GROUPSCHEMES WITH STRICT $\mathcal{O}$-ACTION

GERD FALTINGS

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn, Germany

1. Introduction

In [1] V.G.Drinfeld introduced the notion of a $\mathcal{O}$-module where $\mathcal{O}$ denotes the integers of a local field K. It is a formal group over an $\mathcal{O}$-algebra on which $\mathcal{O}$ acts such that the induced action on the Lie-algebra is by scalar multiplication. I call such an $\mathcal{O}$-action strict. The purpose of this paper is to find a generalisation to finite flat groupschemes, that is to define the notion of a finite flat groupscheme with strict $\mathcal{O}$-action and the notion of a strict $\mathcal{O}$-linear map. This is motivated by the previous paper [7] where I noticed the lack of such a theory. Another instance where one could use it are the complications around lemma 2.5 in chapter I of [10].

The main innovation in this paper is to provide this missing definition, the rest consisting of analogues to the usual theory. For example in our category we have a Cartier-duality where the Lubin-Tate formal group replaces the multiplicative group. We also study liftings over $\mathcal{O}$-DP-ideals. Here things are somehow complicated by the fact that we cannot embed into π-divisible groups, so we do not know a priori that a lift exists. Also there is no analogue of the crystalline site used in [12]. We solve this problem by embedding into infinite dimensional formal $\mathcal{O}$-modules.

Of course having developed an $\mathcal{O}$-version of finite flat groupschemes one can also ask whether there exists such versions for crystalline cohomology, or even for étale cohomology of schemes over K.

I thank the referee for his very useful comments. It gives me great pleasure to dedicate this paper to my colleague Yu Manin.

This paper has been accepted for publication by the Moscow Mathematical Journal.

2. Basic definitions

We consider affine flat commutative groupschemes over a ring R. These are given by a finitely presented flat R-algebra $A = \mathcal{O}_G$ together with a comultiplication. It is known that A is a relative complete intersection, that is of the form $A = R[T_1, ..., T_d]/I$ with I (Zariski-locally) generated by a regular sequence which remains regular after all basechanges (Sketch: It suffices to test this over an algebraically closed field. Then G is an extension of a smooth groupscheme by an infinitesimal group which is a successive extension of α_p's.). We define by $I_0 \subset R[T_1, ..., T_d]$ the ideal defining the zerosection of G, and by $A^\flat$ the ring $A^\flat = R[T_1, ..., T_d]/(I \cdot I_0)$. This definition makes sense for any pointed affine R-scheme but we only use it for flat relative complete intersections. It depends on the choice of a presentation but not in an essential way:

Denote by

$$L_A^* = I/(I \cdot I_0) \to I_0/I_0^2$$
$$= N_A^* \to \Omega_A$$

the fibre at the origin of the cotangent complex of A/R. We consider it as a complex concentrated in degrees -1 and 0. Its differential factors over $A^\flat$ as $I/(I \cdot I_0) \to A^\flat \to I_0/I_0^2$ where the second map is the universal derivation. Any homotopy (map of degree -1) $h : N_A^* \to \Omega_A$ defines an endomorphism of $A^\flat$ trivial on A and these endomorphisms correspond bijectively to homotopies. More generally any homomorphism $f : A \to B$ of augmented R-algebras can be lifted to an $f^\flat : A^\flat \to B^\flat$ and the possible lifts form a principal homogeneous space under homotopies $\Omega_A \to N_B^*$. Thus the thickening $A^\flat$ is unique up to a homotopy equivalence which in turn is unique up to a unique homotopy.

An alternative is define small thickenings of A as surjections $B \twoheadrightarrow A$ with kernel of square zero and annihilated by I_0. The definition of maps between two small thickenings is obvious, as is the notion of homotopy. Two maps with the same source and target are equivalent via a unique homotopy. A versal small thickening is a projective object in this category, and $A^\flat$ is an example of such a versal object. Two versal objects are then equivalent up to homotopy. Also each versal object defines a cotangent complex.

If $G = Spec(A)$ is a (flat) groupscheme denote $G^\flat = Spec(A^\flat)$. The comultiplication $A \to A \otimes_R A$ lifts to an $A^\flat \to (A \otimes_R A)^\flat$, or equivalently $(G \times G)^\flat \to G^\flat$, and the lift is unique if we require that it induces the identity on $0_G \times G^\flat$ and $G^\flat \times 0_G$. These lifts satisfy commutativity and associativity (on $(G \times G \times G)^\flat$), but do not define a groupscheme because $(G \times G)^\flat$ is a proper subscheme of $G^\flat \times G^\flat$. Also any pointed lift of a group-homomorphism $G \to H$ respects these "additions". It follows that two such lifts can be added, that is the lifts form a commutative group which is an extension of $Hom(G, H)$ by $Hom_R(\Omega_H, N_G^*)$. Especially all endomorphisms of G lift to $G^\flat$ and we obtain an extension (of associative unital rings, with the kernel an ideal)

$$Hom_R(\Omega_G, N_G^*) \subset End(G^\flat, G) \twoheadrightarrow End(G).$$

However more important for us is the subring $End'(G^\flat, G)$ consisting of endomorphisms which acts by a (common) scalar on Ω_G and N_G^*. It has a homomorphism into $End(G) \times R$ whose kernel is a central ideal of square zero isomorphic to $H^{-1}(End_R(L_G^*))$.

Finally we come to our main subject. Suppose $\mathcal{O}$ are the integers in a local field K, that is either $\mathcal{O}$ is a discrete valuationring finite over $\mathbb{Z}_p$, or $\mathcal{O} = \mathbb{F}_q[[\pi]]$ is a ring of powerseries over a finite field $\mathbb{F}_q$. We denote by π a uniformiser of $\mathcal{O}$ and by $\mathbb{F}_q$ its residue-field. We also assume from now on that the base R is an $\mathcal{O}$-algebra.

Definition 1. *Suppose G is a flat affine groupscheme over R. A strict $\mathcal{O}$-action on G is a homomorphism $\mathcal{O} \to End(G^\flat, G)$ such that the induced action on Ω_G and N_G^* is given by scalar multiplication via $\mathcal{O} \to R$. Equivalently it is a lifting of $\mathcal{O} \to End(G) \times R$ into $End'(G^\flat, G)$.*

A strict homomorphism $G \to H$ between two groupschemes with strict $\mathcal{O}$-action is a homomorphism which can be lifted to an $\mathcal{O}$-linear $G^\flat \to H^\flat$.

Remarks a) If one lift is $\mathcal{O}$-linear so are all of them because two lifts differ by a homotopy which commutes with scalar multiplication.

b) The definition is independant of the choices involved in the construction of $G^\flat$: Namely if we have defined a strict $\mathcal{O}$-action by action on one choice $G_1^\flat$ we obtain a unique such action on any other choice $G_2^\flat$ such that any $G_1^\flat \to G_2^\flat$ lifting the identity of G respects it. This is clear if $G_1^\flat$ is isomorphic to $G_2^\flat$ and one easily reduces to that case.

An alternative is to require a compatible system of $\mathcal{O}$-actions on each small thickening, scalar on the cotangent complex.

c) If $\mathcal{O}$ has characteristic zero it contains a subring $\mathcal{O}_0 = W(\mathbb{F}_q)$, the Witt-vectors over the residuefield $\mathbb{F}_q$, which contains roots of unity isomorphic to the multiplicative group $\mathbb{F}_q^*$. Firstly an $\mathcal{O}_0$-action on G lifts to a strict action if and only if the induced action of $\mathbb{F}_q^*$ on the cohomology of the cotangent complex L_G^* is via scalar multiplication, and then this action is unique:

One direction is obvious. For the other lift a generator ζ of $\mathbb{F}_q^*$ to an endomorphism ϕ of G^*. As ζ has (multiplicative) order $q-1$ then $\phi^{q-1}-1$ is nullhomotopic on $G^\flat$. For the induced action on L_G^* we have $\phi^{q-1}-1 = (\phi-\zeta)\cdot(\phi^{q-2}+\ldots+\zeta^{q-2})$, where the second factor is a quasiisomorphism. Thus the first factor is nullhomotopic and we can find a homotopic new lift ϕ' which acts on L_G^* as ζ. Hence $\mathcal{O}_0$ lies in the image of $End'(G^\flat, G)$, and by étaleness there is a unique lift defining a strict $\mathcal{O}_0$-action. Also any $\mathcal{O}_0$-linear $G \to H$ is strict.

If $\mathcal{O}$ differs from $\mathcal{O}_0$ choose a uniformiser π. It satisfies an Eisenstein-equation $f(\pi) = 0$ that is f is a unital polynomial with coefficients in $\mathcal{O}_0$ all (except for the leading) divisible by p, and the last one $p \cdot unit$. To extend an $\mathcal{O}$-action on G to a strict action we first have to extend $\mathcal{O}_0$ and this has been analysed. It remains to lift π. To do this it is certainly necessary that π acts by scalar multiplication on the cohomology of L_G^*, or slightly stronger that the endomorphism of L_G^* induced by $\pi \in \mathcal{O}$ is homotopic to multiplication by $\pi \in R$, that is that π lifts to an endomorphism of $G^\flat$ acting by scalar multiplication on Ω_G and N_G^*. This in turn again means that $\mathcal{O}$ lies in the image of $End'(G^\flat, G)$. However we need a lift of π annihilated by $f(T)$. If it exists it is unique up to a class in $H^{-1}(End_R(L_G^*))$ annihilated by the derivative $f'(\pi)$. Also not any $\mathcal{O}$-linear $G \to H$ need to be strict except if $f'(\pi)$ is a regular element in R.

d) If $\mathcal{O} = \mathbb{F}_q[[\pi]]$ has positive characteristic to make an $\mathcal{O}$-action on G strict we need firstly that $\mathbb{F}_q^*$ acts by scalar multiplication on the cohomology of L_G^*. In addition the action of π has to be homotopic to the scalar multiplication by π, and then the possible strict actions are a torsor under $H^{-1}(End_R(L_G^*))$. If G is annihilated by a power of π this describes the structure completely, otherwise we face somehow esoteric problems trying to extend from $\mathbb{F}_q[\pi]$ to $\mathbb{F}_q[[\pi]]$.

Of course there is no good reason for a general $\mathcal{O}$-linear map to be strict.

3. Examples

An obvious example for a groupscheme with strict $\mathcal{O}$-action is the additive group $\mathbb{G}_a$ with $\mathcal{O}$ acting by scalars. Also any abstract finite $\mathcal{O}$-module defines a constant (étale) groupscheme which has a strict $\mathcal{O}$-action. More generally any smooth groupscheme with an $\mathcal{O}$-action is strict if the induced action on the Lie-algebra is via scalars.

In characteristic p we also have the subscheme $G = \alpha_q \subset \mathbb{G}_a$ which is the kernel of the q-th power map (which is $\mathcal{O}$-linear as opposed to the usual Frobenius given by the p-th power). That G satisfies the condition follows easily by embedding $G^\flat \subset \mathbb{G}_a$.

More interesting is the Lubin-Tate π-divisible group. On the powerseries ring $R[[T]]$ there is the unique structure of a strict $\mathcal{O}$-module such that multiplication by π is defined by $\pi T + T^q$. We call this formal $\mathcal{O}$-module $\mathcal{LT}^f$. On it $\zeta \in \mathbb{F}_q^*$ sends T to $\zeta \cdot T$. For any integer n its π^n-divisionpoints $\mathcal{LT}[\pi^n]$ are finite flat groupschemes with strict $\mathcal{O}$-actions (strictness follows because they are kernels of a map of strict formal groups). They depend on the choice of π but only up to twist with an unramified character of K. $\mathcal{LT}^d$ is defined as the ind-groupscheme which is the union of all $\mathcal{LT}[\pi^n]$. It is embedded into the affine line and the $\mathcal{O}$-action extends to $\mathcal{LT}^{d,\flat}$ by the "same formulas" (ζ acts as ζT, π as $\pi T + T^q$): Namely the formal π-adic schemes coincide, and this implies the necessary identities. Both versions are contained in the ind-groupscheme $\mathcal{LT} \subset \mathbb{A}^1$ which is the union of the closed subschemes $X_{a,b}$ defined by powers F_n^{a+1}, where F_n denotes the n-fold iteration of $\pi \cdot T + T^q$ (one checks that the product sends $X_{a,n} \times X_{b,n}$ into $X_{a+b,n}$). All three versions coincides over bases R in which π is nilpotent.

Instead of our version of $\mathcal{LT}$ we could use a different one with logarithm $\sum T^{q^n}/\pi^n$ which is isomorphic to $\mathcal{LT}$ over the maximal unramified extension of $\mathcal{O}$.

Over $R = \mathcal{O}[u,v]/(u \cdot v + \pi)$ we define a groupscheme $G_{u,v}$ as follows:

As a scheme $G_{u,v} = Spec(\mathcal{O}[Z]/(u \cdot Z + Z^q)$. On it $\zeta \in \mathbb{F}_q$ acts by sending Z to $\zeta \cdot Z$. Addition and π-multiplication are given by the following formulas: The comultiplication on $\mathcal{LT}$ is defined by a sum $m^*(T) = \sum a_{ij} T^i \otimes T^j$, with $a_{ij} \in \mathcal{O}$. Here a_{ij} vanishes unless $i+j \equiv 1 mod(q-1)$ (necessarily so because of the $\mathbb{F}_q$-action), and the terms in degree one are $T \otimes 1 + 1 \otimes T$. Now comultiplication on $G_{u,v}$ is defined by $m^*(Z) = \sum a_{ij}(-v)^{(i+j-1)/(q-1)} T^i \otimes T^j$. Also on $G^\flat_{u,v}$ multiplication by $\zeta \in \mathbb{F}_q$ or by π are defined by $\zeta^*(Z) = \zeta \cdot Z$, $\pi^*(Z) = \pi \cdot Z - v \cdot Z^q$. To see that the necessary identities hold we remark that $G_{\pi,-1}$ is isomorphic to $\mathcal{LT}[\pi]$ so satisfies them. Furthermore if we invert $-v$ and adjoin a $(q-1)$-st root of it $G_{u,v}$ becomes isomorphic to $G_{\pi,-1}$ (multiply Z by this root). Thus all identities hold over the Zariski open subset of $Spec(R)$ where v is invertible. As it is Zariski-dense it first follows that $G_{u,v}$ becomes a commutative groupscheme with $\mathcal{O}$-action. That the action is strict then amounts to assertions about the vanishing of certain endomorphisms of $L^*_{G_{u,v}}$. But this complex is also free over R and the result holds over a Zariski-dense subset.

