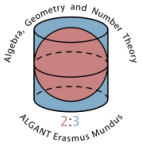


Università de Bordeaux 1

Département de Mathématiques

Mémoire Master 2

presented by

Marco Galvagni

Group schemes of prime order

advisor

Professor Dajano Tossici

Academic year 2015/2016


université
de BORDEAUX

Contents

1 Introduction on group schemes **3**

1.1 Preliminaries on Group Schemes . . . 3

1.1.1 Group objects in a category . . . 3

1.1.2 Affine group schemes . . . 5

1.1.3 Subgroups; injective morphisms . . . 7

1.1.4 Quotient groups; surjective homomorphisms . . . 9

1.1.5 Examples . . . 10

1.2 The connected components of an affine group . . . 13

1.2.1 Idempotents and connected components . . . 13

1.2.2 Affine groups . . . 16

2 A classification of group schemes of prime order **18**

2.1 Two general theorems . . . 18

2.2 A classification theorem . . . 23

2.2.1 Witt vectors . . . 23

2.2.2 A classification theorem . . . 24

2.2.3 Examples . . . 30

Introduction

Our aim is to give a classification of commutative group schemes G of prime order p over a base scheme S. It is well known that there exists only one group of order p. Despite of this there exist a lot of group schemes of order p. The complete classification, under weak hypothesis, has been obtained by Oort and Tate in [TO70] and this is the object of this thesis.

In the first part we will give some preliminaries on group schemes which are basically a generalisation of the concept of groups in the context of the theory of schemes. We start with the definition of group object in a general category, and then we explain in details what is this object in the categories of affine schemes. In particular we show that it coincides with the concept of Hopf algebras in the category of rings and that there is a canonical way to pass from one to the other.

We continue with some generalities on morphisms of affine group schemes; what does it mean to be injective, surjective? Similarly we give the definition of subgroup and quotient group.

It follows a section of examples: first we construct the Cartier Dual of a finite and locally free affine group scheme, and then we present some example such as the multiplicative group scheme, the constant group scheme and the group of nth-roots of unity μ_n.

We conclude the first part with a section about the connected components of a finite and locally free affine group scheme over a field. In particular we show that we can assign to each group G a connected subgroup G° (which represent the connected component of the identity) and an ètale quotient group $\pi_0(G)$ such that the sequence

$$1 \to G^\circ \to G \to \pi_0(G) \to 1$$

is exact.

In the second part of the thesis we generalize the concept of affine schemes: we don't require any more that G is of the form $\operatorname{Spec} A$ with A an Hopf-algebra, but we ask that G is a scheme over S with an affine morphism $G \to S$. This permits us to cover G with affine group schemes which determine completely G; in particular when we will write $G = \operatorname{Spec} A$, A will be a quasi coherent sheaf of algebras over the scheme S. We also ask that such group schemes have a fixed prime dimension.

We begin with a theorem due to Deligne which is the analogous of Lagrange Theorem for groups and states that a commutative group of order m is "killed" by m; note that we don't know if this result is true for non commutative group schemes. This will be essential in the manipulation of the group scheme μ_p in such a way that every group scheme of order p can be written similarly. Deligne's Theorem permits us also to consider an action of $\mathbb{F}_p$ over our group schemes; in particular the requirement that $\mathbb{F}_q$ with $q = p^n$ acts on G will permit to extend the classification on commutative group schemes of order p^n due to Raynaud work.

After the proof that all group schemes of prime order must be commutative, (even though this is not in general true for example for group of order p^2) we arrive to the classification of Tate and Oort.

Here we have to assume that the base group scheme is over the ring

$$\Lambda_p = \mathbb{Z}[\chi(\mathbb{F}_p), \frac{1}{p(p-1)}] \cap \mathbb{Z}_p.$$

where $\chi : \mathbb{F}_p \to \mathbb{Z}_p$ is the Teichmuller character. Note in particular the $\Lambda_2 = \mathbb{Z}$ and so we have a completely classification of commutative group schemes of order 2.

Theorem 0.0.1. *For any scheme S over* $\operatorname{Spec}(\Lambda)$ *we have a bijection between the isomorphism classes of S-groups of order p and the isomorphism classes of triples (L, a, b) consisting of an invertible $\mathcal{O}_S$-module L, a section $a \in \Gamma(S, L^{\otimes(p-1)})$, and a section $b \in \Gamma(S, L^{\otimes(1-p)})$, such that $a \otimes b = w_p 1_{\mathcal{O}_S}$.*

The idea is that L represents the structure of module of the sheaf of algebras, a its multiplication and b the multiplication of the group.

This theorem applies in particular to the case of group schemes over a local complete noetherian base ring. In this case the isomorphism classes of group schemes of order p correspond to equivalence classes of the factorizations $p = ac$; two such factorizations $p = a_1c_1$, $p = a_2c_2$ are considered equivalent if there is an invertible element u in the base ring such that $a_2 = u^{p-1}a_1$ and $c_2 = u^{1-p}c_1$.

Chapter 1

Introduction on group schemes

1.1 Preliminaries on Group Schemes

1.1.1 Group objects in a category

Let $\mathfrak{C}$ be a category with arbitrary finite products.

Definition 1.1.1. A group object in $\mathfrak{C}$ is a representable functor G : $\mathfrak{C} \to \mathfrak{Set}$ together with a natural transformation $\mu : G \times G \to G$ such that, for all R-algebras S,

$$\mu(S) : G(S) \times G(S) \to G(S)$$

is a group structure on $G(S)$.

In the following we want to show that the properties of group of $G(S)$ pass on G which can be seen in some sense as a group.

Let $F : \mathfrak{C} \to \mathfrak{Set}$ be a controvariant functor, A be an object of $\mathfrak{C}$ and define $h_A := \mathrm{Hom}_{\mathfrak{C}}(\_, A)$. The Yoneda Lemma says that to give a natural transformation $h_A \to F$ is the same as giving an element of $F(A)$. More precisely a natural transformation $T : h_A \to F$ defines an element

$$a_T = T_A(\mathrm{Id}_A)$$

of $F(A)$. Conversely an element a of $F(A)$ defines a map

$$h_A(R) \to F(R)$$

$$f \to F(f)(a)$$

for each $R \in \mathfrak{C}$. The map is natural in R and so this family of maps is a natural transformation.

Lemma 1.1.2. *The maps $T \to a_T$ and $a \to T_a$ are inverse bijections*

$$\mathrm{Nat}(h_A, F) \cong F(A)$$

natural in both A and F.

Remark. Take $F = h_B$; in this case we have that $\underline{\mathrm{Hom}}(h_A, h_B) \cong \mathrm{Hom}(A, B)$. In particular if G is an object in $\mathfrak{C}$, give a map $G \times G \to G$ is the same as give a map $h_{G\times G} \cong h_G \times h_G \to h_G$. So it's easy to see that the old definition of affine group coincide with this new one:

Definition 1.1.3. A group object in the category $\mathfrak{C}$ is a pair consisting of an object $G \in \mathrm{Ob}(\mathfrak{C})$ and a morphism $\mu : G \times G \to G$ such that for any object $Z \in \mathrm{Ob}(\mathfrak{C})$ the obvious map $G(Z) \times G(Z) \to G(Z)$ defines a group, where $G(Z) := \mathrm{Hom}(Z, G)$.

So in the previous remark we have substantially seen that the product of $h_G(Z)$ pass to a product map $G \times G \to G$. So it is natural to think that this passage happens also for all the other properties concerning the product.

Proposition 1.1.4. *An object G and a morphism $\mu : G \times G \to G$ define a group object if and only if the following properties hold:*

1. *(Associativity) The following diagram is commutative:*

$$\begin{array}{ccc} G\times G\times G & \xrightarrow{\mu\times id} & G\times G \\ {\scriptstyle id\times\mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ G\times G & \xrightarrow{\mu} & G \end{array}$$

2. *(Identity Element) There exists a morphism $e : * \to G$ where $*$ is the final object of $\mathfrak{C}$, such that the following diagram commutes:*

$$\begin{array}{ccc} *\times G & \xrightarrow{e\times id} & G\times G \\ & {\scriptstyle pr_2}\searrow \quad \swarrow{\scriptstyle \mu} & \\ & G & \end{array}$$

3. *(Inverse Element) There exists a morphism $i : G \to G$ such that the following diagram commutes:*

$$\begin{array}{ccc} G\times G & \xrightarrow{id\times i} & G\times G \\ {\scriptstyle diag}\uparrow & & \downarrow{\scriptstyle \mu} \\ G & \xrightarrow{e\circ\epsilon} & G \end{array}$$

where ϵ is the final morphism.

Proof. The 'if' part follows by taking Z-valued points. For the 'only if' part:

1. (Associativity) Take $Z = G \times G \times G$ and apply the associativity in $G(Z)$. In detail take p_1, p_2, p_3 $G \times G \times G \to G$. Now
$$(p_1 * p_2) * p_3 = \mu(\mu(p_1, p_2), p_3) = \mu(\mu \times \mathrm{Id})$$
$$p_1 * (p_2 * p_3) = \mu(p_1, \mu(p_2, p_3)) = \mu(\mathrm{Id} \times \mu).$$
We conclude using the associativity of the product.

2. (Identity element) The morphism $e : * \to G$ is defined as the identity element of $G(*)$. For any Z consider the map $G(*) \to G(Z)$ defined by composing a morphism $* \to G$ with the unique morphism $Z \to *$. It's easy to see that this map is a morphism of groups and so maps e to the identity element of $G(Z)$. In particular taking $Z = G$ and remembering that the map $\epsilon \times \mathrm{Id} : G \to * \times G$ is an isomorphism we obtain

$$\begin{array}{ccc} G & \xrightarrow{\epsilon\times\mathrm{Id}} & *\times G \\ {\scriptstyle \mathrm{Id}}\downarrow & & \downarrow{\scriptstyle e\times\mathrm{Id}} \\ G & \xleftarrow{\mu} & G\times G \end{array}$$

3. (Inverse element) The morphism $i : G \to G$ is defined as the inverse in the group $G(G)$ of the element $\mathrm{Id} \in G(G)$. The rest is analogous to the previous one.

□

Definition 1.1.5. A group object G is said to be commutative if for every object $Z \in \mathrm{Ob}(\mathfrak{C})$, $G(Z)$ is a commutative group.

Lemma 1.1.6. *A group object is commutative if and only if the following diagram is commutative:*

$$\begin{array}{ccc} G\times G & \xrightarrow{\sigma} & G\times G \\ & {\scriptstyle \mu}\searrow \quad \swarrow{\scriptstyle \mu} & \\ & G & \end{array}$$

where σ is the morphism which interchanges the two factors.

Proof. Take $Z = G \times G$ and we apply the commutativity in $G(Z)$ to $\mathrm{Id} \in (G \times G)(Z)$. In detail: take p_1 and p_2 the projections $G \times G \to G$. Now $p_1 * p_2 = \mu \circ (p_1, p_2) = \mu \circ \mathrm{Id} = \mu$ and $p_2 * p_1 = \mu \circ (p_2, p_1) = \mu \circ \sigma$. By the commutativity it follows that $\mu = \mu \circ \sigma$. □

1.1.2 Affine group schemes

Let $\mathfrak{Rings}$ be the category of commutative noetherian rings with unity; from now on all rings are supposed to be in $\mathfrak{Rings}$. Let $R, A \in \mathfrak{Rings}$, together with a morphism $R \to A$, then A is called a unitary R-algebra. Equivalently A is an R-module together with two morphisms of R-modules $e : R \to A$ and $\mu : A \otimes_R A \to A$ such that μ is associative and commutative and e induces a unit.

We denote the category of unitary R-algebras by $R - \mathfrak{Alg}$ and so we have an anti-equivalence

$$R - \mathfrak{Alg} \longleftrightarrow \mathfrak{aff}.R - \mathfrak{Sch}$$

where $\mathfrak{aff}.R - \mathfrak{Sch}$ denotes the category of affine schemes over Spec R. The object $* =$ Spec R is a final object in $\mathfrak{aff}.R - \mathfrak{Sch}$.

Definition 1.1.7. Let R be a unitary ring. An affine commutative group scheme over Spec R is a commutative group object in the category of affine schemes over Spec R.

The morphisms associated with the group object G correspond to the following homomorphisms of R-modules:

1. $e : R \to A$ and $\mu : A \otimes_R A \to A$ which are the structure map of the R-algebra A.
2. $\epsilon : A \to R$ called the counit, corresponds to the morphism $* \to G$.
3. $m : A \to A \otimes_R A$, called the comultiplication, corresponds to the map $G \times G \to G$.
4. $i : A \to A$, corresponds to the morphism $G \to G$ sending an element to its inverse.

In particular the axioms for a commutative affine group scheme translate to those:

1. μ is associative and m is coassociative:

$$\mu \circ (\mathrm{Id} \otimes \mu) = \mu \circ (\mu \otimes \mathrm{Id})$$

$$(m \otimes \mathrm{Id}) \circ m = (\mathrm{Id} \otimes m) \circ m$$

2. μ is commutative and m is cocommutative:

$$\mu \circ \sigma = \mu$$

$$\sigma \circ m = m$$

3. e is unit for μ and ϵ is counit for m:

$$\mu \circ (e(1) \otimes \mathrm{Id}) = \mathrm{Id}$$

$$(\epsilon \otimes \mathrm{Id}) \circ m = 1 \otimes \mathrm{Id}$$

4. m is morphism of unitary rings (preserves product and unity):

$$m \circ \mu = (\mu \otimes \mu) \circ (\mathrm{Id} \otimes \sigma \otimes \mathrm{Id}) \circ (m \otimes m)$$

$$m(e(1)) = e(1) \otimes e(1)$$

5. ϵ is morphism of unitary rings:

$$\epsilon \circ \mu = \epsilon \otimes \epsilon$$

$$\epsilon \circ e = \mathrm{Id}$$

6. i is morphism of unitary rings:

$$i \circ \mu = \mu \circ (i \otimes i)$$

$$i \circ e = e$$

7. i is coinverse for m:

$$e \circ \epsilon = \mu \circ (\mathrm{Id} \otimes i) \circ m$$

Definition 1.1.8. An R-module A together with maps μ, ϵ, e, m, and i satisfying the above axioms is called a cocommutative R-Hopf algebra.

We have seen that give an affine group scheme G over R is the same as giving a R-Hopf algebra A. In particular we show that there exist a canonical choice for A which is called the coordinate ring of G and denoted by $\mathcal{O}(G)$.

Let $\mathbb{A}^1$ be the functor sending a R-algebra S to its underlying set,

$$\mathbb{A}^1 : \mathfrak{Alg}_R \to \mathfrak{Set}.$$

Let $\mathrm{G} : \mathfrak{Alg}_R \to \mathfrak{Grp}$ be a a functor, and let $G_0 = (\text{forget}) \circ G$ be the underlying set - valued functor. Define A to be the set of natural transformation from G_0 to $\mathbb{A}^1$

$$A = \mathrm{Nat}(G_0, \mathbb{A}^1).$$

Thus an element f of A is a family of maps of sets

$$f_R : G_0(S) \to S$$

such that, for every morphism of R-algebras $\phi : S \to S'$, the diagram

$$\begin{array}{ccc} G_0(S) & \xrightarrow{f_S} & S \\ {\scriptstyle G_0(\phi)}\downarrow & & \downarrow{\scriptstyle \phi} \\ G_0(S') & \xrightarrow{f_{S'}} & S' \end{array}$$

commutes. For $f, f' \in A$ and $g \in G_0(S)$, define

$$(f \pm f')_S(g) = f_S(g) \pm f'_S(g)$$
$$(ff')_S(g) = f_S(g) f'_S(g).$$

With these operations, A becomes a commutative ring, and even a R-algebra because each $c \in R$ defines a natural transformation

$$c_S : G_0(S) \to S,$$
$$c_S(g) = c \text{ for all } g \in G_0(S).$$

An element $g \in G_0(S)$ defines a morphism $f_S \to f_S(g) : A \to S$ of R-algebras. In this way, we get a natural transformation $\alpha : G_0 \to h^A$ of set valued functors.

