The universal extension

Let R be a unitary ring. We consider functors from the category of R-algebras to the category of abelian groups. We write Hom_{ab} for homomorphisms of functors which respect the group structure and a bare Hom for homomorhisms of the set-valued functors.

Let M be an R-module. Then we define the functor $\underline{M}$:

$$\underline{M}(T) = M \otimes_R T, \quad \text{where } T \text{ is an } R-\text{algebra},$$

with the additive group structure on the right hand side.

Let $G = \operatorname{Spec} A$ be a finite locally free group scheme. Let $G^* = \operatorname{Spec} A^*$ be its Cartier dual. Let $J \subset A^*$ be the ideal of the neutral element. We set

$$\omega_{G^*} = J/J^2.$$

Proposition 1. *There is a canonical isomorphism:*

$$\mathrm{Hom}_{ab}(G, \underline{M}) \cong Hom_{R\text{-}mod}(\omega_{G^*}, M).$$

Proof: We start with a homomorphism $u : G \to \underline{M}$. If we regard u as a morphism of set-valued functors u is just an element of $\underline{M}(A) = A \otimes_R M$. Let $\xi : A \otimes_R M$ be the element which corresponds to u.

Let us denote $\epsilon_A : A \to R$ and $\epsilon_{A^*} : A^* \to R$ the augmentations which correspond to the neutral elements in G resp. G^*. The kernel of ϵ_{A^*} is J. We will denote by $1_A \in A$ and $1_{A^*} \in A^*$ the unit elements. If we regard 1_A as the structure map $1_A : R \to A$ then it is dual to $\epsilon_{A^*} : A^* \to R$.

The condition that the group homomorphism u maps the unit element in G to the zero element in $\underline{M}$ is

$$\epsilon_A \otimes \mathrm{id}_M(\xi) = 0$$

Moreover we use the natural isomorphism

$$\begin{array}{ccc} A \otimes_R M & \to & \mathrm{Hom}_{R\text{-mod}}(A^*, M) \\ \eta & \mapsto & \breve{\eta}. \end{array}$$

On checks in general that

$$(\epsilon_A \otimes \mathrm{id}_M)(\eta) = \breve{\eta}(1_{A^*}).$$

Therefore the condition that u respects neutral elements translates into

$$\breve{\xi}(1_{A^*}) = 0. \tag{1}$$

In other words $\breve{\xi}$ annihilates the first summand of the decomposition

$$A^* = R \oplus J.$$

Conversely let us start with an element $\breve{\xi} : A^* \to M$ which satisfies (1). It corresponds to a morphism $u : G \to \underline{M}$ which respects unit elements. Then the Proposition follows if we prove that u is a group homomorphism, iff $\breve{\xi}$ anihilates J^2.

The condition that u is a homomorphism is equivalent to the commutativity of the following diagram:

$$\begin{array}{ccc} G\times G & \xrightarrow{u\times u} & \underline{M}\times\underline{M} \\ {\scriptstyle m_G}\big\downarrow & & \big\downarrow{\scriptstyle +} \\ G & \xrightarrow{u} & \underline{M} \end{array} \tag{2}$$

Here m_G denotes the multiplication of G. We have

$\mathrm{Hom}(G\times G, \underline{M}\times\underline{M}) = \underline{M}(A\otimes_R A)\oplus\underline{M}(A\otimes_R A) = (A\otimes_R A\otimes_R M)\oplus(A\otimes_R A\otimes_R M).$

The morphism $u\times u$ corresponds on the right hand side of these equations to an element $\xi_1\oplus\xi_2$ which is described as follows:

We define maps

$$p_1, p_2 : A\otimes_R M \to A\otimes_R A\otimes_R M.$$

where $p_1(a\otimes m) = a\otimes 1_A\otimes m$ and $p_2(a\otimes m) = 1_A\otimes a\otimes m$. Then we have

$$\xi_1 = p_1(\xi), \quad \xi_2 = p_2(\xi).$$

Let us denote by $\Delta : A\to A\otimes_R A$ the comorphism of the multiplication m_G. We set $\Delta_M = \Delta\otimes\mathrm{id}_M$. Then the commutativity of (2) is equivalent with the equation:

$$\Delta_M(\xi) = \xi_1+\xi_2.$$

The last equation takes place in $A\otimes_R A\otimes_R M$. We want to rewrite it as an equation in the isomorphic module $\mathrm{Hom}_{R\text{-mod}}(A^*\otimes_R A^*, M)$. The element ξ_1 corresponds to $\breve{\xi}\otimes\epsilon_{A^*}$ and the element ξ_2 to $\epsilon_{A^*}\otimes\breve{\xi}$. Taking into account that Δ is dual to the multiplication $m_{A^*} : A^*\otimes_R A^*\to A^*$ we obtain the following form of the condition that u is a group homomorphism

$$\breve{\xi}\circ m_{A^*} = \breve{\xi}\otimes\epsilon_{A^*} + \epsilon_{A^*}\otimes\breve{\xi}. \tag{3}$$

But the right hand side is zero on $J\otimes J$ which means that $\breve{\xi}(J^2) = 0$. Conversely the last equation implies the condition (3). *Q.E.D.*

For a functor $X : (R\text{-Alg})\to(ab)$ we consider its completion $\hat{X} : \mathrm{Aug}_R\to(ab)$ on the category of augmented nilpotent algebras, which is given by

$$\hat{X}(A) = \mathrm{Ker}(X(A)\to X(R))$$

We will now restrict ourselves to the case, where G is a local finite group scheme, i.e. the augmentation ideal of G is nilpotent. Then $\mathrm{Hom}(\hat{G},\hat{\underline{M}}) = \mathrm{Hom}(G,\underline{M})$.

From now on we shall work with functors on Aug_R. Then we write simply $\underline{M}$ and mean the completion. We shall also assume that p is nilpotent in R.

The functors $F : \mathrm{Aug}_R\to(ab)$, with $F(R) = 0$ form an abelian category. Unless otherwise stated exact sequences and extensions are meant in this category.

Theorem 2. *Let G be a formal p-divisible group over R. Then there is a locally free and finite R-module U and an extension*

$$0\to\underline{U}\to L\to G\to 0 \tag{4}$$

such that for any extension

$$0 \to \underline{M} \to E \to G \to 0$$

where M is an R-module, there is a uniquely determined R-module homomorphism $U \to M$ which sits in a morphism of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \underline{U} & \longrightarrow & L & \longrightarrow & G & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \underline{M} & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 0. \end{array}$$

The extension (4) is called the universal extension of G. It commutes with base change $R \to R'$ to another ring.

In other words, the map induced from the connecting homomorphism of (4).

(5) $$\mathrm{Hom}_{R\text{-mod}}(U, M) \to \mathrm{Hom}_{ab}(\underline{U}, \underline{M}) \to \mathrm{Ext}^1(G, \underline{M})$$

is an isomorphism.

To explain the argument in [Messing] for this Theorem we need a category of sheaves. Let us denote by $\mathcal{S}_R$ the situs whose underlying category are the representable functors on Aug_R and whose coverings are flat morphisms $\mathrm{Spec}\, A_1 \to \mathrm{Spec}\, A_2$. (There is no localization with respect to $\mathrm{Spec}\, R$.)

It is known that the Cech cohomology $H^i(A_1 \to A_2, \underline{M}) = 0$ for $i \geq 1$. This shows that there is no difference between extension of G by $\underline{M}$ in the category of functors or in the category of sheaves. The situs is only needed to make the sequence

(6) $$0 \to G(p^n) \to G \xrightarrow{p^n} G \to 0$$

exact, which is not true in the category of functors.

