Finite group schemes

Lecture course in WS 2004/05

by Richard Pink, ETH Zürich
pink@math.ethz.ch

Contents

Outline

The aim of the lecture course is the classification of finite commutative group schemes over a perfect field of characteristic p, using the classical approach by contravariant Dieudonné theory. The theory is developed from scratch; emphasis is placed on complete proofs. No prerequisites other than a good knowledge of algebra and the basic properties of categories and schemes are required. The original plan included p-divisible groups, but there was no time for this.

Acknowledgements

It is my great pleasure to thank the participants of the course for their active and lively interest. In particular I would like to thank Alexander Caspar, Ivo Dell'Ambrogio, Stefan Gille, Egon Rütsche, Nicolas Stalder, Cory Edwards, and Charles Mitchell for their efforts in preparing these notes.

Zürich, February 10, 2005 Richard Pink

Lecture 1

October 21, 2004
Notes by Egon Rütsche

§1 Motivation

Let A be a g-dimensional abelian variety over a field k, and let p be a prime number. Let $k^{sep} \subset \bar{k}$ denote a separable, respectively algebraic closure of k. For all $n \geq 0$, define

$$A(\bar{k})[p^n] := \{a \in A(\bar{k}) \mid p^n a = 0\}.$$

Then the following holds:

$$A(\bar{k})[p^n] \cong \begin{cases} \big(\mathbb{Z}/p^n\big)^{\oplus 2g} & \text{if } p \neq \operatorname{char}(k) \\ \big(\mathbb{Z}/p^n\mathbb{Z}\big)^{\oplus h} & \text{if } p = \operatorname{char}(k), \end{cases}$$

where h is independent of n, and $0 \leq h \leq g$.

Definition. *The p-adic Tate module of A* is defined by

$$T_pA := \varprojlim A(\bar{k})[p^n]\,.$$

Then we have the following isomorphisms

$$T_pA \cong \begin{cases} \mathbb{Z}_p^{\oplus 2g} & \text{if } p \neq \operatorname{char}(k) \\ \mathbb{Z}_p^{\oplus h} & \text{if } p = \operatorname{char}(k). \end{cases}$$

If p is not equal to the characteristic of k, we have a famous theorem, which compares the endomorphisms of the abelian variety with those of the Tate module.

Theorem (Tate conjecture for endomorphisms of abelian varieties). If $p \neq \operatorname{char}(k)$ and k is finitely generated over its prime field, then the natural homomorphism

$$\operatorname{End}(A) \otimes \mathbb{Z}_p \to \operatorname{End}_{\mathbb{Z}_p[\operatorname{Gal}(k^{sep}/k)]}(T_pA)$$

is an isomorphism.

Remark. This theorem was proven by Tate for finite k, by Faltings for number fields, and by others in other cases.

The Tate module can be considered as the first homology group of the abelian variety. For this, assume that $\mathrm{char}(k) = 0$ and embed k into the complex numbers. Then the isomorphism $A(\mathbb{C}) \cong (\mathrm{Lie}\, A_{\mathbb{C}})/\, \mathrm{H}_1\big(A(\mathbb{C}), \mathbb{Z}\big)$ induces an isomorphism $T_pA \cong \mathrm{H}_1\big(A(\mathbb{C}), \mathbb{Z}\big) \otimes \mathbb{Z}_p$.

Let us now consider what happens if p is equal to the characteristic of k. This gives us a motivation to consider finite group schemes and p-divisible groups. For any positive integer m consider the morphism $m \cdot \mathrm{id} : A \to A$. It is a finite morphism of degree m^{2g}, so its scheme theoretic kernel $A[m]$ is a finite group scheme of degree m^{2g}. We can write $m \cdot \mathrm{id}$ as the composite of the two maps

$$A \xrightarrow{\mathrm{diag}} \underbrace{A \times \ldots \times A}_{m} \xrightarrow{\Sigma} A\,.$$

Looking at the tangent spaces, we can deduce that the derivative of $m \cdot \mathrm{id}$ is again the endomorphism $m \cdot \mathrm{id}$ on the Lie algebra of A. If $p \nmid m$, this is an isomorphism, which implies that the kernel of multiplication by m is an étale group scheme. But if p divides m, the derivative is 0, and in this case $A[m]$ is non-reduced.

Taking $m = p^n$ for $n \to \infty$, we have the inclusions $A[p^n] \subset A[p^{n+1}] \subset \ldots$. The union of these finite group schemes is called *the p-divisible group of A*, and is denoted by $A[p^\infty]$. Since the $A[p^n]$ contain arbitrarily large infinitesimal neighbourhoods of 0, their union $A[p^\infty]$ contains the formal completion of A at 0. This shows that studying group schemes and p-divisible groups gives us information on both the abelian variety and its formal completion.

The goal of this course is to present the basic theory and classification of finite commutative group schemes over a perfect field. With this knowledge it will be possible to study general p-divisible groups and to formulate and understand the significance of an analogue of the above mentioned theorem for the p-divisible group of an abelian variety in characteristic p. However, there will be no mention of these further lines of developments in the course, or even of p-divisible groups and abelian varieties, at all.

We finish this motivation with some examples of commutative group schemes and finite subgroup schemes thereof:

Example. Define $\mathbb{G}_{m,k} := \mathrm{Spec}\, k[T, T^{-1}]$. The multiplication is given by $(t, t') \mapsto t \cdot t'$. This group scheme is called *the multiplicative group over k*. The homomorphism $m \cdot \mathrm{id} : \mathbb{G}_{m,k} \to \mathbb{G}_{m,k}$ is given by $t \mapsto t^m$. We want to know its kernel, which is denoted by $\mu_{m,k}$. This is defined as the fiber product in the following commutative diagram

$$\begin{tikzcd}
\mathbb{G}_{m,k} \arrow[r, "m\cdot\mathrm{id}"] & \mathbb{G}_{m,k} \\
\mu_{m,k} \arrow[u] \arrow[r] & \operatorname{Spec} k\,. \arrow[u, "1"']
\end{tikzcd}$$

Since the fiber product corresponds to the tensor product of the associated rings of functions, this diagram corresponds to the commutative diagram

$$\begin{tikzcd}
k[T, T^{-1}] \arrow[d] & k[S, S^{-1}] \arrow[l, "T^m \mapsfrom S"'] \arrow[d] \\
k[T]/(T^m - 1) & k. \arrow[l]
\end{tikzcd}$$

Thus we get the equality $\mu_{m,k} = \operatorname{Spec} k[T]/(T^m - 1)$ with the group operation $(t, t') \mapsto t \cdot t'$. If $p = \mathrm{char}(k)$, we have $T^{p^n} - 1 = (T - 1)^{p^n}$ and therefore $\mu_{p^n,k} \cong \operatorname{Spec} k[U]/(U^{p^n})$ where $U = T - 1$. This is therefore a non-reduced group scheme possessing a single point. Note that the group operation in terms of the coordinate U is given by $(u, u') \mapsto u + u' + u \cdot u'$.

Example. For comparison let $\mathbb{G}_{a,k} := \operatorname{Spec} k[X]$ with the operation $(x, x') \mapsto x + x'$ denote *the additive group over* k. Since $(x + x')^{p^n} = x^{p^n} + x'^{p^n}$ over k, the finite closed subscheme $\operatorname{Spec} k[X]/(X^{p^n})$ is a subgroup scheme of $\mathbb{G}_{a,k}$. Although its underlying scheme is isomorphic to the scheme underlying $\mu_{p^n,k}$, we will see later that these group schemes are non-isomorphic.

§2 Group objects in a category

The definition of an abstract group G includes a map $G \times G \to G$. In order to define group objects in a category, we need to make sense of '$G \times G$' in that category, that is, we need products. For any two objects X, Z of a category, we denote the set of morphisms $Z \to X$ by $X(Z)$. Let $\mathscr{C}$ be a category with arbitrary finite products. This means that the following two properties hold:

(i) For any two objects $X, Y \in \mathrm{Ob}(\mathscr{C})$ there exists a triple consisting of an object $X \times Y \in \mathrm{Ob}(\mathscr{C})$ and two morphisms $\pi_X : X \times Y \to X$ and $\pi_Y : X \times Y \to Y$ such that for any object $Z \in \mathrm{Ob}(\mathscr{C})$ the natural map of sets

$$(X \times Y)(Z) \to X(Z) \times Y(Z),\ \varphi \mapsto (\pi_X \circ \varphi, \pi_Y \circ \varphi)$$

is bijective.

(ii) There exists a *final object* $* \in \mathrm{Ob}(\mathscr{C})$, that is, an object such that for every $Z \in \mathrm{Ob}(\mathscr{C})$ there exists a unique morphism $Z \to *$.

Remark. If we have products of two objects, then by iterating we get products of more than two objects. Property (ii) is what comes out by requiring the existence of an empty product. The existence of a product of just one object is clear.

In (i) one easily shows that $X \times Y$ together with its two 'projection morphisms' π_X, π_Y is determined up to unique isomorphism. Any choice of it is called *the product of X and Y in $\mathscr{C}$.* Similarly, the final object $*$, and therefore arbitrary finite products, are defined up to unique isomorphism.

Definition. *A commutative group object in the category $\mathscr{C}$* is a pair consisting of an object $G \in \mathrm{Ob}(\mathscr{C})$ and a morphism $\mu : G \times G \to G$ such that for any object $Z \in \mathrm{Ob}(\mathscr{C})$ the map $G(Z) \times G(Z) \to G(Z),\ (g, g') \mapsto \mu \circ (g, g')$ defines a commutative group.

Let us check what associativity, commutativity, and the existence of an identity and an inverse for all Z means.

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

(i) (Associativity) The following diagram is commutative:

$$\begin{tikzcd}
G \times G \times G \arrow[r, "\mu \times \mathrm{id}"] \arrow[d, "\mathrm{id} \times \mu"'] & G \times G \arrow[d, "\mu"] \\
G \times G \arrow[r, "\mu"] & G\,.
\end{tikzcd}$$

(ii) (Commutativity) The following diagram is commutative:

$$\begin{tikzcd}
G \times G \arrow[r, "\mu"] \arrow[d, "\sigma"'] & G \\
G \times G\,, \arrow[ur, "\mu"'] &
\end{tikzcd}$$

where σ is the morphism which interchanges the two factors.
(Deduce the existence of σ from the defining property of products!)

(iii) (Identity Element) There exists a morphism $e : * \to G$ such that the following diagram commutes:

$$\begin{tikzcd}
* \times G \arrow[r, "e \times \mathrm{id}"] \arrow[d, "pr_2"', "\wr"] & G \times G \arrow[dl, "\mu"] \\
G\,. &
\end{tikzcd}$$

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

$$\begin{tikzcd}
G \times G \arrow[rr, "\mathrm{id} \times i"] & & G \times G \arrow[d, "\mu"] \\
G \arrow[u, "\mathrm{diag}"] \arrow[r] & * \arrow[r, "e"] & G
\end{tikzcd},$$

where e is the morphism from (iii).

Sketch of the proof. The 'if' part follows easily by taking Z-valued points. For the 'only if' part:

(i) Take $Z = G \times G \times G$ and apply the associativity in $G(Z)$ to the tautological element $\mathrm{id} \in (G \times G \times G)(Z) = G(Z) \times G(Z) \times G(Z)$.

(ii) Analogous with $Z = G \times G$.

(iii) The morphism $e : * \to G$ is defined as the identity element of $G(*)$. For any Z consider the map $G(*) \to G(Z)$ defined by composing a morphism $* \to G$ with the unique morphism $Z \to *$. Clearly this map is compatible with μ, so it is a group homomorphism and therefore maps e to the identity element of $G(Z)$. The commutativity of the diagram can now be deduced by taking $Z = G$.

(iv) The morphism $i : G \to G$ is defined as the inverse in the group $G(G)$ of the tautological element $\mathrm{id} \in G(G)$. The rest is analogous to (iii).

Remark. The definition of group objects in a category is often given in terms of the commutativity of the diagrams above. But both definitions have their advantages. The first, functorial, definition allows us to automatically translate all the usual formulas for groups into formulas for group objects. For example, since the identity and inverse elements in an abstract group are uniquely determined, we deduce at once that the morphisms e and i are unique. The same goes for formulas such as $(x^{-1})^{-1} = x$ and $(xy)^{-1} = y^{-1}x^{-1}$. All these formulas for group objects can also be derived from the second definition, but less directly.

Lecture 2

October 28, 2004
Notes by Stefan Gille

§3 Affine group schemes

Let $\mathfrak{Rings}$ be the category of commutative noetherian rings with 1, called the *category of unitary rings*. Morphisms in this category are maps $\varphi : R \longrightarrow S$ which are additive and multiplicative and satisfy $\varphi(1) = 1$. The last condition is important, but sometimes forgotten. As is well known the assignment $R \longmapsto \operatorname{Spec} R$ is an anti-equivalence of categories:

$$\mathfrak{Rings} \longleftrightarrow \mathfrak{aff.Sch}\,,$$

where $\mathfrak{aff.Sch}$ denotes the category of affine schemes. Let R be in $\mathfrak{Rings}$. An object A of $\mathfrak{Rings}$ together with a morphism $R \longrightarrow A$ in $\mathfrak{Rings}$ is called a *unitary R-algebra*. Equivalently A is an R-module together with two homomorphisms of R-modules

$$\begin{tikzcd} R \arrow[r, "e"] & A & A \otimes_R A \arrow[l, "\mu"'] \end{tikzcd}\,,$$

such that μ is associative and commutative, i.e.,

$$\begin{aligned} \mu(a \otimes a') &= \mu(a' \otimes a) \quad \text{and} \\ \mu(a \otimes \mu(a' \otimes a'')) &= \mu(\mu(a \otimes a') \otimes a'')\,, \end{aligned}$$

and e induces a unit, i.e.,

$$\mu(e(1) \otimes a) = a.$$

We denote the category of unitary R-algebras by R-$\mathfrak{Alg}$. The above anti-equivalence restricts to an anti-equivalence

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

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

Definition. Let R be a unitary ring. An *affine commutative group scheme over* $\operatorname{Spec} R$ is a commutative group object in the category of affine schemes over $\operatorname{Spec} R$.

Convention. In the following all groups schemes are assumed to be affine and commutative.

Let $G = \operatorname{Spec} A$ be such a group scheme over $\operatorname{Spec} R$. The morphisms associated with the group object G correspond to the following homomorphisms of R-modules:

(3.1)
$$\begin{tikzcd} R \arrow[r, bend right, "e"'] & A \arrow[l, bend right, "\epsilon"'] \arrow[r, bend right, "m"'] \arrow[loop below, "\iota"] & A \otimes_R A \arrow[l, bend right, "\mu"'] . \end{tikzcd}$$

Here μ and e are the structure maps of the R-algebra A. The map m, called the *comultiplication*, corresponds to the group operation $G \times G \to G$. The map ϵ, called the *counit*, corresponds to the morphism $* \longrightarrow G$ yielding the unit in G, and ι, the *antipodism*, corresponds to the morphism $G \longrightarrow G$ sending an element to its inverse.

The axioms for a commutative group scheme translate to those in the following table. Here $\sigma : A \otimes_R A \longrightarrow A \otimes_R A$ denotes the switch map $\sigma(a \otimes a') = a' \otimes a$, and the equalities marked $\overset{!}{=}$ at the bottom right are consequences of the others.

meaning	axiom	axiom	meaning
μ associative	$\mu \circ (\mathrm{id} \otimes \mu) = \mu \circ (\mu \otimes \mathrm{id})$	$(m \otimes \mathrm{id}) \circ m = (\mathrm{id} \otimes m) \circ m$	m coassociative
μ commutative	$\mu \circ \sigma = \mu$	$\sigma \circ m = m$	m cocommutative
e unit for μ	$\mu \circ (e(1) \otimes \mathrm{id}) = \mathrm{id}$	$(\epsilon \otimes \mathrm{id}) \circ m = 1 \otimes \mathrm{id}$	ϵ counit for m
m homomorphism	$m \circ \mu = (\mu \otimes \mu) \circ (\mathrm{id} \otimes \sigma \otimes \mathrm{id}) \circ (m \otimes m)$		
of unitary rings	$m(e(1)) = e(1) \otimes e(1)$	$\epsilon \circ \mu = \epsilon \otimes \epsilon$	ϵ homomorphism
	$\epsilon \otimes e = \mathrm{id}$		of unitary rings
ι homomorphism	$\iota \circ \mu = \mu \circ (\iota \otimes \iota)$	$m \circ \iota = (\iota \otimes \iota) \circ m$	$(xy)^{-1} \overset{!}{=} x^{-1}y^{-1}$
of unitary rings	$\iota \circ e = e$	$\epsilon \circ \iota = \epsilon$	$1 \overset{!}{=} 1^{-1}$
ι coinverse for m	$e \circ \epsilon = \mu \circ (\mathrm{id} \otimes \iota) \circ m$		

Definition. An R-module A together with maps μ, ϵ, e, m, and ι satisfying the above axioms is called an *associative, commutative, unitary, coassociative, cocommutative, counitary R-bialgebra with antipodism*, or shorter, a *cocommutative R-Hopf algebra with antipodism.*

Definition. A *homomorphism of group schemes* $\Phi : G \longrightarrow H$ over $\operatorname{Spec} R$ is a morphism in $\mathfrak{aff}.R\text{-}\mathfrak{Sch}$, such that the induced morphism $G(Z) \longrightarrow H(Z)$ is a homomorphism of groups for all Z in $\mathfrak{aff}.R\text{-}\mathfrak{Sch}$. For $G = \operatorname{Spec} A$ and $H = \operatorname{Spec} B$ this morphism corresponds to a homomorphism of R-modules $\phi : B \longrightarrow A$ making the following diagram commutative:

(3.2)
$$\begin{tikzcd}
R \arrow[r, bend right, "e_A"'] \arrow[d, dash, "\mathrm{id}"] & A \arrow[l, bend right, "\epsilon_A"'] \arrow[r, bend right, "m_A"'] & A \otimes_R A \arrow[l, bend right, "\mu_A"'] \\
R \arrow[r, bend right, "e_B"'] & B \arrow[u, "\phi"] \arrow[l, bend right, "\epsilon_B"'] \arrow[r, bend right, "m_B"'] & B \otimes_R B \,. \arrow[l, bend right, "\mu_B"'] \arrow[u, "\phi\otimes\phi"']
\end{tikzcd}$$

Definition. The *sum* of two homomorphisms $\Phi, \Psi : G \longrightarrow H$ is defined by the commutative diagram

(3.3)
$$\begin{tikzcd}
G \arrow[r] \arrow[d, "\Phi+\Psi"'] & G \times G \arrow[d, "\Phi\times\Psi"] \\
H & H \times H \arrow[l] \ ,
\end{tikzcd}$$

where the upper arrow is the diagonal morphism and the lower arrow the group operation of H. We leave it to the reader to check that $\Phi + \Psi$ is a homomorphism of group schemes.

The category of commutative affine group schemes over $\operatorname{Spec} R$ is additive.

§4 Cartier duality

We now assume that the group scheme $G = \operatorname{Spec} A$ is finite and flat over R, i.e. that A is a locally free R-module of finite type. Let $A^* := \operatorname{Hom}_R(A, R)$ denote its R-dual. Dualizing the diagram (3.1), and identifying $R = R^*$ and $(A \otimes_R A)^* = A^* \otimes_R A^*$ we obtain homomorphisms of R-modules

(4.1)
$$\begin{tikzcd}
R \arrow[r, bend right, "\epsilon^*"'] & A^* \arrow[l, bend right, "e^*"'] \arrow[r, bend right, "\mu^*"'] \arrow[loop below, "\iota^*"] & A^* \otimes_R A^* \,. \arrow[l, bend right, "m^*"']
\end{tikzcd}$$

A glance at the self dual table above shows that the morphisms $e^*, m^*, \mu^*, \epsilon^*$, and ι^* satisfy the axioms of a cocommutative Hopf algebra with antipodism, and therefore $G^* := \operatorname{Spec} A^*$ is a finite flat group scheme over $\operatorname{Spec} R$, too.

