A course on finite flat group schemes and p-divisible groups

HEIDELBERG — SUMMER TERM 2009

JAKOB STIX

dedicated to a marvelous cube

ABSTRACT. — The theory of p-divisible groups plays an important role in arithmetic. The purpose of this course was to carefully lay the foundations for finite flat group schemes and then to develop enough of the theory of p-divisible groups in order to prove the Hodge–Tate decomposition for H^1.

1. Introduction

1.1. **Examples.** Let us begin with a list of the basic examples for p-divisible groups.

(1) The discrete group

$$\mathbb{Q}_p/\mathbb{Z}_p = \bigcup_n \frac{1}{p^n}\mathbb{Z}/\mathbb{Z}$$

has a surjective multiplication by p map. How much more "divisible by p" can a group be? Well, the finite abelian groups of order prime to p share this property, but are not considered p-divisible in our sense.

(2) The p-primary torsion of $\mathbb{G}_\mathrm{m}$: that is

$$\mu_{p^\infty} = \bigcup_n \mu_{p^n}.$$

Let's say we work over a field k with algebraic closure $\bar{k}$ of characteristic 0, then μ_{p^n} is a $\mathrm{Gal}_k = \mathrm{Gal}(\bar{k}/k)$-module, which as a group is free of rank 1 as a $\mathbb{Z}/p^n\mathbb{Z}$-module. Here μ_{p^∞} is a version of $\mathbb{Q}_p/\mathbb{Z}_p$ endowed with a continuous Galois action. But we did not specify a field or any basis, simply because μ_{p^∞} works just over any base scheme S as a union of finite flat group schemes over S. When $S = \mathrm{Spec}(k)$ is a field of characteristic p, then μ_{p^n} is infinitesimal for every n, and so the underlying reduced space is just $\mathrm{Spec}(k)$. This shows the importance to study finite flat group schemes in general to capture important arithmetic of p-primary sort in characteristic p.

(3) A more general version of example (2) replaces $\mathbb{G}_\mathrm{m}$ by let's say an abelian variety A and considers the p-primary torsion

$$A[p^\infty] = \bigcup_n A[p^n]$$

which is a union of finite flat group schemes of rank p^{hn} where $h = 2\dim(A)$.

Date: July 2009, revised September 2012, version of September 18, 2012.

1.2. **. . . and what they are good for.** Special properties of p-divisible groups are used in:

(1) Analysis of the local p-adic Galois action on p-torsion points of elliptic curves, see Serre's theorem on open image for non-CM elliptic curves over number fields [Se72], and more recently in modularity results.
(2) As a tool for representing p-adic cohomology, for example in p-adic Hodge theory.
(3) To describe local properties of the moduli spaces of abelian varieties. These map to moduli of p-divisible groups, which are much simpler being essentially a piece of semi-linear algebra. The map is formally étale due to a Theorem of Serre and Tate.
(4) Explicit local class field theory: via Lubin–Tate formal groups we can describe the wildly ramified abelian extensions, see Section §10.4.
(5) The true(?) fundamental group in characteristic p must include infinitesimal group schemes, and p-divisible groups enter through their p-adic Tate module.

1.3. **Goal and structure of the course.** Section §2 and Sections §3 – §8 discuss the foundational material on group schemes and finite group schemes, with a detailed discussion of étale group schemes in Section §7 and quotients of finite flat equivalence relations in Section §6. After the introduction of p-divisible groups in Section §9, in Section §10, the discussion of formal groups that following [Ta66] leads in Section §11 towards the main goal of the course: the p-adic Hodge-Tate decomposition for the Tate-module

$$\mathrm{T}_p(G) \otimes_K \widehat{\overline{K}} = \big(t_G(K) \otimes_K \widehat{\overline{K}}\big)(1) \oplus \big(t^*_{G^D}(K) \otimes_K \widehat{\overline{K}}\big).$$

Serious omissions which make the course less about p-divisible groups but rather about finite flat group schemes are the absence of Witt vectors, the Cartier-ring and Dieudonné theory, see [Gr74], [De72]. Quite recently, a truly p-adic proof of the Hodge Tate decomposition and classification of p-divisible groups have been worked out by Scholze and Weinstein using the theory of perfectoid spaces.

Another sort of omissions concerns exercises. These should be included in any thorough version of course notes. Here there are none. Instead, we may refer to exercises on Brian Conrad's web page from a course of Andreatta, Conrad and Schoof in Oberwolfach 2005, see [ACS05] and [Sc00].

1.4. **Conventions, intentions and a warning.** We usually work over an arbitrary Noetherian ring R as a base. Whenever convenient (or necessary) we work over a complete Noetherian local ring, or even a perfect field. We try to avoid to use explicitly scheme theory.

I would like to express my gratitude for feedback from the participants of my course in Heidelberg in 2009, and especially to Dmitriy Izychev for a thorough reading of these notes. However, these course notes come with no warranty. Please use at your own risk.

Contents

1. Introduction 1
2. Group schemes 3
3. Finite flat group schemes 9
4. Grothendieck topologies 14
5. fpqc sheaves 18
6. Quotients by finite flat group actions 22
7. Étale finite flat group schemes 33
8. Classification of finite flat group schemes 38
9. p-divisible groups 54
10. Formal groups 57
11. Hodge–Tate decomposition 68

References 76

2. Group schemes

References: [Sh86] §2, [De72] Chapter I + II.

2.1. **The functor of points.** All rings are commutative with 1. A **group functor** over a ring R is a covariant functor

$$G : \mathscr{A}_R \to \mathscr{G}rps$$

$$T \mapsto G(T)$$

on the category $\mathscr{A}_R$ of R-algebras with values in the category of groups $\mathscr{G}rps$. A **group scheme** over R is a group functor over R which has special properties, that we need not bother with when dealing with affine group schemes, to be defined below. They will satisfy them automatically. For an R-homomorphism $\varphi : T \to S$ we abbreviate for $g \in G(T)$ the image $G(\varphi)(g)$ by $\varphi(g)$.

Here are some examples of group schemes.

(1) The additive group $\mathbb{G}_{\mathrm{a}}$ with $\mathbb{G}_{\mathrm{a}}(T) = (T, +)$.

(2) The multiplicative group $\mathbb{G}_{\mathrm{m}}$ with $\mathbb{G}_{\mathrm{m}}(T) = (T^\times, \cdot)$. Here and in these notes we denote the group of units in a ring T by $T^\times$.

(3) The general linear group GL_n with

$$\mathrm{GL}_n(T) = \{n \times n \text{ matrices } A \text{ with entries in } T \text{ and } \det(A) \in T^\times\}.$$

(4) The special linear group SL_n with

$$\mathrm{SL}_n(T) = \{A \in \mathrm{GL}_n(A) \ ; \ \det(A) = 1\}.$$

(5) The nth roots of unity μ_n with

$$\mu_n(T) = \{t \in T^\times \ ; \ t^n = 1\}.$$

(6) When $p \cdot R = 0$, then we also have the kernel of Frobenius α_p with

$$\alpha_p(T) = \{t \in (T, +) \ ; \ t^p = 0\}.$$

(7) The **constant group scheme**: let G be a finite (discrete) group. The associated constant group scheme $G = \underline{\mathrm{G}}$ over R maps an R-algebra T to the group of partitions of unity indexed by G:

$$\underline{\mathrm{G}}(T) = \{(e_g)_{g \in \mathrm{G}} \ ; \ e_g \in T, \quad 1 = \sum_{g \in G} e_g, \quad e_g e_h = \delta_{g,h} e_g\},$$

that is decompositions of $1 \in T$ into mutually orthogonal idempotents. The group structure comes from convolution

$$(e_g) \cdot (f_g) := (\sum_{g = h \cdot h'} e_h \cdot f_{h'})_g$$

with unit

$$\mathbf{1} = (\delta_{1,g})_g.$$

If T is an integral domain, then all $e_g = 0$ except form one. This yields a group homomorphism

$$\underline{\mathrm{G}}(T) = G$$

in this case. The constant group is more conveniently described by its algebra $A = \prod_g R$, see below.

2.2. **Affine group schemes.** For any category $\mathscr{C}$ the functor

$$\mathscr{C} \to Fun(\mathscr{C}, \mathscr{S}ets)$$

$$X \mapsto h_X := \mathrm{Hom}_{\mathscr{C}}(X, -)$$

is contravariant fully faithful. A functor $F : \mathscr{C} \to \mathscr{S}ets$ isomorphic to $\mathrm{Hom}(X, -)$ for an object X is said to be **represented by** X and the element $f_{\mathrm{univ}} \in F(X)$ corresponding to $\mathrm{id}_X \in \mathrm{Hom}(X, X)$ is the **universal element**. More precisely, F is represented by the pair (X, f_{univ}), which fixes also the isomorphism as a special case of the Yoneda Lemma: We have a natural identification

$$F(X) = \mathrm{Hom}(h_X, F)$$

by

$$f \in F(X) \mapsto \big(\varphi : X \to T \in h_X(T) \mapsto \varphi(f) \in F(T)\big)$$

which holds for any functor F. For $F = h_Y$ it shows the assertion of fully faithfulness above.

An **affine group scheme over** R is a representable group functor $G : \mathscr{A}_R \to \mathscr{G}rps$. So an affine group scheme over R is given by an R-algebra A as $G = h_A$ and comes endowed with its universal element $g_{\mathrm{univ}} \in G(A)$.

All the examples given in Section §2.1 are in fact affine group schemes. For example, for a finite discrete group G, we have

$$\underline{\mathrm{G}} = \mathrm{Hom}(\prod_{g \in G} R, -)$$

for the constant group functor $\underline{\mathrm{G}}$ over R.

2.3. **The Hopf algebra.** The pair (A, g_{univ}) only determines G as a functor with values in the category $\mathscr{S}ets$. What describes its group structure?

Let $G = h_A$ be a group functor on R-algebras. Note that $h_A \times h_B : T \mapsto \mathrm{Hom}(A, T) \times \mathrm{Hom}(B, T)$ is represented by $h_{A \otimes_R B}$. By this observation and the Yoneda Lemma we deduce that

(i) the multiplication $G \times G \to G$ yields a comultiplication $\Delta : A \to A \otimes_R A$;
(ii) the unit $1 \in G$ yields a counit map $\epsilon : A \to R$, as $A \mapsto \{1\}$ is represented by R, necessarily surjective;
(iii) the inverse $\mathrm{inv} : G \to G,\ g \mapsto g^{-1}$ yields the antipode $S : A \to A$.

All these maps are R-algebra maps. We leave as an exercise to spell out the various commutative diagrams which encode the laws for multiplication, unit and inverse, namely:

(i) associativity,
(ii) being a unit (on both sides),
(iii) being an inverse.

A **commutative Hopf algebra** over R is by definition an R-algebra A with comultiplication Δ, augmentation ε and antipode S that make these diagrams commutative.

We work out the example GL_n over $\mathbb{Z}$. It is represented by

$$A = \mathbb{Z}[X_{i,j};\ 1 \leq i,j \leq n][1/\det(\underline{X})]$$

as a functor with values in sets and GL_n obtains its group structure by the following Hopf algebra structure.

(i) Comultiplication: let $Y_{i,j}$ (resp. $Z_{i,j}$) denote the variables in the first (resp. second factor).

$$\Delta(X_{i,j}) = \sum_k Y_{i,k} \otimes Z_{k,j}.$$

(ii) Counit:

$$\varepsilon(X_{i,j}) = \delta_{i,j}.$$

(iii) Antipode: we define $(\underline{X}_{\hat{j},\hat{i}}) = (\underline{X}$ with j^{th} row and i^{th} column omitted) and then the antipode map is given by

$$S_{i,j} = S(X_{i,j}) = (-1)^{i+j}\det(\underline{X}_{\hat{j},\hat{i}}) \cdot \det(\underline{X})^{-1}.$$

Why do these formulas induce a group structure on $\mathrm{GL}_n(T)$ for any ring T? Check well-definedness of the maps and the axioms for the universal element: the matrix

$$(\underline{X}) = (X_{i,j}).$$

To be well-defined means

$$\begin{aligned} \Delta(\det(\underline{X})) &= \det(\underline{Y}) \otimes \det(\underline{Z}) \in (A \otimes_R A)^\times, \\ \varepsilon(\det(\underline{X})) &= 1 \in A^\times, \\ S(\det(\underline{X})) &= \det(\underline{S}) = 1/\det(\underline{X}) \in A^\times. \end{aligned}$$

We leave checking the axioms to the reader: associative, unit, inverse. All this may be checked for the universal matrix and hence in an integral domain or even its quotient field, hence a field, where this is the topic of a first course in Linear Algebra.

2.3.1. *Algebraic affine group schemes.* An **algebraic affine group scheme over** R is an affine group scheme such that its Hopf algebra is finitely generated as an R-algebra, which means that 'we have only finitely many coordinates'.

2.3.2. *Translation action.* For $g \in G(R)$ we have the **left translation**

$$\lambda_g : G \to G,$$

given on G as functor with values in sets by $\lambda_g(T) : G(T) \to G(T)$ mapping for the R-algebra $i : R \to T$ an element $t \in G(T)$ to $i(g)t \in G(T)$. The same with **right translation**

$$\rho_g : t \mapsto ti(g).$$

There are corresponding automorphisms on the level of representing objects.

2.3.3. *Base change.* Let $R \to R'$ be a ring homomorphism. Then we have a **base change functor** $G \mapsto G \otimes_R R'$ from group functors over R to group functors over R' by

$$(G \otimes_R R')(T'/R') = G(T'/R),$$

where we regard the R'-algebra T' as an R-algebra via $R \to R' \to T'$. A handy shorthand notation for $G \otimes_R R'$ is $G_{R'}$ when R is understood from the context.

If G is representable by A then its base change is representable by $A' = A \otimes_R R'$ as a Hopf algebra:

$$\mathrm{Hom}_{R'}(A \otimes_R R', T') = \mathrm{Hom}_R(A, T').$$

An example for base change is given by

$$GL_{n,R} \otimes_R R' = \mathrm{GL}_{n,R'}\,.$$

2.4. **Algebraic group schemes in characteristic** 0 **are reduced.** We give the elegant proof of Oort from [Oo66] of the following theorem of Cartier. See also [Sh86] Theorem §3.

Theorem 1 (Cartier, Oort)**.** *An algebraic group G over a field k of characteristic 0 is reduced.*

This means of course in our language that the k-algebra A which represents G is reduced, i.e., has trivial nilradical. It follows that G is smooth over k by generic smoothness and homogeneity.

Proof: Step 1: As $A \subset A \otimes_k k^{\mathrm{alg}}$ we may base change to the algebraic closure k^{alg} or assume that k is algebraically closed to start with.

Step 2: Let $N \subset A$ be the nilradical. Vanishing $N = 0$ is by locality of modules and Nakayama's Lemma equivalent to $N \otimes_A A/\mathfrak{m} = 0$ for all maximal ideals $\mathfrak{m}$ of A. By Hilbert's Nullstellensatz, equivalently, N has only to vanish at each k-point in $G(k)$. The translation by $g \in G(k)$ acts transitively on the set of maximal ideals and thus it is sufficient to discuss vanishing of N in the localisation $N_{\mathfrak{m}}$ at $\mathfrak{m} = \ker(\varepsilon : A \to k)$ corresponding to the localisation at $1 \in G(k)$.

Step 3: As $A_{\mathrm{red}} = A/N$ is a reduced k-algebra of finite type, it is regular at a non-trivial Zariski-open set of maximal ideals. But $G(k)$ still acts transitive on those maximal ideals of A/N, hence A_{red} is regular everywhere. If $N \subseteq \mathfrak{m}^2$, then in particular we have the inequality

$$\dim(A) = \dim(A_{\mathrm{red}}) = \dim_k(\mathfrak{m}/(\mathfrak{m}^2 + N)) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$$

showing that A is regular at $\mathfrak{m}$ as well. A regular ring is an integral domain and thus reduced. It is therefore enough to know $N \subseteq \mathfrak{m}^2$.

Step 4: Take $x \in N_{\mathfrak{m}}$ with $x^n = 0$ but $x^{n-1} \neq 0$ for some $n \geq 2$. We consider now the composite

$$s : A \xrightarrow{\Delta} A \otimes_k A \twoheadrightarrow (A/x^{n-1}\mathfrak{m}) \otimes_k A/\mathfrak{m}^2.$$

As $\Delta(x) = x \otimes 1 + 1 \otimes x + y$ with $y \in \mathfrak{m} \otimes_k \mathfrak{m}$ we get

$$0 = s(x^n) = (s(x))^n \equiv (x \otimes 1 + 1 \otimes x + y)^n \equiv \binom{n}{1} x^{n-1} \otimes x \mod x^{n-1}\mathfrak{m} \otimes_k \mathfrak{m}^2.$$

The assumption of characteristic 0 allows us to cancel the binomial coefficient.

Step 5: By Nakayama's Lemma, $x^{n-1} \in x^{n-1}\mathfrak{m}$ would imply $x^{n-1} = 0$ in $A_{\mathfrak{m}}$ contradicting the assumption on n.

Step 6: Having a vanishing tensor in a tensor product over a field with first factor non-vanishing, we may conclude that the second factor vanishes: $x = 0$ in $A/\mathfrak{m}^2$. As x was arbitrary, we conclude $N \subseteq \mathfrak{m}^2$, and the proof is complete. □

2.5. **Homomorphisms.** A **homomorphism** $\varphi : G \to H$ between group functors is a natural transformation as functors with values in groups. For affine group schemes over R a homomorphism corresponds contravariant functorially to an R-algebra homomorphism, which is compatible with the structure of a Hopf algebra in a natural way. The set of all homomorphisms from G to H is denoted by $\mathrm{Hom}(G, H)$.

Proposition 2. *The category of affine group schemes over R is contravariant equivalent to the category of commutative Hopf algebras, with a Hopf algebra A corresponding to the affine group scheme $G = \mathrm{Hom}_R(A, -)$ that it represents.*

Proof: Obvious. □

2.5.1. *Kernel.* Let $\varphi : G \to H$ be a homomorphism of affine group schemes over R represented by $\varphi^* : A \to B$. The **kernel** is the group functor

$$\ker(\varphi) : \mathscr{A}_R \to \mathscr{G}rps$$

$$\ker(\varphi)(T) = \ker\big(\varphi(T) : G(T) \to H(T)\big).$$

The kernel $\ker(\varphi)$ is represented by $B \otimes_{A,\varepsilon_A} R$ and hence is also an affine group scheme over R. In more diagrammatic words, the kernel is the following fibre product of group valued functors:

$$\begin{tikzcd}
\ker(\varphi) \arrow[r] \arrow[d] & 1 \arrow[d, "\varepsilon_B"] \\
G \arrow[r, "\varphi"] & H.
\end{tikzcd}$$

The natural map $\ker(\varphi) \to G$ is a surjection $B \twoheadrightarrow B \otimes_A R$ on the level of R-algebras, i.e., a closed immersion.

2.5.2. *The Frobenius morphism.* See [De72] Chapter I.9+10. The Frobenius map is a special feature of positive characteristic, so we have to assume $p \cdot R = 0$, and we are in characteristic $p > 0$. The **Frobenius map** of an R-algebra A is

$$F_A : A \to A$$

defined by

$$a \mapsto F_A(a) = a^p.$$

The base change by $F_R : R \to R$ is denoted by $A^{(p)} = A \otimes_{R,F_R} R$. For an affine R-group scheme G the base change by Frobenius is $G^{(p)} = G \otimes_{R,F_R} R$. Base change by Frobenius is also called **Frobenius twist**. On points we have

$$G^{(p)}(R \to T) = G(R \xrightarrow{F_R} R \to T).$$

The Frobenius map commutes with any ring homomorphism. We can therefore define the **relative Frobenius** as the R-linear map $F_{A/R} : A^{(p)} \to A$ by the following diagram

(2.1)
$$\begin{tikzcd}
A & & \\
& A^{(p)} \arrow[ul, dashed, "F_{A/R}"] & A \arrow[l] \arrow[ull, bend right=20, "F_A"'] \\
& R \arrow[u] \arrow[uul, bend left=20] & R \arrow[u] \arrow[l, "F_R"']
\end{tikzcd}$$

The corresponding map $F_{G/R} : G \to G^{(p)}$ for an affine group scheme G is

(2.2)
$$\begin{tikzcd}
G \arrow[dr, dashed, "F_{G/R}"] \arrow[drr, bend left=20, "F_G"] \arrow[ddr, bend right=20] & & \\
& G^{(p)} \arrow[r] \arrow[d] & G \arrow[d] \\
& h_R \arrow[r, "F_R"] & h_R
\end{tikzcd}$$

In terms of points the relative Frobenius map acts as follows.

$$F_{G/R} : G(T) \to G^{(p)}(T) = G(R \xrightarrow{F_R} R \to T),$$

$$g \mapsto F_T(g),$$

so $F_{G/R}$ is a group homomorphism. This also follows from the fact that Frobenius twist, as a base change preserves products and Frobenius commutes with everything, in particular, the multiplication map $G \times G \to G$ of the affine group scheme. If we do a scalar extension $- \otimes_R R'$, then

$$\big(G \otimes_R R'\big)^{(p)} = \big(G^{(p)}\big) \otimes_R R'$$

and

$$F_{G \otimes_R R'/R'} = \big(F_{G/R}\big) \otimes \mathrm{id}'_R\,.$$

Remember that $G \rightsquigarrow G^{(p)}$ raises the coefficients to pth powers, whereas $F_{G/R}$ raises coordinates to pth powers.

2.6. **Commutative group schemes.** A group scheme is commutative if it takes values in the subcategory of abelian groups $\mathscr{A}b$.

2.6.1. *Sums and differences for homomorphisms into a commutative group scheme.* Let φ, ψ be homomorphisms from a group scheme G to a commutative group scheme H. Then we can define $\varphi + \psi$ (resp. $\varphi - \psi$) as the homomorphisms which are given by addition (resp. subtraction) for each argument $T \in \mathscr{A}_R$, e.g.,

$$(\varphi + \psi)(T) = \varphi(T) + \psi(T) : G(T) \to H(T).$$

For an affine group scheme G represented by A and a commutative affine group scheme represented by B the corresponding map on Hopf algebras is given by

$$\varphi + \psi \ : \ B \xrightarrow{\Delta} B \otimes_R B \xrightarrow{\varphi \otimes \psi} A \otimes_R A \to A$$

and

$$\varphi - \psi \ : \ B \xrightarrow{\Delta} B \otimes_R B \xrightarrow{\mathrm{id} \otimes S} B \otimes_R B \xrightarrow{\varphi \otimes \psi} A \otimes_R A \to A$$

where $A \otimes_R A \to A$ is the multiplication map of the R-algebra A. Clearly, for H commutative, the set

$$\mathrm{Hom}(G, H)$$

has thus been equipped with the structure of an abelian group functorially in both arguments. The 0 morphism is given by

$$B \xrightarrow{\varepsilon} R \to A$$

on the level of Hopf algebras.

2.7. **Products and coproducts.** The product of two affine group schemes is again an affine group scheme. On the level of Hopf algebras, this is given simply by the tensor product and for merely functors to $\mathscr{S}ets$ this was discussed above.

So we have projection maps $\mathrm{pr}_\alpha : G_1 \times G_2 \to G_\alpha$ and inclusion maps $i_\alpha : G_\alpha \to G_1 \times G_2$. When the G_α are commutative, so is their product. Since then

$$i_1 \,\mathrm{pr}_1 + i_2 \,\mathrm{pr}_2 = \mathrm{id}$$

the usual abstract nonsense allows to give the categorical product also the structure of a categorical sum.

Proposition 3. *The category of commutative affine group schemes forms an additive category.*

2.8. **Failure of the naive cokernel.** The naive cokernel of a map $\varphi : G \to H$ of commutative group schemes is the group functor

$$T \mapsto H(T)/\varphi(G(T))$$

The naive cokernel is rarely representable, even in situations which are far from pathological. For example, the map $n\cdot : \mathbb{G}_\mathrm{m} \to \mathbb{G}_\mathrm{m}$, which raises units to their nth power. If the element of the naive cokernel $u \in T^\times/(T^\times)^n = \mathbb{G}_\mathrm{m}(T)/n\mathbb{G}_\mathrm{m}(T)$ is nontrivial, then it becomes trivial when mapped via

$$T \hookrightarrow T' = T[V]/(V^n - u)$$

as $V \in \mathbb{G}_\mathrm{m}(T')$ is an nth root of u. If the naive cokernel functor $\mathscr{C}$ were representable, then we would have

$$\mathscr{C}(T) \hookrightarrow \mathscr{C}(T'),$$

a contradiction.

The solution to this failure comes by relaxing the notion of surjectivity by the introduction of the fpqc-topology, a Grothendieck topology on $\mathscr{A}_R$ to be discussed in Section §6.

3. Finite flat group schemes

References: [Sh86] §3, [Pk05].

3.1. **Examples of finite flat group schemes.** A **finite flat group scheme** G over R is an affine group scheme, represented by a finite flat R-algebra A. The **order of** G is the locally constant function $\#G$ with respect to the Zariski topology on $\mathrm{Spec}(R) = \{\text{prime ideals of R}\}$ given at $\mathfrak{p}$ by the rank of the free $R_\mathfrak{p}$ module $A_\mathfrak{p}$.

Here are some examples.

(1) The group μ_n is represented by $R[X]/(X^n - 1)$ with

$$\Delta(X) = X \otimes X, \quad \varepsilon(X) = 1, \quad S(X) = X^{-1}.$$

Thus μ_n is finite flat of order n. In fact, the representing algebra is even a free R-module of rank n.

(2) The constant group scheme $\underline{\mathrm{G}}$ is represented by $\prod_{g \in G} R$ and hence finite flat of order the order of G.

(3) In characteristic $p > 0$ the affine group scheme α_p is represented by $R[X]/(X^p = 0)$ with

$$\Delta(X) = X \otimes 1 + 1 \otimes X, \quad \varepsilon(X) = 0, \quad S(X) = -X.$$

Hence α_p is finite flat of order p.

(4) An **isogeny** is a group homomorphism $\varphi : G \to H$ which corresponds to a finite flat map $\varphi^* : A \to B$ of the corresponding representing R-algebras. The kernel of an isogeny is a finite flat group scheme, as $B \otimes_A R$ is finite and flat over R by the preservation of the properties finite and flat under base change.

3.2. **Cartier duality.** Let G be a finite flat group scheme over R represented by A. The R-algebra A is a commutative Hopf algebra with multiplication $\mu : A \otimes_R A \to A$, unit $\eta : R \to A$, comultiplication $\Delta : A \to A \otimes_R A$, counit $\varepsilon : A \to R$, and antipode $S : A \to A$ satisfying various compatibility conditions.

Let $A^\vee = \mathrm{Hom}_R(A, R)$ be the R-linear dual of A. Using the canonical identification $R^\vee = R$ and $(A \otimes_R A)^\vee = A^\vee \otimes_R A^\vee$ we find on the dual again the structure of a Hopf algebra over R with

$$\begin{aligned} \mu_{A^\vee} &= (\Delta_A)^\vee, \\ \eta_{A^\vee} &= (\varepsilon_A)^\vee, \\ \Delta_{A^\vee} &= (\mu_A)^\vee, \\ \varepsilon_{A^\vee} &= (\eta_A)^\vee, \\ S_{A^\vee} &= (S_A)^\vee. \end{aligned}$$

Clearly, this dual Hopf algebra is cocommutative and it is moreover commutative if and only if A was cocommutative, or what amounts to the same, G is a commutative finite flat group scheme over R.

The **Cartier dual** of a finite flat commutative group scheme G represented by A is the finite flat commutative group scheme group scheme G^D represented by the dual Hopf algebra $A^\vee$. The following is obvious from the definition.

Proposition 4. *A commutative finite flat group scheme is canonically isomorphic to its double Cartier dual. Cartier duality is a contravariant involutory autoequivalence of the category of finite flat commutative group schemes over R.*

3.2.1. *The constant group scheme revisited.* Let E be a finite set and consider the associated functor $\underline{E}_R : \mathscr{A}_R \to \mathscr{S}ets$ represented by $\prod_{e\in E} R$. For an arbitrary representable functor $h_B : \mathscr{A}_R \to \mathscr{S}ets$ we have

$$\mathrm{Hom}(\underline{E}_R, h_B) = \mathrm{Hom}_R(B, \prod_{e\in E} R) = \prod_{e\in E} \mathrm{Hom}_R(B,R) = \mathrm{Hom}_{\mathscr{S}ets}(E, h_B(R)), \tag{3.1}$$

so the covariant functor $E \mapsto \underline{E}_R$ from $\mathscr{S}ets$ to set-valued representable functors $\mathscr{A}_R \to \mathscr{S}ets$ is left-adjoint to the functor evaluation at R. Hence $E \mapsto \underline{E}_R$ preserves finite colimits. But we need products, which are luckily preserved by

$$\prod_{(e,f)\in E\times F} R = \big(\prod_{e\in E} R\big) \otimes_R \big(\prod_{f\in F} R\big). \tag{3.2}$$

For a finite group G we thus get a finite affine group scheme $\underline{G}_R$ with underlying Hopf algebra $A = \prod_{g\in G} R = \mathrm{Maps}(G,R)$. Let $e_g \in A$ denote the map which has value 1 at g and 0 elsewhere. The coproduct maps $\Delta(e_g) = \sum_{g'g''=g} e_{g'} \otimes e_{g''}$, the counit ε evaluates at $1 \in G$ and the antipode does $S(e_g) = e_{g^{-1}}$. The R-dual of A becomes the group algebra $A^\vee = \mathrm{Hom}_R(A,R) = R[G]$ with $g \in R[G]$ being the dual basis element to $e_g \in \mathrm{Maps}(G,R)$, so $g \in R[G]$ is evaluation at g on $\mathrm{Maps}(G,R)$. We have

$$\Delta(g) = g \otimes g, \quad \varepsilon(g) = 1, \quad S(g) = g^{-1}. \tag{3.3}$$

3.2.2. *Some formulas for Cartier duality.* Let G be a finite flat group scheme over R. The functor of points for the Cartier dual G^D is

$$G^D(T) = \mathrm{Hom}_T(G \otimes_R T, \mathbb{G}_{\mathrm{m},T}), \tag{3.4}$$

which means that the inner Hom

$$\mathscr{H}om(G, \mathbb{G}_{\mathrm{m}})$$

is representable by a finite flat group scheme, namely the Cartier dual. Indeed, a $g \in G^D(T)$ is an R-algebra morphism $g : A^\vee \to T$, i.e.,

$$\begin{tikzcd}
A^\vee \otimes_R A^\vee \arrow[r, "\Delta^\vee"] \arrow[d, "g\otimes g"] & A^\vee \arrow[d, "g"] \\
T \otimes_R T \arrow[r, "\mu_T"] & T,
\end{tikzcd}$$

hence an element $g \in A \otimes_R T$, such that $(\Delta \otimes \mathrm{id}_T)(g) = g \otimes_T g$ in $(A \otimes_R A) \otimes_R T$. That $g : A^\vee \to T$ respects 1 yields $g(1_{A^\vee}) = 1_T$, i.e.,

$$(\varepsilon \otimes \mathrm{id}_T)(g) = 1.$$

Moreover, $g \in A \otimes_R T$ is a unit as

$$\begin{aligned} g \cdot (S \otimes \mathrm{id}_T)(g) &= \mu \circ (\mathrm{id}_A \otimes S \otimes \mathrm{id}_T) g \otimes_T g \\ &= \mu \circ (\mathrm{id}_A \otimes S \otimes \mathrm{id}_T) \circ (\Delta \otimes \mathrm{id}_T)(g) = (\eta_A \otimes \mathrm{id}_T) \circ (\varepsilon \otimes \mathrm{id}_T)(g) = 1. \end{aligned} \tag{3.5}$$

So g can also be interpreted as a T-map

$$T[X, X^{-1}] \to A \otimes_R T$$

that sends $X \mapsto g$ and commutes with Δ and ε as the corresponding maps for $\mathbb{G}_{\mathrm{m}}$ are

$$\Delta(X) = X \otimes X, \quad \varepsilon(X) = 1,$$

and (3.4) follows.

We can write (3.4) as a functorial pairing $G(T) \times G^D(T) \to \mathbb{G}_{\mathrm{m}}(T)$, so a pairing of affine group schemes

$$G \times G^D \to \mathbb{G}_{\mathrm{m}}, \tag{3.6}$$

which is perfect by the above in the sense that the natural adjoint maps from one side into the $\mathscr{H}om$ with values in $\mathbb{G}_{\mathrm{m}}$ of the other side are isomorphisms. The achieved symmetry between G and its dual G^D shows again, that G is canonically isomorphic to its double Cartier dual. The pairing map (3.6) is given by the map

$$R[X, X^{-1}] \to A \otimes_R A^\vee$$

which sends X to the identity element $\mathrm{id}_A \in \mathrm{End}_R(A) = A \otimes_R A^\vee$.

We may want to use (3.4) applied to G^D and get a description

$$G(T) = \{g \in A^\vee \otimes_R T;\ \mu^\vee(g) = g \otimes_T g,\ \eta^\vee(g) = 1\}. \tag{3.7}$$

Here $G(T)$ lies even in the units of $A^\vee \otimes_R T$ by (3.5) and the map $G(T) \to A^\vee \otimes_R T$ is a group homomorphism.

$$g \cdot h = \mu(g \otimes h)\Delta : A \to T$$

corresponds exactly to the product in $A^\vee \otimes T$ of the corresponding elements $g, h \in A^\vee \otimes_R T$.

3.2.3. *Examples for Cartier duality.* We compute the Cartier dual for the three typical examples of order p.

(1) The Cartier dual of the constant group scheme $G = \underline{\mathbb{Z}/n\mathbb{Z}}_R$ is $\mu_{n,R}$, because in

$$G^D = \mathscr{H}om(\underline{\mathbb{Z}/n\mathbb{Z}}_R, \mathbb{G}_{\mathrm{m}})$$

the image of $1 \in \underline{\mathbb{Z}/n\mathbb{Z}}_R$ is mapped to an nth root of unity. In terms of algebras, we have that G^D is given by the group algebra $R[\mathbb{Z}/n\mathbb{Z}] = R[X]/(X^n - 1)$ and comultiplication, counit and antipode

$$\Delta(X) = X \otimes X, \quad \varepsilon(X) = 1, \quad S(X) = X^{n-1}.$$

This Hopf algebra represents $\mu_{n,R}$.

(2) It follows that the Cartier dual of $\mu_{n,R}$ is $\underline{\mathbb{Z}/n\mathbb{Z}}_R$.

(3) The Cartier dual of α_p is α_p. Namely, α_p is represented by $R[X]/(X^p = 0)$ with

$$\Delta(X) = X \otimes 1 + 1 \otimes X, \quad \varepsilon(X) = 0, \quad S(X) = -X.$$

The dual algebra has a basis Y_i dual to the basis X^i for $0 \le i < p$. The multiplication is given by

$$Y_i \cdot Y_j = \sum_{k=0}^{p-1} \Delta^\vee(Y_i \otimes Y_j)(X^k) Y_k = \sum_{k=0}^{p-1} Y_i \otimes Y_j\big(\Delta(X^k)\big) Y_k$$

$$= \sum_{k=0}^{p-1} Y_i \otimes Y_j \left(\sum_{a+b=k} \binom{k}{a} X^a \otimes X^b \right) Y_k = \begin{cases} \binom{i+j}{i} Y_{i+j} & \text{if } i+j < p, \\ 0 & \text{else.} \end{cases}$$

Consequently, with $Y = Y_1$ we have $A^\vee = R[Y]/(Y^p = 0)$. Moreover,

$$\Delta(Y) = \sum_{a,b} \mu^\vee(Y)(X^a \otimes X^b) Y_a \otimes Y_b = \sum_{a,b} Y(X^{a+b}) Y_a \otimes Y_b = Y \otimes 1 + 1 \otimes Y,$$

$$\varepsilon(Y) = \eta^\vee(Y) = Y(1) = 0,$$

$$S(Y) = \sum_{i=0}^{p-1} S^\vee(Y)(X^i) Y_i = Y\big(S(X)\big) Y = Y(-X)Y = -Y,$$

and indeed, the Cartier dual of α_p is again α_p. The pairing map $\alpha_p \times \alpha_p \to \mathbb{G}_{\mathrm{m}}$ is given by the truncated exponential, not a surprise as we map an additive group into a multiplicative group, namely

$$R[U, U^{-1}] \to R[X]/(X^p) \otimes_R R[Y]/(Y^p)$$

$$U \mapsto \exp(X \otimes Y) = \sum_{a=0}^{p-1} \frac{1}{a!} X^a \otimes Y^a$$

because the dual to X^a is $Y_a = \frac{1}{a!} Y^a$.

Corollary 5. *For a ring R with $p \cdot R = 0$ the group schemes $\underline{\mathbb{Z}/p\mathbb{Z}}_R$, $\mu_{p,R}$ and $\alpha_{p,R}$ are mutually non-isomorphic.*

Proof: We may take a fibre in a point and replace R by a field of characteristic p. Then if G is one of $\underline{\mathbb{Z}/p\mathbb{Z}}$, μ_p or α_p and G^D its Cartier dual, then

$$\begin{aligned} G = \underline{\mathbb{Z}/p\mathbb{Z}} \quad & \text{if} \quad G \text{ is reduced and } G^D \text{ non-reduced}, \\ G = \mu_p \quad & \text{if} \quad G^D \text{ is reduced and } G \text{ non-reduced}, \\ G = \alpha_p \quad & \text{if} \quad G \text{ and } G^D \text{ are non-reduced}. \end{aligned}$$

□

3.3. The order kills the group [after Deligne].

Theorem 6. *Let G be a finite flat commutative group scheme over R of order n. Then n kills G, i.e., the multiplication by n map $n\cdot : G \to G$ is the zero map.*

We present the proof found by Deligne, see [OT70] §1, apparently in the bus on his way to service in the Belgian army.

3.3.1. *The norm map.* Let $B \to C$ be a finite flat map of constant rank. The **norm map** $N : C \to B$ is the multiplicative map given by sending $c \in C$ to the determinant $N(c) = \det_B(\lambda_c)$ relative B of the left multiplication by c on C as a B-module. This definition makes sense, whenever C is in fact a free B-module of finite rank, which locally on B is the case. The local norms obtained in such a way glue to define the global norm. Alternative: the B-module endomorphism $\lambda_c : C \to C$ induces an endomorphism $\det_B(\lambda_c) : \det_B C \to \det_B C$, but $\det_B C$ is an invertible B-module and thus has only the scalars B as endomorphisms. This again defines the norm.