Proof of Theorem 2: We fix a natural number n such that $p^n R = 0$. Then for each $\mathcal{N} \in \mathrm{Nil}_R$. We define a map $s_{\mathcal{N}}$ which makes the following diagram commutative

$$\begin{array}{ccccccccc} & & & & & & G(\mathcal{N}) & & \\ & & & & & \swarrow^{s_{\mathcal{N}}} & \downarrow p^n & & \\ 0 & \longrightarrow & M \otimes_R \mathcal{N} & \longrightarrow & E(\mathcal{N}) & \longrightarrow & G(\mathcal{N}) & \longrightarrow & 0. \end{array}$$

Let $\bar{\xi} \in G(\mathcal{N})$. We choose an element $\eta \in E(\mathcal{N})$ which maps to ξ by $E(\mathcal{N}) \to G(\mathcal{N})$. Then we define

$$s_{\mathcal{N}}(\xi) = p^n \eta.$$

Because $p^n(M \otimes_R \mathcal{N}) = 0$ this definition is independent of the choice of η and therefore functorial in $\mathcal{N}$. We obtain a morphism $s : G \to E$. If $s' : G \to E$ is any other morphism making the diagram commutative we obtain a morphism $s - s' : G \to \underline{M}$. This morphism has to be zero because $p^n \underline{M} = 0$ but the group G is p-divisible. The restriction of the section s to $G(p^n)$ is a well defined map

$$\mathrm{Ext}^1(G, \underline{M}) \to \mathrm{Hom}_{ab}(G(p^n), \underline{M}).$$

To see that this is an isomorphism we have to use sheaves.

Indeed in the category of abelian sheaves we obtain from (6) the exact Ext-sequence

$$\mathrm{Hom}(G, \underline{M}) \to \mathrm{Hom}(G(p^n), \underline{M}) \to \mathrm{Ext}^1(G, \underline{M}) \xrightarrow{p^n} \mathrm{Ext}^1(G, \underline{M}).$$

We have shown by construction of s above that the last arrow is zero. But in this calculus we see it directly from the fact, that $p^n \underline{M} = 0$. Since $\mathrm{Hom}(G, \underline{M}) = 0$ we obtain an isomorphism

$$\mathrm{Hom}(G(p^n), \underline{M}) \to \mathrm{Ext}^1(G, \underline{M}).$$

Combining this with Proposition 1 we obtain (5).

Finally we have to prove the compatability with base change. If F is a functor on Nil_R we denote by F' its restriction to $\mathrm{Nil}_{R'}$.

Now the universal extension is characterized by the property that it sits in a commutative diagram of functors

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G(p^n) & \longrightarrow & G & \xrightarrow{p^n} & G & & \\ & & \downarrow & & \downarrow & & \downarrow \mathrm{id} & & \\ 0 & \longrightarrow & \underline{U} & \longrightarrow & L & \longrightarrow & G & \longrightarrow & 0, \end{array}$$

where the arrow $G(p^n) \to \underline{U}$ is the universal map of Proposition 1. It follows from this Proposition that $G'(p^n) \to \underline{U'}$ is the universal arrow for $G'(p^n)$. Considering the base change of the above diagram to R' we obtain therefore the universal extension over R'. *Q.E.D.*

Let us consider a surjection of rings $\pi : S \to R$ with kernel $\mathfrak{a}$. We assume that p is nilpotent in S and that $\mathfrak{a}$ is endowed with divided powers γ, but we do not assume that the divided powers are nilpotent nor that the ideal $\mathfrak{a}$ is nilpotent. We fix a natural number n, such that $p^n S = 0$.

Let E be a strictly prorepresentable abelian functor on Aug_S. For each nilpotent S-algebra $\mathcal{N}$, which is endowed with nilpotent divided powers δ, we have the Grothendieck-Messing exponential, which is an isomorphism

$$\exp : \mathrm{Lie}\, E(\mathcal{N}) \to E(\mathcal{N})$$

If E is moreover a formal group we have $\mathrm{Lie}\, E(\mathcal{N}) = \mathcal{N} \otimes_S t_E$.