Definition. G^* is called the *Cartier dual* of G.

If $\Phi : G \longrightarrow H$ is a homomorphism of finite flat group schemes corresponding to the homomorphism $\phi : B \longrightarrow A$, the symmetry of diagram (3.2) shows that $\phi^* : A^* \longrightarrow B^*$ corresponds to a homomorphism of group schemes $\Phi^* : H^* \longrightarrow G^*$. Therefore Cartier duality is a contravariant functor from the category of finite flat commutative affine group schemes to itself.

Moreover this functor is additive. Indeed, for any two homomorphisms $\Phi, \Psi : G \longrightarrow H$ the equation $(\Phi + \Psi)^* = \Phi^* + \Psi^*$ follows directly by dualizing the diagram (3.3).

Remark. The Cartier duality functor is involutive. Indeed, the natural evaluation isomorphism id $\longrightarrow^{**}$ induces a functorial isomorphism $G \simeq G^{**}$.

§5 Constant group schemes

Let Γ be a finite (abstract) abelian group, whose group structure is written additively. We want to associate to Γ a finite commutative group scheme over $\operatorname{Spec} R$. The obvious candidate for its underlying scheme is

$$G \;:=\; \text{“}\Gamma \times \operatorname{Spec} R\text{”} \;:=\; \coprod_{\gamma \in \Gamma} \operatorname{Spec} R\,,$$

the disjoint union of $|\Gamma|$ copies of the final object $* = \operatorname{Spec} R$ in the category $\mathfrak{aff}.R\text{-}\mathfrak{Sch}$. The group operation on G is defined by noting that

$$G \times G \;\cong\; \text{“}\Gamma \times \Gamma \times \operatorname{Spec} R\text{”} \;:=\; \coprod_{\gamma, \gamma' \in \Gamma} \operatorname{Spec} R\,,$$

and mapping the leaf $\operatorname{Spec} R$ of $G \times G$ indexed by (γ, γ') identically to the leaf of G indexed by $\gamma + \gamma'$. One easily sees that this defines a finite flat commutative group scheme over $\operatorname{Spec} R$.

Definition. This group scheme is called the *constant group scheme over R with fiber* Γ and denoted $\underline{\Gamma}_R$.

Let us work out this construction on the underlying rings. The ring of regular functions on $\underline{\Gamma}_R$ is naturally isomorphic to the ring of functions

$$R^\Gamma \;:=\; \{\, f : \Gamma \longrightarrow R \,|\, f \text{ is a map of sets } \}\,,$$

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

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

$$e_\gamma \,:\, \Gamma \longrightarrow R, \qquad \gamma' \longmapsto \begin{cases} 1 & \text{if } \gamma = \gamma' \\ 0 & \text{otherwise.} \end{cases}$$

One checks that μ, ϵ, e, m, and ι are given on this basis by

$$\begin{aligned}
\mu(e_\gamma \otimes e_{\gamma'}) &= \begin{cases} e_\gamma & \text{if } \gamma = \gamma' \\ 0 & \text{otherwise} \end{cases} \\
\epsilon(e_\gamma) &= \begin{cases} 1 & \text{if } \gamma = 0 \\ 0 & \text{otherwise} \end{cases} \\
e(1) &= \sum_{\gamma\in\Gamma} e_\gamma \\
m(e_\gamma) &= \sum_{\gamma'\in\Gamma} e_{\gamma'} \otimes e_{\gamma-\gamma'} \\
\iota(e_\gamma) &= e_{-\gamma}
\end{aligned}$$

To calculate the Cartier dual of $\underline{\Gamma}_R$ let $\{\hat{e}_\gamma\}_{\gamma\in\Gamma}$ denote the basis of $(R^\Gamma)^*$ dual to the one above, characterized by

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

The dual maps are then given by the formulas

$$\begin{aligned}
\mu^*(\hat{e}_\gamma) &= \hat{e}_\gamma \otimes \hat{e}_\gamma \\
\epsilon^*(1) &= \hat{e}_0 \\
e^*(\hat{e}_\gamma) &= 1 \\
m^*(\hat{e}_\gamma \otimes \hat{e}_{\gamma'}) &= \hat{e}_{\gamma+\gamma'} \\
\iota^*(\hat{e}_\gamma) &= \hat{e}_{-\gamma}
\end{aligned}$$

The formulas for m^* and ϵ^* show that $(R^\Gamma)^*$ is isomorphic to the group ring $R[\Gamma]$ as an R-algebra, such that e^* corresponds to the usual augmentation map $R[\Gamma] \longrightarrow R$.

Example. Let $\Gamma := \mathbb{Z}/\mathbb{Z}n$ be the cyclic group of order $n \in \mathbb{N}$. Then with $X := \hat{e}_1$ the above formulas show that $(R^\Gamma)^* \cong R[X]/(X^n - 1)$ with the comultiplication $\mu^*(X) = X \otimes X$. Thus we deduce that

$$(\underline{\mathbb{Z}/\mathbb{Z}n}_R)^* \cong \boldsymbol{\mu}_{n,R}.$$

Example. Assume that $p \cdot 1 = 0$ in R for a prime number p. Recall that $\boldsymbol{\alpha}_{p,R} = \operatorname{Spec} A$ with $A = R[T]/(T^p)$ and the comultiplication $m(T) = T \otimes 1 + 1 \otimes T$. In terms of the basis $\{T^i\}_{0 \le i < p}$ all the maps are given by the formulas

$$\begin{aligned}
\mu(T^i \otimes T^j) &= \begin{cases} T^{i+j} & \text{if } i+j<p \\ 0 & \text{otherwise} \end{cases} \\
\epsilon(T^i) &= \begin{cases} 1 & \text{if } i=0 \\ 0 & \text{otherwise} \end{cases} \\
e(1) &= T^0 \\
m(T^i) &= \sum_{0 \le j \le i} \tbinom{i}{j} \cdot T^j \otimes T^{i-j} \\
\iota(T^i) &= (-1)^i \cdot T^i
\end{aligned}$$

Let $\{u_i\}_{0 \le i < p}$ denote the dual basis of A^*. Then using the above formulas one easily checks that the R-linear map $A^* \longrightarrow A$ sending u_i to $T^i/i!$ is an isomorphism of Hopf algebras. Therefore

$$(\boldsymbol{\alpha}_{p,R})^* \cong \boldsymbol{\alpha}_{p,R}.$$

Proposition. For any field k of characteristic $p > 0$, the group schemes $\underline{\mathbb{Z}/\mathbb{Z}p}_k$, $\boldsymbol{\mu}_{p,k}$, and $\boldsymbol{\alpha}_{p,k}$ are pairwise non-isomorphic.

Proof. The first one is étale, while both $\boldsymbol{\mu}_{p,k} = \operatorname{Spec} k[X]/(X^p - 1)$ and $\boldsymbol{\alpha}_{p,k} = \operatorname{Spec} k[T]/(T^p)$ are non-reduced. Although the underlying schemes of the latter two are isomorphic, the examples above show that this is not the case for their Cartier duals. The proposition follows. □

Lecture 3

November 4, 2004
Notes by Cory Edwards

§6 Actions and quotients in a category

Our goal is to define the notions of group actions and quotients in a general category. Let $\mathscr{C}$ be a category with arbitrary finite products.

Definition. A *(left) action* of a group object G on an object X is a morphism $m : G \times X \to X$ such that for all objects $Z \in \mathrm{Ob}(\mathscr{C})$, the map

$$G(Z) \times X(Z) = (G \times X)(Z) \xrightarrow{m \circ (\ )} X(Z)$$

is a left action of the group $G(Z)$.

We do not distinguish between the use of m for the group operation in G and for the action of G on X.

Equivalent definition. A *(left) action* is equivalent to the commutativity of the following two diagrams. The first expresses associativity of the action:

$$\begin{tikzcd}
G \times G \times X \arrow[r, "m \times \mathrm{id}"] \arrow[d, "\mathrm{id} \times m"'] & G \times X \arrow[d, "m"] \\
G \times X \arrow[r, "m"] & X.
\end{tikzcd}$$

The second says that the unit element acts as the identity:

$$\begin{tikzcd}
* \times X \arrow[r, "e \times \mathrm{id}"] \arrow[d, "pr_2"', "\wr"] & G \times X \arrow[dl, "m"] \\
X \ . &
\end{tikzcd}$$

Now we turn our attention to quotients.

Definition. A morphism $X \to Y$ is *G-invariant* if and only if for all $Z \in \mathrm{Ob}(\mathscr{C})$, the map

$$X(Z) \xrightarrow{f \circ ()} Y(Z)$$

is G-invariant.

Fact. The G-invariance is equivalent to requiring the diagram

$$\begin{tikzcd}
G \times X \arrow[r, "m"] \arrow[d, "pr_2"'] & X \arrow[d, "f"] \\
X \arrow[r, "f"] & Y
\end{tikzcd}$$

to be commutative.

Definition. A *categorical quotient* of X by G is a G-invariant morphism $X \xrightarrow{\pi} Y$, such that for all objects Z and for all G-invariant morphisms $X \xrightarrow{f} Z$, there exists a unique morphism $g : Y \to Z$ such that $f = g \circ \pi$.

Fact. If a categorical quotient exists, it is unique up to unique isomorphism.

We usually call Y the quotient, with the morphism π being tacitly included, although it is really π that matters.

The categorical quotient is the only meaningful concept of quotient in a general category, although it doesn't necessarily have all of the "nice" properties we would like. For examples see the following section.

Next, recall that a morphism $X \xrightarrow{f} Y$ is a *monomorphism* if for all $Z \in \mathrm{Ob}(\mathscr{C})$, the map

$$\mathrm{Hom}(Z, X) \xrightarrow{f \circ ()} \mathrm{Hom}(Z, Y)$$

is injective. The morphism f is an *epimorphism* if for all objects Z, the map

$$\mathrm{Hom}(Y, Z) \xrightarrow{() \circ f} \mathrm{Hom}(X, Z)$$

is injective.

Consider the morphism

$$\lambda : G \times X \xrightarrow{(m, pr_2)} X \times X,$$

which sends (g, x) to (gx, x). It is natural to call the action m *free* if λ is a monomorphism. If $X \xrightarrow{\pi} Y$ is a categorical quotient and if $\mathscr{C}$ has fiber products, there is a natural monomorphism $X \times_Y X \longrightarrow X \times X$, and one shows (exercise!) that λ factors through a unique morphism

$$\lambda' \colon G \times X \longrightarrow X \times_Y X.$$

Definition. Assume that the action is free. Then Y is called a *good quotient* if λ' is an isomorphism.

In the category of sets, the categorical quotient is simply the set of G-orbits. An action is free if and only if all stabilizers are trivial, and in this case the quotient is a good quotient.

§7 Quotients of schemes by finite group schemes, part I

We will assume that all schemes are affine of finite type over a field k. We are actually interested in finite schemes, but this added generality will not make things any more difficult for the time being.

Let $G = \operatorname{Spec} R$ act on $X = \operatorname{Spec} A$, i.e. $m : A \to R \otimes A$ is a unitary k-algebra homomorphism such that the duals of the above diagrams commute:

$$\begin{aligned}(m \otimes id) \circ m &= (id \otimes m) \circ m \\ (\epsilon \otimes 1) \circ m &= id.\end{aligned}$$

Then a function $a \in A = \operatorname{Hom}(X, \mathbb{A}^1_k)$ is G-invariant if and only if

$$m(a) = 1 \otimes a.$$

Set

$$B := A^G := \{a \in A \mid m(a) = 1 \otimes a\}$$

and $Y := \operatorname{Spec} B$. By direct application of the definitions one obtains this easy theorem:

Theorem. $X \to Y$ is a categorical quotient of X by G in the category of affine schemes over k.

Example. Let $G = \mathbb{G}_{m,k}$ act on $\mathbb{A}^n_k$ by $t(x_1, \ldots, x_n) := (tx_1, \ldots, tx_n)$. Then $A = k[X_1, \ldots, X_n]$ implies that $B = k$, so we might write "$\mathbb{A}^n_k/\mathbb{G}_{m,k}$"$=$ $\operatorname{Spec} k$. We use the quotes because this quotient does not have the nice properties we desire. For example, its dimension is smaller than expected. The reason for this is that the orbit structure for the action is "bad": The closure of every orbit contains the origin, and so every fiber of π contains the origin; hence π is constant and Y is a point. Thus this quotient is not good.

Example. Now take $U := \mathbb{G}_{m,k} \times \mathbb{A}^{n-1}_k$, which is a G-invariant open subset of $\mathbb{A}^n_k$. Write

$$U = \operatorname{Spec} k[x_1^{\pm 1}, x_2, \ldots, x_n] = \operatorname{Spec} k\Big[x_1^{\pm 1}, \frac{x_2}{x_1}, \ldots, \frac{x_n}{x_1}\Big].$$

Then "$U/\mathbb{G}_{m,k}$"$=$ $\operatorname{Spec} k[\frac{x_2}{x_1}, \ldots, \frac{x_n}{x_1}] \cong \mathbb{A}^{n-1}_k$ is a good quotient. In fact, the union of copies of such $\mathbb{A}^{n-1}_k$ make up $\mathbb{P}^{n-1}_k$, the categorical quotient of $\mathbb{A}^n_k \smallsetminus \{0\}$ by $\mathbb{G}_{m,k}$ in the category of all schemes. But although $U \subset \mathbb{A}^n_k$ is open, the induced morphism "$U/\mathbb{G}_{m,k}$"$\longrightarrow$"$\mathbb{A}^n_k/\mathbb{G}_{m,k}$" is no longer an open embedding!

From now on let G be finite, and let $\pi : X \longrightarrow Y$ be as above.

Theorem 7.1. (a) $\pi : X \longrightarrow Y$ is finite and surjective.

(b) The topological space underlying Y is the quotient of X by the equivalence relation induced by G.

(c) $\mathscr{O}_Y \xrightarrow{\sim} (\pi_* \mathscr{O}_X)^G$.

Proof. (See [Mu70] Section 12, Theorem 1) The main point is to show that every element $a \in A$ is integral over B. For this we need to find a monic equation satisfied by a. Define a norm map $N : A \to A$ by

$$N(a) := \mathrm{Nm}_{(R \otimes A)/A}(m(a)),$$

where we identify A with $1 \otimes A$. The right side is defined as the determinant over $1 \otimes A$ of the endomorphism "multiply by $m(a)$" of $R \otimes A$, where we use the fact that $\dim_k R$ is finite.

Lemma. $N(a) \in B$.

Sketch of the proof. To show that $N(a)$ is invariant under translation by $G(k)$, one notes simply that this translation induces an automorphism of A that is compatible with the comultiplication m. In general, one must do the same for translation by $G(Z)$ for all Z, or equivalently for translation by the universal element $\mathrm{id} \in G(G)$ after tensoring with another copy of R. The proof is written out in [Mu70], pp. 112-3.

Lemma. A is integral over B.

Proof. We apply the previous lemma to $X \times \mathbb{A}^1_k$ in place of X, where G acts trivially on $\mathbb{A}^1_k$. For its coordinate ring $A[T]$ we deduce

$$N(A[T]) \subset (A[T])^G = B[T].$$

For all $a \in A$, the element

$$\chi_a(T) := N(T - a) = \det_A\big((T - m(a) \cdot \mathrm{id}) | R \otimes A\big) \in B[T]$$

is a monic polynomial of degree $\dim_k R$. The identity map on A decomposes as

$$\begin{tikzcd} A \arrow[r, "m"] & R \otimes A \arrow[r, "\epsilon\otimes\mathrm{id}"] \arrow[loop below, "m(a)"] & A \arrow[loop below, "a"] \end{tikzcd},$$

where the self-maps denote multiplication by $m(a)$ and a, respectively. Thus

$$\chi_a(a) = \det_A\big((\mathrm{id} \otimes a - m(a)) \cdot \mathrm{id}\, | R \otimes A\big) = 0,$$

and so a is integral over B. □

Now we can prove (a). Suppose that A is generated by $a_1, \ldots, a_n$ as a k-algebra. Let $C \subset B$ be the subalgebra generated by the coefficients of all $\chi_{a_i}(T)$. Then A is integral over C. Thus A is of finite type as a C-module. Since C is a finitely generated k-algebra, it is noetherian. Therefore the C-submodule $B \subset A$ is itself of finite type as a C-module. This implies that B is a finitely generated k-algebra. Finally A is also a B-module of finite type. Since $B \subset A$, the morphism $X \to Y$ is thus finite surjective, as desired.

We turn to (b). For $x \in X$, the image (as a set) of the map $G \times \{x\} \xrightarrow{m} X$ is the G-orbit Gx of x. Using the commutative diagram for associativity, one can show that any two distinct orbits are disjoint. Let Gx and Gy be two disjoint orbits. After possibly interchanging x and y, none of the points in Gx specializes to a point in Gy. In this case there exists a function $a \in A$ that vanishes identically on Gx but is invertible on Gy. This in turn implies that $N(a) \in B$ vanishes on $\pi(x)$ but is invertible on $\pi(y)$. Thus π separates G-orbits. Since π is finite, hence closed, and is also continuous, this implies that Y has the quotient topology, proving (b).

To show (c) note that for any open subset $V \subset Y$ we have

$$(\pi_* \mathscr{O}_X)(V) = \mathscr{O}_X\bigl(\pi^{-1}(V)\bigr) = \mathrm{Hom}\bigl(\pi^{-1}(V), \mathbb{A}^1_k\bigr),$$

and a function f in this set is G-invariant if and only if $m(f) = 1 \otimes f$. Thus the subsheaf of all G-invariant functions $(\pi_* \mathscr{O}_X)^G$ is the kernel of the homomorphism of sheaves

$$\pi_* \mathscr{O}_X \to R \otimes_k \pi_* \mathscr{O}_X, \ f \mapsto m(f) - 1 \otimes f.$$

As these sheaves are coherent sheaves of $\mathscr{O}_Y$-modules, the kernel is the coherent sheaf associated to the kernel of the homomorphism of B-modules

$$A \longrightarrow R \otimes A, \ a \mapsto m(a) - 1 \otimes a.$$

By definition this kernel is B; hence its associated sheaf is $\mathscr{O}_Y$, as desired. □

Lecture 4

November 11, 2004
Notes by Nicolas Stalder

§8 Quotients of schemes by finite group schemes, part II

As before all schemes are supposed to be affine of finite type over a field k. Let $X = \operatorname{Spec} A$ be an affine scheme with an action of a finite group scheme $G = \operatorname{Spec} R$, and let $\pi : X \longrightarrow Y = \operatorname{Spec} A^G$ be the quotient map from the preceding lecture.

Definition. The *order* of G is

$$|G| := \dim_k R.$$

Note that a constant finite group scheme $\underline{\Gamma}_k$ has order $|\Gamma|$.

Definition. The action of G on X is called *free* if the morphism

$$\lambda : G \times X \xrightarrow{(m,pr_2)} X \times X$$

is a closed embedding.

Theorem 8.1. If the action of G on X is free, the quotient map $\pi : X \longrightarrow Y$ is faithfully flat everywhere of degree $|G|$, and the morphism λ above is an isomorphism.

Proof. For missing details, see [Mu70, pp. 115-6]. Set $B := A^G$. Since everything commutes with extension of k, we may assume that k is infinite. By the preceding lecture we may also localize at any prime ideal of B. Thus we may and do assume that B is local with infinite residue field. By assumption, the ring homomorphism

$$\begin{array}{rcl} \lambda : A \otimes_B A & \longrightarrow & R \otimes_k A \\ a \otimes a' & \longmapsto & m(a) \cdot (1 \otimes a') \end{array}$$

is surjective. We must prove that λ is an isomorphism, and that A is locally free over B of rank $n := |G|$.