Remarks a) By pushout $G_{u,v}$ is defined over any base R if $u, v \in R$ satisfy $u \cdot v = -\pi$. Also for any unit w, $G_{u,v} \cong G_{u',v'}$ if $u' = uw^{q-1}$, $v' = vw^{1-q}$. We shall see that over an algebraically closed field k all simple finite strict $\mathcal{O}$-groupschemes are of the form $G_{u,v}$.

b) There exists a pairing $G_{u,v} \times G_{v,u} \to \mathcal{LT}[\pi]$, which on the level of rings sends the coordinate T of $\mathcal{LT}$ to the product $Z_{u,v} \otimes Z_{v,u}$ of the two coordinates. It follows easily from the definitions that this pairing is $\mathcal{O}$-bilinear. For example for linearity in the first variable one has

$$\begin{aligned} m^*_{u,v} \otimes 1(Z_{u,v} \otimes Z_{v,u}) &= \sum a_{ij}(-v)^{(i+j-1)/(q-1)} Z^i_{u,v} \otimes Z^j_{u,v} \otimes Z_{v,u} \\ &= \sum a_{ij} Z^i_{u,v} \otimes Z^j_{u,v} \otimes Z^{i+j}_{v,u} = m^*_{\mathcal{LT}}(Z_{u,v} \otimes Z_{v,u}). \end{aligned}$$

Furthermore this defines over the base $G_{v,u}$ a strict homomorphism $G_{u,v} \to \mathcal{LT}[\pi]$: It suffices to check over the open locus where v is invertible, and then at $v = 1$. But $G_{\pi,1} = \mathbb{F}_q$ which acts via multiplication on $G_{1,\pi} = \mathcal{LT}[\pi]$.

Even better one checks that $G_{v,u}$ represents the strict homomorphisms from $G_{u,v}$ into $\mathcal{LT}[\pi]$: Such a homomorphism (over any base) sends T into a multiple $z \cdot Z_{u,v}$, for a suitable constant z, because these are the unique $\mathbb{F}_q$-eigenvectors. Strict commutation with the element π means

$$\pi z Z_{u,v} + z^q Z_{u,v}^q = \pi_{u,v}^*(zZ_{u,v}) = z(\pi Z_{u,v} - vZ_{u,v}^q)$$

in $N_{G_{u,v}}^*$, which is a free module with basis $uZ_{u,v} + Z_{u,v}^q$. This translates into $z^q = -vz$, that is the equation for $G_{v,u}$.

We shall see later that the strict homomorphisms from $G_{u,v}$ to $\mathcal{LT}$ naturally have the structure of a strict $\mathcal{O}$-groupscheme which is the analogue of the usual Cartier-dual.

For later use we conclude this section not by another example but by an important general remark.

Proposition 2. *The kernel of a flat strict map of strict $\mathcal{O}$-groupschemes admits the structure of a strict $\mathcal{O}$-groupscheme which makes it a kernel in the additive category of strict $\mathcal{O}$-groupschemes. The analogue statement also holds for quotients under finite flat strict $\mathcal{O}$-subgroupschemes.*

Proof: Suppose $G_2 \to G_3$ is a strict flat map (of strict $\mathcal{O}$-groupschemes), with kernel G_1. An embedding of G_2 into a smooth R-scheme induces such an embedding of G_1 for which $G_1^\flat \subseteq G_2^\flat$ is defined by the product of the augmentation-ideal for $G_2^\flat$ and the pullback of the augmentation-ideal for $G_3^\flat$, thus inherits an $\mathcal{O}$-action. That the induced action on $L_{G_1}^*$ is via scalars follows because $N_{G_1}^*$ is generated by the images of $N_{G_2}^*$ and of Ω_{G_3}, and $\Omega_{G_1} = \Omega_{G_2}$. Also it is clear that with this action G_1 is a kernel in the category of strict $\mathcal{O}$-groupschemes.

For cokernels assume given an exact sequence

$$0 \to G_1 \to G_2 \to G_3 \to 0,$$

with G_1, G_2, and the map between them strict, and G_1 finite and flat over R. Obviously G_3 inherits an $\mathcal{O}$-action. Choose generators $S_i \in \mathcal{O}_{G_2}$ of the affine ring of G_2 as algebra over $\mathcal{O}_{G_3}$. These project to generators (over R) of $\mathcal{O}_{G_1}$. If we also choose R-generators T_j of $\mathcal{O}_{G_3}$ we obtain compatible embeddings of the G_i into affine spaces, with coordinates $\{S_i\}$, $\{S_i\} \cup \{T_j\}$, and $\{T_j\}$, and thus also maps between the $G_i^\flat$. Furthermore the sequence

$$0 \to \Omega_{G_3} \to \Omega_{G_2} \to \Omega_{G_1} \to 0$$

is exact.

For the conormal-bundles we obtain the same: As $\mathcal{O}_{G_2}$ is a relative complete intersection over $\mathcal{O}_{G_3}$ the fibre at the origin of its relative conormal-bundle coincides with $N_{G_1}^*$, and we also obtain an exact sequence

$$0 \to N_{G_3}^* \to N_{G_2}^* \to N_{G_1}^* \to 0.$$

We derive easily that $\mathcal{O}_{G_3}^\flat$ is a subring of $\mathcal{O}_{G_2}^\flat$ and equal to the intersection of the preimages of $\mathcal{O}_{G_3} \subseteq \mathcal{O}_{G_2}$ and of $R \subseteq \mathcal{O}_{G_1}^\flat$. It is thus stable under $\mathcal{O}$ which acts by scalar multiplication on Ω_{G_3} and $N_{G_3}^*$, hence a strict structure which also defines a cokernel in the strict category.

4. Strict $\mathcal{O}$-schemes over a field

As a starting point for various devissage arguments we first study the situation over a field k (which has to be an $\mathcal{O}$-algebra). We first show that kernels and cokernels of strict maps are naturally strict.

Theorem 3. *The strict $\mathcal{O}$-groupschemes over k form an abelian category. The forgetful functor to groupschemes is faithful and exact.*

Proof: We first show that the kernel G_1 of a strict map $f : G_2 \to G_3$ is strict again. It is obviously $\mathcal{O}$-stable and $G_1^\flat$ is a closed subscheme of $G_2^\flat$ whose ideal is generated by Ω_{G_3}. It is thus stable under the action of $\mathcal{O}$ which acts on Ω_{G_1} and $N^*_{G_1}$ by scalar multiplication because these are quotients of Ω_{G_2} respectively $N^*_{G_2} \oplus \Omega_{G_3}$. Also G_1 with its strict structure is obviously a kernel of f in the strict category.

For cokernels it now suffices to treat closed immersions (divide by the kernel), which we did in the previous proposition.

Next we classify simple finite strict $\mathcal{O}$-groupschemes over an algebraically closed field k.

Theorem 4. *Over an algebraically closed field k each nontrivial strict $\mathcal{O}$-groupscheme G contains a strict closed subscheme which is either $\mathbb{F}_q$, or isomorphic to α_q, or to $\mathcal{LT}[\pi]$.*

More precisely if the image of π in k is invertible each finite strict $\mathcal{O}$-groupscheme is constant.

Proof: If G is étale it is constant and contains $\mathbb{F}_q$. For example this happens if k has characteristic zero, or (as we shall see at the end) if π is invertible in k. If G is not étale (and simple) we may replace it by its connected component which is infinitesimal. Then the kernel of the Frobenius $Frob_q$ (q-th power map) is strict again, so we may assume that $Frob_q$ annihilates G. We first study the implications of that, without using the additional information that G is simple.

Consider the kernels of powers of the usual Frobenius $Frob_p$, the p-th power map. They are $\mathcal{O}$-stable but not strict and define a filtration (if $q = p^r$)

$$(0) \subset G_1 \subseteq G_2 ... \subseteq G_r = G.$$

The quotients G_i/G_{i-1} are annihilated by $Frob_p$ and such groupschemes are classified by a finite dimensional k-vectorspace E_i (the Lie-algebra, or the space of invariant derivations) together with a Frobenius-semilinear map $E_i \to E_i$ (p-th power of derivations). Furthermore $Frob_p$ induces semilinear injections $E_{i+1} \hookrightarrow E_i$ compatible with the powermaps. Finally $\mathcal{O}$ acts on the E_i by k-linear endomorphisms which commute with these semilinear maps.

The affine algebra $\mathcal{O}_G$ can be generated by elements $t_1, ..., t_d$ which are $\mathbb{F}_q^*$-eigenvectors to the standard embedding and form a basis of the dual of E_1. That is $\mathcal{O}_G = k[[t_1, ..., t_d]]/I$, and as I is also generated by $\mathbb{F}_q$-eigenvectors to the standard-embedding it contains only powerseries of degree $\geq q$. Especially any nontrivial k-linear combination of the $t_i^{q/p}$ does not lie in I, which translates into the fact that $Frob_p^{r-1}$ induces an isomorphism $E_r \cong E_1$. We derive that G has order q^d, and that I is generated by $t_1^q, ..., t_d^q$ (these elements lie in I because $Frob_q$ annihilates G).

Let us assume first that π vanishes in k, so multiplication by π has trivial differential and the kernel of π contains G_1. By the previous it must be all of G, thus $\mathcal{O}$ acts via its quotient $\mathbb{F}_q$ on G and on each E_i. On E_1 the action is by scalars $\mathbb{F}_q \subset k$, and thus on E_i via $Frob_p^{1-i}$.

If $r > 1$ all power maps vanish ($\mathbb{F}_q$-operation) so the subquotients are direct sums of α_p's. Next we analyse the extensions between them:

It is known that the space of extensions (of groupschemes) $Ext^1_k(\alpha_p, \alpha_p)$ is two dimensional, with possible generators α_{p^2} and the kernel of Frobenius on the Witt-vectors of length two (look at Dieudonneé-modules, or adapt the usual calculation of cocycles on the additive group). If $r > 2$ the latter lies in the wrong eigenspace under the $\mathbb{F}_q^*$-action, so cannot occur. Thus G_2 is isomorphic to a direct sum of α_{p^2}'s. Continuing this way we obtain that G_{r-1} is a direct sum of $\alpha_{q/p}$'s. Finally G itself is an extension of α_p^d by $\alpha_{q/p}^d$, and is the Baer sum of the extension α_q^d and an extension which is given by a $d \times d$ matrix of k-multiples of the extension $0 \to \alpha_{q/p} \to E \to \alpha_p \to 0$ which lies in the Witt-vectors of length 2 (this also uses that the tangentspace has dimension d). In Witt-coordinates it consists of those $(X_0, X_1) \in W_2$ for which $X_1^p = X_2^{q/p} = 0$. Thus we can describe G explicitely:

Denote by $\Phi_q(x, y) = ((x+y)^q - x^q - y^q)/p$ the standard cocycle for the additive group. Then there exists a matrix a_{ij} such that G is the subscheme of affine space defined by $t_1^q = ... = t_d^q = 0$, with addition

$$(x_i) +_G (y_i) = (x_i + y_i + \sum_j a_{ij} \Phi_q(x_j, y_j)).$$

Multiplication by p on $G^\flat$ is then

$$p \cdot_G (x_i) = (\sum_j a_{ij} x_j^q).$$

If K is ramified over $\mathbb{Q}_p$ multiplication by p on $G^\flat$ is divisible by the square of multiplication by π which in turn vanishes on G and thus is given by a homotopy. Thus p acts as zero which means that the matrix a_{ij} vanishes, and G is a direct sum of α_q. On $G^\flat$ π acts via a homotopy which is a k-linear map from the space generated by the t_i to that generated by the t_i^q, thus corresponds to a semilinear endomorphism of k^d. It has an eigenvector, so we can find a strict subscheme $H = \alpha_q$ such that π acts either as 0 or as nontrivial homotopy on $H^\flat$. These two cases are realised by $H = \alpha_q$ and $H = \mathcal{LT}[\pi]$.

If K is unramified over $\mathbb{Q}_p$ we can find an eigenvector of the matrix a_{ij} (which gives naturally a semilinear map) and find an $\mathcal{O}$-stable subscheme H which is necessarily strict. Again we have two possible isomorphism classes distinguished by the action of $p = \pi$ on $H^\flat$, and realised by α_q or $\mathcal{LT}[\pi]$.

In both cases $G = H$ if G is simple.

It remains the case that $\mathcal{O}$ injects into k. It then acts by scalar multiplication on E_1. Thus the action on E_2 must be via p-th roots of these, etc.. By linearity all powermaps vanish, so the subquotients are direct sums of α_p. Also the successive extensions can involve only α_{p^2} and one derives that G is a direct sum of α_{p^i} with scalar $\mathcal{O}$-action. However such sum cannot be made strict because $\mathcal{O}$ acts on N_G^* via higher powers of $Frob_p$. Thus simple G's are étale if $\mathcal{O}$ injects into k.

In fact our proof gives a little bit more, namely over any field k annihilated by π the classification of strict $\mathcal{O}$-groupschemes annihilated by $Frob_q$:

Proposition 5. *Suppose k is an extension field of $\mathbb{F}_q$, not necessarily algebraically closed. Then the category of finite strict $\mathcal{O}$-groupschemes G annihilated by $Frob_q$ is equivalent to the category of finite dimensional k-vectorspaces E together with a $Frob_q$-semilinear map $\alpha : E \to E$. The underlying vectorspace E is the Lie-algebra of G.*

Proof: We associate to (E, α) the group-scheme G whose underlying scheme is the kernel of $Frob_q$ on E. On it $\mathbb{F}_q$ acts by scalar multiplication. If K is ramified over $\mathbb{Q}_p$ the addition on G is given by that on E and π acts trivially on G itself but the extension to $G^\flat$ (which we construct using the embedding $G \subset E$) is described by the homotopy defined by α: $Frob_q$ defines an isomorphism between N_G^* and the $Frob_q$-pushout $\Omega_G \otimes_k k$, and Ω_G is dual to E. Then π is defined as the adjoint of α.

If K is unramified over $\mathbb{Q}_p$ the addition on the kernel of $Frob_q$ is modified by multiples of Φ_q as presribed by α.

The proof above shows that this induces an equivalence of categories over the algebraic closure $\bar{k}$ of k. It follows firstly that the above functor is fully faithful, because any map between G's induces a map between E's which is over $\bar{k}$ compatible with α's, thus also over k. Secondly it is essentially surjective: Given G, we take $E = Lie(G)$. As addition and multiplication by π are defined over k so is α.

Finally we study extensions of a finite strict G by $\mathbb{G}_a$ or by $\mathcal{LT}$.

Proposition 6. *Suppose G is a finite strict $\mathcal{O}$-groupscheme over an algebraically closed field field k. Then $dim(Ext_k^1(G, \mathbb{G}_a)) \leq dim(Hom_k(G, \mathbb{G}_a))$ (Homomorphisms and extensions in the category of strict $\mathcal{O}$-groupschemes).*

Also $Ext_k^1(G, \mathcal{LT}) = (0)$.

Proof It suffices to show this for simple G's using the long exact sequence for Ext-groups. If $G = \mathbb{F}_q$ is étale and π vanishes in k, $Hom_k(G, \mathbb{G}_a)$ is one-dimensional and generated by the inclusion $\mathbb{F}_q \subset k$. $Ext_k^1(G, \mathbb{G}_a)$ is generated by the pushout $\mathcal{O} \to k$ of $\mathcal{O} \xrightarrow{\pi} \mathcal{O} \to \mathbb{F}_q$. If π does not vanish in k both Hom_k and Ext_k^1 vanish because π acts as isomorphism on $\mathbb{G}_a$. Finally extensions by $\mathcal{LT}$ always split: First lift a generator of $\mathbb{F}_q$ to a k-point in the extension. As $\mathcal{LT}$ is π-divisible we can modify the lift so that it is annihilated by π and have a section.

