n^{th}-composition of the Frobenius morphism.

Definition 3.35 A (commutative) formal k-group G is called **formal p-group** if it can be identifyed with the inductive limit $\varinjlim_n G[p^n] := \varinjlim_n \ker(G \xrightarrow{[p^n]} G)$ (if k is only a pseudocompact artinian ring then the $G[p^n]$'s need also to be flat groups).

Definition 3.36 A (commutative) formal p-group G is called **p-divisible (formal) group** if $[p] : G \to G$ is surjective (if k is only a pseudocompact artinian ring then $[p] : G \to G$ is required to be faithfully flat i.e. surjective and flat) and $G[p]$ is a finite (flat) group of order p^h, in this case h is said to be the **height** of G.

Remark 3.37 The conditions of the definition above, i.e. that $[p]$ must be surjective (faithfully flat) and that $\ker G[p]$ must be finite, are equivalent to requiring $[p]$ to be an *isogeny*.

By definition and thanks to previous Remark [3.37]: if a formal k-group is connected then it is a formal p-group, hence if $G = G^0 \times G_{\acute{e}t}$, then G is a formal p-group if and only if $G_{\acute{e}t}$ is formal p-group and as a consequence of this, a connected formal group G is p-divisible if and only if $[p] : G \to G$ is an isogeny.

We can now rephrase what already written at the beginning of the section.

Theorem 3.38 There is an equivalence between the category of Barsotti-Tate groups $\mathbf{BT}_p(k)$ as defined in the previous section, and the category of formal p-divisible group schemes.

We have shown that what we called Barsotti Tate groups (or p-divisible groups) in the previous sections, are actually p-divisible formal groups, i.e. formal p-groups such that $[p] : G \to G$ is an isogeny, and we also worked out that if G is connected (as a formal group) it is always a formal p-group (i.e. p-torsion), so that for connected formal groups it is sufficient (and necessary) that $[p] : G \to G$ is surjective and with finite kernel in order to be a p-divisible group. We can go a step further and prove a much more interesting equivalence.

3.3.2 Formal power series, formal Lie groups

We start with some definitions, in order to show the connection between the objects involved. Then we prove an important result due to Tate which clarify the relationship between p-divisible groups and formal Lie groups. Let k be a field as before (or a noetherian local pseudocompact ring) with characteristic $p \neq 0$.

Definition 3.39

- A *connected* (i.e. local) formal (commutative) k-group scheme is said to be **of finite type** if $G = \mathrm{Spf}_k A$ and A is a noetherian ring (i.e. it is finitely generated as a formal k-algebra);
- a *connected* (i.e. local) formal (commutative) k-group scheme is said to be **smooth** if its associated algebra is a power-series algebra: i.e. $A \simeq k[\![X_1, ..., X_n]\!]$.

In the whole section G is a connected smooth k-formal group, so that $G = \mathrm{Spf}_k A$, with $A = k[\![X_1, ..., X_n]\!]$. Recall that, as written in Definition [2.37], a *finite* formal k-group $G = \mathrm{Spf}_k A$ means that A is a finite formal k-algebra, and so that it is finite as (topological) k-module and hence both of finite length and profinite. This is different from A being *of finite type*, which means that A is only finitely generated as k-algebra.

Clearly, if $A = k[\![X_1, ..., X_n]\!]$ is the associated algebra of a smooth formal k-group, then the co-product map $\Delta : A \to A\widehat{\otimes}A$ is given by:

$$\Phi(\underline{X}, \underline{Y}) := (\Phi_1(X_1, ..., X_n; Y_1, ..., Y_n), ..., \Phi_n(X_1, ..., X_n; Y_1, ..., Y_n)) \tag{3.44}$$

satisfying:

- $\Phi(\Phi(\underline{X}, \underline{Y}), \underline{Z}) = \Phi(\underline{X}, \Phi(\underline{Y}, \underline{Z}))$
- $\Phi(0, \underline{X}) = \Phi(\underline{X}, 0) = \underline{X}$
- (commutativity) $\Phi(\underline{X}, \underline{Y}) = \Phi(\underline{Y}, \underline{X})$

where $\Phi(\underline{X}, \underline{Y}) = \underline{X} + \underline{Y} +$ higher order terms; the inversion σ is obtained from these axioms, and one has $\Phi(\underline{X}, \sigma(\underline{X})) = \Phi(\sigma(\underline{X}), \underline{X}) = 0$ (for a proof of this see for example [St], 10).

Definition 3.40 Let k be a noetherian local (topological) pseudocompact ring with residue field of characteristic $p > 0$. A **formal Lie group** over k of dimension n is a connected and smooth formal k-group such that its associated formal k-algebra A is isomorphic to $k[\![X_1, ..., X_n]\!]$.

Now we are ready to state and give an outline of the proof of the following:

Theorem 3.41 Let k be a local noetherian (pseudocompact) ring with residue field of characteristic $p > 0$. Then there exists an equivalence between the category of connected (formal) p-divisible groups and that of commutatve p-divisible formal Lie groups over k.

Proof. We only give an idea of the outline of the proof (see [St] for details).

Step 1: We write X instead of $\underline{X}$. Let $A = k[\![X_1, ..., X_n]\!]$ and $G := \mathrm{Spf}_k A$ be a commutative Lie formal group. Then G is said to be p-divisible if the multiplication map $[p] : G \to G$ is, as always, is an isogeny. This means that the map $\psi : A \to A$ given by:

$$\psi(X) = \overset{\text{p-times}}{\Phi(X, \Phi(X, \Phi(X, ...)))} = X + (X + ...) \tag{3.45}$$

turns A into a free (finitely generated) A-module, i.e. a ring with a basis.

Step 2: Using similar considerations to what we did in Proposition [2.17] (but also for the costruction of the p-divisible groups of abelian schemes in [3.26]), given the formal Lie group G we can consider $G(p) := \ker([p])$. The last one is a p-divisible connected formal group if $[p]$ is an isogeny. Indeed $\ker([p])$ is a connected finite (flat) group scheme of order p^h thanks to considerations similar to those we made for example in [2.17], and so (by induction) we have an inductive system of connected finite (flat) group schemes of order p^{nh}. Equivalently the group schemes $G_n := G[p^n]$ are such that $\mathcal{O}(G_n) = A/\psi^n(I)A$ (where ψ^n means the n^{th}-composition of ψ) and $I := \ker(\varepsilon : A \to k) \simeq (X_1, ..., X_n)$. (Here ε is also called the *augmentation*). Each $\mathcal{O}(G_n)$ is local and $(G_n)_n$ is an inductive system of connected group schemes.

Step 3: Now consider the unique maximal ideal $\mathfrak{M}$ of k. Then $\mathfrak{M}A + I$ is a maximal ideal for the k-formal algebra A. From above considerations the algebra:

$$A_n := \mathcal{O}(G_n) = A/\psi^n(I)A$$

is a finite (flat) k-algebra and hence it is complete for the $\mathfrak{M}$-adic topology, with a fundamental system of neighbourhoods given by $(\mathfrak{M}^n + \psi^n(I))A$; indeed we have local artinian rings:

$$A/(\mathfrak{M}^n + \psi^n(I))A = A_n/\mathfrak{M}^n A_n$$

and so $(\mathfrak{M}A + I)^k \subseteq (\mathfrak{M}^n + \psi^n(I))$ for sufficiently big k. Moreover,

$$\psi(X_i) = pX_i + \text{higher order terms}$$

therefore we have $\psi(I) = pI + I^2 \subseteq (\mathfrak{M}A + I)I$, and by induction:

$$\psi^n(I) \subseteq (\mathfrak{M}A + I)^n I \subseteq ... \subseteq (\mathfrak{M}A + I)I$$

and so the ideal $\psi(I)$ becomes arbitrarily "smaller" with (the growth of) n. Hence:

$$\varprojlim_k A/(\mathfrak{M}A + I)^k = \varprojlim_n A/(\mathfrak{M}^n + \psi^n(I)) = \varprojlim_n A_n/\mathfrak{M}^n A_n = \varprojlim_n A_n$$

from which we get a bijection $A \to \varprojlim A_n$, and we can conclude that the functor:

$$G \mapsto G_p = \varinjlim G_n$$

is fully faithful and G_p is called the p-divisible group associated to the Lie group G.

Step 4: Now let $G_p := (G_n, i_n)_n$ be a connected p-divisible formal group as in the second definition we gave ([3.32]). We want to show that G_p is the associated p-divisible group to a formal Lie group G. In order to do this it would be sufficient that, being $G_n := \mathrm{Sp}_k A_n$, then $A = \varprojlim_n A_n \simeq k[\![X_1, ..., X_n]\!]$. In this case we would be done since we would have a projective system of connected finite flat group schemes $(G_n)_n$ of order p^{nh}, and letting $G := \varinjlim_n G_n$, thanks to considerations as in proof of Proposition [3.32], $[p]$ would be an isogeny, so that $G := \varinjlim_n \ker([p^n])$ would be a commutative, connected, p-divisible, smooth formal k-group.

Step 5: Now we proceed with an argument similar to that of Proposition [2.40], where we showed the commutativity with filtrant projective limits as a characterisation of formal k-schemes. So recall that k is a noetherian local pseudocompact ring; let $G_n := \mathrm{Sp}_k A_n$ and $G := \mathrm{Spf}_k A$, such that $A = \varprojlim A_n$ as a complete profinite k-algebra. But each A_n is a finite flat (equiv. free) algebra; hence thanks to the maps $j_n : A_{n+1} \twoheadrightarrow A_n$ coming from the maps $i_n : G_n \to G_{n+1}$ for $n \in \mathbb{N}$, and to the finiteness of the A_n, we get $\varprojlim A_n = \varprojlim A'_n$ where $A'_n = \bigcap_{m \geq n} j_{m,n}(A_m) = A_{m_n}$ for a suitable m_n; and the $j_{m,n}$ are surjective too so that $p_n : \varprojlim A_n \to A_n$ is surjective. Now using the fact that each A_n is free of rank n, we immediately get $A = \varprojlim A'_n = \prod_n k \simeq k[\![T]\!]$. We can also conclude that A is hence (topologically) flat. But hence the composition:

$$k[\![X_1, ..., X_n]\!] \xrightarrow{\varphi} k[\![T]\!] = A \twoheadrightarrow A_n$$

where φ is a continuous homomorphism, is surjective too.

Step 6: Now we use the fact that $\mathbb{N}^3$ is a filtrant category/set (that is cofinal) and we can apply the Mittag-Leffler conditions (see [1.48], *(iv)* for details), and so projective limits inexed by $\mathbb{N}$ preserve exact sequences. In particular, the exact sequence of modules of finite length, setting $M_{i,j} := (\mathfrak{M}^i k[\![X_1, ..., X_n]\!] + I^j)$:

$$0 \to M_{i,j} + \ker(p_n)/M_{i,j} \to k[\![X_1, ..., X_n]\!]/M_{i,j} \to A_n/M_{i,j}A_n \to 0$$

for $I = (X_1, ..., X_n)$, remains exact after applying $\varprojlim_{i,j,n}$ and gives:

$$0 \to k[\![X_1, ..., X_n]\!] \xrightarrow{\varphi} A \to 0$$

and thus φ is a bijection.

Step 7: Now we may suppose that k is a field with characteristic $p > 0$, since from a bijection like φ in the previous step, and quotienting with $\mathfrak{M}$, we get again a bijection.

Step 8: Now we can define $H_n := \ker(F^n : G_t \to G_t^{(p^n)})$ and for $t >> 0$, since $V^n \circ F^n = [p^n]$, we get $H_n \subset G_n$. Conversely since G has finite Frobenius heigth then

$G_n \subset H_n$. So that passing to the limit, their associated algebras coincide:

$$\varprojlim_n A_n = \varprojlim_n B_n \tag{3.46}$$

for $G_n = \mathrm{Sp}_k A_n$ and $H_n = \mathrm{Sp}_k B_n$. Now with a dimensional argument (see [St], pp. 61-62) it can be shown that:

- taken elements $X_1, ..., X_n \in I := \varprojlim I_n$, where I_n is the augmentation ideal of B_n, such that they form a basis of I_1/I_1^2, for each $n \geq 0$ and since the sequence $0 \to H_1 \to H_n \xrightarrow{F} H_n^{(p)}$ is exact, then we find isomorphisms $I_1/I_1^2 \simeq I_n/I_n^2$.
- the elements $X_1, ..., X_h$ form a basis of I_n for each n, so that the surjective maps:

  $$k[\![X_1, ..., X_h]\!]/(X_i^{p^n}) \twoheadrightarrow B_n \tag{3.47}$$

  for each $0 \leq i \leq h$, when taken to the limit give:

  $$k[\![X_1, ..., X_h]\!] \to \varprojlim B_n \simeq A \tag{3.48}$$

- by induction, since the cardinality of H_1 is $p^h = \dim_k B_1$, it can be proven that the sequence:

  $$0 \to H_1 \to H_n \xrightarrow{F} H_{n-1}^{(p)} \to 0 \tag{3.49}$$

  is exact (thanks to the properties of F and V). Therefore the cardinality of each H_n equals $p^{hn} = \dim_k B_n$ and we can conclude the proof of the theorem.

□

We conclude with a characterization of p-divisible groups, whose proof can be found for example in [De], II.11.

Proposition 3.42 A formal k-group G is a p-divisible formal group if and only if it satisfies:

- G^0 is of finite type, it is smooth and $\ker(V : (G^0)^{(p)} \to G^0)$ is finite;
- $\pi_0(G)(\bar{k}) = G_{\acute{e}t}(\bar{k}) \simeq (\mathbb{Q}^p/\mathbb{Z}^p)$

where $V : (G^0)^{(p)} \to G^0$ is the Verschiebung morphism, and G^0 the connected component of G.

3.3.3 Dieudonné modules and p-divisible groups

In this section we apply some concepts introduced at the end of the previous chapter, such as Witt vectors and Dieudonné rings, in order to show another important connection between those objects and p-divisible groups. For this purpose let k be a perfect field of characteristic p along the whole section. Moreover, let $W(k)$ be the ring of Witt vectors (over k) and $W[F, V]$ the Dieudoinné ring over k sucht that if τ is an automorphism

between k, then letting $\tau(F) = F$ and $\tau(V) = V$, it is again an automorphism of $W[F, V]$. Whenever clear from the context we write W instead of W_k and CW instead of CW_k; W_n means the truncated Witt ring as in definition [2.93].