For an arbitrary nilpotent algebra $\mathcal{N}$ the algebra $\mathfrak{a} \otimes_S \mathcal{N}$ inherits a pd-structure $\tilde{\gamma}$ from $\mathfrak{a}$ which is uniquely determined by

$$\tilde{\gamma}_m(a \otimes x) = \gamma_m(a) \otimes x^m.$$

Clearly $\tilde{\gamma}$ is a nilpotent divided power structure and therefore we have the isomorphism

$$\exp : \mathrm{Lie}\, E(\mathfrak{a} \otimes_S \mathcal{N}) \to E(\mathfrak{a} \otimes \mathcal{N}),$$

which is functorial in E and in $\mathcal{N}$.

If E is a strictly prorepresentable formal group we obtain an exact sequence

$$\mathfrak{a} \otimes_S \mathcal{N} \otimes_S t_E \to E(\mathcal{N}) \to E(\mathcal{N}/\mathfrak{a}\mathcal{N}) \to 0. \tag{7}$$

This sequence is also left exact if $\mathcal{N}$ is a flat S-module because then we have $\mathfrak{a} \otimes_S \mathcal{N} = \mathfrak{a}\mathcal{N}$.

Let H be a p-divisible group over S. Let V be a finitely generated locally free S-module. Assume we are given an extension

$$0 \to \underline{V} \to E \to H \to 0. \tag{8}$$

It is obvious that E is a finite dimensional formal group and therefore strictly prorepresentable.

The exponentials for E and H give us an exact sequence:

$$((V \oplus \mathfrak{a} \otimes_S t_E)/(\mathfrak{a} \otimes_S V)) \otimes_S \mathcal{N} \to E(\mathcal{N}) \to H(\mathcal{N}/\mathfrak{a}\mathcal{N}) \to 0. \tag{9}$$

Morover this sequence is left exact if $\mathcal{N}$ is a flat S-module.

We will now start with a p-divisible formal group G on S. If we mention sheaves it will be always sheaves on $\mathcal{S}_S$. We take a universal extension of G:

$$0 \to \underline{U} \to L \to G \to 0,$$

where U is a finite locally free S-module. We will write $G_0 = \pi_{\bullet} G$ for the base change to R. The base change of $\underline{U}$ is the functor associated to the R-module $U_0 = U \otimes_S R$. Let $\bar{\rho} : G_0 \to H_0$ be a morphism of p-divisible groups over R.

Because the universal extension commutes with base change by Theorem 2 we obtain a uniquely determined diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \underline{U}_0 & \longrightarrow & L_0 & \longrightarrow & G_0 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \bar{\tau}} & & \downarrow{\scriptstyle \bar{\mu}} & & \downarrow{\scriptstyle \bar{\rho}} & & \\ 0 & \longrightarrow & \underline{V}_0 & \longrightarrow & E_0 & \longrightarrow & H_0 & \longrightarrow & 0, \end{array}$$

such that $\bar{\tau}$ is induced by an R-module homomorphism $U_0 \to V_0$ which we denote by the same letter. We note that it is very important to distinguish between arbitrary morphisms $\underline{U}_0 \to \underline{V}_0$ and those which are induced by R-module homomorphisms $U_0 \to V_0$.

Theorem 3. *There is a unique morphism of formal groups $\mu : L \to E$ which lifts $\bar{\mu}$ and which has the following property:*

Let $\tau : U \to M$ be an arbitrary R-module homomorphism which lifts of τ_0 and consider the following diagram

$$\begin{array}{ccc} \underline{U} & \longrightarrow & L \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \mu} \\ \underline{V} & \longrightarrow & E. \end{array}$$

It need not to be commutative but the difference of the two maps $\underline{U} \to E$ factors

$$\underline{U} \to \underline{\mathfrak{a} \otimes_S t_E} \xrightarrow{\exp} E,$$

where the first map is induced by an R-module homomorphism $U \to \mathfrak{a} \otimes_S t_E$.