Remark. In the following for affine groups we mean affine group schemes.

Proposition 1.1.9. *The functor G is an affine group if and only if α is an isomorphism.*

Proof. If α is an isomorphism, then certainly G_0 is representable (and so G is an affine group). Conversely, suppose that $G_0 = h^B$. Then

$$A = \mathrm{Nat}(G_0, \mathbb{A}^1) = \mathrm{Nat}(h^B, \mathbb{A}^1) \cong \mathbb{A}^1(B) = B.$$

Thus $A \cong B$ as set but it's not difficult to show that it is an isomorphism of R-algebras. Denote with $y : A \cong B$ the isomorphism. The main point is that in this case the Yoneda Lemma tells us that $\mathrm{Nat}(h^B, \mathbb{A}^1)$ are the "evaluations". So for example we check that the isomorphism preserves products: let $a, b \in A = \mathrm{Nat}(h^B, \mathbb{A}^1)$ and $a_1, b_1 \in B$ their image through the isomorphism. Then fix an R-algebra S and let $g \in h^B(S)$:

$$ab(g) = a(g) * b(g) = g(a_1) * g(b_1) = g(a_1 b_1)$$

which implies that $a_1 b_1$ is the image of ab through the isomorphism.

Clearly y induces another isomorphism

$$h^B \to h^A$$

which for a fixed R-algebra S works as

$$g \to g \circ y$$

if $g \in h^B(S)$. We want to show that this isomorphism is α. We remember that

$$\alpha_S : h^B(S) \to h^A(S)$$
$$g \to (a \to a(g))$$

but $a(g) = g(b)$ where $b = y(a)$ and so we see that α and our isomorphism coincide. □

Thus, for an affine group G, $\mathcal{O}(G) := \mathrm{Hom}(G, \mathbb{A}^1)$ is a canonical coordinate ring. We already know how the maps μ, m, ϵ, e, i work on this ring (i.e. they have to satisfies all the previous axioms of Hopf-algebras); but it's also interesting to understand their behaviour when A is seen as $\mathcal{O}(G) = \mathrm{Hom}(G, \mathbb{A}^1)$. If $f_1 \in \mathcal{O}(G)$ and $f_2 \in \mathcal{O}(G)$, then $f_1 \otimes f_2$ defines a function $(f_1 \otimes f_2)_S : G(S) \times G(S) \to S$ by the rule:

$$(f_1 \times f_2)_S(a, b) = (f_1)_S(a) * (f_2)_S(b).$$

For $f \in \mathcal{O}(G)$, $m(f)$ is the unique element of $\mathcal{O}(G) \otimes \mathcal{O}(G)$ such that

$$(m(f))_S(a, b) = f_S(ab) \text{ for all R-algebra S and } a, b \in G(S)$$

and $\epsilon(f)$ is the element $f(1_G)$ of R, moreover $i(f)$ is the unique element of $\mathcal{O}(G)$ such that

$$(if)_S(a) = f_S(a^{-1}) \text{ for all S and all } a \in G(S).$$

All the proofs follow by definitions, we prove only the last to give an example:

$$f_S(a^{-1}) = i(a)(f_S) = (a \circ i)(f_S) = (a)(i(f_S)) = (if_S)(a).$$

1.1.3 Subgroups; injective morphisms

Definition 1.1.10. A homomorphism of affine groups $\phi : G \to H$ over Spec S is a morphism in $\mathfrak{aff}.S - \mathfrak{Sch}$ such that the induced morphism $G(Z) \to H(Z)$ is a homomorphism of groups for all $Z \in \mathfrak{aff}.S - \mathfrak{Sch}$.

Remark. Obviously there is an analogous definition of homomorphism of affine group stated in terms of S-Hopf algebras; a morphism of S-Hopf algebras is a S linear map which "commutes" with the maps μ, m, ϵ, e, i.

Proposition 1.1.11. *A morphism of affine groups $u : H \to G$ is an isomorphism if and only if*

1. *the map $u(R) : H(R) \to G(R)$ is injective for all S-algebras R, and*
2. *the morphism $u^\natural : \mathcal{O}(G) \to \mathcal{O}(H)$ is faithfully flat.*

When S is a field 2) *can be replaced with:*

1. *the morphism $u^\natural : \mathcal{O}(G) \to \mathcal{O}(H)$ is injective.*

Proof. See Proposition 1.1 pag 87 of [Mil12]. □

Definition 1.1.12. Let $u : H \to G$ be a morphism of affine groups over S.

1. We say that u is a monomorphism if $u(R) : H(R) \to G(R)$ is injective for all S-algebras R.
2. We say that u is a closed immersion if the map $u^\natural : \mathcal{O}(G) \to \mathcal{O}(H)$ is surjective.

Remark. We observe that a morphism is a monomorphism if and only if it is a epimorphism in the category of $\mathcal{O}_S$-algebras if and only if it is a monomorphism in the category of affine groups over S.

Proposition 1.1.13. *If $u : H \to G$ is a closed immersion, then it is a monomorphism. The converse is true when S is a field.*

Proof. if $u^\natural$ is surjective, then any two morphisms $\mathcal{O}(H) \to R$ that become equal when composed with $u^\natural$ must already be equal, but this means that $H(R) \to G(R)$ is injective.

Now suppose that S is a field and that $u(R)$ is injective for all R. The morphism $u^\natural$ factors into morphism of Hopf algebras

$$\mathcal{O}(G) \twoheadrightarrow u^\natural(\mathcal{O}(G)) \hookrightarrow \mathcal{O}(H).$$

Let H' be the affine group whose Hopf algebra is $u^\natural(\mathcal{O}(G))$. Then u factors into

$$H \to H' \to G$$

and the injectivity of $u(R)$ implies that $H(R) \to H'(R)$ is injective for all S-algebras R. Because $\mathcal{O}(H') \to \mathcal{O}(H)$ is injective, the previous proposition shows that the map $H \to H'$ is an isomorphism. □

Definition 1.1.14. An affine closed subgroup H of an affine group G is a functor $\mathfrak{aff}.S - \mathfrak{Sch} \to \mathfrak{Groups}$ such that:

1. H_0 is a subfunctor of G_0,
2. $H(R)$ is a subgroup of $G(R)$ for all S-algebras R, and
3. H is representable by a quotient of $\mathcal{O}(G)$.

Definition 1.1.15. Let A be an Hopf algebra. An ideal I of A is said to be an Hopf ideal if

1. $m(I) \subseteq I \otimes A + A \otimes I$,
2. $\epsilon(I) = 0$, and
3. $i(I) \subseteq I$.

Remark. In particular the kernel of any morphism of Hopf algebras is a Hopf ideal.

Proposition 1.1.16. *The affine closed subgroups of an affine group G are in natural one - to - one correspondence with the Hopf ideals on $\mathcal{O}(G)$.*

Proof. Take H an affine closed subgroup of G and let $i : H \to G$ the inclusion map.

Now we have the relative map between the algebras

$$\mathrm{Hom}(G, \mathbb{A}^1) = \mathcal{O}(G) \to \mathcal{O}(H) = \mathrm{Hom}(H, \mathbb{A}^1)$$

and so

$$f \to (g \to f(i(g)))$$

$$I(H) = \{f \in \mathcal{O}(G) | f(h) = 0 \text{ for all } h \in H(R) \text{ and all the } S\text{-algebras } R\}$$

is a Hopf ideal because is the kernel of $\mathcal{O}(G) \to \mathcal{O}(H)$. Conversely if I is a Hopf ideal in $\mathcal{O}(G)$, then the functor

$$R \rightsquigarrow \{g \in G(R) |\ f(g) = 0 \text{ for all } f \in I\ \}$$

is an affine subgroup of G (it is represented by $\mathcal{O}(G)/I$). These maps are one the inverse of the other. □

Definition 1.1.17. The kernel of a homomorphism $u : H \to G$ of affine groups is the functor

$$R \rightsquigarrow N(R) := Ker(u(R) : H(R) \to G(R)).$$

Let $\epsilon : \mathcal{O}(G) \to S$ be the identity element of $G(S)$. Then an element $h : \mathcal{O}(H) \to R$ of $H(R)$ lies in $N(R)$ if and only if its composite with $u^\natural : \mathcal{O}(G) \to \mathcal{O}(H)$ factors through ϵ:

$$\begin{array}{ccc} \mathcal{O}(H) & \xleftarrow{u^\natural} & \mathcal{O}(G) \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle \epsilon} \\ R & \longleftarrow & S \end{array}$$

Let I_G be the kernel of ϵ (the augmentation ideal), and let $I_G\mathcal{O}(H)$ denote the ideal generated by its image in $\mathcal{O}(H)$. Then the elements of $N(R)$ correspond to the morphisms $\mathcal{O}(H) \to R$ that are zero on $I_G\mathcal{O}(H)$, i.e.,

$$N(R) = \mathrm{Hom}_{S-alg}(\mathcal{O}(H)/I_G\mathcal{O}(H), R).$$

We have proved:

Proposition 1.1.18. *For any morphism $H \to G$ of affine groups, there is an affine subgroup N of H (called the kernel of the morphism) such that*

$$N(R) = Ker(H(R) \to G(R))$$

for all R; its coordinate ring is $\mathcal{O}(H)/I_G\mathcal{O}(H)$.

Corollary 1.1.19. *In particular a map between affine groups $H \to G$ is a monomorphism if and only if the kernel is trivial.*

Proof. We remember that a map is a monomorphism if the map $H(R) \to G(R)$ is injective for every S-algebra R. □

1.1.4 Quotient groups; surjective homomorphisms

What does it mean for a morphism of affine groups $G \to Q$ to be surjective? One might guess that it means that $G(R) \to Q(R)$ is surjective for all R, but this condition is too stringent.

Definition 1.1.20. A morphism $G \to Q$ of affine groups is said to be surjective (and Q is called a quotient of G) if the morphism $\mathcal{O}(Q) \to \mathcal{O}(G)$ is faithfully flat.

Proposition 1.1.21. *A morphism of affine groups that is both a closed immersion and surjective is an isomorphism.*

Proof. A faithfully flat map is injective. Therefore the map on coordinate rings is both surjective and injective, and hence is an isomorphism. □

Theorem 1.1.22. *Let k be a field. The following conditions on a morphism $G \to Q$ are equivalent:*

1. *$G \to Q$ is surjective;*
2. *$\mathcal{O}(Q) \to \mathcal{O}(G)$ is injective;*
3. *for every k-algebra R and $q \in Q(R)$, there exists a faithfully flat R-algebra R' and a $g \in G(R')$ mapping to the image of q in $Q(R')$.*

Proof. 1) ⇒ 3) : let $q \in Q(R)$ a morphism $\mathcal{O}(Q) \to R$, and we consider $R' = \mathcal{O}(G) \otimes_{\mathcal{O}(Q)} R$:

$$\begin{array}{ccc} \mathcal{O}(G) & \xleftarrow{\text{faithfully flat}} & \mathcal{O}(Q) \\ {\scriptstyle g=id\otimes 1}\downarrow & & \downarrow{\scriptstyle q} \\ R' & \longleftarrow & R \end{array}$$

Then R' is a faithfully flat R-algebra because $\mathcal{O}(G)$ is faithfully flat $\mathcal{O}(Q)$-algebra. The commutativity of the square means that $g \in G(R')$ maps to the image q' of q in $Q(R')$.

3) ⇒ 2) : consider the universal element $id_{\mathcal{O}(Q)} \in Q(\mathcal{O}(Q))$. By hypothesis there exists a $g \in G(R')$, with R' faithfully flat over $\mathcal{O}(Q)$, such that g and $id_{\mathcal{O}(Q)}$ map to the same element of $Q(R')$ such that the diagram commutes:

$$\begin{array}{ccc} \mathcal{O}(G) & \longleftarrow & \mathcal{O}(Q) \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle id_{\mathcal{O}(Q)}} \\ R' & \xleftarrow{\text{faithfully flat}} & \mathcal{O}(Q) \end{array}$$

But the map $\mathcal{O}(Q) \to R'$ is injective because it is faithfully flat, and so also the map $\mathcal{O}(Q) \to \mathcal{O}(G)$ is injective.

2) ⇒ 1) we use a fact: for any Hopf algebras $A \subset B$ over a field k, B is faithfully flat over A.

□

Corollary 1.1.23. *Every morphism $H \to G$ of affine groups over a field factors into*

$$H \to H' \to G$$

with $H \to H'$ surjective and $H' \to G$ a closed immersion.

Proof. The morphism $\mathcal{O}(G) \to \mathcal{O}(H)$ factors into

$$\mathcal{O}(G) \twoheadrightarrow B \hookrightarrow \mathcal{O}(H)$$

where B is the image of the map $\mathcal{O}(G) \to \mathcal{O}(H)$. It's easy to see that B is an Hopf algebra and so we can consider the affine group $H' = \operatorname{Spec} B$. Then the first map implies that $H' \to G$ is a closed immersion, and by the previous proposition the injectivity of the second map implies that $H \to H'$ is surjective. □

The affine group H' in the corollary is called the image of the morphism $H \to G$.

1.1.5 Examples

From now on we have to assume some more hypothesis on the affine groups. Let $S \in \mathfrak{Rings}$.

Definition 1.1.24. An affine group G over S is finite (resp. finite and locally free) if $\mathcal{O}(G)$ is finitely generated (resp. finitely generated and projective) as S-module.

An affine group G over S is finite and locally free if and only if $\mathcal{O}(G)$ satisfies the following equivalent conditions:

1. $\mathcal{O}(G)$ is finitely generated and projective ad a S-module;
2. $\mathcal{O}(G)$ is finitely generated as a S-module and $\mathcal{O}(G)_{\mathfrak{m}}$ is a free $S_{\mathfrak{m}}$-module for all maximal ideals $\mathfrak{m}$ of S;
3. there exists a finite family $(f_i)_{i\in I}$ generating the ideal S and such that, for all $i \in I$, the S_{f_i}-module $\mathcal{O}(G)_{f_i}$ is free of finite rank;
4. $\mathcal{O}(G)$ is finitely generated and flat as a S-module;
5. (S an integral domain) $\mathcal{O}(G)$ is finitely generated and $\dim_{S(p)}(\mathcal{O}(G) \otimes_S S(\mathfrak{p}))$ is the same for all prime ideals $\mathfrak{p}$ of S (here $S(\mathfrak{p})$ is the field of fractions of $S/\mathfrak{p}$).

In general, if G is finite and locally free, the function

$$\mathfrak{m} \to dim_{S(\mathfrak{m})}\mathcal{O}(G) \otimes S(\mathfrak{m}) : \mathrm{Spm}(S) \to \mathbb{N}$$

is locally constant. It is called the order of G over S.

Note in particular that if $G = \mathrm{Spec}\, A$ is finite, then A is locally free $\iff$ A is projective as R-module $\iff$ A is flat as R-module $\iff$ G is finite and locally free.