Consider the category of $W(k)$-modules, and observe that on each $W_n(R)$ (that are $W(k)$-modules for each $R \in \mathbf{Alg_k}$ thanks to [2.107]) there are $W(k)$-modules homomorphisms $V_n : W_n(R) \to W_{n+1}(R)$; starting from this we introduce the important notion of Dieudonné modules as functors.

Definition 3.43 Let G be a commutative affine k-group, if G is **unipotent**, i.e. it is the corresponding dual of a formal connected k-scheme, through $G \mapsto \widehat{\mathtt{D}(G)}$, then we can define a functor $M : G \mapsto M(G) := \mathrm{Hom}_{k-fnct}(G, \varinjlim_n W_n) = \mathrm{Hom}_{k-fnct}(G, CW^u)$. Clearly $M(G)$ has a $W(k)$-module structure thanks to the $W(k)$ action on each W_n, so that M is a contravariant functor between the category of affine unipotent k-schemes and that of $W(k)$-modules, and its called **Dieudonné module** of G. Indeed $M(G)$ can be viewed as a D_k-module by letting $F, G : M(G) \to M(G)$ be such that $F(w \cdot m) = w^p F(m)$ and $V(w^p \cdot m) = wV(m)$, for $w \in W(k)$ and $m \in M(G)$.

In the definition above we denoted with w^p the absolute frobenius $F_k : W(k) \to W(k)$ which is an automorphism since k is perfect, and with $F : M(G) \to M(G)^{(p)}$ and $V : M(G)^{(p)} \to M(G)$ the Frobenius and Verschiebung morphisms coming from $F_G : G \to G^{(p)}$ and $V_G : G^{(p)} \to G$, defined as in [3.33]. Notice that $M(G)^{(p)} = M(G^{(p)})$. Hence we are using relations given in definition [2.107] of Dieudonné ring. We state without proving the folloing:

Theorem 3.44 The functor M induces an antiequivalence between the category of commutative affine unipotent k-group schemes and the category of all D_k-modules of V-torsion. Moreover if G is a finite k-group scheme then $M(G)$ is a D_k-module of finite length.

The proof is based on the fact that, from the definition, it turns out that the monomorphisms $V_m : W_m \to W_{m+1}$ gives injective maps $\mathrm{Hom}_{k-fnct}(G, W_m) \to \mathrm{Hom}_{k-fnct}(G, W_{m+1})$ and clearly $\mathrm{Hom}_{k-fnct}(G, W_m) = \{m \in M(G) | V^n(m) = 0\}$. For details see ([Fo], II).

We can go a step further and define the dual functor M^*:

Definition 3.45 For any D_k-module M let $M^* := \mathrm{Hom}_{W(k)-mod}(M, \varinjlim_n W_n)$ such that for each $f \in M^*$ we have $F(f)(m) = f(V(m))^p$ and $V(f)(m) = (F(m))^{p^{-1}}$. So that we have an auto-duality of D_k-modules of finite length over $W(k)$. M^* is called **dual Dieudonné module** of M.

We now state without proving the main theorem of this section, and we give some hints of the main structure of a proof.

If G is a finite (affine) k-group scheme of p-torsion, i.e. such that $G := \varinjlim(\ker[p^n])$ and it is of rank p^h (or equiv $\ker[p]$ is finite), then it can be written uniquely as $G \simeq G_1 \times G_2 \times G_3$, such that G_1 is finite unipotent infinitesimal, G_2 is finite unipotent étale and G_3 is finite infinitesimal multiplicative. (See [De], II for details).

Theorem 3.46 The functor $G \mapsto M(G)$ is an antiequivalence between the category of all finite (affine) k-groups of p-torison and the category of D_k-modules with finite $W(k)$-length. Moreover M is such that, denoting F, V the morphisms induced by F_G, V_G on M:

(i) $F(wm) = w^p F(m)$, $wV(m) = V(w^p m)$, $F(V(m)) = V(F(m)) = p \cdot m$;

(ii) G is étale/infinitesimal/unipotent/multiplicative if and only if F is (respectively) an isomorphism/F is nilpotent/V is nilpotent/V is an isomrphism;

(iii) $\text{rank}(G) = p^{\text{length}(M(G))}$;

(iv) there exists a natural isomorphism $M^*(G) \simeq M(\mathtt{D}(G))$.

Proof. For an idea of the proof consider that:

- the equivalence is quite trivial for the unipotent component, thanks to previous theorem on unipotent groups, since if G is unipotent infinitesimal (resp. étale) then $M(G)$ is a finite length D_k-module, F is clearly bijective (becouse G is p-torsion) and $M(G)$ is killed by a power of V (resp. it is also killed by a power of F).

- As a consequence $\text{rank}(G) = p^{\text{length}(M(G))}$.

- Again if G is p-torsion unipotent infinitesimal then we can see that $M(G) = \text{Hom}_{k-fnct}(G, \ker(F^n : W_n \to W_n))$ and hence $M(\mathtt{D}(G)) = \text{Hom}_{k-fnct}(\mathtt{D}(G), \ker(F^n : W_n \to W_n))$.

- So we can define a map $f : M(\mathtt{D}(G)) \to M^*(G)$ starting from a map $\mathtt{D}(G) \to \ker(F^n : W_n \to W_n)$ wich gives a map $\ker(F^n : W_n \to W_n) \to \mathtt{D}(\ker(F^n : W_n \to W_n)) \to \mathtt{D}(\mathtt{D}(G)) \simeq G$; and this shows that the map f is an isomorphism. And for infinitesimal unipotent groups we are done.

- If G is infinitesimal multiplicative then define $M(G) := M^*(\mathtt{D}(G))$. One can give an explicit description of this module in terms of Galois modules and using the action of the Galois group π.

- Using the Cartiér duality between étale unipotent and infinitesimal multiplicative groups, and using the first step of this outline, by duality, we get that there is an antiequivalence between the category of multiplicative infinitesimal groups and D_k-modules of finite length where V gives a bijection and F is nilpotent.

□

A complete proof of the theorem can be found using both [De] and [Fo]. Now we focus on the theorem which gives an equivalence between categories involving our main object of study: p-divisible groups.

We now define an intermediate notion for a (finite - commutative) formal k-group scheme G, between being a formal p-group and a formal p-divisible group.

Definition 3.47 A formal k-group is said to be a (formal) p-**torsion** group if it satisfies:

(i) $G := \varinjlim_n \ker([p^n] : G \to G)$;

(ii) $\ker([p] : G \to G)$ is a finite group.

as a consequence, letting $G(n) := G[p^n] = \ker([p^n] : G \to G)$ we have exact sequences:

$$0 \to G(n) \to G(n+1) \xrightarrow{[p^n]} G(n+1) \tag{3.50}$$

$$0 \to G(n) \to G(n+m) \xrightarrow{[p^n]} G(m) \tag{3.51}$$

hence we define the associated Dieudonné module: $M(G) := \varprojlim_n M(G(n))$.

We are ready to state the equivalence involving p-torsion groups thanks to the Dieudinné functor M; as before we give a brief outline of the proof.

Theorem 3.48 The Dieudonné functor $G \mapsto M(G)$ gives an antiequivalence between the category of p-torsion formal k-groups and the category of D_k-modules that are finitely generated as $W(k)$-modules and such that the Frobenius and the Verschiebung are endomorphisms of M satisfying:

$$F(wm) = w^p F(m), wV(m) = V(w^p m), F(V(m)) = V(F(m)) = p \cdot m \tag{3.52}$$

Clearly to be a p-divisible formal group means to be a p-torsion group where $[p]$ is moreover an epimorphism (surjective in this case, while we needed faithfully flat when k is a topological pseudocompact ring noetherian and local). Hence we immediately have the following:

Corollary 3.49 Let G be a formal p-torsion group, then G is a finite (formal k-scheme) if and only if $M(G)$ is a finite* D_k-module (*topologically, if considering the p-adic topology; so in this case we mean profinite and of finite length and hence it coincide with the above definitions). Moreover, G is p-divisible if and only if $M(G)$ is free as D_k-module (i.e. it admits a basis), and $ht(G) = \dim M(G)$.

Proof. The proof of Theorem [3.48] is based on the following result that we write in steps:

Step 1: ($\Rightarrow$): we proceed as follows dividing this part in two more subsections:

Substep 1: if G is a p-torsion formal group, let:

$$M_n := M(G(n))) = M(\ker([p^n] : G \to G)) \tag{3.53}$$

Then $(M_n)_n$ is a projective system of $W(k)$-modules such that: M_n is finite for all n, being $\ker([p^n] : G \to G)$ finite (inductively by definition of p-torsion), and:

$$M_{n+1} \xrightarrow{M([p^n])} M_{n+1} \xrightarrow{M(i_n)} M_n \to 0 \tag{3.54}$$

is an exact sequence obtained from the exact sequence of (finite) k-group schemes:

$$0 \to G(n) \xrightarrow{i_n} G(n+1) \xrightarrow{[p^n]} G(n+1) \tag{3.55}$$

($[p^n]$ is the multiplication map and i_n the injective morphism representing a closed immersion). From now on $M = M(G)$. But then we get exact sequences:

$$M_{n+m} \xrightarrow{M([p^n])} M_{n+m} \xrightarrow{M(i_n \circ ... \circ i_{m-1})} M_n \to 0$$

and we can pass them to the limit $\varprojlim_m$, (we can do it again thanks to the Mittag-Leffler condition as we did in the proof of the theorem of the previous section), since $M_{n+1} \to M_n$ is surjective, and we get:

$$M \xrightarrow{M([p^n])} M = \varprojlim_m M_m \twoheadrightarrow M_n \to 0$$

where the second map is the canonical projection. As a consequence:

$$M_n \simeq M/p^n M$$

for each $n \in \mathbb{N}$.

Substep 2: Now $M_1 = M/pM$ is a finite length (so finitely generated) $W(k)$-module and we take $m_1, ..., m_s \in M$ s.t. $\overline{m_i}$ are generators of M_1 mod.p. Then thanks to the surjection $W(k)^s/pW(k)^s \to M_1$ we get surjections $W(k)^s/p^n \to M_n$ for each n and hence we get a sucrjection $W(k)^s \to M$ when passing to the limit. We conclude that:

$$M_n \simeq M(G)/p^n M(G) \tag{3.56}$$

and $M(G)$ is a finitely generated $W(k)$-module.

Step 2: ($\Leftarrow$): conversely, let M be a finitely generated D_k-module that can be viewed as a Dieudonné functor, then set $G := \varinjlim_n G_n$ where $M(G_n) := M/p^n M$ and the thesis follows. □

The purpose is now to define a "formal" Dieudonné module as a contravariant functor of formal k-groups with target the formal functor that we can obtain from the ring of Witt

vectors.

Definition 3.50 Let CW_k be the ring of Witt covectors over k. Then $CW_{(-)} : k \mapsto CW_{(k)}$ is a k-functor of groups in $\mathrm{Fnct}(\mathbf{Alg_k}, \mathbf{Gps})$. If k is a pseudocompact topological ring (or field as in this section) then we denote as $\widehat{CW_k}$ the **completion**, as a k-algebra, of the ring of Witt covectors over k. We define also the completion $\widehat{D_k} = \varprojlim_n D_k/p^n D_k$ for the p-adic topology.

Remark 3.51 The completion $\widehat{CW_k}(R) = CW_k(R)$ can be considered as a topological $\widehat{D_k}$-module, for each $R \in PM_k$. It can be proven that one has $\widehat{D_k} \simeq \mathrm{End}_{k-f.fnct,cont}(\widehat{CW_k})$. The prove is based on the fact that the unipotent completion $\widehat{CW_k}^u(R)$ is dense in $\widehat{CW_k}(R)$ for each R, and this ring can be espressed through an inverse limit. For a detailed proof se [Fo], II. Both D_k and $\widehat{D_k}$ are subrings of $\mathrm{End}_{k-f.fnct,cont}(\widehat{CW_k})$. Furthermore, since $\widehat{CW_k}(R)$ is espressed through a direct limit, hence it is a formal p-group, namely $\widehat{CW_k}(R) := \mathrm{Spf}_k A$ where A is the formal k-algebra obtained from the completion of the formal algebra:

$$k^0[\![\underline{X}]\!] := \mathbb{Z}^0[\![\underline{X}]\!] \otimes k = \varprojlim_{r,s} k[..., X_{-n}, ..., X_0]/\mathfrak{I}_r^s \tag{3.57}$$

where $\mathfrak{I}_r = (X_{-n})$, for $n \geq r$, varies over the nilpotent ideals as in the limit of Definition [2.106].

Clearly $\widehat{CW_k}$ is a p-formal group thanks to the above remark. Now we are ready for the following definition:

Definition 3.52 Let G be a formal k-group, consider the set $\widehat{M}(G) := \mathrm{Hom}_{k-f.fnct}(G, \widehat{CW_k})$ of morphisms between formal k-schemes which, thanks to Yoneda, can be identified with $\widehat{CW_k}(A_G)$ if $G := \mathrm{Spf}_k A_G$. $\widehat{M}$ is called **Dieudonné formal module** of G.

Without showing the details precisely, we can say that $\widehat{CW_k}(A_G)$ as a D_k-module can be also viewed as a $W(k)[F]$-proartinian module as a topological module (meaning that the open $W(k)[F]$-submodules form a system of open neighbourhoods of 0) and this comes from the fact that $\widehat{CW_k}(A_G) = \widehat{CW_k}^0(A_G) \times \widehat{CW_{kt}}(A_G)$, and that the two components are respectively a $W(k)[F]$-profinite closed submodule and a D_k-proartinian closed submodule. (For a detailed proof see [Fo], II, 4.1).

Proposition 3.53 Since $\widehat{CW_k}(A_G)$ is a topological D_k-submodule which is $W(k)[F]$-proartinian, then $\widehat{M}(G)$ can be viewed as a closed topological D_k-submodule.