We consider the source and the target of λ as A-modules via the action on the second factor. Note that $R \otimes_k A$ is a free A-module of rank n, and the surjectivity of λ means that $R \otimes_k A$ is generated as an A-module by $m(A)$. Note also that m is B-linear by the calculation

$$m(ab) = \lambda(ab \otimes 1) = \lambda(a \otimes b) = m(a) \cdot (1 \otimes b)$$

for all $a \in A$ and $b \in B$; hence $m(A)$ is a B-submodule of $R \otimes_k A$. We claim that $m(A)$ contains a basis of the free A-module $R \otimes_k A$. Indeed, since B is local it suffices to prove this after tensoring everything with the residue field of B, in which case it results from the following lemma:

Lemma 8.2. Consider an infinite field K, a finite dimensional K-algebra A, a finitely generated free A-module F, and a K-subspace $M \subset F$ that generates F as an A-module. Then M contains a basis of F over A.

Proof. We prove this by induction on the rank of F. The case $F = 0$ being trivial, suppose that $F \neq 0$ and choose a surjection $\varphi : F \twoheadrightarrow A$. The assumption implies that $\varphi(M)$ is not contained in any maximal ideal $\mathfrak{p} \subset A$. In other words $M \cap \varphi^{-1}(\mathfrak{p})$ is a proper subspace of M. Since K is infinite, it is well-known that M possesses an element m that does not lie in any of these finitely many subspaces. Then $\varphi(m)$ generates A, and so m generates a direct summand of F that is free of rank 1. By the induction hypothesis applied to the image of M in F/Am we can find elements of M whose images form a basis of F/Am over A. Thus these elements together with m form a basis of F over A, as desired. □

Now by the claim we can choose $a_1, \ldots, a_n \in A$ such that the elements $m(a_1), \ldots, m(a_n)$ are a basis of $R \otimes_k A$ over A. Thus we have an isomorphism of A-modules

$$A^{\oplus n} \longrightarrow R \otimes A, \qquad (\alpha_i)_i \mapsto \sum_{i=1}^{n} m(a_i) \cdot (1 \otimes \alpha_i). \tag{8.3}$$

Lemma 8.4. For all $a, \alpha_1, \ldots, \alpha_n \in A$:

$$m(a) = \sum_{i=1}^{n} m(a_i) \cdot (1 \otimes \alpha_i) \quad \Longleftrightarrow \quad \left(a = \sum_{i=1}^{n} a_i \alpha_i, \text{ and all } \alpha_i \in B \right)$$

Proof. The implication "$\Leftarrow$" follows directly from the definition of $A \otimes_B A$. For the implication "$\Rightarrow$", let us explain the idea in terms of points g of G and x of X. The left hand side means: $\forall g\, \forall x : \ a(gx) = \sum a_i(gx) \cdot \alpha_i(x)$. Because of the isomorphy (8.3), the $\alpha_i \in A$ are uniquely determined by this identity. Replacing x by hx and g by gh^{-1} has the sole effect of replacing $\alpha_i(x)$ by $\alpha_i(hx)$ in this identity. Letting h vary, we see that the α_i are translation invariant, i.e., that $\alpha_i \in A^G = B$. The equation $a = \sum a_i \alpha_i$ follows by evaluation at $g = 1$.

This argument must of course be done with Z-valued points, or directly with $\mathrm{id} \in G(G)$: see [Mu70, p. 116]. □

Now for all $a \in A$, there exist unique $\alpha_i \in A$ as on the left hand side of Lemma 8.4. So there exist unique $\alpha_i \in B$ as on the right hand side. This means that the a_i are a basis of A as a B-module, which is thus locally free of rank n, and so faithfully flat. Also, it follows that the $a_i \otimes 1$ are a basis of $A \otimes_B A$ as an A-module via the second factor, and since λ maps these elements to a basis of $R \otimes A$, we deduce that λ is an isomorphism. □

§9 Abelian categories

Let us recall some basic notions from the theory of categories (cf. also [We94]).

Definition. An *additive category* is a category $\mathcal{A}$ together with an abelian group structure on each $\mathrm{Hom}(X, Y)$, such that the composition map

$$\mathrm{Hom}(Y, Z) \times \mathrm{Hom}(X, Y) \longrightarrow \mathrm{Hom}(X, Z)$$

is bilinear, and such that there exist arbitrary finite direct sums. (In particular, there is a zero object.)

Let $X \xrightarrow{f} Y$ be a homomorphism in such an additive category $\mathcal{A}$.

Definition. (a) A homomorphism $K \xrightarrow{i} X$ is called a *kernel of* f, if for all $Z \in \mathcal{A}$, the following sequence is exact:

$$0 \longrightarrow \mathrm{Hom}(Z, K) \xrightarrow{i\circ(\ )} \mathrm{Hom}(Z, X) \xrightarrow{f\circ(\ )} \mathrm{Hom}(Z, Y).$$

(b) A homomorphism $Y \xrightarrow{p} C$ is called a *cokernel of* f, if for all $Z \in \mathcal{A}$, the following sequence is exact:

$$0 \longrightarrow \mathrm{Hom}(C, Z) \xrightarrow{(\ )\circ p} \mathrm{Hom}(Y, Z) \xrightarrow{(\ )\circ f} \mathrm{Hom}(X, Z).$$

Fact. If a kernel (resp. a cokernel) of f exists, it is unique up to unique isomorphism.

Notation. As usual, we will write $\ker f$ for the domain of the kernel of f, tacitly assuming the homomorphism i to be included. Same for $\operatorname{coker} f$.

Assuming that all kernels and cokernels exist, we can construct two further objects. The *coimage of* f is $\operatorname{coim} f := \operatorname{coker}(\ker f)$, whereas the *image of* f is $\operatorname{im} f := \ker(\operatorname{coker} f)$. Furthermore, using the universal properties of kernels and cokernels, we find a unique homomorphism $\operatorname{coim} f \longrightarrow \operatorname{im} f$, making the following diagram commutative:

$$\begin{tikzcd}
\ker f \arrow[r] & X \arrow[r, "f"] \arrow[d] & Y \arrow[r] & \operatorname{coker} f \\
 & \operatorname{coim} f \arrow[r, "\exists!"] & \operatorname{im} f \arrow[u] &
\end{tikzcd}$$

Definition. An additive category $\mathcal{A}$ is called an *abelian category*, if all kernels and cokernels exist and all canonical homomorphisms $\operatorname{coim} f \longrightarrow \operatorname{im} f$ are isomorphisms.

Examples. The category of abelian groups, the category of modules over a ring R, the category of sheaves of abelian groups on a topological space.

Fact. In an abelian category, all the usual diagram lemmas hold, for example the Snake Lemma, the 5-Lemma, and the 3×3-Lemma.

§10 The category of finite commutative group schemes

In this subsection, we work in the category of finite commutative group schemes over a field k. The aim is to show that this category is abelian.

Let $f : G \longrightarrow H$ be a homomorphism of finite commutative group schemes, and let $\phi : A \longleftarrow B$ be the corresponding homomorphism of Hopf algebras. It may be checked that $\phi(B)$ is again a Hopf algebra, and thus, setting $\overline{G} := \operatorname{Spec} \phi(B)$, we may factor f as

$$G \xrightarrow{p} \overline{G} \xrightarrow{i} H,$$

where $\overline{G}$ is again a finite commutative group scheme, and the morphisms are homomorphisms. Note also that i is a closed embedding, since $B \longrightarrow \phi(B)$ is surjective. Looking at the coordinate rings, we can see easily that i is a monomorphism and p is an epimorphism, in the categorical sense.

Proposition 10.1. The kernel of f exists and is a closed subgroup scheme of G.

Proof. If the kernel exists, then for all Z we have

$$\begin{aligned} \operatorname{Hom}(Z, \ker f) &= \ker\big(\operatorname{Hom}(Z,G) \longrightarrow \operatorname{Hom}(Z,H)\big) \\ &= \left\{ Z \longrightarrow G \;\middle|\; \begin{tikzcd} Z \arrow[r] \arrow[d] & G \arrow[d, "f"] \\ * \arrow[r, "\varepsilon"] & H \end{tikzcd} \text{ commutes} \right\} \\ &= \operatorname{Hom}(Z, G \times_H *) \end{aligned}$$

In fact, the fibre product $G \times_H *$, i.e., the scheme theoretic inverse image in G of the unit section of H, is a closed subgroup scheme of G. Tracing backwards, we see that it has the universal property of the kernel of f. □

Proposition 10.2. The quotient $\overline{H} := H/\overline{G}$, given by Theorem 7.1, carries a unique structure of group scheme such that $\pi : H \longrightarrow \overline{H}$ is a homomorphism. Moreover, π is an epimorphism, and $\overline{G} = \ker \pi$.

Proof. Let $\overline{G}$ act on H by left translation. This action is free, so Theorem 8.1 applies. To get the group structure, we consider the commutative diagram:

$$\begin{tikzcd}
H \times H \arrow[r, "m"] \arrow[d, "\pi\times\pi"] \arrow[dr] & H \arrow[d, "\pi"] \\
\overline{H} \times \overline{H} & \overline{H}
\end{tikzcd}$$

One checks that $(H \times H)/(\overline{G} \times \overline{G}) \cong \overline{H} \times \overline{H}$ naturally as schemes. By the universal property of this quotient, since the diagonal arrow is $\overline{G} \times \overline{G}$-invariant, we find a unique map $\overline{H} \times \overline{H} \xrightarrow{\overline{m}} \overline{H}$ making the above square commutative. Likewise, the morphisms $* \xrightarrow{\varepsilon} H \xrightarrow{i} H$ induce morphisms $* \xrightarrow{\overline{\varepsilon}} \overline{H} \xrightarrow{\overline{i}} \overline{H}$. Also, the uniqueness part of the universal property can be used every time to deduce that $\overline{m}$ satisfies the axioms of a commutative group structure for which π is a homomorphism. This proves the first sentence of this Proposition.

By the construction of $\overline{H}$ as a quotient, π is an epimorphism. Next, the morphism $\lambda : \overline{G} \times H \xrightarrow{(m,\mathrm{pr}_2)} H \times_{\overline{H}} H$ is an isomorphism by Theorem 8.1. Thus for all $h \in H(Z)$ we have

$$h \in \ker(\pi)(Z) \iff \pi(h) = e \iff \exists\, \overline{g} \in \overline{G}(Z) :\ h = \overline{g}e = \overline{g}$$

which is true if and only if $h \in \overline{G}(Z)$. Therefore, $\ker(\pi) = \overline{G}$. □

Proposition 10.3. (a) $\operatorname{coker} f$ exists and is isomorphic to $\overline{H}$.

(b) $\operatorname{im} f$ is isomorphic to $\overline{G}$.

Proof. Since $f = i \circ p$ and p is an epimorphism, we have $\operatorname{coker} f = \operatorname{coker} i$. Moreover $\operatorname{coker} i = \overline{H}$ by the universal property of the quotient, proving (a). Part (b) follows from (a) together with Proposition 10.2. □

Proposition 10.4. $\operatorname{coim} f$ is isomorphic to $\overline{G}$.

Proof. A direct proof in greater generality is given in [Mu70, p. 119]. In our case, it is easier to use Cartier duality. Since this is an antiequivalence of categories, it interchanges kernels and cokernels, and hence images and coimages. Also, clearly the diagram

$$\begin{tikzcd}
G \arrow[rr, "f"] \arrow[dr, "p"'] & & H \\
& \overline{G} \arrow[ur, "i"'] &
\end{tikzcd}$$

dualizes to the diagram

$$\begin{tikzcd}
G^* & & H^* \arrow[ll, "f^*"'] \arrow[dl, "i^*"] \\
& \overline{G}^* \arrow[ul, "p^*"] &
\end{tikzcd}$$

Thus $(\operatorname{coim} f)^* = \operatorname{im}(f^*) = \overline{G}^*$, and hence $\operatorname{coim} f = \overline{G}$. □

Combining these four propositions, we deduce:

Theorem 10.5. The category of finite commutative group schemes over a field k is abelian.

Theorem 10.6. (a) The following conditions are equivalent:

(i) f is a kernel.

(ii) f is a monomorphism.

(iii) $\ker f = 0$.

(iv) ϕ is surjective.

(v) f is a closed embedding.

(b) The following conditions are equivalent:

(i) f is a cokernel.

(ii) f is an epimorphism.

(iii) $\operatorname{coker} f = 0$.

(iv) ϕ is injective.

(v) f is faithfully flat.

Proof. For both items, the equivalences $(i) \iff (ii) \iff (iii)$ hold in all abelian categories. In (a), the implication $(iii) \implies (iv)$ results from Proposition 10.4, the equivalence $(iv) \iff (v)$ is clear, and the direction $(v) \implies (i)$ follows from Proposition 10.2. In (b), the implication $(i) \implies (v)$ results from Proposition 10.3 (a) and Theorem 8.1, the direction $(v) \implies (iv)$ is clear, and the implication $(iv) \implies (i)$ is a special case of Proposition 10.4. □

Theorem 10.7. For any short exact sequence of finite group schemes

$$0 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 0$$

we have $|G| = |G'| \cdot |G''|$.

Proof. Combine Proposition 10.3 (a) with the faithful flatness of Theorem 8.1. □

Theorem 10.8. For any field extension $k'|k$, the additive functor $G \mapsto G \times_k k'$ is exact and preserves group orders.

Proof. Base extension commutes with fiber products; hence by the proof of Proposition 10.1 also with kernels. It also commutes with Cartier duality, and so (cf. the proof of Proposition 10.4) also with cokernels. □

Note. Cartier duality is an exact functor, and we have used this already several times.

Note. Theorems 10.5, 10.6 and 10.8 hold more generally in the category of affine commutative group schemes over k, but are harder to prove. The main problem in general is still the construction of quotients. For this, see [DG70]. Also, the inclusion of categories is exact, i.e., kernels and cokernels in the smaller category remain the same in the bigger category.

Lecture 5

November 18, 2004
Notes by Alexander Caspar

§11 Galois descent

Let k'/k be a finite Galois extension of fields with Galois group Γ. Let $k'[\Gamma]$ denote the *twisted group ring of* Γ *over* k', that is, the set of formal linear combinations $\sum_{\gamma\in\Gamma} x'_\gamma[\gamma]$ for $x'_\gamma \in k'$, with coefficientwise addition and the multiplication $(x'[\gamma]) \cdot (y'[\delta]) = (x' \cdot \gamma(y'))[\gamma\delta]$. Note that giving a left module over $k'[\Gamma]$ is the same as giving a k'-vector space together with a semilinear action by Γ, that is, an additive action satisfying $\gamma(x'v') = \gamma(x')\gamma(v')$. Extension of scalars gives us a functor

$$\mathfrak{Vec}_k = \mathfrak{Mod}_k \longrightarrow \mathfrak{Mod}_{k'[\Gamma]},\ V \mapsto V \otimes_k k', \tag{11.1}$$

where $\gamma \in \Gamma$ acts on $V \otimes_k k'$ via $\mathrm{id} \otimes \gamma$.

Theorem 11.2. This functor is an equivalence of categories.

Proof. We prove that the functor $V' \mapsto (V')^\Gamma$ is a quasi-inverse. Indeed, the natural isomorphism

$$(V \otimes_k k')^\Gamma = V \otimes_k (k')^\Gamma = V \otimes_k k \cong V$$

shows that the composite $\mathfrak{Vec}_k \to \mathfrak{Mod}_{k'[\Gamma]} \to \mathfrak{Vec}_k$ is isomorphic to the identity. For the other way around we consider the natural $k'[\Gamma]$-linear homomorphism

$$(V')^\Gamma \otimes_k k' \longrightarrow V',\ v' \otimes x' \mapsto x'v'.$$

Claim. It is injective.

Proof. Assume that it is not, and let $\sum_{i=1}^r v'_i \otimes x'_i$ be a non-zero element in the kernel with r minimal. Then $r \geq 1$ and all v'_i and all x'_i are linearly independent over k. In particular $x'_1 \neq 0$, so after dividing by x'_1 we may assume that $x'_1 = 1$. Then for every $\gamma \in \Gamma$ the element

$$\sum_{i=2\ \text{(sic!)}}^r v'_i \otimes (\gamma(x'_i) - x'_i) \ = \ \gamma\Big(\sum_{i=1}^r v'_i \otimes x'_i\Big) - \sum_{i=1}^r v'_i \otimes x'_i$$

again lies in the kernel. Thus the minimality of r and the linear independence of the v'_i imply that $\gamma(x'_i) = x'_i$. Thus all $x'_i \in k$; hence $\sum_{i=1}^r v'_i \otimes x'_i = \big(\sum_{i=1}^r v'_i x'_i\big) \otimes 1 = 0$, and we get a contradiction. □

Consequence. $\dim_k(V')^\Gamma \leq \dim_{k'}(V')$.

Claim. It is bijective.

Proof. It is enough to prove this when $d := \dim_{k'} V'$ is finite, because every finite dimensional k'-subspace of V' is contained in a Γ-invariant one. Choose a basis $v_1', ..., v_d'$ of V' over k' and consider the surjective $k'[\Gamma]$-linear map

$$\varphi' : \ W' := k'[\Gamma]^{\oplus d} \to V', \ \Big(\sum_\gamma x'_{i,\gamma}[\gamma]\Big)_i \mapsto \sum_{i,\gamma} x'_{i,\gamma} \cdot \gamma(v_i').$$

Then the short exact sequence

$$0 \to \ker(\varphi') \to W' \to V' \to 0$$

induces a left exact sequence

$$0 \to \ker(\varphi')^\Gamma \to (W')^\Gamma \to (V')^\Gamma.$$

Now observe that $k'[\Gamma]$ is a free $k[\Gamma]$-module; hence W' is one. Therefore

$$\dim_k(W')^\Gamma = \frac{\dim_k W'}{|\Gamma|} = \frac{[k'/k] \cdot |\Gamma| \cdot d}{|\Gamma|} = d|\Gamma|.$$

On the other hand, the above Consequence applied to $\ker(\varphi')$ shows that

$$\dim_k \ker(\varphi')^\Gamma \leq \dim_{k'} \ker(\varphi') = d(|\Gamma| - 1).$$

Thus the left exactness implies that $\dim_k(V')^\Gamma \geq d|\Gamma| - d(|\Gamma| - 1) = d$. This plus the injectivity shows the bijectivity. □

This finishes the proof of Theorem 11.2. □

Note. The functor (11.1), and hence the equivalence in Theorem 11.2, is compatible with the tensor product (over k, respectively over k'). Therefore, it extends to an equivalence for vector spaces with any additional multilinear structures, such as that of an algebra or a Hopf-algebra (over k, resp. k'), together with the appropriate homomorphisms. In particular we deduce:

Theorem 11.3. The base change functor $X \mapsto X \times_k k'$ induces an equivalence from the category of affine schemes over k to the category of affine schemes over k' together with a covering action by Γ. The same holds for the categories of affine group schemes, or of finite group schemes.

Note. By going to the limit over finite Galois extensions we deduce the same for any infinite Galois extension k'/k with profinite Galois group Γ, provided that the action of Γ on an affine scheme over k' is continuous, in the sense that the stabilizer of every regular function is an open subgroup of Γ.

§12 Étale group schemes

Let k^{sep} denote a separable closure of k.

Proposition 12.1. A finite group scheme G is étale iff $G_{k^{\text{sep}}}$ is constant.