When S is a field an affine group G over S is finite if and only if $dim_S\mathcal{O}(G)$ is finite (and $dim_S\mathcal{O}(G)$ is then the order of G over S).

From now on all the group schemes are assumed to be affine, commutative, finite and locally free even though we will call them only "affine groups".

Cartier Duality

Lemma 1.1.25. *Let R be a noetherian ring. A and M two R-modules where A is finitely generated and M is projective. Then*

$$\mathrm{Hom}_R(A, M) \cong \mathrm{Hom}_R(A, R) \otimes M.$$

Proof. We know that a projective module has a "dual base" i.e. there exists a set I and $\{m_i \in M\}$ and $\{f_i \in \mathrm{Hom}(M, R)\}$ with $i \in I$ such that for every $m \in M$, $f_i(m)$ is only nonzero for finitely many i and $m = \sum f_i(m)m_i$.

Now we observe that the maps

$$\mathrm{Hom}_R(A, R) \otimes M \to \mathrm{Hom}_R(A, M)$$

$$\sum h_k \otimes x_k \to \sum h_k x_k$$

and

$$\mathrm{Hom}_R(A, M) \to \mathrm{Hom}_R(A, R) \otimes M$$

$$g \to \sum f_i \circ g \otimes m_i$$

are one the inverse of the other. Note that A is finitely generated and so there are only a finite number of f_i which are nonzero on the image of g and so the last sum is over a finite index. □

Corollary 1.1.26. *Let A be a R-Hop algebra finitely generated and projective. Then*

$$(A \otimes A)^\vee \cong A^\vee \otimes A^\vee.$$

Proof.

$$A^\vee \otimes A^\vee = \mathrm{Hom}_R(A, R) \otimes A^\vee \cong \mathrm{Hom}_R(A, \mathrm{Hom}_R(A, R)) \cong \mathrm{Hom}_R(A \otimes A, R) = (A \otimes A)^\vee.$$

□

Let $A^\vee := \mathrm{Hom}_{R-lin}(A, R)$ denote its R-dual; since A is flat and R is noetherian, A is projective and so $(A \otimes_R A)^\vee = A^\vee \otimes_R A^\vee$ and we can define $e^\vee$, $m^\vee$, $\mu^\vee$, $\epsilon^\vee$ and $i^\vee$ as the R-dual of e, m, μ, ϵ and i. It's easy to check that these maps satisfy the axiom of Hopf algebra, and so $G^\vee := \mathrm{Spec}\ (A^\vee)$ is an affine group over Spec R too.

Definition 1.1.27. $G^\vee$ is called the *Cartier dual* of G.

One of the first examples of affine group is the multiplicative group scheme $\mathbb{G}_m$; it is called the multiplicative group because

$$\mathbb{G}_m(S) = \mathrm{Hom}_{R-alg}(R[X, X^{-1}], S) \cong \mathrm{Hom}_{R-alg}(R[X, Y]/(XY - 1), S) \cong \{a \in S \mid \text{a is invertible } \}$$

is the multiplicative part of the R-algebra S. Note in particular that we define the maps $m(X) = X \otimes X$, $\epsilon(f) = f(1, 1)$ and i which interchanges X and X^{-1}. So the product of the elements of $\mathbb{G}_m(S)$ coincide with the once of S.

For an R-algebra S, let $\underline{\mathrm{Hom}}(G, \mathbb{G}_m)(S)$ be the set of morphisms of $u : G_S \to \mathbb{G}_{m,S}$ of affine groups over S. This becomes a group under the multiplication

$$(u_1 * u_2)(g) = u_1(g) * u_2(g)\ g \in G(S'),\ S' \text{ an } S\text{-algebra.}$$

In this way

$$S \rightsquigarrow \underline{\mathrm{Hom}}(G, \mathbb{G}_m)(S)$$

becomes a functor $\mathfrak{Alg}_R \to \mathfrak{Grp}$.

Theorem 1.1.28. *There is a canonical isomorphism*

$$G^\vee \cong \underline{\mathrm{Hom}}(G, \mathbb{G}_m)$$

of functors $\mathfrak{Alg}_R \to \mathfrak{Grp}$.

Proof. Let S be a R-algebra. We have

$$G(S) = \mathrm{Hom}_{R-alg}(\mathcal{O}(G), S) = \mathrm{Hom}_{S-alg}(\mathcal{O}(G)_S, S) \hookrightarrow \mathrm{Hom}_{S-lin}(\mathcal{O}(G)_S, S) = \mathcal{O}(G^\vee)_S.$$

If we take $f \in \mathrm{Hom}_{S-alg}(\mathcal{O}(G)_S, S) \hookrightarrow \mathrm{Hom}_{S-lin}(\mathcal{O}(G)_S, S)$ then $m^\vee(f) = f \otimes f$ because

$$m^\vee(f)(a \otimes b) = f(\mu(a \otimes b)) = f(ab) = f(a)f(b) = (f \otimes f)(a \otimes b) \text{ with } a, b \in \mathcal{O}(G)_S\ .$$

On the other hand $\mathrm{Hom}(G_S^\vee, \mathbb{G}_{m,S}) = \mathrm{Hom}_{S-alg}(S[X, X^{-1}], \mathcal{O}(G^\vee)_S)$ also consists of the elements of $\mathcal{O}(G^\vee)_S$ such that $m^\vee(g) = g \otimes g$. In fact if we take $f \in \mathrm{Hom}_{S-alg}(S[X, X^{-1}], \mathcal{O}(G^\vee)_S)$, then

$$m^\vee(f(X)) = (f \otimes f)(m(X)) = (f \otimes f)(X \otimes X) = f(X) \otimes f(X).$$

Thus

$$G(S) \cong \underline{\mathrm{Hom}}(G^\vee, \mathbb{G}_m)(S).$$

This isomorphism is natural in S, and so we have shown that $G \cong \underline{\mathrm{Hom}}(G^\vee, \mathbb{G}_m)$. To obtain the required isomorphism, replace G with $G^\vee$ and use that $(G^\vee)^\vee \cong G$. □

1. μ_n. For an integer $1 \leq n$,

   $$\mu_n(S) = \{s \in S \mid s^n = 1\ \} \cong \mathrm{Hom}_{R-alg}(R[X]/(X^n - 1), S)$$

   is a subgroup of $\mathbb{G}_m$.

2. Constant group schemes. We start with Γ a finite abelian group and we define the ring of functions

   $$R^\Gamma := \{f : \Gamma \to \mathrm{R} \mid \text{f is a map of sets}\}$$

   whose addition and multiplication are defined componentwise, and whose 0 and 1 are the constant maps with value 0, respectively 1. The comultplication $m : R^\Gamma \to R^\Gamma \otimes_R R^\Gamma \cong R^{\Gamma \times \Gamma}$ is given by the formula $m(f)(\gamma, \gamma') = f(\gamma + \gamma')$, the counit $\epsilon : R^\Gamma \to R$ by $\epsilon(f) = f(0)$, and the coinverse $i : R^\Gamma \to R^\Gamma$ by $i(f)(\gamma) = f(-\gamma)$.

Next we observe that the following elements $\{e_\gamma\}_{\gamma\in\Gamma}$ constitute a canonical basis of the free R-module R^Γ:

$$e_\gamma(\gamma') = \begin{cases} 1 & \text{if } \gamma = \gamma' \\ 0 & \text{otherwise} \end{cases}$$

One checks that μ, ϵ, e, m, and i are given by

$$\mu(e_\gamma \otimes e_{\gamma'}) = \begin{cases} e_\gamma & \text{if } \gamma = \gamma' \\ 0 & \text{otherwise} \end{cases}$$

$$\epsilon(e_\gamma) = \begin{cases} 1 & \text{if } \gamma = 0 \\ 0 & \text{otherwise} \end{cases}$$

$$e(1) = \sum_{\gamma\in\Gamma} e_\gamma$$

$$m(e_\gamma) = \sum_{\gamma'\in\Gamma} e_{\gamma'} \otimes e_{\gamma-\gamma'}$$

$$i(e_\gamma) = e_{-\gamma}$$

Now to calculate the Cartier dual we can use the base characterized by

$$\hat{e}_\gamma(e_{\gamma'}) = \begin{cases} 1 & \text{if } \gamma = \gamma' \\ 0 & \text{otherwise} \end{cases}$$

The dual maps are given by the formulas

$$m^\vee(\hat{e}_\gamma) = \hat{e}_\gamma \otimes \hat{e}_\gamma$$

$$e^\vee(1) = \hat{e}_0$$

$$\epsilon^\vee(\hat{\epsilon}_\gamma) = 1$$

$$\mu^\vee(\hat{e}_\gamma \otimes \hat{e}_{\gamma'}) = \hat{e}_{\gamma+\gamma'}$$

$$i^\vee(\hat{e}_\gamma) = \hat{e}_{-\gamma}$$

The proof of these formulas follow directly from the definition, we prove the last to give an example.

$$i^\vee(\hat{e}_\gamma)(e_{\gamma'}) = (\hat{e}_\gamma \circ i)(e_{\gamma'}) = \hat{e}_\gamma(e_{-\gamma'}) = \begin{cases} 1 & \text{if } \gamma = -\gamma' \\ 0 & \text{otherwise} \end{cases}$$

and so we conclude by the definition of e_γ.

In particular the formulas for $\mu^\vee$ and $e^\vee$ show that $(R^\Gamma)^\vee$ is isomorphic to the group ring $R[\Gamma]$ as an R-algebra, such that $\epsilon^\vee$ corresponds to the usual augmentation map $R[\Gamma] \to R$.

As an example if $\Gamma := \mathbb{Z}/n\mathbb{Z}$, then $(R^\Gamma)^\vee \cong \mu_n$.

3. α_p. In characteristic $p \neq 0$ we have $(a+b)^p = a^p + b^p$; therefore, for any R-algebra S over a ring with characteristic p, we can define

$$\alpha_p(S) = \{s \in S \mid s^p = 0\} \cong \mathrm{Hom}_{R-alg}(R[T]/T^p, S).$$

In terms of the basis $\{T^i\}_{0\leq i<p}$ all the maps are given by the formulas

$$\mu(T^i \otimes T^j) = \begin{cases} T^{i+j} & \text{if } i+j < p \\ 0 & \text{otherwise} \end{cases}$$

$$\epsilon(T^i) = \begin{cases} 1 & \text{if } i = 0 \\ 0 & \text{otherwise} \end{cases}$$

$$e(1) = T^0$$

$$m(T^i) = \sum_{0 \le j \le i} \binom{i}{j} T^i \otimes T^{i-j}$$

$$i(T^i) = (-1)^i T^i$$

Let $\{u_i\}$ denote the dual basis of $A^\vee$. Then one checks that the R-linear map $\phi : A^\vee \to A$ sending u_i to $T^i/i!$ is an isomorphism of Hopf algebras. For example we prove that this map preserves products; it's immediate to check that

$$u_i u_j = \binom{i+j}{i} u_{i+j}$$

so

$$\phi(u_i u_j) = \binom{i+j}{i} u_{i+j}\phi(u_{i+j}) = \binom{i+j}{i} u_{i+j} \frac{T^{i+j}}{(i+j)!} = \frac{T^i}{i!}\frac{T^j}{j!} = \phi(u_i)\phi(u_j).$$

1.2 The connected components of an affine group

Recall that a topological space X is connected if it is not the union of two disjoint non empty open subsets. This amounts to saying that, apart from X itself and the empty set, there is no subset of X that is both open and closed. For each point x of X, the union of the connected subsets of X containing x is again connected, and so it is the largest connected subset containing x — it is called the connected component of x. The set of the connected components of the points of X is a partition of X by closed subsets. Write $\pi_0(X)$ for the set of connected components of X. In a topological group G, the connected component of the neutral element is a closed normal connected subgroup G° of G, called the neutral (or identity) component of G. Therefore, the quotient $\pi_0(G) = G/G^\circ$ is a separated topological group. In this chapter, we discuss the identity component G° of an affine group and the (étale) quotient group $\pi_0(G)$ of its connected components. Throughout, k is a field.

1.2.1 Idempotents and connected components

Let A be a commutative ring and $e_1, ..., e_n$ a set of n idempotents and orthogonal elements. If that set is also complete which means that $e_1 + ... + e_n = 1$, then Ae_i becomes a ring with the addition and multiplication induced by that of A (but with the identity element e_i) and $A = Ae_1 \times ... \times Ae_n$.

Conversely if $A = A_1 \times ... \times A_n$ then the elements $e_1 = (1, 0, 0, ..)$, ... $e_n = (0, ..., 0, 1)$ form a complete set of orthogonal idempotents.

Lemma 1.2.1. *The space* Spec A *is disconnected if and only if A contains a non trivial idempotent.*

Proof. See Lemma 1.1 pag 204 of [Mil12]. □

Proposition 1.2.2. *Let $\{e_1, ..., e_n\}$ be a complete set of orthogonal idempotents in A. Then*

$$\text{Spec } A = D(e_1) \sqcup ... \sqcup D(e_n)$$

is a decomposition of Spec A *into a disjoint union of open subsets. Moreover, every such decomposition arises in this way.*

Remark. We recall that a ring A is said to be Jacobson if every prime ideal is an intersection of maximal ideals, and that every finitely generated algebra over a field is Jacobson. In a Jacobson ring, the nilradical is an intersection of maximal ideals. When A is Jacobson, "prime ideal" can be replaced by "maximal ideal" and "Spec" with "Spm" in the above discussion. In particular, for a Jacobson ring A, there are natural one-to-one correspondences between

1. the decompositions of Spm A into a finite disjoint union of open subspaces,
2. the decompositions of A into a finite direct products of rings, and
3. the complete sets of orthogonal idempotents in A.

Now consider a ring $A = k[X_1, ..., X_n]/I$. If k is an algebraically closed field,

$$\operatorname{Spm} A \cong \text{ the zero set of } I \text{ in } k^n$$

as topological space, and so Spm A is connected if and only if the zero set of I in k^n is connected.

Definition 1.2.3. An algebra A over a field k is diagonalizable if it is isomorphic to the product algebra k^n for some n, and it is étale if $L \otimes A$ is diagonalizable for some field L containing k.

Remark. Let k be a field, and let A be a finite k-algebra. For any finite set S of maximal ideals in A, the Chinese remainder theorem shows that the map $A \to \prod_{\mathfrak{m} \in S} A/\mathfrak{m}$ is surjective with kernel $\cap_{\mathfrak{m} \in S} \mathfrak{m}$. In particular $|S| \leq |A : k|$, and so A has only finitely many maximal ideals. If S is the set of all maximal ideals in A, then $\cap_{\mathfrak{m} \in S} \mathfrak{m}$ is the nilradical N of A and so A/N is a finite product of fields.