Proof.

With an argument analogous to Theorem [1.78], from the maps $\widehat{\Delta} : A_G \to A_G \widehat{\otimes} A_G$ and $\widehat{i_1} : x \mapsto 1\widehat{\otimes}x$, $\widehat{i_2} : x \mapsto x\widehat{\otimes}1$, we get the corresponding maps $\widehat{CW_k}(A_G) \to \widehat{CW_k}(A_G \widehat{\otimes} A_G)$ and the elements of $\widehat{CW_k}(A_G)$ are exactly the f such that $\widehat{\Delta}(f) = f\widehat{\otimes}1 + 1\widehat{\otimes}f$. Moreover, if G is a p-formal group, and denoting with $G(n)$ the kernel of the multiplication map

$[p^n]$, then as we did before we can analogously define $\widehat{M}(G) = \varprojlim_n \widehat{M(G(n))}$, and being each $G(n)$ killed by $[p^n]$, then one gets $\bigcap_{n=0}^{\infty} p^n \widehat{M(G)} = 0$, hence $\widehat{M(G)}$ is a D_k-module $W(k)[F]$-profinite.

□

If $\widehat{M(G)}$ is given being G a p-formal group, then we call $\widehat{M}$ **p-Dieudonné formal module**, it is a functor between the category of p-formal groups over k and the category of D_k-modules $W(k)[F]$-profinites.

We conclude this section by stating an important result. The proof of which can be found for example in [Fo], III.

Theorem 3.54 The functor $\widehat{M} : G \mapsto \widehat{M(G)}$ induces an antiequivalence between the category of p-formal groups over k and the category of D_k-modules $W(k)[F]$-profinites. It has a quasi-inverse $\widehat{G}$ defined for a D_k-module M, that is $W(k)[F]$-profinite, as $\widehat{G}(M)(R) := \mathrm{Hom}_{D_k-mod,cont}(M, \widehat{CW_k}(R))$, i.e. all the continuous D_k-linear maps with the natural induced topology (of the simple convergence).

Notice that $\widehat{M}$ and $\widehat{G}$ are an adjoint pair. Moreover, if G is a finite p-formal group of rank p^h then $\widehat{M(G)}$ is a finite $W(k)$-module of length h. Hence when restricting to p-formal finite groups that are p-divisible we get the same result proved in the previous theorems.

3.4 Tate and Serre main theorem on p-divisible groups

The aim of this section is to give an outline of the proof for one of the most important results due to Serre and Tate about p-divisible groups. We start by stating the theorem and some direct consequences, then we discuss some aspects which stand at the base of the proof. Let k be our base commutative unital ring.

3.4.1 The main statement

We now state the main theorem with some direct implications, then we write down a sketch of the main steps of the proof. Let k be an integrally closed, noetherian integral domain, and let its field of fractions $K := \mathrm{Quot}(k)$ be with characteristic 0.

Theorem 3.55 If G and H are p-divisible groups over k, then a homomorphism $f_K : G \otimes_k K \to H \otimes_k K$ extends uniquely to a homomorphism $f : G \to H$.

Corollary 3.56 The map $\mathrm{Hom}_{p-div}(G, H) \to \mathrm{Hom}_{\pi}(T(G), T(H))$ is a bijection.

Remark 3.57 Here $\pi := \mathcal{G}(\overline{K}/K)$ is the Galois group of $\overline{K}/K$ ($\overline{K}$ is an algebraically closure of K) and we write $T(G)$ meaning the **Tate module** of G defined as:

$$T(G) := \varprojlim G_n(\overline{K}) \tag{3.58}$$

forthe projective system given by the maps $j_n : G_{n+1} \to G_n$ (of a given p-divisible group G_n). But then $T(G)$ is a $\mathbb{Z}_p$-module

$$T(G) \simeq \mathbb{Z}_p^h \tag{3.59}$$

where h =height(G). This is true since $\text{char}(K) = 0$ and so $G_n \otimes_k \overline{K}$ is reduced and hence $G_n \otimes_k K$ is étale. But then $G_n(\overline{K})$ is the constant group scheme.

Notice that if $k = K$ then the theorem becomes trivial and if K is such that char$K > 0$ then one can substitute k with a complete discrete valuation ring.

We recall also another important result that shows the deep connection between p-divisible groups and Tate modules.

Theorem 3.58 The functor $G \mapsto T(G)$ gives an equivalence between the category $\mathbf{BT}_p(k)$ of p-divisible groups and the category of finite free $\mathbb{Z}_p$-modules with a continuous Galois action of π (i.e. p-adic Galois representations).

3.4.2 Outline of the proof

The proof of the theorem is based on the following facts:

- first one must prove that if $g : G \to H$ is a morphism between p-divisible groups, such that the restriction $g_K : G \otimes_k K \to H \otimes_k K$ is an isomprhism then g is an isomorphism too. (In doing this one can, again, reduce to the case with k a complete discrete valuation ring).

- Secondly one prove the fact that: if k is a complete discrete valuation ring, F is a p-divisible group, and M a π-submodule of $T(F)$ that is a direct $\mathbb{Z}_p$-summand, then there exists a p-divisible group J over k and a map $J \to G$ that induces $T(J) \simeq M$.

- Now given the previous two steps it is sufficient to set $F := G \times H$, so that $T(F) = T(G) \times T(H)$. Clearly from the map $T(g_K) : T(G \otimes_k K) \to T(H \otimes_k K)$ one gets the graph $M \subseteq T(F_K)$ such that $T(F_K) = M \times T(H_K)$ as *direct sum* of π-submodules. But now thanks to step 2, let $\phi : J \to G \times H$ be such that $T(\phi_K) : T(J_K) \simeq M \subseteq T(F_K)$.

- We have an isomorphism $T((\text{pr}_1 \circ \phi)_K) : T(J \otimes_k K) \to T(G \otimes_k K)$ and thanks to the above equivalence stated in theorem [3.58], we get an isomorphism $(\text{pr}_1 \circ \phi)_K : J \otimes_k K \to G \otimes_k K$ and hence by applying step 1 $\text{pr}_1 \circ \phi : J \to G$ is an isomorphism too.

- Therefore we get $f := \mathrm{pr}_2 \circ \phi \circ (\mathrm{pr}_1 \circ \phi)^{-1} : G \to H$ that extend f_K. It is unique since each p-divisible group is finite *flat* and hence, for example the maps $G \to G \otimes_k K$ is injective.

Chapter 4

Elliptic Curves

4.1 Definition and main properties

Along the whole section, if not specified, we let k be an algebraically closed field of characteristic $\neq 2, 3$. We start by giving the definition of *elliptic curve* as an abelian variety, afterwards we proceed by clarifying all the concepts related to the definition of this object and we give some characterisations.

Definition 4.1 (Elliptic curve) If k is an algebraically closed field of char. $\neq 2, 3$, we define an **elliptic curve** $\mathcal{C}$ to be a (non singular cfr. [4.8]) smooth projective plane curve of genus 1 whose affine equation in $\mathbb{A}^2_k$, using the coordinate ring $k[x, y]$, is given by:

$$y^2 + a_1xy + a_2y = f(x) \tag{4.1}$$

where $f(x) \in k[x]$ is such that:

$$f(x) = x^3 + b_1x^2 + b_2x + b_3 \tag{4.2}$$

for $(a_1, a_2, b_1, b_2, b_3) \in k^5$. The equation above is called **Weierstrass standard equation** of the elliptic curve $\mathcal{C}$.

Remark 4.2 Observe that an elliptic curve $\mathcal{C}$ as defined in [4.1]:

- has (homogenized) projective equation given by:

$$y^2z + a_1xyz + a_2yz^2 = x^3 + b_1x^2z + b_2xz^2 + b_3z^3 \tag{4.3}$$

- has a **point at infinity** given by the point O of projective coordinates $O := [0 : 1 : 0]$ (cfr. [4.8] below).

We shall clarify the framework in which we have given these defnitions.

4.1.1 Elliptic curves as plane curves

Now let us be more clear on the conditions a (projective) plane curve must satisfy in order to be an elliptic curve and then let us show how the equation describing an elliptic curve can be simplifyed thanks to some affine changes of coordinates. We give some definitions and we list some notions (also some facts without proving them in detail) that are useful in order to understand the geometrical framework in which we are working.

We use the common notations for the **affine plane** over k, $\mathbb{A}^2_k \simeq k^2$ and for the **projective plane** $\mathbb{P}^2_k := k^3 \setminus \{(0,0,0)\}/\sim$, where $(x,y,z) \in k^3$ is such that $(x,y,z) \sim (x',y',z')$ if and only if $(x',y',z') = (\lambda x, \lambda y, \lambda z)$ for a $\lambda \in k^\times$. We denote a point in affine coordinates as $\underline{x} := (x,y)$, while we denote a point in projective coordinates as $\underline{x} := [x : y : z]$. Notice that clearly one can write $\mathbb{P}^2_k = \mathbb{A}^2_k \sqcup Z_0$ (thanks to the identification $(x,y) \mapsto [x,y,1]$) where $Z_0 : \{z = 0\}$ is the hyperplane (at infinity) .

Definition 4.3

(i) An **affine plane curve** is an affine variety $\mathcal{C} \subseteq \mathbb{A}^2_k$ which is given, following what already written in [2.7], by $\mathcal{C} := V(f) = \{(x,y) \in \mathbb{A}^2_k | f(x,y) = 0\}$ for a non-constant polynomial $f \in k[x,y]$. Equivalently thanks to [2.15] $\mathcal{C}$ can be viewed as a finite type affine k-scheme such that $\mathcal{C} \simeq \mathrm{Spec}(k[x,y]/(f))$, see Remark [4.5] and Definition [4.7] below;

(ii) A **projective plane curve** is a projective variety $\mathcal{C} \subseteq \mathbb{P}^2_k$, which is determined by the zeroes of a non-constant homogeneous polynomial $F \in k[x,y,z]$ with no repeated factors (we will better discuss this last condition in [4.5]). Namely:

$$\mathcal{C} := \{(x,y,z) \in \mathbb{P}^2_k \mid F(x,y,z) = 0\} \tag{4.4}$$

(iii) The projective space $\mathbb{P}^n_k$ can be viewed as a k-scheme defined as the union of the open affine k-schemes given by:

$$U_i := \mathrm{Spec}\left(k\left[\frac{x_1}{x_i}, ..., \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, ..., \frac{x_n}{x_i}\right]\right) \tag{4.5}$$

i.e. as the union of all the n-dimensional affine spaces contained in $\mathbb{P}^n_k$ and given by letting the hyperplane at infinity be $\{x_i = 0\}$, so that as a scheme we can write $\mathbb{P}^n_k := \bigcup_i U_i$. One can show that this open covering satisfies the gluing property for the Zariski-Grothendieck topology (the transition maps passing from an open to another are nothing but the affine ri-parametrizations);

(iv) as a consequence of *(iii)* a **projective plane curve** $\mathcal{C}$ can be viewed as a k-scheme $\mathcal{C} := \bigcup_i U_i$ where:

$$U_i := \mathrm{Spec}\left(k\left[\frac{x_1}{x_i}, ..., \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, ..., \frac{x_n}{x_i}\right]\right) / f\left(\frac{x_1}{x_i}, ..., \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, ..., \frac{x_n}{x_i}\right) \tag{4.6}$$

Notice that in definition [4.3] it is meaningless to compute the value of F at a representative (x, y, z) for the equivalence class $[x : y : z]$. However it makes sense to consider the *zeroes* of an homogeneous polynomial defining a projective variety, since $F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x, y, z)$ where $n := \deg(F)$ is the degree of F.

4.1.2 The ring of regular functions

We make a short discussion on how we can rigorously define the ring of regular functions on an affine (resp. projective) plane curve.

Remark 4.4 An affine (projective) plane curve $\mathcal{C}$ can be defined on a generic field k (not necessarily algebraically closed) in the same way as in previous definition [4.3]. Then one can consider an algebraic closure $\overline{k}$ of k, and as a consequence **extend** the set of the zeroes of f (the defining polynomial) with those zeros belonging to $\overline{k} \setminus k$, if they exist. For example, in the affine case, we denote this set by

$$\mathcal{C}(\overline{k}) := \{(x, y) \in \mathbb{A}^2_{\overline{k}} | f(x, y) = 0\} \tag{4.7}$$

When we "compute" the curve on a field L, that is a field extension of k, we write $\mathcal{C}(L)$ and we mean the points of $\mathcal{C}$ (i.e. the zeroes of f) having coordinates in L. Whenever clear from the context we shall write $\mathcal{C}$ meaning the points $\mathcal{C}(k)$ over the base field k. If $k' \subseteq k$ is a sub-field of k then we denote $\mathcal{C}(k')$ the set of the so called **k'-rational points** of $\mathcal{C}$ over k, i.e. $\mathcal{C}(k') = \mathcal{C}(k) \cap k'^2$.