Proof. By definition a morphism of schemes is étale if and only if it is smooth of relative dimension zero, i.e., if it is flat of finite type and the sheaf of relative differentials vanishes. Since k is a field, G is automatically flat over k; hence it is étale if and only if $\Omega_{G/k} = 0$. As the formation of $\Omega_{G/k}$ is invariant under base change, this is equivalent to $\Omega_{G_{k^{\text{sep}}}/k^{\text{sep}}} = 0$. This in turn means that $G_{k^{\text{sep}}}$ is reduced with all residue fields separable over k^{sep}. But k^{sep} is separably closed; hence it is equivalent to saying that $G_{k^{\text{sep}}} \cong \coprod \operatorname{Spec} k^{\text{sep}}$ as a scheme. The group structure on $G_{k^{\text{sep}}}$ then corresponds to the group structure on $G(k^{\text{sep}})$ as in §5, yielding a natural isomorphism

$$G_{k^{\text{sep}}} \cong \underline{G(k^{\text{sep}})}_{k^{\text{sep}}}.$$

□

Theorem 12.2. The functor $G \mapsto G(k^{\text{sep}})$ defines an equivalence from the category of finite étale group schemes over k to the category of continuous finite $\mathbb{Z}[\operatorname{Gal}(k^{\text{sep}}/k)]$-modules.

Proof. By the remark after Theorem 11.3 the base change functor $G \mapsto G_{k^{\text{sep}}}$ induces an equivalence from the category of étale finite group schemes over k to the category of étale finite group schemes over k^{sep} together with a continuous covering action by $\operatorname{Gal}(k^{\text{sep}}/k)$. Proposition 12.1 implies that the latter is equivalent to the category of continuous finite Galois-modules. □

§13 The tangent space

Let $G = \operatorname{Spec} A$ be a finite commutative group scheme over k, and denote by $T_{G,0}$ the tangent space at the unit element 0.

Proposition 13.1. There is a natural isomorphism of k-vector spaces

$$T_{G,0} \cong \operatorname{Hom}(G^*, \mathbb{G}_{a,k}),$$

where k acts on the right hand side through $\mathbb{G}_{a,k}$.

Proof. The tangent space $T_{G,0}$ is naturally isomorphic to the kernel of the restriction map

$$G(\operatorname{Spec}(k[t]/(t^2)) \longrightarrow G(\operatorname{Spec} k).$$

This is the set of k-algebra homomorphisms $A \to k[t]/(t^2) \cong k \oplus t\,k$ whose first component is the counit ϵ. Such a homomorphism has the form $\varphi = \epsilon + t\lambda$ for a homomorphism of k-vector spaces $\lambda\colon A \to k$, and the relations $\varphi(ab) = \varphi(a)\varphi(b)$ and $\varphi(e(1)) = 1$ making φ a homomorphism of k-algebras translate into the relations $\lambda(ab) = \lambda(a)\epsilon(b) + \epsilon(a)\lambda(b)$ and $\lambda(e(1)) = 0$. In dual terms we get the set of $\lambda \in A^*$ such that $\mu^*(\lambda) = \lambda \otimes \epsilon^*(1) + \epsilon^*(1) \otimes \lambda$ and $e^*(\lambda) = 0$. But giving an element $\lambda \in A^*$ is equivalent to giving the homomorphism of k-algebras $k[T] \to A^*$ sending T to λ, which in turn corresponds to a morphism $\ell : G^* = \operatorname{Spec} A^* \to \mathbb{A}^1_k$. The first condition on λ then amounts to saying that ℓ is a group homomorphism, and the second condition to $\ell(0) = 0$. But the latter is already a consequence of the former. This proves the bijectivity; the k-linearity is left to the reader. □

Theorem 13.2. All finite commutative group schemes over a field of characteristic zero are étale.

Proof. Without loss of generality we can assume that k is algebraically closed. Then the translation action of $G(k)$ on G is transitive. Therefore it is enough to prove étaleness at 0, that is, $T_{G,0} = 0$. By Proposition 13.1 we must show that any homomorphism $G^* \to \mathbb{G}_{a,k}$ vanishes. Since its image is a finite subgroup scheme of $\mathbb{G}_{a,k}$, it suffices to show that any finite subgroup scheme $H \subset \mathbb{G}_{a,k}$ vanishes.

For any such H, the group $H(k)$ is a finite subgroup of $\mathbb{G}_{a,k}(k)$, the additive group of k. Since this is a $\mathbb{Q}$-vector space, it contains no non-zero finite subgroup; hence $H(k) = 0$. Thus H is purely local, i.e. $H = \operatorname{Spec} k[X]/(X^n)$ for some $n \geq 1$. The fact that H is a subgroup scheme means that the comultiplication $X \mapsto X \otimes 1 + 1 \otimes X$ on $k[X]$ induces a homomorphism $k[X]/(X^n) \longrightarrow k[X]/(X^n) \otimes_k k[X]/(X^n)$. This means that

$$(X \otimes 1 + 1 \otimes X)^n \;=\; \sum_{m=1}^{n} \tbinom{n}{m} \cdot X^m \otimes X^{n-m} \;\in\; (X^n \otimes 1, 1 \otimes X^n).$$

Here all binomial coefficients are non-zero in k, because k has characteristic zero. Thus $n = 1$ and hence $H = 0$, as desired. □

Proposition 13.3. For any field k of characteristic $p > 0$, the finite group scheme $\boldsymbol{\alpha}_{p,k} = \operatorname{Spec} k[X]/(X^p) \subset \mathbb{G}_{a,k}$ is simple.

Proof. Any proper subgroup scheme $H \subset \boldsymbol{\alpha}_{p,k}$ has the form $\operatorname{Spec} k[X]/(X^n)$ for some $n < p$. Thus all binomial coefficients $\binom{n}{m}$ are non-zero in k for $0 < m < n$, so as in the preceding proof we deduce that $n = 1$ and $H = 0$. □

Lecture 6

November 25, 2004
Notes by Charles Mitchell

§14 Frobenius and Verschiebung

Definition. The *absolute Frobenius morphism* $\sigma_X : X \to X$ of a scheme over $\mathbb{F}_p$ is the identity on points and the map $a \mapsto a^p$ on sections. Note that this is functorial: for all morphisms $\varphi : X \to Y$ of schemes over $\mathbb{F}_p$, the diagram

$$\begin{tikzcd}
X \arrow[r, "\varphi"] \arrow[d, "\sigma_X"'] & Y \arrow[d, "\sigma_Y"'] \\
X \arrow[r, "\varphi"] & Y
\end{tikzcd}$$

commutes. Also, absolute Frobenius is compatible with products in the sense that $\sigma_{X\times Y} = \sigma_X \times \sigma_Y$.

For the following we fix a field k of characteristic p. All tensor products and fiber products are taken over k, unless explicitly stated.

Definition. For any scheme X over $\operatorname{Spec} k$ define $X^{(p)}$ as the fiber product and F_X as the induced morphism in the following commutative diagram:

$$\begin{tikzcd}
X \arrow[dr, dashed, "F_X"] \arrow[drr, bend left, "\sigma_X"] \arrow[ddr, bend right] & & \\
& X^{(p)} \arrow[r] \arrow[d] & X \arrow[d] \\
& \operatorname{Spec} k \arrow[r, "\sigma_{\operatorname{Spec} k}"] & \operatorname{Spec} k
\end{tikzcd}$$

F_X is called the *relative Frobenius morphism* of X over $\operatorname{Spec} k$.

Proposition 14.1. (a) F_X is functorial in X: for all morphisms $\varphi : X \to Y$ of schemes over k, the following diagram commutes:

$$\begin{tikzcd}
X \arrow[r, "F_X"] \arrow[d, "\varphi"] & X^{(p)} = X \otimes_{k,\sigma} k \arrow[d, "\varphi^{(p)} = \varphi\otimes id"] \\
Y \arrow[r, "F_Y"'] & Y^{(p)} = Y \otimes_{k,\sigma} k
\end{tikzcd}$$

(b) F_X is compatible with products, i.e., the following diagram commutes:

$$\begin{tikzcd}
X \times_k Y \arrow[r, "F_X \times F_Y"] \arrow[dr, "F_{X\times Y}"'] & X^{(p)} \times_k Y^{(p)} \arrow[d, phantom, "\wr\|"] \\
& (X \times_k Y)^{(p)}
\end{tikzcd}$$

(c) F_X is compatible with base extensions $k \hookrightarrow k'$, i.e., the following diagram commutes:

$$\begin{tikzcd}
X_{k'} \arrow[r, "F_{X_{k'}}"] \arrow[dr, "(F_X)_{k'}"'] & (X_{k'})^{(p)} \arrow[d, phantom, "\wr\|"] \\
& (X^{(p)})_{k'}
\end{tikzcd}$$

Corollary 14.2. For any group scheme G over k, the morphism $F_G : G \to G^{(p)}$ is a homomorphism.

Now let G be a finite commutative group scheme over k. Then the Frobenius morphism of G^* induces a homomorphism $F_{G^*} : G^* \to (G^*)^{(p)} \cong (G^{(p)})^*$.

Definition. The homomorphism $V_G : G^{(p)} \to G$ dual to F_{G^*} is called the *Verschiebung of* G.

Frobenius and Verschiebung are thus two morphisms going in opposite directions. It seems natural to attempt

(a) to extend the definition of the Verschiebung to arbitrary affine group schemes, and

(b) to determine the composites $V_G \circ F_G$ and $F_G \circ V_G$.

To achieve (a), we write $G = \operatorname{Spec} A$ and let $\operatorname{Sym}^p A$ denote the p-th symmetric power of A over k. We can then expand the definition of F_G on coordinate rings as the composite in the top line of the commutative diagram

$$\begin{tikzcd}
x \cdot a^p & {[x(a \otimes \cdots \otimes a)]} \arrow[l, mapsto] & a \otimes x \arrow[l, mapsto] \\
A & \operatorname{Sym}^p A \arrow[l, two heads] & A \otimes_{k,\sigma} k \arrow[l, hook'] \\
& A^{\otimes p} \arrow[u, two heads] \arrow[ul, two heads, "\mathrm{mult}"]
\end{tikzcd}$$

We claim that the formula on the upper right defines a k-linear homomorphism. Indeed, only the additivity needs to be checked. But the mixed terms in the expansion

$$x(a+b) \otimes \cdots \otimes (a+b) = x(a \otimes \cdots \otimes a) + x(b \otimes \cdots \otimes b) + \text{mixed terms}$$

can be grouped into orbits under the symmetric group S_p, and since the length of each orbit is a multiple of p, the corresponding sums vanish in $\operatorname{Sym}^p A$, proving the claim.

If A is finite-dimensional over k, we can take the above diagram for A^* instead of A and dualize it over k to represent Verschiebung as the composite in a commutative diagram

$$\begin{tikzcd}
A \arrow[r, hook] \arrow[dr, hook, "\text{comult}"'] & (A^{\otimes p})^{S_p} \arrow[r, two heads, "\lambda_A"] \arrow[d, hook] & A \otimes_{k,\sigma} k \\
& A^{\otimes p} &
\end{tikzcd}$$

Here λ_A is the unique k-linear map taking any element $x \cdot (a \otimes \cdots \otimes a)$ to $a \otimes x$. One easily verifies that this map exists for any k-vector space A, so the above diagram can be constructed for any affine commutative group scheme $G = \operatorname{Spec} A$. It can be checked that the composite map $A \to A \otimes_{k,\sigma} k$ is a homomorphism of k-algebras compatible with the comultiplication. It therefore corresponds to a homomorphism of group schemes $V_G : G^{(p)} \to G$.

Definition. This V_G is the *Verschiebung* for general G.

Proposition 14.3. (a) V_G is functorial in G, i.e., the following diagram commutes:

$$\begin{tikzcd}
G^{(p)} \arrow[r, "V_G"] \arrow[d, "\varphi^{(p)}"'] & G \arrow[d, "\varphi"] \\
H^{(p)} \arrow[r, "V_H"'] & H
\end{tikzcd}$$

(b) V_G is compatible with products, i.e., the following diagram commutes:

$$\begin{tikzcd}
(G \times H)^{(p)} \arrow[r, phantom, "\cong"] \arrow[dr, "V_{G\times H}"'] & G^{(p)} \times H^{(p)} \arrow[d, "V_G \times V_H"] \\
& G \times H
\end{tikzcd}$$

(c) V_G is compatible with base extensions, i.e., the following diagram commutes:

$$\begin{tikzcd}
(G_{k'})^{(p)} \arrow[r, phantom, "\cong"] \arrow[dr, "V_{(G_{k'})}"'] & (G^{(p)})_{k'} \arrow[d, "(V_G)_{k'}"] \\
& G
\end{tikzcd}$$

We are now in a position to tackle the above question (b).

Theorem 14.4. For any affine commutative group scheme G,

(a) $V_G \circ F_G = p \cdot \mathrm{id}_G$,

(b) $F_G \circ V_G = p \cdot \mathrm{id}_{G^{(p)}}$.

Proof. (a) By the above constructions, Frobenius and Verschiebung correspond to the maps F_A and V_A in the following diagram:

$$\begin{tikzcd}
A \arrow[r] \arrow[rr, bend left, "V_A"] \arrow[dr, "\text{comult}"'] & (A^{\otimes p})^{S_p} \arrow[r, "\lambda_A"] \arrow[d, hook] & A \otimes_{\sigma,k} k \arrow[d, "F_A"] \\
& A^{\otimes p} \arrow[r, "\text{mult}"'] & A
\end{tikzcd}$$

The definition of λ_A implies that the right hand square commutes. In terms of group schemes, this diagram becomes

$$\begin{tikzcd}
G & & G^{(p)} \arrow[ll, "V_G"'] \\
& G^{\times p} \arrow[ul, "\text{mult}"] & G \arrow[l, "\text{diag}"] \arrow[u, "F_G"'] \arrow[ull, "p\cdot\mathrm{id}_G"]
\end{tikzcd}$$

where the composite is by definition $p \cdot \mathrm{id}_G$.

(b) As Verschiebung is compatible with base change, we have $(V_G)^{(p)} = V_{G^{(p)}}$. The functoriality of Frobenius thus implies that the diagram

$$\begin{tikzcd}
G^{(p)} \arrow[r, "F_{G^{(p)}}"] \arrow[d, "V_G"'] & G^{(p^2)} \arrow[d, "(V_G)^{(p)} = V_{G^{(p)}}"] \\
G \arrow[r, "F_G"'] & G^{(p)}
\end{tikzcd}$$

commutes; its diagonal is already known by (a) to be $p \cdot \mathrm{id}_{G^{(p)}}$. □

Examples.

- F_G and V_G are zero for $G = \alpha_{p,k}$.
- F_G is zero and V_G an isomorphism for $G = \mu_{p,k}$.
- F_G is an isomorphism for $G = \underline{\mathbb{Z}/n\mathbb{Z}}_k$.

§15 The canonical decomposition

Let G be a finite commutative group scheme over k.

Proposition 15.1. The following are equivalent:

(i) $G_{k^{\mathrm{sep}}}$ is constant.

(ii) G is étale.

(iii) F_G is an isomorphism.

Proof. The equivalence (i) $\Leftrightarrow$ (ii) has already been shown in Proposition 12.1. To show (ii) $\Leftrightarrow$ (iii), note that the group scheme G is étale iff its tangent space at 0 is trivial. As the absolute and relative Frobenius morphisms are zero on this tangent space, the étaleness of G is equivalent to F_G being an infinitesimal isomorphism, which — as F_G is a bijection on points — is in turn equivalent to F_G being an isomorphism as such. $\square$

Dualizing Proposition 15.1 yields:

Proposition 15.2. The following are equivalent:

(i) $G_{k^{\mathrm{sep}}}$ is a direct sum of $\mu_{n_i,k^{\mathrm{sep}}}$ for suitable n_i.

(ii) G^* is étale.

(iii) V_G is an isomorphism.

Proposition 15.3. The connected component G^0 of the zero section in G is a closed subgroup scheme, and G/G^0 is étale.

Proof. Since the unique point in G^0 is defined over the base field k, the product $G^0 \times G^0$ over k is connected. It is also open in $G \times G$; therefore it is the connected component of zero in $G \times G$. Thus the restriction to $G^0 \times G^0$ of the multiplication morphism $G \times G \to G$ factors through G^0, showing that G^0 is a (closed) subgroup scheme of G.

To show that G/G^0 is étale, we may assume without loss of generality that k is algebraically closed. Then G decomposes as $\coprod_{g \in G(k)} G^0 \cdot g$ and we can infer that

$$G/G^0 = \coprod_{g \in G(k)} \operatorname{Spec} k,$$

which is the constant group scheme $\underline{G(k)}_k$, and therefore étale. $\square$

From now on we impose the standing

Assumption. The field k is perfect.

Proposition 15.4. The reduced closed subscheme $G^{\text{red}} \subset G$ with the same support as G is a closed subgroup scheme, and the map $(g, g') \mapsto g + g'$ defines an isomorphism $G^0 \oplus G^{\text{red}} \xrightarrow{\sim} G$.

Proof. As k is perfect, all residue fields of G^{red} are separable over k, implying that $G^{\text{red}} \times G^{\text{red}} \subset G \times G$ is again reduced. Therefore the restriction to $G^{\text{red}} \times G^{\text{red}}$ of the multiplication morphism $G \times G \to G$ factors through G^{red}, showing that G^{red} is a (closed) subgroup scheme of G.

To prove the second assertion it suffices to show that the morphism $G^{\text{red}} \to G/G^0$ is an isomorphism. Since the formation of both sides is compatible with base extension, we may assume that k is separably closed. Then $G^{\text{red}} \to G/G^0$ is a bijective homomorphism between constant group schemes and hence an isomorphism. □

Example. Regard an inseparable field extension $k' = k(\sqrt[p]{u}) \supsetneqq k$. Set $G_i := \operatorname{Spec} k[t]/(t^p - u^i)$ and define a group operation on $G := \coprod_{i=0}^{p-1} G_i$ by

$$\begin{aligned} G_i \times G_j &\to G_{i+j}, & (t,t') &\mapsto tt' & &\text{if } i+j<p, \\ G_i \times G_j &\to G_{i+j-p}, & (t,t') &\mapsto tt'/u & &\text{if } i+j \geq p. \end{aligned}$$

Then $G^0 = G_0 \cong \boldsymbol{\mu}_{p,k}$, and we have a short exact sequence

$$0 \to \boldsymbol{\mu}_{p,k} \to G \to \underline{\mathbb{F}_p}_k \to 0.$$

This sequence is non-split, because $G_i \cong \operatorname{Spec} k' \not\cong G_0$ for $i \neq 0$.

Example. With k'/k as above, set $G_i := \operatorname{Spec} k[t]/(t^p - iu)$ and define a group operation on $G := \coprod_{i=0}^{p-1} G_i$ by

$$G_i \times G_j \to G_{i+j},\ (t,t') \mapsto t + t'.$$

Then $G^0 = G_0 \cong \boldsymbol{\alpha}_{p,k}$, and we have a short exact sequence

$$0 \to \boldsymbol{\alpha}_{p,k} \to G \to \underline{\mathbb{F}_p}_k \to 0.$$

This sequence is non-split, because $G_i \cong \operatorname{Spec} k' \not\cong G_0$ for $i \neq 0$.

Definition. A finite commutative group scheme G is called *local* if $G = G^0$ and *reduced* if $G = G^{\text{red}}$. It is called *of x-y type* if G is x and G^* is y.

Theorem 15.5. There is a unique and functorial decomposition of G as

$$G = G_{rr} \oplus G_{r\ell} \oplus G_{\ell r} \oplus G_{\ell\ell}$$

where the direct summands are of reduced-reduced, reduced-local, local-reduced, and local-local type, respectively.