Proposition 1.2.4. *The following conditions on a finite k-algebra A are equivalent:*

1. *A is étale*
2. *$L \otimes A$ is reduced (i.e. it has no non-zero nilpotent elements) for all fields L containing k*
3. *A is a product of separable field extensions of k.*

Proof. 1) $\Rightarrow$ 2): let L be a field containing k. By hypothesis, there exists a field L' containing k such that $L' \otimes A$ is diagonalizable. Take L'' a field which contains L and L', then $L'' \otimes A$ is diagonalizable and the map $L \otimes A \to L'' \otimes A$ defined by the inclusion $L \to L''$ is injective, and so $L \otimes A$ is reduced. 2) $\Rightarrow$ 3): suppose that $L \otimes A$ is reduced, then also A is reduced because A is contained in $L \otimes A$. This fact and the remark above tell us that A is a finite product of fields. Let k' be one of the factors of A. If k' is not separable over k, then k has characteristic $p \neq 0$ and there exists an element $u \in k'$ whose minimum polynomial is of the form $f(X^p)$ with $f \in k[X]$. Let L be a field containing k such that all the coefficients of f are pth powers in L. Then

$$L \otimes k[u] \cong L \otimes (k[X]/f(X^p)) \cong L[X]/f(X^p)$$

which is not reduced because $f(X^p) = f(X)^p$ is a p-th power in $L[X]$. Hence $L \otimes A$ is not reduced. 3) $\Rightarrow$ 1): suppose that A itself is separable field extension of k. From the primitive element theorem, we know that $A = k[u]$ for some u. Because $k[u]$ is separable over k, the minimum polynomial $f(X)$ of u is separable, which means that

$$f(X) = \prod (X - u_i), \ u_i \neq u_j \text{ for } i \neq j \ ,$$

in a splitting field L for f. Now

$$L \otimes A \cong L \otimes k[X]/(f) \cong L[X]/(f)$$

and according to the Chinese remainder theorem

$$L[X]/(f) \cong \prod L[X]/(X - u_i) \cong L \times L \times ... \times L.$$

□

Corollary 1.2.5. *Let k^{sep} a separable closure of k. A k-algebra A is étale if and only if $k^{sep} \otimes A$ is diagonalizable.*

Proof. The proof that 3) $\Rightarrow$ 2) shows that $L \otimes A$ is diagonalizable if certain separable polynomials splits in L. But by definition, all separable polynomials split in k^{sep}. □

Remark. Finite products, tensor products, and quotients of diagonalizable (resp. étale) k-algebras are diagonalizable (resp. étale).

Corollary 1.2.6. *The composite of any finite set of étale subalgebras of a k-algebra is étale.*

Proof. Let A_i be étale subalgebras of B. Then $A_1 * ... * A_n$ is the image of the map

$$a_1 \otimes ... \otimes a_n \to a_1 * ... * a_n$$

and so is a quotient of $A_1 \otimes ... \otimes A_n$. □

Proposition 1.2.7. *If A is étale over k, then $k' \otimes A$ is étale over k' for every field k' containing k.*

Proof. Let L be such that $A \otimes L \cong L^m$, and let L' be a field containing L and k'. Then

$$L' \otimes_{k'} (k' \otimes A) \cong L' \otimes A \cong L' \otimes_L L \otimes A \cong L' \otimes_L L^m \cong (L')^m.$$

□

Lemma 1.2.8. *Let A be a finitely generated algebra over a separably closed field k. The number of connected components of* Spm A *is equal to the largest degree of an étale k-subalgebra of A (and both are finite).*

Proof. Because Spm A is noetherian, it's a finite disjoint union of its connected components, each of which is open.

Let E be an étale k-subalgebra of A. Because k is separably closed, E is a product of copies of k. A decomposition of E corresponds to a complete set $(e_i)_{1 \le i \le m}$ of orthogonal idempotents in E, and $m = [E : k]$. Conversely, a complete set $(e_i)_{1 \le i \le m}$ of orthogonal idempotents in A defines an étale k-subalgebra of A of degree $m : \sum ke_i$. □

Lemma 1.2.9. *Let A be a finitely generated k-algebra. Assume that k is algebraically closed, and let K be an algebraically closed field containing k. If* Spm A *is connected, so also is* Spm A_K

Proof. Write $A = k[X_1, ..., X_n]/\mathfrak{a}$, so that $A_K = K[X_1, ..., X_n]/\mathfrak{b}$ where $\mathfrak{b}$ is the ideal generated by $\mathfrak{a}$. By assumption, the zero set $V(\mathfrak{a})$ in k^n is connected, and it lies in the zero set $V(\mathfrak{b})$ in K^n. As the closure of a connected set is connected, we want to show that $V(\mathfrak{b})$ is contained in the the closure of $V(\mathfrak{a})$ in K^n. Choose a basis $(a_i)_{i \in I}$ for K over k, let $f \in K[X_1, ..., X_n]$ be a polynomial which is zero on $V(\mathfrak{a})$ and we want to show that it is zero on $V(\mathfrak{b})$. Write

$$f = \sum a_i f_i \;\; f_i \in k[X_1, ..., X_n].$$

As f is zero on $V(\mathfrak{a})$, so also is each f_i. By the Strong Nullstellensatz some power of f_i lies in $\mathfrak{a} \subset \mathfrak{b}$ hence each f_i is zero on $V(\mathfrak{b})$ and so f is zero on $V(\mathfrak{b})$. □

Let A be a finitely generated k-algebra. An étale k-subalgebra of A will give an étale k^{al}-subalgebra of the same degree of $A_{k^{al}}$, and so its degree is bounded by the number of connected components of Spm $A_{k^{al}}$. The composite of two étale subalgebras of A is étale, and so there is a largest étale k-subalgebra $\pi_0(A)$ of A, containing all other subalgebras.

Let K be a field containing k. Then $K \otimes \pi_0(A)$ is an étale K-subalgebra of $K \otimes A$. We shall need to know that it is the largest étale subalgebra.

Proposition 1.2.10. *Let A be a finitely generated k-algebra, and let K be a field containing k. Then*

$$K \otimes \pi_0(A) = \pi_0(K \otimes A).$$

Proof. See Proposition 2.1 pag 206 of [Mil12]. □

Corollary 1.2.11. *Let A be a finitely generated k-algebra. The degree $[\pi_0(A) : k]$ is equal to the number of connected components of* Spm $(k^{al} \otimes A)$.

Proof.

$$[\pi_0(A) : k] = [k^{al} \otimes \pi_0(A) : k^{al}] = [\pi_0(k^{al} \otimes A) : k^{al}]$$

and the proof follows from 1.2.5. □

Proposition 1.2.12. *Let A and A' be finitely generated k-algebras. Then*

$$\pi_0(A \otimes A') = \pi_0(A) \otimes \pi_0(A').$$

Proof. See Proposition 2.3 pag 207 of [Mil12]. □

1.2.2 Affine groups

Let G be an affine group with coordinate ring $A = \mathcal{O}(G)$. The map $m : A \to A \otimes A$ is a k-algebra morphism and so sends $\pi_0(A)$ into $\pi_0(A \otimes A) = \pi_0(A) \otimes \pi_0(A)$; similarly $i : A \to A$, sends $\pi_0(A)$ into $\pi_0(A)$ and we can restrict ϵ on $\pi_0(A)$, therefore $\pi_0(A)$ becomes a Hopf subalgebra of A. Let's see it in details. Suppose $\phi : A \to B$ is a morphism of Hopf algebras, then we want to show that we can restrict $\phi : \pi_0(A) \to \pi_0(B)$. In particular we will show that the image of $\pi_0(A)$ is an ètale algebra. First $\pi_0(A) = \prod_{i=1}^n k_i$ where k_i are separable extensions of k; in particular there exist $e_1, ..., e_n$ a complete set of idempotents. Clearly $\phi(e_1), ..., \phi(e_n)$ is still a complete set of idempotents which implies that $\phi(\pi_0(A)) = \prod_{i=1}^n (\phi(\pi_0(A))\phi(e_i)) = \prod_{i=1}^n \phi(k_i)$. So in order to conclude we have only to prove that $\phi(k_i)$ remains a separable field extension for all i. Using the multiplicativity of ϕ we see that $\phi(k_i)$ is a field which implies that $\phi_{|k_i}$ is injective. It easily follows that taken an element $\phi(j) \in \phi(k_i)$, it's minimal polynomial over k is the same of the once of j and so it can not have multiple roots in $\phi(k_i)$.

Definition 1.2.13. 1. The group of connected component $\pi_0(G)$ of G is the quotient affine group corresponding to $\pi_0(\mathcal{O}(G))$.

2. The identity component G° of G is the kernel of the morphism $G \to \pi_0(G)$.

Proposition 1.2.14. *The following four conditions on an affine group G are equivalent:*

1. *the étale affine group $\pi_0(G)$ is trivial;*
2. *the topological space* Spm $(\mathcal{O}(G))$ *is connected;*
3. *the topological space* Spm $(\mathcal{O}(G))$ *is irreducible;*
4. *the ring $\mathcal{O}(G)/N$ is an integer domain.*

Proof. 2) $\Rightarrow$ 1): $\pi_0(\mathcal{O}(G))$ has no non trivial idempotents and so it is a field. The existence of $\epsilon : \mathcal{O}(G) \to k$ implies that $\pi_0(\mathcal{O}(G)) = k$.

3) $\Rightarrow$ 2): trivial.

3) $\iff$ 4): Spm (A) is irreducible if and only if the nilradical of A is prime.

1) $\Rightarrow$ 4) If $\pi_0(G)$ is trivial, so also is $\pi_0(G_{k^{al}})$. Write $\mathrm{Spm}(\mathcal{O}(G_{k^{al}}))$ as a union of its irreducible components. By definition, no irreducible component is contained in the union of the remainder. Therefore, there exists a point that lies on exactly one irreducible component. By homogeneity, all points have this property and so the irreducible components are disjoint. As $\mathrm{Spm}(\mathcal{O}(G_{k^{al}}))$ is connected, there must be only one irreducible component, and so Spm $\mathcal{O}(G_{k^{al}})$ is irreducible. Let N' the nilradical of $\mathcal{O}(G_{k^{al}})$; the implication 3) $\Rightarrow$ 4) tells us that $\mathcal{O}(G_{k^{al}}))/N'$ is a domain. The canonical map $\mathcal{O}(G) \to k^{al} \otimes \mathcal{O}(G) \cong \mathcal{O}(G_{k^{al}})$ is injective: this tells us that the inverse image of N' is contained in N and the other inclusion follows from the multiplicativity of the map. So it remains injective after quotients by the respective nilradicals, and so $\mathcal{O}(G)/N$ is an integral domain.

□

Definition 1.2.15. An affine group is connected if it satisfies the equivalent conditions of the proposition.

Proposition 1.2.16. *The fibres of the map* Spm $G \to$ Spm $\pi_0(G)$ *are the connected components of the topological space* Spm G.

Proof. The connected components of Spm G and the points of Spm $\pi_0(G)$ are both indexed by the elements of a maximal complete set of orthogonal idempotents. □

Proposition 1.2.17. *Every morphism from G to an étale affine group factors uniquely through $G \to \pi_0(G)$.*

Proof. Let $G \to H$ be a morphism from G to an étale affine group H. The image of $\mathcal{O}(H)$ is an étale algebra and so it is contained in $\pi_0(\mathcal{O}(G)) = \mathcal{O}(\pi_0 G)$. □

Proposition 1.2.18. *The subgroup G° of G is connected.*

Proof. The morphism of k-algebras $\epsilon : \mathcal{O}(\pi_0(G)) \to k$ decomposes $\mathcal{O}(\pi_o(G))$ into a direct product

$$\mathcal{O}(\pi_0(G)) = k \times B$$

where B is the augmentation ideal of $\mathcal{O}(\pi_0(G))$. Let $e = (1, 0)$.

$$\mathcal{O}(G) = e\mathcal{O}(G) \times (1 - e)\mathcal{O}(G)$$

with

$$e\mathcal{O}(G) \cong \mathcal{O}(G)/(1 - e)\mathcal{O}(G) = \mathcal{O}(G^\circ).$$

Now $k = \pi_0(e\mathcal{O}(G)) \cong \pi_0(\mathcal{O}(G^\circ))$. Therefore $\pi_0(G^\circ) = 1$ which implies that G° is connected. □

Proposition 1.2.19. *The subgroup G° is the unique connected normal affine subgroup of G such that G/G° is étale.*

Proof. We have only to prove the unicity. Suppose that H is a second normal affine subgroup of G. If G/H is étale, then the morphism $G \to G/H$ factors through $\pi_0(G)$, and so we get a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G^\circ & \longrightarrow & G & \longrightarrow & \pi_0(G) & \longrightarrow & 1 \\ \| & & \downarrow & & \| & & \downarrow & & \| \\ 1 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & G/H & \longrightarrow & 1 \end{array}$$

with exact rows; note that the second row is exact because H is an affine subgroup of G and G/H is the cokernel of the first map. The similar diagram with each $*$ replaced by $*(R)$ gives, for each k-algebra R, an sequence

$$1 \to G^\circ(R) \to H(R) \to \pi_0(G)(R).$$

Let's check the exactness of the sequence: the first map is injective because $G^\circ(R)$ is contained in the kernel of the map $G(R) \to G/H(R)$ which is $H(R)$.The exactness in the middle follows from the fact that the map $H(R) \to \pi_0(G)(R)$ is the restriction to $H(R)$ of the map $G(R) \to \pi_0(G)(R)$; the kernel of this last map is $G^\circ(R)$ which is contained in $H(R)$ and so it's also the kernel of the map $H(R) \to \pi_0(G)(R)$. Since this is functorial in R and we are over a field, Proposition 1.1.13 tells us that a closed immersion can be checked on "points"; so the sequence of affine groups

$$1 \to G^\circ \to H \to \pi_0(G)$$

is exact. The exactness shows that G° is the kernel of $H \to \pi_0(G)$. This map factors through $\pi_0(H)$ and so if $\pi_0(H) = 1$, it's kernel is H : therefore $G^\circ \cong H$. □

Remark. This proposition tell us that for any affine group G there exist a unique exact sequence

$$1 \to G^\circ \to G \to \pi_0(G) \to 1$$

such that G° is connected and $\pi_0(G)$ is étale. This is called the connected - étale exact sequence.

Proposition 1.2.20. *For any field extension $k \subset k'$*

$$\pi_0(G_{k'}) \cong \pi_0(G)_{k'}$$

$$(G_{k'})^\circ \cong (G^\circ)_{k'}.$$

In particular G is connected if and only if $G_{k'}$ is connected.

Proof. Take the exact sequence

$$1 \to G^\circ \to G \to \pi_0(G) \to 1.$$

Applying $\_ \otimes k'$ to the algebras we obtain

$$1 \to (G^\circ)_{k'} \to G_{k'} \to \pi_0(G)_{k'}$$

but we remember that Proposition 1.2.10 tells us that $\pi_0(G)_{k'} = \pi_0(G_{k'})$ and so we conclude that $(G^\circ)_{k'}$ is the kernel of $G_{k'} \to \pi_0(G_{k'})$ and so $(G^\circ)_{k'} = (G_{k'})^\circ$. □

Proposition 1.2.21. *For any field k of characteristic $0 < p$, the affine groups $(\mathbb{Z}/p\mathbb{Z})_k$, $\mu_{p,k}$ and $\alpha_{p,k}$ are pairwise non-isomorphic.*

Proof. The first one is étale, while both $\mu_{p,k}$ and $\alpha_{p,k}$ are reduced. Now the Cartier duals of $\mu_{p,k}$ and $\alpha_{p,k}$ are respectively $\mathbb{Z}/p\mathbb{Z}_k$ and $\alpha_{p,k}$ which are not isomorphic as we said. So $\alpha_{p,k}$ and $\mu_{p,k}$ are not isomorphic too. □

Chapter 2

A classification of group schemes of prime order

2.1 Two general theorems

Until now we have studied the group object in the category of affine group schemes. Now we want to extend this notion in the category of group schemes; as we will see the notion of Hopf algebra will be substituted by the once of quasi coherent sheaf of Hopf-algebras. How to pass from the one to the other? Let $S = (S, \mathcal{O}_S)$ be a scheme and $\mathcal{A}$ be a quasi-coherent sheaf of $\mathcal{O}_S$-algebras; we want to define a scheme which is in some sense the analogous of $\operatorname{Spec} A$ when A was an algebra.