A DISCUSSION: More explicitly, if k is a generic field, and $\mathcal{C}$ an affine plane curve defined by

$$\mathcal{C} := \mathrm{Spec}(k[x, y]/f(x, y)) \tag{4.8}$$

then using the scheme-theoretical notations, we can say equivalently that the points $(x, y) \in \mathcal{C}(k)$ with coordinates in k are given by the sections (geometrical points):

$$C(k) := \mathrm{Sp}_k(k[x, y]/f(x, y))(k) = \mathrm{Hom}_{k-fnct}(\mathrm{Sp}_k(k), \mathrm{Sp}_k(k[x, y]/f(x, y))) \tag{4.9}$$

i.e. all morphisms $\mathrm{Spec}(k) \to \mathrm{Spec}(k[x, y]/f(x, y))$ arising from k-algebras morphisms $k[x, y]/f(x, y) \to k$. So that, given any field extension $L \supseteq k$, writing $C(L)$ we mean the set of all the sections $\sigma_L : \mathrm{Spec}(L) \to \mathrm{Spec}(k[x, y]/f(x, y))$, which are **lifts** arising from the sections σ_k:

$$\begin{array}{ccc} \mathrm{Spec}(L) & \longrightarrow & \mathrm{Spec}(k) \\ & \searrow^{\sigma_L} & \downarrow \sigma_k \\ & & \mathrm{Spec}(k[x, y]/f(x, y)) \end{array}$$

Whenever we consider the algebraic closure $\overline{k} \supseteq k$ of k, these lifts are the geometric points in the sense of definition [3.24]:

$$\begin{array}{ccc} \mathrm{Spec}(\overline{k}) & \longrightarrow & \mathrm{Spec}(k) \\ & \searrow^{\sigma_{\overline{k}}} & \downarrow{\scriptstyle \sigma_k} \\ & & \mathrm{Spec}(k[x,y]/f(x,y)) \end{array}$$

To see concretely that those morphisms (the sections) represents points of the curve with coordinates in some field, it is enough to notice that the maps $\mathrm{Spec}(L) \to \mathrm{Spec}(k[x,y]/f(x,y))$ are those arising from the maps $k[x,y]/f(x,y) \to L$ which respects the k-algebras structure, i.e. that can be thought as **valuations maps**:

$$\nu_{(a,b)} : k[x,y]/f(x,y) \to L \tag{4.10}$$

$$\overline{g(x,y)} \mapsto \overline{g(a,b)} \tag{4.11}$$

for $(a,b) \in k^2$ and denoting $\overline{g(x,y)} := g(x,y) \text{ mod. } f(x,y)$.

Using this constructions and repeating what we already did at the beginning of Chapter 2 when dealing with affine varieties, which can be viewed as reduced, separated affine k-schemes of finite type (see [2.7], [2.8], [2.11] with warnings [W1], [W2] and [W3]), we can define the ring or **regular functions** on an affine plane curve $\mathcal{C}$ using the functorial Definition [2.27].

Definition 4.5 A **regular function** φ of the affine variety $\mathcal{C} := \mathrm{Spec}(k[x,y]/f(x,y))$ is an element of the ring:

$$\mathcal{O}_{\mathcal{C}}(\mathcal{C}) := \mathrm{Hom}_{k-fnct}(\mathcal{C}, \mathbb{O}_a) \simeq k[x,y]/f(x,y) \tag{4.12}$$

If the base field k is algebraically closed then $\varphi \in k[x,y]/f(x,y)$ can be viewed as the map $(a,b) \mapsto \varphi(a,b)$. A **rational function** of $\mathcal{C}$ over k is an element of the quotient field $\mathrm{Quot}(k[x,y]/f(x,y))$ and can be viewed as $\varphi := \frac{g(x,y)}{h(x,y)}$ for $h(x,y)$ not divided by $f(x,y)$. We denote this field field of fraction as:

$$\mathrm{Quot}(\mathcal{C}) \tag{4.13}$$

One must be careful that the construction holds when we consider this ring as a sheaf, namely the sheaf of k-algebras $\mathcal{O}_{\mathcal{C}} : \mathrm{Fnct}(\mathbf{Alg_k}, \mathbf{Set}) \to \mathbf{Alg_k}$ (as in [2.27]), however if k is not an algebraically closed field, the set $C(k)$ may be empty, meaning that there could be irreducible polynomials (which are also prime elements in the unique factorization domain $k[x,y]$) that are not separable in k (i.e. not all their roots are in k). To be more concrete, if f is the irreducible polynomial defining the irreducible variety $\mathcal{C}$, it could happen that one can not find valuation maps $\nu_{(a,b)} : k[x,y]/f(x,y) \to k$ respecting the k-algebra (equiv. k-field) structure: namely if f is irreducible of degree greater than 1, it is not possible to find $(a,b) \in k^2$ such that $f(a,b) = 0$.

As a consequence of the previous observation it is not always possible to think of functions of the ring $\mathcal{O}_{\mathcal{C}}(\mathcal{C}) \simeq k[x,y]/f(x,y)$ as functions defined on $\mathcal{C}(k)$, i.e. $\mathcal{C}(k) \to k$, so that a

regular function has to be considered, followign our definition, as a "family" of functions $\varphi_K : C(K) \to K$, functorially for each compatible field extension $K \supseteq k$.

Definition 4.6 If $\mathcal{C}$ is a projective plane curve over k defined by $F(x, y, z)$, we define the ring of **regular functions** in an analogous way as we did in [4.5] and [2.27], with the difference that in this case the associated algebra $\mathcal{O}(\mathcal{C})$ is not itself the ring $k[x, y, z]/F(x, y, z)$ (which is the homogeneous coordinate ring of $\mathcal{C}$) since $\mathcal{C}$ is not affine. However there exist a well defined map:

$$\varphi := \frac{G(x, y, z)}{H(x, y, z)} \mapsto ([a : b : c] \mapsto \frac{G(a, b, c)}{H(a, b, c)}) \tag{4.14}$$

where φ belongs to the subfield $\mathfrak{K}$ of the quotient field $\mathrm{Quot}(k[x, y, z]/F(x, y, z))$, made of the elements of the form $\frac{G(x,y,z)}{H(x,y,z)}$ for H, G homogeneous polynomial of the same degree such that F do not divide H. Clearly $[a : b : c] \mapsto \varphi([a : b : c])$ is a well defined map $\mathcal{C}(K) \to K$, for all field extension $K \supseteq k$. We denote (with abuse of notation) this subfield $\mathfrak{K} \subseteq \mathrm{Quot}(k[x, y, z]/F(x, y, z))$ as:

$$\mathrm{Quot}(\mathcal{C}) := \mathfrak{K} \tag{4.15}$$

and we mean all the possible **rational** functions defined on $\mathcal{C}$. As a consequence there exist a well defined map:

$$\mathcal{O}(\mathcal{C}) = \{ \text{ regular functions on } \mathcal{C}\} \to \{ \text{ rational functions on } \mathcal{C}\} \tag{4.16}$$

given by (functorially in K):

$$\varphi \mapsto (f : U \subseteq \mathcal{C}(K) \to K) \tag{4.17}$$

such that f has no poles in U and $f \equiv \varphi_K$ on U.

Let now k be an algebraically closed field again. In order to show the relation between affine/projective curves and the scheme theory we developed in previous chapters, we make an **important** remark:

Remark 4.7 From definition [4.3] above, an affine (resp. projective) plane curve is a 1-dimensional **closed** subscheme $\mathcal{C} \subseteq \mathbb{A}^2_k$ (resp. $\subseteq \mathbb{P}^2_k$), for the Zariski topology on $\mathrm{Spec}(k[x, y])$ (resp. $\mathrm{Spec}(k[x, y, z])$). In this context the main difference with respect to definitions given in [2.7], is that we require also $\mathcal{C}$ to be **geometrically reduced** as a scheme i.e. such that the defining associated algebra $R := \mathrm{Spec}(k[x, y]/(f))$ is a reduced ring, meaning that it has no **nilpotent elements** different from $0, 1$. (See also remark after definition [2.20] p.).

Now since $k[x, y]$ is a unique factorisation domain, denoting with (f) the ideal generated by the polynomial $f(x)$ defining the associated algebra $k[x, y]/(f)$, we have that (f) is a principal ideal and hence an ideal of **height** 1 (definition of Krull dimension - from where

the dimension of the scheme; see for example [1.58] or [Ga]) and it is uniquely determined up to multiplication by a constant.

We have proven the following:

Proposition 4.8 A geometrically reduced affine plane curve over k of dimension 1 is completely determined by a polynomial $f \in k[x, y]$ up to multiplicative constant.

Definition 4.9 From what already observed before (cfr. [4.5]), since k is a field, and in particular a unique factorization domain, then $k[x, y]$ is a unique factorization domain too, so that each $f \in k[x, y]$ can be written uniquely as $f = f_1^{m_1} \cdot ... \cdot f_n^{m_n}$, for $m_i \in \mathbb{N}$, with each $f_i^{m_i}$ irreducible element of $k[x, y]$. The f_i such that $m_i > 0$ are called **repeated factors**.

Definition 4.10 Let k be a generic field. Let $f \in k[x, y]$ be the polynomial defining an affine plane curve $\mathcal{C}$. Then:

- the curve $\mathcal{C}$ is said to be **irreducible** if f is irreducible in $k[x, y]$;
- the curve $\mathcal{C}$ is said to be **geometrically irreducible** if f remains irreducible in $\overline{k}[x, y]$, for $\overline{k}$ algebraic closure of k;
- if $f = f_1 \cdot ... \cdot f_n$, the curves $\mathcal{C}_{f_i}$ defined by the f_i's are called **irreducible components** of $\mathcal{C}$ and $\mathcal{C}(L) = \bigcup_i \mathcal{C}_{f_i}(L)$, for every field extension L of k.
- a point $(a, b) \in \mathcal{C}(L)$ is said to be **non singular** if $\nabla f(a, b) \neq (0, 0)$, where:

$$\nabla f := (\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}) \tag{4.18}$$

- the curve $\mathcal{C}(L)$ is said to be **non singular** if all of its points are non singular.

After all these preliminaries let us focus again on elliptic curves, which we are going to consider as abelian varieties. Our purpose is to endow those cubic plane curves with a group law structure and then use the informations contained in their natural k-group scheme structure in order to deduce in a general way their associated p-divisible group.

4.2 Elliptic curves as abelian varieties

Proposition 4.11 An elliptic curve $\mathcal{C}$ as in Definition [4.1], is an abelian variety of dimension 1.

Proof. Following Definition [4.1], $\mathcal{C}$ is a smooth projective variety of dimension 1 over the (algebraically closed) field k, that can be viewed as a finite k-scheme with associated algebra $k[x, y]/(f)$ for $f \in k[x, y]$. This implies that, following definitions in [3.24] and Remark [3.25], that $\mathcal{C}$ is connected (when viewed as a geometrical fiber) and it is also

regular thanks to smoothness; being an affine variety it is a finite type k-scheme and being projective it is also separated (as closed immersion of a closed variety, the projective plane) and universally closed. The last thing we have to prove is that there is a commutative group law defined on $\mathcal{C}$ which will follows from the next paragraphs. $\square$

From now on we use Definition [4.1] to consider an elliptic curve as an affine plane curve in an algebraically closed field k of char. $\neq 2, 3$. We start by reconducing the equation defining an elliptic curve $\mathcal{C}$ as in [4.1], i.e. $y^2 + a_1xy + a_2y = x^3 + b_1x^2 + b_2x + b_3$ into a simpler **standard** equation $y^2 = 4x^3 + g_2x + g_3$ thanks to some (linear) changes of variables.

Proposition 4.12 Let k an algebraically closed field of char. $\neq 2, 3$. Let $\mathcal{C}$ an elliptic curve as in definition [4.1]. Its defining Weierstrass equation $y^2 + a_1xy + a_2y = x^3 + b_1x^2 + b_2x + b_3$ can be turned into a simpler equation, i.e. the curve is isomorphic to the plane curve defined by the equation:

$$y^2 = 4x^3 + g_2x + g_3 \tag{4.19}$$

for some $(g_2, g_3) \in k^2$.

Proof. Starting from the Weierstrass equation $y^2 + a_1xy + a_2y = x^3 + b_1x^2 + b_2x + b_3$ defining $\mathcal{C}$, then the change of variables:

$$x' = x \tag{4.20}$$

$$y' = 2y + a_1x \tag{4.21}$$

will eliminate the term a_1xy. Giving:

$$\frac{1}{4}y^2 + \frac{a_2}{2}y = x^3 + (\frac{a_1^2}{4} + b_1)x^2 + (\frac{a_1a_2}{2} + b_2)x + b_3 \tag{4.22}$$

Then we multiply by 4:

$$y^2 + 2a_2y = 4x^3 + 4(\frac{a_1^2}{4} + b_1)x^2 + (2a_1a_2 + 4b_2)x + 4b_3 \tag{4.23}$$

and we set $a := 2a_2$, $b := (\frac{a_1^2}{4} + b_1)$, $c := (2a_1a_2 + 4b_2)$ and $d := 4b_3$ so that the equation becomes:

$$y^2 + ay = 4x^3 + 4bx^2 + cx + d \tag{4.24}$$

then we apply the coordinate change:

$$x' = x + \frac{b}{3} \tag{4.25}$$

$$y' = y + \frac{a}{2} \tag{4.26}$$

so that we get:

$$y^2 = 4x^3 + (\frac{8}{3}b^2 + c)x + \frac{8}{27}b^3 - \frac{cb}{3} + d + \frac{a^2}{4} \tag{4.27}$$

therefore putting $g_2 := (\frac{8}{3}b^2 + c)$ and $g_3 := \frac{8}{27}b^3 - \frac{cb}{3} + d + \frac{a^2}{4}$ the thesis holds:

$$y^2 = 4x^3 + g_2x + g_3 \tag{4.28}$$

The equation above is called **reduced equation** of the elliptic curve $\mathcal{C}$. □

To complete our discussion we only state without proving the following:

Proposition 4.13 A projective nonsingular plane **cubic** curve over k with an inflection point O can be reduced to an elliptic curve with standard Weierstrass equation such as in [4.1], with a unique point at infinity $O := [0 : 1 : 0]$. (For a proof see for example [Mil, II, 1.2])

Remark/Definition 4.14 We recall the definition of the **discriminant of a polynomial** $f := a_nx^n + ... + a_1x + a_0 \in k[x]$, which is given by:

$$\Delta := a_n^{2n-2} \prod_{i<j} (x_i - x_j)^2 \in k \tag{4.29}$$

where $(x_i)_i$ vary over all the rooths of f in the algebraically closed field k. Therefore for a generic cubic of the form:

$$ax^3 + bx^2 + cx + d \tag{4.30}$$

splitting into the polynomial $a(x - x_1)(x - x_2)(x - x_3)$, one can see (using the relations between the x_i's $\in k$) that:

$$\Delta = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd \tag{4.31}$$

Hence for a cubic equation of the form $4x^3 + g_2x + g_3$ we get:

$$\frac{\Delta}{16} = g_2^3 - 27g_3^2 \tag{4.32}$$

Remark 4.15 Observe that from the definition of singular point [4.10], a point (a, b) is singular for the curve of equation $y^2 = 4x^3 + g_2x + g_3$ if and only if the discriminant of the right hand side polynomial is different from zero. Indeed if $\Delta = 0$ this means that there is at least repeated rooth for the polynomial $4x^3 + g_2x + g_3$, and hence we can write $y^2 = 4(x-x_1)(x-x_2)^2$ so that $\nabla(y^2-4(x-x_1)(x-x_2)^2) = (2y, -4x(x-x_2)^2-8(x-x_1)(x-x_2))$ and hence the point $(0, x_2)$ is a singular point for the curve (see [4.17]).