Proof. The decomposition $G = G^0 \oplus G^{\mathrm{red}}$ is functorial in G, as both G^0 and G^{red} are. Applying this functoriality in turn to G^* and dualizing back using the equality $(G \oplus H)^* = G^* \oplus H^*$ completes the proof. □

Remark. The functoriality includes the fact that any homomorphism between groups of different types is zero. The decomposition is also invariant under base extension.

Definition. The *n-th iterates* of Frobenius and Verschiebung are the composite homomorphisms

$$\begin{aligned} F_G^n : \;\; & G \xrightarrow{F_G} G^{(p)} \xrightarrow{F_{G^{(p)}}} \ldots \longrightarrow G^{(p^n)}, \\ V_G^n : \;\; & G^{(p^n)} \longrightarrow \ldots \xrightarrow{V_{G^{(p)}}} G^{(p)} \xrightarrow{V_G} G. \end{aligned}$$

We call F_G *nilpotent* if $F_G^n = 0$ for some $n \geq 0$, and similarly for V_G.

Proposition 15.6. We have the following equivalences:

(a) G is reduced-reduced $\Leftrightarrow$ both F_G and V_G are isomorphisms.

(b) G is reduced-local $\Leftrightarrow$ F_G is an isomorphism and V_G is nilpotent.

(c) G is local-reduced $\Leftrightarrow$ F_G is nilpotent and V_G is an isomorphism.

(d) G is local-local $\Leftrightarrow$ both F_G and V_G are nilpotent.

Proof. Consider the decomposition $G = G^0 \oplus G^{\mathrm{red}}$ from Proposition 15.4. Since the maximal ideal at the unit element of G^0 is nilpotent, it is annihilated by some power of the absolute Frobenius, and hence by the same power of the relative Frobenius. Thus Frobenius is nilpotent on G^0, while by Proposition 15.1 it is an isomorphism on G^{red}. From this it follows formally that G is reduced, resp. local, if and only if F_G is an isomorphism, resp. nilpotent. Applying this to G^* as well finishes the proof. □

Note. By §12 we already understand G_{rr} and $G_{r\ell}$, and by duality also $G_{\ell r}$. So the goal now is to understand $G_{\ell\ell}$. The problem is the complicated extension structure of such groups!

§16 Split local-local group schemes

(This section was actually presented on December 16, but logically belongs here.)

Proposition 16.1. There is a natural isomorphism $\mathrm{End}(\boldsymbol{\alpha}_{p,k}) \cong k$.

Proof. There are natural homomorphisms $k \to \mathrm{End}(\boldsymbol{\alpha}_{p,k}) \to k$, the first representing the multiplication action of k, the second the action on the tangent space of $\boldsymbol{\alpha}_{p,k}$. Clearly their composite is the identity, so the second map is surjective. On the other hand, consider an endomorphism $\varphi \in \mathrm{End}(\boldsymbol{\alpha}_{p,k})$ with $d\varphi = 0$. Then $\ker\varphi$ has a non-zero tangent space, so it is a non-zero subgroup scheme of $\boldsymbol{\alpha}_{p,k}$. Since $\boldsymbol{\alpha}_{p,k}$ is simple by Proposition 13.3, it follows that $\ker\varphi = \boldsymbol{\alpha}_{p,k}$ and hence $\varphi = 0$. This shows that the second map is injective. We conclude that the two maps are mutually inverse isomorphisms. □

Proposition 16.2. Any finite commutative group scheme G with $F_G = 0$ and $V_G = 0$ is isomorphic to a direct sum of copies of $\boldsymbol{\alpha}_{p,k}$.

Proof. In fact we will prove that $G \cong \boldsymbol{\alpha}_{p,k}^{\oplus n}$ for $n := \dim_k T_{G,0}$. For this write $G = \mathrm{Spec}\, A$ and $A = k \oplus I$, where I is the augmentation ideal. Then the isomorphy $T_{G,0} \cong (I/I^2)^*$ implies that I is generated by n elements. On the other hand, since $F_G = 0$, we have $\xi^p = 0$ for every $\xi \in I$. In particular I is nilpotent; hence its n generators generate A as a k-algebra. (This is a standard result from commutative algebra, and a nice exercise!) Write $A = k[X_1, \ldots, X_n]/J$ and $I = (X_1, \ldots, X_n)/J$ for some ideal J. Then $X_i^p \in J$ for all $1 \leq i \leq n$, and therefore A is a quotient of $k[X_1, \ldots, X_n]/(X_1^p, \ldots, X_n^p)$. In particular $|G| = \dim_k A \leq p^n$.

Next note that for any homomorphism $\varphi\colon G^* \to \mathbb{G}_{a,k}$, the functoriality of Frobenius and the assumption $V_G = 0$ imply that

$$F_{\mathbb{G}_{a,k}} \circ \varphi \overset{14.1}{=} \varphi^{(p)} \circ F_{G^*} = \varphi^{(p)} \circ (V_G)^* = 0.$$

Thus φ factors through the kernel of $F_{\mathbb{G}_{a,k}}$, that is, through $\boldsymbol{\alpha}_{p,k}$. Taking Proposition 13.1 into account, we find that

$$n = \dim_k T_{G,0} = \dim_k \mathrm{Hom}(G^*, \mathbb{G}_{a,k}) = \dim_k \mathrm{Hom}(G^*, \boldsymbol{\alpha}_{p,k}).$$

We claim that there exists an epimorphism $G^* \twoheadrightarrow \boldsymbol{\alpha}_{p,k}^{\oplus n}$. Indeed, suppose that an epimorphism $\psi : G^* \twoheadrightarrow \boldsymbol{\alpha}_{p,k}^{\oplus i}$ has been constructed for some $0 \leq i < n$. Then the induced linear map $k^i \cong \mathrm{Hom}(\boldsymbol{\alpha}_{p,k}^{\oplus i}, \boldsymbol{\alpha}_{p,k}) \hookrightarrow \mathrm{Hom}(G^*, \boldsymbol{\alpha}_{p,k})$ is a proper embedding. Any homomorphism $\varphi : G^* \to \boldsymbol{\alpha}_{p,k}$ not in the image has a non-trivial restriction to $\ker\psi$, and since $\boldsymbol{\alpha}_{p,k}$ is simple, the combined homomorphism $(\psi, \varphi) : G^* \to \boldsymbol{\alpha}_{p,k}^{\oplus i} \oplus \boldsymbol{\alpha}_{p,k}$ is again an epimorphism. Thus the claim follows by induction on i. Finally, by Cartier duality the claim yields a monomorphism $\boldsymbol{\alpha}_{p,k}^{\oplus n} \hookrightarrow G$. By the above inequality $|G| \leq p^n$, this monomorphism must be an isomorphism, finishing the proof. □

Theorem 16.3. Every simple finite commutative group scheme of local-local type is isomorphic to $\boldsymbol{\alpha}_{p,k}$.

Proof. Combine Propositions 15.6 (d) and 16.2. □

Lecture 7

December 2, 2004
Notes by Ivo Dell'Ambrogio

§17 Group orders

Recall from Theorem 15.5 that every finite commutative group scheme possesses a unique and functorial decomposition

$$G = G_{rr} \oplus G_{r\ell} \oplus G_{\ell r} \oplus G_{\ell\ell}$$

where the direct summands are of reduced-reduced, reduced-local, local-reduced, and local-local type, respectively.

Theorem 17.1. (a) The group orders in the above decomposition are, respectively: prime to p for G_{rr}, and a power of p for $G_{r\ell}$, $G_{\ell r}$ and $G_{\ell\ell}$.

(b) ("Lagrange") $|G| \cdot \mathrm{id}_G = 0$.

Proof. The statements are invariant under base extension; hence we may assume that k is separably closed. Recall that the group order is multiplicative in any short exact sequence $0 \to G' \to G \to G'' \to 0$. Similarly, if the Lagrange equation holds for G' and G'', one easily shows that it also holds for G. Therefore both statements reduce to the case of simple G.

If G is also reduced, then it must be the constant group scheme associated to a simple finite commutative group, and therefore $G \cong \underline{\mathbb{Z}/\ell\mathbb{Z}}$ for a prime ℓ. Its Cartier dual is then $G^* \cong \boldsymbol{\mu}_{\ell,k}$, which is reduced if and only if $\ell \neq p$. This determines the simple reduced group schemes up to isomorphism, and by Cartier duality also those of local-reduced type. Taking Theorem 16.3 into account, we deduce that the simple finite commutative group schemes over a separably closed field up to isomorphism are the following:

Type	Group	Order
reduced-reduced	$\underline{\mathbb{Z}/\ell\mathbb{Z}}$	$\ell \neq p$
reduced-local	$\underline{\mathbb{Z}/p\mathbb{Z}}$	p
local-reduced	$\boldsymbol{\mu}_{p,k}$	p
local-local	$\boldsymbol{\alpha}_{p,k}$	p

In each case G is annihilated by its order, and the proposition follows. □

§18 Motivation for Witt vectors

Let R be a complete discrete valuation ring with quotient field of characteristic zero, maximal ideal pR, and residue field $k = R/pR$. Then we can write all elements of R as power series in p. In fact, for any given (set theoretic) section $s : k \to R$ we have a bijection

$$\prod_{n=0}^{\infty} k \longrightarrow R, \quad (x_n) \longmapsto \sum_{n=0}^{\infty} s(x_n) \cdot p^n.$$

A natural problem is then to describe the ring structure of R in terms of the coefficients x_n. This of course depends on the choice of s, so the question is: How can this be done canonically? For the following we shall again assume that k is a perfect field.

Proposition 18.1. Let R be a complete noetherian local ring with perfect residue field k of characteristic p and maximal ideal $\mathfrak{m}$. Then there exists a unique section $i : k \to R$ with the equivalent properties:

(a) $i(xy) = i(x)i(y)$ for all $x, y \in k$,

(b) $i(x) = \lim_{n\to\infty} s(x^{p^{-n}})^{p^n}$ for any section s and any $x \in k$.

The image $i(x)$ is called the *Teichmüller representative of* x.

Proof. The main point is to show that the limit in (b) is well-defined. First notice that for all $n \geq 1$ and $x, y \in R$ we have

$$x \equiv y \bmod \mathfrak{m}^n \quad \Rightarrow \quad x^p \equiv y^p \bmod \mathfrak{m}^{n+1}.$$

This is because with $z := y - x \in \mathfrak{m}^n$ the binomial formula implies that

$$y^p - x^p = (z + x)^p - x^p \in (z^p, pz) \subset \mathfrak{m}^{n+1}.$$

By induction on n we deduce for all $n \geq 0$ and $x, y \in R$ that

$$x \equiv y \bmod \mathfrak{m} \quad \Rightarrow \quad x^{p^n} \equiv y^{p^n} \bmod \mathfrak{m}^{n+1}.$$

Note also that the assumptions imply that $R \cong \varprojlim_n R/\mathfrak{m}^n$.

Now consider any section $s \colon k \to R$. Then for all $x \in k$ and $n \geq 1$ we have $s(x^{p^{-n}})^p \equiv s(x^{p^{1-n}}) \bmod \mathfrak{m}$ and therefore $s(x^{p^{-n}})^{p^n} \equiv s(x^{p^{1-n}})^{p^{n-1}} \bmod \mathfrak{m}^n$. This shows that the sequence in (b) converges. If $s' : k \to R$ is another section, we have $s(y) \equiv s'(y) \bmod \mathfrak{m}$ for all $y \in k$; hence $s(x^{p^{-n}})^{p^n} \equiv s'(x^{p^{-n}})^{p^n} \bmod \mathfrak{m}^{n+1}$ for all $x \in k$ and $n \geq 0$, and so the limits coincide. Thus we have proved (b), and to prove that (b) is equivalent to (a) one proceeds similarly. □

In order to reconstruct the ring R from k, the main problem is now to describe its additive structure in terms of i. Once this is done, the multiplication can be deduced from Proposition 18.1 (a) and the distributive law:

$$\Big(\sum_n i(x_n)p^n\Big) \cdot \Big(\sum_m i(y_m)p^m\Big) = \sum_{n,m} i(x_n y_m)p^{n+m}.$$

One may wonder here: Does the addition depend on further structural invariants of R, or is it given by universal formulae? A hint towards the second option is given by the fact that the addition in the ring of p-adic integers $\mathbb{Z}_p \subset R$ is already unique. Indeed the latter is the case, and the problem is solved by the so-called ring of Witt vectors. This solution actually turnes everything around and defines a natural ring structure on $\prod_{n=0}^{\infty} k$ without prior presence of R. Notice that this produces a ring of characteristic zero from a field of characteristic p!

The construction is related to the fact that, although the *additive* group of the ring of power series $k[[t]]$ is annihilated by p, its *multiplicative* group of 1-units $1 + t \cdot k[[t]]$ is torsion free! Thus some aspect of characteristic zero is present in characteristic p.

The strategy is to first use power series over $\mathbb{Q}$ to produce some formulae which—somewhat miraculously—turn out to be integral at p, and then to reduce these formulae mod p.

§19 The Artin-Hasse exponential

Recall the Möbius function defined for integers $n \geq 1$ by

$$\mu(n) = \begin{cases} (-1)^{(\text{number of prime divisors of} n)} & \text{if } n \text{ is square-free,} \\ 0 & \text{otherwise.} \end{cases}$$

It is also characterized by the basic property

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 19.1. In $1 + t \cdot \mathbb{Q}[[t]]$ we have the equality

$$\exp(-t) = \prod_{n \geq 1} (1 - t^n)^{\frac{\mu(n)}{n}},$$

where the factors are evaluated by the binomial series.

Proof. Taking logarithms the equality follows from the calculation

$$\begin{aligned}\sum_{n\geq 1}\frac{\mu(n)}{n}\log(1-t^n) &= \sum_{n\geq 1}\frac{\mu(n)}{n}\sum_{m\geq 1}\Big(-\frac{t^{nm}}{m}\Big)\\ &\overset{d=nm}{=} -\sum_{d\geq 1}\Big(\sum_{n|d}\mu(n)\Big)\frac{t^d}{d} \quad = \quad -t.\end{aligned}$$

□

Note. On the right hand side above, all denominators come from the powers of $\frac{\mu(n)}{n}$ in the binomial series. The following definition will separate the p-part of these denominators from the non-p-part. Observe that the localization $\mathbb{Z}_{(p)}$ is the ring of rational numbers without p in the denominator.

Definition. $F(t) := \prod_{p\nmid n}(1-t^n)^{\frac{\mu(n)}{n}} \in 1+t\cdot\mathbb{Z}_{(p)}[[t]]$.

Lemma 19.2. $F(t) = \exp\Big(-\sum_{m\geq 0}\frac{t^{p^m}}{p^m}\Big)$.

Note. Thus we have the interesting situation that $F(t)$ is a power series without p in the denominators, but its logarithm has only powers of p in the denominators, while of course the logarithm and exponential series have all primes in their denominators. Insofar the definition of $F(t)$ is not as artificial as it might seem.

Proof. We again apply the logarithm:

$$\begin{aligned}\log F(t) &= \sum_{p\nmid n}\frac{\mu(n)}{n}\cdot\log(1-t^n)\\ &\overset{19.1}{=} -t-\sum_{p|n}\frac{\mu(n)}{n}\cdot\log(1-t^n)\\ &\overset{n=mp}{=} -t-\sum_{m}\frac{\mu(mp)}{mp}\cdot\log(1-t^{mp})\\ &\overset{(*)}{=} -t+\frac{1}{p}\sum_{p\nmid m}\frac{\mu(m)}{m}\log(1-t^{mp})\\ &= -t+\frac{1}{p}\log F(t^p)\end{aligned}$$

where $(*)$ uses the observation that if $p|m$, then mp is not square free and hence $\mu(mp)=0$. The lemma follows by iterating this formula. □

Lemma 19.3. There exist unique polynomials $\psi_n \in \mathbb{Z}[x,y]$ such that:

$$F(xt)\cdot F(yt) \;=\; \prod_{n\geq 0} F\big(\psi_n(x,y)\cdot t^{p^n}\big).$$

Proof. Since the power series $F(t)$ is congruent to $1-t \mod t^2$ and has coefficients in $\mathbb{Z}_{(p)}$, by successive approximation we find unique polynomials $\lambda_d \in \mathbb{Z}_{(p)}[x,y]$ such that

$$F(xt)\cdot F(yt) \;=\; \prod_{d\geq 1} F\big(\lambda_d(x,y)\cdot t^{d}\big).$$

Taking logarithm on both sides and using Lemma 19.2, this formula is equivalent to

$$\begin{aligned} -\sum_{m\geq 0}(x^{p^m}+y^{p^m})\cdot\frac{t^{p^m}}{p^m} \;&=\; -\sum_{d\geq 1}\sum_{m\geq 0}\lambda_d(x,y)^{p^m}\cdot\frac{t^{dp^m}}{p^m} \\ &=\; -\sum_{e\geq 1}\Bigg(\sum_{\substack{m\geq 0\\ p^m|e}}\frac{\lambda_{e/p^m}(x,y)^{p^m}}{p^m}\Bigg)\cdot t^e. \end{aligned}$$

Comparing coefficients, this shows that each λ_e is given recursively as a polynomial over $\mathbb{Z}[\frac{1}{p}]$ in x, y, and $\lambda_{e'}$ for certain $e'<e$. Thus by induction on e we deduce that λ_e lies in $\mathbb{Z}[\frac{1}{p}][x,y]$. Since a priori it is also in $\mathbb{Z}_{(p)}[x,y]$, we find that actually $\lambda_e \in \mathbb{Z}[x,y]$.

Moreover, suppose that $\lambda_e \neq 0$ for some $e\geq 1$ which is not a power of p. Then there exists a smallest e with this property, and for this e the above formula shows that λ_e is a $\mathbb{Q}$-linear combination of $\lambda_{e/p^m}^{p^m}$ for $m>0$ with $p^m|e$. But all those terms vanish by the minimality of e, yielding a contradiction. Therefore $\lambda_e=0$ whenever e is not a power of p, and so the lemma follows with $\psi_n := \lambda_{p^n}$. □

Now for any ring R we set

$$\Lambda_R \;:=\; \prod_{d\geq 1}\mathbb{A}^1_R \;=\; \operatorname{Spec} R[U_1,U_2,\cdots].$$

This is a scheme over R, only not of finite type. Identifying sequences $(u_1,u_2,\ldots)$ with power series $1+u_1t+u_2t^2+\ldots$ turns $\Lambda_R \cong$ "$1+t\cdot\mathbb{A}^1_R[[t]]$" into a commutative group scheme over R by the usual multiplication of power series

$$(1+u_1t+u_2t^2+\ldots)\cdot(1+v_1t+v_2t^2+\ldots) = 1+(u_1+v_1)t+(u_2+u_1v_1+v_2)t^2+\ldots.$$

Lemma 19.3 suggests that products of the form $\prod_{n\geq 0} F(x_n\cdot t^{p^n})$ form a subgroup of Λ_R. For any ring R we let

$$W_R \ := \ \prod_{n\geq 0} \mathbb{A}^1_R \ = \ \operatorname{Spec} R[X_0, X_1, \ldots]$$

and write points in it in the form $\underline{x} = (x_0, x_1, \ldots)$.

Definition. The *Artin-Hasse exponential* is the morphism E given by

$$\mathrm{W}_{\mathbb{Z}_{(p)}} \longrightarrow \Lambda_{\mathbb{Z}_{(p)}}, \quad \underline{x} \mapsto E(\underline{x}, t) := \prod_{n\geq 0} F(x_n\cdot t^{p^n}).$$

Proposition 19.4. There exists unique polynomials $s_n \in \mathbb{Z}[x_0, \ldots, x_n, y_0, \ldots, y_n]$ such that $E(\underline{x}, t) \cdot E(\underline{y}, t) = E(\underline{s}(\underline{x}, \underline{y}), t)$ with $\underline{s} = (s_0, s_1, \ldots)$. Moreover, the morphism $\underline{s}\colon \mathrm{W}_{\mathbb{Z}} \times \mathrm{W}_{\mathbb{Z}} \to \mathrm{W}_{\mathbb{Z}}$ defines the structure of a commutative group scheme over $\mathbb{Z}$.