Proof: We begin with the construction of μ. We fix a natural number n such that $p^n S = 0$. For $\mathcal{N} \in \mathrm{Nil}_S$ we consider the canonical map

$$G(\mathcal{N}) \to G(\mathcal{N}/\mathfrak{a}) = G_0(\mathcal{N}/\mathfrak{a}) \xrightarrow{\bar{\mu}} H_0(\mathcal{N}/\mathfrak{a}) \tag{10}$$

We will construct a morphism $t : G \to E$ such that the following diagram becomes commutative.

(11)

$$\begin{array}{ccccccc} G(p^n)(\mathcal{N}) & \longrightarrow & G(\mathcal{N}) & \xrightarrow{p^n} & G(\mathcal{N}) & & \\ & & \big\downarrow t & & \big\downarrow & & \\ ((V \oplus (\mathfrak{a} \oplus t_E))/(\mathfrak{a} \otimes V)) \otimes_S \mathcal{N} & \longrightarrow & E(\mathcal{N}) & \longrightarrow & H_0(\mathcal{N}/\mathfrak{a}\mathcal{N}) & \longrightarrow & 0 \end{array}$$

In this diagram the rows are exact (see (9)). The first arrow of the upper row is always injective and for the first arrow of the lower row this is true if $\mathcal{N}$ is a flat R-module.

We see that the kernel of $E(\mathcal{N}) \to H_0(\mathcal{N}/\mathfrak{a}\mathcal{N})$ in annihilated by p^n.

Let $\xi \in G(\mathcal{N})$. We denote by $\eta \in H_0(\mathcal{N}/\mathfrak{a}\mathcal{N})$ is image by right vertical map (10). Take an inverse image $\tilde{\eta} \in E(\mathcal{N})$. We define $t(\xi) = p^n\tilde{\eta}$. Clearly this is well-defined and gives the desired commutativity.

Let $\mathcal{N}$ be a flat S-module so that the lower row of the diagram is also left exact. In this case we obtain a map

$$G(p^n)(\mathcal{N}) \to \underline{M}(\mathcal{N}).$$

where M denotes the S-module $(V \oplus (\mathfrak{a} \oplus t_E))/(\mathfrak{a} \otimes V))$. Inserting for $\mathcal{N}$ the flat augmentation ideal of $G(p^n)$ and taking the image of $\mathrm{id} \in G(p^n)(\mathcal{N})$ we obtain a morphism of functors

$$G(p^n) \to \underline{M}. \qquad (12)$$

One has to check that this is a morphism of group functors. Indeed, let $G(p^n) = \operatorname{Spec} A$. Then it suffices to show that

$$G(p^n)(A \otimes_S A) \to \underline{M}(A \otimes_S A)$$

is a group homomorhism. But since $A \otimes_S A$ is flat, this follows from the definition.

The morphism (12) fits into a commutative diagram

$$\begin{array}{ccc} G(p^n) & \longrightarrow & G \\ \big\downarrow & & \big\downarrow \\ \underline{M} & \longrightarrow & E. \end{array}$$

By Proposition 1 and the the proof of Theorem 2 the last map factors through an R-module homomorphism

$$G(p^n) \to \underline{U} \to \underline{M}.$$

Therefore the last commutative diagram implies a commutative diagram

$$\begin{array}{ccc} G(p^n) & \longrightarrow & G \\ \big\downarrow & & \big\downarrow \\ \underline{U} & \longrightarrow & E. \end{array} \qquad (13)$$

Again by the construction of the universal extension the following diagram is a cofibre product in the abelian category of abelian sheaves of $\mathcal{S}_S$:

$$\begin{array}{ccc} G(p^n) & \longrightarrow & G \\ \downarrow & & \downarrow \\ \underline{U} & \longrightarrow & L \end{array}$$

Therefore the diagram (13) provides the desired map $\mu : L \to E$. It enjoys the required property because $\underline{U} \to \underline{M}$ is induced by an R-module homomorphism.