Definition 4.16 The **j-invariant** of an elliptic curve $\mathcal{E}$ of reduced equation:

$$y^2 = 4x^3 + g_2x + g_3 \tag{4.33}$$

is given by:

$$j(\mathcal{E}) := \frac{(12g_2)^3}{\Delta} \tag{4.34}$$

We will clarify later the importance of this number which is strictly related to the discriminant of the curve.

Proposition 4.17 Let $\mathcal{E}$ the elliptic curve of reduced equation $y^2 = 4x^3 + g_2x + g_3$, then:

(i) $\mathcal{E}$ is non-singular if and only if $\Delta \neq 0$;

(ii) if $\Delta = 0$ and $g_2 \neq 0$, the curve has a **node**

(iii) if $\Delta = 0$ and $g_2 = 0$, the curve has a **cusp**

(iv) $\mathcal{E}$ has at most one singular point;

(v) $\mathcal{E}$ is isomorphic to another elliptic curve $\mathcal{E}'$ if and only if $j(\mathcal{E}) = j(\mathcal{E}')$ (from which the importance of j);

(vi) for every $a \in k$ there exist $\mathcal{E}$ such that $j(\mathcal{E}) = a$.

Proof. The proof is easy and we only give some indications, for details see for example [Si]. We already proved *(i)* in Remark [4.15]. A **node** (a, b) is a singular point with different tangent lines i.e. such that, considering that the polynomial $f(x, y)$ can be written in form $f(x, y) = f_m(x-a, y-b)+$*terms of higher degree*, with f_m homogeneous of degree m, then f_m is the product of m distinct polynomials of degree 1. In the case of a cubic curve clearly $m = 2$. If the polynomials coincide i.e. $m = 1$ then the point is said to be a **cusp**. So that from *(i)* easily descend *(ii)* and *(iii)*. To prove *(v)* it is sufficient to consider that the only affinities (affine change of variables) such that the equation $y^2 = 4x^3 + g_2x + g_3$ is preserved are of the form $x = u^2x'$ and $y = u^3y'$. □

Definition 4.18 Let k be algebraically closed. Since from Definition ([4.1]) an elliptic curve $\mathcal{E}$ of reduced equation $y^2 = 4x^3 + g_2x + g_3$ is non-singular, then its defining equation can be written, after an appropriate change of variables, in the form:

$$y^2 = x(x-1)(x-\lambda) \tag{4.35}$$

for $\lambda \in k \setminus \{0, 1\}$. The family of elliptic curves of affine equations given by:

$$k \setminus \{0, 1\} \ni \lambda \mapsto \mathcal{E}_\lambda : y^2 = x(x-1)(x-\lambda) \tag{4.36}$$

is called **Legendre family**, and each of these curves has j-invariant:

$$j(\lambda) := j(\mathcal{E}_\lambda) = \frac{2^8(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2} \tag{4.37}$$

Now we sum up some properties about the notions of divisors of a rational function on an affine curve $\mathcal{C}$ which, together with the Riemann-Roch theorem (that we will only state without a proof), will be useful in the description of the multiplicative law that we are going to define on an elliptic curve.

Definition 4.19 Given an affine plane curve $\mathcal{C} = \mathrm{Spec}(k[x,y]/f(x,y))$ (which is non-singular in our case) over an algebraically closed field k, we denoted with:

$$\mathcal{O}_{\mathcal{C}}(\mathcal{C}) \simeq k[x,y]/f(x,y) \tag{4.38}$$

the sheaf of its regular functions (cfr. [4.5]). We define:

- the **group of divisors** $\mathrm{Div}(\mathcal{C})$ as the free abelian group generated by the set $\mathcal{C}(k)$ i.e. each **divisor** $D \in \mathrm{Div}(\mathcal{C})$ can be written as:

$$D = \sum n_P P \tag{4.39}$$

  for $P \in \mathcal{C}(k)$ (points of the curve over k) and $n_P \in \mathbb{Z}$, where $n_P = 0$ for all but a finite number of points P; the zero of the group is given by the 0-divisor where $n_P = 0$ for all $P \in \mathcal{C}(k)$;

- if φ is a rational function on $\mathcal{C}$ then we define the **divisor** of φ to be:

$$div(\varphi) := (\varphi) = \sum \mathrm{ord}_P(\varphi) P \tag{4.40}$$

  where $\mathrm{ord}_P(\varphi)$ is the order of **vanishing** of the function at P, it is effectively a positive integer that counts the multiplicity of P as a zero of φ while it is negative if P is a pole (also in this case counting multiplicity);

- let D be a divisor, then we denote with $\mathfrak{L}(D)$, the k-**vector space**:

$$\mathfrak{L}(D) := \{\varphi \in \ \mathrm{Quot}(\mathcal{C}) \ | (\varphi) + D \geq 0\} \tag{4.41}$$

- we denote with $l(D) := \dim_k \mathfrak{L}(D)$, the dimension over k of $\mathfrak{L}(D)$;

- we denote with $\deg(D)$ the degree of the divisor $D = \sum n_P P$ given by:

$$\deg(D) := \sum n_P \tag{4.42}$$

- the **canonical divisor** K of a curve is the divisor of a global meromorphic 1-form on $\mathcal{C}$;

- we define as (ω) the **canonical differential divisor** of an elliptic curve $\mathcal{E}$ coming from the differential (form) given by $\omega := \frac{dx}{y}$.

Remark 4.20 Let us clarify some aspects of the definition.

(i) A meromorphic 1-form is given by a differential 1-form $\omega := \sum_i f_i dx_i$, where the f_i's are meromorphic functions, i.e. holomorphic everywhere (in the whole space or in an open subset) except for a discrete set of points. Any two meromorphic 1-forms ω_1, ω_2 give divisors that are linearly equivalent, namely $(\omega_1) = (\omega_2) + (f)$ for f a meromorphic function on $\mathcal{C}$ (see [Si] for details). Hence we can choose one canonical divisor up to linear equivalence.

(ii) Notice that for an elliptic curve $\mathcal{E}$ of the form $y^2 = 4x^3 + g_2x + g_3$, an explicit computation shows that:

$$2ydy = (3x^2 + g_2)dx \tag{4.43}$$

so that:

$$\frac{dx}{y} = \frac{2dy}{3x^2 + g_2} \tag{4.44}$$

and since $3x^2 + g_2 \neq 0$ (from the fact that the curve is not singular) then ω is holomorphic (it has no poles) and has no zeroes as well.

(iii) from what observed above in *(ii)*, the canonical divisor (ω) of an elliptic curve is equal to zero and thus the vector space of **holomorphic differentials** on $\mathcal{E}$ is a 1-dimensional k-vector space. This is the true meaning of the fact that $\mathcal{E}$ has **genus** 1. We will show the relationship between the genus g of a curve and the rational functions we can define on it in theorem [4.21].

According to our definition, the vector field $\mathfrak{L}(D)$, consists of functions having poles that coincides with some of the zeroes of the divisor D, and such that their multiplicity is at most the multiplicity of the corresponding zeroes. There is an important result connecting a divisor D to the vector space $\mathfrak{L}(D)$ and to the canonical divisor K (of the differential $\omega = \frac{dx}{y}$) of an elliptic curve with reduced equation 4.35. It is the following:

Theorem (Riemann-Roch) 4.21 Let $\mathcal{C}$ be a non-singular projective (affine) plane curve defined by a polynomial $F(x, y, z)$ (resp. $f(x, y)$ over k, algebraically closed field. Then there exist an integer g such that for all divisors D:

$$l(D) = l(K - D) + \deg(D) - g + 1 \tag{4.45}$$

Where K is the canonical divisor of the curve.

We do not give a proof for this theorem (we suggest for example to see [Fulton], 1969 p.196), however from the statement we can deduce important informations about the rational functions we can define on the curve $\mathcal{C}$. First of all if $\deg(D) \geq \deg(K)$ clearly $l(K - D) = 0$ (is the 0 dimensional vector space) so that $l(D) = \deg(D) - g + 1$ and in particular for an elliptic curve we have that since $g = 1$ then $l(D) = \deg(D)$. But the importance of the theorem lies on the fact that we can endow with an **abelian group structure** every elliptic curve $\mathcal{E}$ once given the choice of a point $O \in \mathcal{E}$, which will play the role of the neutral element.

Definition 4.22 Let $\mathcal{E}$ be an elliptic curve of reduced equation $y^2 = 4x^3 + g_2x + g_3$ (over an algebraically closed field k). Then

- we say that two divisors D and D' on $\mathcal{E}$ are **linearly equivalent** if $D = D' + (f)$, for a rational function $f \in \mathrm{Quot}(\mathcal{C})$;
- $\mathrm{Div}^0(\mathcal{E})$ the (free abelian) group of divisors D of $\mathcal{E}$ of degree $\deg(D) = 0$;

- $\mathrm{Pic}^0(\mathcal{E})$ the **Picard group** of equivalence classes of $\mathrm{Div}^0(\mathcal{E})$ where $D \simeq D'$ if and only if thei are linearly equivalent.

Proposition 4.23 The free abelian group $\mathrm{Div}(\mathcal{C})$ of divisors of a projective/affine (non-singular) plane curve $\mathcal{C}$ has a partial order structure.

Proof. We define the partial order on $\mathrm{Div}(\mathcal{C})$ to be such that for two divisors $D = \sum_P n_P P$ and $D' = \sum_P m_P P$, then $D \geq D'$ if and only if $n_P \geq m_P$ for all $P \in \mathcal{C}$. It is well defined and clearly one has that $D = \sum_P n_P P \geq 0$ if and only if $n_P \geq 0$ for all P.

Corollary 4.24 In particular, $\mathrm{Div}^0(\mathcal{E})$, for an elliptic curve $\mathcal{E}$ (in reduced form 4.35) is a partial ordered group such that $D = \sum_P n_P P = 0$ if and only if $n_P = 0$ for all $P \in$, i.e. D is the (0-divisor) divisor of a function on $\mathcal{E}$ that has no zeroes and no poles, and therefore is a **constant** function.

Proposition 4.25 Let $\mathcal{E}$ be an elliptic curve of reduced equation $y^2 = 4x^3 + g_2 x + g_3$ (over an algebraically closed field k). Then all the rational functions $\varphi \in \mathrm{Quot}(\mathcal{E})$, are 0-divisors of $\mathcal{E}$ i.e. they are such that $(\varphi) = \sum_P n_P P$ with $n_P = 0$ for all points P.

Proof. Given a rational function φ on $\mathcal{E}$ such that $(\varphi) := 0$, from the above corollary [4.24], this means that it has no zeroes neither poles (on $\mathcal{E}$) so that φ must be a constant $\in k$. Conversely if we look at $\mathcal{E}$ as a projective non-singular plane curve, then a rational function is given by

$$\varphi := \frac{G(x, y, z)}{H(x, y, z)} \tag{4.46}$$

where G and H are homogeneous polynomials of degree m and, being $F(x, y, z)$ the defining polynomial of $\mathcal{E}$, then H is not divided by F. Notice that G neither is divided by F otherwise φ would be constantly 0, so that as a consequence none of the points P in $\mathcal{E}$ is a pole or a zero of φ, hence $(\varphi) \in \mathrm{Div}^0(\mathcal{E})$ as a divisor, i.e. it has order (=degree) zero (it has many zeroes as its poles counting multiplicity). □

Warning! The group $\mathrm{Div}^0(\mathcal{E})$ is the group of divisors of order (i.e. degree) 0 which is different from being the 0-divisor $D \equiv 0$ (with all $n_P = 0$). For simplicity thanks to what observed in the previous proof we assume that a rational function φ is not the constantly zero function on $\mathcal{E}$.

Proposition 4.26 Let $\mathcal{E}$ be an elliptic curve of reduced equation $y^2 = 4x^3 + g_2 x + g_3$ (over an algebraically closed field k). Then there exist an exact sequence of groups:

$$0 \to k^\times \to \mathrm{Quot}(\mathcal{E}) \to \mathrm{Div}^0(\mathcal{E}) \to \mathrm{Pic}^0(\mathcal{E}) \to 0 \tag{4.47}$$

Proof. There is a natural injection of $k^\times$, viewed as multiplicative group, into $\mathrm{Quot}(\mathcal{E})$, since all the elements of $k^\times$ can be considered as the constant rational functions on $\mathcal{E}$. The exactness at $\mathrm{Quot}(\mathcal{E})$ (which for simplicity we are considering without the constant

function $\varphi \equiv 0$) is given thanks to the previous Proposition [4.25] and Corollary [4.24]. The exactness at $\mathrm{Div}^0(\mathcal{E})$ is given by definition of linear equivalence and Picard group [4.22]. The last map is given by the surjection $\mathrm{Div}^0(\mathcal{E}) \twoheadrightarrow \mathrm{Div}^0(\mathcal{E})/\sim$. □

Proposition 4.27 For $\mathcal{E}$ an elliptic curve, defined as before, and let O a point of $\mathcal{E}$. There is a bijection:

$$\mathcal{E}(k) \to \mathrm{Div}^0(\mathcal{E}) \to \mathrm{Pic}^0(\mathcal{E}) \tag{4.48}$$

$$P \mapsto P - O \mapsto [P - O] \tag{4.49}$$

that can be viewed as a morphism between groups ([4.28]).

Proof. We proceed by steps.

Step 1 Observe that if $D = P$ is a divisor of $\mathcal{E}$, then, thanks to Riemann-Roch [4.21] and to the observations below, $l(D) = \deg(D) = 1$ so that $\mathfrak{L}(D)$ is a 1-dimensional k-vector space and hence, since $k \subseteq \mathfrak{L}(D)$ then $\mathfrak{L}(D) \simeq k$.