First we observe that for each affine subset $U \subset S$ we have a map $\mathcal{O}_S(U) \to \mathcal{A}(U)$ and the related once $f : \operatorname{Spec}(\mathcal{A}(U)) \to \operatorname{Spec}(\mathcal{O}_S(U)) = U$. So the idea is to define $\operatorname{Spec}\mathcal{A}$ and a morphism $\epsilon : \operatorname{Spec}\mathcal{A} \to S$ as the unique scheme such that $\epsilon^{-1}(U) = \operatorname{Spec}(\mathcal{A}(U))$ for every open affine $U \subset S$. It's possible to check that $\operatorname{Spec}\mathcal{A}$ is an appropriate gluing of the affine schemes $\operatorname{Spec}(\mathcal{A}(U))$ and the map ϵ the extension of the maps f. So the main point is that we have constructed a scheme $\operatorname{Spec}\mathcal{A}$ with an affine morphism $\epsilon : \operatorname{Spec}\mathcal{A} \to S$ where affine means that for each $U \subset S$ affine, $\epsilon^{-1}(U)$ is affine. To see how much important is this property, take two group schemes G and B over S and a S-morphism $\phi : G \to B$. By the S-linearity of ϕ the following commutes

$$\begin{array}{ccc} G & \xrightarrow{\phi} & B \\ & {\scriptstyle\epsilon_1}\searrow \quad \swarrow{\scriptstyle\epsilon_2} & \\ & S & \end{array}$$

In particular $\phi_{|\epsilon^{-1}(U)} : \epsilon_1^{-1}(U) \to \epsilon_2^{-1}(U)$ which means that covering G and B with opens of such form, we can determine completely the behaviour of ϕ studying it locally on affine schemes.

Note that if S is an affine scheme, then also $\operatorname{Spec}\mathcal{A}$ it is and it coincides with $\operatorname{Spec}(\mathcal{A}(S))$. From now on we will write $\operatorname{Spec} A$ even though we are speaking of schemes not necessary affine; it will be clear from the context if A is an algebra or a sheaf of algebras.

We remind that all the groups schemes are assumed to be commutative, finite and locally free. Let $G \to S$ be an S-group scheme. For each integer $m \in \mathbb{Z}$ we denote by

$$m_G : G \to G$$

the morphism obtained by raising to the m-th power all elements of the group functor G. Suppose $G =$ Spec (A), then we use $[m] : A \to A$ for the corresponding $\mathcal{O}_S$-algebra morphism. In particular let $n \in \mathbb{Z}$, R an $\mathcal{O}_S$-algebra, $u \in G(R)$ and $a \in A$; we have the following relation

$$n_G(u)(a) = u([n]a).$$

The "laws of exponents" $(\xi^n)^m = \xi^{nm}$ and $(\xi^m)(\xi^n) = \xi^{n+m}$ amount to the identities

$$[m][n] = [mn]$$

$$\mu_A \circ ([m] \otimes [n]) \circ m_A = [m+n].$$

Clearly $[1] = id_A$ and $[0] = e \circ \epsilon$.

Theorem 2.1.1. *A commutative S-group of order m is killed by m (i.e. $m_G = 0_G$).*

Remark. We know from group theory that if G is a finite commutative group of order m, then the order of each element divides m. We can prove this showing that if $x \in G$, then

$$\prod_{y \in G} y = \prod_{y \in G} xy = (\prod_{y \in G} y)x^m$$

and so $x^m = 1$. Obviously we can not apply these equalities in case of G is a group scheme because in general $G(R)$ has not a finite number of elements, where R is a S-group scheme, and so $\prod_{y \in G(R)} y$ makes no sense. So we have to find an object which can substitute $\prod_{y \in G(R)} y$; a good starting point is analyse what happen for affine constant group schemes.

We remember that the constant group C associated to a finite group G of order m has $A := \mathcal{O}(C) = \prod_{g \in G} R$. Consider the free $A^\vee$-algebra $A^\vee \otimes A$; to each element $g \in A^\vee \otimes A$ we can associate it's norm $\mathcal{N}(g)$ which is the determinant associated to matrix of the linear map

$$A^\vee \otimes A \to A^\vee \otimes A$$

$$a \to g * a.$$

Denoting with $\{e_i\}$ and $\{e_i'\}$ respectively the base and the dual base, take $\mathrm{Id}_A \in G(A)$ which can be written as

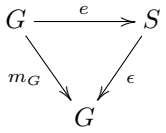
$$\sum_{i=1}^{m} e_i' \otimes e_i$$

as an element of $A^\vee \otimes A$. We want to calculate $\mathcal{N}(\mathrm{Id}_A)$. Take $1 \otimes e_i$ a generic element of the base of $A^\vee \otimes A$ over $A^\vee$,

$$(\mathrm{Id}_A)(1 \otimes e_j) = e_j' \otimes e_j$$

and so the matrix associated to the multiplication of Id_A is $(e_1', ..., e_m') * \mathrm{Id}$ which implies that $\mathcal{N}(\mathrm{Id}_A) = \prod_{i=1}^m e_i'$ is invertible; so this easy case suggests us that the norm is the right object to consider.

Remark. We basically have to prove the commutativity of the following



But we remember that G is a gluing of affine schemes of the form $\mathrm{Spec}(\mathcal{A}(U))$ where $\mathcal{A}$ is a quasi-coherent sheaf of $\mathcal{O}_S$-algebras and $U \subset S$ open affine. So we can prove the commutativity of the diagram in each affine scheme $\mathrm{Spec}(\mathcal{A}(U))$ and so we can assume S affine.

We can also assume that $\mathcal{O}_S = R$ is a local ring; in fact take $a \in A$ and suppose that $([m]a - \epsilon \circ e(a)) \neq 0$ in A but $([m]a - \epsilon \circ e(a)) = 0$ in $A \otimes R_{\mathfrak{p}}$ for each $\mathfrak{p}$ primes of R. Then consider the annihilator of $([m]a - \epsilon \circ e(a))$ which is a proper ideal of R and consider a maximal ideal $\mathfrak{m}$ which contains it. Then obviously $([m]a - \epsilon \circ e(a)) \neq 0$ in $A \otimes R_{\mathfrak{m}}$; absurd.

Proof. So in conclusion we have reduced ourselves to prove that a finite flat commutative S-scheme $G = \mathrm{Spec}\, A$ of order m is killed by m_G. Let $R = \mathcal{O}_S$. R is local which implies that A is free. We should prove that for any R-algebra B, each element of $G(B)$ has order dividing m. But we note that if $A = \mathcal{O}(G)$, then

$$G(B) = \mathrm{Hom}_R(A, B) = \mathrm{Hom}_B(A \otimes B, B)$$

and so we can reduce to the case $B = R$ and check that for each $u \in G(R)$, $u^m = 1$.

Lemma 2.1.2. *Let S be a finite and free R-algebra. Then we have a map*

$$G(R) \to G(S) \xrightarrow{\mathcal{N}} G(R).$$

We postpone the proof of this result. Basically the Lemma tells us that the following diagram commutes

$$\begin{array}{ccc} G(A) & \longrightarrow & A^\vee \otimes A = \mathrm{Hom}_{R-lin}(A,A) \\ \downarrow \mathcal{N} & & \downarrow \mathcal{N} \\ G(R) & \longrightarrow & A^\vee \end{array}$$

showing that the norm "preserves" the invertible elements.

Let $u \in G(R) \hookrightarrow A^\vee$ and consider the multiplication by u, $m_u : A^\vee \otimes A \to A^\vee \otimes A$. First this is an automorphism of $A^\vee$-algebras because $u \in G(R)$ and so it is invertible also in $A^\vee$ observing that the product in $G(R)$ coincide with the product of $G(R)$ inside $A^\vee$. We note also that the map $e : R \to A$ is injective since A is free and so u can be seen as an element of $G(A)$ and of $A^\vee \otimes A$; in particular $\mathcal{N}(u) = u^m$ (in this case we write u instead of $u * 1_{A^\vee \otimes A}$), because $u \in A^\vee$ and so the matrix associated to the multiplication is $u * Id$. Furthermore if $a \in A^\vee \otimes A$, then $\mathcal{N}(u * a) = \mathcal{N}(m_u(a)) = \mathcal{N}(a)$; the last equality follows because m_u is an isomorphism and the norm map is independent from the choice of a base.

Finally let's take $\mathrm{Id}_A \in G(A) \hookrightarrow A^\vee \otimes A$.

$$\mathcal{N}(\mathrm{Id}_A) = \mathcal{N}(m_u(\mathrm{Id}_A)) = \mathcal{N}(u * \mathrm{Id}_A) = \mathcal{N}(u)\mathcal{N}(\mathrm{Id}_A) = u^m \mathcal{N}(\mathrm{Id}_A).$$

But $\mathcal{N}(\mathrm{Id}_A) \in G(R)$ is invertible, so $u^m = 1$. □

Proof. We continue with the proof of the Lemma.

S is finite and free over R and so also $A^\vee \otimes S$ is finite and free as $A^\vee$-algebra. Thus we have a norm map $\mathcal{N} : A^\vee \otimes S \to A^\vee$ which sends an element $s \in A^\vee \otimes S$ to the element $\mathcal{N}(s)$ that is the determinant of the matrix of the $A^\vee$-linear mapping $A^\vee \otimes S \to A^\vee \otimes S$ that takes $x \in A^\vee \otimes S$ to sx. Now we claim that this norm induces a map $G(S) \to G(R)$ and that the follows commutes:

$$\begin{array}{ccc} G(S) & \longrightarrow & A^\vee \otimes R_{\mathfrak{p}} \\ \downarrow ? & & \downarrow \mathcal{N} \\ G(R) & \longrightarrow & A^\vee \end{array}$$

where the horizontal maps are the inclusions in fact

$$G(R) \subset \mathrm{Hom}_{R-lin}(A,R) = A^\vee$$

and

$$G(S) \subset \mathrm{Hom}_{R-lin}(A,S) = \mathrm{Hom}_{S-lin}(A \otimes S, S) = (A \otimes S)^\vee \cong A^\vee \otimes S.$$

In order to prove this claim we have to prove a general *remark*:

Lemma 2.1.3. *Let S be as before a finite and free R-algebra, B and C two R-algebras. If $f : B \to C$ is a homomorphism of R-algebras, then*

$$\begin{array}{ccc} B \otimes S & \xrightarrow{f \otimes id_S} & C \otimes S \\ \downarrow \mathcal{N} & & \downarrow \mathcal{N} \\ B & \xrightarrow{f} & C \end{array}$$

is commutative.

Proof. Let e_i be a basis for S over R, so that $\{1 \otimes e_i\}$ are a B-basis for $B \otimes S$ and a C-basis for $C \otimes S$. If $\alpha \in B \otimes S$,

$$\alpha * (1 \otimes e_i) = \sum_j \mu_{i,j}(1 \otimes e_j) = \sum_j (\mu_{i,j} \otimes e_j)$$

for $\mu_{i,j} \in B$ and so $\mathcal{N}(\alpha) = det(\mu_{i,j})$.

Hence if we try to calculate $\mathcal{N}(f \otimes id_S(\alpha))$:

$$(f \otimes id_S)(\alpha) * (1 \otimes e_i) = f \otimes id_S(\alpha) * f \otimes id_S(1 \otimes e_i) = f \otimes id_S(\alpha * (1 \otimes e_i)) = \sum_j (f(\mu_{i,j}) \otimes e_j) = \sum_j f(\mu_{i,j})(1 \otimes e_j)$$

and $\mathcal{N}(f \otimes id_S(\alpha)) = det(f(\mu_{i,j}) = f(\mathcal{N}(\alpha))$. □

Returning to the Lemma we have to prove that if $f \in G(S)$ then $\mathcal{N}(f) \in G(R)$ which is equivalent to prove that $m^\vee(\mathcal{N}(f)) = \mathcal{N}(f) \otimes \mathcal{N}(f)$. We apply the remark to

1.
$$\begin{array}{ccc} A^\vee \otimes S & \xrightarrow{id_{A^\vee} \otimes 1 \otimes id_S} & A^\vee \otimes A^\vee \otimes S \\ \downarrow \mathcal{N} & & \downarrow \mathcal{N} \\ A^\vee & \xrightarrow{id_{A^\vee} \otimes 1} & A^\vee \otimes A^\vee \end{array}$$
which tells us that if $f \in A^\vee \otimes S$, then $\mathcal{N}(f) \otimes 1 = \mathcal{N}(f \otimes 1)$;

2.
$$\begin{array}{ccc} A^\vee \otimes S & \xrightarrow{m^\vee \otimes id_S} & A^\vee \otimes A^\vee \otimes S \\ \downarrow \mathcal{N} & & \downarrow \mathcal{N} \\ A^\vee & \xrightarrow{m^\vee} & A^\vee \otimes A^\vee \end{array}$$
First we notice that $m^\vee \otimes id_S$ is equal to the comultiplication of $A^\vee \otimes S = (A \otimes S)^\vee$; and so the commutativity of the diagram tells us that $\mathcal{N}(m^\vee(f)) = m^\vee(\mathcal{N}(f))$.

Now if $f \in G(S)$, then $m^\vee(f) = f \otimes f$. Hence

$$m^\vee(\mathcal{N}(f)) = \mathcal{N}(m^\vee(f)) = \mathcal{N}(f \otimes f) = \mathcal{N}(1 \otimes f)\mathcal{N}(f \otimes 1) = (\mathcal{N}(f) \otimes 1)(1 \otimes \mathcal{N}(f)) = \mathcal{N}(f) \otimes \mathcal{N}(f).$$

This proves the lemma. □

Theorem 2.1.4. *An S-group scheme of order p is commutative and killed by p.*

Proof. By Deligne's theorem we have only to prove commutativity. We can suppose to be in the case S = Spec R where R is a local ring with algebraically closed residue class field.

Remark. Also in this case we have basically to prove that 2 morphisms coincide i.e.

$$\begin{array}{ccc} A & \xrightarrow{m} & A \otimes A \\ & {\scriptstyle m} \searrow \quad \swarrow {\scriptstyle \sigma} & \\ & A \otimes A & \end{array}$$

where σ switches the factors. So we can reduce ourselves to the case R affine and local. But why can we assume that R has a residue field algebraically closed?

Definition 2.1.5. Let $(R, \mathfrak{m}, k)$ be a local ring where $\mathfrak{m}$ is the unique maximal ideal of R and k is the residue field.

1. We say R is henselian if for every monic $f \in R[X]$ and every root $a_0 \in k$ of $\tilde{f}$ (where $\tilde{}$ denotes the reduction modulo $\mathfrak{m}$) such that $\tilde{f}'(a_0) \neq 0$ there exists an $a \in R$ such that $f(a) = 0$ and $a_0 = \tilde{a}$.
2. We say R is strictly henselian if R is henselian and its residue field is separably algebraically closed.

But a result due to Nagata tell us that in fact for each local ring R it exists an henselian ring R^{hen} and a strictly henselian ring $R^{s.hen}$ such that

$$R \hookrightarrow R^{hen} \hookrightarrow R^{s.hen}.$$

Now we know that A over R is flat (because it's free), and so the map

$$A \hookrightarrow A \otimes R^{s.hen}$$

is injective. This obviously means that the commutativity of the diagram above is implicated by the commutativity of

$$\begin{array}{ccc} A_{R^{s.hen}} & \xrightarrow{m} & A_{R^{s.hen}} \otimes A_{R^{s.hen}} \\ & {\scriptstyle m} \searrow \quad \swarrow {\scriptstyle \sigma} & \\ & A_{R^{s.hen}} \otimes A_{R^{s.hen}} & \end{array}$$

By definition $R^{s.hen}$ is a local ring with algebraically closed residue field, and so we conclude.