3.3.2. *The trace map.* Let G be a finite flat commutative group scheme over R represented by A, and let $f : B \to C$ be a finite flat map of constant rank of R-algebras. The diagram

$$\begin{tikzcd} G(C) \arrow[r, hook] \arrow[d, dashed, "\mathrm{tr}_f"] & A^\vee \otimes_R C \arrow[d, "N"] \\ G(B) \arrow[r, hook] & A^\vee \otimes_R B \end{tikzcd} \tag{3.8}$$

defines a unique trace map homomorphism

$$\mathrm{tr}_f : G(C) \to G(B). \tag{3.9}$$

Indeed, we calculate

$$\begin{aligned} \mu^\vee(N(g)) &= \mu^\vee\big(\det_{A^\vee \otimes_R B}(g\cdot : A^\vee \otimes_R C \to A^\vee \otimes_R C)\big) \\ &= \det_{A^\vee \otimes A^\vee \otimes_R B}(\mu^\vee(g)\cdot : A^\vee \otimes A^\vee \otimes_R C \to A^\vee \otimes A^\vee \otimes_R C) \\ &= \det_{A^\vee \otimes A^\vee \otimes_R B}(g \otimes_C g\cdot : A^\vee \otimes A^\vee \otimes_R C \to A^\vee \otimes A^\vee \otimes_R C) \\ &= \big(\det_{A^\vee \otimes_R B}(g\cdot : A^\vee \otimes_R C \to A^\vee \otimes_R C)\big) \otimes_B \big(\det_{A^\vee \otimes_R B}(g\cdot : A^\vee \otimes_R C \to A^\vee \otimes_R C)\big) \\ &= N(g) \otimes_B N(g) \end{aligned}$$

and

$$\begin{aligned}
\eta^\vee(N(g)) &= \eta^\vee\big(\det_{A^\vee\otimes_R B}(g\cdot : A^\vee\otimes_R C \to A^\vee\otimes_R C)\big)\\
&= \det_B(\eta^\vee(g)\cdot : C\to C)\\
&= \det_B(1\cdot : C\to C) \quad = \quad 1
\end{aligned}$$

It follows directly from the definition that the composition

$$G(B) \xrightarrow{f} G(C) \xrightarrow{\mathrm{tr}_f} G(B) \tag{3.10}$$

is multiplication by the rank of C as a B-module:

$$\mathrm{tr}_f(f(u)) = u^{\mathrm{rk}(C/B)} \tag{3.11}$$

for $u\in G(B)$. Furthermore, if we compose with a B-automorphism $\gamma : C\to C$, then the trace does not change: for $u\in G(C)$

$$\mathrm{tr}_f(\gamma(u)) = \mathrm{tr}_f(u), \tag{3.12}$$

because left multiplication by u and by $\gamma(u) = (1\otimes\gamma)(u)$ are conjugate to each other by means of $1\otimes\gamma$:

(3.13)
$$\begin{tikzcd}
A^\vee\otimes_R C \arrow[r, "u\cdot"] \arrow[d, "1\otimes\gamma"] & A^\vee\otimes_R C \arrow[d, "1\otimes\gamma"]\\
A^\vee\otimes_R C \arrow[r, "\gamma(u)\cdot"] & A^\vee\otimes_R C
\end{tikzcd}$$

3.3.3. *The proof.* The proof of Theorem 6 is now fairly easy. Let n be the order of G. We take $f : B\to C$ to be $\eta : R\to A$ and pick $u\in G(R)$ arbitrary. The universal element g_{univ} is $\mathrm{id}_A\in G(A)$. The R-automorphism left translation by u

$$\lambda_u : A \xrightarrow{\Delta} A\otimes_R A \xrightarrow{u\otimes\mathrm{id}} A \tag{3.14}$$

equals

$$\eta(u)\cdot g_{\mathrm{univ}} : A \xrightarrow{\Delta} A\otimes_R A \xrightarrow{(\eta\circ u)\otimes\mathrm{id}} A\otimes_R A \xrightarrow{\mu} A, \tag{3.15}$$

hence in $G(R)$ we have

$$u^n\cdot\mathrm{tr}_\eta(g_{\mathrm{univ}}) = \mathrm{tr}_\eta(\eta(u))\cdot\mathrm{tr}_\eta(g_{\mathrm{univ}}) = \mathrm{tr}_\eta(\eta(u)\cdot g_{\mathrm{univ}}) = \mathrm{tr}_\eta(\lambda_u(g_{\mathrm{univ}})) = \mathrm{tr}_\eta(g_{\mathrm{univ}}) \tag{3.16}$$

and cancelling $\mathrm{tr}_\eta(g_{\mathrm{univ}})$ yields

$$u^n = 1.$$

As the order is preserved under base change we can argue in exactly the same manner for the base change of G to A and the special choice of

$$u = g_{\mathrm{univ}} \in G\otimes_R A(A)$$

which shows that

$$g_{\mathrm{univ}}^n = 1$$

in $G(A) = G\otimes_R A(A)$. And we are done, as it is clearly sufficient to show that the universal element is killed by the order of the group.

Remark 7. The result of Theorem 6 is conjectured in SGA 3 to hold also for non-commutative finite flat groups. This is known over a reduced base from the case of fields. The best known result over a general base is due to Schoof and can be found in [Sc01].

4. Grothendieck topologies

References: [Tm94].

4.1. Sheaves for Grothendieck topologies.

4.1.1. *Grothendieck topology.* A **Grothendieck topology** on a category $\mathscr{C}$, that for simplicity we assume has a final object and fibre products, is a collection of **coverings** Cov_X for each object $X \in \mathscr{C}$, i.e., a collection of families of maps

$$\{j_\alpha : U_\alpha \to X;\ \alpha \in A\}$$

from $\mathscr{C}$ subject to the following list of axioms.

Intersection: If $Y \to X$ is a map in $\mathscr{C}$ and $\{j_\alpha : U_\alpha \to X;\ \alpha \in A\}$ a covering of X, then the family of fibre products $\{j_\alpha \times \mathrm{id} : U_\alpha \times_X Y \to Y;\ \alpha \in A\}$ is a covering of Y.

Composition: If $\{j_\alpha : U_\alpha \to X;\ \alpha \in A\}$ is a covering of X and for each $\alpha \in A$ we have coverings $\{j_{\alpha,i} : U_{\alpha,i} \to U_\alpha;\ i \in I_\alpha\}$ then the composites

$$\{j_\alpha \circ j_{\alpha,i} : U_{\alpha,i} \to X;\ \alpha \in A, i \in I_\alpha\}$$

form again a covering of X.

Isomorphism: The family $\{j : X' \to X\}$ consisting of just one isomorphism is a covering.

For the basic example take a topological space X and form the category Off_X of all open subsets with only inclusions as morphisms. A covering is a collection of inclusions $j_\alpha : U_\alpha \to V$ of opens such that the union $\bigcup_\alpha U_\alpha$ equals V. The axioms are modelled on this example and preserve everything what is necessary for a good theory of sheaves.

4.1.2. *Presheaves.* The category of **presheaves** $\mathrm{PShv}(\mathscr{C}, \mathscr{S}ets)$ with values in sets on a category $\mathscr{C}$ is the category of contravariant functors $\mathscr{F} : \mathscr{C} \to \mathscr{S}ets$ with values in sets.

The category of **presheaves** $\mathrm{PShv}(\mathscr{C})$ with values in abelian groups on a category $\mathscr{C}$ is the category of contravariant functors $\mathscr{F} : \mathscr{C} \to \mathscr{A}b$ with values in abelian groups.

Variants with other target categories are evident. If the target category is abelian, then the category of presheaves is abelian as well: kernel and cokernel as presheaves are determined 'pointwise', namely for a map $\varphi : \mathscr{F} \to \mathscr{G}$ of presheaves we have

$$\ker(\varphi)(U) = \ker\big(\varphi_U : \mathscr{F}(U) \to \mathscr{G}(U)\big),$$
$$\mathrm{coker}(\varphi)(U) = \mathrm{coker}\big(\varphi_U : \mathscr{F}(U) \to \mathscr{G}(U)\big).$$

4.1.3. *Sheaves.* Let $\mathscr{C}$ be a category equipped with a Grothendieck topology $\mathscr{T}$. For a covering $\{j_\alpha : U_\alpha \to U;\ \alpha \in A\}$ of $\mathscr{T}$ and a presheaf $\mathscr{F}$ on $\mathscr{C}$ we may look at the diagram

$$\mathscr{F}(U) \xrightarrow{\mathscr{F}(j_\alpha)} \prod_\alpha \mathscr{F}(U_\alpha) \underset{\mathscr{F}(\mathrm{pr}_2)}{\overset{\mathscr{F}(\mathrm{pr}_1)}{\rightrightarrows}} \prod_{\alpha,\beta} \mathscr{F}(U_\alpha \times_U U_\beta), \tag{4.1}$$

which encodes the **sheaf property** with respect to the chosen covering. We say that $\mathscr{F}$ satisfies the sheaf property for $\{j_\alpha : U_\alpha \to U;\ \alpha \in A\}$ if (4.1) is **exact** in the sense that $\mathscr{F}(U)$ via $\mathscr{F}(j_\alpha)$ is identified with the coequalizer of the two maps denoted $\mathscr{F}(\mathrm{pr}_1)$ and $\mathscr{F}(\mathrm{pr}_2)$. For presheaves with values in abelian groups (or abelian categories) this amounts to

$$0 \to \mathscr{F}(U) \xrightarrow{\mathscr{F}(j_\alpha)} \prod_\alpha \mathscr{F}(U_\alpha) \xrightarrow{\mathscr{F}(\mathrm{pr}_1) - \mathscr{F}(\mathrm{pr}_2)} \prod_{\alpha,\beta} \mathscr{F}(U_\alpha \times_U U_\beta) \tag{4.2}$$

being an exact sequence. The category of **sheaves** $\mathrm{Shv}(\mathscr{C}_\mathscr{T}, \mathscr{S}ets)$ with values in sets (resp. $\mathrm{Shv}(\mathscr{C}_\mathscr{T})$ with values in abelian groups) on a category $\mathscr{C}$ with respect to a Grothendieck topology $\mathscr{T}$ is the full subcategory of those presheaves $\mathscr{F} \in \mathrm{PShv}(\mathscr{C}, \mathscr{S}ets)$ with values in sets (resp. presheaves $\mathscr{F} \in \mathrm{PShv}(\mathscr{C})$ with values in abelian groups) on $\mathscr{C}$ such that for all coverings in $\mathscr{T}$ the sheaf property holds for $\mathscr{F}$.

4.2. **Čech-cohomology.** Let X be an object of a category $\mathscr{C}$ endowed with a Grothendieck topology $\mathscr{T}$ and family of coverings Cov_X. A **refinement** of a covering $\{j_\alpha : U_\alpha \to X;\ \alpha \in A\}$ by a covering $\{j_\beta : V_\beta \to X;\ \beta \in B\}$ consists of a map $\varphi : B \to A$ and maps $\varphi_\beta : V_\beta \to U_{\varphi(\beta)}$ compatible with the maps $j_\beta, j_{\varphi(\beta)}$ to X. The notion of refinement makes Cov_X a category.

The functor 0-th Čech-cohomology on the category of presheaves on $\mathscr{C}$ with values in abelian groups is defined as

$$\check{H}^0(X,\mathscr{F}) = \varinjlim_{\mathrm{Cov}_X} \ker\left(\prod_\alpha \mathscr{F}(U_\alpha) \xrightarrow{\mathscr{F}(\mathrm{pr}_1)-\mathscr{F}(\mathrm{pr}_2)} \prod_{\alpha,\beta} \mathscr{F}(U_\alpha \times_X U_\beta)\right)$$

Note that the functor depends on the topology $\mathscr{T}$ without being mentioned in the notation. The transfer map $\mathscr{F}(\varphi)$ along a refinement φ with notation as above is induced by the commutative diagram

$$\begin{tikzcd}
\prod_\alpha \mathscr{F}(U_\alpha) \arrow[r, "\mathscr{F}(\mathrm{pr}_1)-\mathscr{F}(\mathrm{pr}_2)"] \arrow[d, "\mathscr{F}(\varphi_\beta)"] & \prod_{\alpha_1,\alpha_2} \mathscr{F}(U_{\alpha_1} \times_X U_{\alpha_2}) \arrow[d, "\mathscr{F}(\varphi_{\beta_1}\times\varphi_{\beta_2})"] \\
\prod_\alpha \mathscr{F}(V_\beta) \arrow[r, "\mathscr{F}(\mathrm{pr}_1)-\mathscr{F}(\mathrm{pr}_2)"] & \prod_{\beta_1,\beta_2} \mathscr{F}(V_{\beta_1} \times_X V_{\beta_2}).
\end{tikzcd}$$

Proposition 8. *The functor* $\check{\mathrm{H}}^0(X,-) : \mathrm{PShv}(\mathscr{C}) \to \mathscr{A}b$ *is left exact.*

Proof: The only problem comes from the fact that the index category Cov_X of coverings with refinement is not filtered and thus the left exactness of the functors $\varinjlim_{\mathrm{Cov}_X}$ is obscured.

Let φ, ψ be two refinements from the covering $\{j_\alpha : U_\alpha \to X;\ \alpha \in A\}$ to the covering $\{j_\beta : V_\beta \to X;\ \beta \in B\}$. For (s_α) from

$$\ker\left(\prod_\alpha \mathscr{F}(U_\alpha) \xrightarrow{\mathscr{F}(\mathrm{pr}_1)-\mathscr{F}(\mathrm{pr}_2)} \prod_{\alpha,\beta} \mathscr{F}(U_\alpha \times_X U_\beta)\right)$$

we compute the difference of the β component of the induced transfer maps as

$$\mathscr{F}(\varphi)\big(s_\alpha)\big)_\beta - \mathscr{F}(\psi)\big(s_\alpha)\big)_\beta = \mathscr{F}(\varphi_\beta)(s_{\varphi(\beta)}) - \mathscr{F}(\psi_\beta)(s_{\psi(\beta)})$$

$$= \mathscr{F}(\varphi_\beta,\psi_\beta)\left(\mathscr{F}(\mathrm{pr}_1) - \mathscr{F}(\mathrm{pr}_2)\right)\big(s_\alpha)\big) = 0$$

via the detour of $\mathscr{F}(U_{\varphi(\beta)} \times_X U_{\psi(\beta)})$. Consequently, any two refinements between the same coverings define the same transfer map.

Therefore, the limit $\varinjlim_{\mathrm{Cov}_X}$ can be computed as a limit over the filtered category of Cov_X with unique map whenever there exist a refinement. As two coverings have a common refinement by exploiting the fibre product, the new category is clearly filtered. We conclude that the $\varinjlim_{\mathrm{Cov}_X}$ from the definition of $\check{\mathrm{H}}^0(X,-)$ is indeed exact which proves the proposition. □

For $X \in \mathscr{C}$ and an abelian group A we define the presheaf $\underline{A}_U$ by

$$\underline{A}_U(V) = \prod_{\mathrm{Hom}_{\mathscr{C}}(U,V)} A.$$

The functor $A \mapsto \underline{A}_U$ is right adjoint

(4.3) $$\mathrm{Hom}_{\mathscr{A}b}(\mathscr{F}(U), A) = \mathrm{Hom}_{\mathrm{PShv}(\mathscr{C})}(\mathscr{F}, \underline{A}_U)$$

$$(\varphi : \mathscr{F}(U) \to A) \longmapsto \left(\mathscr{F}(V) \xrightarrow{\varphi \circ \mathscr{F}(j)} \prod_{j \in \mathrm{Hom}_{\mathscr{C}}(U,V)} A \right)_V$$

to the exact functor of evaluating at U, hence preserves injective objects.

Proposition 9. *The category* $\mathrm{PShv}(\mathscr{C})$ *has enough injective objects.*

Proof: The category of abelian groups has enough injective objects. We choose for each $U \in \mathscr{C}$ an injection $\mathscr{F}(U) \hookrightarrow I(U)$ into an injective abelian group. The adjointness of (4.3) defines a map

$$\mathscr{F} \to \mathscr{I} := \prod_U \underline{I(U)}_U$$

which is clearly injective. The presheaf $\mathscr{I}$ is injective by the above adjointness and the fact that being injective is inherited in arbitrary products. □

We may thus derive the functor $\check{\mathrm{H}}^0(X, -)$. The higher derived functors are denoted by $\check{\mathrm{H}}^i(X, -)$ and form the cohomological δ-functor of Čech-cohomology of presheaves with values in abelian groups.

4.2.1. *Sheafification.* We sheafify $\check{\mathrm{H}}^0(X, -)$ to the functor $\check{\mathscr{H}}^0 : \mathrm{PShv} \to \mathrm{PShv}$ of **sheafified 0-th Čech-cohomology** by

$$\check{\mathscr{H}}^0(\mathscr{F})(U) := \check{\mathrm{H}}^0(U, \mathscr{F})$$

with restriction maps induced from the restriction maps of $\mathscr{F}$. If $\mathscr{F}$ is a sheaf, then the natural map $\mathscr{F} \to \check{\mathscr{H}}^0(\mathscr{F})$ is an isomorphism.

A **separated** presheaf is a sheaf such that for every covering $\{j_\alpha : U_\alpha \to U;\ \alpha \in A\}$ the map

$$\mathscr{F}(U) \xrightarrow{\mathscr{F}(j_\alpha)} \prod_\alpha \mathscr{F}(U_\alpha)$$

is injective.

Lemma 10. *(1) Let $\mathscr{F}$ be a presheaf. Then $\check{\mathscr{H}}^0(\mathscr{F})$ is a separated presheaf.*

(2) Let $\mathscr{F}$ be a separated presheaf. Then $\check{\mathscr{H}}^0(\mathscr{F})$ is a sheaf.

Proof: (1) Let

$$\{j_\alpha : U_\alpha \to U;\ \alpha \in A\}$$

be a covering, and let

$$s \in \check{\mathscr{H}}^0(\mathscr{F})(U) = \check{\mathrm{H}}^0(U, \mathscr{F})$$

map to 0 in

$$\prod_\alpha \check{\mathscr{H}}^0(\mathscr{F})(U_\alpha) = \prod_\alpha \check{\mathrm{H}}^0(U_\alpha, \mathscr{F}).$$

This means that each U_α has a covering

$$\{j_{\alpha,i} : U_{\alpha,i} \to U_\alpha;\ i \in I_\alpha\},$$

such that s restricts to 0 in each $\mathscr{F}(U_{\alpha,i})$. The composed covering

$$\{j_\alpha \circ j_{\alpha,i} : U_{\alpha,i} \to U;\ \alpha \in A, i \in I_\alpha\}$$

is therefore fine enough to kill s in the limit that defines $\check{\mathrm{H}}^0(U, \mathscr{F})$. Hence s vanishes itself proving part (1).

For (2) we only have to prove exactness in the middle of (4.2), as (1) describes exactness on the left. Let $s_\alpha \in \check{\mathrm{H}}^0(U_\alpha, \mathscr{F})$ be a compatible family of sections given through $s_{\alpha,i} \in \mathscr{F}(U_{\alpha,i})$ for coverings $\{j_{\alpha,i} : U_{\alpha,i} \to U_\alpha;\ i \in I_\alpha\}$. Being compatible means that the images of $\mathscr{F}(\mathrm{pr}_1)(s_{\alpha_1,i_1})$ and $\mathscr{F}(\mathrm{pr}_2)(s_{\alpha_2,i_2})$ agree in $\check{\mathrm{H}}^0(U_{\alpha_1,i_1} \times_U U_{\alpha_2,i_2}, \mathscr{F})$, and thus, by $\mathscr{F}$ being separated, already in $\mathscr{F}(U_{\alpha_1,i_1} \times_U U_{\alpha_2,i_2})$. The datum of all $s_{\alpha,i}$ forms a compatible collection of sections for the composite covering

$$\{j_\alpha \circ j_{\alpha,i} : U_{\alpha,i} \to U;\ \alpha \in A, i \in I_\alpha\}$$

and thus an element s in $\check{\mathrm{H}}^0(U, \mathscr{F})$. The element s restricts to s_α. Indeed, this can be checked by restricting to the covering $\{j_{\alpha,i} : U_{\alpha,i} \to U_\alpha;\ i \in I_\alpha\}$, because $\mathscr{F}$ is separated. This shows the sheaf property for $\check{\mathscr{H}}^0(\mathscr{F})$. □

Theorem 11. *(1) The functor sheafification*

$$(-)^\# : \mathrm{PShv}(\mathscr{C}) \to \mathrm{Shv}(\mathscr{C}_\mathscr{T})$$

defined by

$$\mathscr{F}^\# = \check{\mathscr{H}}^0(\check{\mathscr{H}}^0(\mathscr{F}))$$

is a left adjoint for the inclusion functor $i : \mathrm{Shv}(\mathscr{C}_\mathscr{T}) \to \mathrm{PShv}(\mathscr{C})$, and $(i(\mathscr{F}))^\# = \mathscr{F}$ canonically for each sheaf $\mathscr{F}$.

(2) The category $\mathrm{Shv}(\mathscr{C}_\mathscr{T})$ is an abelian category.

(3) The functor sheafification $\mathscr{F} \mapsto \mathscr{F}^\#$ is exact.

(4) The category $\mathrm{Shv}(\mathscr{C}_\mathscr{T})$ has enough injective objects.

Proof: (1) By Lemma 10, the functor $(-)^\#$ is well defined. For a presheaf $\mathscr{F}$ the natural map

$$\mathscr{F} \to \check{\mathscr{H}}^0(\mathscr{F}) \to \check{\mathscr{H}}^0(\check{\mathscr{H}}^0(\mathscr{F})) = \mathscr{F}^\#$$

defines for a sheaf $\mathscr{G}$ a natural bijection

$$\mathrm{Hom}_{\mathrm{Shv}(\mathscr{C}_\mathscr{T})}(\mathscr{F}^\#, \mathscr{G}) = \mathrm{Hom}_{\mathrm{PShv}(\mathscr{C})}(\mathscr{F}, \mathscr{G}).$$

(2) The presheaf kernel of a map of sheaves $\varphi : \mathscr{F} \to \mathscr{G}$ is already a sheaf and thus satisfies the property of a kernel also for the subcategory of sheaves. The cokernel is given by

$$\mathrm{coker}(\varphi) = (U \mapsto \mathscr{G}(U)/\mathscr{F}(U))^\#$$

the sheafification of the presheaf cokernel, as can be seen by the adjointness in (1). The map

$$f : \mathrm{coim}(\varphi) \to \mathrm{im}(\varphi)$$

has trivial kernel and cokernel. Hence for each $U \in \mathscr{C}$ the map

$$f(U) : \mathrm{coim}(\varphi)(U) \to \mathrm{im}(\varphi)(U)$$

is injective.

We will now show that $f(U)$ is even bijective. For $s \in \mathrm{im}(\varphi)(U)$ there is a covering

$$\{j_\alpha : U_\alpha \to U;\ \alpha \in A\},$$

such that the restrictions $s_\alpha = \mathscr{G}(j_\alpha)(s)$ lift to

$$t_\alpha \in \mathrm{coim}(\varphi)(U_\alpha).$$

The various t_α are compatible, because the difference of restrictions of the t_α's being 0 can be checked after applying the injective map f, hence it follows from the compatibility of the s_α's. Therefore the sections t_α glue to an element $t \in \mathrm{coim}(\varphi)(U)$ which maps to s because it does so after restriction to the given covering. Hence the map $\mathrm{coim}(\varphi) \to \mathrm{im}(\varphi)$ is an isomorphims.

(3) As a left adjoint functor, sheafification is right exact. That $(-)^\#$ preserves kernels is the content of Proposition 8.

(4) The existence of enough injective objects follows from delicate set-theoretic considerations relying on three properties that the abelian category $\mathrm{Shv}(\mathscr{C}_\mathscr{T})$ has: existence of arbitrary direct sums over arbitrary index sets (AB3), direct limits of filtered direct systems of subobjects exist and are subobjects again (AB5), and the existence of a (set of) generators, see [Gr57] I.1.10. □

5. fpqc SHEAVES

We now turn our attention towards the relevant example of a Grothendieck topology for the theory of finite flat group schemes.

5.1. **fpqc topology.** We work on the category Aff_R of affine R-schemes which for us by definition is the opposite category $\mathscr{A}_R^{\mathrm{opp}}$ to the category of R-algebras. Our group functors on $\mathscr{A}_R$ have thus become presheaves with values in $\mathscr{G}rps$ on Aff_R.

An **fpqc (fidèlement plat quasi-compact)** covering of an R-algebra T is given by a finite family $j_i : T \to T_i$ for $i \in I$ with T_i being a flat T-algebra via j_i for all $i \in I$ and such that a T-module M vanishes if and only if $M_i = M \otimes_T T_i$ vanishes for all $i \in I$. The latter is equivalent to the map $\coprod_i \mathrm{Spec}(T_i) \to \mathrm{Spec}(T)$ being faithfully flat, or equivalently flat and surjective.

The category Aff_R together with fpqc coverings forms a Grothendieck topology, because flatness and surjectivity are preserved by fibre products and composition. We denote the category of sheaves on Aff_R with respect to the fpqc topology by

$$\mathrm{Shv}(R_{\mathrm{fpqc}}).$$

5.2. **Representable presheaves are sheaves.** Let $\mathscr{F} = \mathrm{Hom}_R(A,-)$ be a representable presheaf. As $\mathscr{F}(\prod_i T_i) = \prod_i \mathscr{F}(T_i)$ we may replace each covering as above by the covering $T \to T' = \prod_i T_i$ which has only one index, but still describe the same sheaf property for representable presheaves.

Theorem 12. *Representable presheaves in* $\mathrm{PShv}(\mathrm{Aff}_R, \mathscr{S}ets)$ *are sheaves with respect to the fpqc topology.*

Proof: Let $\mathscr{F} = \mathrm{Hom}_R(A,-)$ be a representable presheaf. The sheaf property is equivalent to the exactness in $\mathscr{S}ets$ of

$$\mathrm{Hom}_R(A,T) \longrightarrow \mathrm{Hom}_R(A,T') \overset{\mathrm{pr}_1}{\underset{\mathrm{pr}_2}{\rightrightarrows}} \mathrm{Hom}_R(A, T' \otimes_T T') \tag{5.1}$$

for each fpqc covering $T \to T'$. This follows from the exactness of the Amitsur complex in low degrees as explained in Proposition 13 below. □

Let B be an A-algebra. The Amitsur complex of $A \to B$ is

$$0 \to A \to B \to B \otimes_A B \to \ldots \underbrace{B \otimes_A \ldots \otimes_A B}_{q+1} \xrightarrow{\partial} \underbrace{B \otimes_A \ldots \otimes_A B}_{q+2} \ldots$$

with

$$\partial(b_0 \otimes \ldots \otimes b_q) = \sum_{i=0}^{q+1} (-1)^i b_0 \otimes \ldots \otimes b_{i-1} \otimes 1 \otimes b_i \otimes \ldots \otimes b_q.$$

Proposition 13. *The Amitsur complex for a faithfully flat map $A \to B$ is exact.*

Proof: Exactness may be checked after a faithfully flat base change. If we base change by $A \to B$ itself we encounter that $B \to B \otimes_A B$ admits a retraction $B \otimes_A B \to B$ via multiplication. So we have reduced to the case where $A \to B$ has a retraction $r : B \to A$ to begin with.

The retraction allows us to write down the following homotopy

$$r_q : \underbrace{B \otimes_A \ldots \otimes_A B}_{q+1} \to \underbrace{B \otimes_A \ldots \otimes_A B}_{q}$$

$$r_q(b_0 \otimes \ldots \otimes b_q) = r(b_0) \otimes b_1 \otimes \ldots \otimes b_q$$

and we compute

$$r_{q+1}\partial + \partial r_q = \mathrm{id}$$

so that the identity is null-homotopic, hence the complex is acyclic. □

5.3. **Embedding of affine group schemes in fpqc sheaves.** The obvious embedding of the category of affine group schemes over R to the category of fpqc sheaves on R with values in abelian groups is compatible with kernel, sums and is fully faithful. This gives us the opportunity to define a reasonable cokernel, namely the sheaf cokernel in $\mathrm{Shv}(R_{\mathrm{fpqc}})$. The natural question arises: Is this fpqc sheaf cokernel representable? In this case the representing object would also be a cokernel in the category of affine group schemes over R.

5.4. **fpqc descent.** References: [SGA1] Exp VI.

Theorem 14. *A sheaf $\mathscr{F} \in \mathrm{Shv}(R_{\mathrm{fpqc}}, \mathscr{S}ets)$ which is representable locally in the fpqc topology is representable.*

Proof: Let $R \to R'$ be fpqc such that $\mathscr{F}|_{R'}$ as a sheaf in $\mathrm{Shv}(R'_{\mathrm{fpqc}}, \mathscr{S}ets)$ is representable by an R'-algebra B together with the universal element $b \in \mathscr{F}(B)$. For each fpqc map $f : R' \to S$ the restriction $\mathscr{F}|_S$ is then represented by $B \otimes_{R'} S$ and the universal element

$$(\mathrm{id}_B \otimes f)(b) \in \mathscr{F}(B \otimes_{R'} S).$$

Let $R'' = R' \otimes_R R'$ with inclusions $\mathrm{pr}_i : R' \to R''$, dito $R''' = R' \otimes_R R' \otimes_R R'$ with inclusions $\mathrm{pr}_i : R' \to R'''$ and $\mathrm{pr}_{ij} : R'' \to R'''$. The restriction $\mathscr{F}|_{R''}$ via pr_i is represented by $C_i = B \otimes_{R',\mathrm{pr}_i} R''$ and a universal element

$$c_i = (\mathrm{id}_B \otimes \mathrm{pr}_i)(b) \in \mathscr{F}(C_i).$$

We get R'' isomorphisms

$$h_{C_2} \xrightarrow{c_2} \mathscr{F}|_{R''} \xleftarrow{c_1} h_{C_1},$$

which yields an isomorphism

$$\varphi = (c_2)^{-1} \circ c_1 : C_2 \to C_1.$$

Let φ_{ij} be the base change

$$\mathrm{pr}_{ij}(\varphi) : B \otimes_{R',\mathrm{pr}_j} R''' = C_2 \otimes_{R'',\mathrm{pr}_{ij}} R''' \to C_1 \otimes_{R'',\mathrm{pr}_{ij}} R''' = B \otimes_{R',\mathrm{pr}_i} R'''.$$

It satisfies the cocycle condition

$$\varphi_{12} \circ \varphi_{23} = \varphi_{13}$$

which is short for the following correct commutative diagram.

(5.2)
$$\begin{tikzcd}
 & h_{C_1 \otimes_{R'',\mathrm{pr}_{23}} R'''} \arrow[dl, "\circ\varphi_{23}"'] \arrow[drr, "c_1"] & = & h_{B \otimes_{R',\mathrm{pr}_2} R'''} \arrow[d, "b"] & = & h_{C_2 \otimes_{R'',\mathrm{pr}_{12}} R'''} \arrow[dll, "c_2"'] & \\
h_{C_2 \otimes_{R'',\mathrm{pr}_{23}} R'''} \arrow[rrr, "c_2"] \arrow[dd, equal] & & & \mathscr{F}|_{R'''} & & & h_{C_1 \otimes_{R'',\mathrm{pr}_{12}} R'''} \arrow[lll, "c_1"'] \arrow[ul, "\circ\varphi_{12}"'] \arrow[dd, equal] \\
 & & & & & & \\
h_{B \otimes_{R',\mathrm{pr}_3} R'''} \arrow[uurrr, "b"] & = & h_{C_2 \otimes_{R'',\mathrm{pr}_{13}} R'''} \arrow[uur, "c_2"'] & & h_{C_1 \otimes_{R'',\mathrm{pr}_{13}} R'''} \arrow[ll, "\circ\varphi_{13}"] \arrow[uul, "c_1"] & = & h_{B \otimes_{R',\mathrm{pr}_1} R'''} \arrow[uulll, "b"']
\end{tikzcd}$$

The pair (B, φ) which satisfies the cocycle condition (5.2) is called a descent datum for algebras relative $R \to R'$. From Theorem 15 below we conclude that there is an R-algebra A with $B = A \otimes_R R'$ and $\varphi = \mathrm{id}_A \otimes \mathrm{id}_{R''}$. So $A \to B$ is fpqc and the sheaf property gives us an exact sequence of sets

$$\begin{tikzcd}
\mathscr{F}(A) \arrow[r] & \mathscr{F}(B) \arrow[r, shift left, "\mathrm{pr}_1^*"] \arrow[r, shift right, "\mathrm{pr}_2^*"'] & \mathscr{F}(A \otimes_R R'').
\end{tikzcd}$$

As $b \in \mathscr{F}(B)$ maps to

$$\mathscr{F}(\mathrm{pr}_1)(b) = c_1 = c_2 \circ \varphi = c_2 = \mathscr{F}(\mathrm{pr}_2)(b),$$

the element b descends uniquely to an $a \in \mathscr{F}(A)$, hence a map $a : h_A \to \mathscr{F}$. This map a becomes the isomorphism $b : B \to \mathscr{F}|_{R'}$ when restricted to $\mathrm{Shv}(R'_{\mathrm{fpqc}}, \mathscr{S}ets)$. Hence the map a is an isomorphism already, as being an isomorphism for sheaves can be checked locally in the respective topology. Indeed, take a map $\mathscr{F} \to \mathscr{G}$ of sheaves that locally is an isomorphism, then

$$\mathscr{F} = \check{\mathscr{H}}^0(\mathscr{F}) \xrightarrow{\sim} \check{\mathscr{H}}^0(\mathscr{G}) = \mathscr{G},$$

because $\check{\mathscr{H}}^0(-)$ only depends on the input locally. □

Theorem 15. *Any descent datum (B, φ) for algebras relative an fpqc map $R \to R'$ is canonically isomorphic to $(A \otimes_R R', \mathrm{id}_A \otimes \mathrm{id}_{R''})$ for an R-algebra A.*

Proof: Recall that the map φ is an R''-isomorphism

$$\varphi : B \otimes_{R',\mathrm{pr}_2} R'' \xrightarrow{\sim} B \otimes_{R',\mathrm{pr}_1} R'',$$

that satisfies $\varphi_{12} \circ \varphi_{23} = \varphi_{13}$ in the sense of (5.2) above, namely

(5.3)
$$\begin{tikzcd}
B \otimes_{R',\mathrm{pr}_3} R''' \arrow[rr, "\varphi_{13}"] \arrow[dr, "\varphi_{23}"] & & B \otimes_{R',\mathrm{pr}_1} R''' \\
& B \otimes_{R',\mathrm{pr}_2} R''' \arrow[ur, "\varphi_{12}"] &
\end{tikzcd}$$

commutes. We define

$$A = \{b \in B;\ \mathrm{pr}_1(b) = \varphi(\mathrm{pr}_2(b))\},$$

which is an R-subalgebra of the R'-algebra B, that sits in the commutative diagram

(5.4)
$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "="] & A \otimes_R R' \arrow[r, "\mathrm{id}_A \otimes \mathrm{pr}_1 - \mathrm{id}_A \otimes \mathrm{pr}_2"] \arrow[d, "a \otimes r' \mapsto ar'"] & A \otimes_R R'' \arrow[d] \\
0 \arrow[r] & A \arrow[r] & B \arrow[r, "\mathrm{pr}_1 - \varphi \circ \mathrm{pr}_2"] & B \otimes_{R',\mathrm{pr}_1} R''.
\end{tikzcd}$$

The commutativity of the right scale follows from the calculation:

$$a \otimes r' \mapsto a \otimes r' \otimes 1 \mapsto a \otimes_{R'} \mathrm{pr}_1(r') = ar' \otimes_{R'} 1 = \mathrm{pr}_1(ar')$$

$$a \otimes r' \mapsto a \otimes 1 \otimes r' \mapsto a \otimes_{R'} \mathrm{pr}_2(r') = \varphi(\mathrm{pr}_2(a))\,\mathrm{pr}_2(r') = \varphi(\mathrm{pr}_2(a)\,\mathrm{pr}_2(r')) = \varphi(\mathrm{pr}_2(ar')).$$

The second row is exact by definition of A and the first row is exact by Proposition 13 being the $A \otimes_R -$ of the Amitsur complex of $R \to R'$ in low degrees.

We claim, that the vertical maps in (5.4) are isomorphisms. For this we may perform an fpqc base change, which preserves the exactness of the bottom row and thus the definition of A. We may therefore assume without loss of generality that $R \to R'$ admits a retraction $\rho : R' \to R$.