Step 2 We prove injectivity. Let $[P - O] = [P' - O]$ be the same equivalence class for two points $P, P' \in \mathcal{E}$. Then $P - O = P' - O + (f)$ so that $[P - P'] = 0$, for $f \in \mathrm{Quot}(\mathcal{E})$. Therefore $P = P' + (f)$ and hence $f \in \mathfrak{L}(P')$. But thanks to step 1 this means that $f \in k^\times$ and so $P = P' + 0 = P'$.

Step 3 We now prove surjectivity. Let $[D]$ in $\mathrm{Pic}^0(\mathcal{E})$. Then by definition $\deg(D) = 0$ so that obviously $\deg(D + O) = 1 = l(D + O)$. Now again thanks to step 1 $\mathfrak{L}(D + O) \simeq k^\times$. By definition for $f \in \mathfrak{L}(D + O)$ we have that $D + O + (f) \geq 0$ but since $f \in k^\times$ this means $D + O \geq 0$. Together with $1 = l(D + O)$ we get that $D + O = P$ for a point P in $\mathcal{E}$, and the thesis holds. □

Corollary 4.28 For $\mathcal{E}$ an elliptic curve, defined as before, and let O a point of $\mathcal{E}$. Thanks to proposition [4.27], we can define a **group law** on $\mathcal{E}$ given by:

$$m : \mathcal{E} \times \mathcal{E} \to \mathcal{E} \tag{4.50}$$

$$(P, Q) \mapsto m(P, Q) := R \tag{4.51}$$

which is commutative, with neutral element O and inverse $i : \mathcal{E} \to \mathcal{E}$ given by $P \mapsto -P$.

Proof. The morphisms m and i are morphisms between projective (affine) varieties, or equivalently, morphisms between affine k-schemes that arise from the composition law that makes $\mathcal{E}(k) \to \mathrm{Pic}^0(\mathcal{E})$ an isomoprhism of groups, i.e. we define (thanks to the bijection proved in [4.28]):

$$\mathcal{E}(k) \times \mathcal{E}(k) \to \mathrm{Pic}^0(\mathcal{E}) \tag{4.52}$$

$$(P, Q) \mapsto [P - O] + [Q - O] =: [R - O] \tag{4.53}$$

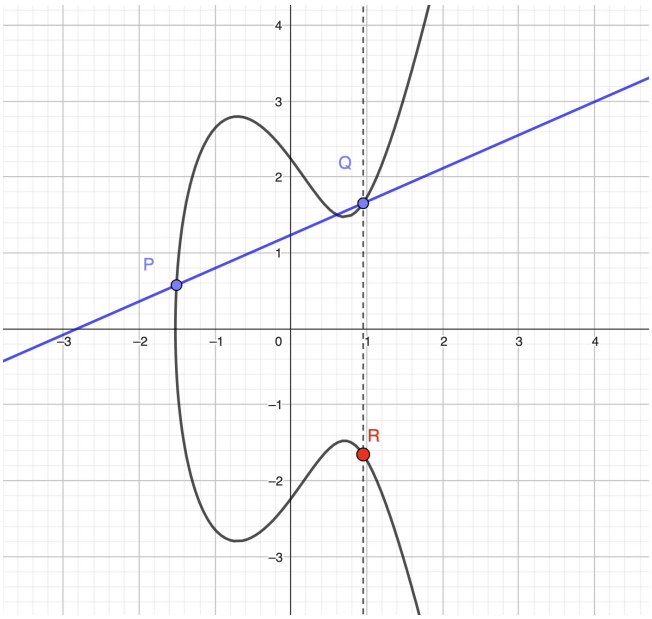


Figure 4.1: Sum of two points in the given elliptic curve of equation $y^2 = 4x^3 - 6x + 5$: $P + Q = R$

where R is the unique point of $\mathcal{E}(k)$ such that:

$$P + Q - 2O = R - O + (f) \tag{4.54}$$

as divisors for $f \in \mathrm{Quot}(\mathcal{E})$. In other words we have defined R in such a way that the divisors $P + Q$ and $R + O$ are linearly equivalent as divisors, which means that R is the unique point of the curve that makes $[P - O] + [Q - O]$ equal to $[R - O]$ for the internal group operation of $\mathrm{Pic}^0(\mathcal{E})$. From this descends that $m(P, O) = P$ since $[P-O]+[O-O] = [P - O] + 0_\sim = [P + O]$, moreover if $[P - O] + [Q - O] = 0_\sim$ clearly $[P + Q - 2O] = 0_\sim$ hence $P + Q = (f)$ as divisors and so $P = -P$. □

Construction 4.29 We insert two images that show the construction of the group law on the elliptic curve of equation $y^2 = 4x^3 - 6x - 5$.

In the first image, [F1], letting $\mathcal{O}$ being the point at infinity, it clearly appear that $P+Q \sim R + O$ as divisors. In the second figure, [F2], it is shown that $P + O \sim O$ as divisors.

We have endow with an abelian group law the elliptic curve $\mathcal{E}$ which, as a consequence, can be considered as an abelian k-**group** of dimension $g = 1$, and this completes Proposition [4.11].

Warning! Let $\mathcal{E}$ an elliptic curve, defined as before, of affine equation given by $y^2 = f(x)$, for $f(x) := 4x^3 + g_2x + g_3$. Let $R := k[x, y, z]/(F)$ be the ring of homogeneous coordinates of $\mathcal{E}$ in $\mathbb{P}^2$, where $F(x, y, z) = zy^2 - 4x^3 - g_2xz^2 - g_3z^3$ is the defining polynomial of $\mathcal{E}$.

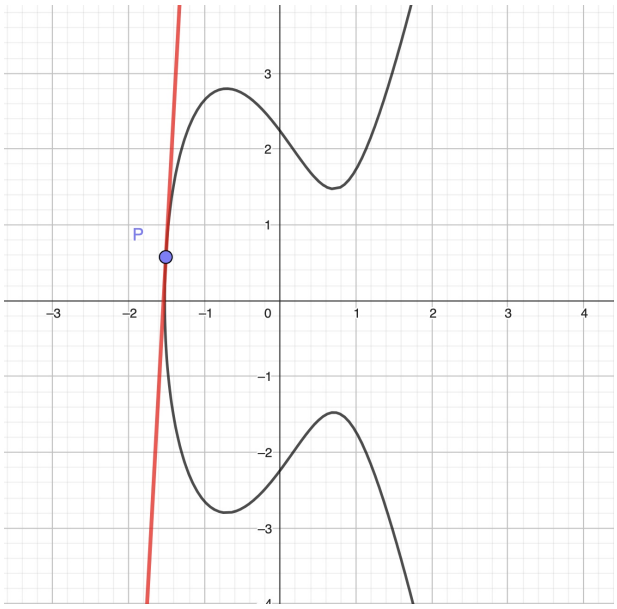


Figure 4.2: Sum a point with the neutral element in the given elliptic curve of equation $y^2 = 4x^3 - 6x + 5$: $P + O = P$.

Then the group law given by Theorem [4.28], namely:

$$m : \mathcal{E} \times \mathcal{E} \to \mathcal{E} \tag{4.55}$$

$$(P, Q) \mapsto m(P, Q) \tag{4.56}$$

does not induce a morphism of k-algebras:

$$R \to R \otimes_k R \tag{4.57}$$

since $R \otimes_k R$ is not the associated coordinate ring of $\mathcal{E} \times \mathcal{E}$. So that $R := k[x, y, z]/(F)$ is **NOT** a Höpf algebra. This is becouse the projective curve $\mathcal{E}$ can not be viewed as an **affine** k-scheme (i.e. of the form $\mathrm{Spec}(A)$ for a k-algebra A), although $\mathcal{E}$ with the above commutative law can be viewed as a commutative k-group scheme with associated algebra $\mathcal{O}(\mathcal{E})$. The reason of this subtle difference lies in the fact that when considering the associated affine equation of $\mathcal{E}$, the affine points of $\mathcal{E}(k)$ do not coincide with the whole set of points of $\mathcal{E}_{\mathcal{E}}(k)$, having the curve $\mathcal{E}$ a **point at infinity**, i.e. using the above coordinates homogenization, a point $[0 : 1 : 0]$ belonging to the hyperplane $\{z = 0\}$. The law we have given is defined on the whole set of points $\mathcal{E}(k)$, also on the point at infinity, and allows to consider it as an abelian group. Moreover, the point $[0 : 1 : 0]$, is almost always chosen as the O point of the group law, so that it is also an essential point of the curve.

In conclusion if a projective plane (non-singular) curve is defined as $\mathcal{C} := \mathrm{Spec}(A)$ for some k-algebra $A \simeq k[x, y]/f(x, y)$ (in $\mathbb{A}^2_k$), then it is affine and clearly $\mathcal{O}(\mathcal{C}) \simeq A$, otherwise, for example for a generic elliptic curve $\mathcal{E}$ as above, the ring of regular functions $\mathcal{O}(\mathcal{E})$ is isomorphic to $k[x, y]/(f)$, being $f(x, y)$ de defining polynomial of $\mathcal{E}$, thanks to [4.5], but can **NOT** be considered as k-bi-algebra, since $R \to R \otimes_k R$ above is not a co-multiplication law.

Despite this observations we can do a step further in order to describe the p-divisible group associated to those abelian varieties of dimension 1.

4.3 The formal group of an elliptic curve

In this section we prepare for the final result we want to prove, i.e. the structure of the p-torsion subgroups of elliptic curves.

From the previous section we know that an elliptic curve $\mathcal{E}$ over a (algebraically closed) field k, of affine reduced equation $y^2 = 4x^3 + g_2x + g_3$ has a commutative k-group structure given by the map:

$$m : \mathcal{E} \times \mathcal{E} \to \mathcal{E} \tag{4.58}$$

$$(P, Q) \mapsto m(P, Q) \tag{4.59}$$

which can be considered as a map:

$$m : \mathcal{E}(k) \times \mathcal{E}(k) \to \mathcal{E}(k) \tag{4.60}$$

$$(P, Q) \mapsto m(P, Q) \tag{4.61}$$

where $m(P, Q)$ is the sum $R = P + Q$ (and heare it is not the divisor) of two points of $\mathcal{E}$ with coordinates in k.

Proposition 4.30 The map

$$m : \mathcal{E}(k) \times \mathcal{E}(k) \to \mathcal{E}(k) \tag{4.62}$$

$$(P, Q) \mapsto m(P, Q) = R \tag{4.63}$$

defined as above, induces a map

$$\mathcal{O}_{\mathcal{E},R} \to \mathcal{O}_{\mathcal{E}^2,(P,Q)} \tag{4.64}$$

where $\mathcal{O}_{\mathcal{E},P}$ is the stalk of the sheaf of regular functions of $\mathcal{E}$ at its point P. In particular, for the neutral element O of $\mathcal{E}$:

$$\mathcal{O}_{\mathcal{E},O} \to \mathcal{O}_{\mathcal{E}^2,(O,O)} \tag{4.65}$$

Where, in order to obtain a local ring, by definition:

$$\mathcal{O}_{\mathcal{E}^2,(P,Q)} := (\mathcal{O}_{\mathcal{E},P} \otimes_k \mathcal{O}_{\mathcal{E},Q})_{\mathcal{M}_{(P,Q)}} \tag{4.66}$$

and $\mathcal{M}_{(P,Q)}$ is the maximal ideal given by:

$$\mathcal{M}_{(P,Q)} := \mathcal{M}_P \otimes_k \mathcal{O}_{\mathcal{E},Q} + \mathcal{O}_{\mathcal{E},P} \otimes_k \mathcal{M}_Q \tag{4.67}$$

Proof. The proof comes from the definition of the sheaf (of regular functions) and of the stalk of a k-scheme at a point, see for example Equation (2.14) of [2.13]. Notice that despite the observation of previous warning [W5], the ring $\mathcal{O}_{\mathcal{E}}$ is a k-bi-algebra thanks to the map $\mathcal{O}_{\mathcal{E}}(\mathcal{E}) \to \mathcal{O}_{\mathcal{E}}(\mathcal{E}) \otimes \mathcal{O}_{\mathcal{E}}(\mathcal{E})$ induced by $\mathcal{E} \times \mathcal{E} \to \mathcal{E}$ and since a k-group scheme is a group object in the category of k-schemes [2.59]. □

As a consequence of previous proposition, since the local morphisms, such as $\mathcal{O}_{\mathcal{E},O} \to \mathcal{O}_{\mathcal{E}^2,(O,O)}$, are **continuous** considering the $\mathcal{M}_O$-adic and the $\mathcal{M}_{(O,O)}$-adic topologies then we can extend them by continuity to their completion and we get the following:

Corollary 4.31 Let $\mathcal{E}$ the elliptic curve viewed as a k-group scheme as above, then:

$$\widehat{\mathcal{O}}_{\mathcal{E},O} \simeq k[\![x]\!] \tag{4.68}$$

and

$$\widehat{\mathcal{O}}_{\mathcal{E}^2,(O,O)} \simeq k[\![x]\!] \widehat{\otimes} k[\![x]\!] \tag{4.69}$$

where x is a generator of $\mathcal{M}_O$.

Proof. We give an idea of the proof, which is based on the fact that the completion for the $\mathcal{M}$-adic topology on a (topological) k-module R, for $\mathcal{M}$ maximal ideal, is given by

$$\widehat{R} := \varprojlim_n R/\mathcal{M}^n R \tag{4.70}$$

so that if R is isomorphic, as a k-algebra, to the finitely generated k-algebra (here the topological pseudocompact ring k is a field) of the form $k[X]$, where (X) is the unique maximal ideal we can conclude that $\widehat{R} \simeq [\![X]\!]$. Notice that $k[m]$ for m a generator of the unique maximal ideal of $\mathcal{M}_O$ is indeed isomorphic to the 1-dimensional finitely generated k-algebra $\mathcal{O}_{\mathcal{E},O}$. □

Corollary 4.32 The map:

$$m : \mathcal{E} \times \mathcal{E} \to \mathcal{E} \tag{4.71}$$

on the elliptic curve $\mathcal{E}$ as above induces morphisms of formal k-algebras:

$$\widehat{\Delta} : \widehat{\mathcal{O}}_{\mathcal{E},O} \to \widehat{\mathcal{O}}_{\mathcal{E},O} \widehat{\otimes} \widehat{\mathcal{O}}_{\mathcal{E},O} \tag{4.72}$$

$$\widehat{i} : \widehat{\mathcal{O}}_{\mathcal{E},O} \to \widehat{\mathcal{O}}_{\mathcal{E},O} \tag{4.73}$$

$$\widehat{\epsilon} : \widehat{\mathcal{O}}_{\mathcal{E},O} \to k \tag{4.74}$$

$$\widehat{e} : k \to \widehat{\mathcal{O}}_{\mathcal{E},O} \tag{4.75}$$

which turn $(\widehat{\mathcal{O}}_{\mathcal{E},O}, \widehat{\Delta}, \widehat{\epsilon}, \widehat{i})$ into a **formal k-bi-algebra**.