Lemma 2.1.6. *Let k be an algebraically closed field, and suppose $G = \text{Spec } A$ is a k-group scheme of order p. Then either G is the constant group scheme, or the characteristic of k is p and $G = \mu_{p,k}$ or $G = \alpha_{p,k}$. In particular G is commutative and the k-algebra A is generated by a single element.*

Proof. We recall that the order of G is the product of the order of G^0 and G/G^0. Since G has prime order, or it is connected, or its connected component is Spec k. In the last case $G = \pi_0(G) = \text{Spec } (k^{\oplus p})$ because k is algebraically closed and so G is the constant group scheme; because there is only one group of order p, $G = \mathbb{Z}/p\mathbb{Z}$. Note that if we suppose that $char(k) = 0$, then $\mu_{p,k}$ is represented by $k^{\oplus p}$ too. So one may think that $\mu_{p,k} \neq (\mathbb{Z}/p\mathbb{Z})_k$ because they have different multiplication; actually we will see that they have the same and so in this case they are isomorphic. Note also that in case $char(k) = p$ the situation is completely different because $\mu_{p,k} = \text{Spec}(k[X]/(X-1)^p)$ and so it is connected.

Suppose now that G is connected. We know that G has a finite number of maximal ideals and so there is only one; so $A = \mathcal{O}(G)$ is artinian (because it is finitely generated over a field) and local. We are over a field and so the augmentation ideal I is maximal; due to the fact that there is only one maximal ideal, it coincide with the Jacobson ideal which is nilpotent (because we are in an artinian ring). Now Nakayama Lemma states that for a generic finitely generated A-module M, if J is an ideal contained in the Jacobson radical of A, then $JM = M$ implies that $M = 0$. Applying the Lemma to $J = M = I$ (note that I is finitely generated because it is a sub vector space of A) we see that $I/I^2 \neq 0$.

I/I^2 is not 0 hence it exists a k-derivation $d : A \to k$. Because of the linearity of k-derivation, d belongs to $I^\vee \subset A^\vee$ and $m_{A^\vee}(d) = d \otimes 1 + 1 \otimes d \in A^\vee \otimes A^\vee$. So $k[d]$ is a sub-bialgebra of $A^\vee$ and we have a surjective morphism $(A^\vee)^\vee = A \to (k[d])^\vee$; as the order of G is prime, then the order of $k[d]$ is p and so $k[d] = A^\vee$. Now $G^\vee$ must be étale or connected. In the first case $G = \mu_{p,k}$; G is connected, it has only one maximal ideal and so k must have characteristic p so that $x^p - 1 = (x-1)^p$. If $G^\vee$ is connected, $I^\vee$ is nilpotent and also $d \in I^\vee$ it is. Because $k[d]$ is of rank p, $d^{p-1} \neq 0$ and $d^p = 0$ and remembering that $m_{A^\vee}(d) = d \otimes 1 + 1 \otimes d$ we conclude that $G^\vee = \alpha_{p,k} = G$. Finally, because $m_{A^\vee}$ is a morphism, $p = 0$ in k and so $p = \text{char}(k)$. □

Now we can conclude the proof of the theorem. Denote with $\tilde{}$ the reduction modulo the unique maximal ideal $\mathfrak{m}$ of R. $\tilde{G}$ is commutative by the previous lemma; now we want to apply the lemma to the dual $(\tilde{G})^\vee = \text{Spec}((\tilde{A})^\vee)$. Note that

$$\tilde{A^\vee} = \text{Hom}_{R-lin}(A, R) \otimes R/\mathfrak{m} = \text{Hom}_{R-lin}(A, R/\mathfrak{m}) =$$
$$= \text{Hom}_{R-lin}(A, \text{Hom}_{R/\mathfrak{m}-lin}(R/\mathfrak{m}, R/\mathfrak{m})) = \text{Hom}_{R/\mathfrak{m}-lin}(A \otimes R/\mathfrak{m}, R/\mathfrak{m}) = (\tilde{A})^\vee.$$

We remember that the Lemma gives us an element which generates the algebra; the equality $(\tilde{A^\vee}) = (\tilde{A})^\vee$ implies that this element is of the form $\tilde{x}$ with $x \in A^\vee$. Now

$$\tilde{R[x]} = k[\tilde{x}] = \tilde{A^\vee}.$$

A generalization of Nakayama Lemma tells that if a finitely generated R-module M is such that $M/IM = 0$ for an ideal $I \subset R$, then it exixts $r \in R$ such that $r - 1 \in I$ and $rM = 0$. We can apply this result to $A^\vee/R[x]$ and $I = \mathfrak{m}$; we conclude that $r(A^\vee/R[x]) = 0$ but r is invertible and so $A^\vee = R[x]$. Remembering that for each R-algebra S, $G(S)$ consist of the invertible elements of $A^\vee \otimes S$, the fact that $A^\vee$ is commutative implies that G is commutative. □

Definition 2.1.7. An affine group G is said to be a semidirect product of its affine subgroups N and Q, denoted $G = N \rtimes Q$, if N is normal in G and the map

$$N(S) \times Q(S) \to G(S)$$
$$(n, q) \to nq$$

is a bijection of sets for all R-algebras S.

Remark. In contrast with group theory there exists a group scheme of rank p which acts non - trivially on another group scheme of rank p, namely μ_p and α_p. Hence there exist group schemes of rank p^2 which are not commutative. For example let R an $\mathbb{F}_p$-algebra, and define $A = R[\tau, \sigma]$, with $\tau^p = 1$, $\sigma^p = 0$, $m(\tau) = \tau \otimes \tau$ and $m(\sigma) = \tau \otimes \sigma + \sigma \otimes 1$.

The R-group scheme $G = \text{Spec (A)}$ is isomorphic to the semidirect product of the normal subgroup scheme defined by $\tau = 1$, which is isomorphic to $\alpha_{p,R}$, and the subgroup scheme defined by $\sigma = 0$, which is isomorphic to $\mu_{p,R}$. Taking $\psi \in \alpha_{p,R}(S)$ and $\phi \in \mu_{p,R}(S)$ we note that

$$\psi * \phi(\sigma) = (\psi \otimes \phi)(\tau \otimes \sigma + \sigma \otimes 1) = \psi(\sigma)$$

$$\psi * \phi(\tau) = (\psi \otimes \phi)(\tau \otimes \tau) = \phi(\tau)$$

and so obviously the above map $N(S) \times Q(S) \to G(S)$ is a bijection. In order to conclude we prove that $\alpha_{p,R}$ is a normal subgroup choosing $\psi' \in \alpha_{p,R}(S)$ such that $\phi * \psi' = \psi * \phi$.

$$\phi * \psi'(\tau) = \phi(\tau)$$

$$\phi * \psi'(\sigma) = \phi(\tau)\psi'(\sigma)$$

and so it's suffice to take ψ' such that

$$\psi'(\sigma) = (\phi(\tau))^{-1}\psi(\sigma).$$

Remark. The theorem already proved has another important consequence. We know that for each group scheme $G = \mathrm{Spec}(A)$ of order p and each S-algebra R the elements of $G(R)$ are the invertible elements of $A_R^\vee$ i.e.

$$G(R) = \mathrm{Hom}(G_R^\vee, \mathbb{G}_{m,R}).$$

But now we know the extra information that each element of $G(R)$ is killed by p, and so

$$G(R) = \mathrm{Hom}(G_R^\vee, \mu_{m,R}).$$

Saying it in other words the Cartier pairing

$$G \times G^\vee \to \mathbb{G}_{m,S}$$

factors through $\mu_{p,S}$.

2.2 A classification theorem

2.2.1 Witt vectors

Let p be a prime integer, $(X_0, ..., X_n, ...)$ a sequence of indeterminates, and consider the following polynomials called " Witt polynomials ":

$$W_0 = X_0$$

$$W_1 = X_0^p + pX_1$$

$$...$$

$$W_n = \sum_{i=0}^{n} p^i X_i^{p^{n-i}}$$

$$...$$

Theorem 2.2.1. *For every $\phi \in \mathbb{Z}[X, Y]$, there exists a unique sequence $(\phi_0, \phi_1, ..., \phi_n, ...)$ of elements of $\mathbb{Z}[X_0, ..., X_n, ...; Y_0, ..., Y_n, ...]$ such that*

$$W_m(\phi_0, ..., \phi_n, ...) = \phi(W_m(X_0, ...), W_m(Y_0, ...))$$

with $m = 0, 1, ...$

In particular we denote by $S_0, ..., S_n, ...$ (resp. $P_0, ..., P_n, ...$) the polynomials $\phi_0, ..., \phi_n, ...$ associated to

$$\phi(X, Y) = X + Y$$

(resp.

$$\phi(X, Y) = XY$$

).

Now let A be a commutative ring, we denote with $A^{\mathbb{N}}$ the set $\{(a_0, ..., a_n, ...)$ such that $a_i \in A\}$. Given a and $b \in A^{\mathbb{N}}$ we can define

$$a + b = (S_0(a, b), ..., S_n(a, b), ...)$$

$$a * b = (P_0(a, b), ..., P_n(a, b), ...).$$

Theorem 2.2.2. *With the two operations defined above, $A^{\mathbb{N}}$ becomes a commutative unitary ring called the ring of Witt vectors with coefficients in A; it is denoted by $W(A)$.*

Remark. Note that the map

$$W_* : W(A) \to A^{\mathbb{N}}$$
$$a = (a_0, ..., a_n, ...) \to (W_0(a), ..., W_n(a), ...)$$

is a morphism and it is also an isomorphism if p is invertible.

Remark. Observe that the polynomials ϕ_i involve only variables of index $\leq i$; one concludes that the vectors $(a_0, ..., a_{n-1})$ form a ring that one denotes $W_n(A)$. It's easy to see that $W_1(A) = A$ and that $W(A)$ is the projective limit of the rings $W_n(A)$ as $n \to \infty$. If $x \in A$, set

$$\chi(x) = (x, 0, ..., 0, ...).$$

This defines a map $\chi : A \to W(A)$; composing it with W_* we obtain a map $A \to A^{\mathbb{N}}$ which sends x into $(x, x^p, ..., x^{p^n}, ...)$.

In particular

$$\chi(xy) = \chi(x)\chi(y).$$

Theorem 2.2.3. *$W(\mathbb{F}_p) = \mathbb{Z}_p$ and $W_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}$.*

Remark. So taking $A = \mathbb{F}_p$ we obtain a multiplicative map

$$\mathbb{F}_p \to W(\mathbb{F}_p) = \mathbb{Z}_p$$

which is a right inverse of the obvious map $\mathbb{Z}_p \to \mathbb{F}_p$. We also observe that $\chi(0) = 0$ and thanks to Hensel Lemma, for $m \in \mathbb{F}_p^*$, $\chi(m)$ is the unique $(p-1)$ - root of unity in $\mathbb{Z}_p$ whose residue (mod p) is m. The restriction of χ to $\mathbb{F}_p^*$ is a generator of the group $\mathrm{Hom}(\mathbb{F}_p^*, \mathbb{Z}_p^*)$.

2.2.2 A classification theorem

Fix a prime p and assume our ground scheme S is over $\mathrm{Spec}(\Lambda_p)$ where

$$\Lambda_p = \mathbb{Z}[\chi(\mathbb{F}_p), \frac{1}{p(p-1)}] \cap \mathbb{Z}_p.$$

From now on we will write $\Lambda = \Lambda_p$.

At the end of this section we will give a theorem which classifies every group scheme G of prime order p over S.

To have also a practical idea of what happen we will proceed alternating theory and the basic example of an affine group scheme of order 2 over a field.

Let $G = \mathrm{Spec}(A)$ be an S-group scheme of order p. By Theorem 2.1.1 we know that $\mathbb{F}_p^*$ acts on G, and we can therefore regard A and I as a sheaf of modules over the group algebra $\mathcal{O}_S[\mathbb{F}_p^*]$.

For each $i \in \mathbb{Z}$, let $I_i = e_i I$ where e_i is the $\mathcal{O}_S$-linear operator

$$e_i = \frac{1}{p-1} \sum_{m \in \mathbb{F}_p^*} \chi^{-i}(m)[m].$$

Because χ has order $p-1$, e_i and I_i depend only on i mod(p - 1).

Lemma 2.2.4. *We have $I = \sum_{i=1,...,p-1} I_i$ direct sum. For each i, I_i is an invertible $\mathcal{O}_S$-module, consisting of the local sections of A s.t. $[m]f = \chi^i(m)f$ for all $m \in \mathbb{F}_p$. We have $I_i I_j \subset I_{i+j}$ for all i and j and $I_1^i = I_i$ for $1 \leq i \leq p-1$.*

Proof. First of all the operators e_i are orthogonal idempotents and their sum is 1, so I is the direct sum of the I_i for $1 \leq i \leq p-1$. Then we note that e_i satisfies $[m]e_i = \chi^i(m)e_i$ for $m \in \mathbb{F}_p^*$ and so I_i consists of the local sections f of I s.t. $[m]f = \chi^i(m)f$ for all $m \in \mathbb{F}_p^*$ or equivalently of the local sections $f \in A$ s.t. $[m]f = \chi^i(m)f$ for all $m \in \mathbb{F}_p^*$. This follows from the fact that $\chi(0) = 0$ and $[0] = e \circ \epsilon$ so the equality $e \circ \epsilon(f) = 0$ implies that $f \in I$.

Now take $f \in I_i$ and $g \in I_j$; using the fact that $[m]fg = [m]f[m]g$ we deduce that

$$[m]fg = [m]f[m]g = \chi^i(m)f\chi^i(m)g = \chi^{i+j}(m)fg$$

and so $I_iI_j \subset I_{i+j}$.

We know that A is a locally free sheaf, so we deduce that also I and I_i are locally free $\mathcal{O}_S$-modules; in particular since I is of rank $p-1$, its direct summands I_i are of rank r_i s.t. $r_1 + ... + r_{p-1} = p-1$. To prove that $r_i = 1$ for each i and that $I_1^i = I_i$ for $1 \leq i \leq p-1$ it's suffice to estimate the case $S = \mathrm{Spec}(k)$, with k an algebraically closed field. Obviously we can reduce to the affine case on $S = \mathrm{Spec}\, R$. Here we have to calculate the rank of I_i which is the dimension of $I_i \otimes R(\mathfrak{p})$ (where $R(\mathfrak{p})$ denotes the filed of fractions of $R/\mathfrak{p}$); clearly this dimension remains the same if we calculate it over an algebraically closed extension of $R(\mathfrak{p})$. Finally we want to exhibit in that case a section $f_1 \in I_1$ s.t. $f_1^i \neq 0$ (which is the same as asking that $f_1^i \notin k$ because $\epsilon(k) = k$ and $\epsilon(I) = 0$) for $1 \leq i \leq p-1$; then $kf_1^i \subset I_i$ implies $1 \leq r_i$, but $r_i \leq 1$ and so $r_i = 1$ and $kf_1^i = I_i$. By Lemma 2.1.6 there are only three cases to consider, namely $G \cong (\mathbb{Z}/p\mathbb{Z})_k$, $\alpha_{p,k}$ or $\mu_{p,k}$ and the last 2 only for $\mathrm{char}(k) = p$, in which case $\chi(m) = m$. If $G \cong (\mathbb{Z}/p\mathbb{Z})_k$, then A is the algebra of functions with values in k from $\mathbb{F}_p$, and $([m]f)(n) = f(mn)$ for $f \in A$ and $m, n \in \mathbb{F}_p$. χ is a good choice in fact $\chi^i \neq 0$ because it is a generator of $\mathrm{Hom}(\mathbb{F}_p^*, \mathbb{Z}_p^*)$ and it belongs to I_1 because

$$([m]\chi)(n) = \chi(mn) = \chi(m)\chi(n).$$

If $G = \alpha_{p,k}$ (resp. $\mu_{p,k}$), then $A = k[t]$ with $t^p = 0$ and $m(t) = t \otimes 1 + 1 \otimes t$ and so $[m]t = mt$ (resp. $s(1+t) = (1+t) \otimes (1+t)$ and so $[m](1+t) = (1+t)^m - 1$). Using the fact that in both cases

$$[m]t \equiv mt \equiv \chi(m)t \pmod{t^2}$$

it's easy to see that $e_1 t \equiv t \not\equiv 0 \pmod{t^2}$, and so we can take $f_1 = e_1 t$. □

In particular this Lemma shows us that the module structure of a finite group scheme of prime order is completely determined by an invertible module.