Thus we may assume that G is infinitesimal and annihilated by $Frob_q$, so given by a pair (E, α). Also π vanishes in k. Any homomorphism into $\mathbb{G}_a$ factors over α_q and as $Frob_q$ is surjective on $\mathbb{G}_a$ and $\mathcal{LT}$ also all extensions are induced by extensions whose total space is annihilated by $Frob_q$. We are thus reduced to maps and extensions of vectorspaces E with semilinear α.

Maps into α_q correspond to maps $E \to k$ factoring over the cokernel of α. For extensions we consider vectorspaces F with a semilinear $\beta : F \to F$ such that F contains a β-stable line L, and $F/L = E$ with β inducing α on the quotient. For the $\mathbb{G}_a$- or α_q-case β vanishes on L, thus induces a semilinear lift $E \to F$ of α. Such lifts form a principal homogeneous space under the semilinear maps $E \to L$. Two such a semilinear map define isomorphic extensions if their difference factors over α. It follows that $Hom_k(G, \mathbb{G}_a)$ has dimension equal to that of the cokernel of α which is also un upper bound for the dimension of $Ext_k^1(G, \mathbb{G}_a)$.

For $\mathcal{LT}$- or $\mathcal{LT}[\pi]$-extensions β induces an isomorphism on L. Then (F, β) is the direct sum of two subobjects on which β is either nilpotent or isomorphic. L

is contained in the latter and the extension splits because the category of E with isomorphic β is equivalent to $\mathbb{F}_q$-vectorspaces.

5. Cartier-duality and vectorextensions

We show that strict homomorphisms into $\mathcal{LT}$ give rise to a duality. Assume G is a finite flat strict $\mathcal{O}$-groupscheme over a ring R.

Lemma 7. *G is annihilated by a power of π.*

Proof: This is true if G is étale or if R is a field (devissage reduces to simple objects). In these cases G is even annihilated by π^h if its rank is q^h (it is always a power of q, and locally constant). It follows that, in the general case, multiplication by π^h defines an endomorphism of the ideal $I_G \subset \mathcal{O}_G$ (defining 0) whose matrix-coefficients are nilpotent, so some power of this map vanishes.

As an application we note that G is defined over a finitely generated $\mathcal{O}$-subalgebra of R as $\mathcal{O}$ acts via a finitely generated quotient. This will allow us in the sequel to assume that R is noetherian.

Remark It is natural to conjecture that G is annihilated by π^h if it has rank q^h.

The strict homomorphisms of G into the π-divisible $\mathcal{O}$-module $\mathcal{LT}$ are representable by a finitely presented affine scheme G^{dual} over R: If G is annihilated by π^h such a homomorphism factors over $\mathcal{LT}[\pi^h]$, which is a closed subscheme of the affine line. Hence such a homomorphism is determined by the pullback of the affine coordinate T of $\mathcal{LT}$, which is an element of $\mathcal{O}_G$ or better the ideal I_G defining the origin. That such an element defines a strict homomorphism amounts to certain equations. Thus homomorphisms are represented by a quotient of the symmetric algebra over I_G^{dual}. It is obvious that G^{dual} is a groupscheme and admits an action of $\mathcal{O}$. Also G^{dual} is quasifinite over R: Namely it suffices to check that over an algebraically closed field k it has only finitely many points. By devissage we reduce to simple G's. These are isomorphic to a $G_{u,v}$ with finite dual $G_{v,u}$.

Theorem 8. *G^{dual} is finite and flat over R, of the same rank as G. It is a strict $\mathcal{O}$-groupscheme (that is there is a natural way to define a strict structure) such that its dual is again isomorphic to G. The duality functor exchanges closed immersions and faithfully flat homomorphisms.*

All strict extensions of G by $\mathcal{LT}^d$ split locally in the flat topology.

Proof: We may assume that R is noetherian. To show that G^{dual} is finite and flat of the same rank as G it then suffices to check over artinian basis: If the assertion holds there G^{dual} is already quasifinite. Over the completion of any local ring of R it then becomes the disjoint union of a finite scheme and another scheme with empty special fibre. The finite part is flat of the same rank as G thus the rest has empty fibres (check ranks) and we are done. The same reasoning applies to the fact that the dual of a closed immersion is faithfully flat. Finally splittings of an $\mathcal{LT}^d$-extension are representable, and to show that the scheme representing them is faithfully flat we can also reduce to the artinian case.

So let us assume that R is local artinian. Then G becomes an extension

$$0 \to G^{inf} \to G \to G^{et} \to 0,$$

with G^{inf} connected and the quotient G^{et} étale. By descent to the constant case the assertions hold for G^{et}, and there is an exact sequence (of fppf-sheaves)

$$0 \to G^{et,dual} \to G^{dual} \to G^{inf,dual} \to 0.$$

We thus may assume that G is connected, that is the ideal I_G is nilpotent, and also that π is nilpotent in R (otherwise everything is étale). We define a unipotent groupscheme $\mathcal{MAP}_0(G, \mathcal{LT}^f)$ (pointed maps into the formal group $\mathcal{LT}^f$) as follows:

The underlying scheme is the affine space I_G, that is the affine algebra is the symmetric algebra in I_G^{dual}. The comultiplication is defined by the formula for the Lubin-Tate group law, applied to two elements of I_G. As I_G is nilpotent we obtain indeed polynomials and not just powerseries. Similarly we get an $\mathcal{O}$-action by the Lubin-Tate formulas, that is $\mathbb{F}_q$ acts by scalar multiplication and π by sending $T \in I_G$ to $\pi \cdot T + T^q$.

We define an $\mathcal{O}$-linear map from $\mathcal{MAP}_0(G, \mathcal{LT}^f)$ to the product of $\mathcal{MAP}_0(G \times G, \mathcal{LT}^f)$ and two copies of $\mathcal{MAP}_0(G^\flat, \mathcal{LT}^f)$, as follows:

For a pointed map $f : G \to \mathcal{LT}^f$ the first component of its image is given by $f(x+y) - f(x) - f(y)$, that is it measures the lack of additivity for f. The other two components measure the commutation with π and a generator of $\mathbb{F}_q^*$. (The latter could be dropped if we replace I_G by the correct eigenspace for the $\mathbb{F}_q$-action.) Obviously G^{dual} is the kernel of our map.

Its image is contained in a certain closed subscheme $\mathcal{Z}$ (1-cocycles), which parametrises extensions

$$0 \to \mathcal{LT}^f \to E \to G \to 0$$

of strict $\mathcal{O}$-ind-groupschemes together with a pointed map of schemes $G \to E$ which is a section: Namely as an ind-scheme E is the product of $\mathcal{LT}^f$ and G but the addition differs from that of the product by a map from $G \times G$ to $\mathcal{LT}^f$ which is symmetric and satisfies a cocycle equation. Similar considerations apply to the action of $\mathbb{F}_q^*$ and of π. The subscheme $\mathcal{Z}$ is defined by the various conditions and compatabilites these must satisfy. The homomorphism $\mathcal{MAP}_0(G, \mathcal{LT}^f) \to \mathcal{Z}$ describes sections of the trivial extension E.

We remark that for any R-algebra S the cokernel of $\mathcal{MAP}_0(G, \mathcal{LT}^f)(S) \to \mathcal{Z}(S)$ is equal to $Ext^1_S(G, \mathcal{LT}^f)$: This means that any extension has a scheme-theoretic section. This holds for the formal completions along the origin (lift a coordinate T of $\mathcal{LT}^f$ to a formal function on E), and this suffices because G is infinitesimal.

We claim that the map $\mathcal{MAP}_0(G, \mathcal{LT}^f) \to \mathcal{Z}$ is faithfully flat:

It is surjective because for any algebraically closed field k (over R) the induced map on k-points is surjective (extensions are trivial). Also over such a field the dimension of the tangent-space of $\mathcal{Z}$ can be estimated by proposition 5:

Namely we have to consider isomorphism-classes (extension+section) over the dual numbers $k[\epsilon]$, trivial module ϵ. The extensions are classified by $Ext^1_k(G; \mathbb{G}_a)$, the sections form a principal homogeneous space under I_G, and the automorphisms are $Hom_k(G, \mathbb{G}_a)$. By proposition 5 the tangent-space to $\mathcal{Z}$ has dimension $\leq$ the rank of I_G, that is the relative dimension of $\mathcal{MAP}_0(G, \mathcal{LT}^f)$. As the kernel G^{dual} of the map from this group into $\mathcal{Z}$ is quasifinite it follows that (over k algebraically closed) the map is finite and faithfully flat and $\mathcal{Z}$ is smooth. Now we use the following easy to show

Lemma 9. *Suppose A and B are finitely generated algebras over the local artinian ring R, with B flat over R, and $A \to B$ an R-linear homomorphism which is faithfully flat over the residue field of R. Then it is faithfully flat over R.*

It implies that $\mathcal{MAP}_0(G, \mathcal{LT}^f) \to \mathcal{Z}$ is faithfully flat and its image is smooth. Especially the kernel G^{dual} is flat. Also any class in $Ext^1_R(G, \mathcal{LT})$ is trivial locally in the fppf-topology.

Next we show that the rank of G^{dual} is equal to that of G: It suffices to show this over an algebraically closed field k. The assertion holds for simple G's, all isomorphic to a $G_{u,v}$. Furthermore short exact sequences

$$0 \to G_1 \to G_2 \to G_3 \to 0$$

induce exact sequences

$$0 \to G_3^{dual} \to G_2^{dual} \to G_1^{dual}.$$

It thus suffices to show that closed immersions dualise to faithfully flat surjections which follows from local triviality of Ext^1.

To finish the proof of the theorem we have to define a strict $\mathcal{O}$-action on G^{dual}, and show biduality, over an arbitrary G over an arbitrary noetherian base R (not assumed to be artinian). For the strict $\mathcal{O}$-action we not that G^{dual} is a closed subscheme of the ind-groupscheme $\mathcal{MAP}_0(G, \mathcal{LT})$ whose underlying ind-scheme consists of $T \in I_G$ annihilated by some F_n^{a+1}, F_n the n-fold iteration of the polynomial $\pi \cdot T + T^q$. It is formally smooth thus contains also (a model of) $G^{dual,\flat}$.

The $\mathcal{O}$-action stabilises $G^{dual,\flat}$ and acts by scalar multiplication on $N^*_{G^{dual}}$ because G^{dual} is the kernel of a map into products of ind-groupschemes like $\mathcal{MAP}_0(G \times G, \mathcal{LT})$ whose formal completions at the origin are strict $\mathcal{O}$-modules.

Finally this implies that sections of G define strict homomorphisms $G^{dual} \to \mathcal{LT}$, thus $G \to (G^{dual})^{dual}$. That this is strict follows because the pairs consisting of a strict homomorphism from G to $\mathcal{LT}$ together with an extension to $G^\flat$ are representable by a strict vectorextension EG^{dual} of G^{dual} which is the kernel of a map from $\mathcal{MAP}_0(G^\flat, \mathcal{LT})$ to the product $\mathcal{MAP}_0(G \times G, \mathcal{LT}) \times \mathcal{MAP}_0(G^\flat, \mathcal{LT})^2$, so that we get an $\mathcal{O}$-bilinear pairing $G^\flat \times EG^{dual} \to \mathcal{LT}$ which suffices to derive strictness.

That the biduality map is an isomorphism can be checked over algebraically closed fields. By devissage it suffices to consider simple objects $G_{u,v}$ where the assertion follows by direct calculation: We have already seen that $G_{v,u}$ represents the strict homomorphisms into $\mathcal{LT}$ and need to check that the strict structures coincide. It suffices to do this over the base $R = \mathcal{O}[u,v]/(u \cdot v + \pi)$. But the difference of two strict structures is given by endomorphisms of degree -1 of $L^*_{G_{v,u}}$ which necessarily vanish over this base.

So finally the theorem is completely shown.

Next we discuss vectorextensions. A vectorgroup is a groupscheme which is Zariski-locally isomorphic to the product of finitely many copies $\mathbb{G}_a$, and a linear map between vectorgroups is a map defined by a matrix with entries in R (in positive characteristics $\mathbb{G}_a$ has more endomorphisms).

Definition 10. *A vectorextension of G by a complex $U \to V$ (a linear map of vectorgroups) is a strict extension*

$$0 \to U \to E \to G \to 0$$

of strict $\mathcal{O}$-groupschemes, together with a strict $\mathcal{O}$-linear map $E \to V$ which induces the given linear map on U. It is called universal if any strict extension of G by a *vectorgroup is pushout from E via a linear map, and any strict map of E into a vectorgroup factors uniquely over V, provided it is linear on U.*

One checks easily that if E is a universal extension of G by $U \to V$ any other extension by (say) $U' \to V'$ is pushout by a map of complexes from $U \to V$ to $U' \to V'$, unique up to homotopy. The homotopy is not unique but two homotopies differ by a map of complexes of degree -1, and such maps act as automorphisms of the extensions.

Our basic example of an extension is constructed as follows: Consider the dual G^{dual}. Any section of G defines a strict $\mathcal{O}$-linear map $G^{dual} \to \mathcal{LT}$ which extends to an $\mathcal{O}$-linear $G^{dual,\flat} \to \mathcal{LT}^{\flat}$. The ambiguity of this extension defines a vectorextension

$$0 \to N^*_{G^{dual}} \to EG \to G \to 0,$$

which admits an $\mathcal{O}$-action. That is EG is the fibered product of G and $\mathcal{MAP}_0(G^{dual,\flat}, \mathcal{LT})$ over $\mathcal{MAP}_0(G^{dual}, \mathcal{LT})$. Here the mapping-schemes are formally smooth ind-schemes with a strict $\mathcal{O}$-action, inherited from $\mathcal{LT}$. For example for any R-algebra S the S-points of $\mathcal{MAP}_0(G^{dual}, \mathcal{LT})$ consists of elements of $\mathcal{O}_{G^{dual}} \otimes_R S$ which lie in the augmentation-ideal and are annihilated by a power of an iteration of the polynomial $\pi T + T^q$. The $\mathcal{O}$-action on the fibered product is strict.

Furthermore the projection from $I_{G^{dual,\flat}}$ or $\mathcal{O}_{G^{dual,\flat}}$ to $\Omega_{G^{dual}}$ defines a strict map $EG \to \Omega_{G^{dual}}$. Thus an extension of G by $L^*_{G^{dual}}$.

Proposition 11. *EG is a universal vectorextension of G.*

Proof: We may assume that our base R is noetherian. Any strict extension $\mathbb{G}_a \to E \to G$ has a section, thus is defined by a cocycle which is given by pointed maps from $G \times G$ and $G^{\flat}$ (twice) to the affine line satisfying certain identities which are the additive analogues of the identities defining $\mathcal{Z}$. This defines a submodule Z of $\mathcal{O}_{G\times G} \times \mathcal{O}^2_{G^{\flat}}$ which is the intersection of kernels of certain linear forms. Elements of Z are in bijection with isomorphism classes of strict extensions $\mathbb{G}_a \to E \to G$ together with a pointed (nonlinear) section. The first coordinate describes the lack of additivity for such a section, the other two the lack of commutation with π or ζ.