Definition 4.33 Let $\mathcal{E}$ as above, then we denote

$$\widehat{\mathcal{E}} := \mathrm{Spf}_k \widehat{\mathcal{O}}_{\mathcal{E},O} \tag{4.76}$$

the k-**formal group associated** to $\mathcal{E}$.

We have shown that an elliptic curve $\mathcal{E}$ can be considered as a k-formal group scheme which is (smooth and) also a **connected** group (see the section of Lie algebras) since the k-formal algebra associated is a local ring.

4.4 Morphisms between curves

Remark 4.34 From Definition [4.33] above, we deduce that there is a functor $\mathcal{E} \mapsto \widehat{\mathcal{E}}$ from the category of elliptic curves **EC** with their group structure, to the category of smooth connected k-formal groups, such that if:

$$\varphi : (\mathcal{E}_1, O_1) \to (\mathcal{E}_2, O_2) \tag{4.77}$$

is a (k-)group (scheme) homomorphism (i.e. $\varphi(O_1) = O_2$, $\varphi(P+Q) = \varphi(P) + \varphi(Q)$), then there is an induced morphism:

$$\widehat{\varphi} : \widehat{\mathcal{E}_1} \to \widehat{\mathcal{E}_2} \tag{4.78}$$

Before stating and proving the main theorem (of structure of p-divisible groups associated to an elliptic curve $\mathcal{E}$), we state some preparation lemmas and propositions and we give some schematic details of the proof of each of them. From now on $\mathcal{C}$ is a smooth (connected in the elliptic curve case) projective plane curve.

Proposition 4.35 A morphism:

$$\varphi : \mathcal{C}_1 \to \mathcal{C}_2 \tag{4.79}$$

between smooth projective non-singular plane curves is either the constant morphism or it is surjective. Moreover, if φ is not constant then it induces an immersion:

$$\varphi^* : \mathrm{Quot}(\mathcal{C}_2) \to \mathrm{Quot}(\mathcal{C}_2) \tag{4.80}$$

$$f \mapsto f \circ \varphi \tag{4.81}$$

Proof. We give an outline of the proof. By definition of projective subvariety, $\varphi(\mathcal{C}_1)$ must be a closed immersion in the projective plane: the idea is that one can repeat a similar argument as we did in proof of [3.7], considering that in definition ([4.3], *iii*) we defined the variety $\mathcal{C}_1$ as a finite union of affine k-schemes. The points belonging to those affine schemes (which are given by the riparametrizations of the projective plane) are the zeroes of the affine polynomial corresponding to the defining polynomial in those coordinates. Hence we are embedding a finite union of closed subschemes into the projective plane. Being projective, $\varphi(\mathcal{C}_1)$ is also proper (it is a closed complete subvariety of the projective variety $\mathcal{C}_2$) and we let, by definition, the defining polynomial F_1 be irreducible so that $\varphi(\mathcal{C}_1)$ is also irreducible and hence it must be a single point ($\mathcal{C}_1$ is reduced and hence connected) or the whole $\mathcal{C}_2$, being $\mathcal{C}_2$ defined by an irreducible polynomial and hence irreducible too. □

Proposition 4.36 The functor:

$$\mathcal{C} \mapsto \mathrm{Quot}(\mathcal{C}) \tag{4.82}$$

induces an antiequivalence of categories, between the category of the (smooth projective non-singular) curves (over k) and the category of finite transcendent field extensions K/k of dimension 1.

Proof. Again we only suggest how to prove the statement. Consider that the field of rational functions of $\mathcal{C}$ is the field obtained from the elements as in [4.6]. Hence a rational function $\frac{G(x,y,z)}{H(x,y,z)}$ viewed in affine coordinates (with the hyperplane at infinity given by $\{z = 0\}$) is an element $f \in \mathrm{Quot}(k[x,y]/f(x,y))$ being f the defining polynomial of $\mathcal{C}$. Hence we have $\mathrm{Quot}(k[x,y]/f(x,y)) \simeq \mathrm{Quot}(k[x])$ thanks to the relation f between x and y, so that this quotient field is also denoted with $k(x)$, the field obtained from k adding the variable x which is a transcendent extension of k of degree 1. □

Definition 4.37 Let $\varphi : \mathcal{C}_1 \to \mathcal{C}_2$ as above. The degree of the field extension

$$\mathrm{Quot}(\mathcal{C}_1)/\varphi^*(\mathrm{Quot}(\mathcal{C}_2)) \tag{4.83}$$

is called **degree of the morphism** φ and denoted as $\deg(\varphi)$.

Definition/Remark 4.38 Recall that a **discrete valuation ring** R is a local principal ideal domain that is not a field. On $\mathrm{Quot}(R)$ can be defined a discrete valuation:

$$\nu : \mathrm{Quot}(R) \to \mathbb{Z} \cup \infty \tag{4.84}$$

such that $\nu(ab) = \nu(a) + \nu(b)$, $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$, $\nu(0) = \infty$.

Proposition 4.39 Let $\varphi : \mathcal{C}_1 \to \mathcal{C}_2$ a morphism between smooth plane curves over k, which is not constant and such that its degree is n. Then for each point $P \in \mathcal{C}_2(k)$ and points of the fiber $\varphi^{-1}(P) := \{Q_1, ..., Q_r\} \subseteq \mathcal{C}_1(k)$, there are induced (local) morphisms:

$$\varphi_i^* : \mathcal{O}_{\mathcal{C}_2,P} \to \mathcal{O}_{\mathcal{C}_1,Q_i} \tag{4.85}$$

and $\mathcal{O}_{\mathcal{C}_2,P}$, $\mathcal{O}_{\mathcal{C}_1,Q_i}$ are **discrete valuation rings**.

Proof. We give the main idea of the proof, that is based on the fact that, clearly $\mathcal{O}_{\mathcal{C}_2,P}$, $\mathcal{O}_{\mathcal{C}_1,Q_i}$ are local rings having a non-trivial maximal ideal by definition, then one can study the stalk of the associated algebra of an affine variety (which is a finitely generated algebra and also a unique factorization domain) and notice that this is the localization of the associated algebra at the point (maximal ideal) P (resp. Q_i). □

Definition 4.40 Let $\varphi : \mathcal{C}_1 \to \mathcal{C}_2$ a morphism between smooth plane curves over k, which is not constant as above, we denote:

- the value $e_\varphi(Q_i) := \nu(\varphi_i^*(x_P))$, where ν is the discrete valuation of $\mathcal{O}_{\mathcal{C}_1,Q_i}$ and x_P is a generator of the unique maximal ideal of $\mathcal{O}_{\mathcal{C}_2,P}$, is called **ramification index** of φ at Q_i;
- φ is said to be **unramified** at Q if $e_\varphi(Q) = 0$; if this is true for all $Q \in \mathcal{C}_1(k)$ then φ is said to be **unramified**.

We state without proving the following:

Lemma 4.41 Let $\varphi : \mathcal{C}_1 \to \mathcal{C}_2$ a morphism between smooth plane curves over k, then:

$$\deg(\varphi) = \sum_{i=1}^{r} e_\varphi(Q_i) \tag{4.86}$$

for all $P = \varphi(Q_i) \in \mathcal{C}_2(k)$.

The proof is based on the properties of valuations defined on discrete valuation rings and morphisms between them. (See for example [Si]).

Lemma 4.42 Let $\mathcal{C}$ be a smooth (connected in the elliptic curve case) projective plane curve over a field k of char. $p > 0$. Then:

(i) The Frobenius morphism defined as in [3.33]

$$F_{\mathcal{C}}^n : \mathcal{C} \to \mathcal{C}^{(p^n)} \tag{4.87}$$

is (purely) inseparable of degree $q = p^n$.

(ii) If $\varphi : \mathcal{C}_1 \to \mathcal{C}_2$ a non constant morphism between curves, then it factors as:

$$\begin{array}{ccc} \mathcal{C}_1 & \xrightarrow{\quad\varphi\quad} & \mathcal{C}_2 \\ & {\scriptstyle F^n}\searrow \quad \nearrow{\scriptstyle \psi} & \\ & \mathcal{C}^{(p^n)} & \end{array} \tag{4.88}$$

where $p^n = [\mathrm{Quot}(\mathcal{C}_1) : \varphi^*(\mathrm{Quot}(\mathcal{C}_2))]$ and ψ is separable.

4.5 Isogenies

With abuse of notation we denote O both the neutral elements O_1 and O_2 of the two corresponding elliptic curves $\mathcal{E}_1$ and $\mathcal{E}_2$.

Definition 4.43 Let $\varphi : \mathcal{E}_1 \to \mathcal{E}_2$ be a morphism between elliptic curves such that $\varphi(O) = (O)$, such a morphism is called **isogeny**.

Proposition 4.44 The isogenies $\varphi : \mathcal{E}_1 \to \mathcal{E}_2$ as above ar all the (algebraic) group homomorphism (between elliptic curves).

Remark 4.45 As observed in [4.35], if φ is an isogeny that is not the constant morphism $\varphi \equiv O$, then $\varphi(\mathcal{E}_1) = \mathcal{E}_2$, i.e. φ is surjective, and being a homomorphism of groups (schemes) it has finite dimensional kernel since the dimension of the kernel is given thanks to [4.44] by $[\mathrm{Quot}(\mathcal{E}_1) : \varphi^*(\mathrm{Quot}(\mathcal{E}_2))]$ and thanks to the group isomorphism $\mathcal{E}_1/ker(\varphi) \simeq \mathcal{E}_2$. As a consequence the definition of isogeny coincide with the one given in [3.18].

Proposition 4.46 Let $m \in \mathbb{Z}$ and $m \neq 0$.Then the multiplication-by-m map:

$$[m] : \mathcal{E} \to \mathcal{E} \tag{4.89}$$

$$\text{if } m > 0,\ P \mapsto P + \overset{m\text{-times}}{P + ... + P} \tag{4.90}$$

$$\text{if } m < 0,\ P \mapsto [-m](-P) \tag{4.91}$$

for an elliptic curve $\mathcal{E}$, is a non-constant **isogeny**.

From the above propositions, clearly:

- $\mathrm{Hom}_{k-gps}(\mathcal{E}, \mathcal{E}')$ is a torsion-free $\mathbb{Z}$-module:
- $\mathrm{End}_{k-gps}(\mathcal{E})$ is an integral domain of char. $= 0$:

Proposition 4.47 Let $\varphi : \mathcal{E}_1 \to \mathcal{E}_2$ be a non constant isogeny between elliptic curves. Then:

(i) for every $Q \in \mathcal{E}_2$, the cardinality of the fiber $\varphi^{-1}(Q)$ is constant and it is exactly the degree $\deg(\varphi)$;

(ii) for every $Q \in \mathcal{E}_1$ then $e_\varphi(Q)$ is constant and it is exactly the degree $\deg(\varphi)$;

(iii) the map:

$$\ker \varphi(k) \to \mathrm{Gal}(\mathrm{Quot}(\mathcal{E}_1)/\varphi^*(\mathrm{Quot}(\mathcal{E}_2))) \tag{4.92}$$

given by:

$$P \mapsto \tau_P \tag{4.93}$$

is a group isomorphism, where $\tau_P : \mathrm{Quot}(\mathcal{E}_1) \to \mathrm{Quot}(\mathcal{E}_1)$ is the automorphism induced by $Q \mapsto Q + P$.

Proposition 4.48 Let $\varphi : \mathcal{E}_1 \to \mathcal{E}_2$ be a non constant isogeny between elliptic curves of degree $\deg(\varphi) = m$. Consider the map:

$$\widehat{\varphi} : \mathcal{E}_2 \to \mathcal{E}_1 \tag{4.94}$$

induced by:

$$\mathcal{E}_2 \xrightarrow{i_2} \mathrm{Pic}^0(\mathcal{E}_2) \xrightarrow{\varphi^*} \mathrm{Pic}^0(\mathcal{E}_1) \xrightarrow{i_1^{-1}} \mathcal{E}_1 \tag{4.95}$$

then $\widehat{\varphi}$ is the unique isogeny such that:

$$\widehat{\varphi} \circ \varphi = [m]_{\mathcal{E}_1} \tag{4.96}$$

$\widehat{\varphi}$ is called **dual isogeny** of φ.

Proposition 4.49 Let $\mathcal{E}$ be an elliptic curve over a (algebraically closed) field k of charcteristic $p > 0$. Let $[m] : \mathcal{E} \to \mathcal{E}$ be the multiplication-by-m map as before. Then:

(i) if $p \nmid m$, we have that $\ker[m](k) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$;

(ii) if $m = p^n$ then it could happen that:

- $\ker[p^n](k) = \{0\}$ and we call the curve **supersingular** elliptic curve;
- $\ker[p^n](k) = \mathbb{Z}/p^n\mathbb{Z}$ and we call the curve **ordinary** elliptic curve.

4.6 p-divisible group of an elliptic curve

Thanks to the previous considerations about isogenies between elliptic curves we can now give an outline of the proof of the main result of this section. Our purpose is to understend not only the groups $\ker[p^n](k)$ as we did before, but also in general the behaviour of the groups $\ker[m]$.