The example of $\mu_{p,\Lambda}$. In this section we want to rewrite the algebra and group structure of $\mu_{p,\Lambda}$. We will also introduce some notations necessary to our main aim: the classification.

Let $\mu_{p,\Lambda} = \mathrm{Spec}\ (B)$ with $B = \Lambda[z]$ and $z^p = 1$. The comultiplication in B is given by $m(z) = z \otimes z$ and so $[m]z = z^m$ for all $m \in \mathbb{F}_p$. We remember that $\epsilon(z) = 1$ so the augmentation ideal is $J = B(z-1)$ and it has a Λ-base consisting of the elements $z^m - 1$ for $m \in \mathbb{F}_p^*$:

$$B(z-1) = \Lambda(z-1) + ... + \Lambda(z^{p-1} - 1).$$

Now for each $i \in \mathbb{Z}$ we put

$$y_i = (p-1)e_i(1-z) = \sum_{m \in \mathbb{F}_p^*} \chi^{-i}(m)(1 - z^m) = \begin{cases} p - \sum_{m \in \mathbb{F}_p} z^m & \text{if } i \equiv 0 \bmod (p-1) \\ -\sum_{m \in \mathbb{F}_p^*} \chi^{-i}(m) z^m & \text{if } i \not\equiv 0 \bmod (p-1) \end{cases}$$

Note that y_i depends only on $i \bmod (p-1)$. Then

$$1 - z^m = \frac{1}{p-1} \sum_{i=1}^{p-1} \chi^i(m) y_i$$

for $m \in \mathbb{F}_p^*$ and

$$m(y_i) - y_i \otimes 1 - 1 \otimes y_i = -\sum_{m \in \mathbb{F}_p^*} \chi^{-i}(m)((1 - z^m) \otimes (1 - z^m))$$

$$= \frac{-1}{(p-1)^2} \sum_{m \in \mathbb{F}_p^*} \chi^{-i}(m) \sum_{j=1}^{p-1} \sum_{k=1}^{p-1} \chi^j(m)\chi^k(m) y_j \otimes y_k$$

$$= \frac{-1}{p-1} \sum_{j+k \equiv i(p-1)} y_j \otimes y_k.$$

Hence the comultiplication works as

$$m(y_i) = y_i \otimes 1 + 1 \otimes y_i + \frac{1}{1-p} \sum_{j=1}^{p-1} y_j \otimes y_{i-j}.$$

Note that

$$1 - z^m = \frac{1}{p-1} \sum_{i=1}^{p-1} \chi^i(m) y_i$$

implies that

$$J = \Lambda y_1 + ... + \Lambda y_{p-1}$$

and so $J_i = \Lambda y_i$ for each $i \in \mathbb{Z}$ in fact $\Lambda y_i \subset J_i$ because $y_i \in J_i$ and the equality follows because the Λy_i with $1 \leq i \leq p-1$ generate completely J. Putting $y = y_1$ we can define a sequence of elements

$$1 = w_1, w_2, ...$$

in Λ by

$$y^i = w_i y_i.$$

Note that this is a good definition because in this case the I_i are free Λ-modules and so there is exactly one possible choice for w_i.

Proposition 2.2.5. *The elements w_i are invertible for $1 \leq i \leq p-1$, and $w_p = pw_{p-1}$. We have $B = \Lambda[y]$, with $y^p = w_p y_p$, and*

1. $$m(y) = y \otimes 1 + 1 \otimes y + \frac{1}{1-p} \sum_{i=1}^{p-1} \frac{y^i}{w_i} \otimes \frac{y^{p-i}}{w_{p-i}}$$

2. $$[m]y = \chi(m)y \text{ for } m \in \mathbb{F}_p$$

3. $$w_i \equiv i! \pmod{p} \text{ for } 1 \leq i \leq p-1$$

4. $$z = 1 + \frac{1}{1-p}(y + \frac{y^2}{w_2} + ... + \frac{y^{p-1}}{w_{p-1}}).$$

Proof. By Lemma 2.2.4, we know that

$$\Lambda y^i = (\Lambda y)^i = (J_1)^i = J_i = \Lambda y_i$$

thus the w_i are invertible for $1 \leq i \leq p-1$. Clearly $(z-1)^p \equiv 0 \pmod{p}$, thus $y^p \equiv 0 \pmod{p}$; moreover from

$$1 - z^m = \frac{1}{p-1} \sum_{i=1}^{p-1} \chi^i(m) y_i$$

and the fact that $\frac{1}{1-p} \equiv 1 \pmod{p}$ we deduce that

$$z \equiv 1 + y + \frac{y^2}{w_2} + ... + \frac{y^{p-1}}{w_{p-1}} \pmod{p}.$$

To prove that $w_i \equiv i! \pmod{p}$ it's sufficient to compare the coefficients of $y^i \otimes y$, $1 \leq i < p-1$ of

$$m(z) = (1 + y + ... + \frac{y^{p-1}}{w_{p-1}}) \otimes (1 + y + ... + \frac{y^{p-1}}{w_{p-1}}) \equiv 1 + m(y) + ... + \frac{(m(y))^{p-1}}{w_{p-1}} \pmod{p}$$

which gives us $w_{i+1} \equiv (i+1)w_i$ and remembering that $w_1 = 1$ we conclude.

The last thing to prove is that $w_p = pw_{p-1}$. Choose an embedding $\Lambda \to K$ where K is a field with a primitive p-th root of unity ζ and extend the embedding to $\Lambda[z]$ sending z in ζ; the field can be for example an algebraic closure of $\mathbb{Q}_p \supset \mathbb{Z}_p \supset \Lambda$. Let $y_i \to \eta_i$ and rename $\eta = \eta_1$. Using the fact that

$$y_{p-1} = p - \sum_{m \in \mathbb{F}_p} z^m$$

we observe that $\eta_{p-1} = p \neq 0$ and because also $w_{p-1} \neq 0$, we conclude that $\eta \neq 0$. So we obtain

$$pw_{p-1} = \eta_{p-1} w_{p-1} = \eta^{p-1} = \frac{\eta^p}{\eta} = w_p$$

because we embedded Λ in K obviously $pw_{p-1} = w_p$ also in Λ. □

Lemma 2.2.6. *The $w_i \in \Lambda$ can be compute inductively from $w_1 = 1$ and the following relations:*

$$\frac{w_{i+j}}{w_i w_j} = \begin{cases} p & \text{if } i \equiv 0 \text{ or } j \equiv 0 \\ (-1)^i & \text{if } i \not\equiv 0 \ , \ j \not\equiv 0 \text{ but } i+j \equiv 0 \\ (-1)^{i+j+1}\mathfrak{J}(-i,-j) & \text{if } i \not\equiv 0 \ , \ j \not\equiv 0 \text{ and } i+j \not\equiv 0 \end{cases} \tag{2.2.2.1}$$

where the congruences are mod$(p-1)$, and where $\mathfrak{J}$ denotes the Jacobi sums

$$\mathfrak{J}(i,j) = \sum_{m+n=1, m,n \in \mathbb{F}_p^*} \chi^i(m)\chi^j(n).$$

Proof. Choose an embedding $\Lambda \to K$ as in the previous proof; then

$$\frac{w_{i+j}}{w_i w_j} = \frac{\eta_i \eta_j}{\eta_{i+j}}$$

because

$$w_{i+j}\eta_{i+j} = \eta^{i+j} = \eta^i \eta^j = w_i \eta_i w_j \eta_j.$$

Let's see the first case: suppose that $i \equiv 0$, then $\eta_i = p$ and $\eta_{i+j} = \eta_j$, so

$$\frac{w_{i+j}}{w_i w_j} = \frac{\eta_i \eta_j}{\eta_{i+j}} = \frac{p\eta_j}{\eta_j} = p.$$

Suppose now $i \not\equiv 0$ and $j \not\equiv 0 \pmod{(p-1)}$; then $p \neq 2$ and $\chi(-1) = -1$; letting l, m, n run through $\mathbb{F}_p$ we have

$$\begin{aligned} \eta_i \eta_j &= (\sum_{m \neq 0} \chi^{-i}(m)\zeta^m)(\sum_{n \neq 0} \chi^{-j}(n)\zeta^n) \\ &= \sum_{mn \neq 0} \chi^{-i}(m)\chi^{-j}(n)\zeta^{i+j} \\ &= \sum_l \zeta^l \sum_{m+n=l, mn \neq 0} \chi^{-i}(m)\chi^{-j}(n) \\ &= \sum_{n \neq 0} \chi^{-i}(-n)\chi^{-j}(n) + \sum_{l \neq 0} \sum_{m+n=-1, mn \neq 0} \zeta^l \chi^{-i}(-lm)\chi^{-j}(-ln) \\ &= (-1)^i \sum_{n \neq 0} \chi^{-(i+j)}(n) + (-1)^{(i+j)} \sum_{l \neq 0} \zeta^l \chi^{-(i+j)}(l) * \sum_{m+n=-1, mn \neq 0} \chi^{-i}(m)\chi^{-j}(n) \\ &= \begin{cases} (-1)^{i+j+1}\eta_{i+j}\mathfrak{J}(-i,-j) & \text{if } i+j \not\equiv 0 \\ (-1)^i(p-1) - \sum_{m+n=-1, mn \neq 0} \chi^i(\frac{n}{m}) & \text{if } i+j \equiv 0 \end{cases} \end{aligned}$$

This proves the third case of 2.2.2.1, and the second results on replacing n by mn in the last formula

$$\sum_{m+n=-1, mn \neq 0} \chi^i(\frac{n}{m}) = \sum_{m(1+n)=-1, n \neq 0, -1} \chi^i(n) = -\chi^i(-1) = -(-1)^i.$$

□

Take now our example group scheme of order 2 over a field k. We would like to find a pair of "object" which in some sense define it. The module structure is $k \oplus k$ thanks to Lemma 2.2.4. So for sure the two parameters we are finding must concern the algebra structure, and the group structure. First consider $a \in k$ such that $x^2 = ax$ where x is a generator of I. Using the fact that $\mathrm{Id} = \mu \circ (\mathrm{Id} \otimes \epsilon) \circ m = \mu \circ (\epsilon \otimes \mathrm{Id}) \circ m$ it's immediate to check that $m(x) = x \otimes 1 + 1 \otimes x - c(x \otimes x)$. So (a, c) could be the right objects. Now we claim that $ac = 2$. We notice that $m(x)^2 = m(x^2) = am(x)$ and so comparing the coefficients of $x \otimes x$ in the writing of $m(x)^2$ and of $am(x)$ we obtain $ac = a^2c^2 + +2 - 4ac$ which implies $(ac-1)(ac-2) = 0$. Now the inverse of 1 is 1 and so $\epsilon \circ i = \epsilon$ and so $i(x) \in I$ and $i(x) = \beta x$ (with $\beta \in k$ and $\beta^2 = 1$ because $ß \circ ß = id$). We also observe that $x \otimes 1 + 1 \otimes \beta x - c\beta x \otimes x$ becomes 0 under multiplication and so $1 + \beta = ac\beta$. Multiplying by β we obtain $ac = \beta + 1$, and so $ac - 1$ is invertible. Remembering that $(ac-1)(ac-2) = 0$ we deduce that $ac = 2$ and so $\beta = 1$.

Let's see first how to generalize this idea on affine group schemes over a local ring. Let G be an $S - group$ of order p with $A = \mathcal{O}_G$.

Now assume that $\mathcal{O}_S$ is a local and complete ring. Lemma 2.2.4 tells us that I_i is free of rank 1 over $\mathcal{O}_S$ and so if x is a generator of I_1 then

$$A = \mathcal{O}_S \oplus \mathcal{O}_S x \oplus \mathcal{O}_S x^2 \oplus ... \oplus \mathcal{O}_S x^{p-1}.$$

In particular from the fact that $I_i I_j \subseteq I_{i+j}$ for every $i, j \in N$ we see that it exists $a \in \mathcal{O}_S$ s.t.

$$x^p = ax$$

and let $a^\vee$ be the analogous in $A^\vee$. In this case we have apparently considered a different representative of the group multiplication respect to the previous example; but we will see that they are basically the same.

Remark. Suppose that M is another S-group isomorphic to G. Then $B = \mathcal{O}_M \cong A$. It's easy to show that if J is the augmentation ideal of B, then the isomorphism sends J in I and J_1 in I_1. In particular a generator of J_1 is sent in a generator of I_1 and so it is of the form $y = ux$ where $u \in \mathcal{O}_S$ is an invertible element and x is a generator of I_1. Then

$$y^p = u^p x^p = u^p ax = au^{p-1} y$$

and so to each isomorphic class of groups we can assign the equivalence class of the multiplication where $[a_1] = [a_2] \iff a_1 = u^{p-1} a_2$ for some invertible $u \in \mathcal{O}_S$.

Now remember that we have proved that the pairing

$$G \times G^\vee \to \mathbb{G}_{m,S}$$

factors through $\mu_{p,S}$. This is the same to say that we have a morphism

$$\phi : \mathcal{O}_S \otimes_\Lambda \Lambda[y] = \mathcal{O}_S[y] \to A \otimes A^\vee.$$

The next Lemma is the affine and local version of Lemma 2.2.8 so we state it and postpone the proof in the general case.

Lemma 2.2.7. *The image $\phi(y) = x \otimes x'$ is a generator of $I_1 \otimes I_1^\vee$ and $aa^\vee = w_p$ with a (resp.$a^\vee$) s.t. $x^p = ax$ (resp. $x'^p = a^\vee x'$).*

We now continue our discussion on the S-group G where S is a general scheme over Spec(Λ). Let

$$\mathbf{S}_{\mathcal{O}_S}[I_1] = \mathcal{O}_S \oplus I_1 \oplus I_1^{\otimes 2} \oplus ...$$

denote the symmetric algebra generated by I_1 over $\mathcal{O}_S$; note that in this case there are invertible modules which are not trivial. We know that the morphism $\mathbf{S}_{\mathcal{O}_S}[I_1] \to A$ induced by the inclusion is surjective, and that its kernel is the ideal generated by $(a-1) \otimes I_1^{\otimes p}$, where

$$a \in \Gamma(S, I_1^{\otimes(1-p)}) = \mathrm{Hom}_{\mathcal{O}_S}(I_1^{\otimes p}, I_1)$$

is the element corresponding to the morphism $I_1^{\otimes p} \to I_1$ induced by the multiplication in A; we stress the fact that the presence of invertible not trivial modules forbids us to see a as an element in $\mathcal{O}_S$.