Proof. The first part is proved by successive approximation using Lemma 19.3. For the "moreover" part we must produce the unit section and the inversion morphism of $W_{\mathbb{Z}}$. The former is defined as $\underline{0} = (0, 0, \ldots)$ and satisfies $E(\underline{0}, t) = 1$. For the latter we first show by explicit calculation that

$$F(t)^{-1} = \begin{cases} F(-t) & \text{if } p \neq 2, \\ \prod_{n\geq 0} F\big(-t^{p^n}\big) & \text{if } p = 2, \end{cases}$$

taking logarithms and using Lemma 19.2. By successive approximation we then find a unique morphism $\underline{i}\colon W_{\mathbb{Z}} \to W_{\mathbb{Z}}$ satisfying $E(\underline{x}, t)^{-1} = E(\underline{i}(\underline{x}), t)$. It remains to verify the group axioms for $\underline{s}$, $\underline{0}$, and $\underline{i}$, and that in turn can be done over $\mathbb{Z}_{(p)}$. But it is clear by construction that the Artin-Hasse exponential defines a closed embedding $E : \mathrm{W}_{\mathbb{Z}_{(p)}} \hookrightarrow \Lambda_{\mathbb{Z}_{(p)}}$. Thus by the above formulas relating E with $\underline{s}$, $\underline{0}$, and $\underline{i}$ the desired group axioms follow at once from those in $\Lambda_{\mathbb{Z}_{(p)}}$, finishing the proof. □

The next proposition will not be needed in the sequel, but it serves as an illustration of what is going on here.

Proposition 19.5. The morphism below is an isomorphism of group schemes:

$$\prod_{p\nmid m} \mathrm{W}_{\mathbb{Z}_{(p)}} \xrightarrow{\sim} \Lambda_{\mathbb{Z}_{(p)}}, \quad (\underline{x}_m)_m \mapsto \prod_{p\nmid m} E(\underline{x}_m, t^m) = \prod_{\substack{p\nmid m \\ n\geq 0}} F(x_{mn} \cdot t^{mp^n}).$$

Proof. Easy, using Proposition 19.4. □

Note. One can show that $\mathrm{W}_{\mathbb{Z}_{(p)}}$ is an indecomposable group scheme over $\mathbb{Z}_{(p)}$; hence by Proposition 19.5 it can be regarded as the unique indecomposable component of $\Lambda_{\mathbb{Z}_{(p)}}$ up to isomorphism. This illustrates a certain canonicity of $\mathrm{W}_{\mathbb{Z}_{(p)}}$, independent of the precise choice of F in its construction.

Lecture 8

December 9, 2004
Notes by Egon Rütsche

§20 The ring of Witt vectors over $\mathbb{Z}$

In this section we show that the group scheme structure on $\mathrm{W}_{\mathbb{Z}}$ from Proposition 19.4 is the addition for a certain ring scheme structure on $\mathrm{W}_{\mathbb{Z}}$. Set

$$\Phi_\ell(\underline{x}) \;:=\; \sum_{n=0}^{\ell} p^n x_n^{p^{\ell-n}} \;=\; x_0^{p^\ell} + p x_1^{p^{\ell-1}} + \ldots + p^\ell x_\ell. \tag{20.1}$$

Then using Lemma 19.1 we can rewrite

$$\begin{aligned} E(\underline{x},t) &= \prod_{n\geq 0} \exp\Big(-\sum_{m\geq 0} \frac{(x_n t^{p^n})^{p^m}}{p^m}\Big) \\ &= \exp\Big(-\sum_{n,m\geq 0} p^n x_n^{p^m} \cdot \frac{t^{p^{n+m}}}{p^{n+m}}\Big) \;=\; \exp\Big(-\sum_{\ell\geq 0} \Phi_\ell(\underline{x}) \cdot \frac{t^{p^\ell}}{p^\ell}\Big). \end{aligned}$$

The relation in Proposition 19.4 becomes

$$\log E(\underline{x},t) + \log E(\underline{y},t) = \log E(\underline{s}(\underline{x},\underline{y}),t),$$

which is equivalent to

$$-\sum_{\ell\geq 0} \Phi_\ell(\underline{x}) \frac{t^{p^\ell}}{p^\ell} - \sum_{\ell\geq 0} \Phi_\ell(\underline{y}) \frac{t^{p^\ell}}{p^\ell} = -\sum_{\ell\geq 0} \Phi_\ell\big(\underline{s}(\underline{x},\underline{y})\big) \frac{t^{p^\ell}}{p^\ell}.$$

By equating coefficients, we deduce that Proposition 19.4 is equivalent to

Proposition 20.2. The above group law on $\mathrm{W}_{\mathbb{Z}}$ is the unique one for which each $\Phi_\ell : \mathrm{W}_{\mathbb{Z}} \longrightarrow \big(\mathbb{A}^1_{\mathbb{Z}}, +\big)$ is a homomorphism.

Remark. We write this group law additively, i.e. $\underline{s}(\underline{x},\underline{y}) =: \underline{x} + \underline{y}$.

Terminology. An element $\underline{x} = (x_0, x_1, \ldots) \in \mathrm{W}(R)$ is called a *Witt vector*, and the $x_0, x_1, \ldots$ its *components*. The expressions $\Phi_\ell(\underline{x})$ are called *phantom components*. The reason for this is that over $\mathbb{Z}[\frac{1}{p}]$, giving the x_ℓ is equivalent to giving the $\Phi_\ell(\underline{x})$, because we have an isomorphism

$$\mathrm{W}_{\mathbb{Z}[\frac{1}{p}]} \longrightarrow \prod_{\ell=0}^{\infty} \mathbb{A}^1_{\mathbb{Z}[\frac{1}{p}]}, \;\; \underline{x} \mapsto \big(\Phi_\ell(\underline{x})\big)_\ell. \tag{20.3}$$

But the expressions reduce to $\Phi_\ell(\underline{x}) \equiv x_0^{p^\ell} \mod p$, so only a "phantom" of what was there remains.

Proposition 20.2 also generalizes as follows, with an independent proof:

Theorem 20.4. There are unique morphisms $+, \cdot : \mathrm{W}_{\mathbb{Z}} \times \mathrm{W}_{\mathbb{Z}} \longrightarrow W_{\mathbb{Z}}$ defining a unitary ring structure, such that each $\Phi_\ell : \mathrm{W}_{\mathbb{Z}} \longrightarrow \mathbb{A}^1_{\mathbb{Z}}$ is a unitary ring homomorphism (and $+$ coincides with that from Propositions 19.4 and 20.2).

Remark. On Witt vectors $+$ and $\cdot$ will always denote the above morphisms, not the componentwise addition and multiplication.

Proof. The isomorphism (20.3) shows that the theorem holds over $\mathbb{Z}[\frac{1}{p}]$. To prove it over $\mathbb{Z}$ we must show that $+$ and $\cdot$, as well as the respective identity sections and the additive inverse, are morphisms defined over $\mathbb{Z}$. For $+$ and $\cdot$ this is achieved conveniently by Lemma 20.5 below. One easily checks that $\underline{0} = (0, 0, \ldots)$ and $\underline{1} = (1, 0, 0, \ldots)$ are the additive and multiplicative identity sections. For the additive inverse the reader is invited to adapt Lemma 20.5. Finally, once all morphisms are defined over $\mathbb{Z}$, the ring and homomorphism axioms over $\mathbb{Z}$ follow directly from those over $\mathbb{Z}[\frac{1}{p}]$. □

Lemma 20.5. For every morphism $u : \mathbb{A}^1_{\mathbb{Z}} \times \mathbb{A}^1_{\mathbb{Z}} \longrightarrow \mathbb{A}^1_{\mathbb{Z}}$ there exists a unique morphism $\underline{v} : \mathrm{W}_{\mathbb{Z}} \times \mathrm{W}_{\mathbb{Z}} \longrightarrow \mathrm{W}_{\mathbb{Z}}$ such that for all $\ell \geq 0$: $\Phi_\ell \circ \underline{v} = u \circ (\Phi_\ell \times \Phi_\ell)$.

Proof. By the isomorphism (20.3) there exist unique $\underline{v} = (v_0, v_1, \ldots)$ with $v_n \in \mathbb{Z}[\frac{1}{p}][x_0, \ldots, x_n, y_0, \ldots, y_n]$ satisfying the desired relations. It remains to show that $v_n \in A := \mathbb{Z}[x_0, \ldots, y_0, \ldots]$. Since $\Phi_0(\underline{x}) = x_0$, this is clear for $v_0 = u(x_0, y_0)$. So fix $n \geq 0$ and assume that $v_i \in A$ for all $i \leq n$. For any sequence $\underline{x} = (x_0, x_1, \ldots)$ we will abbreviate $\underline{x}^p = (x_0^p, x_1^p, \ldots)$. Then the definition (20.1) of Φ_ℓ implies that

$$\Phi_{n+1}(\underline{x}) \;=\; \Phi_n(\underline{x}^p) + p^{n+1} x_{n+1}.$$

Using this and the relation defining $\underline{v}$ we deduce that

$$\begin{aligned} \Phi_n(\underline{v}^p) + p^{n+1} v_{n+1} &= \Phi_{n+1}(\underline{v}) \\ &\overset{\text{def}}{=} u\big(\Phi_{n+1}(\underline{x}), \Phi_{n+1}(\underline{y})\big) \\ &= u\big(\Phi_n(\underline{x}^p) + p^{n+1} x_{n+1}, \Phi_n(\underline{y}^p) + p^{n+1} y_{n+1}\big). \end{aligned}$$

Here note that the right hand side and $\Phi_n(\underline{v}^p)$ are already in A. Thus we have $p^{n+1} v_{n+1} \in A$ and

$$\begin{aligned} p^{n+1} v_{n+1} &\equiv u\big(\Phi_n(\underline{x}^p), \Phi_n(\underline{y}^p)\big) - \Phi_n(\underline{v}^p) \mod p^{n+1} A \\ &\overset{\text{def}}{=} \Phi_n\big(\underline{v}(\underline{x}^p, \underline{y}^p)\big) - \Phi_n(\underline{v}^p). \end{aligned} \tag{20.6}$$

To evaluate this further recall that $v_i \in A$ for all $0 \leq i \leq n$; hence

$$v_i(\underline{x}^p, \underline{y}^p) \equiv v_i(\underline{x}, \underline{y})^p \mod pA.$$

This implies that

$$\begin{array}{rcl} v_i(\underline{x}^p, \underline{y}^p)^{p^{n-i}} & \equiv & \big(v_i(\underline{x}, \underline{y})^p\big)^{p^{n-i}} \mod p^{n-i+1}A, \text{ hence} \\ p^i v_i(\underline{x}^p, \underline{y}^p)^{p^{n-i}} & \equiv & p^i \big(v_i(\underline{x}, \underline{y})^p\big)^{p^{n-i}} \mod p^{n+1}A, \text{ and therefore} \\ \Phi_n\big(\underline{v}(\underline{x}^p, \underline{y}^p)\big) & \equiv & \Phi_n(\underline{v}^p) \mod p^{n+1}A. \end{array}$$

Together with (20.6) we deduce that $p^{n+1}v_{n+1} \in p^{n+1}A$, and hence $v_{n+1} \in A$. The lemma follows by induction on n. □

Examples. We write $\underline{s} = (s_0, s_1, \ldots)$ for the morphism $+$, and $\underline{p} = (p_0, p_1, \ldots)$ for the morphism $\cdot$. Using the relations $\Phi_0(\underline{x}) = x_0$ and $\Phi_1(\underline{x}) = x_0^p + px_1$, elementary calculation shows that

$$\begin{array}{rcl} s_0(\underline{x}, \underline{y}) & = & x_0 + y_0, \\ p_0(\underline{x}, \underline{y}) & = & x_0 \cdot y_0, \\ s_1(\underline{x}, \underline{y}) & = & x_1 + y_1 + \dfrac{1}{p}\big(x_0^p + y_0^p - (x_0 + y_0)^p\big) \\ & = & x_1 + y_1 - \displaystyle\sum_{i=0}^{p-1} \frac{1}{p}\binom{p}{i} x_0^i y_0^{p-i}, \\ p_1(\underline{x}, \underline{y}) & = & x_0^p y_1 + x_1 y_0^p + p x_1 y_1. \end{array}$$

As one can see, the formulas are quickly becoming very complicated. One should not use them directly, but think conceptually.

For use in the next section we note:

Proposition 20.7. The morphism $\tau : \mathbb{A}^1_{\mathbb{Z}} \longrightarrow \mathrm{W}_{\mathbb{Z}},\ x \mapsto (x, 0, \ldots)$ is multiplicative, i.e., it satisfies $\tau(xy) = \tau(x) \cdot \tau(y)$.

Proof. It is enough to check this over $\mathbb{Z}[\frac{1}{p}]$, i.e., after applying each Φ_ℓ. But $\Phi_\ell\big(\tau(x)\big) = x^{p^\ell}$ is obviously multiplicative. □

Finally, we introduce *Witt vectors of finite length* $n \geq 1$. For this recall that the m-th components of $\underline{x} + \underline{y}$ and $\underline{x} \cdot \underline{y}$ and $-\underline{x}$ depend only on the first m components of $\underline{x}$ and $\underline{y}$. Thus the same formulas define a ring structure on $W_{n,R} := \prod_{m=0}^{n-1} \mathbb{A}^1_R$ for any ring R, such that the truncation map

(20.8) $$W_R \longrightarrow W_{n,R},\ \underline{x} \mapsto (x_0, \ldots, x_{n-1})$$

is a ring homomorphism.

§21 Witt vectors in characteristic p

From now on let k be a perfect field of characteristic $p > 0$. For any scheme X over $\mathbb{F}_p$ we abbreviate $X_k := X \times_{\mathrm{Spec}\,\mathbb{F}_p} \mathrm{Spec}\,k$. Then there is a natural isomorphism $X_k^{(p)} \cong X_k$ which turns the relative Frobenius of X_k into the endomorphism $\sigma_X \times \mathrm{id}$ of X_k, where σ_X denotes the absolute Frobenius of X. Indeed, this follows from the definition of Frobenius from §14 and the fact that the two rectangles in the following commutative diagram are cartesian:

$$\begin{tikzcd}
X_k \arrow[dr, dashed, "F_{X_k} = \sigma_X \times \mathrm{id}"] \arrow[drr, bend left, "\sigma_{X_k}"] \arrow[ddr, bend right] & & & \\
& X_k^{(p)} = X_k \arrow[r, "\mathrm{id} \times \sigma_{\mathrm{Spec}\,k}"] \arrow[d] & X_k \arrow[r, "\mathrm{pr}_1"] \arrow[d] & X \arrow[d] \\
& \mathrm{Spec}\,k \arrow[r, "\sigma_{\mathrm{Spec}\,k}"] & \mathrm{Spec}\,k \arrow[r] & \mathrm{Spec}\,\mathbb{F}_p
\end{tikzcd}$$

In particular we can apply this to $W_k = W_{\mathbb{F}_p} \times_{\mathrm{Spec}\,\mathbb{F}_p} \mathrm{Spec}\,k$. Thus the Frobenius and Verschiebung for the additive group of W_k become *endomorphisms* satisfying $F \circ V = V \circ F = p \cdot \mathrm{id}$. The following proposition collects some of their properties.

Proposition 21.1. (a) $F\big((x_0, x_1, \ldots)\big) = (x_0^p, x_1^p, \ldots)$.

(b) $V\big((x_0, x_1, \ldots)\big) = (0, x_0, x_1, \ldots)$.

(c) $p \cdot (x_0, x_1, \ldots) = (0, x_0^p, x_1^p, \ldots)$.

(d) $F(\underline{x} + \underline{y}) = (F\underline{x}) + (F\underline{y})$.

(e) $F(\underline{x} \cdot \underline{y}) = (F\underline{x}) \cdot (F\underline{y})$.

(f) $\underline{x} \cdot (V\underline{y}) = V\big((F\underline{x}) \cdot \underline{y}\big)$.

(g) $E\big(\underline{x} \cdot (V\underline{y}), t\big) = E\big((F\underline{x}) \cdot \underline{y}, t^p\big)$.

Remark. Part (b) is probably the reason why V is called Verschiebung.

Proof. (a), (d), and (e) are clear from the definition and functoriality of F. (b) is equivalent to (c) by the relation $p \cdot \underline{x} = VF\underline{x}$, because $F : \mathrm{W}_k \to \mathrm{W}_k$ is an epimorphism. For (c) we cannot use the phantom components, because we are in characteristic $p > 0$. Instead we use the Artin-Hasse exponential

$E(\underline{x},t) = \prod_{n=0}^{\infty} F(x_n t^{p^n})$. Recall that it defines a homomorphism and a closed embedding $W_{\mathbb{Z}_{(p)}} \to \Lambda_{\mathbb{Z}_{(p)}}$, and hence also $W_k \to \Lambda_k$. Therefore

$$\begin{aligned} E(p \cdot \underline{x}, t) \;=\; E(\underline{x},t)^p \;&=\; \prod_{n=0}^{\infty} F(x_n t^{p^n})^p \;\overset{(*)}{=}\; \prod_{n=0}^{\infty} F(x_n^p t^{p^{n+1}}) \\ &=\; \prod_{n=1}^{\infty} F(x_{n-1}^p t^{p^n}) \;=\; E\big((0, x_0^p, x_1^p, \ldots), t\big), \end{aligned}$$

where $(*)$ follows from the fact that we are working over k and that F has coefficients in $\mathbb{Z}_{(p)}$. This shows (c). Next, since F is an epimorphism, it suffices to prove (f) for $\underline{y} = F\underline{z}$. But for this it follows from the calculation

$$\begin{aligned} \underline{x} \cdot (V\underline{y}) \;&=\; \underline{x} \cdot (VF\underline{z}) \;=\; \underline{x} \cdot (p \cdot \underline{z}) \;=\; p \cdot (\underline{x} \cdot \underline{z}) \\ &=\; VF(\underline{x} \cdot \underline{z}) \;\overset{\text{(e)}}{=}\; V\big((F\underline{x}) \cdot (F\underline{z})\big) \;=\; V\big((F\underline{x}) \cdot \underline{y}\big). \end{aligned}$$

Finally, (g) results from

$$E\big(\underline{x} \cdot (V\underline{y}), t\big) \;\overset{\text{(f)}}{=}\; E\big(V\big((F\underline{x}) \cdot \underline{y}\big), t\big) \;\overset{\text{def. of } E}{=}\; E\big((F\underline{x}) \cdot \underline{y}, t^p\big). \qquad \square$$

Theorem 21.2. $\mathrm{W}(k)$ is a complete discrete valuation ring with uniformizer p and residue field k.

Proof. Since k is perfect, we have $p^n\,\mathrm{W}(k) = V^n\big(\mathrm{W}(k)\big)$ for all $n \geq 1$. By iterating Proposition 21.1 (b) this is also the kernel of the truncation homomorphism $W(k) \to W_n(k)$ from (20.8). Thus $W(k)/p^nW(k) \cong W_n(k)$ and $W(k)/pW(k) \cong W_1(k) \cong k$. Using this, by induction on n one shows that $W_n(k)$ is a $W(k)$-module of length n. Since clearly $W(k) \cong \varprojlim_n W_n(k)$, the theorem follows. □

Theorem 21.3 (Witt). Let R be a complete noetherian local ring with residue field k.