Once we have proven the claim, the rest of the theorem follows as $B = A \otimes_R R'$ and the glueing map φ transforms into the identity by the commutativity of the following diagram.

$$\begin{tikzcd}
A \otimes_R R'' \arrow[r, "\mathrm{id}"] \arrow[d] & A \otimes_R R'' \arrow[d] \\
B \otimes_{R',\mathrm{pr}_2} R'' \arrow[r, "\varphi"] & B \otimes_{R',\mathrm{pr}_1} R''
\end{tikzcd}$$

Indeed, for all $a \in A$ and $r'' \in R''$ we compute by the definition of A that

$$\varphi(a \otimes r'') = \varphi(\mathrm{pr}_2(a)) \otimes r'' = \mathrm{pr}_1(a) \otimes r'' = a \otimes r''.$$

From now on we assume that we have a retraction $\rho : R' \to R$. The map φ when base changed via $\operatorname{id}\otimes\rho : R'' \to R'$ yields an R'-isomorphism

$$\psi : (B \otimes_{R',\rho} R) \otimes_R R' = B \otimes_{R',(\operatorname{id}\otimes\rho)\circ\operatorname{pr}_2} R' \xrightarrow{\operatorname{id}\otimes\rho(\varphi)} B \otimes_{R',(\operatorname{id}\otimes\rho)\circ\operatorname{pr}_1} R' = B.$$

We set $\tilde{A} := B \otimes_{R',\rho} R$ and get a commutative diagram with exact rows by Proposition 13.

$$\begin{tikzcd}
0 \arrow[r] & \tilde{A} \arrow[r] \arrow[d, dotted] & \tilde{A} \otimes_R R' \arrow[rr, "\operatorname{id}_{\tilde{A}} \otimes \operatorname{pr}_1 - \operatorname{id}_{\tilde{A}} \otimes \operatorname{pr}_2"] \arrow[d, "\psi", "\cong"'] & & \tilde{A} \otimes_R R'' \arrow[d, "\operatorname{pr}_1(\psi) = \psi\otimes\operatorname{id}_{R''}", "\cong"'] \\
0 \arrow[r] & A \arrow[r] & B \arrow[rr, "\operatorname{pr}_1 - \varphi\circ\operatorname{pr}_2"] & & B \otimes_{R',\operatorname{pr}_1} R''
\end{tikzcd} \tag{5.5}$$

The commutativity of the right scale follows from the trivial equation

$$\psi \otimes \operatorname{id}_{R''} \circ (\operatorname{id}_{\tilde{A}} \otimes \operatorname{pr}_1) = \operatorname{pr}_1 \circ \psi$$

and the less trivial equation

$$\operatorname{pr}_1(\psi) \circ (\operatorname{id}_{\tilde{A}} \otimes \operatorname{pr}_2) = \varphi \circ \operatorname{pr}_2 \circ \psi$$

which we obtain by base changing (5.3) via $\rho_3 = \operatorname{id}\otimes\operatorname{id}\otimes\rho : R''' \to R''$. It is only here that the cocycle condition on the gluing isomorphism plays a role. Indeed, we get

$$\begin{tikzcd}
\tilde{A} \otimes_R R' \arrow[r, "\operatorname{id}_{\tilde{A}} \otimes \operatorname{pr}_2"] \arrow[dd, "\psi"'] & \tilde{A} \otimes_R R'' \arrow[rr, "\operatorname{pr}_1(\psi)"] \arrow[d, equal] \arrow[rdd, "\operatorname{pr}_2(\psi)"] & & B \otimes_{R',\operatorname{pr}_1} R'' \arrow[d, equal] \\
& (B \otimes_{R',\operatorname{pr}_3} R''') \otimes_{R''',\rho_3} R'' \arrow[rr, crossing over, "\rho_3(\varphi_{13})"] \arrow[rdd, "\rho_3(\varphi_{23})"'] & & (B \otimes_{R',\operatorname{pr}_1} R''') \otimes_{R''',\rho_3} R'' \\
B \arrow[rr, "\operatorname{pr}_2"'] & & B \otimes_{R',\operatorname{pr}_2} R'' \arrow[ruu, "\varphi"] \arrow[d, equal] & \\
& & (B \otimes_{R',\operatorname{pr}_2} R''') \otimes_{R''',\rho_3} R'', \arrow[ruu, "\rho_3(\varphi_{12})"'] &
\end{tikzcd}$$

using

$$\rho_3 \circ \operatorname{pr}_{13} = \operatorname{pr}_1 \circ (\operatorname{id}\otimes\rho), \quad \rho_3 \circ \operatorname{pr}_{12} = \operatorname{id}_{R''}, \quad \rho_3 \circ \operatorname{pr}_{23} = \operatorname{pr}_2 \circ (\operatorname{id}\otimes\rho).$$

We conclude that canonically $\tilde{A} = A$ and that (5.5) is identical to diagram (5.4) showing that in the latter the vertical maps are isomorphisms. This proves the claim and the theorem. □

Corollary 16. *Let $R \to R'$ be an fpqc map. The base change functor $- \otimes_R R'$ describes an equivalence of categories between the category of R-algebras and the category of descent data relative $R \to R'$ for algebras.*

Proof: Theorem 15 shows that the functor is essentially surjective. Being fully faithful follows from the Amitsur complex:

$$\begin{tikzcd}
0 \arrow[r] & A_1 \arrow[r] \arrow[d, "f"] & A_1 \otimes_R R' \arrow[r, "\operatorname{pr}_1 - \operatorname{pr}_2"] \arrow[d, "F"] & A_1 \otimes_R R'' \arrow[d, "\operatorname{pr}_1(F)"] \\
0 \arrow[r] & A_2 \arrow[r] & A_2 \otimes_R R' \arrow[r, "\operatorname{pr}_1 - \operatorname{pr}_2"] & A_2 \otimes_R R''.
\end{tikzcd} \tag{5.6}$$

An R-linear f corresponds via $F = f \otimes \operatorname{id}_{R'}$ uniquely to an R'-linear F that commutes with the descent glueing map, which here means that $\operatorname{pr}_1(F) = \operatorname{pr}_2(F)$, thus $\operatorname{pr}_1(F) \circ \operatorname{pr}_2 = \operatorname{pr}_2 \circ F$. □

Corollary 16 allows to construct algebras or more generally modules locally for the fpqc topology. This justifies to consider the fpqc topology for Aff_R, because we are used to exploiting a topology for local constructions. Hence whenever local constructions are possible in a Grothendieck topology, we should be ok with our usual intuition of a topology.

6. Quotients by finite flat group actions

References: [Ra66], [Fa01].

6.1. Quotients by finite flat equivalence relations.

We work in the category of sheaves on Aff_R with respect to the fpqc topology.

6.1.1. *Equivalence relations.* An **equivalence relation** on a sheaf of sets $X \in \mathrm{Shv}(R_{\mathrm{fpqc}}, \mathscr{S}ets)$ is a sheaf of sets $\Gamma \in \mathrm{Shv}(R_{\mathrm{fpqc}}, \mathscr{S}ets)$ together with an inclusion $\Gamma \subset X \times_R X$, such that for each $T \in \mathscr{A}_R$ the set $\Gamma(T)$ in $X(T) \times X(T)$ is a graph of an equivalence relation on $X(T)$. This can be encoded in a list of axioms for Γ as follows.

(i) reflexive: the diagonal $\Delta : X \to X \times_R X$ factors over Γ.

(ii) symmetric: we have $\tau(\Gamma) = \Gamma$ where $\tau : X \times_R X \to X \times_R X$ is the involution which flips the factors.

(iii) transitive: the map $\mathrm{pr}_{13} : \Gamma \times_{\mathrm{pr}_2, X, \mathrm{pr}_1} \Gamma \to X \times_R X$ factors over Γ.

A **strict equivalence relation** is an equivalence relation $\Gamma \subset X \times_R X$ for a representable sheaf $X = \mathrm{Hom}_R(B, -)$ with a representable graph $\Gamma = \mathrm{Hom}_R(C, -)$ such that the induced map $B \otimes_R B \twoheadrightarrow C$ is surjective.

6.1.2. *Quotients.* The **quotient sheaf** $Y = X/\Gamma$ of an equivalence relation $\Gamma \subset X \times_R X$ is defined as the sheaf associated to the naive quotient

$$T \mapsto X(T)/\Gamma(T).$$

By the universal property of the sheafification, the quotient X/Γ indeed has the property of a categorical quotient:

$$\mathrm{Hom}_{\mathrm{Shv}}(X/\Gamma, \mathscr{F}) = \{f : X \to \mathscr{F};\ f \circ \mathrm{pr}_1 = f \circ \mathrm{pr}_2 : \Gamma \to \mathscr{F}\}$$

An **effective quotient** is a quotient as above which moreover satisfies that the natural map

$$\Gamma \to X \times_{X/\Gamma} X$$

is an isomorphism.

6.1.3. *Finite flat equivalence relation.* A **finite flat equivalence relation** is a strict equivalence relation

$$\Gamma = \mathrm{Hom}_R(C, -) \subset X \times_R X$$

with $X = \mathrm{Hom}_R(B, -)$ such that the induced maps $\mathrm{pr}_i : B \to C$ are finite and flat for $i = 1, 2$. In fact, it suffices to know that one projection is finite flat as the other is isomorphic to the first one via property (ii) and the twist τ.

An **R-scheme of finite type** is a contravariant functor $\mathscr{A}_R \to \mathscr{S}ets$ which is representable by a finitely generated R-algebra.

Theorem 17 (Grothendieck). *Let R be a Noetherian ring (as always). The fpqc-quotient sheaf of an affine R-scheme of finite type X by a finite flat equivalence relation $\Gamma \subset X \times_R X$ is representable by an affine R-scheme $Y = X/\Gamma$ of finite type.*

The map $X \to Y$ is finite and faithfully flat and the quotient is effective:

$$\Gamma = X \times_Y X \subset X \times_R X.$$

Proof: Let X be represented by the R-algebra B, and let Γ be represented by the R-algebra C. Then by assumption $B \otimes_R B \twoheadrightarrow C$ is surjective and the induced maps $\mathrm{pr}_i : B \to C$ are finite flat. The proof proceeds in several steps.

Step 1: The candidate. We define the R-subalgebra

$$A = \{a \in B;\ \mathrm{pr}_1(a) = \mathrm{pr}_2(a)\}$$

and the problem essentially is to find enough elements in A. The trick: coefficients of characteristic polynomials.

We consider the following commutative diagram

$$\begin{tikzcd}
 & B \arrow[r, shift left, "\mathrm{pr}_1"] \arrow[r, shift right, "\mathrm{pr}_2"'] \arrow[d, "\mathrm{pr}_2"] & C \arrow[d, "\mathrm{pr}_{23}"] \\
B \arrow[r, "\mathrm{pr}_1"] & C \arrow[r, shift left, "\mathrm{pr}_{12}"] \arrow[r, shift right, "\mathrm{pr}_{13}"'] & C \otimes_{\mathrm{pr}_1,B,\mathrm{pr}_1} C,
\end{tikzcd} \tag{6.1}$$

where both scales on the right are cocartesian. The maps together with their notation is best understood by giving the effect on T-valued points described as subsets of T-valued points of powers of X:

$$\begin{tikzcd}
 & t_2 \text{ or } t_3 & (t_2,t_3) \arrow[l, mapsto, shift right, "\mathrm{pr}_1"'] \arrow[l, mapsto, shift left, "\mathrm{pr}_2"] \\
t_1 & (t_1,t_2) \text{ or } (t_1,t_3) \arrow[l, mapsto, "\mathrm{pr}_1"'] \arrow[u, mapsto, "\mathrm{pr}_2"'] & (t_1,t_2,t_3). \arrow[l, mapsto, shift right, "\mathrm{pr}_{12}"'] \arrow[l, mapsto, shift left, "\mathrm{pr}_{13}"] \arrow[u, mapsto, "\mathrm{pr}_{23}"']
\end{tikzcd} \tag{6.2}$$

As the maps $\mathrm{pr}_i : B \to C$ are finite flat, we conclude that also the maps $\mathrm{pr}_{ij} : C \to C \otimes_{\mathrm{pr}_1,B,\mathrm{pr}_1} C$ are finite flat.

We regard C as a finite flat B-module via pr_2. For $b \in B$, the characteristic polynomial of multiplication by $\mathrm{pr}_1(b)$ on C is given by the norm map for the finite flat map

$$\mathrm{pr}_2[\lambda] : B[\lambda] \to C[\lambda]$$

of polynomial rings as the following element

$$P(\lambda) = \det_{\mathrm{pr}_2[\lambda]} \big(\lambda \cdot \mathrm{id} - \mathrm{pr}_1(b)\big) \in B[\lambda].$$

From the base change compatibility of the norm map we deduce that when we map with $\mathrm{pr}_1[\lambda]$ or $\mathrm{pr}_2[\lambda]$ to $C[\lambda]$ we obtain the same polynomial

$$\begin{aligned} \mathrm{pr}_1\big(\det_{\mathrm{pr}_2[\lambda]} \big(\lambda \cdot \mathrm{id} - \mathrm{pr}_1(b)\big)\big) &= \det_{\mathrm{pr}_{23}[\lambda]} \big(\lambda \cdot \mathrm{id} - \mathrm{pr}_{12} \circ \mathrm{pr}_1(b)\big) \\ = \det_{\mathrm{pr}_{23}[\lambda]} \big(\lambda \cdot \mathrm{id} - \mathrm{pr}_{13} \circ \mathrm{pr}_1(b)\big) &= \mathrm{pr}_2\big(\det_{\mathrm{pr}_2[\lambda]} \big(\lambda \cdot \mathrm{id} - \mathrm{pr}_1(b)\big)\big). \end{aligned} \tag{6.3}$$

Consequently, the polynomial $P(\lambda)$ has coefficients in A.

Step 2: B is integral over A. By the Cayley–Hamilton Theorem, the evaluation of $P(\lambda)$ in $\lambda = \mathrm{pr}_1(b)$ vanishes in $C \subset \mathrm{End}_B(C)$, where C has the B-module structure via pr_2. Hence

$$0 = ({}^{\mathrm{pr}_2}P)(\mathrm{pr}_1(b)) = ({}^{\mathrm{pr}_1}P)(\mathrm{pr}_1(b)) = \mathrm{pr}_1(P(b)),$$

and thus $P(b) = 0$, because $\mathrm{pr}_1 : B \to C$ is injective. As $P \in A[\lambda]$ is monic we deduce that $A \to B$ is an integral extension, where each element of B satisfies an integral equation of degree $\leq \mathrm{rk}_B(C)$. In particular, B is a finite A-module, as it is finitely generated as an R-algebra. It is proven later in step 7 that $\mathrm{rk}_B(C)$ is constant.

Step 3: A is of finite type over R and thus Noetherian. This follows from a general lemma due to Artin–Tate. The argument is as follows. Let $A_0 \subset A \subset B$ be the finitely generated R-subalgebra which is generated by all the coefficients of the characteristic polynomials as above for a finite collection of R-generators of B. Then B is a finite A_0-module, hence, by the Noetherian property, A is also a finite A_0-module. We conclude that A is a finitely generated R-algebra.

Step 4 – claim I: For any $\mathfrak{p} \in \operatorname{Spec}(A)$ and $\mathfrak{q}_1, \mathfrak{q}_2 \in \operatorname{Spec}(B)$ with $\mathfrak{q}_i \cap A = \mathfrak{p}$ we find a $\tilde{\mathfrak{q}} \in \operatorname{Spec}(C)$ with $\mathrm{pr}_i(\tilde{\mathfrak{q}}) = \mathfrak{q}_i$.

We argue by contradiction. We assume that $\mathfrak{q}_1$ is not contained in $\mathrm{pr}_1(\mathrm{pr}_2^{-1}(\mathfrak{q}_2)) \subseteq \operatorname{Spec}(B)$. As all these prime ideals lie over $\mathfrak{p}$ and all maps are finite, the Cohen-Seidenberg Theorems state that these prime ideals can only be contained one in the other if they in fact agree. Thus prime avoidance tells us that

$$\mathfrak{q}_1 \not\subseteq \bigcup_{\mathfrak{q}' \in \mathrm{pr}_1(\mathrm{pr}_2^{-1}(\mathfrak{q}_2))} \mathfrak{q}'$$

Let $b \in \mathfrak{q}_1$ which is not contained in any $\mathfrak{q}' \in \mathrm{pr}_1(\mathrm{pr}_2^{-1}(\mathfrak{q}_2))$, so b is a function with a zero at $\mathfrak{q}_1$ but invertible along all $\mathfrak{q}'$'s. We conclude that $\mathrm{pr}_1(b)$ is invertible along the fibre of pr_2 over $\mathfrak{q}_2$ and is 0 at the point in the fibre above $\mathfrak{q}_1$ corresponding to the diagonal $(\mathfrak{q}_1, \mathfrak{q}_1) \in \operatorname{Spec}(C)$ which is there due to reflexivity $\Delta \subset \Gamma \subset X \times_R X$.

The element $a = \det_{\mathrm{pr}_2}\big(\mathrm{pr}_1(b)\big)$ belongs to A by the argument from (6.3). The determinant construction commutes with base change. Hence the value of a at $\mathfrak{q}_2$ is the determinant of $\mathrm{pr}_1(b)$ in the fibre $C \otimes_{\mathrm{pr}_2, B} \kappa(\mathfrak{q}_2)$. This fibre is artinian and the image of $\mathrm{pr}_1(b)$ is a unit by construction. Thus a lies not in $\mathfrak{q}_2$. In the fibre above $\mathfrak{q}_1$ there is one point at which $\mathrm{pr}_1(b)$ vanishes, hence the multiplication operator acts on the corresponding local artinian algebra by a nilpotent endomorphism. This kills the determinant and thus $a \in \mathfrak{q}_1$. This leads to a contradiction as

$$a \in \mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A \subset \mathfrak{q}_2.$$

Step 5 – claim II: (i) $A \to B$ is fpqc and even finite, (ii) the map

$$\mathrm{pr}_1 \otimes \mathrm{pr}_2 : B \otimes_A B \to C$$

is an isomorphism.

The assertion of the claim are local on A and can moreover be checked after base change with an fpqc map $A \to A'$. We first replace A by the localisation $A_{\mathfrak{p}}$ for a $\mathfrak{p} \in \operatorname{Spec}(A)$ and then by a flat integral local extension with infinite residue field. Thus B and C are now semilocal with $\mathfrak{p}B$ and $\mathfrak{p}C$ contained in the respective radical and A is local with infinite residue field. Before we continue with step 5, we need two more auxiliary steps.

Step 6: C is a finite flat B-module of constant rank. C as a B-module via pr_1 is isomorphic via the flip τ to C as a B-module via pr_2. So the answer does not depend on the choice of the projection. The rank of C over B is a locally constant function, so it suffices to compare the ranks at the finitely many closed points. Let $\mathfrak{q}_1, \mathfrak{q}_2$ be maximal ideals of B, hence above $\mathfrak{p}$. We choose $\tilde{\mathfrak{q}} \in \operatorname{Spec}(C)$ as in step 4. From diagram (6.1) follows that

$$\mathrm{rk}_{\mathrm{pr}_2 : B \to C}(\mathfrak{q}_1) = \mathrm{rk}_{\mathrm{pr}_{23} : C \to C \otimes_{\mathrm{pr}_1, B, \mathrm{pr}_1} C}(\tilde{\mathfrak{q}}) = \mathrm{rk}_{\mathrm{pr}_2 : B \to C}(\mathfrak{q}_2).$$

Step 7: C is a free B-module of finite rank. $B/\mathfrak{p}B$ is artinian, hence locally free of constant rank implies free. Thus $C/\mathfrak{p}C$ is a free $B/\mathfrak{p}B$-module. We lift a basis of $C/\mathfrak{p}C$ to elements $c_1, \ldots, c_n \in C$ which still generate C as a B-module by the more precise Nakayama Lemma where the maximal ideal is replaced by an ideal which is contained in the radical. We obtain an exact sequence

$$0 \to K \to \bigoplus_{i=1}^{n} B \cdot c_i \to C \to 0,$$

which splits as C is a projective B module. But C is of constant rank n, so $K = 0$.

We return to step 5 and the proof of claim II. Because the equivalence relation is strict the map $B \otimes_A B \to C$ is surjective. The set $\mathrm{pr}_1(B)$ thus generates C as a B-module via pr_2. We claim next that $\mathrm{pr}_1(B)$ contains a basis of C as a B-module.

Because B is semilocal, by the more precise Nakayama Lemma and by quotienting out the radical of B, we may reduce to the case B is a product $\prod_{i=1}^{m} k_i$ of fields, A is an infinite field k and the generating subset $M = \mathrm{pr}_1(B)$ of the free B module C is a k-subspace. The prime $\mathfrak{q}_i \in \mathrm{Spec}(B)$ corresponds to the subset of $B = \prod_{i=1}^{m} k_i$ where the i^{th} component vanishes. The submodule $C_i = \mathfrak{q}_i C$ of C consists similarly of those elements of the B-module C which vanish at $\mathfrak{q}_i$.

We argue by induction on the rank of C as a B-module. For the induction step it is enough to find an element

$$v \in M - \bigcup_{i=1}^{m} C_i$$

which then generates a free direct factor. By assumption all k-subspaces $M \cap C_i$ are proper subspaces of M. As k is an infinite field, the vector space M is not covered by finitely many proper subspaces, which proves the existence of such a v. Then we proceed by induction with the complement and the projection of M as the new B-generating k-vector space of the complement.

Thus, we may choose $b_1, \ldots, b_n \in B$ with $C = \bigoplus_{i=1}^{n} B \cdot \mathrm{pr}_1(b_i)$. We claim that the $b_1, \ldots, b_n$ form a basis of B as an A-module.

Let for $b \in B$ be $x_i \in B$ with $\mathrm{pr}_1(b) = \sum_{i=1}^{n} \mathrm{pr}_2(x_i)\,\mathrm{pr}_1(b_i)$. Then using again diagram (6.1) we get

$$\sum_{i=1}^{n} \mathrm{pr}_{23}\left(\mathrm{pr}_1(x_i)\right) \cdot \mathrm{pr}_{12}\left(\mathrm{pr}_1(b_i)\right) = \sum_{i=1}^{n} \mathrm{pr}_{12}\left(\mathrm{pr}_2(x_i)\right) \cdot \mathrm{pr}_{12}\left(\mathrm{pr}_1(b_i)\right) = \mathrm{pr}_{12}(\mathrm{pr}_1(b))$$

$$= \mathrm{pr}_{13}(\mathrm{pr}_1(b)) = \sum_{i=1}^{n} \mathrm{pr}_{13}\left(\mathrm{pr}_2(x_i)\right) \cdot \mathrm{pr}_{13}\left(\mathrm{pr}_1(b_i)\right) = \sum_{i=1}^{n} \mathrm{pr}_{23}\left(\mathrm{pr}_2(x_i)\right) \cdot \mathrm{pr}_{12}\left(\mathrm{pr}_1(b_i)\right)$$

and comparison of coefficients yields $\mathrm{pr}_{23}\left(\mathrm{pr}_1(x_i)\right) = \mathrm{pr}_{23}\left(\mathrm{pr}_2(x_i)\right)$. As the finite flat pr_{23} is injective, we see that $\mathrm{pr}_1(x_i) = \mathrm{pr}_2(x_i)$ hence $x_i \in A$. Now

$$\mathrm{pr}_1(b) = \sum_{i=1}^{n} \mathrm{pr}_2(x_i)\,\mathrm{pr}_1(b_i) = \sum_{i=1}^{n} \mathrm{pr}_1(x_i)\,\mathrm{pr}_1(b_i) = \mathrm{pr}_1\left(\sum_{i=1}^{n} x_i b_i\right)$$

and pr_1 being injective we deduce $b = \sum_{i=1}^{n} x_i b_i$. So indeed the b_i generate B as an A-module. The b_i actually form a basis, as $\sum_{i=1}^{n} x_i b_i = 0$ implies

$$0 = \mathrm{pr}_1\left(\sum_{i=1}^{n} x_i b_i\right) = \sum_{i=1}^{n} \mathrm{pr}_2(x_i)\,\mathrm{pr}_1(b_i)$$

and from $\mathrm{pr}_1(b_i)$ being a basis of C we conclude $\mathrm{pr}_2(x_i) = 0$, hence $x_i = 0$ for all $1 \le i \le n$. This proves that B is a flat A-module, in fact with the extra information that a basis $b_1, \ldots, b_n$ remains a basis of C after base changing to B, ergo the map $B \otimes_A B \to C$ is an isomorphism. This proves claim II.

Step 8: A represents the quotient X/Γ. Let $\mathscr{F}$ be an arbitrary fpqc-sheaf. From claim II it follows that

$$\begin{tikzcd}\mathscr{F}(A) \arrow[r] & \mathscr{F}(B) \arrow[r, shift left, "\mathrm{pr}_1^*"] \arrow[r, shift right, "\mathrm{pr}_2^*"'] & \mathscr{F}(C)\end{tikzcd}$$

is exact in $\mathscr{S}ets$. Via Yoneda this interprets as

$$\mathrm{Hom}_{\mathrm{Shv}}(h_A, \mathscr{F}) = \{f : h_B \to \mathscr{F};\ f \circ \mathrm{pr}_1 = f \circ \mathrm{pr}_2 : h_C \to \mathscr{F}\}$$

which shows that $A \to B$ represents a categorical quotient $X \to X/\Gamma$. Furthermore the claim states that $X \to X/\Gamma$ is finite flat and that the quotient is effective: $\Gamma = X \times_{X/\Gamma} X$ in $X \times_R X$. This finishes the proof of the theorem. □

As a warning we give the following example. Let B be the semi-local ring $\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$ and let $C = B$ be the free B-module of rank 1. The $\mathbb{F}_2$-vector subspace M given by

$$(1,1,0),\ (1,0,1),\ (0,1,1),\ (0,0,0)$$

generates C as a B-module but does not contain a basis of C as a B-module.

Proposition 18. *Let Y be the quotient by a finite flat equivalence relation on the affine R-scheme X. If X is finite (resp. fpqc) over R, then Y is finite (resp. fpqc) over R.*

Proof: finite: Let $X \to Y$ be represented by the map $A \subset B$ of R-algebras. Recall that we assume that R is Noetherian! Hence A is a sub-R-module of the finite R-module B, hence also finite.

fpqc: $R \to A$ is fpqc if and only if for each R-module M the A-modules $\mathrm{Tor}^i_R(A, M)$ vanish for $i > 0$ and do not vanish for $i = 0$ and $M \neq (0)$. Note that the Tor's can be computed as the derived functors of $A \otimes_R - : \mathrm{Mod}(R) \to \mathrm{Mod}(A)$. Now the assertion follows from $A \subset B$ being fpqc by Theorem 17 and the resulting formula

$$\mathrm{Tor}^i_R(A, M) \otimes_A B = \mathrm{Tor}^i_R(B, M)$$

from the composite of the functor $A \otimes_R -$ with the exact functor $B \otimes_A -$. □

6.2. **Group actions.** A **(right) group action** of a group scheme G on a scheme X over R is a map of sheaves $m : X \times G \to X$ such that for each $U \in \mathrm{Aff}_R$ the induced map on sections over U is an action of the group $G(U)$ on the set $X(U)$ from the right. We give a few examples. Note that the formulas express the action on the coordinates of the generic elements. All examples are commutative, which makes it unnecessary to distinguish between right and left actions.

(1) The group $\mathbb{G}_{\mathrm{m}}$ acts on $\mathbb{A}^n$ by scaling

$$R[X_1, \ldots, X_n] \to R[T, T^{-1}] \otimes_R R[X_1, \ldots, X_n]$$

$$X_i \mapsto T \otimes X_i.$$

The action is compatible with the inclusion

$$U = \{\underline{x} \in \mathbb{A}^n; x_1 \in \mathbb{G}_{\mathrm{m}}\} \subset \mathbb{A}^n$$

represented by $R[X_1, X_1^{-1}, X_2, \ldots, X_n]$.

(2) The group $\underline{\mathbb{Z}/2\mathbb{Z}}_R$ is represented by

$$\mathrm{Maps}(\mathbb{Z}/2\mathbb{Z}, R) = R[T]/(T^2 - T)$$

with $T = 0$ defining $0 \in \mathbb{Z}/2\mathbb{Z}$ and $T = 1$ defining $1 \in \mathbb{Z}/2\mathbb{Z}$ and thus multiplication given by

$$R[T]/(T^2 - T) \to R[T]/(T^2 - T) \otimes_R R[S]/(S^2 - S)$$

$$T \mapsto T \otimes (1 - S) + (1 - T) \otimes S.$$

It acts on $\mathbb{A}^1$ represented by $R[X]$ by $X \mapsto -X$. The associated map on representing objects is

$$R[X] \to R[T]/(T^2 - T) \otimes_R R[X]$$

$$X \mapsto (1 - T) \otimes X - T \otimes X.$$

(3) The group μ_2 acts on $\mathbb{A}^1$ also by $X \mapsto -X$ with associated multiplication map

$$R[X] \to R[T]/(T^2 - 1) \otimes_R R[X]$$

$$X \mapsto T \otimes X.$$

(4) The group μ_6 represented by $R[T]/(T^6-1)$ acts on the scheme X given by

$$X(A) = \{(x,y) \in A^2;\ y^2 = x^3 - 1\}$$

represented by $R[X,Y]/(Y^2 = X^3 - 1)$ by the formula

$$R[X,Y]/(Y^2 = X^3-1) \to R[T]/(T^6-1) \otimes_R R[X,Y]/(Y^2 = X^3-1)$$
$$X \mapsto T^2 \otimes X,$$
$$Y \mapsto T^3 \otimes Y.$$

Note that for the action itself no restriction on the characteristic of R is necessary.

(5) The group μ_4 represented by $R[T]/(T^4-1)$ acts on the scheme X given by

$$X(A) = \{(x,y) \in A^2;\ y^2 = x^3 - x\}$$

represented by $R[X,Y]/(Y^2 = X^3 - X)$ by the formula

$$R[X,Y]/(Y^2 = X^3-X) \to R[T]/(T^4-1) \otimes_R R[X,Y]/(Y^2 = X^3-X)$$
$$X \mapsto T^2 \otimes X,$$
$$Y \mapsto T \otimes Y.$$

Note that for the action itself no restriction on the characteristic of R is necessary.

A **free (right) group action** is a group action $m : X \times G \to X$ such that the map

$$\Gamma = X \times G \to X \times X$$

defined on points as $(x,g) \mapsto (x, m(x,g))$ is a closed immersion.

It follows immediately from the definition that a free group action of a finite flat group G over R on an affine R-scheme X defines via the above map

$$\Gamma \subseteq X \times X$$

a finite flat equivalence relation on X. Indeed, the projection map

$$\Gamma = X \times G \to X$$

is a base change of $G \to h_R$ and thus finite flat if G is a finite flat R-group scheme. The Γ is anyway a graph of a strict equivalence relation and thus the flip of coordinates yields an isomorphism from the first projection to the second projection showing that

$$m : X \times G \to X$$

is also finite flat in this case.

A quotient $X \to X/\Gamma$ for this group action is a quotient $X \to X/G$ which satisfies the following universal property

$$\mathrm{Hom}_{\mathrm{Shv}}(X/G, \mathscr{F}) = \{f : X \to \mathscr{F};\ f \circ \mathrm{pr}_1 = f \circ m : X \times G \to \mathscr{F}\}$$

which describes G-invariant maps $X \to \mathscr{F}$. We discuss the examples above.

(1) The map

$$\mathbb{G}_{\mathrm{m}} \times \mathbb{A}^n \to \mathbb{A}^n \times \mathbb{A}^n$$

is not a closed immersion. No negative powers of T are in the image of

$$R[\underline{X}, \underline{Y}] \to R[T, T^{-1}] \otimes_R R[\underline{X}],$$
$$X_i \mapsto X_i,$$
$$Y_i \mapsto T \otimes X_i.$$

But if we invert X_1 and move on to $U \subset \mathbb{A}^n$, then we get a surjection

$$R[\underline{X}, X_1^{-1}, \underline{Y}, Y_1{}^{-1}] \twoheadrightarrow R[T, T^{-1}] \otimes_R R[\underline{X}, X_1^{-1}]$$
$$X_i \mapsto X_i,$$
$$Y_i \mapsto T \otimes X_i.$$

Anyway, $\mathbb{G}_{\mathrm{m}}$ is not finite flat, so this example is only of marginal interest to the course.

(2) The action of the finite flat $\underline{\mathbb{Z}/2\mathbb{Z}}_R$ on $\mathbb{A}^1$ yields

$$R[X,Y] \to R[X,T]/(T^2 - T),$$
$$X \mapsto X,$$
$$Y \mapsto X - 2TX$$

and is visibly not free if 2 is not invertible in R. But also when 2 is invertible, the point $X = 0$ causes problems (not surjective mod (X)). When one removes $0 \in \mathbb{A}^1$, then the action of $\underline{\mathbb{Z}/2\mathbb{Z}}_R$ becomes free on $\mathbb{G}_{\mathrm{m}} \subset \mathbb{A}^1$ away from characteristic 2.

(3) The action of the finite flat μ_2 given by $R[T]/(T^2 - 1)$ on $\mathbb{A}^1$ yields

$$R[X,Y] \to R[X,T]/(T^2 - 1),$$
$$X \mapsto X,$$
$$Y \mapsto TX$$

and is not free at $X = 0$. But removing $0 \in \mathbb{A}^1$ gives us a free action of μ_2 on $\mathbb{G}_{\mathrm{m}} \subset \mathbb{A}^1$, also when 2 is not invertible in R.

The action of $\underline{\mathbb{Z}/2\mathbb{Z}}_R$ and of μ_2 are isomorphic, when 2 is invertible, but we see that the extension as μ_2 compared to as $\underline{\mathbb{Z}/2\mathbb{Z}}_R$ yields the better action, when 2 is not invertible.

(4) The action of μ_6 above is not free at $X = 1, Y = 0$.

(5) The action of μ_4 above is not free at $X = 0, Y = 0$.

6.2.1. *Exercise: Inseparable* 2*-descent.* Work out an example in characteristic 2 of an ordinary elliptic curve E acted upon via translation by its infinitesimal 2-torsion $E[2]$ in the spirit of examples (4), (5) above. Leads to a free finite flat group action on the affine $E - \{0\}$, the quotient of which should be made explicit.

Theorem 19. *Let G be a finite flat group scheme over R which acts freely from the right on an affine R-scheme X of finite type. Then $Y = X/G$ is representable by an affine R-scheme of finite type.*

The map $X \to Y$ is finite and faithfully flat and $G \times_R X \subset X \times_R X$ is identical to $X \times_Y X$. Moreover, if X is finite (resp. fpqc) over R, then Y is finite (resp. fpqc) over R. And if G has order n then the quotient map $X \to Y$ is finite flat of degree n.

Proof: This follows from Theorem 17 and Proposition 18 with the exception of the assertion about the degree. But that is obvious from

$$\deg(X/Y) = \deg(X \times_Y X/X) = \deg(G \times X/X) = \#G$$

as the quotient is an effective quotient. □

The examples (1)–(5) do not satisfy the assumptions for Theorem 19. Let us discuss for (1)–(3) what still holds and what goes wrong. In particular we compute the R-algebra

$$A = \{b \in B;\ \mathrm{pr}_1(b) = \mathrm{pr}_2(b)\}$$

of the hypothetical quotient.

(1) The group $\mathbb{G}_{\mathrm{m}}$ is not finite. The hypothetical quotient is represented by

$$A = \{f(X) \in R[X];\ f(X) = f(TX)\} = R.$$

The closure of the orbits meet in $0 \in \mathbb{A}^n$, hence there is no $\mathbb{G}_{\mathrm{m}}$-invariant function other than the constants. If we remove the origin, we find the quotient

$$\mathbb{A}^n - \{0\}/\mathbb{G}_{\mathrm{m}} = \mathbb{P}^{n-1}.$$

An affine chart of this is given by the quotient $U/\mathbb{G}_{\mathrm{m}}$. The corresponding hypothetical quotient is

$$A = \{f(\underline{X} \in R[\underline{X}, X_1^{-1}];\ f(\underline{X}) = f(T\underline{X})\} = R\left[\frac{X_2}{X_1}, \dots, \frac{X_n}{X_1}\right]$$

which describes a reasonable quotient. The map $U \to U/\mathbb{G}_{\mathrm{m}}$ is flat and

$$U \times_{U/\mathbb{G}_{\mathrm{m}}} U = \mathbb{G}_{\mathrm{m}} \times U.$$

The assumption *finite* in Theorem 19 prevents this phenomenon of non-closed orbits with bad orbit closures.

(2) The $G = \underline{\mathbb{Z}/2\mathbb{Z}}$ action on $\mathbb{A}^1$ is not free. The hypothetical quotient is

$$\begin{aligned} A &= \{f \in R[X];\ f(X) = f(X - 2TX) \text{ in } R[X,T]/(T^2 - T)\} \\ &= \{f \in R[X];\ f(X) = f(-X) \text{ in } R[X]\} \quad \supseteq \quad R[X^2] \end{aligned}$$

with equality if 2 is invertible. In that case we still get a good finite flat quotient map for the category of R-schemes

$$\begin{aligned} q : \mathbb{A}^1 &\to \mathbb{A}^1, \\ X &\mapsto X^2. \end{aligned}$$

But

$$G \times \mathbb{A}^1 \to \mathbb{A}^1 \otimes_{q,\mathbb{A}^1,q} \mathbb{A}^1$$

is not an isomorphism over $X = 0$, where the group action has a fixed point, so is not free.

(3) The $G = \mu_2$ action on $\mathbb{A}^1$ is not free. The hypothetical quotient is

$$A = \{f \in R[X];\ f(X) = f(TX)\} = R[X^2]$$

regardless of the role of $2 \in R$. We still get a good finite flat quotient map for the category of R-schemes

$$\begin{aligned} q : \mathbb{A}^1 &\to \mathbb{A}^1, \\ X &\mapsto X^2. \end{aligned}$$

But

$$G \times \mathbb{A}^1 \to \mathbb{A}^1 \otimes_{q,\mathbb{A}^1,q} \mathbb{A}^1$$

is not an isomorphism over $X = 0$, where the group action has a fixed point, so is not free.

6.3. **Cokernels.**

6.3.1. *Quotient groups by finite flat normal subgroups.* Let H be a finite flat normal subgroup of an affine algebraic group G over R. The restriction of multiplication to

$$G \times H \to G$$

defines a free group action of H on G. Indeed, the corresponding map

$$G \times H \to G \times G$$

is a closed immersion by H being finite over R and thus being a closed subgroup of G. The quotient G/H which exists by Theorem 19 inherits a group structure by the universal property of the quotient and the assumption, that H is a normal subgroup. So the sheaf cokernel G/H is representable and Theorem 19 translates into the following theorem.

Theorem 20. *Let H be a finite flat closed normal subgroup of the affine algebraic R-group G. Then the quotient group sheaf G/H is representable by an affine algebraic R-group, which is a categorical cokernel for the inclusion $H \subset G$.*

The map $G \to G/H$ is finite and faithfully flat and $H \times_R G \subset G \times_R G$ is identical to $G \times_{G/H} G$. Moreover, if G is finite (resp. fpqc) over R, then G/H is finite (resp. fpqc) over R.

6.3.2. *Failure over arbitrary base R.* It is not true that the category of finite flat group schemes over R is an abelian category in general.

Lemma 21. *Let R be a ring with $p \cdot R = 0$. The functor on R-algebras*

$$T \mapsto \mathrm{End}(\alpha_{p,T})$$

is representable by the ring scheme $\mathcal{O}$ which is $\mathbb{G}_{\mathrm{a}} = \mathbb{A}^1$ with the usual underlying structure of addition and multiplication.