I_G maps into Z as space of pointed sections on the trivial extension. In fact it extends to $I^{(1)}_{EG}$, the space of pointed maps $EG \to \mathbb{G}_a$ which are affine linear under translation with $N^*_{G^{dual}}$: Namely such a map defines a section for the vectorextension defined by pushforward via its restriction to $N^*_{G^{dual}}$. Also an element of $I^{(1)}_{EG}$ defines the trivial pair (extension+section) if and only if it is a strict homomorphism from EG to $\mathbb{G}_a$. Our claim amounts to the fact that the space of such strict homomorphisms is $\Omega^{dual}_{G^{dual}}$ and that the map from $I^{(1)}_{EG}$ into Z is surjective. It suffices to check that after tensoring with a field, so we may assume that R is an algebraically closed field.

In this case the assertion holds for simple objects by the calculations in proposition 5. Namely for $\mathcal{LT}[\pi]$ extensions and homomorphisms vanish. For the other two simple objects there exists a nontrivial universal extension by $\mathbb{G}_a$. Any homomorphisms of it into $\mathbb{G}_a$ factor over G and are parametrised by the Lie-algebra of G^{dual}, as they define over the dual numbers strict homomorphisms into $\mathcal{LT}$. To see that our vectorextension is isomorphic to EG note that otherwise the extension EG would be trivial (it is after all a pushout from the universal extension). That means G lifts to maps from $G^{dual,\flat}$ into $\mathcal{LT}^{\flat}$, or $G^{dual,\flat}$ to maps from G to $\mathcal{LT}^{\flat}$.

The fact that the splitting of EG is strict translates into the fact that $G^{dual,\flat}$ gives strict maps, that is $G^{dual,\flat}$ retracts into G^{dual}. However this is impossible.

Also for an exact sequence

$$0 \to G_1 \to G_2 \to G_3 \to 0$$

we can choose representatives for the G_i^{dual} such that the sequence of complexes

$$0 \to L^*_{G_1^{dual}} \to L^*_{G_2^{dual}} \to L^*_{G_3^{dual}} \to 0$$

is exact as well. It then follows by an easy devissage that the assertion for G_1 and G_3 implies it also for G_2.

Remark: More generally any R-module M defines a functor on flat R-algebras, sending S to $M \otimes_R S$. We then can define maps into M respectively extensions by M as maps respectively extensions of functors. They are governed by a complex, which is essentially the previous complex tensored with M. It then follows that EG retains its universal properties also in this extended category: Check over a field and for finitely generated M, in which case there is no difference.

In the following we will often encounter such "module-extensions".

¿From a universal vectorextension we construct a complex $M(G)$, the "first homology" of G:

Extend the map $EG \to \Omega_{G^{dual}}$ to $EG^\flat$. This induces $Lie(EG) = \Omega_{EG}^{dual} \to \Omega_{G^{dual}}$. Also we have the canonical $Lie(EG) \to Lie(G) \to N_G$, and $M(G)$ is defined as the complex

$$Lie(EG) \to N_G \oplus \Omega_{G^{dual}}.$$

There is an exact sequence

$$0 \to L^*_{G^{dual}}[-1] \to M(G) \to L_G \to 0,$$

so $M(G)$ is a filtered complex.

Next we analyze the degree of arbitrariness involved in the construction:

a) Two different choices for the extension $EG^\flat \to \Omega_{G^{dual}}$ differ by an $N_G \to \Omega_{G^{dual}}$, which defines a unipotent automorphism of $N_G \oplus \Omega_{G^{dual}}$ and a filtered isomorphism between the two complexes. That is EG determines $M(G)$ up to unique automorphism.

b) For a map $G_1 \to G_2$ any extension to $EG_1 \to EG_2$ and $EG_1^\flat \to EG_2^\flat$ defines a map on $M(G)$'s. Different extensions to $EG^\flat$'s and homotopies of EG's give rise to filtered homotopies of maps.

That is all in all $M(G)$ is a filtered complex, functorial in G up to filtered homotopy.

Remark: With some effort one can show at this stage that $M(G^{dual})$ is the dual of $M(G)$, inducing the obvious duality on the filtered subquotients. Namely one checks that the ambiguity in extending $EG \to \Omega_{G^{dual}}$ to $EG^\flat$ is the same is that in splitting $\Omega_{G^{dual}} \to \Omega_{EG^{dual}}$, so that $M(G)$ can be represented by a map $Lie(EG) \to Lie(EG^{dual})^{dual}$, which is the adjoint of the analogeous map constructed for G^{dual}. We postpone this verification since it will follow quite easily from the (infinite dimensional) constructions used in lifting-theory.

6. Liftings over nilpotents

In this section we present some lifting constructions for infinitesimal thickenings. Their common feature is that liftings of objects and maps exist but are not unique modulo homotopy. In the next section we show how to remedy this for DP-thickenings. In this section we use the Lubin-Tate group $\mathcal{LT}'$ with logarithm $\sum T^{q^n}/\pi^n$ which differs from $\mathcal{LT}$ by an unramified character of $Gal(\bar{K}/K)$. It has the property that $T = t$ defines a typical curve fixed by F_π, so that its Dieudonné-module $Hom_R(\hat{W}_{\mathcal{O}}, \mathcal{LT}')$ is isomorphic to $W_{\mathcal{O}}(R)$. Recall that a formal $\mathcal{O}$-module is an ind-groupscheme representable by an algebra of powerseries (in possibly infinitely many variables), with an $\mathcal{O}$-action inducing scalar multiplication on the Lie-algebra. For example the Witt-vectors $\hat{W}_{\mathcal{O}}$ are the (infinite dimensional) formal $\mathcal{O}$-module such that $\hat{W}_{\mathcal{O}}(R)$ consists of infinite sequences $(x_0, x_1, ...)$ of elements of R, all nilpotent and almost all of them vanishing. Addition and multiplication are defined by certain universal polynomials uniquely determined by the fact that $w_n = x_0^{q^n} + ... + \pi^{n-1} \cdot x_{n-1} + \pi^n \cdot x_n$ is a functorial homomorphism into R.

Formal $\mathcal{O}$-modules $\mathcal{H}$ are classified by their Dieudonné module $M(\mathcal{H})$ which is a left module over the Cartier-ring $Cart_{\mathcal{O}}(R) = Cart(R)$. Elements of $Cart(R)$ are formal sums $\sum_{m,n} V^m[a_{m,n}]F^n$, with $a_{m,n} \in R$, and for fixed m almost all $a_{m,n}$ vanish. Multiplication is given by certain universal formulas (see [1]). The Dieudonné-modules of formal $\mathcal{O}$-modules have the property that multiplication by V is injective, and its cokernel is a free R-module (the Lie-algebra). For example the Dieudonné-module of $\hat{W}_{\mathcal{O}}$ is $Cart(R)$ itself. Thus any direct sum (even infinite) of $\hat{W}_{\mathcal{O}}$'s is "projective" in the sense that we can lift over smooth maps $\mathcal{H}_1 \twoheadrightarrow \mathcal{H}_2$ of formal $\mathcal{O}$-modules, or that a map $\hat{W}_{\mathcal{O}} \to \mathcal{H}$ defined over a quotient R/J lifts to a map defined over R. Any formal $\mathcal{O}$-module $\mathcal{H}$ has a presentation

$$\hat{W}_{\mathcal{O}}^{(M)} \to \hat{W}_{\mathcal{O}}^{(N)} \twoheadrightarrow \mathcal{H},$$

that is the sequence is exact and the last map is smooth.

If we have an ind-groupscheme $\mathcal{G}$ which can be written as $\mathcal{G} = \varinjlim Spec(A_n)$ with a countable system of finitely presented R-algebras A_n and surjections $A_{n+1} \twoheadrightarrow A_n$, we can form its formal completion $\hat{\mathcal{G}}$ whose S-points are elements of $\mathcal{G}(S)$ trivial modulo some nilpotent ideal of S. It can be ind-represented by a similar system B_n where the B_n are now finite over R. If $\mathcal{G}$ is formally smooth so is $\hat{\mathcal{G}}$ and it can be ind-represented by (the discrete quotients) of a topological algebra $\hat{S}(P)$, the completed symmetric algebra of a topological module P which is a direct summand in $\varprojlim R^n$. If in addition $\mathcal{O}$ acts on $\mathcal{G}$ such that the induced action on the Lie-algebra is via scalars $\hat{\mathcal{G}}$ satisfies all the axioms of a formal $\mathcal{O}$-module except that its Lie-algebra may not be a free module. However it is a direct summand of a formal $\mathcal{O}$-module. It follows by passing to the formal completion that any formally smooth morphism $\mathcal{G} \to \hat{W}_{\mathcal{O}}$ admits a section.

One of our basic object of interest is the following formal $\mathcal{O}$-module: Start with the functor which associates to an R-algebra S the ring $S[[T_1, ..., T_d]]$ of powerseries in d variables. With the Lubin-Tate group law $\mathcal{LT}'$ the ideal $(T_1, ..., T_d)$ of powerseries without constant term becomes an $\mathcal{O}$-module which is functorial in S. It is a prounipotent algebraic group U_d with $\mathcal{O}$-action acting by scalar multiplication on its Lie-algebra, and a successive extension of additive groups. As such its is isomorphic to an infinite product of $W_{\mathcal{O}}$'s: For example in one variable we obtain the functor of all curves in $\mathcal{LT}$ which admits the usual operations F_n and V_n. It contains the p-typical curves and the Dieudonné-module $M(\mathcal{LT})$ of $\mathcal{LT}$ which is $W_{\mathcal{O}}$. Furthermore the module of all curves is the product of the transforms of $M(\mathcal{LT})$ by all operators V_n, n an integer whose greatest common divisor with q is a p-power $p^i < q$. For several variables one uses instead operators $F_{n,i}$ and $V_{n,i}$ separately for each variable. The factors of twisted $W_{\mathcal{O}}$ are naturally indexed by monomials $\prod T_i^{n_i}$ where not all the exponents are divisible by q.

Similarly we could start with the polynomialring $S[T_1, ..., T_d]$ and consider the formal $\mathcal{O}$-module $\mathcal{U}_d$ defined by adding nilpotent polynomials without constant term according to the Lubin-Tate law $\mathcal{LT}'$. It is an infinite sum of copies of $\hat{W}_{\mathcal{O}}$ indexed by monomials with exponent not divisible by q. For example the p-typical curves $t \cdot \prod T_i^{n_i}$ define homomorphisms $\hat{W}_{\mathcal{O}} \to \mathcal{U}_d$. There exists a pairing $U_d \times \mathcal{U}_d \to \mathcal{LT}'$ defined componentwise, inducing $U_d = Hom(\mathcal{U}_d, \mathcal{LT}')$.

Conversely $\mathcal{U}_d$ maps to $Hom(U_d, \mathcal{LT}')$ (maps of functors). I do not know whether this is an isomorphism but I can show that it is formally étale: It suffices to consider the duality between $W_{\mathcal{O}}$ and $\hat{W}_{\mathcal{O}}$. Suppose $J \subset R$ is an ideal of square zero, and suppose given a homomorphism $W_{\mathcal{O}} \to \mathcal{LT}'$ which modulo J is induced by an element of $\hat{W}_{\mathcal{O}}(R/J)$. If we lift this element somehow to $\hat{W}_{\mathcal{O}}$ the difference of the two resulting homomorphisms into $\mathcal{LT}'$ induces on $\hat{W}_{\mathcal{O}} \subset W_{\mathcal{O}}$ an infinite linear combination of w_n's with coefficients in J. As it has bounded polynomial degree almost all the coefficients vanish, so by changing the lift we may assume that the difference of maps vanishes on $\hat{W}_{\mathcal{O}}$ and thus also on $W_{\mathcal{O}}$.

Given G a finite flat strict $\mathcal{O}$-groupscheme over R embed G and G^{dual} into affine spaces $\mathbb{A}^d$ and $\mathbb{A}^e$, and assume that they are defined by d respectively e equations which form a regular sequence (which is always true Zariski-locally). That is $\mathcal{O}_G = R[X_1, ..., X_d]/(f_1, ..., f_d)$ and $\mathcal{O}_{G^{dual}} = R[Y_1, ..., Y_e]/(g_1, ..., g_e)$, and the origin is defined by the vanishing of the S_i respectively T_j. Duality $G \times G^{dual} \to \mathcal{LT}' \subset \mathbb{A}^1$ defines an embedding of G into the affine space $\mathcal{O}_{G^{dual}}$ (even into the ideal generated by the Y_j). Denote by $\mathcal{G}$ the ind-scheme which is formal completion of $\mathcal{O}_{G^{dual}}$ along G. It is prorepresented by the completion of the symmetric algebra $S(\mathcal{O}^{dual}_{G^{dual}})$ in the topology defined by the powers of an ideal locally generated by a regular sequence, and thus an inductive limit of finite flat R-schemes. The Lubin-Tate law $\mathcal{LT}'$ defines on it the structure of a formally smooth ind-groupscheme with $\mathcal{O}$-action acting by scalar multiplication on the Lie-algebra. For any flat R-algebra S $\mathcal{G}(S)$ consists of elements $t \in \mathcal{O}_{G^{dual}} \otimes_R S$ such that modulo some nilpotent ideal of S t lies in the image of G. There exists an extension $E\mathcal{G}$ of $\mathcal{G}$ by $N^*_{G^{dual}} = R^e$ which maps into $\Omega_{G^{dual}}$.

Furthermore $\mathcal{LT}'$ defines the structure of a prounipotent strict $\mathcal{O}$-algebraic group U on the ideal generated by $g_1, ..., g_e$ in the completion $R[Y_1, \hat{...}, Y_e]$ of the polynomial-ring along this ideal, and more generally a functorial $\mathcal{O}$-module structure on the inverse image of $\mathcal{G}$ in this completion. We thus obtain an extension

$$U \to \mathcal{M} \to \mathcal{G}$$

of functors on R-algebras, or of sheaves in the fpqc-topology. It induces $E\mathcal{G}$ via pushout with $U \to N^*_{G^{dual}}$ (map to leading term).

Lemma 12. *There exists an extension $U_e \to \mathcal{E}G \to G$ inducing EG via pushout $U_e \to N^*_{G^{dual}}$ (map to linear terms). Furthermore $G \subset \mathcal{G}$ lifts to $\mathcal{E}G \to \mathcal{M}$ such that the restriction to U_e is induced by a ring-homomorphism $R[[T_1, ..., T_e]] \to$*

$R[Y_1, \hat{...}, Y_e]$ which sends each T_j to the sum of g_j and an element in the product of the ideals (Y_j) and (g_j). All $\mathbb{G}_a$-extensions of $\mathcal{E}G$ are trivial. This also holds for module-extensions.

Proof: The prounipotent group U has a filtration induced by powers of the ideal $(g_1, ..., g_e)$, with subquotients additive groups. If we have defined the homomorphism $R[[T_1, ..., T_e]] \to R[Y_1, \hat{...}, Y_e]$ modulo the n-th power of this ideal such that modulo this power the extension of G induced by $\mathcal{M}$ reduces to U_d, the obstruction in the next step is a vectorextension of G. It is induced from EG via a homomorphism from $N^*_{G^{dual}}$ into the n-th subquotient, which prescribes how one has to modify the homomorphism $R[[T_1, ..., T_e]] \to R[Y_1, \hat{...}, Y_e]$.