(a) There exists a unique ring homomorphism $u : \mathrm{W}(k) \longrightarrow R$ such that the following diagram commutes:

$$\begin{tikzcd} \mathrm{W}(k) \arrow[rr, "u"] \arrow[dr] & & R \arrow[dl] \\ & k. & \end{tikzcd}$$

(b) If R is a complete discrete valuation ring with uniformizer p, then u is an isomorphism.

Proof. Recall that by Proposition 18.1 there are unique multiplicative sections

$$\begin{tikzcd}
\mathrm{W}(k) & & R \\
& k. \arrow[ul, "\tau"] \arrow[ur, "i"'] &
\end{tikzcd}$$

Since u is also multiplicative, it must therefore satisfy the equation $i = u \circ \tau$. By Proposition 20.7 we have $\tau(x) = (x, 0, \ldots)$. In view of Proposition 21.1 (c) this implies that any element $\underline{x} = (x_0, x_1, \ldots) \in \mathrm{W}(k)$ has the power series expansion

$$\underline{x} \;=\; \tau(x_0) + p \cdot \tau(x_1^{1/p}) + p^2 \cdot \tau(x_2^{1/p^2}) + \ldots .$$

So the ring homomorphism u must be given by

$$u(\underline{x}) \;=\; i(x_0) + p \cdot i(x_1^{1/p}) + p^2 \cdot i(x_2^{1/p^2}) + \ldots .$$

In particular u is unique, but we must verify that this formula does define a ring homomorphism. For this, let $\mathfrak{m}$ be the maximal ideal of R, which contains p, and calculate:

$$\begin{aligned} u(\underline{x}) &\equiv i(x_0) + p \cdot i(x_1^{1/p}) + \ldots + p^n \cdot i(x_n^{1/p^n}) \quad \bmod \mathfrak{m}^{n+1}, \\ &= i(x_0^{p^{-n}})^{p^n} + p \cdot i(x_1^{p^{-n}})^{p^{n-1}} + \ldots + p^n \cdot i(x_n^{p^{-n}}) \\ &= \Phi_n\big(i(x_0^{p^{-n}}), \ldots, i(x_n^{p^{-n}})\big). \end{aligned}$$

It is enough to show that this defines a ring homomorphism $W(k) \to R/\mathfrak{m}^{n+1}$ for any n, because R is complete noetherian and hence $R = \varprojlim R/\mathfrak{m}^{n+1}$. Since Frobenius defines a ring automorphism of $W(k)$, this is equivalent to showing that $\Phi_n\big(i(x_0), \ldots, i(x_n)\big)$ defines a ring homomorphism $W(k) \to R/\mathfrak{m}^{n+1}$. But $\Phi_n : \mathrm{W}(R) \to R$ is a ring homomorphism by the construction of Witt vectors. Moreover, we have $\Phi_n(x_0, \ldots, x_n) \in \mathfrak{m}^{n+1}$ if all $x_i \in \mathfrak{m}$, by the definition of Φ_n. Thus the composite homomorphism in the diagram

$$\begin{tikzcd}
\mathrm{W}(R) \arrow[r, "\Phi_n"] \arrow[d, two heads] & R \arrow[d, two heads] \\
\mathrm{W}(k) \arrow[r, dashed] & R/\mathfrak{m}^{n+1}
\end{tikzcd}$$

vanishes on the kernel of the left vertical map; hence it factors through a ring homomorphism along the lower edge. The lower arrow is then given explicitly by $\Phi_n\big(i(x_0), \ldots, i(x_n)\big) \bmod \mathfrak{m}^{n+1}$ for any section i, in particular for the canonical one. Therefore this defines a ring homomorphism, proving (a).

(b) follows from the fact that any homomorphism of complete discrete valuation rings with the same uniformizer and the same residue field is an isomorphism. $\square$

Lecture 9

December 16, 2004
Notes by Richard Pink
(§16 was also presented on that day, but moved to its proper place in the text.)

§22 Finite Witt group schemes

From now on we abbreviate $W := W_k$, restoring the index $_k$ only when the dependence on the field k is discussed. Also, we will no longer underline points in W or in quotients thereof.

For any integer $n \geq 1$ we let $W_n \cong W/V^nW$ denote the additive group scheme of Witt vectors of length n over k. Truncation induces natural epimorphisms $r\colon W_{n+1} \twoheadrightarrow W_n$, and Verschiebung induces natural monomorphisms $v\colon W_n \hookrightarrow W_{n+1}$, such that $rv = vr = V$. For any n, $n' \geq 1$ they induce a short exact sequence

$$0 \longrightarrow W_{n'} \xrightarrow{v^n} W_{n+n'} \xrightarrow{r^{n'}} W_n \longrightarrow 0.$$

(The exactness can be deduced from the fact that $r^{n'}$ possesses the scheme theoretic splitting $x \mapsto (x, 0, \ldots, 0)$, although we have not proved in this course that the category of all affine commutative group schemes is abelian.) Together with the natural isomorphism $W_1 \cong \mathbb{G}_a$, these exact sequences describe W_n as a successive extension of n copies of $\mathbb{G}_a$.

For any integers n, $m \geq 1$ we let W_n^m denote the kernel of F^m on W_n. As above, truncation induces natural epimorphisms $r : W_{n+1}^m \twoheadrightarrow W_n^m$, and Verschiebung induces natural monomorphisms $v\colon W_n^m \hookrightarrow W_{n+1}^m$, such that $rv = vr = V$. Similarly, the inclusion induces natural monomorphisms $i\colon W_n^m \hookrightarrow W_n^{m+1}$, and Frobenius induces natural epimorphisms $f\colon W_n^{m+1} \twoheadrightarrow W_n^m$, such that $if = fi = F$. For any n, n', m, $m' \geq 1$ they induce short exact sequences

$$0 \longrightarrow W_{n'}^m \xrightarrow{v^n} W_{n+n'}^m \xrightarrow{r^{n'}} W_n^m \longrightarrow 0,$$
$$0 \longrightarrow W_n^m \xrightarrow{i^{m'}} W_n^{m+m'} \xrightarrow{f^m} W_n^{m'} \longrightarrow 0.$$

Together with the natural isomorphism $W_1^1 \cong \boldsymbol{\alpha}_p$, these exact sequences describe W_n^m as a successive extension of nm copies of $\boldsymbol{\alpha}_p$. For later use note the following fact:

Lemma 22.1. *Let G be a finite commutative group scheme with $F_G^m = 0$ and $V_G^n = 0$. Then any homomorphism $\varphi : G \to W_{n'}^{m'}$ with $m' \geq m$ and $n' \geq n$ factors uniquely through the embedding $i^{m'-m}v^{n'-n}\colon W_n^m \hookrightarrow W_{n'}^{m'}$.*

Proof. By the functoriality of Frobenius from Proposition 14.1, the assumption implies that $F^m_{W^{m'}_{n'}} \circ \varphi = \varphi^{(p^m)} \circ F^m_G = 0$. Thus φ factors through the kernel of F^m on $W^{m'}_{n'}$, which is the image of $i^{m'-m} : W^m_{n'} \hookrightarrow W^{m'}_{n'}$. The analogous argument with V^n_G in place of F^m_G shows the rest. □

We will show that all commutative finite group schemes of local-local type can be constructed from the *Witt group schemes* W^m_n. The main step towards this is the following result on extensions:

Proposition 22.2. For any short exact sequence $0 \to W^m_n \to G \to \boldsymbol{\alpha}_p \to 0$ there exists a homomorphism φ making the following diagram commute:

$$\begin{tikzcd}
0 \arrow[r] & W^m_n \arrow[r] \arrow[d, hook, "iv"'] & G \arrow[r] \arrow[dl, "\varphi"] & \boldsymbol{\alpha}_p \arrow[r] & 0 \\
& W^{m+1}_{n+1} & & &
\end{tikzcd}$$

Note. In more highbrow language this means that the homomorphism induced by iv on the Yoneda Ext groups $\mathrm{Ext}^1(\boldsymbol{\alpha}_p, W^m_n) \to \mathrm{Ext}^1(\boldsymbol{\alpha}_p, W^{m+1}_{n+1})$ is zero. I prefer to stay as down to earth as possible in this course.

Lemma 22.3. Proposition 22.2 holds in the case $n = m = 1$.

Proof. As a preparation let U denote the kernel of the epimorphism $rf : W^2_2 \twoheadrightarrow W^1_1 = \boldsymbol{\alpha}_p$. Then r and f induce epimorphisms

$$\begin{array}{rcl}
r' : U & \twoheadrightarrow & \ker(f \colon W^2_1 \twoheadrightarrow W^1_1) \cong W^1_1 = \boldsymbol{\alpha}_p, \\
f' : U & \twoheadrightarrow & \ker(r \colon W^1_2 \twoheadrightarrow W^1_1) \cong W^1_1 = \boldsymbol{\alpha}_p,
\end{array}$$

which together yield a short exact sequence

$$0 \longrightarrow \boldsymbol{\alpha}_p = W^1_1 \xrightarrow{iv} U \xrightarrow{(r',f')} \boldsymbol{\alpha}_p^{\oplus 2} \longrightarrow 0.$$

Since $F = V = 0$ on $\boldsymbol{\alpha}_p$, one easily shows that F_U and V_U are induced from

$$k^{\oplus 2} \;\cong\; \mathrm{Hom}(\boldsymbol{\alpha}_p^{\oplus 2}, \boldsymbol{\alpha}_p) \;\hookrightarrow\; \mathrm{Hom}(U, U).$$

In fact, going through the construction one finds that F_U and V_U correspond to the elements $(0, 1)$ and $(1, 0)$ of $k^{\oplus 2}$, respectively. Essentially the proof will show that U represents the universal extension of $\boldsymbol{\alpha}_p$ with $\boldsymbol{\alpha}_p$.

For any short exact sequence $0 \to \boldsymbol{\alpha}_p \to G \xrightarrow{\pi} \boldsymbol{\alpha}_p \to 0$ we define a group scheme G' such that the upper left square in the following commutative diagram with exact rows and columns is a pushout:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
0 \arrow[r] & \boldsymbol{\alpha}_p \arrow[r] \arrow[d] & G \arrow[r] \arrow[d] & \boldsymbol{\alpha}_p \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & U \arrow[r] \arrow[d, "{(r',f')}"'] & G' \arrow[r, "\pi'"] \arrow[d, "\rho'"'] & \boldsymbol{\alpha}_p \arrow[r] & 0 \\
 & \boldsymbol{\alpha}_p^{\oplus 2} \arrow[r, equal] \arrow[d] & \boldsymbol{\alpha}_p^{\oplus 2} \arrow[d] & & \\
 & 0 & 0 & &
\end{tikzcd}$$

By looking at the induced short exact sequence

$$0 \longrightarrow \boldsymbol{\alpha}_p \longrightarrow G' \overset{(\pi',\rho')}{\longrightarrow} \boldsymbol{\alpha}_p^{\oplus 3} \longrightarrow 0$$

one shows as above that $F_{G'}$ and $V_{G'}$ are induced from

$$k^{\oplus 3} \;\cong\; \mathrm{Hom}(\boldsymbol{\alpha}_p^{\oplus 3}, \boldsymbol{\alpha}_p) \;\hookrightarrow\; \mathrm{Hom}(G', G').$$

In fact, comparison with the result for U shows that $F_{G'}$ and $V_{G'}$ correspond to triples $(x, 0, 1)$ and $(y, 1, 0)$, respectively, for certain elements x, $y \in k$. Define a subgroup scheme $G'' \subset G'$ as the pullback in the following commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & \boldsymbol{\alpha}_p \arrow[r] & G' \arrow[r] & \boldsymbol{\alpha}_p^{\oplus 3} \arrow[r] & 0 \\
0 \arrow[r] & \boldsymbol{\alpha}_p \arrow[r] \arrow[u, equal] & G'' \arrow[r] \arrow[u, hook] & \boldsymbol{\alpha}_p \arrow[r] \arrow[u, hook, "{(1,-y,-x)}"'] & 0
\end{tikzcd}$$

Then by construction one finds that $F_{G''} = 0$ and $V_{G''} = 0$. (In fact, G'' is just the right Baer linear combination of the extension G with the two basic extensions W_2^1 and W_1^2 which enjoys this property.) Thus Proposition 16.2 implies that $G'' \cong \boldsymbol{\alpha}_p^{\oplus 2}$ is split. This splitting yields an embedding $\iota\colon \boldsymbol{\alpha}_p \hookrightarrow G'$ satisfying $\pi'\iota = \mathrm{id}$, which in turn splits the extension $0 \to U \to G' \to \boldsymbol{\alpha}_p \to 0$.

Finally, the resulting homomorphism $G' \to U$ yields a composite arrow making the following diagram commute:

$$\begin{tikzcd}
\boldsymbol{\alpha}_p \arrow[r] \arrow[d, hook] \arrow[dd, hook, bend right=60, "iv"'] & G \arrow[d, hook] \arrow[ddl, bend left=60] \\
U \arrow[d, hook] & G' \arrow[l] \\
W_2^2 &
\end{tikzcd}$$

as asserted by Proposition 22.2. $\square$

Lemma 22.4. (a) Fix $n \geq 1$. If Proposition 22.2 holds for this n and $m = 1$, then it holds for this n and all $m \geq 1$.

(b) Fix $m \geq 1$. If Proposition 22.2 holds for this m and $n = 1$, then it holds for this m and all $n \geq 1$.

Proof. For any short exact sequence $0 \to W_n^m \to G \to \boldsymbol{\alpha}_p \to 0$, define G' such that the left square in the following commutative diagram with exact rows is a pushout:

$$\begin{tikzcd}
0 \arrow[r] & W_n^m \arrow[r] \arrow[d, hook, "i"'] & G \arrow[r] \arrow[d, "\psi"] & \boldsymbol{\alpha}_p \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & W_n^{m+1} \arrow[r] & G' \arrow[r] & \boldsymbol{\alpha}_p \arrow[r] & 0
\end{tikzcd}$$

As $F = 0$ on $\boldsymbol{\alpha}_p$, and $F^m = 0$ on W_n^m, one easily shows that $F^{m+1} = 0$ on G. Thus F^{m+1} vanishes on $W_n^{m+1} \oplus G$, and since G' can be constructed as a quotient thereof, also on G'. Consider the following commutative diagram with exact rows, where the dashed arrows are not yet defined:

$$\begin{tikzcd}
0 \arrow[r] & W_n^{m+1} \arrow[rr] \arrow[dd, "F"] \arrow[dr, "f"'] & & G' \arrow[r] \arrow[dd, "F"] \arrow[dl, dashed, "F''"'] \arrow[ddll, dashed, "F'"] & \boldsymbol{\alpha}_p \arrow[r] \arrow[dd, "F=0"] & 0 \\
& & W_n^m \arrow[dl, hook, "i"'] & & & \\
0 \arrow[r] & W_n^{m+1} \arrow[rr] \arrow[d, "F^m"] & & G'^{(p)} \arrow[r] \arrow[d, "F^m"] & \boldsymbol{\alpha}_p \arrow[r] & 0 \\
0 \arrow[r] & W_n^{m+1} \arrow[rr] & & G'^{(p^{m+1})} & &
\end{tikzcd}$$

The dashed arrow F' is obtained from the fact that the upper right square commutes and that $F = 0$ on $\boldsymbol{\alpha}_p$. Looking at the lower left part of the diagram, the fact that $F^m \circ F = F^{m+1} = 0$ on G' implies that F' factors through the kernel of F^m on W_n^{m+1}. But this kernel is just the image of W_n^m under i, which yields the dashed arrow F'' making everything commute. Since the oblique arrow f is an epimorphism, the same holds a fortiori for F''. Setting $G'' := \ker F''$ we obtain a commutative diagram with exact rows and columns

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
0 \arrow[r] & W_n^1 \arrow[r] \arrow[d, "i^m"'] \arrow[dr, phantom, "(*)"] & G'' \arrow[r] \arrow[d] & \boldsymbol{\alpha}_p \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & W_n^{m+1} \arrow[r] \arrow[d, "f"'] & G' \arrow[r] \arrow[d, "F''"] & \boldsymbol{\alpha}_p \arrow[r] & 0 \\
 & W_n^m \arrow[r, equal] \arrow[d] & W_n^m \arrow[d] & & \\
 & 0 & 0 & &
\end{tikzcd}$$

Here by diagram chasing we find that the square marked $(*)$ is a pushout. By assumption we may apply Proposition 22.2 to G'', obtaining a homomorphism φ'' making the upper triangle of the following Toblerone diagram commute:

$$\begin{tikzcd}
W_n^1 \arrow[rr] \arrow[dd, hook, "i^m"'] \arrow[dr, hook, "iv"'] & & G'' \arrow[dl, "\varphi''"] \arrow[dd] \\
 & W_{n+1}^2 \arrow[dd, hook, "i^{m-1}"'] & \\
W_n^{m+1} \arrow[rr] \arrow[dr, hook, "v"'] & & G' \arrow[dl, dashed, "\varphi'"] \\
 & W_{n+1}^{m+1} &
\end{tikzcd}$$

Since $(*)$ is a pushout, this commutative diagram can be completed by the dashed homomorphism φ' at the lower right. Altogether, the composite homomorphism $\varphi := \varphi'\psi : G \to G' \to W_{n+1}^{m+1}$ has the desired properties, proving (a). The proof of (b) is entirely analogous, with V in place of F. $\square$

Proof of Proposition 22.2. By Lemma 22.3 the proposition holds in the case $n = m = 1$. By Lemma 22.4 (a) the proposition follows whenever $n = 1$, and from this it follows in general by Lemma 22.4 (b). $\square$

Proposition 22.5. Every commutative finite group scheme of local-local type can be embedded into $(W_n^m)^{\oplus r}$ for some n, m, and r.

Proof. To prove this by induction on $|G|$, we may consider a short exact sequence $0 \to G' \to G \to \boldsymbol{\alpha}_p \to 0$ and assume that there exists an embedding $\psi = (\psi_1, \ldots, \psi_r) : G' \hookrightarrow (W_n^m)^{\oplus r}$. For $1 \leq i \leq r$ define G_i such that the upper left square in the following commutative diagram with exact rows is a pushout:

$$\begin{tikzcd}
0 \arrow[r] & G' \arrow[r] \arrow[d, "\psi_i"'] & G \arrow[r] \arrow[d] & \boldsymbol{\alpha}_p \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & W_n^m \arrow[r] \arrow[d, hook, "iv"'] & G_i \arrow[r] \arrow[dl, dashed] & \boldsymbol{\alpha}_p \arrow[r] & 0 \\
& W_{n+1}^{m+1} & & &
\end{tikzcd}$$

The dashed arrows, which exist by Proposition 22.2, determine an extension of the composite embedding $iv\psi : G' \hookrightarrow (W_{n+1}^{m+1})^{\oplus r}$ to a homomorphism $G \to (W_{n+1}^{m+1})^{\oplus r}$. The direct sum of this with the composite homomorphism $G \twoheadrightarrow \boldsymbol{\alpha}_p = W_1^1 \hookrightarrow W_{n+1}^{m+1}$ is an embedding $G \hookrightarrow (W_{n+1}^{m+1})^{\oplus r+1}$. $\square$

Proposition 22.6. Every commutative finite group scheme G with $F_G^m = 0$ and $V_G^n = 0$ possesses a copresentation (i.e., an exact sequence) for some r, s

$$0 \longrightarrow G \longrightarrow (W_n^m)^{\oplus r} \longrightarrow (W_n^m)^{\oplus s}\,.$$

Proof. By Proposition 22.5 there exists an embedding $G \hookrightarrow (W_{n'}^{m'})^{\oplus r}$ for some n', m', and r. After composing it in each factor with the embedding $iv\colon W_{n'}^{m'} \hookrightarrow W_{n'+1}^{m'+1}$, if necessary, we may assume that $n' \geq n$ and $m' \geq m$. Then Lemma 22.1 implies that the embedding factors through a homomorphism $G \to (W_n^m)^{\oplus r}$, which is again an embedding. Let H denote its cokernel. Since $F^m = 0$ and $V^n = 0$ on W_n^m, the same is true on $(W_n^m)^{\oplus r}$ and hence on H. Repeating the first part of the proof with H in place of G, we therefore find an embedding $H \hookrightarrow (W_n^m)^{\oplus s}$ for some s. The proposition follows. $\square$

Lecture 10

December 23, 2004
Notes by Nicolas Stalder

§23 The Dieudonné functor in the local-local case

Recall that k is a perfect field, $W = W_k$ is the Witt group scheme over k, W_n is the cokernel of V^n on W, and W_n^m is the kernel of F^m on W_n. The collection of all W_n^m becomes a direct system via the homomorphisms v and i:

$$\begin{tikzcd}
W_n^m \arrow[r, hook, "i"] \arrow[d, hook, "v"] & W_n^{m+1} \arrow[d, hook, "v"] \\
W_{n+1}^m \arrow[r, hook, "i"] & W_{n+1}^{m+1}
\end{tikzcd}$$

Let $\sigma : W(k) \longrightarrow W(k)$ denote the ring endomorphism induced by F. (We use a different letter to avoid confusion with F as an endomorphism of the group scheme W!)