Proof: We recall that α_p is represented by $R[X]/X^p$ with comultiplication given by

$$\Delta(X) = X \otimes 1 + 1 \otimes X.$$

Any endomorphism h over T is determined by its value $h(X)$ on X, which must satisfy

$$\Delta h(X) = h(X) \otimes 1 + 1 \otimes h(X).$$

It follows that $h(X) = \lambda X$ for a unique $\lambda \in T$ and h simply scales by λ. Addition (resp. composition) of endomorphisms correspond obviously to addition (resp. multiplication) of the scaling factors, hence the assertion. □

Let R be a discrete valuation ring of equal characteristic $p > 0$ with uniformiser t. The endomorphism

$$[t] : \alpha_p \to \alpha_p$$

corresponding to $X \mapsto tX$ is an isomorphism in the generic fibre but the zero map in the special fibre, hence its kernel is not a finite flat group scheme over R.

Nevertheless, within the category of finite flat R-group schemes the map $[t]$ has kernel and cokernel, namely the trivial group scheme 1. But $[t]$ is not an isomorphism. So it is the more subtle axiom of abelian categories — that a bijective map has an inverse — that is violated.

More generally, if cokernels exist in the category of finite flat group schemes, then the order has to be locally constant and forming the cokernel has to commute with base change. But

$$\mathscr{E}nd_R(\alpha_p^{\oplus n}) = \mathrm{M}_n$$

is the ring scheme of $n \times n$ matrices, which allows sections of non-constant rank, hence the fibre-wise order of the cokernel jumps.

6.3.3. *When the base is a field.* References: [Pk05] or [De72] Chapter II.6.

Theorem 22. *The category of finite flat commutative group schemes over a field k is an abelian category.*

Proof: The schematic image $\varphi(H)$ of a map $\varphi : H \to G$ of finite flat commutative group schemes over k inherits a group structure which makes it into a normal subgroup $\varphi(H) \subseteq G$. Over a field this subgroup is automatically finite flat and Theorem 20 guarantees the existence of a cokernel.

The map $\mathrm{coim}(\varphi) \to \mathrm{im}(\varphi)$ is bijective, so it remains to argue that a bijective map $\varphi : H \to G$ of finite flat commutative group schemes over k is an isomorphism. Let $\varphi^* : A_G \to A_H$ be the underlying map of Hopf algebras. The image $\varphi(H)$ corresponds to the image $\varphi^*(A_G)$.

We have $G/\varphi(H) = 1$ is a strict quotient, hence $\varphi(H) \times G = G \times_1 G$ and thus the order of G equals the order of $\varphi(H)$. Consequently, $\dim_k(A_G) = \dim_k(\varphi^*(A_H))$ and the map $A_G \to A_H$ on Hopf algebras is injective. It follows that the Cartier dual $G^D \to H^D$ is a closed immersion which has a quotient $Q = H^D/G^D$. As the map $Q^D \to H \to G$ vanishes and $\ker(\varphi) = 1$ we deduce that $Q^D \to H$ and moreover $H^D \to Q$ vanish. Hence $Q = 1$ and the argument above shows that the natural map $A_H^\vee \to A_G^\vee$ of Cartier dual Hopf algebras is injective as well. So $A_G \to A_H$ is an isomorphism which proves the theorem. □

6.4. **Exact sequences.** In this section we discuss what it means to be an exact sequence of group schemes from the point of view of fpqc sheaves.

6.4.1. *Surjective.* Just to make it crystal clear we note the following.

Proposition 23. *Let $\pi : G \to G''$ be a map of affine groups whose underlying map $\pi^* : A'' \to A$ of representing R-algebras is fpqc. Then π is surjective as a map of fpqc sheaves.*

Proof: Let $g \in G''(T)$ be a T-valued point corresponding to $g : A'' \to T$. Then the base change $h : A \to T' = A \otimes_{A''} T$ of g is an element $h \in G(T')$ lifting the element $g|_{T'}$ fpqc locally, because $T \to T'$ is fpqc as a base change of $\pi^* : A'' \to A$. □

The converse to Proposition 23 fails. For example if G' is not flat over R, then the projection of $G = G' \times G''$ to G'' is not flat.

6.4.2. *Representability.* We discuss an exact sequence

$$1 \to G' \xrightarrow{\iota} G \xrightarrow{\pi} G'' \to 1$$

of fpqc sheaves on R_{fpqc} with values in (not necessarily abelian) groups.

Proposition 24. *Let G'' be representable by an fpqc R-scheme, e.g., G'' is finite flat over R.*
(1) fpqc locally $G \cong G' \times G''$ as R-schemes.
(2) G is representable if and only if G' representable.
(3) In particular, extensions of finite flat sheaves are representable by finite flat group schemes.

Proof: (1) Let A be an R-algebra representing G''. There is an fpqc map $A \to A'$ and an element $g' \in G(A')$ lifting the restriction to A' of the universal element $\mathrm{id}_A \in G''(A)$. The element g' defines a scheme theoretic section $s : G''|_{A'} \to G|_{A'}$ of the restriction of $\pi : G \to G''$ to A'. Using the group structure we define an isomorphism $G \to G' \times G''$ via

$$g \mapsto \big(s(\pi(g))^{-1}g, \pi(g)\big).$$

(2) By Theorem 14, it is enough to check representability locally in the fpqc topology. If G' and G'' are representable, then also $G = G' \times G''$ locally in fpqc. Otherwise, if G and G'' are representable, then G' is representable as the kernel of $\pi : G \to G''$.

(3) obvious from (1) and (2). □

For matters of completeness we restate the contents of Theorem 20.

Proposition 25. *If G' and G are representable by algebraic groups over R and moreover G' is finite flat, then G'' is representable.*

6.4.3. *Properties.* We now assume that in the exact sequence

$$1 \to G' \xrightarrow{\iota} G \xrightarrow{\pi} G'' \to 1$$

as above all three sheaves G', G and G'' are representable by R-algebras of finite type.

Proposition 26. *(1) ι is a closed immersion.*
(2) G' is finite flat over R if and only if π is finite flat.
(3) If two out of three from G', G and G'' are finite flat over R, then the third is as well.

Proof: (1) is obvious. (2) The kernel G' over R is a base change of π, hence also finite flat if π is. The converse is part of Theorem 20 above.

(3) Being finite flat can be checked fpqc locally. If G' and G are finite flat, then, by Theorem 20 above, $G \to G''$ is finite flat cover of G'' by a finite flat R-scheme and hence G'' is also finite flat over R.

If G'' is finite flat, then fpqc locally $G \cong G' \times G''$. The first projection $G \to G'$ is a base change of G'' over R and thus G is finite flat if and only if G' is finite flat. □

6.4.4. *Criterion for exactness.*

Corollary 27. *For a sequence* $1 \to G' \xrightarrow{\iota} G \xrightarrow{\pi} G'' \to 1$ *of finite flat* R*-groups the following are equivalent.*

(a) *The sequence is exact in fpqc sheaves on* R*.*
(b) $G' = \ker(\pi)$ *and* π *is finite flat.*
(c) ι *is a closed immersion with image a normal subgroup and* $G'' = \mathrm{coker}(\iota)$ *is the quotient* G/G' *via* π*.*

Proof: (a) implies (b) by Proposition 26 (2). The converse follows from Proposition 23.

(a) implies (c) by Proposition 26 (1). The converse follows from sheafification being exact. Namely we have an obvious short exact sequence of presheaves

$$1 \to G' \xrightarrow{\iota} G \xrightarrow{\pi_{\mathrm{naive}}} (G/G')_{\mathrm{naive}} \to 1$$

whose sheafification is the short exact sequence under discussion. □

Fo sake of clarity we stress that a short exact sequence of finite flat R-groups in $\mathrm{Shv}(R_{\mathrm{fpqc}})$ is also short exact as a sequence in the additive category of finite flat R-groups. But not necessarily conversely, see the discussion in Section §6.3. But if R is a field k, then life is good and the inclusion of finite k-groups into the category of fpqc sheaves on k with values in groups is an exact inclusion, compare Theorem 22 and its proof.

6.4.5. *Multiplicativity of the order.* The **index** of a finite flat group G' as a closed subgroup in a finite flat group G is the locally constant function $(G : G')$ on $\mathrm{Spec}(R)$ given by the degree over R of the quotient R-scheme $X = G/G'$. The right translation action of G' on G has a finite flat quotient by Theorem 19.

The analogue of Lagrange's theorem holds, see [Sh86].

Proposition 28 (Lagrange equation)**.** *Let* G' *be a finite flat closed subgroup of the finite flat* R*-group* G*. Then the following equation of locally constant functions on* $\mathrm{Spec}(R)$ *holds*

$$\#G' \cdot (G : G') = \#G.$$

Proof: Let $X = G/G'$ be the quotient. By Theorem 19 the quotient map $G \to X$ is finite flat of degree $\#G'$. Thus the formula follows from the fibre-wise multiplicativity of the rank in a composite of finite flat maps. □

6.4.6. *The Cartier dual is an exact functor.*

Proposition 29. *The Cartier dual of a short exact sequence of finite flat group schemes is again a short exact sequence of finite flat group scheme.*

Proof: A contravariant additive autoequivalence transforms existing kernels into cokernels and vice versa. The problem here is, that exactness is defined in $\mathrm{Shv}(R_{\mathrm{fpqc}})$, whereas the duality functor $G \mapsto G^D$ lives only in the full subcategory of finite flat group schemes. So we have to be more careful. Let

$$1 \to G' \xrightarrow{\iota} G \xrightarrow{\pi} G'' \to 1 \tag{6.4}$$

be a short exact sequence of finite flat group schemes. Then for each R-algebra T we have an isomorphism

$$\ker\left(G^D \to G'^D\right)(T) = \ker\left(\mathrm{Hom}(G_T, \mathbb{G}_\mathrm{m}) \xrightarrow{\circ\iota} \mathrm{Hom}(G'_T, \mathbb{G}_\mathrm{m})\right) \xleftarrow{\pi^D} \mathrm{Hom}(G''_T, \mathbb{G}_\mathrm{m}) = G''^D(T)$$

by the quotient property and the fact, that (6.4) remains short exact after arbitrary base change $- \otimes_R T$. Hence the Cartier dual of a cokernel is a kernel.

It remains to prove that $\iota^D : G^D \to G'^D$ is surjective in the fpqc topology, or, that ι^D is the quotient map to the inclusion π^D. It follows from Theorem 20, that $\pi^D : G''^D \to G^D$ has a finite flat cokernel G^D/G''^D and by the universal property ι^D gives us a map $G^D/G''^D \to G'^D$, which is an isomorphism because its Cartier dual map

$$G' \to \ker\left((G^D)^D \to (G''^D)^D\right) = \ker(\pi : G \to G'')$$

is an isomorphism. □

6.4.7. *An example.* We present a well known example of a finite flat group of order p^2 in characteristic p which is a semi-direct product, see [Sh86] end of §3. Let R be a ring with $p \cdot R = 0$ and let E be the subgroup scheme of GL_2 over R defined by

$$E(T) = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(T);\ x^p = 1,\ y^p = 0 \right\} \subseteq \mathrm{GL}_2(T)$$

for each R-algebra T. The group sits in an obvious short exact sequence

$$1 \to \alpha_p \to E \to \mu_p \to 1$$

which is split and thus defines the semidirect product of μ_p with α_p coming from the canonical action $\mu_p \to \mathbb{G}_{\mathrm{m}} = \underline{\mathrm{Aut}}(\alpha_p)$.

This example is important because it is not commutative but still of order p^2, which cannot happen for abstract groups. We deduce that therefore E does not admit a lifting into characteristic 0, where the lift would be an étale group of order p^2, see Section §7 below, and thus commutative, forcing commutativity also for E.

We can check the validity of 'order kills group' also in this non-commutative example by

$$\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}^{p^2} = \begin{pmatrix} x^p & y(1+x+\ldots+x^{p-1}) \\ 0 & 1 \end{pmatrix}^{p} = \begin{pmatrix} 1 & py(1+x+\ldots+x^{p-1}) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

working with the universal element. As E has a filtration with commutative subquotients, the result follows anyway by induction on the length from the abelian case.

7. Étale finite flat group schemes

References: [Sh86] §3.

7.1. Étale maps.

7.1.1. *Kähler differentials.* An R-**derivation** of an R-algebra A with values in an A-module M is an R-linear map

$$\delta : A \to M$$

such that

$$\delta(xy) = x\delta(y) + y\delta(x)$$

for all $x, y \in A$ (Leibniz-rule), in particular $\delta(R) = 0$. There is a universal derivation

$$d : A \to \Omega^1_{A/R}$$

which one gets as the quotient of the free A-module on symbols da for each $a \in A$ by the requested relations among them. The module $\Omega^1_{A/R}$ is the module of **Kähler differentials** of A over R. Under base change $R \to R'$ with $A' = A \otimes_R R'$ we have from the universal property that

$$\Omega^1_{A/R} \otimes_R R' = \Omega^1_{A'/R'}.$$

In particular, $\Omega^1_{A/R}$ behaves well under localisation in R — and also under localisation in A by the rule for differentiation of fractions

$$d(\frac{a}{b}) = \frac{b \cdot da - a \cdot db}{b^2},$$

which implies

$$S^{-1}\Omega^1_{A/R} = \Omega^1_{S^{-1}A/R}.$$

There are two fundamental short exact sequences. First, for a map $A \to B$ of R-algebras

$$\Omega^1_{A/R} \otimes_A B \to \Omega^1_{B/R} \to \Omega^1_{B/A} \to 0 \tag{7.1}$$

is exact. Secondly, let $A \twoheadrightarrow A/I$ be the quotient of an R-algebra A by the ideal I. Then the following is exact:

$$I/I^2 \to \Omega^1_{A/R} \otimes_A A/I \to \Omega^1_{A/R} \to 0. \tag{7.2}$$

7.1.2. *Definition and some sorite for étale maps.* An **étale map** is a ring homomorphism $A \to B$ that is flat, of finite presentation and such that $\Omega^1_{B/A}$ vanishes.

It follows from Section §7.1.1 that $A \to B$ being étale is local on A and on B, is preserved under composition and under base change. Moreover, we may test being étale locally in the fpqc topology of the base, again a hint that the notion of the fpqc topology behaves as a topology.

By the assumption of finite presentation, the module $\Omega^1_{B/A}$ is a coherent B-module. The Nakayama Lemma and the base change compatibility for Kähler differentials then give immediately the following proposition.

Proposition 30. *Let $h : A \to B$ be a flat map of finite presentation. Then h is an étale map if and only if for each $\mathfrak{p} \in \mathrm{Spec}(A)$ the fibre $B \otimes_A \kappa(\mathfrak{p})$ is an étale $\kappa(\mathfrak{p})$-algebra.*

7.1.3. *Étale algebras over fields.* As we are primarily interested in finite maps, we resist the temptation to avoid the finiteness assumption in the following theorem.

Theorem 31. *Let A be a finite algebra over the field k. Then the following are equivalent.*

(a) *A is k-isomorphic to a finite product $\prod_i k_i$ of finite separable field extensions k_i/k.*
(b) *$A \otimes_k K$ is reduced for all field extensions K/k.*
(c) *$A \otimes_k k^{\mathrm{alg}}$ is reduced.*
(d) *$A \otimes k^{\mathrm{alg}}$ is isomorphic as a k^{alg}-algebra to a finite product of copies of k^{alg}.*
(e) *$\Omega^1_{A/k} = (0)$.*
(f) *A is an étale k-algebra.*

Proof: (a) implies (b) by

$$k[X]/(f) \otimes_k K = K[X]/(f) = \prod_i K[X]/(f_i)$$

for a separable polynomial f and its irreducible factors f_i in $K[X]$. (b) implies (c) is obvious. (c) is equivalent to (d) by the structure theorem on artinian rings.

Property (e) which by definition is equivalent to (f) can be checked after scalar extension, e.g. to k^{alg}, where it is an immediate consequence of (d).

It remains to prove (a) from (e). We first prove that A is reduced. For that matter we may assume that $k = k^{\mathrm{alg}}$ and that if A is not reduced we have a quotient $A \twoheadrightarrow k[\varepsilon]$. Then (e) implies $\Omega^1_{k[\varepsilon]/k} = (0)$ which contradicts the computation

$$\Omega^1_{k[\varepsilon]/k} = \big(k[\varepsilon]/(2\varepsilon)\big) \cdot d\varepsilon \neq (0).$$

Hence A is reduced and so a product of fields. We may assume that $A = K$ is a field and have to contradict the existence of a k-subfield $K_0 \subset K$ with $K = K_0[X]/(X^p - a)$. But then (e) implies again $\Omega^1_{K/K_0} = (0)$, while the computation reveals

$$\Omega^1_{K/K_0} = \big(K/(d(X^p - a)\big) \cdot dX = K \cdot dX \neq (0),$$

and this contradiction finishes the proof. □

7.2. **The étale fundamental group.** The standard reference for the étale fundamental group is [SGA1]. Here we content ourselves with just the main result. Let Ω be a separably closed field. The category of finite étale maps over $\mathrm{Spec}(\Omega)$ can be naturally identified with the category of finite sets by Theorem 31.

Let X be a connected scheme with a geometric point

$$x : \mathrm{Spec}(\Omega) \to X.$$

The fibre functor F_x associates to a finite étale map $Y \to X$ its fibre $F_x(Y) = Y \times_X x$. The fibre functor maps the category Rev_X of finite étale covers of X to finite sets. As such, the automorphism group

$$\pi_1(X, x)$$

of F_x is naturally a pro-finite group with topology given by the stabilisers of points $y \in F_x(Y)$ for all y, Y.

Theorem 32 ([SGA1] Exp V)**.** *The fibre functor F_x naturally enhances to an equivalence of categories of Rev_X with the category of finite sets equipped with a continuous $\pi_1(X, x)$ action.*

7.2.1. *Example.* When the base scheme X is the spectrum of a field $\mathrm{Spec}(k)$, Theorem 31 above tells us that connected finite étale covers are just finite separable field extensions. We choose a geometric point $x : \mathrm{Spec}(k^{\mathrm{sep}}) \to \mathrm{Spec}(k)$ which corresponds to a separable closure of k. The main results on Galois theory then easily translate into an isomorphism of the fundamental group $\pi_1(X, x)$ with the absolute Galois group $\mathrm{Gal}_k = \mathrm{Gal}(k^{\mathrm{sep}}/k)$.

When the base scheme is $X = \mathrm{Spec}(R)$ for a complete (resp. henselian) local Noetherian ring $(R, \mathfrak{m})$, then idempotents lift uniquely from $k = R/\mathfrak{m}$ to R by (a generalisation of) Hensel's Lemma (resp. more or less by definition) which essentially shows that the category of finite étale covers of $\mathrm{Spec}(R)$ and $\mathrm{Spec}(k)$ agree and with $x : \mathrm{Spec}(k^{\mathrm{sep}}) \to X$ being a geometric point above the closed point we find

$$\pi_1(X, x) = \mathrm{Gal}_k\,.$$

In case R is even a henselian discrete valuation ring with field of fractions K this translates into the isomorphism of the Galois group $\mathrm{Gal}(K^{\mathrm{nr}}/K)$ of the maximal unramified extension K^{nr}/K with the absolute Galois group Gal_k of the residue field.

7.3. **Description of finite étale group schemes.** References: [De72] II.2.

A **finite étale** group scheme over R is a finite flat group scheme G over R which is represented by an étale R-algebra. The multiplication map $\mu : G \times G \to G$, the inverse $\mathrm{inv} : G \to G$ and the unit $\mathrm{Spec}(R) \to G$ are maps between finite étale $\mathrm{Spec}(R)$ schemes. Thus Theorem 32 has the following immediate consequence.

Theorem 33. *Let $S = \mathrm{Spec}(R)$ be a connected base with a geometric point $s \in S$. There is a faithful and exact embedding*

$$\left\{ \begin{array}{l} \textit{finite groups with a} \\ \textit{continuous } \pi_1(S, s) \textit{ action} \end{array} \right\} \hookrightarrow \left\{ \begin{array}{l} \textit{finite flat group schemes} \\ \textit{over } S = \mathrm{Spec}(R) \end{array} \right\}$$

The essential image exactly consists of the finite étale group schemes over S.

In this equivalence the constant group schemes correspond to groups with trivial action by $\pi_1(S, s)$. Moreover, the étale group schemes over S are exactly those group functors which become constant after restricting to a suitable finite étale cover. Indeed, such a group scheme is representable by Theorem 14 and whether the representing algebra is étale may be checked after an fpqc base change.

7.3.1. *Construction.* Let G be a finite group with a continuous $\pi_1(S,s)$ action

$$\rho : \pi_1(S,s) \to \mathrm{Aut}_{\mathscr{G}rps}(G).$$

Let $R \to R'$ be a finite étale map corresponding to a finite quotient $\pi_1(S,s) \twoheadrightarrow \Gamma$ such that the action on G factors through Γ. That means that we have a left R-linear Γ-action on R' and

$$R'' = R' \otimes_R R' = \prod_{\gamma\in\Gamma} R' \quad a \otimes b \mapsto (a \cdot \gamma(b))_{\gamma\in\Gamma}.$$

For an fpqc-sheaf $\mathscr{F}$ the set $\mathscr{F}(T \otimes_R R')$ carries a left Γ-action such that $\mathscr{F}(T)$ equals the invariants $\mathscr{F}(T \otimes_R R')^\Gamma$ due to the sheaf property for

$$\begin{tikzcd}
T \arrow[r] & T \otimes_R R' \arrow[r, shift left, "\mathrm{pr}_1"] \arrow[r, shift right, "\mathrm{pr}_2"'] \arrow[d, equal] & T \otimes_R R'' \arrow[d, equal] \\
& T \otimes_R R' \arrow[r, shift left, "\mathrm{diag}"] \arrow[r, shift right, "a\mapsto\gamma(a)"'] & T \otimes_R \prod_{\gamma\in\Gamma} R'.
\end{tikzcd}$$

We define the associated finite étale group scheme G_ρ as the group of invariants with respect to the diagonal Γ action: on G via ρ and on R' as above

$$G_\rho(T) = \underline{G}(T \otimes_R R')^\Gamma = \mathrm{Hom}_{R[\Gamma]}\big(\prod_{g\in G} R, T \otimes_R R'\big). \tag{7.3}$$

Because taking invariants is left exact G_ρ as in (7.3) describes an fpqc-sheaf, which when restricted to R', hence finite étale locally (fpqc locally),

$$G_\rho|_{R'}(T) = \underline{G}(T \otimes_R R')^\Gamma = \underline{G}\big(T \otimes_{R'} (R' \otimes_R R')\big)^\Gamma = \underline{G}\big(\prod_{\gamma\in\Gamma} T\big)^\Gamma = \underline{G}|_{R'}(T) \tag{7.4}$$

is isomorphic to the constant group scheme $\underline{G}$. We conclude by Theorem 14 that G_ρ is representable. Moreover G_ρ is finite étale because being finite étale is fpqc-local. The fibre above $s : \mathrm{Spec}(\Omega) \to S$ is

$$F_s(G_\rho) = G_\rho(s) = \underline{G}(\Omega \otimes_R R')^\Gamma = \underline{G}\big(\prod_{\gamma\in\Gamma} \Omega\big)^\Gamma = \mathrm{Maps}_\Gamma(\Gamma, G) = G.$$

The last isomorphism is by evaluation at $1 \in \Gamma$. The fundamental group acts through

$$\pi_1(S,s) \twoheadrightarrow \Gamma = \mathrm{Aut}_R(R'),$$

hence $\sigma \in \Gamma$ acts on $\prod_\gamma \Omega$ via

$$\sigma(x_\gamma) = (x_{\gamma\sigma})$$

and thus via translation on $f : \Gamma \to G$ by $\sigma.f(\gamma) = f(\gamma\sigma)$. If follows that

$$(\sigma.f)(1) = f(\sigma) = \rho(\sigma)\big(f(1)\big)$$

and thus the action of $\pi_1(S,s)$ on the fibre of G_ρ above s is via ρ as expected.

Another interpretation for the Γ-action on $G_\rho|_{R'} = \underline{G}_{R'}$ is the structure of a descent datum relative $R \to R'$. So a finite étale group scheme is a twisted form of a constant group scheme.

The R-algebra representing G_ρ can be obtained as follows. The base change via $R \to R'$ of G_ρ is constant and $\underline{G}_{R'} \to G_\rho$ is a quotient by the action of Γ. The representing algebra is thus the Γ invariants

$$\big(\prod_{g\in G} R'\big)^\Gamma = \mathrm{Maps}_\Gamma(G, R').$$

Indeed we have

$$G_\rho(T) = \mathrm{Hom}_{R'[\Gamma]}(\prod_{g\in G} R', T\otimes_R R') = \mathrm{Hom}_R(\mathrm{Maps}_\Gamma(G,R'),T)$$

by

$$\begin{tikzcd}
 & \underline{G}_{R'} \arrow[r, "/\Gamma"] \arrow[d] & G_\rho \arrow[d] \\
 & \mathrm{Spec}(R') \arrow[r, "/\Gamma"] & \mathrm{Spec}(R). \\
T\otimes_R R' \arrow[ur] \arrow[uur, dotted, "\Gamma-\text{invariant}"] \arrow[r, "/\Gamma"] & T \arrow[ur] \arrow[uur, dotted] &
\end{tikzcd}$$

7.4. Finite flat group schemes of invertible order are étale.

Theorem 34. *Let G be a finite flat group scheme over R with order invertible in R. Then G is a finite étale group scheme.*

Proof: Being étale for a flat R-group is decided fibre by fibre. Hence we may assume that $R = k$ is a field, and even that k is algebraically closed.

Let A be the k-algebra representing G and let $\mathfrak{m}\subset A$ be the maximal ideal at 0. It then suffices to prove

$$\Omega^1_{A/k}\otimes_A A/\mathfrak{m} = \mathfrak{m}/\mathfrak{m}^2 = 0.$$

As the multiplication of G reads for $x\in\mathfrak{m}$ in linear order as

$$\Delta(x)\in x\otimes 1 + 1\otimes x + \mathfrak{m}\otimes\mathfrak{m},$$

we see that multiplication by n on the group G acts as multiplication by n on the cotangent space $\Omega^1_{A/k}\otimes_A A/\mathfrak{m}$ at 0.

Commutative case: If we take for n the order of G, then multiplication by n is an isomorphism on $\Omega^1_{A/k}\otimes_A A/\mathfrak{m}$ by assumption and factors as

$$\Omega^1_{A/k}\otimes_A A/\mathfrak{m} \xrightarrow{\varepsilon^*} \Omega^1_{k/k} = 0 \xrightarrow{\eta^*} \Omega^1_{A/k}\otimes_A A/\mathfrak{m}$$

by Deligne's theorem (Theorem 6, case of commutative finite flat groups). Hence $\Omega^1_{A/k}\otimes_A A/\mathfrak{m}$ vanishes.

In characteristic 0: an algebraic group scheme in characteristic 0 is reduced by Theorem 1, hence our finite group scheme is étale by the criterion from Theorem 31. This proves the Theorem in the characteristic 0 case. □

We will provide a proof for the missing case of characteristic p and G not commutative later in Corollary 50.

7.4.1. *Example.* The non-commutative extension of μ_p by α_p over a ring of characteristic p cannot be lifted to characteristic 0. Otherwise, in characteristic 0, the lift would be étale and thus commutative, as all groups of order p^2 are commutative. The decoration of an action by the fundamental group does not alter the situation. As the generic fibre of characteristic 0 would be dense in the total space of the deformation, also the original group must be commutative, a contradiction.

Corollary 35. *Let R be a Noetherian ring that has a connected* $\mathrm{Spec}(R)$.

(1) The category of finite étale commutative R-group schemes is an abelian full subcategory of the category of all finite flat R-group schemes.

(2) The full category of commutative finite flat R-groups of order invertible in R is abelian.

8. Classification of finite flat group schemes

References: [Ta97], [Sh86].

8.1. **The connected component.** In this section we work entirely over a Noetherian local ring $(R, \mathfrak{m})$ which moreover is henselian, e.g., $\mathfrak{m}$-adically complete. We now consider group schemes over $S = \mathrm{Spec}(R)$. The closed point $\mathfrak{m}$ is denoted by s with residue field $k = R/\mathfrak{m}$.

Lemma 36. *Let $(R, \mathfrak{m})$ be a henselian local ring, e.g. $\mathfrak{m}$-adically complete, and let G be a flat affine algebraic group scheme over $S = \mathrm{Spec}(R)$. The connected component G^0 of G containing the locus of the unit section $e \in G(S)$ is a normal open and closed affine algebraic subgroup which is flat over R.*

Proof: The idempotent equation $X^2 - X$ is separable and thus Hensel's Lemma allows for unique lifting of idempotents. We conclude that

$$\pi_0(G_s) \subseteq \pi_0(G)$$

and

$$\pi_0(G_s \times_k G_s) \subseteq \pi_0(G \times_S G).$$

Let $G^0 \subset G$ be the connected component of G that contains the image of the unit section $e \in G(S)$. Its special fibre $(G^0)_s$ equals the connected component $(G_s)^0$ of the image of the unit section $e_s \in G_s(k)$, which therefore is denoted by G_s^0.

As in the proof of Theorem 1 (Cartier) the reduced special fibre G_s is geometrically regular and contains a k-rational point. Thus G_s^0 is geometrically connected and $G_s^0 \times_k G_s^0$ remains connected and open in $G_s \times_k G_s$ making it the connected component $(G \times G)_s^0$ of $(e_s, e_s) \in G_s \times_k G_s(k)$. The upshot of these connectedness considerations is, that multiplication, inverse and unit of G induce corresponding structure of a group on G^0. Moreover $G^0 \subset G$ becomes a normal affine algebraic subgroup which is flat over R. □

The subgroup G^0 of G as in the Lemma 36 is called **the connected component of G.** Taking the connected component is functorial, as a group homomorphism $\varphi : G \to H$ maps the connected component G^0 to a connected subset of H which contains the locus of $e \in H(S)$, hence is contained in H^0.

8.1.1. *The connected–étale exact sequence.*

Proposition 37. *Let R be a henselian local ring, e.g. $\mathfrak{m}$-adically complete, and let G be a finite flat group scheme over R.*

(1) Then there is an exact sequence of finite flat group schemes over R

$$1 \to G^0 \to G \to G^{\text{ét}} \to 1$$

with G^0 the connected component of G and $G^{\text{ét}}$ finite étale over R.

(2) Any group homomorphism $\varphi : G \to H$ to a finite étale R-group scheme H factors uniquely through $G \to G^{\text{ét}}$.

(3) Any group homomorphism $\varphi : H \to G$ from a connected R-group H factors uniquely through $G^0 \to G$.

Proof: (1) From Lemma 36 we know that G^0 is a normal geometrically connected subgroup of G. The quotient G/G^0 exists by Theorem 20 and is a finite flat group scheme. As $G^0/G^0 = 1$ is the trivial group scheme and an open subgroup of G/G^0 we see that the quotient $G^{\text{ét}} = G/G^0$ is étale over R at 1 and thus is a finite étale group by homogeneity.

(3) follows immediately from the functoriality of the connected component

$$\varphi|_{H^0} = \varphi^0 : H = H^0 \to G^0.$$

(2) It remains to prove that any group homomorphism $\varphi : H \to G$ from a connected group H to a finite étale group G is trivial. But again this factors over

$$\varphi : H = H^0 \to G^0 \subset G$$

which dies because of $G^0 = \mathrm{Spec}(k)$, since G is étale. □

Corollary 38. *A flat affine algebraic group scheme G over R is finite étale (resp. connected) if and only if the connected component G^0 (resp. the maximal étale quotient $G^{\text{ét}}$) is trivial.*

Proof: Obvious. □

Proposition 39. *Let G be finite flat group over a perfect field k. Then the connected-étale sequence splits canonically by the subgroup G_{red}.*

Proof: Taking the reduced subscheme $G_{\mathrm{red}} \subseteq G$ is compatible with products because the residue fields are perfect, and moreover is functorial. It follows that $G_{\mathrm{red}} \subseteq G$ is a closed subgroup. The induced map $G_{\mathrm{red}} \to G^{\text{ét}}$ is an isomorphism as can be seen by base changing to an algebraic closure k^{alg}: we have $G_{\mathrm{red}} \cap G^0 = \mathbf{1}$ and $G_{\mathrm{red}} \to G^{\text{ét}}$ surjective as each component of G now contains a k^{alg}-valued point. □

Exercise 8.1. Find an example of a finite flat group over a non-perfect field such that the connected-étale sequence does not split.

For an answer to this exercise see [Pk05] §15. Namely, let k be a non-perfect field with $u \in k \setminus k^p$. Let

$$A_i = k[T]/(T^p - u^i)$$

for $0 \leq i \leq p-1$ and set

$$A = \prod_i A_i$$

and $G = \mathrm{Spec}(A)$ and $G_i = \mathrm{Spec}(A_i)$. We define a multiplication by

$$G_i(R) \times G_j(R) \to G_{i+j}(R),$$
$$(t_i, t_j) \mapsto t_i t_j \quad \text{for } i + j \leq p - 1$$
$$(t_i, t_j) \mapsto t_i t_j / u \quad \text{for } i + j \geq p.$$

This makes G into a group over k which sits in a non-split extension

$$1 \to \mu_p \to G \to \underline{\mathbb{Z}/p\mathbb{Z}} \to 1.$$

An additive version is given by

$$G_i = \mathrm{Spec}(k[T]/(T^p - i \cdot u)$$

with composition

$$(t_i, t_j) \mapsto t_i + t_j$$

which makes $G = \coprod_i G_i$ be a group that fits the short exact sequence

$$1 \to \alpha_p \to G \to \underline{\mathbb{Z}/p\mathbb{Z}} \to 1.$$

Proposition 40. *Let $(R, \mathfrak{m})$ be a henselian local ring, e.g. $\mathfrak{m}$-adically complete.*

(1) The functors $G \mapsto G^0$ and $G \mapsto G^{\text{ét}}$ defined by Proposition 37 on the category of finite flat R-groups are exact.
(2) An extension of connected finite flat R-groups is connected.
(3) An extension of finite étale R-groups is finite étale.
(4) An extension of a connected finite R-group by a finite étale R-group is split as a product of the two.

Proof: (1) Let $1 \to G' \xrightarrow{\iota} G \xrightarrow{\pi} G'' \to 1$ be an exact sequence of finite flat R-groups. The map $\pi^0 : G^0 \to G''^0$ is finite and flat as a restriction of the flat π to open subgroups. Hence π^0 is faithfully flat because G''^0 is connected. The kernel of π^0 is connected, contains G'^0 and is contained in $G' \subseteq G$. Thus $\ker(\pi^0) = G'^0$ and the sequence

$$1 \to G'^0 \xrightarrow{\iota^0} G^0 \xrightarrow{\pi^0} G''^0 \to 1$$

is exact by 27(b). The exactness of the functor $G \mapsto G^{\text{ét}}$ now follows from the 3×3-Lemma.

(2) and (3) follow from (1) and Corollary 38. The splitting and even a retraction in case (4) is given by the maps of the connected-étale short exact sequence. □

8.2. **The tangent space.** References: [Pk05] §13.

Proposition 41. *Let $G = \operatorname{Spec}(A)$ be a finite flat commutative group over a field k. The tangent space at $e \in G(k)$ is given by the k-vector space*

$$\mathrm{T}_e\, G = \operatorname{Hom}(G^D, \mathbb{G}_{\mathrm{a}})$$

with respect to the vector space structure on $\operatorname{Hom}(G^D, \mathbb{G}_{\mathrm{a}})$ from $k = \underline{\operatorname{End}}\big(\mathbb{G}_{\mathrm{a}}\big)(k)$.

Proof: Let $\mathfrak{m} \subset A$ be the kernel of the augmentation $\varepsilon : A \twoheadrightarrow k$ corresponding to the unit $e \in G(k)$. Then the tangent space $\mathrm{T}\, G_e$ is the k-linear dual of $\mathfrak{m}/\mathfrak{m}^2 = \Omega^1_{A/k} \otimes_A A/\mathfrak{m}$, or the kernel of

$$G(k[\varepsilon]) \to G(k).$$

Indeed, $k[\varepsilon] = k \oplus k \cdot \varepsilon$ and so an element v in the kernel is a map $(\varepsilon, \partial_v) : A \to k \oplus k \cdot \varepsilon$, where ∂_v is a derivation on A with values in $k \cdot \varepsilon \cong k = A/\mathfrak{m}$, hence a k-linear form on $\Omega^1_{A/k} \otimes_A A/\mathfrak{m}$. The k-vector space structure comes from scaling and adding the linear forms.

In dual terms, ∂_v determines the image of T and thus a k-algebra map

$$f_v : k[T] \to A^\vee, \qquad f_v(T) = \partial_v.$$

The equation $\partial_v(ab) = \varepsilon(a)\partial_v(b) + \varepsilon(b)\partial_v(a)$ translates into:

$$f_v \otimes f_v(\Delta(T)) = f_v \otimes f_v(T \otimes 1 + 1 \otimes T) = \partial_v \otimes \varepsilon + \varepsilon \otimes \partial_v = ((a,b) \mapsto \varepsilon(a)\partial_v(b) + \varepsilon(b)\partial_v(a))$$

coincides with

$$\Delta(f_v(T)) = \Delta(\partial_v) = ((a,b) \mapsto \partial_v(ab))\,.$$

Hence $f_v : G^D \to \mathbb{G}_{\mathrm{a}}$ is a group homomorphism. The mapping $v \mapsto f_v$ is clearly bijective and k-linear, as the action of $k = \operatorname{End}_k(\mathbb{G}_{\mathrm{a}})$ is by adding and scaling the parameter T. □

We obtain another proof, that finite flat commutative groups of invertible order are finite étale. Namely, we may reduce to geometric fibres, hence a finite flat commutative group over an algebraically closed field k. Then G étale is equivalent that $\mathrm{T}\, G_e$ vanishes, which by Proposition 41 just means that there are no nontrivial group homomorphisms $G^D \to \mathbb{G}_{\mathrm{a}}$. Indeed, the image of such a map $G^D \to \mathbb{G}_{\mathrm{a}}$ is torsion of order prime to p, whereas $\mathbb{G}_{\mathrm{a}}$ has as endomorphism ring k in which the order of G^D is invertible. Hence there is no such torsion and any group homomorphism $G^D \to \mathbb{G}_{\mathrm{a}}$ is trivial.

8.3. **(Split) diagonalizable group schemes.** References: [Ta97] §2.6.