A $\mathbb{G}_a$-extension of $\mathcal{E}G$ splits over U_e because $W_{\mathcal{O}}$ has no such extensions: Reduce to the fact that extensions of $\mathbb{G}_a$ by $\mathbb{G}_a$ are defined by linear combinations of the cocycles $((X+Y)^{q^n} - X^{q^n} - Y^{q^n})/\pi$ which are split by $W_{\mathcal{O}} \to \mathbb{G}_a$. Thus the $\mathbb{G}_a$-extension of $\mathcal{E}G$ is induced from G and already splits over EG.

Concerning uniqueness of the construction one notes that EG was unique up to homotopies $\Omega_{G^{dual}} \to N^*_{G^{dual}}$, which lift to endomorphisms of $\mathcal{E}G$.

Let $(\mathcal{E}G)^*$ represent pair consisting of an element of $\mathcal{U}_e$ and a strict $\mathcal{O}$-linear extension to $\mathcal{E}G$ of the map $U_e \to \mathcal{LT}'$ defined by it. As G^{dual}-torsor are locally trivial such an extension exists locally in the flat topology. It follows that $(\mathcal{E}G)^*$ is representable by an ind-groupscheme sitting in an extension

$$G^{dual} \to (\mathcal{E}G)^* \to \mathcal{U}_e.$$

Furthermore as $\mathcal{E}G$ admits no vectorextensions $(\mathcal{E}G)^*$ is formally smooth: Given a map $\mathcal{E}G \to \mathcal{LT}'$ over R/J with $J^2 = (0)$ whose restriction to U_e is induced by an element of $\mathcal{U}_e$, we can lift the map (liftings over nilpotents gives module-extensions) and it is again induced by an element of $\mathcal{U}_e$. Finally $\mathcal{O}$ acts by scalars on the Lie-algebra of $(\mathcal{E}G)^*$, by considering maps over dual numbers.

We claim that we can combine $\mathcal{E}G$ and $(\mathcal{E}G^{dual})^*$ to a mixed extension, that is a complex

$$U_e \to \mathcal{F}G \to \mathcal{U}_d$$

with cohomology G such that $\mathcal{F}G$ is at the same time an extension of $(\mathcal{E}G^{dual})^*$ by U_e and of $\mathcal{U}_d$ by $\mathcal{E}G$. Namely as $\mathcal{G}$ is formally smooth the extension of $\mathcal{U}_d$ by $\mathcal{G}$ induced from $(\mathcal{E}G^{dual})^*$ via $G \subset \mathcal{G}$ splits, thus a map from $(\mathcal{E}G^{dual})^*$ to $\mathcal{G}$. The pullback of $\mathcal{M}$ defines an extension of $(\mathcal{E}G^{dual})^*$ by U which reduces on G to an extension by U_e. The obstruction for this to extend to $(\mathcal{E}G^{dual})^*$ is an extension of $\mathcal{U}_d$ by U/U_e which splits.

We also remark that any two mixed extensions inducing $\mathcal{E}G$ and $(\mathcal{E}G^{dual})^*$ differ by an extension of $\mathcal{U}_d$ by U_e which necessarily splits. Thus $\mathcal{F}G$ is up to isomorphism independant of choices, or better only dependant on the choices involved in the construction of $\mathcal{E}G$ and of $\mathcal{E}G^{dual}$. Furthermore the isomorphism is unique up to a homomorphism $\mathcal{U}_d \to U_e$. Also if we perform the same construction with G^{dual} and form homomorphisms into $\mathcal{LT}'$ (as in the construction of $(\mathcal{E}G)^*$) we obtain another such mixed extension. It follows that there exists a bilinear pairing $\mathcal{F}G \times \mathcal{F}G^{dual} \to \mathcal{LT}'$ inducing the canonical pairings on the subquotients. It is unique up to a pairing $\mathcal{U}_d \times \mathcal{U}_e \to \mathcal{LT}'$.

Next we come to the lifting problem. Suppose $J \subset R$ is a nilpotent ideal and we are given $\bar{G}$ over $\bar{R} = R/J$ from which we get $\mathcal{F}\bar{G}$, $\mathcal{F}\bar{G}^{dual}$ etc., which we try to lift to R. First of all we can lift $\mathcal{O}_{\bar{G}}$ and $\mathcal{O}_{\bar{G}^{dual}}$ as finite flat algebras which are complete intersections. This induces lifts of $\bar{\mathcal{G}}$, $\bar{\mathcal{M}}$, and of $\bar{U}_e$ and $\bar{\mathcal{U}}_d$. Now $\mathcal{F}\bar{G}$ embeds as a closed subgroup into $\bar{\mathcal{M}} \times \bar{\mathcal{U}}_d$ with formally smooth quotient. If we have already lifted it to R/J^n and try to lift to R/J^{n+1}, the relevant obstruction is a module-extension of $\mathcal{F}\bar{G}$ by $J^n/J^{n+1} \otimes_{\bar{R}} Lie(\bar{\mathcal{M}} \times \bar{\mathcal{U}}_d/\mathcal{F}\bar{G})$. It is trivial as $\mathcal{E}\bar{G}$ as well as $\bar{\mathcal{U}}_d$ have no module-extensions. Thus we have found a lift $\mathcal{F}G$ together with a map $\mathcal{F}G \to \mathcal{U}_d$. Its kernel is a lift $\mathcal{E}G$ of $\mathcal{E}\bar{G}$. Although we can lift $\bar{U}_e$ as a subgroup of $\mathcal{F}G$ it may be impossible to lift it in $\mathcal{E}G$. Namely if that is possible the quotient defines a lift G of $\bar{G}$. Finally the pairing into $\mathcal{LT}'$ lifts to $\mathcal{F}G \times \mathcal{F}G^{dual} \to \mathcal{LT}'$: Obstructions are additive biextensions of $\mathcal{F}\bar{G} \times \mathcal{F}\bar{G}^{dual}$ which are trivial as both factors have no $\mathbb{G}_a$-extensions.

Finally a map $\bar{G}_1 \to \bar{G}_2$ induces a map $\mathcal{F}\bar{G}_1 \to \mathcal{F}\bar{G}_2$ which lifts to $\mathcal{F}G_1 \to \mathcal{F}G_2$ (no vectorextensions). However this lift is far from being unique (or unique up to some reasonable homotopy), nor can we expect it to respect maps into $\mathcal{U}_d$'s.

To conclude the definitions we choose a lift $U_e \to \mathcal{F}G$, and denote by FG the induced vectorextension

$$N^*_{G^{dual}} \to FG \to \mathcal{F}G/U_e.$$

In the next section we will need the following universal property of the extension:

Lemma 13. *Any vectorextension*

$$\mathbb{G}_a \to \mathcal{E} \to \mathcal{F}G/U_e$$

is induced from FG via an element of $N_{G^{dual}}$.

Proof: If the assertion holds modulo J^n, lift the element of $N_{G^{dual}}$ modulo J^{n+1}, to obtain a module extension of $\mathcal{F}\bar{G}/\bar{U}_e$ by J^n/J^{n+1}. Its restriction to $\bar{G}$ splits over $E\bar{G}$ and the remaining extension of $\bar{U}_d$ is trivial.

It follows that the assertion also holds for module-extensions and that the map to $\Omega_{\bar{G}^{dual}}$ lifts to $FG \to \mathbb{G}_a^e = \Omega_{G^{dual}}$ which is linear on $N^*_{G^{dual}}$.

We note that the pairing $\mathcal{F}G \times \mathcal{F}G^{dual} \to \mathcal{LT}'$ induces (by evaluation on dual numbers) a map

$$Lie(\mathcal{F}G) \to Hom(\mathcal{F}G^{dual}, \mathbb{G}_a)$$

which is an isomorphism (reduce modulo J). Also the induced pairing on Lie-algebras

$$Lie(\mathcal{F}G) \times Lie(\mathcal{F}G^{dual}) \to Lie(\mathcal{LT}') = R$$

can be described by evaluating $\mathcal{F}G \times \mathcal{F}G^{dual}$ on "double dual numbers" $R[\epsilon, \epsilon']$, so that we get the same pairing of Lie-algebras if we exchange G and G^{dual}.

Similar assertions hold for $U_e \times \mathcal{U}_e \to \mathcal{LT}'$ and $\mathcal{U}_d \times U_d \to \mathcal{LT}'$.

7. Liftings over divided power thickenings

Here we give the $\mathcal{O}$-analogue of lifting over divided power embeddings (also to be found in [9], sect.10, as "A-divided powers"). As usual all rings are algebras over $\mathcal{O}$. Note that in this section we usually cannot reduce to Noetherian baserings because the DP-hull of a finitely generated $\mathcal{O}$-algebra may not be Noetherian.

Definition 14. *Suppose $I \subseteq R$ is an ideal. An $\mathcal{O}$-DP structure on I is a map*
$\gamma : I \to I$
satisfying
a) $\pi \cdot \gamma(x) = x^q$.

b) $\gamma(a \cdot x) = a^q \cdot \gamma(x)$ $(a \in R)$.
c) $\gamma(x+y) = \gamma(x) + \gamma(y) + \sum_{0<i<q}(\binom{q}{i}/\pi) \cdot x^i \cdot y^{q-i}$.

(The quotient in c) exists in $\mathcal{O}$.)

Obviously these are the axioms satisfied by x^q/π. For example for any family of indeterminates T_i we can form the subring of $K[T_i]$ generated by $T_i^{q^j}/\pi^{1+q+\ldots+q^{j-1}}$, or equivalently the quotient of the polynomial ring $\mathcal{O}[T_{i,j}]$ ($j \geq 0$ an integer) under the ideal generated by $(T_{i,j}^q - \pi \cdot T_{i,j+1})$. Then the ideal generated by the $T_{i,j}$ has an $\mathcal{O}$-DP structure defined by $\gamma(x) = x^q/\pi$ or $\gamma(T_{i,j}) = T_{i,j+1}$, and it is a universal object: Namely for any $I \subseteq R$ with $\mathcal{O}$-DP structure γ and elements $x_i \in I$ there exists a unique DP-map from our universal object to R sending T_i to x_i. Also for any flat R-algebra S γ induces an $\mathcal{O}$-DP-structure on $I \cdot S$.

We denote by γ^n the n-fold iterate of γ, and also abbreviate

$$\delta_n(x) = \pi^{q^{n-1}+\ldots+1-n} \cdot \gamma^n(x)$$

("$= x^{q^n}/\pi^n$").

Definition 15. *Suppose $I \subseteq R$ admits an $\mathcal{O}$-DP structure γ. Define $I^{[n]}$ as the ideal generated by all products $\prod \gamma^{a_i}(x_i)$ with $\sum q^{a_i} \geq n$. It is a sub-DP-ideal of I. γ is called nilpotent if $I^{[n]}$ vanishes for large n.*

A $\mathcal{O}$-DP structure allows to define logarithms on formal $\mathcal{O}$-modules.

If $I \subseteq R$ is an $\mathcal{O}$-DP ideal we define a map $log : \hat{W}_{\mathcal{O}}(I) \to I \cdot Lie(\hat{W}_{\mathcal{O}})$ with components $\delta_n(x_0) + \ldots\delta_1(x_{n-1}) + x_n$ (that is w_n/π^n). One checks (by the usual reduction to baserings where π is invertible) that log is a homomorphism functorial for endomorphisms of $\hat{W}_{\mathcal{O}}$. Furthermore it is an isomorphism if γ is DP-nilpotent (easy devissage reducing to $I^2 = \gamma(I) = 0$).

Lemma 16. *Suppose $I \subseteq R$ has an $\mathcal{O}$-DP structure γ such that $\delta^n(I) = 0$ for large n. Then one can define for any formal $\mathcal{O}$-module $\mathcal{G}$ an $\mathcal{O}$-linear map $log_{\mathcal{G}} : \mathcal{G}(I) \to I \cdot Lie(\mathcal{G})$, such that $log_{\mathcal{G}}$ is functorial in $\mathcal{G}$, and coincides with the just defined log for $\mathcal{G} = \hat{W}_{\mathcal{O}}$. Also any map of formal $\mathcal{O}$-modules $\mathcal{G} \to Lie(\mathcal{H})$, vanishing modulo I, lifts uniquely to a map $\mathcal{G} \to \mathcal{H}$, also vanishing modulo I.*

Furthermore $log_{\mathcal{G}}$ is an isomorphism if γ is DP-nilpotent.

Proof: Any $\mathcal{G}$ is the cokernel of a map of sums of $\hat{W}_{\mathcal{O}}$'s, thus the existence and uniqueness of $log_{\mathcal{G}}$ and also the isomorphism property. For maps into $\mathcal{H}$ it suffices to show that $log_{\mathcal{H}}$ induces an isomorphism on π-typical curves which are trivial modulo I, and this holds because for each n the ideal generated by $t \cdot I$ in $R[[t]]/(t^n)$ is DP-nilpotent.

Now we approach the main result of this section, namely the relations between lifts of $\bar{G}$ from $\bar{R}$ to R and lifts of its homology $M(\bar{G})$ ($\bar{R} = R/I$ with R and I as above). We first have to explain what that means:

For a perfect complex of length one $\bar{M}_\bullet : \bar{M}_1 \to \bar{M}_0$ of finitely generated projective $\bar{R}$-modules a lift consists of such a complex $M_\bullet$ over R and an isomorphism $M_\bullet \otimes_R \bar{R} \cong \bar{M}_\bullet$. They form a category $Lift(\bar{M}_\bullet)$ where we take as maps homomorphisms inducing the identity on $\bar{M}_\bullet$ modulo homotopies which vanish modulo I. One checks that with this definition all morphisms are isomorphisms, that is liftings form a (nonempty) groupoid. Also any morphism $\bar{\alpha} : \bar{M}_\bullet \to \bar{N}_\bullet$ induces an equivalence class of functors on lifts which depends only on the homotopy class of $\bar{\alpha}$.

Namely the category $Lift(\bar{\alpha})$ consisting of lifts $M_\bullet, N_\bullet$ together with a homotopy class of $\alpha : M_\bullet \to N_\bullet$ lifting $\bar{\alpha}$, and maps diagrams commuting up to homotopy (which of course vanish modulo I) is equivalent to $Lift(M_\bullet)$.

For filtered complexes the theory is slightly more complicated. Namely such a complex is an extension

$$0 \to F(M_\bullet) \to M_\bullet \to G(M_\bullet) \to 0$$

of two perfect complexes as before. One defines again the category $Lift_{fil}(M_\bullet)$ using filtered maps and filtered homotopies throughout, and also the equivalence classes of functors induced from maps. Now $Lift_{fil}(M_\bullet)$ can be empty: For example if I has square zero there is an obstruction in $H^1(Hom(G(\bar{M}_\bullet), I \otimes_{\bar{R}} F(\bar{M}_\bullet)))$.