Let $G^\vee = \mathrm{Spec}\ (A^\vee)$ be the Cartier dual of G and let $I^\vee$, $I_i^\vee$ and $a^\vee$ be the analogues for $G^\vee$ of I, I_i and a for G. Note that the notation is consistent as $(I_A)^\vee = I_{A^\vee}$ and $(I_i)^\vee = (e_i I_A)^\vee = (I^\vee)_i$.

Lemma 2.2.8. *The image $\phi(y)$ of y is a generating section of $I_1 \otimes I_1^\vee$; if we use it to identify $I_1^\vee$ with $I_1^{\otimes(-1)}$, then $a \otimes a^\vee = w_p 1_{\mathcal{O}_S}$.*

Proof. The Cartier pairing $(\zeta, \zeta') \to < \zeta, \zeta' >$ satisfies

$$< \zeta^m, (\zeta')^n > = < \zeta, \zeta' >^{mn}.$$

Hence, for all $m, n \in \mathbb{F}_p$

$$([m] \otimes [n])\phi(y) = \phi([mn]y) = \phi(\chi(mn)y) = \chi(m)\chi(n)\phi(y)$$

hence $\phi(y) \in \Gamma(S, I_1 \otimes I_1^\vee)$. Clearly $\phi(y)$ does not vanish at any point $s \in S$, for if it did, then the Cartier pairing on the fibre $G_s \times G_s^\vee \to \mathbb{G}_{m,s}$ would degenerate; this is impossible and the idea is that $G = \mathrm{Hom}(G^\vee, \mathbb{G}_m)$ and so if $< \zeta, \zeta^\vee >= \zeta(\zeta^\vee) = 0$ for every $\zeta^\vee \in G^\vee$ then $\zeta = 0$ in a certain way by definition.

Since ϕ is a morphism of algebras,

$$w_p \phi(y) = (\phi(y))^p = (\phi(y))^{\otimes p} \otimes a \otimes a^\vee$$

and this shows that $a \otimes a^\vee = w_p$ if we identify $I_1 \otimes I_1^\vee$ with $\mathcal{O}_S$ in such a way that $\phi(y) = 1$. □

Finally we are ready to expose the main theorem but first we want to give an idea of what happens using our example.

The most interesting part of the theorem is when it shows how to construct a group scheme starting from an invertible module and a factorization of p.

Note that a generic group of order 2 has a structure of algebra and of group which are very similar to the once of $\mu_{2,k}$. In fact we have seen that $\mu_{2,k}$ is generated by an element y such that:

$$y^2 = 2y \text{ and } m(y) = y \otimes 1 + 1 \otimes y - y \otimes y.$$

In particular if we try to deform the generator multiplying it by an invertible element $Y = u^{-1}y$ with $u \in k$ then

$$Y^2 = 2u^{-1}Y \text{ and } m(Y) = Y \otimes 1 + 1 \otimes Y - uY \otimes Y.$$

So taking $u = 2/a = b$ we obtain the desired group scheme.

Theorem 2.2.9. *For any scheme S over* Spec *(Λ), the map*

$$G \to (I_1^\vee, a, a^\vee)$$

discussed above gives a bijection between the isomorphism classes of S-groups of order p and the isomorphism classes of triples (L, a, b) consisting of an invertible $\mathcal{O}_S$-module L, a section $a \in \Gamma(S, L^{\otimes(p-1)})$, and a section $b \in \Gamma(S, L^{\otimes(1-p)})$, such that $a \otimes b = w_p 1_{\mathcal{O}_S}$.

Proof. First we prove the injectivity of the map; starting from a triple $(I^\vee, a, a^\vee)$ we can reconstruct the structure of S-scheme of G and $G^\vee$ (firstly without the structure of S-group) together with the Cartier morphism $G \times G^\vee \to \mu_{p,S}$. Indeed A is the quotient of the symmetric algebra $\mathbf{S}_{\mathcal{O}_S}[(I_1^\vee)^{\otimes(-1)}]$ by an ideal determined by a, $A^\vee$ is the quotient of $\mathbf{S}_{\mathcal{O}_S}[I_1^\vee]$ by an ideal determined by $a^\vee$, and the morphism $\phi : B[y] \to A \otimes A^\vee$ is determined by $\phi(y) = 1 \in (I_1^\vee)^{\otimes(-1)} \otimes I_1^\vee = \mathcal{O}_S$. But the Cartier morphism determines the group structure of G and $G^\vee$ because it gives for each S-scheme T a map

$$G(T) \hookrightarrow \mathrm{Hom}_{T-schemes}(G_T^\vee, \mu_{p,T})$$

which identifies $G(T)$ as a subgroup of $\mu_p(G_T^\vee)$. The law of composition thus induced on the functor $T \to G(T)$ determines the law of composition in G.

Now we have to show that every triple (L, a, b) comes from a group scheme. The problem is local on the base S, so we can suppose $S = \mathrm{Spec}\, R$ where R is a local ring, $L = R$ and a, b can be viewed as element of R such that $ab = w_p * 1_R$.

Let F denote the field of fractions of Λ, and let U be an indeterminate. We know that $\mu_{p,F(U)}$ is equal to Spec (A) where

$$A = F(U)[y] \text{ and } y^p = w_p y$$

with

$$m(y) = y \otimes 1 + 1 \otimes y + \frac{1}{1-p} \sum_{i=1}^{p-1} \frac{1}{w_i w_{p-i}} y^i \otimes y^{p-i}$$

and

$$[m]y = \chi(m)y.$$

Let $Y = U^{-1}y \in A$. Then

$$A = F(U)[Y] \ , \ Y^p = w_p U^{1-p} Y$$

and

$$m(Y) = Y \otimes 1 + 1 \otimes Y + \frac{1}{1-p} \sum_{i=1}^{p-1} \frac{U^{p-1}}{w_i w_{p-i}} Y^i \otimes Y^{p-i}$$

and $[m]Y = \chi(m)Y$. Let

$$R_0 = \Lambda[w_p U^{1-p}, U^{p-1}] \subset F(U)$$

and

$$C = R_0[Y] \subset A.$$

From the formulas above, we see that C is free of rank p over R_0 and that $m(C) \subset C \otimes_{R_0} C$. Also $[-1]C \subset C$. Hence we define an R_0-group G of order p by $G =$ Spec (C) with the multiplication induced by m. Clearly

$$R_0 \cong \Lambda[X_1, X_2]/(X_1 X_2 - w_p).$$

Hence the triple (R, a, b) determines a morphism of Λ-algebras $h : R_0 \to R$ such that $h(w_p U^{1-p}) = a$ and $h(U^{p-1}) = b$, and then it follows from the explicit formulas for the structure of G that the triple (R, a, b) comes from G_R deduced from G by the base extension via h.

□

We sate now the theorem in the local case.

Theorem 2.2.10. *For any scheme S over $Spec(\Lambda)$, the map $G \to (a, c)$ where $c = a^\vee / w_{p-1}$ gives a bijection between the isomorphism classes of $S-$groups of order p and equivalence classes of factorization $p = ac$ where 2 factorizations $p = a_1 c_1$ and $p = a_2 c_2$ are equivalent if there exists an invertible element $u \in \mathcal{O}_S$ s.t. $a_2 = u^{p-1} a_1$ and $c_2 = u^{1-p} c_1$.*

2.2.3 Examples

In this section we will try to classify all the group schemes of order p over the following base rings; actually we know that thanks to Theorem 2.2.10 this problem is equivalent to find the equivalence classes of factorizations of p.

1. $\mathbb{F}_p$.

   Proposition 2.2.11. *The group schemes of order p over $\mathbb{F}_p$ are of the form $(0,0), (0,a)$ or $(a,0)$ with $a \in \mathbb{F}_p$ different from zero.*

   Proof. $(0,0), (0,a)$ or $(a,0)$ with $a \in \mathbb{F}_p$ different from zero are clearly all the possible factorizations of p in $\mathbb{F}_p$.

   So we have only to show that they are each other not equivalent. Fixing $a \in \mathbb{F}_p$ non zero, clearly the couples $(a,0), (0,0)$ and $(0,a)$ are not equivalent.

   It remains to prove that if a, b are non zero and different from each other then $(a,0)$ and $(b,0)$ are not equivalent (or what is the same that $(0,a)$ and $(0,b)$ are not equivalent). Suppose they are, then there is a unity $u \in \mathbb{F}_p$ such that $a * u^{p-1} = b$; but $u^{p-1} = 1$ which implies that $a = b$; absurd. □

   In particular the couples $(0,0), (0,1), (1,0)$ represent respectively $\alpha_{p,\mathbb{F}_p}, \mu_{p,\mathbb{F}_p}(\mathbb{Z}/p\mathbb{Z})_{\mathbb{F}_p}$.

2. k algebraically closed.

   Proposition 2.2.12. *Let k be an algebraically closed field over Λ_p. If k has characteristic 0, then there exists only one group scheme of order p. If k has characteristic p, then the only group schemes of order p are $\alpha_{p,k}, \mu_{p,k}(\mathbb{Z}/p\mathbb{Z})_k$.*

   We observe that we already know this result thanks to Lemma 2.1.6; let's see an easier proof.

   Proof. If char $(k) = 0$, then p is invertible and so each of its factors too. Note that two distinct factorizations are of the form $(a, b), (a*u, b*u^{-1})$. We basically have to prove that u has a $(p-1)th$ root. But in an algebraically closed field each polynomial has solution in particular $x^{p-1} - u$; this implies that there exist only one group.

   If char $(k) = p$, the possible factorizations are $(0,0), (0,z)$ and $(z,0)$ where z is a unity; but for the same reason as before the factorizations $(0,z), (0,z')$ are equivalent (and also in the dual case $(z,0), (z',0)$) which implies that the group schemes are represented by $(0,0), (1,0)$ and $(0,1)$ which correspond respectively to $\alpha_{p,k}$, $(\mathbb{Z}/p\mathbb{Z})_k$ and $\mu_{p,k}$. □

3. $\mathbb{Z}_p$.

   Theorem 2.2.13 (Hensel's Lemma)**.** *Let R be a ring that is complete with respect to the ideal $\mathfrak{m}$, and let $f(x) \in R[x]$ be a polynomial. If a is an approximate root of f in the sense that*

   $$f(a) = 0 \pmod{f'(a)^2 \mathfrak{m}},$$

   then there is a root b of f near a in the sense that

   $$f(b) = 0 \text{ and } b = a \pmod{f'(a)\mathfrak{m}}.$$

   If $f'(a)$ is a nonzerodivisor in R, then b is unique.

First we notice that $\mathbb{Z}_p$ is a domain of characteristic 0 which implies that an affine group is totally determined by its algebraic structure. Obviously every factorization of p must be of the form $(p * s^{-1}, s)$ or $(s, p * s^{-1})$ where s is a unity.

Lemma 2.2.14. *Let $z \in \mathbb{Z}_p$ a unity. The equation $x^{p-1} = z$ has solution in $\mathbb{Z}_p$ if and only if $z = 1$ in $\mathbb{Z}/p\mathbb{Z}$.*

Proof. Suppose the equation has a solution y. z is a unity and so $z \neq 0 \in \mathbb{Z}/p\mathbb{Z}$ which implies that $y \neq 0 \in \mathbb{Z}/p\mathbb{Z}$. But so $y \in \mathbb{Z}/p\mathbb{Z}$ is a unity and the result follows by Fermat's little theorem.

If $z = 1$ in $\mathbb{Z}/p\mathbb{Z}$ then clearly the equation has a solution in $\mathbb{Z}/p\mathbb{Z}$, but by Hensel's Lemma there is a solution also in $\mathbb{Z}_p$. □

Corollary 2.2.15. *For each $1 \leq i \leq p-1$ choose $a_i \in \mathbb{Z}_p$ such that $a_i = i$ in $\mathbb{Z}/p\mathbb{Z}$. The group schemes of order p over $\mathbb{Z}_p$ are of the form $(a_i, p * a_i^{-1})$ or $(p * a_i^{-1}, a_i)$ where $1 \leq i \leq p-1$.*

Proof. We remember that we are in a dvr, so for each $1 \leq i < j \leq p-1$ it does not exist an invertible element $u \in \mathbb{Z}_p$ such that $a_i * u^{p-1} = p * a_j^{-1}$; so for each $1 \leq i < j \leq p-1$ the couples $(a_i, p * a_i^{-1})$ and $(p * a_j^{-1}, a_j)$ are not equivalent.

Now we want to show that two couples of the form $(a, p * a^{-1})$ and $(b, p * b^{-1})$ with a, b unities, are equivalent if and only if $a = b$ in $\mathbb{Z}/p\mathbb{Z}$. $(a, p * a^{-1})$ is equivalent to $(b, p * b^{-1}) \iff$ it exists u unity such that $a * u^{p-1} = b \iff u^{p-1} = b * a^{-1} \iff b * a^{-1} = 1$ in $\mathbb{Z}/p\mathbb{Z}$ thanks to the Lemma 2.2.14 $\iff a = b$ in $\mathbb{Z}/p\mathbb{Z}$. □

4. $k[[t]]$.

Proposition 2.2.16. *If k has characteristic 0, then each group scheme of order p over $k[[t]]$ is obtained from a unique group scheme over k.*

Proof. We remember that an element in $k[[t]]$ is a unity if and only if its constant term is different from zero. Every factorization of p is also here of the form $(u, p * u^{-1})$ where u is a unity; note that we have considered also the factorizations of the form $(p * u^{-1}, u)$ because p is invertible. Our problem is reduced to understand if the equation $x^{p-1} = u$ has solutions or not. Luckily Hensel's Lemma simplifies the problem stating that the equation has a solution in $k[[t]]$ if and only if it has a solution in k. This permits in particular to conclude that the group schemes of order p on $k[[t]]$ are in bijection with the once over k. □

Proposition 2.2.17. *If k has characteristic p, then each group schemes of order p over $k[[t]]$ is of the form $(t^m a, 0)$ or $(0, t^m a)$ with $m \in \mathbb{N}$ for all a such that $(a, 0)$ denotes distinct group schemes of order p over k.*

Proof. Suppose char $(k) = p$. Every factorization of $p = 0$ is of the form $(0,0)$, $(0,a)$ or $(a,0)$ for every $a \in k[[t]]$ different from zero. Clearly for a fixed a the couples $(0,0)$, $(0,a)$ and $(a,0)$ are not equivalent each other, so our problem is to understand if $(a,0)$ and $(b,0)$ can be equivalent for some $b \in k[[t]]$ different from zero (we can state in analogous way the dual problem with $(0,a)$ and $(0,b)$). So we want to study if the equation $ax^{p-1} = b$ has a solution or not in the unities of $k[[t]]$. The dvr structure of $k[[t]]$ implies that $a = t^n * u$ and $b = t^m * v$ for unique m and n where u, v are unities; this means that if $m \neq n$ there is no chance that our equation has solution and so a and b represent two different group scheme. Suppose $n = m$; in this case we have to check if $x^{p-1} = u/v$ has solution which can be checked on k due to Hensel's Lemma. □

Bibliography

[Mil12] James S. Milne. Basic theory of affine group schemes, 2012.

[Pin04] Richard Pink. Finite group schemes, 2004.

[Sch00] René Schoof. Introduction to finite group schemes, 2000.

[TO70] John Tate and Frans Oort. Group schemes of prime order. *Annales scientifiques de l'E.N.S.*, 1970.