Let X be an ordinary finitely generated commutative group. The group ring

$$A = R[X] = \bigoplus_{x \in X} Rx$$

is a commutative finitely generated R-algebra, which represents the group valued functor $D(X)$ given by

$$D(X)(T) = \operatorname{Hom}_R(R[X], T) = \operatorname{Hom}_{\mathscr{G}rps}(X, T^\times).$$

Hence $D(X)$ is an algebraic affine flat commutative R-group scheme, the **diagonalizable** group scheme associated to the group of **characters** X, see below. A diagonalizable group with a finite group of characters is a finite flat group scheme. The name „diagonalizable" comes from the possibility to embed $D(X)$ into GL_n for suitable n and to then simultaneously diagonalize the image.

The formulas for the group structure of $D(X)$ are as follows.

$$\begin{aligned} \Delta(x) &= x \otimes x, \\ \varepsilon(x) &= 1, \\ \mathrm{inv}(x) &= x^{-1} \end{aligned}$$

The group of characters of a group G is $X(G) = \mathrm{Hom}(G, \mathbb{G}_\mathrm{m})$, and

$$X(D(X)) = \mathrm{Hom}(D(X), \mathbb{G}_\mathrm{m}) = X,$$

because a homomorphism $\varphi : D(X) \to \mathbb{G}_\mathrm{m}$ is a map of Hopf algebras

$$\varphi^* : R[U, U^{-1}] \to R[X]$$

and thus uniquely determined by the image $a = \varphi^*(U) \in R[X]$ subject to the conditions

$$\Delta(a) = a \otimes a, \quad \varepsilon(a) = 1.$$

These conditions are only valid for $a = x \in X \subset R[X]$. As an example we note

$$D(\mathbb{Z}) = \mathbb{G}_\mathrm{m}, \quad D(\mathbb{Z}/n\mathbb{Z}) = \mu_n,$$

and the general case is a product of these by the structure theorem of finitely generated abelian groups and

$$D(X \times Y) = D(X) \times_R D(Y).$$

Corollary 42. *Let G be a finite abstract abelian group. The Cartier dual of $D(G)$ is the constant group scheme $\underline{G}$.*

8.3.1. *Multiplicative finite flat group schemes.* A **multiplicative** (finite flat) group scheme is the Cartier dual to a finite étale group scheme. Because taking the Cartier dual behaves well under base change, we see that a multiplicative group scheme is a group scheme which finite étale locally is isomorphic to the diagonalizable group of a finite commutative group of characters.

Let $S = \mathrm{Spec}(R)$ be connected. Let G/S be a multiplicative group, then the characters

$$X(G) = \varinjlim_{R'} \mathrm{Hom}(G \times_R R', \mathbb{G}_{m,R'}) = \varinjlim_{R'} G^D(R'),$$

where the limit ranges over connected finite étale extensions $R \to R'$, is naturally a finite $\pi_1(S,s)$-module. Namely, the limit stabilises as soon as the finite étale group G^D becomes constant.

Corollary 43. *The association $G \mapsto X(G)$ describes a contravariant equivalence between multiplicative groups over S and finite abelian groups with an action by $\pi_1(S,s)$.*

The algebra representing the multiplicative group with the finite $\pi_1(S,s)$-module X is given by

$$A(X) = \mathrm{H}^0(\pi_1(S,s), R'[X]),$$

where R' is a connected finite étale extension of R that is large enough to trivialise the Cartier dual, resp. the action on X.

8.4. The canonical filtration: connected multiplicative, bi-infinitesimal, étale.

References: [Gr74], [De72] Chap. II.7-9.

A **bi-infinitesimal** group scheme over a henselian local ring $(R, \mathfrak{m})$ is a finite flat R-group G such that G and its cartier dual G^D are both connected.

Theorem 44. *Let $(R, \mathfrak{m})$ be a henselian local ring, e.g. $\mathfrak{m}$-adically complete, and let G be a finite flat commutative group scheme over $S = \mathrm{Spec}(R)$.*

(1) We have a natural filtration

$$0 \subset G_\mu \subset G^0 \subset G$$

such that G_μ is the maximal connected multiplicative subgroup, G^0 is the connected component of G, the quotient $G_{\mathrm{bi}} = G^0/G_\mu$ is bi-infinitesimal, and $G^{\text{ét}} = G/G^0$ is the maximal étale quotient.

(2) The filtration is respected by group homomorphisms.

(3) If R is a perfect field, then the filtration is canonically split and $G = G_\mu \times G_{\mathrm{bi}} \times G^{\text{ét}}$.

Proof: We apply Proposition 37 to the Cartier dual $(G^0)^D$ of the connected component and set

$$G_\mu = (((G^0)^D)^{\text{ét}})^D$$

which is obviously multiplicative and contained in G^0, hence connected, and also maximal with these properties. It follows from the exactness of Cartier duality that $G_{\mathrm{bi}} = G^0/G_\mu$ has Cartier dual

$$G_{\mathrm{bi}}^D = \ker\big((G^0)^D \to ((G^0)^D)^{\text{ét}}\big) = (((G^0)^D)^0)$$

which shows that G_{bi} is indeed bi-infinitesimal. The theorem follows now from Proposition 37 and Proposition 39. □

Remark 45. The filtration $0 \subset G_\mu \subset G^0 \subset G$ is not strictly preserved by group homomorphisms. For example for G of order p any nontrivial $g \in G(R)$ gives rise to a non-trivial map $\underline{\mathbb{Z}/p\mathbb{Z}}_R \to G$ which gives for $G = \mu_p$ (resp. $G = \alpha_p$) — over $R = k[\varepsilon]$ we can take $g = 1 + \varepsilon$ (resp. $g = \varepsilon$) — a nontrivial map from an étale group to a multiplicative connected (resp. bi-infinitesimal) group.

8.5. Characteristic $p > 0$. References: [De72] Chapter II.5.

In this Section we work over a basis $S = \mathrm{Spec}(R)$ in characteristic p.

8.5.1. *Frobenius.* References: [Pk05] §14.

The **Frobenius map**

$$F = F_{G/S} : G \to G^{(p)}$$

of an affine algebraic S-group G/S is the group homomorphism defined by raising to pth power on coordinates. By induction we set

$$\big(G^{(p^i)}\big)^{(p)} = G^{(p^{i+1})}$$

and write the composites of the respective Frobenius maps by abuse of notation as powers of the Frobenius map.

The **Frobenius height** of an affine algebraic S-group is the smallest number $n \in \mathbb{N}$, if such a number exists, such that the n-fold iterated Frobenius

$$F^n_{G/S} : G \to G^{(p)} \to \ldots \to G^{(p^n)}$$

is the 0 homomorphism. Otherwise the Frobenius height is infinite.

Lemma 46. *The Frobenius height of an affine algebraic group G/S is finite if and only if G is finite over S and G is connected after base change to any algebraically closed base $\mathrm{Spec}(k) \to S$.*

Proof: Let G be represented by

$$A = R[X_1, \dots, X_r]/J$$

with kernel of counit $\varepsilon : A \to R$, the augmentation ideal, generated by the X_i. The nth iterated Frobenius maps

$$X_i \mapsto X_i^{p^n}.$$

If G has a finite Frobenius height, then all X_i are nilpotent and thus A is finite as an R-module. Moreover, this property is preserved by base change and A is connected whenever R is.

Conversely, if A is finite and $A \otimes_R k$ is connected for any algebraically closed k, then we see by Noetherian induction on the support of $X_i^{(p^n)}$ (base change to an algebraically closed field dominating a generic point of the support) that for $n \gg 0$ all these have to vanish. □

Lemma 47. *Let G/S be an affine group scheme over $S = \operatorname{Spec}(R)$ represented by the R-algebra A. Then we have a canonical isomorphism*

$$\Omega^1_{G/S} = e^*\Omega^1_{G/S} \otimes_{\mathcal{O}_S} \mathcal{O}_G,$$

or

$$\Omega^1_{A/R} = \big(\Omega^1_{A/R} \otimes_{A,\varepsilon} R\big) \otimes_R A.$$

Proof: Let $m_G : G \times G \to G$ be the multiplication in G. We use the diagram

$$\begin{tikzcd}
G \arrow[r, "(\mathrm{id},e)"] & G \times G \arrow[r, "(\mathrm{id},m_G)"] \arrow[d, "\mathrm{pr}_1"] & G \times G \arrow[r, "\mathrm{pr}_2"] \arrow[d, "\mathrm{pr}_1"] & G \arrow[d] \\
 & G \arrow[r, equal] & G \arrow[r] & S.
\end{tikzcd}$$

The map (id, m_G) is an isomorphism. The behaviour of differentials under base change leads to

$$\Omega^1_{G/S} = \big(\mathrm{pr}_2(\mathrm{id}, m_G)(\mathrm{id}, e)\big)^*\Omega^1_{G/S} = \big((\mathrm{id}, m_G)(\mathrm{id}, e)\big)^*\Omega^1_{G\times G/G,\mathrm{pr}_1} = (\mathrm{id}, e)^*\Omega^1_{G\times G/G,\mathrm{pr}_1}$$
$$= \big(\mathrm{pr}_2(\mathrm{id}, e)\big)^*\Omega^1_{G/S} = e^*\Omega^1_{G/S} \otimes_{\mathcal{O}_S} \mathcal{O}_G.$$

□

Proposition 48 (Structure of Frobenius height 1)**.** *Let $G = \operatorname{Spec}(A)$ be a finite flat group over a field k of Frobenius height 1. Then there is an isomorphism of k-algebras*

$$A = k[X_1, \dots, X_r]/(X_i^p,\ 1 \le i \le r).$$

Proof: By Lemma 46, A is a finite local artinian k-algebra. We choose lifts $x_1, \dots, x_r$ of a basis of $\mathfrak{m}/\mathfrak{m}^2$, where

$$\mathfrak{m} = \ker(\varepsilon : A \twoheadrightarrow k)$$

is the augmentation ideal. Then by Nakayama and the Frobenius height being 1 we have

$$A = k[X_1, \dots, X_r]/J$$

with $x_i = X_i + J$ and $X_i^p \in J$ for all $1 \le i \le r$. By Lemma 47 the differentials

$$\Omega^1_{A/k} = \bigoplus_i A \cdot dX_i/(df,\ f \in J)$$

are free of rank r as an A-module. Hence the dX_i form a basis and for any $f \in J$ the partial differentials $\partial f/\partial X_i$ are again in J.

Let $f \in J$ be a polynomial not in $(X_1^p, \dots, X_r^p)$ containing a monomial $\underline{X}^{\underline{\alpha}}$ of minimal total degree $\deg(\underline{\alpha}) = \sum_i \alpha_i$ among all such f. Clearly $0 \le \alpha_i \le p-1$ and not all $\alpha_i = 0$. But $df = 0$ means that for all i the components $\partial f/\partial X_i$ of df lie in J, a contradiction to minimality. □

Theorem 49. *Let $R = k$ be a perfect field, and let A be the finite k-algebra which represents a connected finite flat k-group G. Then there is a k-isomorphism*

$$A \cong k[X_1, \ldots, X_r]/(X_i^{p^{e_i}},\ 1 \leq i \leq r)$$

for some $r \in \mathbb{N}$ and a tuple $\underline{e} = (e_1, \ldots, e_r) \in \mathbb{N}^r$, which are well-defined invariants of G up to permutation of $\underline{e}$.

Proof: We proceed by induction on the Frobenius height. The case of Frobenius height 0 is obvious and the case of Frobenius height equal to 1 was done in Proposition 48.

For the induction step we look at the image of the Frobenius map. The Frobenius twist is again $\operatorname{Spec}(A)$ but with a different k-structure, nevertheless, the image of $F_{G/k} : G \to G^{(p)}$ is described by the subalgebra $A^p \subset A$, that makes A a finite flat A^p-algebra by Theorem 20.

As the Frobenius height of $\operatorname{im}(F_{G/S}) = \operatorname{Spec}(A^p)$ is one less than the Frobenius height of G, we may choose a presentation

$$A^p \cong k[Y_1, \ldots, Y_s]/(Y_i^{p^{e_i}},\ 1 \leq i \leq s).$$

We choose elements $x_i \in A$ with $x_i^p = Y_i$. Then we consider the Frobenius map $(-)^p : A \twoheadrightarrow A^p$ on tangent spaces at the unit, i.e., the kernel of the augmentation $\mathfrak{m}_A$ (resp. $\mathfrak{m}_{A^p}$).

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{m}_A^2 \arrow[r] \arrow[d, two heads, "(-)^p"] & \mathfrak{m}_A \arrow[r] \arrow[d, two heads, "(-)^p"] & \mathfrak{m}_A/\mathfrak{m}_A^2 \arrow[r] \arrow[d, two heads, "(-)^p"] & 0 \\
0 \arrow[r] & \mathfrak{m}_{A^p}^2 \arrow[r] & \mathfrak{m}_{A^p} \arrow[r] & \mathfrak{m}_{A^p}/\mathfrak{m}_{A^p}^2 \arrow[r] & 0
\end{tikzcd}$$

By the snake lemma we find that

$$\ker((-)^p : \mathfrak{m}_A/\mathfrak{m}_A^2 \to \mathfrak{m}_{A^p}/\mathfrak{m}_{A^p}^2)$$

has a basis of elements that can be lifted to $z_1, \ldots, z_t \in \mathfrak{m}_A$ with $z_j^p = 0$. It follows, that

$$B := k[X_1, \ldots, X_s, Z_1, \ldots, Z_t]/(X_i^{(p^{e_i+1})}, Z_j^p,\ 1 \leq i \leq s, 1 \leq j \leq t) \tag{8.1}$$

has a natural surjection (Nakayama) $B \twoheadrightarrow A$ that maps $X_i \mapsto x_i$ and $Z_j \mapsto z_j$ and moreover is a map of finite flat A^p algebras, where A^p acts on B via $Y_i \mapsto X_i^p$.

As A^p is local artinian, flat equals free and the surjection is an isomorphism if it is a surjection modulo $\mathfrak{m}_{A^p}$. We get the map

$$B \otimes_{A^p} k = k[\underline{X}, \underline{Z}]/(X_i^p, Z_j^p, 1 \leq i \leq s, 1 \leq j \leq t) \twoheadrightarrow A \otimes_{A^p} k = \mathcal{O}(\ker(F_{G/S})) \tag{8.2}$$

with target the k-algebra representing the kernel of Frobenius of G. Because

$$\mathfrak{m}_{A^p} \subset (\mathfrak{m}_A)^p$$

the tangent spaces for G and $\ker(F_{G/S})$ agree and are of dimension $r = s + t$. Applying Proposition 48 to $\ker(F_{G/S})$ we see that the surjection in (8.2) and thus (8.1) is indeed an isomorphism.

The uniqueness of r and the tuple $\underline{e}$ up to permutation comes from $r = \dim \mathrm{T}_e\, G$ and induction by Frobenius height: the image $\overline{G}$ of $F_{G/S}$ has $\underline{e}_{\overline{G}} = \underline{e}_G - (1, \ldots, 1)$. □

A counter-example to Theorem 49 when the base k is not perfect can be found in [Sc00] §4. For $a \in k \setminus k^p$ and a k-algebra T we define a finite flat k-group by

$$G(T) = \{(x, y);\ x^{p^2} = 0,\ x^p = ay^p\}.$$

The group G has order p^3 and is an infinitesimal subscheme of $\mathbb{G}_\mathrm{a} \times \mathbb{G}_\mathrm{a}$. The problem with the theorem comes from the absence of elements

$$z \in A = k[X, Y]/(X^{p^2}, X^p - aY^p]$$

such that $z^p = 0$ and which are nontrivial in $\mathfrak{m}_A/(\mathfrak{m}_A^2 + (X))$. The mapping $G \to \alpha_p$ defined by $(x, y) \mapsto x^p$ determines a short exact sequence

$$0 \to \alpha_p \oplus \alpha_p \to G \to \alpha_p \to 0.$$

Corollary 50. *(1) The order of a connected finite flat group over a field of characteristic p is a power of p.*

(2) The order of a finite flat group G over $S = \mathrm{Spec}(R)$ for an arbitrary R such that G/S is not finite étale is divisible by a residue characteristic.

(3) A finite flat group scheme of order invertible in the base is finite étale.

Proof: Connectedness means Spec of a local artin ring with residue field k and is preserved by base change to the algebraic closure, hence (1) is obvious from Theorem 49, while (2) and hence (3) exploits the fact that for a flat map being étale is a fibre-wise matter that can be checked even on geometric fibres. □

8.5.2. *Verschiebung.* References: [Pk05] §14.

The Cartier dual of Frobenius of a finite flat commutative group G/S, more precisely the Cartier dual of the Frobenius of the Cartier dual finite flat group

$$F^D_{G^D/S} : ((G^D)^{(p)})^D \to (G^D)^D$$

is by definition the homomorphism **Verschiebung**

$$V = V_{G/S} : G^{(p)} \to G.$$

We give a second definition of the Verschiebung map which is valid also for affine group schemes, see [SGA3] VII 4.2-3. Let M be an R-module. The symmetrization operator is the R-module homomorphism

$$N : M^{\otimes p} \to (M^{\otimes p})^{S_p} \tag{8.3}$$

$$m_1 \otimes \ldots \otimes m_p \mapsto \sum_{\sigma \in S_p} m_{\sigma(1)} \otimes \ldots \otimes m_{\sigma(p)}.$$

The map

$$\varphi_M : M \otimes_{R,\mathrm{Frob}} R \to (M^{\otimes p})^{S_p} / \operatorname{im}(N) \tag{8.4}$$

$$m \otimes \lambda \mapsto \lambda \cdot m \otimes \ldots \otimes m$$

is a natural additive transformation because

$$(a+b) \otimes \ldots \otimes (a+b) = a \otimes \ldots \otimes a + b \otimes \ldots \otimes b + \sum_{i=1}^{p-1} \frac{1}{i!(p-i)!} N(\underbrace{a \otimes \ldots \otimes a}_{i} \otimes \underbrace{b \otimes \ldots \otimes b}_{p-i}).$$

Both sides of (8.4) are compatible with direct sums (the mixed terms of the right hand side are in the image of N), and with filtered direct limits. For $M = R$ we get

$$N(a_1 \otimes \ldots \otimes a_p) = p! \cdot \prod_i a_i = 0$$

and thus (8.4) is an isomorphism in this case. It follows that (8.4) is even an isomorphism for all modules M which are filtered inductive direct limits of free R-modules. These are exactly the flat R-modules by a theorem of Lazard. For flat R-modules M of finite rank we may also argue Zariski-local, where M becomes free.

Now we treat (8.3) and (8.4) in the case of M equal to an R-algebra A. The image of N is an ideal and (8.4) is an R-algebra map. Let

$$\mathrm{pr} : A^{\otimes p} \to \mathrm{Sym}^p(A)$$

denote the quotient map of the S_p-coinvariants. Then we compute

$$\operatorname{pr} \circ N(a_1 \otimes \ldots \otimes a_p) = p! \cdot \operatorname{pr}(a_1 \otimes \ldots \otimes a_p) = 0$$

and so we get for a commutative and cocommutative Hopf algebra A the following commutative diagram of R-algebra maps.

(8.5)
$$\begin{tikzcd}
A \arrow[rr, "\Delta"] \arrow[dr, "\overline{\Delta}"'] & & A^{\otimes p} \arrow[rr, "\mu"] \arrow[dr, two heads, "\operatorname{pr}"] & & A \\
& (A^{\otimes p})^{S_p} \arrow[ur, hook, "i"'] \arrow[dr, two heads, "\pi"'] & & \operatorname{Sym}^p A \arrow[ur, "\overline{\mu}"'] & \\
& & (A^{\otimes p})^{S_p} / \operatorname{im}(N) \arrow[ur, "\iota"'] & & \\
& & A^{(p)} = A \otimes_{R,\mathrm{Frob}} R \arrow[u, "\varphi_A"'] & &
\end{tikzcd}$$

The top row is the map which induces the multiplication by p map $[p] : G \to G$ on the associated affine group $G = \operatorname{Spec}(A)$. The right edge leads to

$$\overline{\mu} \circ \iota \circ \varphi_A : A^{(p)} \to A$$

$$a \otimes \lambda \mapsto \lambda \cdot a \otimes \ldots \otimes a \mapsto \operatorname{pr}(\lambda \cdot a \otimes \ldots \otimes a) \mapsto \lambda \cdot a^p$$

which is easily identified with the relative Frobenius $F_{G/R} : G \to G^{(p)}$. For A representing a flat R-group G the left edge leads to the **Verschiebung** $V_{G/R} : G^{(p)} \to G$ by

$$V_G^* = (\varphi_A)^{-1} \circ \pi \circ \overline{\Delta} : A \to A^{(p)}.$$

Because φ_A is natural with respect to maps of R-algebras and tensor products, we get

$$V_{G \times G/R} \circ \Delta = (V_{G/R} \times V_{G/R}) \circ \Delta = \Delta^{(p)} \circ V_{G/R}$$

and the Verschiebung turns out to be a group homomorphism. With this definition we get immediately the following proposition.

Proposition 51. *$V \circ F = [p]$ (resp. $F \circ V = [p]$) is multiplication by p on G (resp. $G^{(p)}$.)*

Proof: $V_{G/R} \circ F_{G/R} = [p]$ follows from the defining diagram (8.5). For the other composition we compute in the diagram

$$\begin{tikzcd}
& G \arrow[dr, "F_{G/R}"] & \\
G^{(p)} \arrow[ur, "V_{G/R}"] \arrow[rr, "{[p]}" description] \arrow[dr, "F_{G^{(p)}/R}"'] & & G^{(p)} \\
& G^{(p^2)} \arrow[ur, "V_{G/R})^{(p)} = V_{G^{(p)}/R}"'] &
\end{tikzcd}$$

because Frobenius is natural with respect to the base change by $\mathrm{Frob} : R \to R$ and the Verschiebung is preserved under base change. □

It remains to verify that both definitions of the Verschiebung agree for A representing a finite flat commutative R-group G. The $\operatorname{Hom}_R(-, R)$-dual of (the right edge of) diagram (8.5) turns out to be canonically (the left edge of) diagram (8.5) for the Cartier dual group, hence $V_{G^D/R} = F^D_{G/R}$. Indeed the maps Δ and μ are interchanged by the definition of the Cartier dual via the duality of Hopf algebras. The $\mathrm{Hom}_R(-,R)$-dual of the defining short exact sequences for the coinvariants

$$\prod_{\sigma\in S_p} A^{\otimes p} \xrightarrow{\sigma-1} A^{\otimes p} \xrightarrow{\mathrm{pr}} \mathrm{Sym}^p A \to 0$$

is the defining sequence for the invariants but for the dual algebra $A^\vee = \mathrm{Hom}_R(A,R)$

$$0 \to ((A^\vee)^{\otimes p})^{S_p} \xrightarrow{i} (A^\vee)^{\otimes p} \xrightarrow{\sigma-1} \prod_{\sigma\in S_p} (A^\vee)^{\otimes p},$$

hence the $\mathrm{Hom}_R(-,R)$-dual of pr and $\overline{\mu}$ are i and $\overline{\Delta}$. It remains to check the commutativity of the following diagram

$$\begin{tikzcd}
\big(\mathrm{Sym}^p A\big)^\vee \arrow[r, "(\varphi_A^{-1}\circ\iota)^\vee"] \arrow[d, equal] & \big(A\otimes_{R,\mathrm{Frob}} R\big)^\vee \arrow[d, equal] \\
\big((A^\vee)^{\otimes p}\big)^{S_p} \arrow[r, "\varphi_{A^\vee}^{-1}\circ\pi"] & (A^\vee)\otimes_{R,\mathrm{Frob}} R.
\end{tikzcd} \tag{8.6}$$

Let $f_{\alpha,i} : A \to R \in A^\vee$ be such that

$$\sum_\alpha f_{\alpha,1}\otimes\ldots\otimes f_{\alpha,p} \in (A^\vee)^{\otimes p}$$

is S_p-invariant. It follows from the computations after (8.4) that there are $h_\beta \in A^\vee$ and $\lambda_\beta \in R$ with

$$\sum_\alpha f_{\alpha,1}\otimes\ldots\otimes f_{\alpha,p} \equiv \sum_\beta \lambda_\beta h_\beta^{\otimes p} \mod \mathrm{im}(N),$$

which means that

$$\varphi_{A^\vee}^{-1}\circ\pi\Big(\sum_\alpha f_{\alpha,1}\otimes\ldots\otimes f_{\alpha,p}\Big) = \sum_\beta h_\beta\otimes\lambda_\beta \in A^\vee\otimes_{R,\mathrm{Frob}} R.$$

On the other hand, the form $\sum_\alpha f_{\alpha,1}\otimes\ldots\otimes f_{\alpha,p}$ maps in $(\mathrm{Sym}^p A)^\vee$ to

$$a_1\otimes\ldots\otimes a_p \mapsto \sum_\alpha\prod_i f_{\alpha,i}(a_i)$$

and via $(\varphi_A^{-1}\circ\iota)^\vee$ to

$$\left(a\otimes 1 \mapsto \sum_\alpha\prod_i f_{\alpha,i}(a) = \sum_\beta \lambda_\beta h_\beta(a)^p\right) \in \big(A\otimes_{R,\mathrm{Frob}} R\big)^\vee.$$

The latter agrees with $\sum_\beta h_\beta\otimes\lambda_\beta$ under the identification $\big(A\otimes_{R,\mathrm{Frob}} R\big)^\vee = A^\vee\otimes_{R,\mathrm{Frob}} R$ which shows the commutativity of (8.6).

Example 52. We compute the Frobenius and Verschiebung for the three typical examples of groups of order p.

(1) The group α_p is connected and thus of finite Frobenius height. Hence the Frobenius

$$F : \alpha_p \to \alpha_p$$

is the homomorphism 0, and by Cartier duality also the Verschiebung

$$V : \alpha_p \to \alpha_p$$

vanishes.

(2) By the same argument the Frobenius

$$F : \mu_p \to \mu_p$$

vanishes, and thus by Cartier duality also the Verschiebung

$$V : \underline{\mathbb{Z}/p\mathbb{Z}} \to \underline{\mathbb{Z}/p\mathbb{Z}}$$

is the homomorphism 0.

(3) The Frobenius

$$F : \underline{\mathbb{Z}/p\mathbb{Z}} \to \underline{\mathbb{Z}/p\mathbb{Z}}$$

is the identity map because on representing R-algebras it is given by

$$\prod_{g \in \mathbb{Z}/p\mathbb{Z}} R = \Big(\prod_{g \in \mathbb{Z}/p\mathbb{Z}} R \Big) \otimes_{R,\mathrm{Frob}} R \to \prod_{g \in \mathbb{Z}/p\mathbb{Z}} R$$

$$(a_g)_{g \in G} \mapsto \sum_g \underbrace{(0,\ldots,1,\ldots,0)}_{1 \text{ at } g} \otimes a_g \mapsto \sum_g a_g \cdot \underbrace{(0,\ldots,1,\ldots,0)}_{1 \text{ at } g}{}^p = (a_g)_{g \in G}.$$

Consequently, the Verschiebung

$$V : \mu_p \to \mu_p$$

is the identity map by Cartier duality.

Proposition 53. *Let $R = k$ be a field and let G/k be a finite flat group.*

(1) G is étale if and only if its Frobenius $F : G \to G^{(p)}$ is an isomorphism.
(2) G is connected if and only if the Frobenius $F : G \to G^{(p)}$ is nilpotent.
(3) G is multiplicative if and only if its Verschiebung $V : G^{(p)} \to G$ is an isomorphism.
(4) G is bi-infinitesimal if and only if Frobenius and Verschiebung are nilpotent.

Proof: (2) has been dealt with in Lemma 46. (1) If G is étale, then $G^0 = 1$ and G has no connected non-trivial subgroup, hence the kernel of Frobenius is trivial. Thus Frobenius is an isomorphism by comparing the order of the image $F(G)$ with that of G. On the contrary, if $G^0 \neq 1$, then the Frobenius has non-trivial kernel because it already has non-trivial kernel on G^0. (3) follows from (1) by Cartier duality. And (4) follows from (2) applied to G and G^D. □

8.5.3. *Simple objects.* In characteristic 0, the simple objects in the category of finite flat group schemes over a connected base S correspond to the irreducible continuous $\pi_1(S,s)$-modules.

Theorem 54. *Let k be an algebraically closed field of characteristic $p > 0$. The simple objects in the abelian category of finite flat commutative group schemes over* $\mathrm{Spec}(k)$ *are*

$$\mu_p, \alpha_p, \mathbb{Z}/p\mathbb{Z}, \text{ and } \mathbb{Z}/\ell\mathbb{Z} \text{ for all } \ell \neq p.$$

Proof: A simple object is either étale, connected multiplicative or bi-infinitesimal. In the étale case the simple group must be $\mathbb{Z}/n\mathbb{Z}$ for some prime number n. A connected multiplicative simple group is Cartier dual to an étale simple group of order p, hence μ_p.

A bi-infinitesimal simple group G must be of Frobenius height 1, with Cartier dual of Frobenius height 1. Hence Frobenius and Verschiebung kill G. Let the group homomorphism $f_v : G \to \mathbb{G}_{\mathrm{a}}$ correspond to a non-trivial tangent vector in

$$v \in \mathrm{T}_e G^D$$

as in Proposition 41. The map f_v must be injective with image contained in the kernel of Frobenius on $\mathbb{G}_{\mathrm{a}}$, hence f_v induces an injective map

$$f_v : G \to \alpha_p$$

which must be an isomorphism by comparing the order of the groups. □

Corollary 55. *The group α_p is the only simple object in the category of bi-infinitesimal finite flat group schemes over a field of characteristic p.*

Proof: The proof of Theorem 54 in the bi-infinitesimal case did not make use of the fact that the field was assumed algebraically closed. □

We conclude that the complexity of the category of finite flat group schemes comes primarily from the complexity of non-trivial extensions of α_p with itself and secondarily from monodromy via Galois action for the étale and multiplicative part.

8.6. **Classification of group schemes of order p.**

8.6.1. *Warm-up: group schemes of order 2.* References: [Ta97] §3.2 or [Sh86].

Let G be a group scheme of order 2 over R represented by A. The counit $\varepsilon : A \to R$ splits the structure map $R \to A$ so that with $I = \ker(\varepsilon)$ we have

$$A = I \oplus R,$$

and I is a line bundle on R, i.e., a projective module of rank 1. Let us assume for simplicity that I is free. Let X be a generator of I. Then there is a unique $a \in R$ with

$$A = R[X]/(X^2 - aX),$$

and a unique $b \in R$ such that the comultiplication reads

$$\Delta : R[X]/(X^2 - aX) \to R[Y,Z]/(Y^2 - aY, Z^2 - aZ)$$

$$X \mapsto \Delta(X) = Y + Z + bYZ.$$

The parameters a, b are subject to the constraint of a well defined comultiplication.

$$0 = \Delta(X^2 - aX) = (Y + Z + bYZ)^2 - a(Y + Z + bYZ)$$

$$= (a^2b^2 - ab + 2 + 4ab)YZ = (ab + 1)(ab + 2)YZ.$$

The inverse map is given by $X \mapsto cX$ for a unique $c \in R$. The constraint from $g \cdot g^{-1} = 1$ reads

$$0 = X + cX + bcX^2$$

or

$$0 = 1 + c + abc = 1 + c(1 + ab).$$

Hence $1 + ab$ is a unit and thus $ab = -2$ and $c = 1$. Associativity is satisfied automatically:

$$Y + (1 + bY)(Z + W + bZW)$$

$$= Y + Z + W + b(YZ + YW + ZW) + b^2YZW$$

$$= (Y + Z + bYZ)(1 + bW) + W.$$

The resulting group scheme represented by $R[X]/(X^2 - aX)$ with comultiplication as above is denoted by $G_{a,b}$ and exists for each factorisation $ab = -2$. Special cases are

$$G_{1,-2} = \underline{\mathbb{Z}/2\mathbb{Z}}_R, \qquad G_{-2,1} = \mu_2.$$

The Cartier dual of $G_{a,b}$ is $G_{b,a}$.

8.6.2. *The classification result by Oort and Tate.* References: [OT70].

We fix a prime number p and choose a primitive $(p-1)$-th root of unity $\zeta = \zeta_{p-1} \in \mathbb{Z}_p$. The resulting embedding $\mathbb{Z}[\zeta_{p-1}] \hookrightarrow \mathbb{Z}_p$ determines a place $\mathfrak{p}|p$ in $\mathbb{Q}(\zeta_{p-1})$. We set

$$\Lambda = \mathbb{Z}[\zeta_{p-1}, \frac{1}{p(p-1)}] \cap \mathbb{Z}_p$$

with respect to this embedding. In other words, Λ is the Dedekind ring of S-integers of $\mathbb{Q}(\zeta_{p-1})$ with S the set of all primes dividing $p(p-1)$ except $\mathfrak{p}$. The residue field at $\mathfrak{p}$ is

$$\Lambda/\mathfrak{p}\Lambda = \mathbb{F}_p.$$

We sketch the content of [OT70] which contains the classification of group schemes G of order p over a base R which is a Λ-algebra. The first result is the following theorem.

Theorem 56 ([OT70] Theorem 1). *Every finite flat R-group of order p is commutative.*

Proof: It is clearly enough to work over a local ring $(R, \mathfrak{m})$ with algebraically closed residue field. The fibre over $\mathfrak{m}$ is a group of order p over an algebraically closed field and thus one of the three choices $\mathbb{Z}/p\mathbb{Z}, \mu_p$ or α_p, see [OT70] Lemma 1. In each case, the dual Hopf algebra is again the algebra of one of $\mathbb{Z}/p\mathbb{Z}, \mu_p$ or α_p and thus is generated by one element [OT70] page 6, hence this holds also for the Hopf algebra over R by Nakayama's Lemma. But monogenic algebras are commutative, and thus the group is commutative. □

Let A be the R-algebra representing G. We can split off the augmentation ideal $I = \ker(\varepsilon)$ as $A = R \oplus I$ via the counit $\varepsilon : A \to R$ and unit $\eta : R \to A$. The multiplication action $\mathbb{Z} \to \mathrm{End}(G)$ factors over $\mathbb{F}_p$ and induces a representation of (distinguished generator ζ)

$$\mathbb{F}_p^\times = \mathbb{Z}/(p-1)\mathbb{Z}$$

on A, respecting the decomposition $A = R \oplus I$. As Λ contains the $(p-1)$th roots of unity, this action can be simultaneously diagonalized. Let

$$I = \bigoplus_\chi I_\chi$$

be the decomposition in isotypical components according to the $\mathbb{F}_p^\times$-action, e.g., by the idempotents

$$e_\chi = \frac{1}{p-1} \sum_{m \in \mathbb{F}_p^\times} \chi(m)^{-1}[m],$$

which project onto $I_\chi = e_\chi I$ because of $[m]e_j = \chi(m)e_j$. The choice of $\zeta \in \Lambda$, or more precisely the place $\mathfrak{p}$ above, determines a generator

$$\chi : \mathbb{F}_p^\times = (\Lambda/\mathfrak{p}\Lambda)^\times = \mu_{p-1}(\Lambda) \hookrightarrow \Lambda^\times$$

for the group of characters with values in Λ. We set $I_j := I_{\chi^j}$ and $e_j = e_{\chi^j}$.

Lemma 57. *The R-modules I_j are locally free of rank 1 and $I_j = I_1^{\otimes j}$ for $1 \leq j \leq p-1$.*

Proof: It is enough to consider the case where the base is an algebraically closed field k, in which case $\chi = \mathrm{id} : \mathbb{F}_p^\times \to k^\times$ and the lemma follows from the inspection of the only three cases:

(1) $\mathbb{Z}/p\mathbb{Z}$: The algebra is

$$A = \prod_{i=0}^{p-1} k = \mathrm{Maps}(\mathbb{Z}/p\mathbb{Z}, k)$$

with $\mathbb{F}_p^\times$-action by $[m]f(n) = f(mn)$. So $I_j \subseteq \mathrm{Maps}(\mathbb{Z}/p\mathbb{Z}, k)$ is generated by the continuation of χ^j on $\mathbb{F}_p^\times \subset \mathbb{Z}/p\mathbb{Z}$ by 0. The different characters are linearly independent and span $\mathrm{Maps}(\mathbb{F}_p^\times, k) \subset \mathrm{Maps}(\mathbb{Z}/p\mathbb{Z}, k)$, which is the augmentation ideal.

(2) μ_p: The algebra is

$$A = k[X]/(X^p - 1) = k[T]/T^p,$$

where $X = 1 + T$, with $\mathbb{F}_p^\times$-action by $[m](X) = X^m$. We have

$$[m](T) = (1+T)^m - 1 \equiv mT \mod I^2$$

and $I^j = (T^j)$. We compute

$$e_jT^j = \frac{1}{p-1}\sum_{m\in\mathbb{F}_p^\times} \chi(m)^{-j}[m](T^j) \equiv \frac{1}{p-1}\sum_{m\in\mathbb{F}_p^\times} \chi(m)^{-j}m^jT^j = T^j \mod (T^{j+1})$$

The element $e_jT^j \in I_j$ is nontrivial which shows I_j is locally free of rank at least and thus exactly 1. Because $(e_1T)^j \equiv T^j \mod (T^{j+1})$ we have that the image of $I_1^{\otimes j} \to I_j$ is nontrivial.

(3) α_p: The algebra is

$$A = k[X]/(X^p)$$

with $\mathbb{F}_p^\times$-action by $[m](X) = mX$. So I_j contains the nontrivial X^j which therefore generates I_j.

□

In the sequel we assume for simplicity that I_1 is free of rank 1 as an R-module, and we choose a generator $x \in I_1$. Then there is an element $a \in R$ with $A = R[X]/(X^p - a)$, where x is the image of X.

Let us examine the case of $\mu_{p,\Lambda}$ with more details. The algebra is $A = \Lambda[X]/(X^p - 1)$ and $I = \Lambda(1-X) + \dots \Lambda(1-X^{p-1})$ is the augmentation ideal. We set

$$y_j = (p-1)e_j(1-X) = \sum_{m\in\mathbb{F}_p^\times} \chi^{-j}(m)(1-X^m)$$

and get

$$\frac{1}{p-1}\sum_{j=1}^{p-1}\chi^j(m)y_j = \left(\sum_{j=1}^{p-1}\chi^j(m)e_j\right)(1-X) = \left(\sum_{j=1}^{p-1}\sum_{m\in\mathbb{F}_p^\times}[m]e_j\right)(1-X)$$
$$= \left(\sum_{j=1}^{p-1}e_j\right)(1-X^m) = 1 - X^m.$$

Consequently, we have with $y = y_1$ that $I_j = \Lambda y_j = \Lambda y^j$ and so for some uniquely defined units $w_j \in \Lambda^\times$ we get

$$y^j = w_jy_j$$

for $1 \leq j \leq p-1$. Of course $w_1 = 1$ and we set $w_0 = 1$ as well. The collection of the w_j is a partial divided power structure.