Finally for affine schemes lifting (filtered or unfiltered) is local in the fpqc-topology, that is $Lift(\bar{M}_\bullet)$ and $Lift_{fil}(\bar{M}_\bullet)$ are stacks over the category of affine schemes with fpqc-topology: Assume given a faithfully flat $R \to S$, a lift of $\bar{M} \otimes_R S$, and an isomorphism of the two induced lifts on $S \otimes_R S$ satisfying transitivity (up to homotopy). Then these are induced from a lift over R, unique up to homotopy. Namely we easily reduce to I finitely generated and then to $I^2 = (0)$. Two homotopies between the same map differ by a class in $H^{-1}(I \otimes_R End(\bar{M}_\bullet))$ which defines a quasicoherent sheaf whose first and second flat cohomologies vanish on the affine scheme $Spec(R)$. The same a holds for the sheaf of homotopies. Now if we have an isomorphism on $S \otimes_R S$ which is transitive up to homotopy, we obtain such a homotopy over the product of three factors S. Its boundary (over four factors) is a homotopy for the trivial map, thus we may modify the homotopy so that this boundary vanishes (the obstruction lies in the second flat cohomology). This in turn implies that our homotopy is a one-cocycle, and the descent-isomorphism can be modified such that it becomes trivial. Thus a true flat descent-datum, and a descended complex over R.

Finally if two flat descent-data have homotopic descent-isomorphisms the boundary of a homotopy between them (on three factors S) is a one-cocycle for homotopies of the trivial map. Thus we can modify the homotopy so that this boundary becomes trivial, and is thus a coboundary of a homotopy over S, which defines (if one adds it to the identity) an isomorphism between the two descent-data.

Theorem 17. *Suppose $I \subset R$ admits an $\mathcal{O}$-DP-structure γ with $\delta_n(I) = (0)$ for large n. Suppose furthermore that $\bar{G}$ is a finite flat strict $\mathcal{O}$-groupscheme over $\bar{R} = R/I$.*

a) $M(\bar{G})$ lifts to a perfect complex over R unique and functorial up to homotopy. This lifting respects duality, that is $M(G^{dual}) = Hom_R(M(G), R)[-1]$.

b) If γ is DP-nilpotent $E\bar{G}$ lifts to a flat strict $\mathcal{O}$-groupscheme over R and $E\bar{G} \to \Omega_{\bar{G}^{dual}}$ to a strict map into a vectorgroup. These liftings are unique and functorial up to homotopies (explained in the proof). Furthermore the duality pairing lifts to $EG \times EG^{dual} \to \mathcal{LT}$, unique up to the exponential of a bilinear pairing $\Omega_{G^{dual}} \times \Omega_G \to I \cdot Lie(\mathcal{LT})$.

c) If γ is DP-nilpotent the category of lifts of $\bar{G}$ finite flat strict $\mathcal{O}$-groupscheme over R if is equivalent to the (stack-theoretical) fibre $Lift_{fil}(M(\bar{G})) \to Lift(M(\bar{G})$, and the same for lifts of maps.

Proof: We may use the twist $\mathcal{LT}'$ instead of $\mathcal{LT}$. Note that any element of I is nilpotent, because $\delta_n(x)$ divides x^{q^n}. Also there exists a finitely generated (thus nilpotent) ideal $J \subseteq I$ such that $\bar{G}$ lifts to R/J.

Choose a lift $U_e \to \mathcal{F}G$. If we try to modify $\mathcal{F}G \to \mathcal{U}_d$ such that it vanishes on U_e, the problem is to extend to $\mathcal{F}G$ a map $U_e \to \mathcal{U}_d$ vanishing modulo I. Composing with the logarithm gives a module-extension of $\mathcal{F}G/U_e$ by $I \cdot Lie(\mathcal{U}_d)$, which splits linearly over FG. This means that we can modify to get a lift on the level of formal $\mathcal{O}$-modules $\hat{FG} \to \mathcal{U}_d$, and a lift of ind-schemes $FG \to \mathcal{U}_d$ if γ is DP-nilpotent. Furthermore its restriction to $N^*_{G^{dual}}$ is "linear", that is its composition with $log_{\mathcal{U}}$ is. All in all we obtain a complex

$$\hat{FG} \to \mathcal{U}_d \times \Omega_{G^{dual}},$$

where we can replace $\hat{FG}$ by FG if γ is DP-nilpotent. We need:

Lemma 18. *For any map $\mathcal{U}_d \to \mathbb{G}_a$ into an additive group (or even a module) the composition $\hat{FG} \to \mathbb{G}_a$ extends naturally to all of FG. Furthermore any homomorphism $FG \to \mathbb{G}_a$ linear on $N^*_{G^{dual}}$ is the sum of a homomorphism induced by a linear map $\Omega_{G^{dual}} \to \mathbb{G}_a$ and of a homomorphism induced as above from $\mathcal{U}_d$.*

Proof: For the first assertion it suffices to consider the induced map on $\hat{\mathcal{F}G}$ which is then a sum of two terms. The first extends because it is induced from $\mathcal{F}G \to \mathcal{U}_d$, and the second extends as the composition $\mathcal{F}G \to I \cdot Lie(\mathcal{U}_d) \to Lie(\mathbb{G}_a) = \mathbb{G}_a$.

For the second choose a finitely generated ideal $J \subseteq I$ such that G is defined modulo J and that the homomorphism $U_e \to I \cdot Lie(\mathcal{U}_d) \subset Lie(\mathcal{U}_d)$ vanishes modulo J. Its restriction to $\bar{G}$ lies in a finitely generated submodule, so by enlarging J we may assume that it vanishes. This induces a map $\mathcal{U}_d \to (I/J) \otimes_R Lie(\mathcal{U}_d)$. Lift it modulo J and apply the induced automorphism of $\mathcal{U}_d$ (which is trivial modulo I). It follows that we may assume that the correction is of the form $\mathcal{F}G \to J \cdot Lie(\mathcal{U}_d)$.

Now as J is finitely generated some power of it vanishes. If we have decomposed a homomorphism $FG \to \mathbb{G}_a$ modulo J^n into the sum of homomorphisms induced from $\Omega_{G^{dual}}$ respectively from $\mathcal{U}_d$ we may lift these modulo J^{n+1}. We are thus left with the problem of decomposing a homomorphism into J^n/J^{n+1}. Its restriction to $\bar{EG}$ extends to $\Omega_{G^{dual}}$, so we may assume that it is trivial, so our map factors over $\bar{\mathcal{U}}_d$ and we are done. Of course instead of $\mathbb{G}_a$ we could have used arbitrary R-modules.

After settling this somehow delicate point we claim that our complex is up to homotopy independant of choices and functorial. Here "homotopy" means linear map $\Omega_{G^{dual}} \to I \cdot Lie(FG)$.

For this we must construct for any map $\bar{G}_1 \to \bar{G}_2$ a map between these complexes well defined up to homotopy and functorial. For this we first lift somehow to $\mathcal{F}G_1 \to \mathcal{F}G_2$, $\mathcal{F}G_1 \to \mathcal{U}_{d_1}$, $\mathcal{U}_{d_1} \to \mathcal{U}_{d_2}$ and also $\Omega_{G_1^{dual}} \to \Omega_{G_2^{dual}}$ (linear). The induced $U_{e_1} \to FG_2 \times_{\mathcal{U}_{d_2}} \mathcal{U}_{d_1}$ has modulo I its image in $N^*_{G_2^{dual}} \times \{0\}$, so applying the logarithm gives a map $U_{d_1} \to (N^*_{G_2^{dual}} + I \cdot Lie(FG_2)) \times_{Lie(\mathcal{U}_{d_2})} I \cdot Lie(\mathcal{U}_{d_1})$. It defines by pushout a module-extension of $\mathcal{F}G_1/U_{d_1}$ which splits over FG_1. It follows that we can find lifts $\hat{FG}_1 \to \hat{FG}_2$ and $\hat{FG}_1 \to \mathcal{U}_{d_1}$ whose restriction to $N^*_{G_1^{dual}}$ is again "linear", which means for the first map that is the sum of a linear map into $N^*_{G_2^{dual}}$ and a map whose logarithm is linear. Also the two compositions into $\mathcal{U}_{d_2}$ coincide. That is we have found a map of complexes after modifying $FG \to \mathcal{U}_{d_1}$ by a map into $I \cdot (Lie(\mathcal{U}_{d_1}) \oplus \Omega_{G_2^{dual}})$ which is linear on $N^*_{G_1^{dual}}$. As we know that it is the sum of maps induced from $\Omega_{G_1^{dual}}$ and from $\mathcal{U}_{d_1}$ we finally find an extension to a map of complexes. Again for DP-nilpotent γ we need not restrict to formal groups.

It is easily seen that the arbitrary choices in the above construction lead to homotopic maps. If γ is DP-nilpotent so that we do not have to restrict to formal groups this can be seen directly: Namely two maps differ by a map of complexes from $FG_1 \to \mathcal{U}_{d_1} \times \Omega_{G_1^{dual}}$ to $I \cdot Lie(FG_2) \to I \cdot (Lie(\mathcal{U}_{d_2}) \oplus \Omega_{G_2^{dual}})$. On FG_1 it is the sum of maps induced from $\Omega_{G_1^{dual}}$ respectively $\mathcal{U}_{d_2}$. So changing by a homotopy we may assume that it vanishes there. As $FG_1 \to \mathcal{U}_{d_1} \times \Omega_{G_1^{dual}}$ is an epimorphism over R/I the second component is zero as well (show by induction that it vanishes modulo I^n).

In contrast to this simple argument we do not know in the general case whether arbitrary liftings of our map of complexes are homotopic. We only show this for liftings constructed by our procedure.

Next we extend any bilinear pairing $\bar{G}_1 \times \bar{G}_2 \to \mathcal{LT}'$ to a pairing on our complexes. We already know that we can lift the pairing on $\mathcal{F}\bar{G}_1 \times \mathcal{F}\bar{G}_2$ to $\mathcal{F}G_1 \times \mathcal{F}G_2 \to \mathcal{LT}'$. We modify this lifting by a bilinear pairing $\mathcal{F}G_1 \times \mathcal{F}G_2$ such that it is on $U_{e_1} \times \mathcal{F}G_2$ the sum of the pairing induced from a lift $U_{e_1} \times \mathcal{U}_{d_2} \to \mathcal{LT}'$ of the canonical pairing, and of a pairing on $\mathcal{F}G_1 \times U_{e_2}$ from $\mathcal{U}_{d_1} \times U_{e_2} \to \mathcal{LT}'$. Also the symmetric condition (exchanging G_1 and G_2) for the restriction to $\mathcal{F}G_1 \times U_{e_2}$ should hold as well. Here "modifying" means adding a linear pairing into I which exponentiates to a pairing of formal groups $\hat{\mathcal{F}G}_1 \times \hat{\mathcal{F}G}_2 \to \mathcal{LT}'$ (it suffices to complete one of the factors).

On $U_{e_1} \times \mathcal{F}G_2$ our pairing is the sum of (some lift) $U_{e_1} \times \mathcal{U}_{d_2} \to \mathcal{LT}'$ and a pairing vanishing modulo I. The logarithm of the latter defines a bilinear $U_{d_1} \times \mathcal{F}G_2 \to I$. Trying to extend this to $\mathcal{F}G_1 \times \mathcal{F}G_2$ defines a biextension of $\mathcal{F}G_1/U_{e_1} \times \mathcal{F}G_2$ which is induced by a bilinear form on $N^*_{G_1^{dual}} \times \mathcal{F}G_2$. That means that we may assume that our pairing is on $U_{e_1} \times \mathcal{F}G_2$ equal to the sum of $U_{e_1} \times \mathcal{U}_{d_2} \to \mathcal{LT}'$ and a pairing $N^*_{G_1^{dual}} \times \mathcal{F}G_2 \to I$ which is linear on the first factor. Its restriction to $\mathcal{F}G_1 \times U_{e_2}$ is the sum of $\mathcal{U}_{d_1} \times U_{e_2} \to \mathcal{LT}'$ and a pairing $FG_1 \times U_{e_2} \to I$ which is linear on the first factor in $N^*_{G_1^{dual}} \times U_{e_2}$. It is the unique sum of pairings induced from $\Omega_{G_1^{dual}} \times U_{e_2}$ and from $\mathcal{U}_{d_1} \times U_{e_2}$, by lemma 18.

The first summand defines a vectorextension of $\mathcal{F}G_2/U_{e_2}$ by the dual of $\Omega_{G_1^{dual}}$, which is as usually induced by a linear map from $N^*_{G_2^{dual}}$. Thus modifying our pairing via $\Omega_{G_1^{dual}} \times \mathcal{F}G_2 \to I$ we may assume that it factors over a linear map from $N^*_{G_2^{dual}}$ (This modification is still linear on $N^*_{G_1^{dual}}$, so does not destroy what we have achieved in the first step). The second summand is used to modify $\mathcal{U}_{d_1} \times U_{e_2} \to \mathcal{LT}'$. Thus also on $\mathcal{F}G_1 \times U_{e_2}$ our pairing is the sum of $\mathcal{U}_{d_1} \times U_{e_2} \to \mathcal{LT}'$ and a pairing $\mathcal{F}G_1 \times N^*_{G_2^{dual}} \to I$ which is linear on the second factor. Finally this determines the modification uniquely up to pairings of $\mathcal{F}G_1 \times (\mathcal{U}_{d_2} \oplus \Omega_{G_1^{dual}}) \to I$ and $(\mathcal{U}_{d_1} \oplus \Omega_{G_2^{dual}}) \times \mathcal{F}G_2 \to I$.

Now to demonstrate the theorem define $M(G)$ as the complex of $Lie(FG) \to Lie(\mathcal{U}_d) \oplus \Omega_{G^{dual}}$. We can use the following easy consequence of lemmas 13 and 18 to give a quasi-isomorphic variant:

Lemma 19. *There exists an exact sequence*

$$0 \to \Omega_G^{dual} \oplus Hom(\mathcal{U}_e, \mathbb{G}_a) \to Hom(\mathcal{F}G^{dual}, \mathbb{G}_a) \to Hom(U_d, \mathbb{G}_a)/N_G \to 0.$$

We derive an exact sequence

$$0 \to \Omega_G^{dual} \oplus Lie(U_e) \to N_G \oplus Lie(\mathcal{F}G) \to Lie(\mathcal{U}_d) \to 0.$$

It induces a quasi-isomorphism between $M(G)$ and a complex

$$\Omega_G^{dual} \oplus N^*_{G^{dual}} \to \Omega_{G^{dual}} \oplus N_G.$$

The maps in this complex are induced by

- the pairing $\Omega_G^{dual} \times \Omega_{G^{dual}}^{dual} \to R$ (end of previous paragraph),
- the composition $N^*_{G^{dual}} \to FG \to \Omega_{G^{dual}}$,
- the composition $N^*_G \to FG^{dual} \to \Omega_G$, and
- the composition $N^*_{G^{dual}} \to FG \to N_G \subset \mathcal{U}_d$ (induced by $U_e \times U_d \to \mathcal{LT}'$).

It satisfies a). Also for DP-nilpotent γ we get b) with $EG = ker(FG \to \mathcal{U}_d)$. The duality pairing is obvious because the alternative description is selfdual.

Finally for c) we first note that if $\bar{G}$ lifts so does the filtration on $M(\bar{G})$. Conversely if the filtration lifts it also lifts on the complex $Lie(FG) \to Lie(\mathcal{U}_d) \oplus \Omega_{G^{dual}}$. On the second term the lift of the filtration is the graph of a homomorphism $\Omega_{G^{dual}} \to I \cdot Lie(\mathcal{U}_d)$ which is induced by a homomorphism $\Omega_{G^{dual}} \to \mathcal{U}_d$ trivial modulo I and defines a unipotent automorphism of the second term. Passing to an isomorphic complex we may assume that the filtration on the second term is given by $\Omega_{G^{dual}}$.