Let μ now an arbitrary lifting of μ_0 with the property of the Theorem. Finally we show that the map μ is unique. By construction the universal extension fits into a commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G(p^n) & \longrightarrow & G & \xrightarrow{p^n} & G & & \\ & & \downarrow & & \downarrow{\scriptstyle \lambda} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & \underline{U} & \longrightarrow & L & \longrightarrow & G & \longrightarrow & 0 \end{array}$$

We begin to show that the map $\mu \circ \lambda$ coincides with the map t in diagram (11). In fact this holds for an arbitrary lifting or μ_0. We make this assertion more explicit: The assumption that μ lifts μ_0 gives us for each $\mathcal{N} \in \mathrm{Nil}_S$ a commutative diagram

(14)
$$\begin{array}{ccc} G(\mathcal{N}) & \xrightarrow{p^n} & G(\mathcal{N}) \\ \downarrow{\scriptstyle \lambda} & & \downarrow \\ L(\mathcal{N}) & \longrightarrow & G(\mathcal{N}/(\mathfrak{a}\mathcal{N}) \\ {\scriptstyle \mu}\downarrow & & \downarrow{\scriptstyle \bar{\rho}} \\ E(\mathcal{N}) & \longrightarrow & H(\mathcal{N}/\mathfrak{a}\mathcal{N}). \end{array}$$

Let $\xi \in G(\mathcal{N})$. Let $\bar{\xi} \in H(\mathcal{N}/\mathfrak{a}\mathcal{N})$ be its image all the way down on the right hand side of the diagram. Let $\eta \in E(\mathcal{N})$ a preimage of $\bar{\xi}$. Then our assertion says

(15)
$$\mu \circ \lambda(\xi) = p^n \eta.$$

The question whether the two maps of sheaves $\mu \circ \lambda, t : G \to E$ agree is local with respect to the situs $\mathcal{S}_S$. Therefore we may assume that there exists an element $\xi_1 \in G(\mathcal{N})$ such that $p^n \xi_1 = \xi$. We conclude that

$$p^n(\mu \circ \lambda(\xi_1)) = \mu \circ \lambda(\xi).$$

But by the diagram (14) the element $\mu \circ \lambda(\xi_1)$ is mapped to $\bar{\xi}$. Therefore we may use this element for η to prove (15). This makes the equation obvious.

Now we know that $\mu \circ \lambda$ is uniquely determined. Consider the commutative diagram

$$
\begin{array}{ccc}
G(p^n) & \longrightarrow & G \\
\big\downarrow & & \big\downarrow \lambda \\
\underline{U} & \longrightarrow & L \\
\breve{\mu} \big\downarrow & & \big\downarrow \mu \\
E & \xrightarrow{\mathrm{id}} & E
\end{array}
\tag{16}
$$

Here $\breve{\mu}$ denotes the restriction of μ. Because the upper square is a push-out in the category of sheaves, it follows that μ is uniquely determined by $\breve{\mu}$ and $\mu \circ \lambda$. It remains to show that $\breve{\mu}$ is uniquely determined.

Let $\mathcal{N} \in \mathrm{Nil}_S$ be flat as S-module. Then we obtain from (16) the morphisms:

$$G(p^n)(\mathcal{N}) \to \underline{U}(\mathcal{N}) \stackrel{\breve{\mu}}{\to} \underline{M}(\mathcal{N})$$

Here M has the same meaning as in (12). We know that the composite of these two maps is uniquely determined. The morphism $\breve{\mu}$ would be uniquely determined by Proposition 1, if we knew that $\breve{\mu}$ induced from a map of R-modules $U \to M$. But this is exactly what condition on μ in the Theorem says.

Q.E.D.