Proposition 58 ([OT70] page 9)**.** *The algebra of $\mu_{p,\Lambda}$ is $\Lambda[X]/(X^p - 1) = \Lambda[y]/(y^p - w_py)$ with*

(1) $w_p = pw_{p-1}$,
(2) $[m](y) = \chi(m)y$ *for* $m \in \mathbb{F}_p^\times$,
(3) $w_j \equiv j! \mod p$ *for* $1 \leq j \leq p-1$,
(4) $\Delta(y) = y\otimes 1 + 1\otimes y + \frac{1}{1-p}\sum_{j=1}^{p-1}\frac{y^j}{w_j}\otimes\frac{y^{p-j}}{w_{p-j}}$,
(5) $p + (1-p)X = \sum_{j=0}^{p-1}\frac{y^j}{w_j}$,
(6) $\mathrm{inv}(y) = -y$*, except for* $p = 2$ *when* $\mathrm{inv}(y) = y$.

Proof: (2) is clear and for (4) we compute

$$\Delta(y) = \Delta\left(\sum_{m\in\mathbb{F}_p^\times}\chi(m)^{-1}[m](1-X)\right) = \sum_{m\in\mathbb{F}_p^\times}\chi(m)^{-1}[m]\otimes[m]\Delta(1-X)$$
$$= \sum_{m\in\mathbb{F}_p^\times}\chi(m)^{-1}[m]\otimes[m](1-X\otimes X) = \sum_{m\in\mathbb{F}_p^\times}\chi(m)^{-1}(1-X^m\otimes X^m).$$

Hence,

$$\Delta(y) - y\otimes 1 - 1\otimes y = -\sum_{m\in\mathbb{F}_p^\times}\chi(m)^{-1}(1-X^m)\otimes(1-X^m)$$
$$= \frac{-1}{(p-1)^2}\sum_{m\in\mathbb{F}_p^\times}\chi(m)^{-1}\sum_{i,j=1}^{p-1}\chi^j(m)\chi^i(m)y_j\otimes y_i = \frac{-1}{(p-1)^2}\sum_{i,j=1}^{p-1}y_j\otimes y_i\sum_{m\in\mathbb{F}_p^\times}\chi(m)^{i+j-1}$$
$$= \frac{1}{1-p}\sum_{j=1}^{p-1}\frac{y^j}{w_j}\otimes\frac{y^{p-j}}{w_{p-j}}.$$

(5) follows from

$$1-X = \left(\sum_{j=1}^{p-1}e_j\right)(1-X) = \frac{1}{p-1}\sum_{j=1}^{p-1}y_j.$$

Modulo p we have $y^p = 0$, so

$$(\Lambda/p\Lambda[X])/(X^p-1) = (\Lambda/p\Lambda[y])/y^p.$$

Now we compare the coefficients at $y^j\otimes y$ for $1\leq j<p-1$ in

$$(\Lambda/p\Lambda[y])/(y^i\otimes y^j;\ i+j\geq p)$$

of the equation

$$\left(1+\frac{1}{1-p}\sum_{j=0}^{p-1}\frac{y^j}{w_j}\right)\otimes\left(1+\frac{1}{1-p}\sum_{j=0}^{p-1}\frac{y^j}{w_j}\right) = X\otimes X = \Delta(X) = 1+\frac{1}{1-p}\sum_{j=0}^{p-1}\frac{\Delta(y)^j}{w_j}$$
$$= 1+\frac{1}{1-p}\sum_{j=0}^{p-1}\frac{\left(y\otimes 1+1\otimes y+\frac{1}{1-p}\sum_{j=1}^{p-1}\frac{y^j}{w_j}\otimes\frac{y^{p-j}}{w_{p-j}}\right)^j}{w_j}$$

which implies

$$\frac{1}{w_j} = \frac{j+1}{w_{j+1}}$$

and shows (3). Next we show (1):

$$y^p = y(y^{p-1}) = y(w_{p-1}y_{p-1}) = yw_{p-1}\sum_{m\in\mathbb{F}_p^\times}\chi(m)^{1-p}(1-X^m) = yw_{p-1}\sum_{m\in\mathbb{F}_p^\times}(1-X^m)$$
$$= w_{p-1}(p-1)e_1(1-X)(p-1-X-X^2-\ldots-X^{p-1}) = pw_{p-1}(p-1)e_1(1-X) = w_py.$$

And now we compute the formula for the inverse

$$\mathrm{inv}(y) = (p-1)e_1\mathrm{inv}(1-X) = \sum_{m\in\mathbb{F}_p^\times}\chi^{-1}(m)(1-X^{-m}) = \chi(-1)\sum_{m\in\mathbb{F}_p^\times}\chi^{-1}(m)(1-X^m) = -y,$$

except for the case $p=2$ when $\mathrm{inv}(y)=y$. □

The examples: The description of $\mu_{p,\Lambda[U^{\pm1}]}$ with the Hopf algebra

$$A = \Lambda[U^{\pm1},y]/(y^p-w_py)$$

as above becomes after the change of variables $Y = U^{-1}y$ the presentation

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

with Hopf algebra structure determined by $\varepsilon(Y) = 0$, and $\mathrm{inv}(Y) = -Y$ for odd p and $\mathrm{inv}(Y) = Y$ for $p = 2$, and

$$\Delta(Y) = Y \otimes 1 + 1 \otimes Y + \frac{U^{p-1}}{1-p} \sum_{j=1}^{p-1} \frac{Y^j}{w_j} \otimes \frac{Y^{p-j}}{w_{p-j}}.$$

This Hopf algebra is defined over the (see below Lemma 59) subalgebra

$$R_{\mathrm{univ}} = \Lambda[A, B]/(AB - w_p) \subset \Lambda[U^{\pm 1}]$$

generated by $A = w_p U^{1-p}$ and $B = U^{p-1}$ as the universal finite flat Hopf algebra of order p by

$$A_{\mathrm{univ}} = R_{\mathrm{univ}}[Y]/(Y^p - AY)$$

via $\varepsilon(Y) = 0$, and $\mathrm{inv}(Y) = -Y$ for odd p and $\mathrm{inv}(Y) = Y$ for $p = 2$, and

$$\Delta(Y) = Y \otimes 1 + 1 \otimes Y + \frac{B}{1-p} \sum_{j=1}^{p-1} \frac{Y^j}{w_j} \otimes \frac{Y^{p-j}}{w_{p-j}}.$$

All necessary formulas hold because they hold in the algebra $A = A_{\mathrm{univ}} \otimes_{R_{\mathrm{univ}}} \Lambda[U^{\pm 1}]$. Let $a, b \in R$ be such that $ab = w_p$. The finite flat R-group $G_{a,b}$ of order p is defined as

$$G_{a,b} = \mathrm{Spec}(R[X]/(X^p - aX)),$$

$$\Delta(X) = X \otimes 1 + 1 \otimes X + \frac{b}{1-p} \sum_{i=1}^{p-1} \frac{X^i}{w_i} \otimes \frac{X^{p-i}}{w_{p-i}},$$

which is the specialisation of $G_{\mathrm{univ}} = \mathrm{Spec}(A_{\mathrm{univ}})$ by base change via $R_{\mathrm{univ}} \to R$ mapping $A \mapsto a$ and $B \mapsto b$.

Lemma 59. *The map $\Lambda[A, B]/(AB - w_p) \to \Lambda[U^{\pm 1}]$ defined by sending $A \mapsto w_p U^{1-p}$ and $B \mapsto U^{p-1}$ is injective.*

Proof: After inverting p the map becomes injective with image $\Lambda[U^{\pm(p-1)}]$. As $\Lambda[U^{\pm 1}]$ does not contain p-torsion, and by Nakayama's Lemma, it suffices to prove injectivity after base change to $\Lambda \twoheadrightarrow \Lambda/p\Lambda = \mathbb{F}_p$. The Laurent polynomials $\sum_i a_i U^{i(p-1)}$ belong to the image if and only if $a_i \in \Lambda$ for $i \geq 0$ and $a_i \in w_p^{-i}\Lambda$ for $i \leq 0$. It follows that the map

$$\Lambda[A, B]/(AB - w_p) \otimes \Lambda/p\Lambda = \mathbb{F}_p[A, B]/(AB) \to \Lambda[w_p U^{1-p}, U^{p-1}] \otimes \Lambda/p\Lambda$$

is an isomorphism. □

Theorem 60 ([OT70] page 12–15)**.** *Let R be a Λ-algebra with* $\mathrm{Pic}(R) = 0$.

(1) Any finite flat R-group G of order p is isomorphic to a group $G_{a,b}$ for some $ab = w_p$ in R.

(2) Two such groups $G_{a,b}$ and $G_{c,d}$ are isomorphic if and only if there is a unit $u \in R^\times$ such that $c = u^{p-1}a$ and $d = u^{1-p}b$.

(3) The moduli space for group schemes of order p over Λ-algebras is the Artin-stack quotient

$$\big(\mathrm{Spec}\,\Lambda[A, B]/(AB - w_p)\big)/\mathbb{G}_{\mathrm{m}},$$

where the $\mathbb{G}_{\mathrm{m}}$ action is by $u.(A, B) = (u^{p-1}A, u^{1-p}B)$.

(4) The Cartier dual to $G_{a,b}$ is the group $G_{b,a}$ with explicit formula for the pairing given by

$$R[T, T^{-1}] \to R[X]/(X^p - aX) \otimes_R R[Y]/(Y^p - bY)$$

$$T \mapsto 1 + \frac{1}{1-p} \sum_{i=1}^{p-1} \frac{(X \otimes Y)^i}{w_i}.$$

9. p-DIVISIBLE GROUPS

References: [Ta66] [Gr74].

9.1. **Definition.** A **p-divisible group** over the base $S = \operatorname{Spec}(R)$ is an inductive system

$$G = \varinjlim G_v$$

indexed by the natural numbers $v \in \mathbb{N}$ of finite flat commutative groups G_v over S such that there is a natural number h, called the **height** and such that

(i) G_v has order p^{hv}, and
(ii) for each v we have an exact sequence

$$0 \to G_v \xrightarrow{i_v} G_{v+1} \xrightarrow{[p^v]} G_{v+1}.$$

Note that $G = \varinjlim G_v$ is not a scheme but an ind-scheme, or a formal R-scheme, which we will discuss in Section §10. We treat it here as a functor of points on R-algebras

$$G : T \mapsto G(T) = \varinjlim G_v(T).$$

Because each covering in S_{fpqc} has a refinement with finite index set, the direct limit of sheaves as a presheaf, so argument-wise, is again a sheaf. Consequently, the group G can be viewed as an fpqc-sheaf. Grothendieck prefers to call p-divisible groups **Barsotti-Tate groups**.

9.1.1. *Torsion.* The composite of the i_v gives closed immersions $i_{v,t} : G_v \to G_{v+t}$ and we will frequently identify G_v with its image.

Lemma 61. *The kernel of $[p^v] : G_{v+t} \to G_{v+t}$ is the subgroup G_v. The group $G = \varinjlim G_v$ is p-primary torsion with p^v-torsion equal to $G[p^v] = G_v$.*

Proof: We prove this by induction on t, with $t = 1$ being part of the definition. Assume the lemma to be true up to t, then for $v \geq 1$ we find

$$G_{v+t+1}[p^v] = G_{v+t+1}[p^{v+t}] \cap G_{v+t+1}[p^v] = G_{v+t} \cap G_{v+t+1}[p^v] = G_{v+t}[p^v] = G_v.$$

□

9.1.2. *Homomorphisms.* A homomorphism of p-divisible group is a homomorphism of inductive systems of groups. Namely a

$$f : \varinjlim G_v \to \varinjlim H_w$$

is given by a compatible collection of

$$f_v : G_v \to H_{v+t_v}.$$

But as the levels G_v (resp. H_v) coincide with the p^v-torsion, any such f has to be automatically compatible with the indexing and the description of homomorphism simplifies to

$$\operatorname{Hom}\left(\varinjlim G_v, \varinjlim H_w\right) = \varprojlim_v \varinjlim_w \operatorname{Hom}(G_v, H_w) = \varprojlim_v \operatorname{Hom}(G_v, H_v).$$

9.1.3. *Multiplication by p.* The image of $[p^v] : G_{v+t} \to G_{v+t}$ is killed by $[p^t]$ and hence factors uniquely over a map

$$j_{v,t} : G_{v+t} \to G_t.$$

Proposition 62. *The sequence*

$$0 \to G_v \xrightarrow{i_{v,t}} G_{v+t} \xrightarrow{j_{v,t}} G_t \to 0$$

is exact.

Proof: It is left exact, because G_v is the kernel of $[p^v] = i_{t,v} \circ j_{v,t}$ with $i_{t,v}$ injective. We get an induced injective map

$$G_{v+t}/i_{v,t}(G_v) \hookrightarrow G_t$$

of finite flat S-groups of the same order p^{ht}, which must therefore be an isomorphism by the following helpful lemma. □

Lemma 63. *Let R be a Noetherian ring and M a finitely generated R-module. Then any surjective endomorphism of M is bijective.*

Proof: Let $\varphi : M \twoheadrightarrow M$ be a surjective R-module homomorphism. The sequence of submodules $M_i = \ker(\varphi^i)$ is increasing and thus stabilises. So for $i \gg 0$ we have $M_i = M_{2i}$. The map φ being surjective we find that $\varphi^i : M_i = M_{2i} \to M_i$ is surjective as well. But this map is also the 0 map, so that $M_i = (0)$, which proves that φ is in fact injective. □

Corollary 64. *Let $G = (G_v)$ be a p-divisible group. The map multiplication by p*

$$[p] : G \to G$$

or more precisely the map induced by the $j_{1,v} : G_{v+1} \to G_v$ is finite faithfully flat (fpqc) of degree $p^h = \# \ker[p]$. In particular, multiplication by p is surjective on the fpqc-sheaf defined by G.

The last property explains the name p-divisible groups. A group homomorphism $f : G \to H$ between p-divisible groups which has finite flat kernel and is surjective as map of fpqc sheaves is called an **isogeny**, the degree of which is the order of its kernel. So $[p] : G \to G$ is an isogeny of degree $\deg[p] = p^h$, where h equals the height of G.

9.2. **Examples.**

(1) The constant p-divisible group

$$G = \mathbb{Q}_p/\mathbb{Z}_p$$

with level v given by $G_v = \frac{1}{p^v}\mathbb{Z}/\mathbb{Z}$ has height $h = 1$.

(2) If a projective system (G_v) of discrete groups satisfies the axioms for p-divisible groups, then we find by induction on v that G_v is a free $\mathbb{Z}/p^v\mathbb{Z}$-module of rank h. Indeed,

$$G_v/pG_v \cong G_1$$

shows that G_v is a $\mathbb{Z}/p^v\mathbb{Z}$-module with h generators and cardinality $p^h v$. The projective system for $\operatorname{Isom}\big(G, (\mathbb{Q}_p/\mathbb{Z}_p)^h\big)$ is level-wise finite and nonempty, so that the projective limit is itself nonempty. So $G = \varinjlim G_v$ is isomorphic to

$$(\mathbb{Q}_p/\mathbb{Z}_p)^h.$$

(3) If G_1 is finite étale, then by induction all G_v are finite étale. Let S be connected with geometric point $s \in S$. The fibre G_s in s of the p-divisible group G/S is a discrete p-divisible group as in (2) and G is determined by the induced continuous representation

$$\pi_1(S, s) \to \operatorname{Aut}(G_s) \cong \operatorname{Aut}\big((\mathbb{Q}_p/\mathbb{Z}_p)^h\big) = \mathrm{GL}_h(\mathbb{Z}_p),$$

where h is the height of G.

(4) The p-divisible group

$$\mu_{p^\infty} = \mathbb{G}_\mathrm{m}[p^\infty]$$

has level groups $G_v = \mu_{p^v} = \mathbb{G}_\mathrm{m}[p^v]$ with transfer maps induced by the inclusions into $\mathbb{G}_\mathrm{m}$. The height of μ_{p^∞} is 1. The group is étale if p is invertible and then corresponds to the p-adic cyclotomic character

$$\chi : \pi_1(S, s) \to \mathbb{Z}_p^\times.$$

(5) In general, over a local henselian base $S = \operatorname{Spec}(R)$ the natural filtration on the finite levels G_v of a p-divisible group G induces the structure of p-divisible groups $G_\mu = (G_{\mu,v})$, $G^0 = (G_v^0)$, $G_{\mathrm{bi}} = (G_{\mathrm{bi},v})$ and $G^{\text{ét}} = (G_v^{\text{ét}})$ on the connected multiplicative, the connected, the bi-infinitesimal and the étale part of G. The condition on the correct group orders comes from Lagrange's theorem, Proposition 28, and exactness of the étale part (resp. the connected component, Proposition 40, and also from Cartier duality Proposition 29). We have a filtration

$$0 \subseteq G_\mu \subseteq G^0 \subseteq G$$

of p-divisible groups with quotients G_μ, G_{bi} and $G^{\text{ét}}$ respectively. If R is a perfect field, then the filtration splits canonically.

(6) **The motivating example**. Let A/S be an abelian scheme of dimension g. Then multiplication by p^v is an isogeny of A/S of degree p^{2gv}, hence the kernels $G_v = A[p^v]$ lead to a p-divisible group

$$G = A[p^\infty]$$

of height $h = 2g$. If p is invertible on S, then the associated representation is the action

$$\pi_1(S, s) \to \operatorname{Aut}(A_s[p^\infty]) = \operatorname{GL}(\mathrm{T}_p\, A_s)$$

on the p-adic Tate-module of the fibre A_s of A/S in s.

9.3. **Cartier duality.** There is a notion of the Cartier dual p-divisible group to a p-divisible group $G = (G_v)$ as follows. We set $(G^D)_v = (G_v)^D$ and use the Cartier duals of the diagram

$$\begin{tikzcd}
 & & & G_1 \arrow[dr, hook, "i_{1,v}"] & & & \\
0 \arrow[r] & G_v \arrow[r, "i_v"] & G_{v+1} \arrow[ur, two heads, "j_{v,1}"] \arrow[rr, "{[p^v]}"] & & G_{v+1} \arrow[r, "j_v=j_{1,v}"] & G_v \arrow[r] & 0
\end{tikzcd}$$

to get inclusions $j_v^D : G_v^D \to G_{v+1}^D$ with the correct properties. Note that only the layers of G and G^D are dual. There is no reasonable duality for the whole ind-groups. The Cartier dual group G^D has the same height as G.

Example 65. (1) The p-divisible groups $\mathbb{Q}_p/\mathbb{Z}_p$ and μ_{p^∞} are Cartier duals of each other.

(2) Let A/S be an abelian scheme and $A^t/S = \underline{\operatorname{Pic}}^0_{A/S}$ the dual abelian scheme. As sheaves on S_{fpqc} we find that $A^t/S = \mathscr{E}xt^1_{\mathrm{fpqc}}(A, \mathbb{G}_\mathrm{m})$, whereas $\mathscr{H}om_{\mathrm{fpqc}}(A, \mathbb{G}_\mathrm{m}) = 0$. It follows that the sheaf-Ext sequence associated to

$$0 \to A[p^v] \to A \xrightarrow{p^v} A \to 0$$

leads to

$$0 \to \mathscr{H}om(A[p^v], \mathbb{G}_\mathrm{m}) \to \mathscr{E}xt^1_{\mathrm{fpqc}}(A, \mathbb{G}_\mathrm{m}) \xrightarrow{p^v} \mathscr{E}xt^1_{\mathrm{fpqc}}(A, \mathbb{G}_\mathrm{m}) \to 0$$

which identifies canonically the Cartier dual $A[p^v]^D = A^t[p^v]$ as the torsion in the dual abelian scheme. It follows that $A[p^\infty]$ and $A^t[p^\infty]$ are Cartier dual p-divisible groups.

9.4. **Frobenius and Verschiebung.** Let $S = \operatorname{Spec}(R)$ be of characteristic $p > 0$. Frobenius and Verschiebung are natural with respect to group homomorphisms in characteristic p and thus define maps of p-divisible groups over R

$$F_G : G \to G^{(p)} \quad \text{and} \quad V_G : G^{(p)} \to G,$$

the composites of which in either way are the multiplication by p map. If follows that $\ker F_G \subseteq \ker[p] = G_1$ and $\ker V_G \subseteq \ker[p] = G_1^{(p)}$ are finite group schemes. Moreover, as multiplication by p is surjective on the corresponding fpqc-sheaves, the same holds for F_G and V_G. Over a field of characteristic $p > 0$ Frobenius and Verschiebung are thus isogenies, which are Cartier dual to each other in an appropriate sense.

10. Formal groups

References: [Sh86] [Ta66] [Fa01].

10.1. Formal functors and formal schemes. References: [De72] Chapter I.6.

Let Λ be a local complete Noetherian ring and $\mathscr{A}_\Lambda^f$ the category of finite length artinian Λ-algebras. A **Λ-formal functor** is a functor $\mathscr{F} : \mathscr{A}_\Lambda^f \to \mathscr{S}ets$.

Recall that $\mathscr{A}_\Lambda$ is the category of Λ-algebras. The **formal completion** of a functor

$$F : \mathscr{A}_\Lambda \to \mathscr{S}ets$$

is the Λ-formal functor

$$\hat{F} : \mathscr{A}_\Lambda^f \to \mathscr{S}ets$$

given by restriction of F to

$$\mathscr{A}_\Lambda^f \subset \mathscr{A}_\Lambda.$$

For $A \in \mathscr{A}_\Lambda^f$ we denote the Λ-formal functor $\widehat{\operatorname{Spec}}(A)$ by $\operatorname{Spf}(A)$. We can now give three definitions of **Λ-formal schemes**. These form a full subcategory of Λ-formal functors $\mathscr{X}$ which are the filtered direct limits $\varinjlim \operatorname{Spf}(A_i)$, or more precisely the corresponding ind-object, for a projective system $A_i \in \mathscr{A}_\Lambda^f$. Equivalently, a Λ-formal scheme is given by a pro-finite Λ-algebra $A = \varprojlim A_i$ with $A_i \in \mathscr{A}_\Lambda^f$, or more precisely the corresponding pro-system, and the Λ-formal functor

$$\operatorname{Spf}(A) = \left(R \mapsto \operatorname{Hom}(A, R) = \varinjlim \operatorname{Hom}(A_i, R)\right).$$

It is a consequence of the representability theorem of Grothendieck [Gr60], that the Λ-formal schemes are exactly the left exact Λ-formal functors, i.e., those which commute with arbitrary finite projective limits.

Let $X = \operatorname{Spec}(A)$ be a representable functor on Λ-algebras. The formal completion $\hat{X}$ is then left exact and thus representable by Grothendieck's theorem. Indeed we find

$$\hat{X} = \operatorname{Spf}(\varprojlim_{Z \subset X} \mathcal{O}_Z),$$

where the limit ranges over all closed subschemes $Z \subset X$ that are artinian and proper over Λ. Indeed, $\mathcal{O}_Z$ is an object of $\mathscr{A}_\Lambda^f$.

10.2. Formal group schemes. References: [De72] Chapter II.4.

A **Λ-formal group** is a Λ-formal scheme that enhances to a functor with values in groups. For $\operatorname{Spf}(A)$ with $A = \varprojlim A_i$ to be a formal group asks for a continuous comultiplication

$$\Delta : A \to A \hat{\otimes} A = \varprojlim A_i \otimes_\Lambda A_i,$$

a continuous inverse $\operatorname{inv} : A \to A$ and a continuous counit $\varepsilon : A \to \Lambda$. A Λ-group scheme G has a formal completion along the 0 section $\hat{G}$ that is a Λ-formal group, namely

$$\hat{G} : R \to \hat{G}(R) = \ker\left(G(R) \to G(R_{\mathrm{red}})\right)$$

for $R \in \mathscr{A}_\Lambda^f$. The connection with the formal completion above of the underlying set-valued functor $X = G$ is as follows. The completion of G at 0 is simply the connected component $\hat{G} = (\hat{X})^0$ of $0 \in X$ in the formal completion $\hat{X}$.

Example 66. (1) The formal completion $\hat{\mathbb{G}}_{\mathrm{a}}$ is represented by $\Lambda[[X]]$ with comultiplication

$$\Delta(X) = X \otimes 1 + 1 \otimes X.$$

The corresponding formal functor maps a finite length local Λ-algebra $(R, \mathfrak{m})$ to $\hat{\mathbb{G}}_{\mathrm{a}}(R) = \mathfrak{m}$ with addition as composition.

(2) The formal completion $\hat{\mathbb{G}}_{\mathrm{m}}$ is represented by $\Lambda[[X]]$ with comultiplication

$$\Delta(X) = X \otimes 1 + 1 \otimes X + X \otimes X = (1+X) \otimes (1+X) - 1.$$

The corresponding formal functor maps a finite length local Λ-algebra $(R, \mathfrak{m})$ to

$$\hat{\mathbb{G}}_{\mathrm{m}}(R) = 1 + \mathfrak{m}$$

with multiplication as composition.

(3) Let $G = (G_v)$ be a p-divisible group over Λ with $G_v = \mathrm{Spec}(A_v)$. The inclusions of G define a pro-finite projective system $A = \varprojlim A_v$ for which the comultiplications of the A_v define a comultiplication $\Delta : A \to A \hat{\otimes} A$, so that we get an associated Λ-formal group $\mathrm{Spf}(A)$.

(4) Let E/Λ be an elliptic curve. The formal completion $\hat{E}$ is represented by the completion

$$\hat{\mathcal{O}}_{E,e} \cong \Lambda[[X]].$$

(5) If Λ is a $\mathbb{Q}$-algebra, then the following holds.

Theorem 67. *Let Λ be a $\mathbb{Q}$-algebra. Then any commutative connected formal group over Λ is isomorphic to a direct sum of copies of $\hat{\mathbb{G}}_{\mathrm{a}}$, including the infinite dimensional case.*

(6) Following Theorem 67 there must be an isomorphism $\hat{\mathbb{G}}_{\mathrm{a}} \cong \hat{\mathbb{G}}_{\mathrm{m}}$ if the constants Λ are a $\mathbb{Q}$-algebra. We choose local coordinates

$$\hat{\mathbb{G}}_{\mathrm{a}} = \mathrm{Spf}\, \Lambda[[X]]$$

with $\Delta(X) = X \otimes 1 + 1 \otimes X$ and

$$\hat{\mathbb{G}}_{\mathrm{m}} = \mathrm{Spf}\, \Lambda[[Y]]$$

with $\Delta(Y) = (1+Y) \otimes (1+Y) - 1$. Then an isomorphism is is given on the functors of points by

$$\exp : \hat{\mathbb{G}}_{\mathrm{a}} \to \hat{\mathbb{G}}_{\mathrm{m}}, \quad \exp(x) = \sum_{n=0}^{\infty} \frac{1}{n!} x^n = 1 + y,$$

and on the representing algebras by

$$\exp^* : \Lambda[[Y]] \to \Lambda[[X]], \quad \exp^*(Y) = \exp(X) - 1 = \sum_{n=1}^{\infty} \frac{1}{n!} X^n,$$

and, again on the functor of points by

$$\log : \hat{\mathbb{G}}_{\mathrm{m}} \to \hat{\mathbb{G}}_{\mathrm{a}}, \quad \log(1+y) = -\sum_{n=1}^{\infty} \frac{(-1)^n}{n} y^n = x,$$

while on the representing algebras by

$$\log^* : \Lambda[[X]] \to \Lambda[[Y]], \quad \log^*(X) = \log(1+Y) = -\sum_{n=1}^{\infty} \frac{(-1)^n}{n} Y^n.$$

The usual computation shows that these are group homomorphisms:

$$\begin{aligned} \Delta(\exp^*(1+Y)) = \Delta(\exp(X)) = \exp(\Delta(X)) &= \exp(X \otimes 1 + 1 \otimes X) \\ = \exp(X) \otimes \exp(X) &= \exp^* \otimes \exp^*((1+Y) \otimes (1+Y)) \\ &= \exp^* \otimes \exp^*(\Delta(1+Y)), \end{aligned}$$

and

$$\begin{aligned} \Delta(\log^*(X)) = \Delta(\log(1+Y)) = \log(\Delta(1+Y)) &= \log((1+Y) \otimes (1+Y)) \\ = \log(1+Y) \otimes 1 + 1 \otimes \log(1+Y) &= \log^* \otimes \log^*(X \otimes 1 + 1 \otimes X) \\ &= \log^* \otimes \log^*(\Delta(X)). \end{aligned}$$

(7) The formal completion of the Witt vectors determines an infinite dimensional (or a pro-system of finite dimensional) connected formal group that plays a key role in the classification of formal groups and thus of p-divisible groups.

10.2.1. *Cartier duality revisited.* References: [De72] Chapter II.4.

The Cartier dual group functor to a group G is the functor

$$G^D : R \mapsto G^D(R) = \mathrm{Hom}_{\mathscr{G}rps}(G_R, \mathbb{G}_{\mathrm{m},R})$$

Theorem 68 ([De72] Chapter II.4)**.** *The functor $G \rightsquigarrow \hat{G^D}$ is a contravariant equivalence of categories between commutative affine Λ-groups and commutative Λ-formal groups.*

From Theorem 68 we deduce that for a field $k = \Lambda$ the commutative Λ-formal groups form an abelian category [De72] Chapter II.6.

10.2.2. *Formal Lie groups and formal group laws.* References: [De72] Chapter II.10, [Fa01].

A **formal Lie group** over Λ is a connected smooth, more precisely formally smooth, Λ-formal group. Being connected and formally smooth for $\mathscr{G} = \mathrm{Spf}(A)$ with a unit $\mathrm{Spec}(\Lambda) \hookrightarrow \mathscr{G}$ is equivalent to an isomorphism $A = \Lambda[[X_1, \ldots, X_n]]$ of pro-finite Λ-algebras. The number n is uniquely defined as the Λ-rank of the tangent space I/I^2, where I is the augmentation ideal $I = (X_1, \ldots, X_n)$, after linear shift of variables, and is called the **dimension** of $\mathscr{G}$.

Example 69. Let Λ be a field k and G/k be a reduced connected algebraic group. Then the completion $\hat{G}$ is a formal Lie group over k of dimension $\dim(G)$ as a k-variety, because reduced groups are smooth.

The group structure on $\mathrm{Spf}(A)$ is given by a map

$$\Delta : \Lambda[[X_1, \ldots, X_n]] \to \Lambda[[X_1, \ldots, X_n]] \hat{\otimes} \Lambda[[Y_1, \ldots, Y_n]] = \Lambda[[X_1, \ldots, X_n, Y_1, \ldots, Y_n]],$$

or more explicitly by a tuple of power series $\Delta(X_i) = \Phi_i(\underline{X}, \underline{Y})$ that satisfy the following axioms:

(i) $\Phi(\underline{X}, \Phi(\underline{Y}, \underline{Z})) = \Phi(\Phi(\underline{X}, \underline{Y}), \underline{Z})$,

(ii) $\Phi(\underline{X}, 0) = \underline{X} = \Phi(0, \underline{X})$.

And, if the formal Lie group is commutative, then we have also

(iii) $\Phi(\underline{X}, \underline{Y}) = \Phi(\underline{Y}, \underline{X})$.

It turns out that (i) and (ii) automatically imply the existence of an inverse map $\mathrm{inv} : A \to A$ given by power series $\mathrm{inv}_i(\underline{X})$ such that

(iv) $\Phi(\underline{X}, \mathrm{inv}(\underline{X})) = 0 = \Phi(\mathrm{inv}(\underline{X}), \underline{X})$.

Proof: We will construct tuples of power series $\lambda(\underline{X})$ and $\rho(\underline{X})$ by induction on the order, such that λ (resp. ρ) is a left (resp. right) inverse to Φ. It then follows as usual by the computation

$$\lambda(\underline{X}) = \Phi(\lambda(\underline{X}), 0) = \Phi(\lambda(\underline{X}), \Phi(\underline{X}, \rho(\underline{X})) = \Phi(\Phi(\lambda(\underline{X}), \underline{X}), \rho(\underline{X})) = \Phi(0, \rho(\underline{X})) = \rho(\underline{X})$$

that λ and ρ agree and are unique.

By symmetry it is enough to construct λ. Up to monomials of second order we have

$$\lambda(\underline{X}) = -\underline{X} + \text{ higher order terms},$$

because by (ii)

$$\Phi(\underline{X}, \underline{Y}) = \underline{X} + \underline{Y} + \text{ higher order terms}.$$

If for $m \geq 1$ we have constructed λ_m so that $\phi(\lambda_m(\underline{X}), \underline{X}) = 0$ up to an error of order higher than m. Then the next approximation is given by

$$\lambda_{m+1}(\underline{X}) = \lambda_m(\underline{X}) + \delta(\underline{X})$$

with equation for $\delta(\underline{X})$ homogeneous of degree $m+1$ given by

$$\Phi(\lambda_m(\underline{X}) + \delta(\underline{X}), \underline{X}) \equiv \Phi(\lambda_m(\underline{X}), \underline{X}) + \delta(\underline{X}) \equiv 0 \mod (X_1, \ldots, X_n)^{m+2}$$

which can be solved by

$$\delta(\underline{X}) \equiv -\Phi(\lambda_m(\underline{X}), \underline{X}) \mod (X_1, \ldots, X_n)^{m+2}$$

The left inverse λ is the well defined limit $\lim_{m\to\infty} \lambda_m \in \Lambda[[\underline{X}]]$. □

10.3. **Theorem of Serre–Tate on connected p-divisible groups.** A **p-divisible formal Lie group** is a commutative formal Lie group $\mathscr{G} = \mathrm{Spf}(\Lambda[[X_1, \ldots, X_n]])$ such that multiplication by p is a finite flat map on representing power series rings, i.e., the map

$$[p]^* : \Lambda[[X_1, \ldots, X_n]] \to \Lambda[[X_1, \ldots, X_n]]$$

makes $\Lambda[[X_1, \ldots, X_n]]$ a free module of finite rank over itself. The degree of $[p]$ is the order of the finite flat group $\ker[p]$ which is connected because it is represented by a quotient of $\Lambda[[X_1, \ldots, X_n]]$. We conclude that the degree of $[p]$ is a power of p and non-trivial at most if the residue characteristic of Λ is $p > 0$. The exponent is called the **height** of the p-divisible formal Lie group.

10.3.1. *The p-divisible group associated to a p-divisible formal Lie group.*

References: [De72] Chapter II.11, [Ta66].

Let $\mathscr{G}$ be a p-divisible formal Lie group of height h. With $[p]$ also the maps $[p^v]$ are finite flat and of degree p^{hv}, hence the kernels $G_v = \ker[p^v] = \mathscr{G}[p^v]$ form an inductive system of connected finite flat groups over Λ of order p^{hv}. Moreover, as obviously the following is exact

$$0 \to G_v \to G_{v+1} \xrightarrow{[p^v]} G_{v+1}.$$

We conclude that $\mathscr{G}_{p^\infty} = (G_v)$ is a connected p-divisible group associated to the p-divisible formal Lie group of the same height.

Theorem 70 (Serre–Tate)**.** *Let Λ be a local complete Noetherian ring with residue characteristic $p > 0$.*

The functor $\mathscr{G} \rightsquigarrow \mathscr{G}_{p^\infty}$ is an equivalence of categories between p-divisible formal Lie groups over Λ and connected p-divisible groups over Λ.

As an example we stress that $\hat{\mathbb{G}}_{\mathrm{m}}$ corresponds to $\hat{\mathbb{G}}_{\mathrm{m},p^\infty} = \mu_{p^\infty}$ and that on representing algebras we have with $T = 1 + X$

$$\varprojlim_n \Lambda[T]/(T^{p^n} - 1) = \varprojlim_n \Lambda[X]/(p^n X + \ldots + X^{p^n}) = \Lambda[[X]],$$

the analogue of which for an arbitrary connected p-divisible group we will encounter below in the proof.

Proof: Let $\mathscr{G} = \mathrm{Spf}(\Lambda[[X_1, \ldots, X_n]])$ be a p-divisible formal Lie group. Let $\mathfrak{m}$ be the maximal ideal of Λ, so that with the augmentation ideal $I = (X_1, \ldots, X_n)$ the maximal ideal of $A = \Lambda[[X_1, \ldots, X_n]]$ is $M = \mathfrak{m}A + I$.

The algebra A_v for the subgroup $G_v = \mathscr{G}[p^v]$ is $A_v = A/[p]^v(I)$, which is finite flat over Λ and thus $\mathfrak{m}$-adically complete. Moreover, the algebra $A/([p]^v(I) + \mathfrak{m}^i) = A_v/\mathfrak{m}^i A_v$ is local artinian and so for $w \gg 0$ we find $M^w \subset ([p]^v(I) + \mathfrak{m}^i)$. We have furthermore

$$[p](X_i) = pX_i + \text{ higher order terms},$$

hence

$$[p](I) \subseteq pI + I^2 \subseteq MI,$$

by induction $[p]^v(I) \subseteq M^v I$ and so $[p]^v(I)$ tends M-adically to 0. We conclude that the natural map $A \to \varprojlim A_v$ is in fact an isomorphism because

$$A = \varprojlim_w A/M^w = \varprojlim_{v,i} A/([p]^v(I) + \mathfrak{m}^i) = \varprojlim_{v,i} A_v/\mathfrak{m}^i A_v = \varprojlim_v A_v.$$

It follows that $\mathscr{G} \rightsquigarrow \mathscr{G}_{p^\infty}$ is fully faithful:

$$\mathrm{Hom}_\Lambda(\mathscr{G},\mathscr{G}') = \mathrm{Hom}_{\Lambda-\mathrm{Hopf}}(A',A) = \varprojlim \mathrm{Hom}_{\Lambda-\mathrm{Hopf}}(A'_v,A_v) = \mathrm{Hom}_\Lambda(\mathscr{G}_{p^\infty},\mathscr{G}'_{p^\infty}).$$

It remains to construct for each connected p-divisible group $G=(G_v)$ a p-divisible formal Lie group $\mathscr{G}$ with $\mathscr{G}_{p^\infty}=(G_v)$. In example 66(3) we have constructed a formal group $\mathscr{G}$ associated to (G_v). Once we can show that $\mathscr{G}$ is smooth and connected, i.e., that $\mathscr{G} = \mathrm{Spf}\,\Lambda[[X_1,\dots,X_n]]$, we are done. The map $[p]:\mathscr{G}\to\mathscr{G}$ is the direct limit of the maps

$$G_{v+1} \xrightarrow{j_v} G_v,$$

hence surjective with finite flat kernel $\mathscr{G}[p]=G_1$, so that $\mathscr{G}$ is a p-divisible commutative formal Lie group. Moreover, $\mathscr{G}[p^v]=G_v$ so that $\mathscr{G}_{p^\infty}=(G_v)$.