Theorem 4.50 Let $\mathcal{E}$ be an elliptic curve over an algebraically closed field k of characteristic $p > 0$. And let, as always, O be the identity of the group law defined on $\mathcal{E}$. Then:

- if l is a prime number such that $l \neq p$, the inductive system $(\ker[l^n], i_n)$ represents the l-divisible group associated to $\mathcal{E}$ given by:

$$\varinjlim_n \ker[l^n] \simeq \varinjlim_n (\mathbb{Z}/l^n\mathbb{Z})^2 \tag{4.97}$$

  which is the constant BT group of height 2.

- if $l = p$ then the p-divisible group associated to $\mathcal{E}$ is:
  - the connected Barsotti-Tate group of height 2 given by:

$$\varinjlim_n \ker[p^n] \simeq \varinjlim_n \mathcal{O}_{\ker[p^n],O} \tag{4.98}$$

    if $\mathcal{E}$ is **supersingular**;
  - the product of a constant BT-group of height 1 with a connected BT-group of heigth 1 given by:

$$\varinjlim_n \ker[p^n] \simeq \varinjlim_n (\mathbb{Z}/p^n\mathbb{Z}) \times \mathcal{O}_{\ker[p^n],O} \tag{4.99}$$

    if $\mathcal{E}$ is **ordinary**.

Proof. Thanks to Definition [4.6], to Proposition [4.10] and to the construction which follows, of the group law of an elliptic curve, the elliptic curve $\mathcal{E}$ can be considered as a k-

group scheme or equivalenltly as an abelian variety of dimension 1 over k. As a consequence we can consider the fibers $\mathrm{Spec}(k) \to \mathcal{E}$, which are the geometrical points of $\mathcal{E}$. Moreover thanks to Corollary [4.31] $\widehat{\mathcal{E}}$ can be viewed as a formal k-scheme with associated (formal) algebra the algebra: $\widehat{\mathcal{O}}_{\mathcal{E},O} \simeq k[\![x]\!]$, where x stands for a generator of the unique maximal ideal $\mathcal{M}_O$ of $\mathcal{O}_{\mathcal{E},O}$. Now we proceed by steps:

Step 1: let l be a prime number and consider the k-scheme morphism

$$[l^n] : \mathcal{E} \to \mathcal{E} \tag{4.100}$$

which is the (isogeny given by) multiplication-by-l^n map (thanks to [4.46]). Then the kernel $\ker[l^n]$ is given, by definition, considering the pull-back (the fiber product):

$$\begin{array}{ccc} \mathcal{E} \times_{\mathcal{E}} \mathrm{Spec}(k) & \xrightarrow{\mathrm{pr}_2} & \mathrm{Spec}(k) \\ {\scriptstyle \mathrm{pr}_1}\downarrow & & \downarrow{\scriptstyle e} \\ \mathcal{E} & \xrightarrow{[l^n]} & \mathcal{E} \end{array} \tag{4.101}$$

where $e : \mathrm{Spec}(k) \to \mathcal{E}$ is the unit map of the multiplication defined on $\mathcal{E}$. As a consequence, the closed points (the sections $\mathrm{Spec}(k) \to \mathcal{E}$), i.e. the points $P \in \ker[l^n](k)$, make this diagram commutative:

$$\begin{array}{ccc} \mathcal{E} & \xrightarrow{[l^n]} & \mathcal{E} \\ & {\scriptstyle P}\nwarrow \quad \nearrow{\scriptstyle e} & \\ & \mathrm{Spec}(k) & \end{array} \tag{4.102}$$

This diagram induces a diagram on the local rings corresponding to the stalks at the points of the curve (thanks to considerations similar to [4.30]), we use the notation $(-)^{\#}$ to indicate the corresponding maps:

$$\begin{array}{ccc} \mathcal{O}_{\mathcal{E},P} & \xleftarrow{[l^n]^{\#}} & \mathcal{O}_{\mathcal{E},O} \\ & {\scriptstyle P^{\#}}\searrow \quad \swarrow{\scriptstyle \epsilon} & \\ & k & \end{array} \tag{4.103}$$

where $\epsilon = O^{\#}$ is induced by the co-unit on $\mathcal{O}_{\mathcal{E}}(\mathcal{E})$. Therefore we deduce from the diagram that:

$$\mathcal{O}_{\ker[p^n],P} \simeq \mathcal{O}_{\mathcal{E},P}/([l^n]^{\#}\mathcal{M}_O)\mathcal{O}_{\mathcal{E},P} \tag{4.104}$$

for every point $P \in \mathcal{E}(k)$, and in particular for O:

$$\mathcal{O}_{\ker[p^n],O} \simeq \mathcal{O}_{\mathcal{E},O}/([l^n]^{\#}\mathcal{M}_O)\mathcal{O}_{\mathcal{E},O} \tag{4.105}$$

To be more explicit consider the image of the maximal ideal given by $[l^n]^{\#}(\mathcal{M}_O)$, then the points $P \in \ker[l^n]$ are those points such that $P^{\#}([l^n]^{\#}(\mathcal{M}_O)) = \epsilon(\mathcal{M}_O) = 0$, since the unique maximal ideal of the field k is 0. Hence $[l^n]^{\#}(\mathcal{M}_O)$ must be the zero of $\mathcal{O}_{\ker[l^n],O}$ in order to make the diagram above commutative.

Step 2: We have that:

$$\ker[l^n] = \mathrm{Spec} \prod_{P \in \ker[l^n](k)} \mathcal{O}_{\ker[l^n],P} \tag{4.106}$$

This is clear if we consider that the disjoint union of two geometric points of $\ker[l^n](k)$: $Q \sqcup P = (\mathrm{Spec}(k) \to \mathcal{E}) \sqcup (\mathrm{Spec}(k) \to \mathcal{E})$ which correspond to the disjoint union of the maps $(\mathcal{O}_{\mathcal{E},P} \to k) \sqcup (\mathcal{O}_{\mathcal{E},Q} \to k)$ which is nothing but the map $\mathcal{O}_{\mathcal{E},P} \times \mathcal{O}_{\mathcal{E},Q} \to k$. Finally the kernel $\ker[l^n]$ is the disjoint union all the geometrical sections such that the first diagram 4.94 above commutes. Moreover, since the translation map:

$$\tau_P : \mathcal{E} \to \mathcal{E} \tag{4.107}$$

$$Q \mapsto P + Q \tag{4.108}$$

is an isomorphism of k-schemes (not of groups) then:

$$\mathcal{O}_{\ker[l^n],P} \simeq \mathcal{O}_{\ker[l^n],Q} \tag{4.109}$$

as k-algebras, for all distinct $P, Q \in \mathcal{E}(k)$.

Step 3: Let now $l \neq p$. Thanks to the above propositions [4.42] and [4.49] $[l^n]$ is inseparable. So that we get, for each $P \in \ker[l^n](k)$ that the map:

$$[l^n]^{\#} : \mathcal{O}_{\mathcal{E},O} \to \mathcal{O}_{\mathcal{E},P} \tag{4.110}$$

is an isomorphism so that:

$$\mathcal{O}_{\ker[l^n],P} \simeq \mathcal{O}_{\mathcal{E},P}/([l^n]^{\#}\mathcal{M}_O)\mathcal{O}_{\mathcal{E},P} \simeq \mathcal{O}_{\mathcal{E},P}/(\mathcal{M}_P)\mathcal{O}_{\mathcal{E},P} \simeq k \tag{4.111}$$

and therefore:

$$\ker[l^n] = \mathrm{Spec}(k^{\ker[l^n](k)}) = \mathrm{Spec}(k^{(\mathbb{Z}/l^n\mathbb{Z})^2}) = (\mathbb{Z}/l^n\mathbb{Z})^2 \tag{4.112}$$

and we proved the firs claim. In particular we used the fact that $\mathrm{Spec}(k^{\ker[l^n](k)})$ is the constant k-scheme of order l^n.

Step 4: Let now $l = p$. Then, if $\ker[p^n](k) = 0$, so that we are in the supersingular case, the formula (4.106) becomes:

$$\ker[p^n] = \mathrm{Spec}(\mathcal{O}_{\ker[p^n],O}) = \mathrm{Spec}(\mathcal{O}_{\mathcal{E},O}/([p^n]^{\#}\mathcal{M}_O)\mathcal{O}_{\mathcal{E},O}) \tag{4.113}$$

which is a connected and finite k-group of order p^{2n}.

Step 5: Now consider the ordinary case when $\ker[p^n](k) = \mathbb{Z}/p^n\mathbb{Z}$. Notice that for each P, $\mathcal{O}_{\ker[p^n],P}$ is a finite k-algebra (of rank p^n) and the maximal étale sub-algebra contained

by $\mathcal{O}_{\ker[p^n],P}$ is k so that:

$$\prod_{P\in\ker[p^n](k)} \mathcal{O}_{\ker[p^n],P} \simeq (k^{\ker[p^n](k)} \otimes_k \mathcal{O}_{\ker[p^n],O}) \tag{4.114}$$

hence:

$$\ker[p^n] = (\mathbb{Z}/p^n\mathbb{Z}) \times \mathrm{Spec}(\mathcal{O}_{\ker[p^n],O}) \tag{4.115}$$

and it is the product of the constant k-group by a connected k-group both of order p^n. The proof is complete. □

Notice that, intuitively, passing to the (direct) limit the systems of k-groups we have obtained from the theorem, the connected part becomes a single point of the variety, and we get the result of Proposition [4.49]. Moreover one could show that the kernel of an isogeny φ is the Cartiér dual of the kernel of the φ-dual isogeny $\widehat{\varphi}$. Namely:

$$\ker\varphi = \ker(\mathtt{D}\widehat{\varphi}) \tag{4.116}$$

and we are rephrasing what we already said in Theorem [3.46] (and the following observations). As a consequence, applying this for the isogeny $[m] = \widehat{[m]}$ we get:

$$\widehat{\mathcal{E}} = \varinjlim_n \ker[p^n] = \varinjlim_n \ker[p^n]^0 \simeq \varinjlim_n \mathtt{D}(\ker[p^n]^0) = \tag{4.117}$$

$$= \varinjlim_n \mathtt{D}(\mathbb{Z}/p^n\mathbb{Z}) = \varinjlim_n \mu_{p^n} = \mu_{p^\infty} = \widehat{\mathbb{G}_m} \tag{4.118}$$

since the formal algebra of the multiplicative group is the algebra of its Cartiér dual, which is the p-divisible group associated to the inductive system of p^n-roots of unit; this comes from [3.30].

Bibliography

[De] Demazure Michel, *Lectures on p-Divisible Groups*, Springer-Verlag, 2^{nd} edition, Berlin, 1986.

[Fo] Fontaine Jean-Marc, *Groupes p-divisibles sur les corps locaux*, Astérisque, tome 47-48, Société mathématique de France, 1977.

[Ga] Gathmann Andreas, *Algebrai Geometry*, Class Notes TU Kaiserslautern, 2021-2022.

[GD] Grothendieck Aléxandre, Dieudonné Jean Alexandre, *Eléments de Géométrie AlgEbrique*, Vol. I-II-III, Springer-Verlag, Berlin, 1971.

[Ha] Robin Hartshorne, *Algebrai Geometry*, Springer Graduate Texts in Mathematics 52, 1977.

[Il] Illusie Luc, *Grothendieck at Pisa : crystals and Barsotti-Tate groups*, Talk at the Colloquium De Giorgi, Pisa, April 23, 2013.

[Lo] Longo Matteo, *Appunti sui gruppi p-divisibili III*, Dispensa sul corso tenuto dal professor Cristante, Padova.

[ML] Mac Lane Saunders, *Categories for the Working Mathematician*, Springer-Verlag, New York, second edition, 1998.

[Ma] Maschio Samuele, *The categorical eyeglasses*, Un corso di teoria delle categorie e logica categoriale, Padova, 2021.

[Mi1] Milne S. James, *Basic Theory of Affine Group Schemes*, Notes, Version 1, 2012.

[Mi2] Milne S. James, *Elliptic Curves*, BookSurge Publishers, 2006.

[Ne] Neukirch Jurgen, *Algebraic Number Theory*, Springer-Verlag, Berlin, English version, 1999.

[Sc] Schapira Pierre, *Algebra and Topology*, Notes for the Course at Paris VI University, 2007-2008.

[Se] Serre Jean-Pierre, *Groupes p-divisibles*, Séminaire N. Bourbaki, 1968.

[Si] Silverman H. Joseph, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer, 2^{nd} edition, New York, 2009.

[St] Stix Jakob, *A course on finite flat group schemes and p-divisible groups*, Class notes, Heidelberg, 2009.

[Ta] Tate John, *p-Divisible groups*, Proceeding of a conference on Local Fields, Driebergen 1966, pp. 158-183, Springer, 1966.

[Vi] Vistoli Angelo, *Notes on Grothendieck topologies, fibered categories and descent theory*, Class notes, Pisa, 2008.

Acknowledgements

In conclusion, I would like to express my deepest gratitude to Professor Matteo Longo, who has assisted, guided, and advised me throughout the writing of this thesis and supported me throughout my academic journey. I also wish to thank Professor Maria Emilia Maietti once again for her guidance during the final phase of my undergraduate studies. My thanks also go to Professors Roberto Monti and Samuele Maschio for their valuable advice at the end of their respective courses (Calculus of Variations and Logic 2) at Padua.

I am profoundly grateful to my family for their unwavering support and belief in me throughout my studies. They have given me the strength to be proactive and the heart to believe in life's opportunities. In particular, I thank my mother Elisabetta, my father Andrea, as well as Chandra and Matteo; my grandparents Giovanna, Gabriella, and Flavio, my dear grandfather Ugo, and everyone who has always been there for me.

I deeply thank Sofia for her affection and support over these months, as well as her patience in always being by my side. I am grateful for her being the best part of me and for bringing light into some difficult moments.

I also wish to thank Antonella and all my dear friends who have always brightened my days with joy and color: Stefano, Davide, Filippo, Ayelen, Lara, Francesca, Sophie, Sharon, Andrea, Filippo, Shanti, Marta, Stefano, Luce and Luana; and all the band members: Alessandro, Alessandro, Michele, and Jacopo, who provide daily inspiration.

Finally, I would like to thank Professor Monica Giacomi, who has always been a guide for my mathematical passion.