On the first term the filtration is the graph of a homomorphism $N^*_{G^{dual}} \to Lie(FG)$ lifting the canonical inclusion modulo I. It again integrates to a homomorphism of ind-groupschemes $N^*_{G^{dual}} \to FG$, and we may form the quotient of FG under it. The quotient is formally smooth, and $\mathcal{O}$ acts on its Lie-algebra by scalar multiplication. Furthermore because of compatibility of filtrations the map to $\mathcal{U}_d$ factors inducing a finite flat morphism from the quotient into $\mathcal{U}_d$. Its kernel is a lift G of $\bar{G}$.

It remains to show that for a given $\bar{G}_1 \to \bar{G}_2$ lifts to $G_1 \to G_2$ correspond bijectively to lifts of maps of filtered complexes, up to filtered homotopy. Our constructions actually gives a functor in the opposite direction and it is easily seen that it is an inverse. Finally everything is shown!

We conclude this chapter by giving an application of the method of proof. Assume π annihilates R. For any R-scheme X let $X^{(q)}$ denote its basechange by $Frob_q$, the q-th power-map on R. The power-map on X then induces the relative Frobenius $Frob_\pi : X \to X^{(q)}$. For any flat strict $\mathcal{O}$-groupscheme or ind-groupscheme G over R there should exist a functorial Verschiebung $Ver_\pi : G^{(q)} \to G$ with $Frob_\pi \cdot Ver_\pi = \pi$, $Ver_\pi \cdot Frob_\pi = \pi$. Unfortunately I do not know a general construction. Here are some special cases:

Suppose $\mathcal{G}$ is a finite dimensional formal $\mathcal{O}$-module or a strict $\mathcal{O}$-ind-groupscheme formally presented by the completion of a polynomial ring $R[T_i]$ in finitely many variables, along an ideal generated by a regular sequence (The reader may think up better conditions). As multiplication by π on $\mathcal{G}$ has trivial differential it factors uniquely over $Frob_p$ (that is where we use the assumptions on $\mathcal{G}$). If $q > p$ the resulting map has still trivial differential ($\mathbb{F}_q$-action) and we can repeat the construction until we find $Ver_\pi : \mathcal{G}^{(q)} \to \mathcal{G}$ with $Ver_\pi \cdot Frob_\pi = \pi$. The other composition coincides with π as well because Frobenius is faithfully flat. Also this construction is obviously functorial.

Another instance where we can define a Verschiebung is for finite flat G, namely as adjoint of $Frob_\pi$ on G^{dual}. The embedding $G \subset \mathcal{G} = \mathcal{MAP}_0(G^{dual}, \mathcal{LT})$ then respects Verschiebung: The definition via duality corresponds to the action by F_π on the arguments in the $\mathcal{MAP}$-space, thus extends to $\mathcal{G}$. Composing it with Frobenius on maps means that we apply Frobenius to a map and to its argument, which by functoriality amounts to applying it to the target $\mathcal{LT}$. However this is defined over $\mathbb{F}_q$ and Frobenius maps as multiplication by π, so the compostion is as it should equal to π-multiplication. It then follows that this Verschiebung is compatible with arbitrary strict maps $G \to \mathcal{H}$ (factor over the inclusion into $\mathcal{G} \times \mathcal{H}$). This suffices to define Verschiebung over fields.

8. Finite strict $\mathcal{O}$-groupschemes over perfect fields, and π-divisible groups

Assume that the base is a perfect field k annihilated by π, and consider finite strict $\mathcal{O}$-groupschemes G over k. The Witt-vectors $W_\mathcal{O}(k)$ are a π-adically complete discrete valuationring with residue field k, with a Frobenius automorphism σ. Its maximal ideal is generated by π and admit a $\mathcal{O}$-DP-structure $\gamma(\pi) = \pi^{q-1}$, topologically DP-nilpotent if $q > 2$. The complex $M(G)$ lifts canonically to each quotient $W_\mathcal{O}(k)/(\pi^n)$ and thus in the limit to a perfect complex over $W_\mathcal{O}(k)$. On it multiplication by a power of π is nullhomotopic so its homology $H(G)$ is concentrated in degree 0, and $M(G)$ is a projective resolution of $H(G)$. The endomorphisms $Frob_\pi$ and Ver_π induce semilinear operators V_π and F_π on $H(G)$ (the exchange of symbols is necessary to conform with the usual notations). We claim:

Theorem 20. *The functor H defines an equivalence of categories from finite strict $\mathcal{O}$-groupschemes G over k to finite $W_\mathcal{O}(k)$-modules with operators F_π, V_π, with F_π σ-linear, V_π σ^{-1}-linear, and $F_\pi \cdot V_\pi = V_\pi \cdot F_\pi = \pi$.*

Proof: We easily reduce to the case where k is algebraically closed. The functor $H()$ is exact because short exact sequences of G's induce exact sequences on the homology of $M(G)$'s. Each G is a direct sum $G = G^{et} \oplus G^m \oplus G'$, with G^{et} étale, G^m the dual of an étale, and G' as well as its dual infinitesimal. The first two summands lift canonically to $W_\mathcal{O}(k)$, so the value of $H(G)$ on them can be computed from these lifts. One finds that H induces an equivalence of categories from étale G's to modules H where V_π is an isomorphism, and multiplicative G's correspond to modules with F_π invertible. Also any potential H is canonical the direct sum of three submodules on which either V_π or F_π are isomorphic, or both of them nilpotent. It thus suffices to show that biinfinitesimal G's correspond to H's of the third category.

Such a G is a successive extension of α_q's. Over k the complex $M(\alpha_q)$ is quasi-isomorphic to $k \xrightarrow{0} k$, with F_π and V_π acting trivially: Namely $E\alpha_q$ maps nontrivially to $\mathbb{G}_a$ via α_q, so the map on Lie-algebras has kernel k on which Frobenius and Verschiebung act trivially (Verschiebung is trivial on $\mathbb{G}_a$). This kernel is equal to the π-torsion in $H(\alpha_q)$, that is to $H(\alpha_q)$.

It follows by devissage that for biinfinitesimal G both F_π and V_π act nilpotently on $H(G)$ and that the length h of $H(G)$ is the height of G, that is $\mathcal{O}_G$ has dimension q^h over k. Also the maps $Hom(\alpha_q, \alpha_q) \to Hom(H(\alpha_q), H(\alpha_q)) = k$ and $Ext^1(\alpha_q, \alpha_q) \to Ext^1((H(\alpha_q), H(\alpha_q)) = k^2$ are bijective:

For the Hom's this is obvious. For the extensions $Ext^1(\alpha_q, \alpha_q)$ has as k-basis the two extensions defined by α_{q^2} and by the kernel of Frobenius on W_2, the Witt-vectors of length 2. They are distinguished by the fact that on the first Verschiebung vanishes but not Frobenius, with the opposite for the second. As $H()$ is exact and preserves lengths it maps these two extension to linearly independant elements in Ext^1 which then form a basis. It follows by devissage that $H()$ is fully faithful and injective on Ext^1's.

Next we can compute $H(\alpha_{q^h})$: It is a k-vectorspace of dimension h on which F_π acts trivially (Ver_π is trivial on α_{q^h}), and V_π has kernel of dimension one. It then has a basis $\{e_1, ..., e_h\}$ with $V_\pi(e_i) = e_{i-1}$. We define $H(\mathbb{G}_a) = \bigcup_h H(\alpha_{q^h})$. It is a k-vectorspace with basis e_i $(i > 0)$, trivial F_π-action, and $V_\pi(e_i) = e_{i-1}$. As H is fully faithful we have for any biinfinitesimal G

$$Hom(G, \mathbb{G}_a) = \bigcup_h Hom(G, \alpha_{q^h}) = \bigcup_h Hom(H(G), H(\alpha_{q^h})) = Hom(H(G), H(\mathbb{G}_a)).$$

The latter is equal to the dual of the k-vectorspace $H(G)/F(H(G))$, that is homomorphisms $f : H(G) \to H(\mathbb{G}_a)$ have the form

$$f(m) = \sum_i \lambda(V_\pi^{i-1}(m)) \cdot e_i,$$

with k-linear $\lambda : H(G)/F_\pi(H(V)) \to k$.

Similarly we find that $Ext^1(H(G), H(\mathbb{G}_a)$ injects into the dual of the kernel of F_π on $H(G)$, with the k-action twisted by σ: For any extension $H(\mathbb{G}_a) \to E \to H(G)$ the action of F_π on E defines a semilinear V_π linear $ker(F_\pi|H(G)) \to H(\mathbb{G}_a)$ which is of the form $\sum_i \lambda(V_\pi^{i-1}((m)) \cdot e_i$. If this map vanishes the image $F_\pi(E)$ defines a splitting over $F_\pi(H(G))$, and E is pullback of an extension of $H(G)/F_\pi(H(G))$ with trivial F_π. Thus we may assume that F_π vanishes on E and $H(G)$. Then the cokernel of V_π on $H(\mathbb{G}_a)$ injects into the cokernel on E, so we can find a k-linear splitting which lifts to a unique splitting $E \to H(\mathbb{G}_a)$ of the extension.

Finally we know for finite strict $\mathcal{O}$-groupschemes that $Hom(G, \mathbb{G}_a)$ and $Ext^1(G, \mathbb{G}_a)$ have the same dimension, equal to that of the Lie-algebra of G^{dual}. It follows that this must be equal to the dimension of either the cokernel or the kernel of $F_\pi|H(G)$ and that $Ext^1(G, \mathbb{G}_a)$ is isomorphic to $Ext^1(H(G), H(\mathbb{G}_a))$. From the long exact homology sequences associated to $\alpha_q \to \mathbb{G}_a \to \mathbb{G}_a$ we derive that also $Ext^1(G, \alpha_q) \cong Ext^1(H(G), H(\alpha_q))$. Thus any extension of $H(G)$ by $H(\alpha_q)$ is realised by a strict $\mathcal{O}$-groupscheme. As $H(\alpha_q)$ is the only simple (F_π, V_π)-module with both F_π and V_π nilpotent it follows by devissage that any such module is realised by a G. This finishes the proof of the theorem.

Remark: For any finite dimensional formal $\mathcal{O}$-module $\mathcal{G}$ over k we define $M(\mathcal{G}) = \varprojlim H(Ker(Frob_q^h|\mathcal{G}))$ (the transition maps are induced by the surjection $Frob_q$ on $\mathcal{G}$). We claim that this functor is isomorphic to the usual Dieudonné-module of $\mathcal{G}$:

Both are reduced modules over the Cartier-ring $Cart_{\mathcal{O}}(k)$ and modulo V_π equal to $Lie(\mathcal{G})$. Furthermore $\mathcal{G}$ is the direct sum of a multiplicative formal group (the dual of an étale π-divisible group) and a formal group for which Verschiebung acts nilpotently on the kernel of Frobenius. The isomorphism for multiplicative $\mathcal{G}$'s is easily constructed, so we concentrate on the other summand.

For the additive group we obtain $M(\mathbb{G}_a) = k[[V_\pi]]$ with trivial F_π-action, using the previous computation of $H(\alpha_{q^h})$. For the Witt-vectors of length two $M(W_2)$

is an extension of two copies of $M(\mathbb{G}_a)$, and F_π maps a generator of the quotient to a generator of the subspace (determination of $M(ker(F_\pi|W_2)))$. It follows that $M(W_2) = Cart_{\mathcal{O}}(k)/F_\pi^2$, and by lifting generators again that $M(W_n) = Cart_{\mathcal{O}}(k)/F_\pi^n$. Finally

$$\begin{aligned} M(\mathcal{G}) &= \varprojlim M(ker(Frob_\pi^h|\mathcal{G})) \\ &= \varprojlim Hom_{Cart}(Cart_{\mathcal{O}}(k)/(V_\pi^h, F_\pi^l), M(ker(Frob_\pi|\mathcal{G})) \\ &= \varprojlim Hom_{Cart}(M(ker(Frob_\pi^h|W_l), M(ker(Frob_\pi^h|\mathcal{G}))) \\ &= \varprojlim Hom(ker(Frob_\pi^h|W_l, ker(Frob_\pi^h|\mathcal{G}))) \\ &= \varprojlim Hom(ker(Frob_\pi^h|\hat{W}_{\mathcal{O}}, ker(Frob_\pi^h|\mathcal{G}))) \\ &= Hom(\hat{W}_{\mathcal{O}}, \mathcal{G}). \end{aligned}$$

For the theory of Barsotti-Tate groups we need an application of these results. Suppose G is annihilated by π. Then the $ker(Frob_\pi|G)$ has order q^d, with d the dimension of the tangentspace of G. Similarly $ker(Ver_\pi|G)$ has order $q^{d'}$, d' the dimension of the tangentspace of G^{dual}. Recall that G is called a BT_1 (Barsotti-Tate of level one) if the kernel of $Frob_\pi$ coincides with the image of Ver_π, or equivalently if G has rank $q^{d+d'}$. If G is a BT_1 so is G^{dual}. We have:

Lemma 21. *G is a BT_1 if and only if no nontrivial vectorextension $\mathbb{G}_a \to E \to G$ is annihilated by π.*

Proof: We know that vectorextensions correspond to the dual of $ker(F_\pi|H(G))$. If G is a BT_1 the kernel of F_π on $H(G)$ lies in the image of $V(H(E))$ ($H(E)$ is defined as the union over the associated extensions by α_{q^n} for $n >> 0$). This is annihilated by F_π if π annihilates E, thus the classifying map is trivial.

If G is not a BT_1 $V_\pi(H(G))$ is a proper subspace of the kernel of F_π, so there exists a nontrivial linear form vanishing on $V_\pi(H(G))$. It defines a nontrivial extension E such that F_π vanishes on $V_\pi(H(E))$. Thus $H(E)$ and E are annihilated by π.

Remark For $n > 1$ G is a BT_n if $H(G)$ is a free module over $W_{\mathcal{O}}(k)/(\pi^n)$. In this case $G[\pi]$ is automatically a BT_1 and no nontrivial vectorextension of G is annihilated by π^n (use that the kernel of $F_\pi|H(G)$ is the image of $\pi^{n-1} \cdot V_\pi$).

We apply this to the theory of π-divisible groups. Suppose G is a finite flat strict $\mathcal{O}$-groupscheme over R annihilated by π^n. Choose a universal vectorextension $N^*_{G^{dual}} \to EG \to \Omega_{G^{dual}}$. Then multiplication by π^n on $G^\flat$ defines a map $\Omega_G \to N^*_G$ which is a nullhomotopy for multiplication by π^n. Especially if π^n annihilates R it is a class in $H^{-1}(End(L_G))$. The same for G^{dual} gives $\Omega_{G^{dual}} \to N^*_{G^{dual}}$ which is induced by multiplication by π^n on EG. Finally multiplication by π^n on either $\mathcal{LT}$ or $G^{dual,\flat}$ defines two endomorphisms of $E\mathcal{G} \subseteq \mathcal{MAP}_0(G^{dual,\flat}, \mathcal{LT})$ which coincide on EG. Thus their difference gives $\mathcal{H} \to E\mathcal{G}$. Together with the previous $\Omega_{G^{dual}} \to N^*_{G^{dual}}$ we get an explicit homotopy on $E\mathcal{G} \to \mathcal{H} \oplus \Omega_{G^{dual}}$ which makes multiplication by π^n nullhomotopic. It is unique and induced from a (unique) such homotopy on the quasi-isomorphic complex $FG \to \mathcal{U}_d \times \Omega_{D^{dual}}$. The latter also survives liftings over $\mathcal{O}$-DP-ideals.