Let A_v be the local Λ-algebra representing G_v and $A=\varprojlim A_v$ the local Λ-algebra formally representing $\mathscr{G}=\mathrm{Spf}(A)$. As each A_v is finite flat over Λ we get that $\varprojlim A_v$ is a surjective system of free Λ-modules of finite rank. Therefore $\varprojlim A_v \cong \prod_{n\in\mathbb{N}}\Lambda \cong \Lambda[[T]]$ as a Λ-module. We conclude that A is Λ-flat, and that a continuous homomorphism

$$f \;:\; \Lambda[[X_1,\dots,X_n]] \to A \tag{10.1}$$

which is an isomorphism mod $\mathfrak{m}\subset\Lambda$ must be an isomorphism itself. Indeed, the projection

$$\mathrm{pr}_v \;:\; \Lambda[[X_1,\dots,X_n]] \to A_v$$

induced by f is then surjective by Nakayama's Lemma for the local Λ-algebra A_v. Let $I=(X_1,\dots,X_n)$ be the augmentation ideal of $\Lambda[[X_1,\dots,X_n]]$, let $\mathfrak{a}_{i,j}$ be the ideal

$$\mathfrak{m}^i\Lambda[[X_1,\dots,X_n]]+I^j$$

and set $\mathfrak{a}_v=\ker(\mathrm{pr}_v)$. Then the short exact sequence of systems of Λ-modules of finite length

$$0\to\big((\mathfrak{a}_{i,j}+\mathfrak{a}_v)/\mathfrak{a}_{i,j}\big)_{i,j,v}\to\big(\Lambda[[X_1,\dots,X_n]]/\mathfrak{a}_{i,j}\big)_{i,j,v}\to\big(A_v/\mathfrak{a}_{i,j}A_v\big)_{i,j,v}\to 0$$

over the index system $(i,j,v)\in\mathbb{N}^3$, which has a cofinal index system isomorphic to $\mathbb{N}$ with its natural ordering, so that the theory of the Mittag-Leffler condition applies, remains exact after performing the projective limit. We deduce that f which is nothing but

$$\Lambda[[X_1,\dots,X_n]] = \varprojlim_{i,j,v}\Lambda[[X_1,\dots,X_n]]/\mathfrak{a}_{i,j} \twoheadrightarrow \varprojlim_{i,j,v} A_v/\mathfrak{a}_{i,j}A_v = \varprojlim_v A_v = A$$

is surjective. Then due to Λ-flatness of A

$$\ker(f)/\mathfrak{m}\ker(f) = \ker(f \mod \mathfrak{m}),$$

and again Nakayama's Lemma for the $\Lambda[[X_1,\dots,X_n]]$-module $\ker(f)$ shows that $\ker(f)=(0)$. We thus may assume that $\Lambda=k$ is a field of characteristic p, because an isomorphism

$$\overline{f} \;:\; k[[X_1,\dots,X_n]] \to A/\mathfrak{m}A = \varprojlim_v A_v/\mathfrak{m}A_v$$

lifts to a morphism f as in (10.1).

We define $H_v=\ker(F^v : G_t\to G_t^{(p^v)})$ for $t\gg 0$. Because of $V^v\circ F^v=[p^v]$ we find $H_v\subset G_v$ as a closed subgroup independent of t. Conversely, $G_v\subset H_w$ for $w\gg 0$ because G_v is of finite Frobenius height. We conclude that $A=\varprojlim A_v=\varprojlim B_v$ where $H_v=\mathrm{Spec}\,B_v$.

Let I_v be the augmentation ideal of B_v and fix elements $X_1,\dots,X_n\in I=\varprojlim I_v$ such that the images form a basis of I_1/I_1^2. As

$$0\to H_1\to H_v\xrightarrow{F} H_v^{(p)}$$

is exact for $v\geq 1$, we find $I_1=I_v \mod I_v^p$ and thus $I_v/I_v^2\to I_1/I_1^2$ is an isomorphism. We deduce that the images of the $X_1,\dots,X_n$ in I_v generate the augmentation ideal $I_v\subset B_v$ for each v. The map

$$k[[X_1,\dots,X_n]]\to\varprojlim B_v = A$$

defined by the X_i is the projective limit of the corresponding surjective maps

$$k[[X_1,\ldots,X_n]]/(X_i^{p^v};\ 1\leq i\leq n)\twoheadrightarrow B_v.$$

It remains to prove that

$$\#H_v=\dim_k B_v \quad \text{equals} \quad p^{nv}=\dim_k k[[X_1,\ldots,X_n]]/(X_i^{p^v};\ 1\leq i\leq n).$$

By the structure theory of finite flat groups of Frobenius height 1, Proposition 48, we have $\#H_1=\dim_k B_1=p^n$ and we only need to show that

$$0\to H_1\to H_v\xrightarrow{F} H_{v-1}^{(p)}\to 0 \tag{10.2}$$

is exact in order to conclude by induction on v; note that $\#H_v=\#H_v^{(p)}=\#\big(H^{(p)}\big)_v$. The multiplication by p map $[p]:G^{(p)}\to G^{(p)}$ for the Frobenius twisted p-divisible group $G^{(p)}$ is surjective as a map of fpqc sheaves. From $[p]=F\circ V$ we deduce that also $F:G\to G^{(p)}$ is surjective as a map of fpqc sheaves. Consequently, the map $F:H_v\to H_{v-1}^{(p)}$ is surjective as map of fpqc-sheaves, and (10.2) is exact, which concludes the proof of the theorem. □

Example 71. Let A/Λ be a smooth connected commutative algebraic group. The completion $\hat{A}$ is a formal Lie group over Λ of dimension $\dim(A)$. If the multiplication by p map $[p]:A\to A$ is finite flat, then $\hat{A}$ is a p-divisible formal Lie group of dimension $\dim(A)$ and height h with p^h equal to the order of $(\ker[p])^0$.

(1) $A=\mathbb{G}_{\mathrm{a}}$, then $[p]:\mathbb{G}_{\mathrm{a}}\to\mathbb{G}_{\mathrm{a}}$ is the zero map in the special fibre and thus neither finite nor flat.
(2) $A=\mathbb{G}_{\mathrm{m}}$, then $[p]:\mathbb{G}_{\mathrm{m}}\to\mathbb{G}_{\mathrm{m}}$ is finite flat and $\hat{\mathbb{G}}_{\mathrm{m}}$ is a p-divisible formal Lie group of dimension 1 and height $h=1$. Multiplication by p is given by $X\mapsto(1+X)^p-1$ with respect to the standard coordinate $X\in\Lambda[[X]]$ with $\Delta(X)=(1+X)\otimes(1+X)-1$.
(3) $A=E$ an elliptic curve over Λ. Then $[p]:E\to E$ is finite flat of degree p^2, so $\hat{E}$ is a p-divisible formal Lie group of dimension 1. The connected component of $\hat{E}$ is of height 1 if E has ordinary reduction, and is of height 2 if E has supersingular reduction.

10.3.2. *Dimension of a p-divisible group.* The **dimension** of a p-divisible group G is the dimension of the formal Lie group associated to the connected component G^0. It follows from the proof of Theorem 70 that for a p-divisible group over a field k of characteristic $p>0$ the dimension computes as

$$\dim(G)=\dim(G^0)=\log_p\#\ker\left(F_{G^0[p]\otimes_\Lambda k}\right)=\log_p\#\ker\left(F_{G\otimes_\Lambda k}\right).$$

The last equality comes from the fact that the kernel of Frobenius is connected and contained in the p-torsion, see Proposition 53.

Theorem 72. *Let G be a p-divisible group over a local henselian ring R with residue characteristic $p>0$. Then we have*

$$\dim G+\dim G^D=\mathrm{height}(G).$$

Proof: The numerical invariants only depend on the closed fibre of G. We may thus assume that $R=k$ is a field of characteristic $p>0$. Because $V_G\circ F_G=[p]$ and because F_G is surjective, we have a short exact sequence of finite flat k-group schemes

$$0\to\ker F_G\to\ker[p]\xrightarrow{F}\ker V_G\to 0.$$

The order of $\ker[p]=G_1$ is p^h where $h=\mathrm{height}(G)$. The order of $\ker F_G$ equals $p^{\dim(G)}$. As $F_GV_G=[p]$ we have $\ker V_G=\ker V_{G_1}$ and an exact sequence

$$0\to\ker V_G\to G_1\xrightarrow{V_{G_1}} G_1\to\operatorname{coker}V_{G_1}\to 0.$$

Thus the order of $\ker V_G$ is

$$\#\ker V_G = \#\operatorname{coker} V_{G_1} = \#\ker F_{G_1^D} = \#\ker F_{G^D} = p^{\dim(G^D)}$$

which proves the theorem. □

Example 73. The p-divisible group $\mathbb{G}_{\mathrm{m}}[p^\infty] = \mu_{p^\infty}$ is of height 1 and dimension 1 and has Cartier dual $\mathbb{Q}_p/\mathbb{Z}_p$ of height 1 and dimension 0.

10.4. **Application: Local class field theory via the Lubin–Tate formal group.**

References: [Fa01]

10.4.1. *Lubin–Tate formal groups.* Let K be a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_q((X))$, let

$$\mathfrak{O} = \mathfrak{O}_K \subset K$$

be the ring of integers with uniformiser π, residue class field $\mathfrak{O}/\pi\mathfrak{O} = \mathbb{F}_q$ of cardinality q.

Theorem 74. *There is a unique connected commutative formal Lie group $\mathscr{G}_\pi = \operatorname{Spf}\mathfrak{O}[[T]]$ of dimension 1 over $\mathfrak{O}$ such that $T \mapsto \pi T + T^q$ is an endomorphism of $\mathscr{G}_\pi$. For any $\alpha \in \mathfrak{O}$ there is a unique endomorphism $[\alpha] : \mathscr{G} \to \mathscr{G}$ such that*

$$[\alpha](T) = \alpha T + \textit{ higher order.}$$

The endomorphism $[\pi]$ is the endomorphism $T \mapsto \pi T + T^q$ required in the definition of $\mathscr{G}_\pi$.

Proof: Step 1: The equation for $F \in K[[X,Y]]$

$$F(\pi X + X^q, \pi Y + Y^q) = \pi F(X,Y) + F(X,Y)^q \tag{10.3}$$

has a unique solution of the form $F(X,Y) = X + Y +$ higher order. Indeed, $F_2(X,Y) = X + Y$ is a solution modulo quadratic terms. Let F_n be a solution modulo terms of order $\geq n$, and let $F = F_n + \delta$, with δ homogeneous of degree n, be an Ansatz for a solution F_{n+1} modulo terms of order $\geq n+1$. Then the condition on δ is

$$(F_n + \delta)(\pi X + X^q, \pi Y + Y^q) \equiv \pi(F_n + \delta)(X,Y) + \big(F_n + \delta\big)^q(X,Y) \mod (X,Y)^{n+1}$$

or

$$F_n(\pi X + X^q, \pi Y + Y^q) - \big(\pi F_n(X,Y) + F_n(X,Y)^q\big) \equiv (\pi - \pi^n)\delta(X,Y) \mod (X,Y)^{n+1}$$

which has a unique solution $\delta \in K[[X,Y]]$ that is homogeneous of degree n, because $\pi \neq \pi^n$ for $n \geq 2$ and because

$$F_n(\pi X + X^q, \pi Y + Y^q) - \big(\pi F_n(X,Y) + F_n(X,Y)^q\big) \in (X,Y)^n.$$

Step 2: The formal multiplication F is commutative. Indeed, $F(Y,X)$ also solves (10.3), thus $F(X,Y) = F(Y,X)$.

Step 3: The solution F from step 1 is a power series in $\mathfrak{O}[[X,Y]]$. Let $F = \sum_{n=1}^\infty F_n$ be the decomposition of F with respect to the total degree of its monomials. The linear coefficients of F_1 are $1 \in \mathfrak{O}$. Let us assume that all coefficients of F_i for $i < n$ are in $\mathfrak{O}$. Then modulo $\pi\mathfrak{O}[[X,Y]] + (X,Y)^{n+1}$ we have in (10.3)

$$\sum_{i=1}^{n-1} F_i(X^q, Y^q) + \pi^n F_n(X,Y) \equiv F(X^q,Y^q) + F_n(\pi X, \pi Y) \equiv F(\pi X + X^q, \pi Y + Y^q)$$

$$= \pi F(X,Y) + F(X,Y)^q \equiv \pi F_n(X,Y) + F(X,Y)^q \equiv \pi F_n(X,Y) + \left(\sum_{i=1}^{n-1} F_i(X,Y)\right)^q$$

which implies

$$(\pi^n - \pi)F_n(X,Y) \equiv \left(\sum_{i=1}^{n-1} F_i(X,Y)\right)^q - \sum_{i=1}^{n-1} F_i(X^q,Y^q) \equiv 0,$$

because the last identity holds in $\mathfrak{O}/\pi\mathfrak{O}[[X,Y]]$. Thus

$$F_n \in \frac{1}{\pi^n - \pi}\pi\mathfrak{O}[[X,Y]] = \mathfrak{O}[[X,Y]].$$

Step 4: The formal multiplication F is associative. As in step 1 we can see that the equation in $K[[X,Y,Z]]$

$$G([\pi](X),[\pi](Y),[\pi](Z) = [\pi]\big(G(X,Y,Z)\big)$$

has a unique solution, namely $F(X,F(Y,Z))$ and $F(F(X,Y),Z)$ which must therefore agree. The formal group $\mathscr{G}_\pi$ is now defined using the formal group law given by F.

Step 5: For $\alpha \in \mathfrak{O}$ there is a unique solution $[\alpha](T) = \alpha T + \ldots \in \mathfrak{O}[[T]]$ for

$$[\alpha](\pi T + T^q) = \pi[\alpha](T) + \big([\alpha](T)\big)^q.$$

This follows by induction on the degree word by word as in step 1 and 3.

Step 6: For $\alpha, \beta \in \mathfrak{O}$ we have $[\alpha]([\beta](T)) = [\alpha\beta](T)$. Indeed, $[\alpha]([\beta](T))$ solves the correct equation

$$[\alpha\beta]([\pi](T)) = [\pi]\big([\alpha\beta](T)\big)$$

and starts with the correct linear term.

Step 6: The power series $[\alpha](T)$ defines an endomorphism of $\mathscr{G}_\pi$.

Clearly $[\pi]$ is an endomorphism of $\mathscr{G}_\pi$. Every α can be written as a $\alpha = u\pi^n$ for some $n \in \mathbb{N}$ and a unit $u \in \mathfrak{O}^\times$. So it remains to check the case of $\alpha = u$. Let v be the inverse of u. Because $[1](T) = (T)$ and by step 5 we find $[u]([v](T)) = T$. The power series $[v](F([u](X),[u](Y)))$ solves (10.3) because

$$[v]F([u][\pi](X),[u][\pi](Y)) = [v]F([\pi][u](X),[\pi][u](Y)) = [v][\pi]F([u](X),[u](Y))$$

$$= [\pi]\big([v](F([u](X),[u](Y)))\big)$$

with the correct linear terms, hence agrees with F. On applying $[u]$ we find that $[u]$ is in fact an endomorphism of $\mathscr{G}_\pi$.

Step 7: The map $\alpha \mapsto [\alpha]$ is an injection of rings $\mathfrak{O} \to \operatorname{End}(\mathscr{G}_\pi)$. The map is injective as the evaluation in linear order shows. The map is multiplicative by step 6 and additive because addition in $\operatorname{End}(\mathscr{G}_\pi)$ is defined via

$$([\alpha]+[\beta])(T) = F([\alpha](T),[\beta](T))$$

which solves

$$[\pi]F([\alpha](T),[\beta](T)) = F([\pi][\alpha](T),[\pi][\beta](T)) = F([\alpha][\pi](T),[\beta][\pi](T)) = F([\alpha],[\beta])\big([\pi](T)\big)$$

with the correct linear term $(\alpha+\beta)T + \ldots$ which determines $[\alpha+\beta]$ uniquely. □

A **Lubin–Tate formal group** is a formal group of the form $\mathscr{G}_\pi$ as in Theorem 74. With this definition $\hat{\mathbb{G}}_{\mathrm{m}}$ is not a Lubin-Tate group. But note that when $K = \mathbb{Q}_p$ is we can pick $\pi = p$ and find an isomorphisms of formal groups

$$\hat{\mathbb{G}}_{\mathrm{m}} = \mathscr{G}_p$$

$$X \mapsto X + \text{ higher order}$$

by the method of inductively approximating up to higher and higher order. The Lubin–Tate formal group $\mathscr{G}_p/\mathbb{Z}_p$ comes equipped with a $\mathbb{Z}_p$-action that extends the action on the tangent space, while $\hat{\mathbb{G}}_{\mathrm{m}}$ a priori is not equipped with this extra structure.

Proposition 75. *Let $K/\mathbb{Q}_p$ be a finite extension. The Lubin–Tate formal group $\mathscr{G}_\pi$ over $\mathfrak{O}_K$ is a p-divisible commutative formal Lie group of height $[K:\mathbb{Q}_p]$.*

Proof: The map $[\pi] : \mathscr{G}_\pi \to \mathscr{G}_\pi$ is finite flat of rank q being given by

$$\mathfrak{O}[[X]] \xrightarrow{X \mapsto \pi X + X^q} \mathfrak{O}[[X]].$$

In K we can factor $p = \pi^e \cdot u$ with a unit u. As $[u]$ is an automorphism, the map $[p]$ is finite flat of rank

$$q^e = \#\mathfrak{O}/p\mathfrak{O} = p^{[K:\mathbb{Q}_p]}.$$

□

Proposition 76. *Let $K/\mathbb{Q}_p$ be a finite extension. The Lubin–Tate formal group $\mathscr{G}_\pi = \operatorname{Spf} \mathfrak{O}_K[[T]]$ over $\mathfrak{O}_K$ becomes isomorphic to $\hat{\mathbb{G}}_{\mathrm{a}} = \operatorname{Spf} K[[X]]$ when restricted to K as formal groups with $\mathfrak{O}_K$-action, i.e., there is a logarithm*

$$\log_{\mathscr{G}_\pi} : \mathscr{G}_\pi \hat{\otimes} K \to \hat{\mathbb{G}}_{\mathrm{a},K}$$

corresponding to

$$\log^*_{\mathscr{G}_\pi} : K[[X]] \to K[[T]], \quad X \mapsto \log_{\mathscr{G}_\pi}(T) = T + \dots$$

with

$$\log_{\mathscr{G}_\pi}(T) + \log_{\mathscr{G}_\pi}(S) = \log_{\mathscr{G}_\pi}(F(T,S))$$

and for every $\alpha \in \mathfrak{O}_K$

$$\log_{\mathscr{G}_\pi}([\alpha](T)) = \alpha \log_{\mathscr{G}_\pi}(T).$$

Proof: The logarithm is uniquely determined by the requirement of

$$\log_{\mathscr{G}_\pi}(\pi T + T^q) = \pi \log_{\mathscr{G}_\pi}(T).$$

This is evident modulo quadratic terms and if $\ell_n(T)$ solves for oder $< n$, then the correction $\delta \in K$ for which $\ell_n(T) + \delta T^n$ solves for order $\leq n$ must satisfy the equation

$$\ell_n(\pi T + T^q) - \pi \ell_n(T) \equiv \delta(\pi - \pi^n) T^n \mod (T^{n+1})$$

which has a unique solution $\delta \in K$. The rest follows as in the proof of Theorem 74. □

10.4.2. *Dependence on π.* We keep the notation as above and assume from now on that K is a finite extension of $\mathbb{Q}_p$. Let $\mathfrak{O}^{\mathrm{nr}}$ be the p-adic completion of the integers in the maximal unramified extension of K. We have $\mathfrak{O}^{\mathrm{nr}}/\pi\mathfrak{O}^{\mathrm{nr}} = \mathbb{F}_q^{\mathrm{alg}}$ is an algebraic closure of $\mathbb{F}_q = \mathfrak{O}/\pi\mathfrak{O}$.

Proposition 77. *Let π', π be uniformisers of $\mathfrak{O}$ and let $v \in \mathfrak{O}^\times$ with $\pi' = v\pi$.*

(1) There is a unit $u \in \mathfrak{O}^{\mathrm{nr},\times}$ with $\sigma(u) = vu$, where σ is the Frobenius map of $\mathfrak{O}^{\mathrm{nr}}$.

(2) Over $\mathfrak{O}^{\mathrm{nr}}$ there is an isomorphism

$$\mathscr{G}_\pi \to \mathscr{G}_{\pi'}, \quad T \mapsto uT + \dots$$

with u as in (1).

Proof: Step 1: We first prove (1) by π-adic approximation. Modulo $\pi\mathfrak{O}^{\mathrm{nr}}$ the equation reads

$$\overline{u}^q = \overline{uv}$$

which admits a non-zero solution in $\mathfrak{O}^{\mathrm{nr}}/\pi\mathfrak{O}^{\mathrm{nr}} = \mathbb{F}_q^{\mathrm{alg}}$. If $u_n \in \mathfrak{O}^{\mathrm{nr},\times}$ solves modulo $\pi^n\mathfrak{O}^{\mathrm{nr}}$, then the equation for the correction $\delta \in \mathfrak{O}^{\mathrm{nr}}$ that $u_{n+1} = u_n + \delta\pi^n$ solves modulo $\pi^{n+1}\mathfrak{O}^{\mathrm{nr}}$ is

$$\sigma(u_n + \delta\pi^n) \equiv (u_n + \delta\pi^n)v \mod 1 + \pi^{n+1}\mathfrak{O}^{\mathrm{nr}}$$

which yields

$$\frac{\sigma(u_n)}{u_n v} \equiv \frac{1 + \frac{\delta}{u_n}\pi^n}{\sigma(1 + \frac{\delta}{u_n}\pi^n)} \equiv \frac{1 + \frac{\delta}{u_n}\pi^n}{1 + (\frac{\delta}{u_n})^q \pi^n} \equiv 1 + \frac{\delta}{u_n}\pi^n - (\frac{\delta}{u_n})^q \pi^n \mod 1 + \pi^{n+1}\mathfrak{O}^{\mathrm{nr}}.$$

This yields the following equation for δ:

$$\delta^q - v\delta \equiv u_n^q \frac{1 - \frac{\sigma(u_n)}{u_n v}}{\pi^n} \mod \pi\mathfrak{O}^{\mathrm{nr}}$$

which again admits a solution because the residue field of $\mathfrak{O}^{\mathrm{nr}}$ is algebraically closed.

Step 2: We deduce from Proposition 76 and Theorem 74 that over $K^{\mathrm{nr}} = \mathfrak{O}^{\mathrm{nr}}[\frac{1}{\pi}]$ there is a unique isomorphism

$$g : \mathscr{G}_\pi \hat{\otimes} K^{\mathrm{nr}} \xrightarrow{\sim} \hat{\mathbb{G}}_{\mathrm{a}} \xrightarrow{\sim} \mathscr{G}_{\pi'} \hat{\otimes} K^{\mathrm{nr}}$$

that is $\mathfrak{O}_K$ linear and in the standard coordinates is given by $T \mapsto g(T) = uT + \ldots$.

Step 3: The isomorphism g has integral coefficients, i.e., $g \in \mathfrak{O}^{\mathrm{nr}}[[T]]$. By construction we have a commutative diagram

$$\begin{tikzcd}
\mathscr{G}_\pi \hat{\otimes} K^{\mathrm{nr}} \arrow[r, "g"] \arrow[d, "\log_{\mathscr{G}_\pi}"'] & \mathscr{G}_{\pi'} \hat{\otimes} K^{\mathrm{nr}} \arrow[d, "\log_{\mathscr{G}_{\pi'}}"] \\
\hat{\mathbb{G}}_{\mathrm{a},K^{\mathrm{nr}}} \arrow[r, "{[u]}"] & \hat{\mathbb{G}}_{\mathrm{a},K^{\mathrm{nr}}} .
\end{tikzcd}$$

As the logarithms are defined over K we find ${}^\sigma g = (\log_{\mathscr{G}_{\pi'}})^{-1}[\sigma(u)] \log_{\mathscr{G}_\pi}$, where ${}^\sigma g$ is the power series g with σ applied to the coefficients. It follows that

$${}^\sigma g = g \circ [v]_\pi .$$

The index π in $[v]_\pi$ reminds us that the corresponding power series realises the $\mathfrak{O}_K$-action on $\mathscr{G}_\pi$. We conclude that

$$[\pi']_{\pi'} \circ g = g \circ [\pi']_\pi = g \circ [v]_\pi \circ [\pi]_\pi = \ {}^\sigma g \circ [\pi]_\pi$$

which means that g satisfies the functional equation

$$\pi' g(T) + g(T)^q = \ {}^\sigma g(\pi T + T^q). \tag{10.4}$$

Now we argue by induction on the order that g has coefficients in $\mathfrak{O}^{\mathrm{nr}}$. Let $g = \sum_{n \geq 1} a_n T^n$ then $a_1 = u \in \mathfrak{O}^{\mathrm{nr}}$ and if $a_i \in \mathfrak{O}^{\mathrm{nr}}$ for $i < n$ we look at (10.4) modulo $\pi \mathfrak{O}^{\mathrm{nr}} = \pi' \mathfrak{O}^{\mathrm{nr}}$ and (T^{n+1}) to obtain

$$\pi' a_n T^n + \left(\sum_{i=1}^{n-1} a_i T^i \right)^q \equiv \sigma(a_n) \pi^n T^n + \sum_{i=1}^{n-1} \sigma(a_i) T^{iq}$$

Hence

$$a_n \pi' - \sigma(a_n) \pi^n = a_n (\pi' - \frac{\sigma(a_n)}{a_n} \pi^n) \in \pi \mathfrak{O}^{\mathrm{nr}}$$

which means $a_n \in \mathfrak{O}^{\mathrm{nr}}$.

Step 4: The morphism g is an isomorphism

$$\mathscr{G}_\pi \hat{\otimes} \mathfrak{O}^{\mathrm{nr}} \cong \mathscr{G}_{\pi'} \hat{\otimes} \mathfrak{O}^{\mathrm{nr}}.$$

This follows because g has an invertible linear term. □

10.4.3. *Torsion points of Lubin–Tate groups.* The multiplication map $[\pi] : \mathscr{G}_\pi \to \mathscr{G}_\pi$ is finite flat of order q, hence the kernel $\mathscr{G}_\pi[\pi^v]$ of multiplication by π^v is a finite flat group over $\mathfrak{O}_K$ of order q^v. The π-adic Tate-module of $\mathscr{G}_\pi$ is

$$\mathrm{T}_\pi \mathscr{G}_\pi = \varprojlim_v \mathscr{G}_\pi[\pi^v](K^{\mathrm{alg}})$$

with transfer maps given by multiplication by $[\pi]$. The group $\mathrm{T}_\pi = \mathrm{T}_\pi \mathscr{G}_\pi$ has an $\mathfrak{O}_K$-module structure by functoriality and carries an $\mathfrak{O}_K$-linear Gal_K-action.

As an $\mathfrak{O}_K$-module T_π is free of rank 1. Indeed, the transfer maps are surjective and

$$\# \mathscr{G}_\pi[\pi^v](K^{\mathrm{alg}}) = \# \mathfrak{O}_K / \pi^v \mathfrak{O}$$

so that T_π is pro-finite, hence a finitely generated $\mathfrak{O}_K$-module with $\mathrm{T}_\pi / \pi \, \mathrm{T}_\pi = \mathscr{G}_\pi[\pi](K^{\mathrm{alg}}) \cong \mathbb{F}_q = \mathfrak{O}_K / \pi \mathfrak{O}_K$. So by Nakayama we have a surjection $\mathfrak{O}_K \twoheadrightarrow \mathrm{T}_\pi$ which must be an isomorphism by the counting argument above. We deduce that the Galois action gives a representation, or rather a character,

$$\chi_\pi : \mathrm{Gal}_K \to \mathrm{GL}(\mathrm{T}_\pi) = \mathrm{GL}_1(\mathfrak{O}_K) = \mathfrak{O}_K^\times.$$

Lemma 78. *The character χ_π is surjective.*

Proof: The $[\pi]$ torsion is given by solutions of $\pi T + T^q = 0$, hence by $t = 0$ and $(q-1)^{\mathrm{th}}$ roots of $-\pi$. Let x_1 be a non-trivial $[\pi]$-torsion point. Then $K(x_1)/K$ is totally but tamely ramified of degree $q-1$.

We construct inductively $[\pi^v]$-torsion points x_v such that x_v solves $\pi T + T^q = x_{v-1}$. This is an Eisenstein equation over $K(x_{v-1})$, hence irreducible and $K(x_v)/K$ is totally ramified of degree $q^{v-1}(q-1) = \#(\mathfrak{O}_K/\pi^v\mathfrak{O}_K)^\times$.

The Galois action on $\mathscr{G}_\pi[\pi^v](K^{\mathrm{alg}})$ is via χ_π modulo $\pi^v\mathfrak{O}$ through a group of order at most $[K(x_v) : K]$. Hence we must have equality and χ_π is surjective. □

10.4.4. *Local class field theory.* The surjective character χ_π realises a totally ramified abelian extension of K with Galois group $\mathfrak{O}_K^\times$. Local class field theory constructs a reciprocity map $\mathrm{rec}_K : K^\times \to \mathrm{Gal}_K^{\mathrm{ab}}$ with dense image that fits in a diagram

$$\begin{tikzcd}
1 \arrow[r] & \mathfrak{O}_K^\times \arrow[r] \arrow[d] & K^\times \arrow[r, "\nu"] \arrow[d, "\mathrm{rec}_K"] & \mathbb{Z} \arrow[r] \arrow[d, "1\mapsto\mathrm{Frob}_q"] & 1 \\
1 \arrow[r] & I_{K^{\mathrm{ab}}/K} \arrow[r] & \mathrm{Gal}_K^{\mathrm{ab}} \arrow[r, "\mathrm{pr}"] & \mathrm{Gal}_{\mathbb{F}_q} \arrow[r] & 1.
\end{tikzcd}$$

The composite

$$\chi_\pi \circ \mathrm{rec}_K|_{\mathfrak{O}_K^\times} : \mathfrak{O}_K^\times \to \mathfrak{O}_K^\times$$

is therefore surjective and thus even an isomorphism.

Corollary 79 (local existence result)**.** *The reciprocity map* $\mathrm{rec}_K : K^\times \to \mathrm{Gal}_K^{\mathrm{ab}}$ *is injective with dense image.*

In order to complete the description we compute the composition $\chi_\pi \circ \mathrm{rec}_K|_{\mathfrak{O}_K^\times}$.

Proposition 80. *The composition* $\chi_\pi \circ \mathrm{rec}_K|_{\mathfrak{O}_K^\times} : \mathfrak{O}_K^\times \to \mathfrak{O}_K^\times$ *equals the inverse map* $u \mapsto u^{-1}$ *and* $\ker(\chi_\pi \circ \mathrm{rec}_K) = \pi^{\mathbb{Z}} \subset K^\times$.

Proof: The field extension associated to χ_π is the compositum of all $K(x_v)$ as in Lemma 78 above. The defining equations $x_1^{q-1} + \pi = 0$ and $x_v^q + \pi X_v = x_{v-1}$ show

$$N_{K(x_1)/K}(-x_1) = \pi \quad \text{and} \quad N_{K(x_v)/K(x_{v-1})}(-x_v) = -x_{v-1}.$$

The norm residue property of rec_K then shows that $\chi_\pi(\mathrm{rec}_K(\pi)) = 1$ which implies the assertion on the kernel.

The isomorphism $g : \mathscr{G}_\pi \hat{\otimes} \mathfrak{O}^{\mathrm{nr}} \to \mathscr{G}_{\pi'} \hat{\otimes} \mathfrak{O}^{\mathrm{nr}}$ from Proposition 77 shows that as a module under the inertia subgroup I_K we have $g : \mathrm{T}_\pi \cong \mathrm{T}_{\pi'}$ which shows that $\chi_\pi = \chi_{\pi'}$ when restricted to inertia. From ${}^\sigma g = g \circ [v]_\pi$ we deduce that for general $\tau \in \mathrm{Gal}_K$ with $\mathrm{pr}(\tau) = \sigma^m$ we find for $x \in \mathrm{T}_\pi$ that

$$g \circ [\chi_{\pi'}(\tau)]_\pi(x) = [\chi_{\pi'}(\tau)]_{\pi'}(g(x)) = \tau(g(x)) = {}^\tau g(\tau(x)) = g \circ [v]_\pi^m [\chi_\pi(\tau)]_\pi(x)$$

and therefore

$$\chi_{\pi'}(\tau) = v^m \chi_\pi(\tau).$$

We deduce that the unramified character $\chi_{\pi'}/\chi_\pi$ equals $\tau = \sigma^m \mapsto v^m \in \mathfrak{O}_K^\times$. It remains to compute for an arbitrary $v \in \mathfrak{O}_K^\times$ with the two uniformisers $\pi' = \pi v$ and π that

$$\chi_\pi(\mathrm{rec}_K(v)) = \chi_\pi(\mathrm{rec}_K(\pi v)) = v^{-\nu(\pi v)} \chi_{\pi'}(\mathrm{rec}_K(\pi')) = v^{-1}.$$

□

11. Hodge–Tate decomposition

References: [Ta66] §3+4 [Fa01] [Sh86] §6.

The aim of this chapter is the discussion of the p-adic Hodge–Tate decomposition for the Tate module of a p-divisible group. There are at least four different proofs, see [Fo82] §5 and [Fa01]. We will present the original approach due to Tate [Ta66] §4, see also [Sh86] §6.

In this chapter we will work over a complete discrete valuation ring Λ with perfect residue field $k = \Lambda/\mathfrak{m}$ of characteristic $p > 0$ and field of fractions K of characteristic 0. The valuation on K and all its prolongations are denoted by ν. Note that some prolongations may take values in a non-discrete subgroup of $\mathbb{Q}$ and thus have non-Noetherian valuation rings.

11.1. **Points.**

Let $G = (G_v)$ be a p-divisible group over Λ. For the p-adic completion L of an algebraic extension of K with p-adically completed ring of integers $\mathfrak{o}_L = V = \varprojlim_i V/\mathfrak{m}^i V$ the set of **V-valued points** of G is defined to be the $\mathbb{Z}_p$-module

$$G(V) = \varprojlim_i G(V/\mathfrak{m}^i V) = \varprojlim_i \varinjlim_v G_v(V/\mathfrak{m}^i V) = \mathrm{Hom}_{\Lambda-\mathrm{formal}}(\mathrm{Spf}(V), \mathscr{G}),$$

where $\mathscr{G} = \varinjlim_v G_v$ is the formal group associated to G. It is dangerous to interchange the limits as

$$0 \to G_v(V/\mathfrak{m}^i V) \to \varinjlim_v G_v(V/\mathfrak{m}^i V) \xrightarrow{[p^v]} \varinjlim_v G_v(V/\mathfrak{m}^i V)$$

is exact and leads to

$$0 \to \varprojlim_i G_v(V/\mathfrak{m}^i V) \to G(V) \xrightarrow{[p^v]} G(V)$$

and thus

$$G(V)_{\mathrm{tors}} = \varinjlim_v \varprojlim_i G_v(V/\mathfrak{m}^i V)$$

gives exactly the torsion part of $G(V)$.

Example 81. (1) Let $\mathfrak{m}_V$ be the maximal ideal of V. For $G = \mu_{p^\infty}$ we get

$$G(V) = \varprojlim_i \mu_{p^\infty}(V/\mathfrak{m}^i V) = \varprojlim_i (1+\mathfrak{m}_V)/(1+\mathfrak{m}^i V) = 1 + \mathfrak{m}_V,$$

the group of 1-units.

(2) For an étale p-divisible group G we have unique lifting of points and thus $G_v(V/\mathfrak{m}^i V) = G_v(k_V)$ for all i with k_V the residue field $V/\mathfrak{m}_V$ of V, hence

$$G(V) = \varprojlim_i \varinjlim_v G_v(V/\mathfrak{m}^i V) = \varprojlim_i \varinjlim_v G_v(k_V) = \varinjlim_v G_v(k_V) = G(k_V)$$

is a torsion group.

(3) Let G be a connected p-divisible group and $\mathscr{G}$ the associated p-divisible formal Lie group with $G = \mathscr{G}_{p^\infty}$. Then $\mathscr{G} \cong \mathrm{Spf}\,\Lambda[[X_1, \ldots, X_d]]$ for $d = \dim G$ and

$$G(V) = \mathrm{Hom}_{\Lambda-\mathrm{formal}}(\mathrm{Spf}(V), \mathscr{G}) \cong \mathrm{Hom}_{\Lambda,\mathrm{cont}}(\Lambda[[X_1, \ldots, X_d]], V)$$

which equals $\mathfrak{m}_V^d$ as a set. The (formal) group law of $\mathscr{G}$ defines the structure of a p-adic analytic group on $G(V) = \mathfrak{m}_V^d$ defined over Λ. The filtration $\mathrm{F}^\delta\, G(V) = \mathfrak{m}_{V,\delta}^d$ with

$$\mathfrak{m}_{V,\delta} = \{x \in V \ ; \ \nu(x) \geq \delta\}$$

is a filtration by subgroups as

$$\mathrm{F}^\delta\, G(V) = \ker\big(G(V) \to G(V/\mathfrak{m}_{V,\delta}),$$

and

$$[p]^*(\mathrm{F}^\delta\, G(V)) \subseteq \mathrm{F}^{\delta+\varepsilon}\, G(V)$$

with $\varepsilon = \min\{\delta, \nu(p)\}$, because

$$[p]^*(X_i) = pX_i + \text{ higher order.}$$

Lemma 82. *Let G be a p-divisible group. The map $G \to G^{\text{ét}}$ has a formal section, i.e., the associated map $\mathscr{G} \to \mathscr{G}^{\text{ét}}$ between formal groups admits a section as maps of formal schemes. Consequently, the sequence*

$$0 \to G^0(V) \to G(V) \to G^{\text{ét}}(V) \to 0$$

is exact.

Proof: Let A, A^0 and $A^{\text{ét}}$ represent the formal groups $\mathscr{G}, \mathscr{G}^0$ and $\mathscr{G}^{\text{ét}}$. Then

$$A^0 = \Lambda[[X_1, \dots, X_d]]$$

and

$$A \otimes_\Lambda k = (A^{\text{ét}} \otimes_\Lambda k)[[X_1, \dots, X_d]]$$

because the sequence

$$0 \to G^0 \to G \to G^{\text{ét}} \to 0$$

splits canonically modulo $\mathfrak{m}$ due to the reduced subgroups $G_{v,\text{red}}$. Lifting the variables we find a continuous map

$$f : A^{\text{ét}}[[X_1, \dots, X_d]] \to A$$

that is an isomorphism modulo $\mathfrak{m}$ and thus an isomorphism as in the proof of Theorem 70. The projection $A \twoheadrightarrow A^{\text{ét}}$ sending $X_i \mapsto 0$ yields the required formal section. The rest is clear. □

Corollary 83. *For $x \in G(V)$ there is a finite extension L' of L with ring of integers V' and a $y \in G(V')$ such that $py = x$.*

Proof: The multiplication by p map $[p] : \mathscr{G}^0 \to \mathscr{G}^0$ is finite flat, so that the corollary holds for $x \in G^0(V)$. By Lemma 82 we may therefore assume $G = G^{\text{ét}}$. If then $x \in G_v(V) \subset G(V)$ we find y from the fpqc surjectivity of $[p] : G_{v+1} \to G_v$. □

Corollary 84. *If the fraction field L of V is algebraically closed, then $G(V)$ is p-divisible.* □

11.2. **The p-adic Tate module and Tate comodule.** Let K^{alg} be an algebraic closure of K and let Gal_K be the absolute Galois group $\text{Gal}(K^{\text{alg}}/K)$ of K. The **p-adic Tate module** of G is the $\mathbb{Z}_p[\text{Gal}_K]$-module

$$\mathrm{T}_p(G) = \varprojlim_v G_v(K^{\text{alg}})$$

with transfer maps induced by multiplication by p maps $[p] : G_{v+1} \to G_v$. The **p-adic Tate comodule** of G is the $\mathbb{Z}_p[\text{Gal}_K]$-module

$$\Phi_p(G) = \varinjlim_v G_v(K^{\text{alg}}).$$

Because the generic fibre G_K of G over $\text{Spec}(K)$ is an étale p-divisible group, we see that $\Phi_p(G)$ only depends on the generic fibre of G and moreover is equivalent to G_K. From the structure of discrete p-divisible groups we deduce that as a $\mathbb{Z}_p$-module we have $\mathrm{T}_p(G) \cong \mathbb{Z}_p^h$ and $\Phi_p(G) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^h$ where h is the height of G. We have

$$\mathrm{T}_p(G) = \text{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \Phi_p(G)),$$

$$\Phi_p(G) = \mathbb{Q}_p/\mathbb{Z}_p \otimes_{\mathbb{Z}_p} \mathrm{T}_p(G),$$

so that any of the three data $\mathrm{T}_p(G), \Phi_p(G)$ or G_K determines the other two.

11.2.1. *The Tate twist.* The Tate module of $\mu_{p^\infty} = \hat{\mathbb{G}}_{\mathrm{m}}$ is by definition

$$\mathbb{Z}_p(1) = \mathrm{T}_p(\mu_{p^\infty}) = \mathrm{T}_p(\mathbb{G}_{\mathrm{m}})$$

the corresponding character is the cyclotomic character

$$\chi : \mathrm{Gal}_K \to \mathbb{Z}_p^\times = \mathrm{Aut}_{\mathbb{Z}_p}\big(\mathbb{Z}_p(1)\big).$$

For a $\mathbb{Z}_p[\mathrm{Gal}_K]$ module M and $n \in \mathbb{Z}$ we define

$$M(n) = M \otimes \mathbb{Z}_p(1)^{\otimes n}$$

which for $n < 0$ means $M(n) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p(-n), M)$. These modules $M(n)$ are addressed as the nth Tate twist of M.

11.2.2. *Cartier duality revisited.* Let $G = (G_v)$ be a p-divisible group over Λ. The Cartier duality pairings $G_v \times G_v^D \to \mu_{p^v}$ for varying v are compatible in the sense of pairings

$$\begin{tikzcd}
G_{t+v} \arrow[d, "j_{t,v}"] & \times & G_{t+v}^D \arrow[r] & \mu_{p^{t+v}} \\
G_v & \times & G_v^D \arrow[u, "i_{v,t}"'] \arrow[r] & \mu_{p^v} \arrow[u, "\mathrm{incl}"']
\end{tikzcd}$$

because by definition $i_{G^D,v,t} = \big(j_{G,t,v}\big)^D$. Cartier duality thus induces a perfect pairing

$$\mathrm{T}_p(G) \times \mathrm{T}_p(G^D) \to \mathrm{T}_p(\mathbb{G}_{\mathrm{m}}) = \mathbb{Z}_p(1)$$

because for $(x_v) \in \mathrm{T}_p(G)$ and $(y_v) \in \mathrm{T}_p(G^D)$ we have

$$\langle x_v, y_v \rangle = \langle j_{t,v}(x_{t+v}), j_{t,v}(y_{t+v}) \rangle = \langle x_{t+v}, i_{v,t} j_{t,v}(y_{t+v}) \rangle = \langle x_{t+v}, p^t y_{t+v} \rangle = \langle x_{t+v}, y_{t+v} \rangle^{p^t}$$

in $\mu_{p^v} \subset \mu_{p^{t+v}}$ and thus

$$\langle (x_v), (y_v) \rangle = (\langle x_v, y_v \rangle)_v \in \mathrm{T}_p(\mathbb{G}_{\mathrm{m}})$$

is well defined and level-wise a perfect pairing.

Corollary 85. *We have an isomorphism of* Gal_K *modules* $\mathrm{T}_p(G) = \mathrm{T}_p\big(G^D\big)(-1)$.

11.3. **The logarithm.**

11.3.1. *Review of tangent space.* Let $G = (G_v)$ be a p-divisible group over Λ and

$$A^0 = \Lambda[[X_1, \ldots, X_d]]$$

with augmentation ideal $I = (X_1, \ldots, X_d)$ be the Λ-algebra representing the p-divisible formal Lie group associated to G^0. The **tangent space of G at 0 with values in a Λ-module M** is the Λ-module of continuous Λ-derivations

$$\mathrm{t}_G(M) = \mathrm{Der}_\Lambda(A^0, M) = \mathrm{Hom}_\Lambda(I/I^2, M)$$

with respect to the A^0-module structure on M by the counit $\varepsilon : A^0 \to \Lambda$. If M is an R-module for some Λ-algebra R then $\mathrm{t}_G(M)$ is naturally an R-module. If M is free of rank 1 as an R-module, then $\mathrm{t}_G(M)$ is free of rank $d = \dim(G)$ as an R-module. In particular

$$\mathrm{t}_G(L) = \mathrm{Der}_\Lambda(A^0, L) = \mathrm{Hom}_\Lambda(I/I^2, L)$$

is an L-vector space of dimension $d = \dim(G)$.

The **cotangent space of G at 0 with values in a Λ-module M** is the Λ-module representing $\mathrm{t}_G(-)$, namely $\mathrm{t}_G^* = I/I^2$ so that

$$\mathrm{t}_G^*(M) = I/I^2 \otimes_\Lambda M,$$

and $\mathrm{t}_G^*(L) = \mathrm{Hom}_L(\mathrm{t}_G(L), L)$.

11.3.2. *The logarithm.* The logarithm of G is the map

$$\log_G : G(V) \to \mathrm{t}_G(L)$$

defined by the formula

$$\log_G(x) = \left(f \in A^0 \mapsto \big(\log_G(x)\big)(f) := \lim_{r\to\infty} \frac{f([p^r]x) - f(0)}{p^r} \in L \right).$$

The fraction in the limit is well defined for $r \gg 0$ as $G^{\text{ét}}(V)$ is torsion. The sequence $[p^r](x) \in G(V)$ converges to 0, thus in order to check that the limit exists it is enough assume that $x \in \mathrm{F}^\delta G(V)$ for some $\delta \gg 0$. We choose $\delta > \nu(p) = \varepsilon$. Then $[p^r](x) \in \mathrm{F}^{\delta+r\varepsilon} G(V)$ which says that $\nu(X_i([p^r]x)) \geq \delta + r\varepsilon$. We find

$$\frac{f([p^{r+1}]x) - f(0)}{p^{r+1}} - \frac{f([p^r]x) - f(0)}{p^r} = \frac{1}{p^{r+1}}\big(\geq \text{quadratic in the } X_i([p^r]x)\big)$$

which yields an estimate

$$\nu\left(\frac{f([p^{r+1}]x) - f(0)}{p^{r+1}} - \frac{f([p^r]x) - f(0)}{p^r}\right) \geq -(r+1)\varepsilon + 2(\delta + r\varepsilon) = 2\delta + (r-1)\varepsilon.$$

The estimate shows that the $\frac{f([p^r]x)-f(0)}{p^r}$ form a Cauchy sequence in L. The formula

$$\big(\log_G\big)(x)(fg) = f(0)\big(\log_G\big)(x)(g) + g(0)\big(\log_G\big)(x)(g)$$

follows because $f \to \big(\log_G(x)\big)(f)$ is Λ-linear in f, vanishes on I^2 by an estimate as above and thus is nothing but a Λ-linear map $I/I^2 \to L$.

The logarithm is a group homomorphism $\log_G(x \cdot_G y) = \log_G(x) + \log_G(y)$ as

$$f(x \cdot_G y) = f(x) + f(y) + \text{ quadratic and higher order terms in } X_i(x) \text{ and } X_i(y).$$

Moreover, the logarithm is continuous with respect to the p-adic topology on L and the filtration topology by $\mathrm{F}^\delta G(V)$ on $G(V)$. Hence, $\log_G$ is $\mathbb{Z}_p$-linear. The logarithm $\log_G : G(V) \to \mathrm{t}_G(L)$ is natural in the variable V and thus in particular Galois equivariant.

Lemma 86. *The logarithm* $\log_G : G(V) \to \mathrm{t}_G(L)$ *is a local homeomorphism. More precisely, for each* $\delta > \frac{\nu(p)}{p-1}$ *in* $\mathbb{Q}$ *we have a homeomorphism*

$$\log_G \;:\; \mathrm{F}^\delta G(V) \xrightarrow{\sim} \{\tau \in \mathrm{t}_G(L) \;;\; \nu(\tau(X_i)) \geq \delta,\ \textit{all } i = 1, \ldots, d\}.$$

Corollary 87. *(1) The kernel of* $\log_G$ *is the torsion subgroup* $G(V)_{\text{tors}}$ *of* $G(V)$.
(2) The logarithm induces an isomorphism $\log_G : G(V) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \xrightarrow{\sim} \mathrm{t}_G(L)$.

Proof: (1) As $\mathrm{t}_G(L)$ is torsion free, the torsion subgroup belongs to the kernel. On the other hand, any $x \in G(V)$ has $[p^r](x)$ for $r \gg 0$ belonging to the source domain where $\log_G$ becomes a local homeomorphism, hence can only be killed by $\log_G$ if $[p^r]x = 0$.

(2) This follows from (1) and

$$\{\tau \in \mathrm{t}_G(L) \;;\; \nu(\tau(X_i)) \geq \delta,\ \text{all } i = 1, \ldots, d\} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \mathrm{t}_G(L).$$

□

11.4. **The p-adic complex numbers.** The field of the p-adic complex numbers is the field

$$C = \widehat{K^{\text{alg}}},$$

the p-adic completion of K^{alg}, which by Krasner's Lemma is again algebraically closed. The ring of integers in C is the ring $\mathfrak{o}_C$ that is the p-adically completed integral closure Λ^{alg} of Λ in K^{alg}. The group Gal_K acts on K^{alg} preserving Λ^{alg} so that the action extends to a continuous action of Gal_K on C that preserves $\mathfrak{o}_C$. We will use below the following fundamental theorem of Tate [Ta66] §3.3, see also [Fo04] §1, and more recently [BC09] Theorem 2.2.7.

Theorem 88 (Tate–Sen)**.** *If the image of the cyclotomic character $\chi : \mathrm{Gal}_K \to \mathbb{Z}_p$ is infinite, then we have canonical isomorphisms*

$$\mathrm{H}^i\big(K, C(j)\big) = \begin{cases} 0 & \textit{for } i \geq 2 \textit{ or } j \neq 0, \\ K & \textit{for } i = 0, 1 \textit{ and } j = 0. \end{cases}$$

11.5. **Pairings.**

11.5.1. *The fundamental pairings à la Tate.* Cartier duality yields isomorphisms

$$G_v^D(\mathfrak{o}_C) = \mathrm{Hom}_{\mathfrak{o}_C-\text{groups}}(G_v \times_\Lambda \mathfrak{o}_C, \mu_{p^v, \mathfrak{o}_C}). \tag{11.1}$$

By the valuative criterion and the fact that the generic fibre of G is étale we get identifications

$$G_v^D(K^{\mathrm{alg}}) = G_v^D(C) = G_v^D(\mathfrak{o}_C)$$

that together with (11.1) leads to an isomorphism

$$\mathrm{T}_p(G^D) = \varprojlim_v \mathrm{Hom}_{\mathfrak{o}_C-\text{groups}}(G_v \times_\Lambda \mathfrak{o}_C, \mu_{p^v, \mathfrak{o}_C}) = \mathrm{Hom}_{p-\text{divisible groups}}(G \times_\Lambda \mathfrak{o}_C, \mu_{p^\infty, \mathfrak{o}_C})$$

of $\mathbb{Z}_p[\mathrm{Gal}_K]$-modules. Applying the functor of $\mathfrak{o}_C$-valued points and the functor tangent space over C we get Gal_K-equivariant maps

$$\mathrm{T}_p(G^D) \to \mathrm{Hom}\big(G(\mathfrak{o}_C), \mu_{p^\infty}(\mathfrak{o}_C)\big) \tag{11.2}$$

and

$$\mathrm{T}_p(G^D) \to \mathrm{Hom}\big(\mathrm{t}_G(C), \mathrm{t}_{\mu_{p^\infty}}(C)\big). \tag{11.3}$$

Proposition 89. *We have a map of exact sequences of $\mathbb{Z}_p[\mathrm{Gal}_K]$-modules*

$$\begin{tikzcd} 0 \arrow[r] & \Phi_p(G) \arrow[r] \arrow[d, "\alpha_{\mathrm{Cartier}}"] & G(\mathfrak{o}_C) \arrow[r, "\log_G"] \arrow[d, "\alpha"] & \mathrm{t}_G(C) \arrow[r] \arrow[d, "d\alpha"] & 0 \\ 0 \arrow[r] & \mathrm{Hom}(\mathrm{T}_p(G^D), \Phi_p(\mu_{p^\infty})) \arrow[r] & \mathrm{Hom}\big(\mathrm{T}_p(G^D), \mu_{p^\infty}(\mathfrak{o}_C)\big) \arrow[r, "\log_{\mu_{p^\infty}}"] & \mathrm{Hom}\big(\mathrm{T}_p(G^D), \mathrm{t}_{\mu_{p^\infty}}(C)\big) \arrow[r] & 0, \end{tikzcd}$$

where $\alpha_{\mathrm{Cartier}}$ is induced by the Cartier pairing

$$\Phi_p(G) \times \mathrm{T}_p(G^D) \to \mathbb{Q}_p/\mathbb{Z}_p(1) = \Phi_p(\mu_{p^\infty})$$

and α (resp. $d\alpha$) is the other adjoint map for the pairings corresponding to (11.2) (resp. (11.3)).

Proof: The Tate comodule $\Phi_p(G)$ equals $\varinjlim_v G_v(K^{\mathrm{alg}}) = \varinjlim_v G_v(\mathfrak{o}_C) = G(\mathfrak{o}_C)_{\mathrm{tors}}$. It follows from Corollary 87 and Corollary 84 that for any p-divisible group the sequence

$$0 \to \Phi_p(G) \to G(\mathfrak{o}_C) \xrightarrow{\log_G} \mathrm{t}_G(C) \to 0 \tag{11.4}$$

is exact. The bottom row is $\mathrm{Hom}(\mathrm{T}_p(G^D), -)$ applied to (11.4) for $G = \mu_{p^\infty}$ and thus also exact.

The right square commutes because the logarithm map is a natural transformation and due to the very definition of the adjoint maps α and $d\alpha$. The left square commutes by the definition of α coming from the Cartier duality isomorphism (11.1). □

11.5.2. *The pairing on W.* We define now a Gal_K-semilinear pairing on C-vector spaces which resembles a continuous $\mathrm{H}^1_{\text{ét}}$. We set

$$W = \mathrm{Hom}_{\mathbb{Z}_p}\big(\mathrm{T}_p(G), C\big) \quad \text{and} \quad W^D = \mathrm{Hom}_{\mathbb{Z}_p}\big(\mathrm{T}_p(G^D), C\big).$$

Cartier duality gives us natural identifications

$$W^D = \mathrm{Hom}_{\mathbb{Z}_p}\big(\mathrm{T}_p(G^D), C\big) = \mathrm{T}_p(G) \otimes_{\mathbb{Z}_p} C(-1) = \mathrm{Hom}_C(W, C(-1))$$

or in other words the perfect $C - \mathrm{Gal}_K$-semilinear pairing

$$W \times W^D \to C(-1)$$

that is the scalar extension to C of the dual to the Cartier pairing $\mathrm{T}_p(G) \times \mathrm{T}_p(G^D) \to \mathbb{Z}_p(1)$.

11.6. **Hodge–Tate representations.**

Lemma 90 (Tate, see [Se66] §2 Prop 4)**.** *Let V be a Gal_K-representation on a finite dimensional $\mathbb{Q}_p$ vector space. The natural C-linear map*

$$\bigoplus_{j\in\mathbb{Z}} \mathrm{H}^0\left(K, V\otimes_{\mathbb{Q}_p} C(-j)\right)\otimes_K C(j)\to V\otimes_{\mathbb{Q}_p} C$$

is injective.

Proof: Let $x_{i,j}$ be a K-basis of

$$\mathrm{H}^0\left(K, V\otimes_{\mathbb{Q}_p} C(-j)\right)\otimes_K K(j)\subset V\otimes_{\mathbb{Q}_p} C.$$

If the claim of the lemma fails then we have $c_{i,j}\in C$ with $\sum_{i,j} c_{i,j}x_{i,j}=0$. We choose a relation of minimal length and with $c_{i_0,j_0}=1$. Now for $\sigma\in\mathrm{Gal}_K$

$$0=\sigma\Big(\sum_{i,j} c_{i,j}x_{i,j}\Big)-\chi(\sigma)^{j_0}\Big(\sum_{i,j} c_{i,j}x_{i,j}\Big)=\sum_{i,j}\Big(\sigma(c_{i,j})\chi(\sigma)^j-\chi(\sigma)^{j_0}c_{i,j}\Big)x_{i,j}$$

gives a shorter relation due to cancellation for the term for (i_0,j_0). Hence all terms must cancel and so

$$\sigma(c_{i,j})=\chi(\sigma)^{j_0-j}c_{i,j}$$

for all (i,j). For $j\neq j_0$ this implies $c_{i,j}=0$ by Theorem 88, while for $j=j_0$ Theorem 88 forces $c_{i,j}\in K$. But then a nontrivial relation contradicts the choice of the $x_{i,j}$ being K-linearly independent. □

Let B_{HT} be the C-algebra $\bigoplus_{j\in\mathbb{Z}} C(j)$. The functor

$$V\rightsquigarrow \mathscr{D}_{\mathrm{HT}}(V)=\Big(V\otimes_{\mathbb{Q}_p} B_{\mathrm{HT}}\Big)^{\mathrm{Gal}_K}=\bigoplus_{j\in\mathbb{Z}}\mathrm{H}^0\left(K, V\otimes_{\mathbb{Q}_p} C(-j)\right)$$

takes values in finite dimensional graded K-vector spaces with the bound

$$\dim_K \mathscr{D}_{\mathrm{HT}}(V)\leq \dim_{\mathbb{Q}_p} V. \tag{11.5}$$

The representation V is a **Hodge–Tate** representation if the corresponding map from Lemma 90 is an isomorphism and if and only if the bound in (11.5) is an equality. So V is Hodge–Tate if and only if $V\otimes_{\mathbb{Q}_p} C$ decomposes into a sum of Tate twists. The twists which appear together with their multiplicity are unique by Theorem 88. Together they describe the tuple of **Hodge–Tate weights** of V. The multiplicity $m_{\mathrm{HT}}(j)=m_{\mathrm{HT}}(V,j)$ of the Hodge–Tate weight j in the representation V is given by

$$m_{\mathrm{HT}}(j)=\dim_K \mathrm{H}^0\left(K, V\otimes_{\mathbb{Q}_p} C(-j)\right)$$

and is the dimension of the j^{th} graded piece of $\mathscr{D}_{\mathrm{HT}}(V)$.

11.7. **Hodge–Tate decomposition for p-divisible groups.**

Theorem 91 (Tate)**.** *The maps*

$$\alpha_\Lambda\ :\ G(\Lambda)\to \mathrm{Hom}_{\mathrm{Gal}_K}\left(\mathrm{T}_p(G^D),\mu_{p^\infty}(C)\right),$$

$$d\alpha_\Lambda\ :\ \mathrm{t}_G(K)\to \mathrm{Hom}_{\mathrm{Gal}_K}\left(\mathrm{T}_p(G^D),\mathrm{t}_{\mu_{p^\infty}}(C)\right),$$

which are the restriction of α (resp. $d\alpha$) from Proposition 89 to the invariants under Gal_K, are isomorphisms.

Proof: Step 1: The map $\alpha_{\mathrm{Cartier}}$ of Proposition 89 is an isomorphism due to Cartier duality. By the snake lemma we find $\ker(\alpha) = \ker(d\alpha)$ and $\operatorname{coker}(\alpha) = \operatorname{coker}(d\alpha)$ are C-vector spaces.

Step 2: The map $\alpha_\Lambda = \alpha(G)_\Lambda$ is functorial in G and exact for the connected étale sequence by Lemma 82, so that we have an exact sequence

$$0 \to \ker(\alpha(G^0)_\Lambda) \to \ker(\alpha(G)_\Lambda) \to \ker(\alpha(G^{\text{ét}})_\Lambda).$$

To prove injectivity of α_Λ we may assume that G is either connected or étale. From Theorem 88 it follows that $G(\Lambda) = \mathrm{H}^0(K, G(\mathfrak{o}_C))$, and

$$\ker(\alpha_\Lambda) = \mathrm{H}^0(K, \ker(\alpha)) = \mathrm{H}^0(K, \ker(d\alpha))$$

is a K-vector space. As the valuation of Λ is discrete we find $[p]\,\mathrm{F}^\delta\, G^0(\Lambda) \subset \mathrm{F}^{\delta+1}\, G^0(\Lambda)$, and moreover $\bigcap_v [p^v] G^0(\Lambda) = 0$, so that $G^0(\Lambda)$ does not contain p-divisible elements.

So in either case, whether G is connected or étale, we find that $G(\Lambda)$ does not contain a K-vector space. Thus α_Λ is injective for arbitrary G.

Step 3: The map $d\alpha_\Lambda$ is injective because

$$\ker(d\alpha_\Lambda) = \mathrm{H}^0(K, \ker(d\alpha)) = \mathrm{H}^0(K, \ker(\alpha)) = \ker(\alpha_\Lambda) = 0.$$

Step 4: As $d\alpha : \mathrm{t}_G(C) \to \operatorname{Hom}\big(\mathrm{T}_p(G^D), \mathrm{t}_{\mu_{p^\infty}}(C)\big)$ factors as

$$\mathrm{t}_G(K) \otimes_K C \xrightarrow{d\alpha_\Lambda \otimes \mathrm{id}} \mathrm{H}^0\Big(K, \operatorname{Hom}\big(\mathrm{T}_p(G^D), \mathrm{t}_{\mu_{p^\infty}}(C)\big)\Big) \otimes_K C \to \operatorname{Hom}\big(\mathrm{T}_p(G^D), \mathrm{t}_{\mu_{p^\infty}}(C)\big)$$

with the second map being injective by Lemma 90, even $d\alpha$ and thus α is injective.

Step 5: Taking invariants being left exact and by the snake lemma we find

$$\operatorname{coker}(\alpha_\Lambda) \subseteq \operatorname{coker}(d\alpha_\Lambda) \subseteq \mathrm{H}^0\big(K, \operatorname{coker}(\alpha)\big) = \mathrm{H}^0\big(K, \operatorname{coker}(d\alpha)\big)$$

so that in order to conclude we may restrict to the case of $d\alpha_\Lambda$, which is linear.

Step 6: We identify $\mathrm{t}_{\mu_{p^\infty}}(C) = C$ and thus $d\alpha$ maps $\mathrm{t}_G(C) \hookrightarrow W^D$.

Step 7: In the pairing $W \times W^D \to C(-1)$ the spaces of invariants $\mathrm{H}^0(K, W)$ and $\mathrm{H}^0(K, W^D)$ pair to $\mathrm{H}^0(K, C(-1))$ which vanishes by Theorem 88. Using Lemma 90 and the C-linearity of the pairing, it follows that the subspace $\mathrm{H}^0(K, W) \otimes_K C \subseteq W$ is orthogonal to the subspace $\mathrm{H}^0(K, W^D) \otimes_K C \subseteq W^D$. Because the dimension count for the subspaces $\mathrm{t}_G(C) \subseteq \mathrm{H}^0(K, W^D) \otimes_K C$ and $\mathrm{t}_{G^D}(C) \subseteq \mathrm{H}^0(K, W) \otimes_K C$ yields

$$\dim_C \mathrm{t}_G(C) + \dim_C \mathrm{t}_{G^D}(C) = \dim(G) + \dim(G^D) = \operatorname{height}(G) = \dim_C W$$

we find that $\mathrm{t}_G(C)$ and $\mathrm{t}_{G^D}(C)$ are exact mutual annihilators and $d\alpha_\Lambda$ is surjective. □

11.7.1. *p-adic Hodge theory for p-divisible groups.*

Corollary 92. *(1) The Gal_K-representation $\mathrm{V}_p(G) = \mathrm{T}_p(G) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is Hodge–Tate with Hodge–Tate weights 0 and 1.*

(2) We have a natural isomorphism of graded vector spaces in degrees 0, 1

$$\mathscr{D}_{\mathrm{HT}}\big(\mathrm{V}_p(G)\big) = \mathrm{t}^*_{G^D}(K) \oplus \mathrm{t}_G(K)$$

so that the multiplicity of the Hodge–Tate weight 1 (resp. 0) is $\dim(G)$ (resp. $\dim(G^D)$).

(3) The Gal_K-module $\mathrm{T}_p(G)$ determines the dimension of G and of G^D.

Proof: (1) follows from (2) and the equality

$$\dim_{\mathbb{Q}_p}\big(\mathrm{V}_p(G)\big) = \operatorname{height}(G) = \dim(G) + \dim(G^D) = \dim_K \mathrm{t}_G(K) + \dim_K \mathrm{t}^*_{G^D}(K).$$

And (3) is obviously encoded in (2). Let us prove (2). We have $\mathrm{t}_{\mu_{p^\infty}}(C) = C$ and thus using $d\alpha_\Lambda$ and Cartier duality

$$\mathrm{t}_G(K) = \operatorname{Hom}_{\mathrm{Gal}_K}\big(\mathrm{T}_p(G^D), C\big) = \mathrm{H}^0\big(K, \mathrm{T}_p(G) \otimes_{\mathbb{Z}_p} C(-1)\big).$$

From the proof of Theorem 91 we know that $\mathrm{t}_G(C) \subset W^D$ and $\mathrm{t}_{G^D}(C) \subset W$ are orthogonal complements for the pairing $W \times W^D \to C(-1)$. We deduce an exact sequence

$$0 \to \mathrm{t}_G(C) \xrightarrow{d\alpha} W^D = \mathrm{Hom}(\mathrm{T}_p(G^D), C) \to \mathrm{Hom}(\mathrm{t}_{G^D}(C), C(-1)) \to 0$$

of Gal_K-modules. Twisting by $C(1)$ and by Cartier duality $\mathrm{T}_p(G) = \mathrm{Hom}\big(\mathrm{T}_p(G^D), \mathbb{Z}_p(1)\big)$ we obtain the exact sequence

$$0 \to \mathrm{t}_G(C) \otimes C(1) \xrightarrow{d\alpha(1)} \mathrm{T}_p(G) \otimes_{\mathbb{Z}_p} C \to \mathrm{t}^*_{G^D}(C) \to 0. \tag{11.6}$$

By Theorem 88 we can compute the cohomology sequence and find

$$\mathrm{H}^0\left(K, \mathrm{T}_p(G) \otimes_{\mathbb{Z}_p} C\right) = \mathrm{t}^*_{G^D}(K).$$

□

Corollary 93. *The semilinear* Gal_K*-representation* $\mathrm{V}_p(G) \otimes_{\mathbb{Q}_p} C$ *has a unique natural decomposition*

$$\mathrm{V}_p(G) \otimes_{\mathbb{Q}_p} C = \Big(\mathrm{t}^*_{G^D}(K) \otimes_K C\Big) \oplus \Big(\mathrm{t}_G(K) \otimes_K C(1)\Big)$$

Proof: By Lemma 90 this holds for every Hodge–Tate representation. The uniqueness comes from the fact that there are no homomorphisms between different Hodge–Tate weights due to Theorem 88.

As an alternative we may show the existence of the decomposition due to (11.6) being necessarily split as $\mathrm{Ext}^1_{\mathrm{Gal}_K}(C, C(1)) = \mathrm{H}^1(K, C(1)) = (0)$. □

Corollary 94. *There is an isomorphism of* Gal_K*-representations*

$$\det\left(\mathrm{V}_p(G) \otimes_{\mathbb{Q}_p} C\right) \cong C(\dim(G)).$$

11.7.2. *p-adic Hodge theory for étale* H^1. Let X/K be a smooth, proper geometrically connected variety with Albanese map $\iota_X : X \to \mathrm{Alb}_X = A$. We assume that the abelian variety A/K has good reduction over Λ, e.g., if X is projective and has good reduction over Λ. The p-adic Tate module $\mathrm{T}_p(A)$ is the p-adic Tate module for the p-divisible group $A[p^\infty]$ over Λ. Hence the Gal_K-representation

$$W = \mathrm{Hom}(\mathrm{T}_p(A), C) = \mathrm{H}^1_{\text{ét}}(\overline{A}, \mathbb{Q}_p) \otimes C = \mathrm{H}^1_{\text{ét}}(\overline{X}, \mathbb{Q}_p) \otimes C$$

with $\overline{A} = A \times_K K^{\mathrm{alg}}$ and $\overline{X} = X \times_K K^{\mathrm{alg}}$, has a Hodge–Tate decomposition

$$W \cong \Big(\mathrm{t}^*_G(K) \otimes_K C(-1)\Big) \oplus \Big(\mathrm{t}_{G^D}(K) \otimes_K C\Big).$$

The space $\mathrm{t}^*_G(K)$ can be identified with the space of A-invariant differentials on A, or $\mathrm{H}^0(A, \Omega^1_{A/K})$, whereas the space $\mathrm{t}_{G^D}(K)$ is the tangent space at 0 for the dual abelian variety $A^t = \mathrm{Pic}^0_{A/K}$ which by deformation theory equals $\mathrm{H}^1(A, \mathcal{O}_A)$.

The pullback by ι_X yields isomorphisms

$$\mathrm{H}^0(A, \Omega^1_{A/K}) = \mathrm{H}^0(X, \Omega^1_{X/K})$$

and

$$\mathrm{H}^1(A, \mathcal{O}_A) = \mathrm{H}^1(X, \mathcal{O}_X)$$

which finally leads to the Hodge–Tate decomposition of p-adic Hodge theory:

$$\mathrm{H}^1_{\text{ét}}(\overline{X}, \mathbb{Q}_p) \otimes C = \Big(\mathrm{H}^0(X, \Omega^1_{X/K}) \otimes_K C(-1)\Big) \oplus \Big(\mathrm{H}^1(X, \mathcal{O}_X) \otimes_K C\Big)$$

or

$$\mathscr{D}_{\mathrm{HT}}\Big(\mathrm{H}^1_{\text{ét}}(\overline{X}, \mathbb{Q}_p)\Big) = \mathrm{H}^0(X, \Omega^1_{X/K}) \oplus \mathrm{H}^1(X, \mathcal{O}_X)$$

so that $\mathscr{D}_{\mathrm{HT}}$ transforms étale cohomology into Hodge cohomology. More generally we know now by work of Bloch/Kato, Fontaine/Messing, Faltings, Tsuji, ... the following result conjectured by Tate [Ta66] §4.1.

Theorem 95. *Let X/K be a smooth proper geometrically connected variety. Then the Gal_K-representations $\mathrm{H}^n(\overline{X}, \mathbb{Q}_p)$ of p-adic étale cohomology are Hodge–Tate and thus*

$$\mathscr{D}_{\mathrm{HT}}\Big(\mathrm{H}^n_{\text{ét}}(\overline{X}, \mathbb{Q}_p)\Big) = \bigoplus_{a+b=n} \mathrm{H}^a(X, \Omega^b_{X/K}),$$

$$\mathrm{H}^n_{\text{ét}}(\overline{X}, \mathbb{Q}_p) \otimes_K C = \bigoplus_{a+b=n} \mathrm{H}^a(X, \Omega^b_{X/K}) \otimes_K C(-b).$$

We have given a proof of Theorem 95 for abelian varieties A/K of good reduction as

$$\mathrm{H}^*(\overline{A}, \mathbb{Q}_p) = \bigwedge \mathrm{H}^1(\overline{A}, \mathbb{Q}_p)$$

following Tate in [Ta66] and the exposition of Tate's work by Shatz [Sh86]. Raynaud extended Tate's Theorem to the case of arbitrary abelian varieties.

References

[ACS05] Andreatta, F., Conrad, B., Schoof, R., homework on p-divisible groups, http://math.stanford.edu/~conrad/papers/gpschemehw1.pdf, gpschemehw2.pdf, gpschemehw3.pdf, gpschemehw4.pdf.

[BC09] Brinon, O., Conrad, B., CMI summer school notes on p-adic Hodge Theory, http://www.claymath.org/programs/summer_school/2009/ConradNotes.pdf, manuscript, 2009.

[De72] Demazure, M., *Lectures on p-divisible groups*, Springer Lecture Notes **302**, 1972.

[Fa01] Faltings, G., Formal groups, private lecture notes of a course held at the University of Bonn 2001/2002.

[Fo82] Fontaine, J.-M., Formes différentielles et modules de Tate des variétés abéliennes sur les corps locaux, *Inventiones Math.* **65** (1982), 379–409.

[Fo04] Fontaine, J.-M., Arithmétique des représentations galoisiennes p-adiques, in: *Cohomologies p-adiques et applications arithmétiques III*, *Astérisque* **295** (2004), xi, 1–115.

[Gr57] Grothendieck, A., Sur quelques points d'algèbre homologique, *Tohoku Math. J.* (2) **9** (1957), 119–221.

[Gr60] Grothendieck, A., Technique de descente et théorèmes d'éxistence en géométrie algébrique II, *Séminaire Bourbaki*, Éxposé **195**, 1960.

[Gr74] Grothendieck, A., *Groupes de Barsotti-Tate et cristaux de Dieudonné*, Séminaire de Mathématiques Supérieures, No. **45**, Les Presses de l'Université de Montréal, Montreal, 1974, 155 pp.

[Oo66] Oort, F., Algebraic group schemes in characteristic zero are reduced, *Invent. Math.* **2** (1966), 79–80.

[OT70] Oort, F., Tate, J., Group schemes of prime order, *Ann. scient. Ec. Norm. Sup.* tome **3** (1970), 1–21.

[Pk05] Pink, R., et al., *Finite group schemes and p-divisible groups*, Seminarskript,ETH Zürich, 2004/2005.

[Ra66] Raynaud, M., Passage au quotient par une relation d'equivalence plate, in: *Proceedings of a conference on Local Fields, Driebergen, 1966*, Springer, 1967, pp. 79–85.

[Sc00] Schoof, R., *Introduction to finite group schemes*, lecture notes taken by John Voight, October – December 2000, http://www.cems.uvm.edu/~voight/notes/274-Schoof.pdf.

[Sc01] Schoof, R., Finite flat group schemes over local Artin rings, *Compositio Math.* **128** (2001), no. 1, 1–15.

[Se66] Serre, J.-P., Sur les groupes de Galois attachés aux groupes p-divisibles, in: *Proceedings of a conference on Local Fields, Driebergen, 1966*, Springer, 1967, pp. 118–131.

[Se72] Serre, J.-P., Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), no. 4, 259–331.

[SGA1] Grothendieck, A., Mme. Raynaud, M., *Revêtements Étales et Groupe Fondamental (SGA 1)*, LNM **224**, Springer, 1971.

[SGA3] Demazure, M., Grothendieck, A., *Schemas en groupes I-III*, Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3), Springer LNM **151, 152, 153**, 1970.

[Sh86] Shatz, St. S., Group schemes, formal groups, and p-divisible groups, in: *Arithmetic Geometry*, ed. G. Cornell and J. H. Silverman, Springer 1986, chapter III.

[Tm94] Tamme, G., *Introduction to Étale Cohomology*, Universitext, Springer, 1994.

[Ta66] Tate, J., p-divisible groups, in: *Proceedings of a conference on Local Fields, Driebergen, 1966*, Springer, 1967, pp. 158–183.

[Ta97] Tate, J., Finite flat group schemes, in: *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, Springer, 1997, 121–154.

Jakob Stix, Mathematisches Institut, Universität Heidelberg, Im Neuenheimer Feld 288, 69120 Heidelberg

E-mail address: stix@mathi.uni-heidelberg.de

URL: http://www.mathi.uni-heidelberg.de/~stix/SoSe09pdiv.html