We obtain an explicit homotopy on $M(G)$ which respects the filtrations, and induces the previous in the subquotients $L_G[1]$ and $L^*_{G^{dual}}$. We say that G is a truncated Barsotti-Tate group of level n (a BT_n) if for any residue field k of R which is annihilated by π it induces a truncated Barsotti-Tate over the algebraic closure $\bar{k}$. This implies (and is in fact equivalent to) that our homotopies induce isomorphisms $H^1(L_G \otimes_R k) \cong H^0(L_G \otimes_R k)$ and $H^0(L^*_{G^{dual}} \otimes_R k) \cong H^{-1}(L^*_{G^{dual}} \otimes_R k)$. It follows that over the π-adic completion $\hat{R}$ $M(G)$ becomes filtered quasiisomorphic to a complex $M \xrightarrow{\pi\cdot} M$, with M a finite projective $\hat{R}$-module filtered by a direct summand:

If R is local with residue-field annihilated by π represent $M(G)$ by a map $P_{-1} \to P_0$ of finite filtered free R-modules such that the induced maps on associated gradeds vanish modulo the maximal ideal. Then the homotopy is a filtered map $P_0 \to P_{-1}$ which induces an isomorphism modulo the maximal ideal, thus is invertible. If we use it to identify P_{-1} and P_0 our complex becomes isomorphic to multiplication by π^n on P_0. In general this argument shows that $H_0(M(G))$ is a projective module over $R/(\pi^n)$ filtered by a direct summand. It lifts to such a P_0 over $\hat{R}$, and we can find a map $P_0 \to M(G)_0$ inducing a surjection onto $H_0(M(G))$. Together with the homotopy it defines a filtered quasiisomorphism between $P_0 \xrightarrow{\pi^n\cdot} P_0$ and $M(G)$.

If $\mathcal{G} = \{G_n\}$ is a usual π-divisible group over a π-adically complete ring R we denote by $M(\mathcal{G})$ the projective limit of the $H_0(M(G_n))$. It is a finite projective R-module with filtration by a direct summand. It lifts canonically over $\mathcal{O}$-DP-ideals.

As consequence we derive as in [11] that over rings annihilated by π^n BT_n's lift over nilpotents, that is if $J \subset R$ is an ideal consisting of nilpotents any BT_n $\bar{G}$ over R/J lifts to R: Reduce to R noetherian, then to $J^2 = (0)$. Then J has a nilpotent $\mathcal{O}$-DP-structure with $\gamma(J) = 0$, so the universal vectorextension of $\bar{G}$ lifts to $EG \to \Omega$, inducing the canonical lift $Lie(EG) \to N_{EG} \oplus \Omega$ of $M(\bar{G})$. Multiplication by π^n on $EG^\flat$ induces on $M(G)$ an endomorphism of degree -1 which lifts the corresponding endomorphism modulo J. It then follows that $M(G)$ is split and can be endoweded with a filtration lifting that on $M(\bar{G})$. Thus a lift of G. Also lifts correspond to lifts of the Hodge-filtration. All in all we can subsume by saying that the stack of BT_n's is formally smooth of relative dimension $d \cdot d'$.

Similarly one can ask whether a BT_n G_n extends to a BT_{n+1} G_{n+1}. If it does the complexes $M(G_n)$ and $M(G_{n+1})$ are filtered isomorphic, and the above argument shows that (for J consisting of nilpotents) extensions $\bar{G}_n \subset \bar{G}_{n+1}$ lift uniquely to $G_n \subset G_{n+1}$. Furthermore over a field k such extensions exist always: If k is perfect this follows by elementary (and wellknown) semilinear algebra. If k is not perfect one can extend over a finite purely inseparable extension k' of k. Over $k' \otimes_k k'$ the two induced extensions coincide modulo the nilpotent maximal ideal, thus a canonical descent datum.

Finally in general extensions are always possible locally in the étale topology or even in the Nisnevich-topology. Again we may say that $BT_{n+1} \to BT_n$ is an étale covering.

9. PERIODS

Denote by V a complete discrete valuation-ring over $\mathcal{O}$, with perfect residue-field k and π a nontrivial nonunit in V. So V is finite over its subring $V_0 = W_{\mathcal{O}}(k)$. Denote by $\bar{V}$ the integral closure of V in a separable closure $\bar{L}$ of its fractionfield L. In characteristic zero Fontaine has defined a ring A_{cr} containing the periods of p-divisible groups, that is the period map from étale to crystalline cohomology has coefficients in A_{cr} ([8]). Furthermore the theory has been extended in [6] to smooth V-algebras, or more generally to V-algebras with toroidal singularities. We want to explain the π-analogue. If K has characteristic zero its only advantage is to improve the size of certain denominators but in positive characteristics the results are new. The proofs are essentially identical to those given by Fontaine so they are only sketched.

For algebras over V there seems to be no analogue of toroidal singularities in positive characteristics so we only treat semistable singularities. Also we only develop the theory to the extent necessary to generalise the applications in [3], [4], [7].

a) Denote by $\chi : Gal(\bar{L}/L) \to \mathcal{O}^*$ the Lubin-Tate character and by "(n)" the twist of Galois-modules with the n-th power of χ. Then the topological Galois-cohomology of the completion $\hat{\bar{L}}$ vanishes in degrees > 1, is equal to L in degree zero, and to $L \cdot \chi$ in degree one. Nontrivial twists $\hat{\bar{L}}(n)$ have trivial Galois-cohomology.

b) The logarithm composed with differentiation defines a map $\mathcal{LT}(\bar{V}) \to \Omega_{\bar{V}/V}$. It induces an isomorphism $(\bar{K}/\rho^{-1} \cdot \bar{V})(1) \cong \Omega_{\bar{V}/V}$, for a certain element $\rho \in \bar{V}$ whose valuation is the sum of $1/(q-1)$ and the valuation of the different of V/V_0 (valuations are normalised so that π has valuation 1).

c) Form the ring $\mathcal{R}(V) = \varprojlim(\bar{V}/(\pi))$. The transition maps are Frobenius $Frob_q$ and are surjective. For $x \in \bar{V}$ choose a sequence $x_n \in \bar{V}$ with $x_0 = x$, $x_n = \pi \cdot x_{n+1} + x_{n+1}^q$. Their reductions modulo π define an element $\underline{x}$ of $\mathcal{R}(\bar{V})$. Furthermore there exists a functorial morphism $R \to W_{\mathcal{O}}(R)$ whose composition with w_n is n-fold iteration of $\pi \cdot T + T^q$. It is a homomorphism for the Lubin-Tate group-law, and the image of $\underline{x}$ is called the Teichmŭller representative $[\underline{x}]$ of $\underline{x}$.

If $x = 0$ we may choose for x_n generators of the π^n-torsion in $\mathcal{LT}(\bar{V})$, and get a homomorphism $\alpha : \mathcal{O}(1) \to \mathcal{LT}(\mathcal{R}(\bar{V}))$. The image of a generator generates the ideal $I^{[1]}$ of elements all whose Frobenius-transforms lie in the kernel of the map (defined below) into $\hat{\bar{V}}$. For general x different choices of the x_n amount to adding in the Lubin-Tate group to $\underline{x}$ an element of the image of α.

The polynomials w_n induce a surjection $W_{\mathcal{O}}(\mathcal{R}) \to \hat{\bar{V}}$ whose kernel is generated by the element $\xi = [\underline{\pi}] - \pi$. Form the $\mathcal{O}$-DP-hull of $W_{\mathcal{O}}(\mathcal{R}(\bar{V}))$, that is adjoin $\xi^{q^n}/\pi^{1+\dots+q^{n-1}}$, and complete π-adically. The result is a ring $A_{cr}(V)$ which admits a continous action of $Gal(\bar{L}/L)$, a Frobenius-endomorphism $Frob_q$, and a DP-filtration $F^i(A_{cr}(\bar{V}))$. Furthermore the Lubin-Tate-logarithm of α defines $\beta : \mathcal{O}(1) \to F^1(A_{cr}(V))$ which induces isomorphism $gr_F^i(A_{cr}(V))[1/\pi] = \hat{\bar{K}}(i)$. β is Galois-invariant and $Frob_q \cdot \beta = \pi \cdot \beta$. We denote by t the image of a generator of $\mathcal{O}(1)$.

The Galois-invariants in $A_{cr}(V)$ are V_0 and those in $A_{cr}(V)(-i)$ are the L_0-multiples of t^i which lie in $A_{cr}(V)$. Similarly the intersection of $F^i(A_{cr}(V))$ and the kernel of $Frob_q - \pi^i$ consists of K-multiples of t^i. Sketch: Similarly as in [8] (but not all the arguments carry over) one shows that that A_{cr} is equal to the π-adic completion of the algebra obtained by adjoining to $W_{\mathcal{O}}(\mathcal{R})$ the divided powers of t^{q-1}/π. The key fact to use is that $t^{q-1}/\pi = \xi^q/\pi$ modulo $W_{\mathcal{O}}(\mathcal{R})$ and terms of higher filtration degree.

c) If $\mathcal{G}$ is a π-divisible group over $\hat{\bar{V}} = A_{cr}(V)/F^1(A_{cr}(V))$ $M(\mathcal{G})$ lifts canonically to an $M(\mathcal{G}/A_{cr}(V))$ over $A_{cr}(V)$. Furthermore any element $\rho \in T_\pi(\mathcal{G})$ of its Tate-module defines a homomorphism from the constant π-divisible group $K/\mathcal{O}$ into $\mathcal{G}$, thus by functoriality an element of $M(\mathcal{G}/A_{cr}(V))$. Similarly any element $\rho^{dual} \in T_\pi(\mathcal{G})^{dual}(1) = T_\pi(\mathcal{G}^{dual})$ defines a homomorphism into $\mathcal{LT}$, so by functoriality a map into $M(\mathcal{LT}/A_{cr}(V)) \cong A_{cr}(V)$. One checks (by reducing to $\mathcal{LT}$) that the composition of these maps is $\beta(<\rho^{dual}, \rho>)$. Especially

$$T_\pi(\mathcal{G}) \otimes_{\mathcal{O}} A_{cr}(V)[1/t] \cong M(\mathcal{G}/A_{cr}(V))[1/t].$$

If $\mathcal{G}$ is defined over V this isomorphism preserves the Galois-action. In addition we may compare $M(\mathcal{G}/A_{cr}(V))$ to the $\mathcal{O}$-module $M(\mathcal{G} \otimes_V k)$: Namely if the reduction of $\mathcal{G}$ modulo π is already defined over $k \subseteq V/(\pi)$ we may use the DP-ideal $\pi \cdot A_{cr}(V) + F^1(A_{cr}(V))$ modulo which $\mathcal{G}$ coincides with $\mathcal{G} \otimes_V k$. It then follows that $M(\mathcal{G}/A_{cr}(V)) = M(\mathcal{G} \otimes_V k) \otimes_{\mathcal{O}} A_{cr}(V)$. In general the hypotheses holds after pushforward by a sufficiently high power of Frobenius thus inducing an isomorphism after inverting π. In any case these maps respect Frobenius and allow to apply Fontaine's theory.

Remark A similar argument has been used in [13] to show that the period-map in [1] coincides with ours.

d) One can extend this theory to algebras R which are smooth over V using the theory of almost étale extensions. In case of characteristic zero this has been done already ([6]), even for toroidal singularities. Some of the theory extends to positive characteristics:

We denote by $\bar{R}$ the normalisation of R in the maximal étale covering of $R[1/\pi]$. In some cases we can determine $\bar{R}$ up to almost étale extensions.

- Assume R is étale over a polynomialring $V[T_1, ..., T_d]$. Define a covering of the affine space by itself defined by the endomorphism which sends T_i to $\pi \cdot T_i + T_i^q$, that is by the Lubin-Tate multiplication by π. Iterating this n-times and pushout defines a subring $R_n \subset \bar{R}$. The methods of [6] show that $\bar{R}$ is almost étale over the subring generated by $\bar{V}$ and all R_n.

- Assume R is étale over $V[T_0, ..., T_d]/(T_1 \cdot ... \cdot T_d - \pi)$. Then define R_n as before, adjoining variables $T_{i,n}$ which give T_i after applying Lubin-Tate multiplication by π^n. One checks that the R_n are still regular (the $T_{i,n}$ give coordinates), and that $\bar{R}$ is almost étale over their union.

In both cases we find that $\bar{R}$ is almost flat over R. Also there is an almost exact sequence of logarithmic differentials (in the first case also of ordinary differentials)

$$0 \to \Omega_{\bar{V}/V} \otimes_{\bar{V}} \bar{R} \to \Omega_{\bar{R}/R} \to \Omega_{\bar{R}/R \otimes_V \bar{V}} \to 0.$$

Here the submodule is canonically isomorphic to $\bar{R}[1/\pi]/\rho_{log}^{-1} \cdot \bar{R}(1)$ and the quotient to $\Omega_{R/V} \otimes_R \bar{R}$. All in all this is enough information to extend the claims in [4] and [7] to positive characteristics.

References

[1] V.G.Drinfeld, *Coverings of p-adic symmetric domains,* Functional Anal. Appl. 10 (1976), 107-115
[2] V.G.Drinfeld, *Elliptic modules,* Math. USSR Sbornik 23(1974), 561-592
[3] G.Faltings, *Hodge-Tate structures and modular forms,* Math. Ann. 278 (1987), 133-149
[4] G.Faltings, *The trace formula and Drinfeld's upper halfplane,* Duke Math. J. 76 (1994), 467-481
[5] G.Faltings, *Integral crystalline cohomology over very ramified ramification rings,* Journ. of the AMS 12 (1999), 117-144
[6] G.Faltings, *Almost etale extensions,* Preprint 1998, to appear in Astérisque
[7] G.Faltings, *Relations between two moduli-spaces studied by Drinfeld,* preprint MPI 1991
[8] J.M.Fontaine, *Le corps de périodes p-adiques,* in "Périodes p-adiques", Astéerisque 223, 1994
[9] B.H.Gross, M.J.Hopkins *Equivariant vector bundles on the Lubin-Tate moduli space,* Cont. Math. 158 (1994), 23-88

[10] M.Harris, R.Taylor, *On the geometry and cohomology of some simple Shimura varieties,* preprint Paris VII, 1999

[11] l. Illusie, *Déformation des groupes de Barsotti-Tate,* in "Séminaire sur les pinceaux arithmétiques", Astérisque 127 (1985), 151-189

[12] B.Mazur, W.Messing, *Universal extensions and one dimensional crystalline cohomology,* Springer lecture Notes 370 (1974)

[13] M.Rapoport, Th.Zink, *Period spaces for p-divisible groups,* Annals of mathematics studies 141, Princeton University Press, Princeton 1996