Definition. Let E be the ring of "noncommutative polynomials" over $W(k)$ in two variables F and V, subject to the following relations:

- $F \cdot \xi = \sigma(\xi) \cdot F \qquad \forall \xi \in W(k)$
- $V \cdot \sigma(\xi) = \xi \cdot V \qquad \forall \xi \in W(k)$
- $FV = VF = p$

Note that E is a free left, or right, module over $W(k)$ with basis

$$\{\ldots, V^2, V, 1, F, F^2, \ldots\}.$$

Example. If $k = \mathbb{F}_p$, then $E = \mathbb{Z}_p[F,V]/(FV - p)$ is a regular commutative ring of Krull dimension 2. In all other cases, E is non-commutative.

Proposition 23.1. There exist unique ring homomorphisms $E \to \operatorname{Aut}(W_n^m)$ for all m, n such that F and V act as such and $\xi \in W(k)$ acts through multiplication by $\sigma^{-n}(\xi)$. Moreover, these actions of E are compatible with the transition homomorphisms i and v of the direct system.

Proof. For any $\xi \in W(k)$ and $x \in W$, the formulas in Proposition 21.1 imply that $F(\xi x) = \sigma(\xi) \cdot F(x)$ and $\xi \cdot V(x) = V(\sigma(\xi)x)$. On the other hand recall that $V \circ F = F \circ V = p \cdot \mathrm{id}$ by Theorem 14.4. Thus there is a unique action of E

on W, where F and V act as such and $\xi \in W(k)$ acts through multiplication by itself. The above relations also imply that this action induces a unique action of E on W_n and on W_n^m for all n and m. Moreover, the functoriality of F and V shows that the homomorphisms i and r are equivariant.

However, since $V = vr$, the relation $\xi \cdot V(x) = V(\sigma(\xi)x)$ implies that $\xi \cdot v(x) = v(\sigma(\xi)x)$. Thus in order to turn v into an E-linear homomorphism, we must modify the action of $W(k)$ by an appropriate power of σ. This is precisely what we accomplish by letting ξ act on W_n^m through multiplication by $\sigma^{-n}(\xi)$. Then E acts compatibly on the whole direct system. □

Definition. For any finite commutative group scheme G over k of local-local type we define

$$M(G) := \varinjlim_{m,n} \operatorname{Hom}(G, W_n^m),$$

with its induced left E-module structure via the actions of E on the W_n^m. Clearly this defines a left exact additive contravariant functor to the category of left E-modules.

Theorem 23.2. The functor M induces an anti-equivalence of categories

$$\left\{\left\{\begin{array}{c}\text{finite commutative}\\ \text{group schemes over}\\ k \text{ of local-local type}\end{array}\right\}\right\} \xrightarrow{\sim} \left\{\left\{\begin{array}{c}\text{left } E\text{-modules of}\\ \text{finite length with}\\ F \text{ and } V \text{ nilpotent}\end{array}\right\}\right\}.$$

This “main theorem of contravariant Dieudonné theory in the local-local case” is essentially a formal consequence of the results obtained so far. As a preparation note that the action of E on W_n^m via Proposition 23.1 and the embedding of W_n^m into the whole direct system induce homomorphisms of left E-modules

$$E_n^m := E/(EF^m + EV^n) \longrightarrow \operatorname{End}(W_n^m) \longrightarrow M(W_n^m).$$

Proposition 23.3. (a) These homomorphisms are isomorphisms.

(b) $\operatorname{length}_{W(k)} M(G) = \log_p |G|$.

Proof. As $W_n^m \hookrightarrow W_{n'}^{m'}$ is a monomorphism for all $n \leq n'$ and $m \leq m'$, the map $\operatorname{End}(W_n^m) \to M(W_n^m)$ is injective. By Lemma 22.1 it is also surjective, and hence bijective. Next Proposition 16.1 implies that

$$k \xrightarrow{\sim} E/(EF + EV) \xrightarrow{\sim} \operatorname{End}(\boldsymbol{\alpha}_p) \xrightarrow{\sim} M(\boldsymbol{\alpha}_p)$$

and hence (a) for $m = n = 1$. More generally, one easily checks that every non-trivial E-submodule of E_n^m contains the residue class of $F^{m-1}V^{n-1}$ (compare Proposition 23.9 below). Since the image of $F^{m-1}V^{n-1}$ in $\operatorname{End}(W_n^m)$ is non-zero, we deduce that the map $E_n^m \to \operatorname{End}(W_n^m)$ is injective.

Before finishing the proof of (a), we prove (b), using induction on $|G|$. The assertion is trivial when $|G| = 1$, and holds for $G = \boldsymbol{\alpha}_p$ by the above. Whenever $|G| \neq 1$ there exists a short exact sequence

$$0 \longrightarrow G' \longrightarrow G \longrightarrow \boldsymbol{\alpha}_p \longrightarrow 0,$$

and we may assume that (b) holds for G'. The induced sequence

$$(23.4) \qquad 0 \longleftarrow M(G') \longleftarrow M(G) \longleftarrow M(\boldsymbol{\alpha}_p) \longleftarrow 0$$

is exact except possibly at $M(G')$. To prove the exactness there consider any element of $M(G')$, say represented by a homomorphism $\varphi : G' \to W_n^m$ for some m, n. Consider the morphism of short exact sequences

$$\begin{tikzcd}
0 \arrow[r] & G' \arrow[r] \arrow[d, "\varphi"'] & G \arrow[r] \arrow[d] & \boldsymbol{\alpha}_p \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & W_n^m \arrow[r] & H \arrow[r] & \boldsymbol{\alpha}_p \arrow[r] & 0
\end{tikzcd}$$

where H is the pushout of the left hand square. Applying Proposition 22.2 to the lower exact sequence yields a homomorphism $H \to W_{n+1}^{m+1}$ extending the homomorphism $iv\colon W_n^m \to W_{n+1}^{m+1}$. The composite homomorphism $G \to H \to W_{n+1}^{m+1}$ then defines an element of $M(G)$ which maps to the given element of $M(G')$. This proves that the sequence (23.4) is exact, and hence

$$\begin{aligned}
\operatorname{length}_{W(k)} M(G) &= \operatorname{length}_{W(k)} M(G') + \operatorname{length}_{W(k)} M(\boldsymbol{\alpha}_p) \\
&= \log_p |G'| + \log_p |\boldsymbol{\alpha}_p| \\
&= \log_p |G|,
\end{aligned}$$

proving (b).

Returning to (a) one directly calculates that $\operatorname{length}_{W(k)} E_n^m = nm$. By (b) and the beginning of §22, we also have $\operatorname{length}_{W(k)} M(W_n^m) = nm$. Thus $E_n^m \to \operatorname{End}(W_n^m)$ is an injective homomorphism of E-modules of equal finite length; hence it is an isomorphism, finishing the proof of (a). □

Lemma 23.5. The functor M is exact.

Proof. By construction it is left exact. For any exact sequence $0 \to G' \to G \to G'' \to 0$, Proposition 23.3 (b) and the multiplicativity of group orders imply that the image of the induced map $M(G) \to M(G')$ has the same finite length over $W(k)$ as $M(G')$ itself. Thus the map is surjective, and M is exact. □

Lemma 23.6. If $F^m_G = 0$ and $V^n_G = 0$, then F^m and V^n annihilate $M(G)$. In particular, the functor M lands in the indicated subcategory.

Proof. The first assertion follows from the definition of $M(G)$ and the functoriality of F and V, the second from the first and Proposition 23.3 (b). □

Lemma 23.7. The functor M is fully faithful.

Proof. For given G, H choose m, n such that F^m and V^n annihilate G, H, and abbreviate $U := W^m_n$. By Proposition 22.6, we may choose a copresentation

$$0 \longrightarrow H \longrightarrow U^r \longrightarrow U^s$$

for some r, s. By the exactness of M, we obtain a presentation of E-modules

$$0 \longleftarrow M(H) \longleftarrow M(U)^r \longleftarrow M(U)^s.$$

Applying the left exact functors $\operatorname{Hom}(G, -)$ and $\operatorname{Hom}_E(-, M(G))$, we obtain a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Hom}(G,H) \arrow[r] \arrow[d, "M"'] & \operatorname{Hom}(G,U^r) \arrow[r] \arrow[d, "M"'] & \operatorname{Hom}(G,U^s) \arrow[d, "M"'] \\
0 \arrow[r] & \operatorname{Hom}_E(M(H),M(G)) \arrow[r] & \operatorname{Hom}_E(M(U^r),M(G)) \arrow[r] & \operatorname{Hom}_E(M(U^s),M(G))
\end{tikzcd}$$

where the vertical arrows are induced by the functor M. We must prove that the left vertical arrow is bijective. By the 5-Lemma it suffices to show that the other vertical arrows are bijective. Since M is an additive functor, this in turn reduces to direct summands of U^r and U^s. All in all, it suffices to prove the bijectivity in the case that $H = U = W^m_n$. For this consider the following commutative diagram:

$$\begin{tikzcd}
\operatorname{Hom}(G,W^m_n) \arrow[r, "M"] \arrow[d] & \operatorname{Hom}_E(M(W^m_n),M(G)) \arrow[d, "\wr"', "23.3\ (a)"] \\
M(G) & \operatorname{Hom}_E(E^m_n,M(G)) \arrow[l, "\varphi([1]) \mapsfrom \varphi"']
\end{tikzcd}$$

Here the left vertical arrow is simply that induced by the embedding of W^m_n into the whole direct system; hence it is an isomorphism by Lemma 22.1. The lower horizontal arrow is an isomorphism by Lemma 23.6. Thus the upper horizontal arrow is an isomorphism, as desired. □

Lemma 23.8. The functor M is essentially surjective.

Proof. Let N be a left E-module of finite length with F and V nilpotent. Suppose that F^m and V^n annihilate N. Then there exists an epimorphism of E-modules $(E_n^m)^{\oplus r} \twoheadrightarrow N$ for some r. Its kernel is again annihilated by F^m and V^n; hence there exists a presentation

$$(E_n^m)^{\oplus s} \xrightarrow{\varphi} (E_n^m)^{\oplus r} \longrightarrow N \longrightarrow 0.$$

Since $E_n^m = M(W_n^m)$ and M is fully faithful, we see that $\varphi = M(\psi)$ for a unique homomorphism $(W_n^m)^{\oplus r} \xrightarrow{\psi} (W_n^m)^{\oplus s}$. Setting $G(N) := \ker(\psi)$, the 5-Lemma shows that $N \cong M(G(N))$. □

Piecing together the above results, we see that Theorem 23.2 is proven.

Proposition 23.9. "$\varinjlim_{m,n} W_n^m$" is the injective hull of $\boldsymbol{\alpha}_p$ in the associated category of ind-objects.

Proof. It is injective, because $\mathrm{Hom}(-, \text{“}\varinjlim_{m,n} W_n^m\text{”}) = M(-)$ is an exact functor. To show that is a hull, we must prove that any non-trivial subgroup scheme $G \subset W_n^m$ contains $i^{m-1}v^{n-1}(W_1^1) \cong \boldsymbol{\alpha}_p$. For this note first that W_n^m, and hence G, is an extension of copies of $\boldsymbol{\alpha}_p$. In particular there exists a monomorphism $\boldsymbol{\alpha}_p \hookrightarrow G$. On the other hand, Lemma 22.1 implies that $i^{m-1}v^{n-1}$ induces an isomorphism $\mathrm{Hom}(\boldsymbol{\alpha}_p, W_1^1) \xrightarrow{\sim} \mathrm{Hom}(\boldsymbol{\alpha}_p, W_n^m)$. Thus $i^{m-1}v^{n-1}(W_1^1)$ is the only copy of $\boldsymbol{\alpha}_p$ inside W_n^m, and so this copy must be contained in G, as desired. □

Remark. For any abelian category $\mathfrak{C}$ with an injective cogenerator I one has a faithful exact contravariant functor $X \mapsto \mathrm{Hom}_{\mathfrak{C}}(X, I)$ to the category of left modules over $\mathrm{End}_{\mathfrak{C}}(I)$. If $\mathfrak{C}$ is artinian, i.e., if every object has finite length, one can show that this defines an anti-equivalence of categories from $\mathfrak{C}$ to the category of left modules of finite length over $\mathrm{End}_{\mathfrak{C}}(I)$. Above we have essentially done this for the category of finite commutative group schemes annihilated by F^m and V^n, with $I = W_n^m$ and $\mathrm{End}_{\mathfrak{C}}(I) = E_n^m$, and then taken the limit over all m, n.

Remark. Instead of the contravariant functor M above, one can define a covariant functor $G \mapsto \varinjlim_{m,n} \mathrm{Hom}(W_n^m, G)$ landing in right E-modules, where the W_n^m are viewed as an inverse system with transition epimorphisms r and f, and on which the action of $W(k)$ must be defined differently. The "main theorem of *covariant* Dieudonné theory in the local-local case" is then the direct analogue of Theorem 23.2 and can be proved similarly. It can also be deduced from Theorem 23.2 itself by showing that $N \mapsto \varinjlim_{m,n} \mathrm{Hom}_E(N, E_n^m)$ defines an antiequivalence between left and right E-modules of finite length with F and V nilpotent.

Lecture 11

January 13, 2005
Notes by Ivo Dell'Ambrogio

§24 Pairings and Cartier duality

Logically, this section could have followed right after §4. Let G, G' and H be commutative group schemes over a scheme S.

Definition. A morphism $G' \times_S G \to H$ of schemes over S is called *bilinear* if it is additive in each factor, or equivalently, if for every scheme T over S the induced map $G'(T) \times G(T) \to H(T)$ is bilinear in the usual sense. The group of such bilinear morphisms will be denoted by $\mathrm{Bilin}_S(G' \times_S G, H)$.

Definition. Denote by $\underline{\mathrm{Hom}}_S(G, H)$ the contravariant functor

$$\mathfrak{Sch}_S \to \mathfrak{Ab},\ T \mapsto \underline{\mathrm{Hom}}_S(G, H)(T) := \mathrm{Hom}_T(G_T, H_T).$$

If it is representable, the representing group scheme over S will also be denoted by $\underline{\mathrm{Hom}}_S(G, H)$.

Note. One can show that $\underline{\mathrm{Hom}}_S(G, H)$ is representable whenever G is finite and flat over S. Unfortunately, the detailed study of $\mathrm{Bilin}_S(G' \times_S G, H)$ and $\underline{\mathrm{Hom}}_S(G, H)$ is beyond the scope of this course because of time constraints.

Proposition 24.1 (Adjunction formula). There exists an isomorphism

$$\mathrm{Bilin}_S(G' \times_S G, H) \cong \mathrm{Hom}_S(G', \underline{\mathrm{Hom}}_S(G, H)),$$

which is functorial in all variables. This of course determines $\underline{\mathrm{Hom}}_S(G, H)$ up to natural isomorphism.

Proof. By definition giving a morphism $\varphi\colon G' \to \underline{\mathrm{Hom}}_S(G, H)$ is equivalent to giving a homomorphism $\varphi'\colon G' \times_S G \longrightarrow G' \times_S H$ of group schemes over G'. Thus φ' must be a morphism of schemes over S whose first component is the projection to G' and whose second component is a morphism $\psi\colon G' \times_S G \to H$ that is additive in G. Moreover, one easily checks that φ is additive if and only if ψ is additive in G'. This sets up the desired bijection, and one easily checks that it is a group isomorphism and functorial in all variables. □

Definition. A bilinear morphism $\beta : G' \times_S G \to H$ is *nondegenerate at* G' if, for all $T \to S$ and all $0 \neq g' \in G'(T)$, the homomorphism $\beta(g', -) : G_T \to H_T$ is nontrivial. One similarly defines the notion *nondegenerate at* G.

Note. It is clear that β is nondegenerate at G' if and only if the associated homomorphism $G' \to \underline{\mathrm{Hom}}_S(G, H)$ is a monomorphism.

Proposition 24.2. If G is finite flat over S, there is a functorial isomorphism $\underline{\mathrm{Hom}}_S(G, \mathbb{G}_{m,S}) \cong G^*$, and in particular $\underline{\mathrm{Hom}}_S(G, \mathbb{G}_{m,S})$ is representable.

Proof. For all schemes T over S we must construct a natural isomorphism $\mathrm{Hom}_T(G_T, \mathbb{G}_{m,T}) \cong G^*(T)$. By passing to an affine covering of T it suffices to do this when T itself is affine. After replacing $G \to S$ by $G_T \to T$, we may also assume that $T = S$. As usual, we then write $S = \operatorname{Spec} R$, $G = \operatorname{Spec} A$, and $G^* = \operatorname{Spec} A^*$, where $A^* = \mathrm{Hom}_R(A, R)$. By definition, $\mathrm{Hom}_S(G, \mathbb{G}_{m,S})$ is the group of morphisms $\varphi\colon G \to \mathbb{G}_{m,S}$ of schemes over S such that the left hand side of the following diagram commutes:

$$\begin{tikzcd}
G \times_S G \arrow[r, "m"] \arrow[d, "\varphi\times\varphi"'] & G \arrow[d, "\varphi"'] & S \arrow[l, "\epsilon"'] \arrow[dl, "1"] \\
\mathbb{G}_{m,S} \times_S \mathbb{G}_{m,S} \arrow[r, "m"] & \mathbb{G}_{m,S} &
\end{tikzcd}$$

Since every homomorphism maps the unit element to the unit element, the whole diagram then commutes. Next, these morphisms are in bijection to morphisms $\varphi : G \to \mathbb{A}^1_S$ of schemes over S such that

$$\begin{tikzcd}
G \times_S G \arrow[r, "m"] \arrow[d, "\varphi\times\varphi"'] & G \arrow[d, "\varphi"'] & S \arrow[l, "\epsilon"'] \arrow[dl, "1"] \\
\mathbb{A}^1_S \times_S \mathbb{A}^1_S \arrow[r, "m"] & \mathbb{A}^1_S &
\end{tikzcd}$$

commutes; in fact, every such $\varphi : G \to \mathbb{A}^1_S$ automatically lands inside $\mathbb{G}_{m,S}$, because for every point g of G we have $\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(\epsilon) = 1$, showing that $\varphi(g)$ is invertible. These morphisms in turn correspond to R-algebra homomorphisms $R[T] \to A$ such that

$$\begin{tikzcd}
A \otimes A & A \arrow[l, "m"'] \arrow[r, "\epsilon"] & R \\
R[T] \otimes R[T] \arrow[u] & R[T] \arrow[l, "T\otimes T \leftarrow\!\shortmid T"'] \arrow[u] \arrow[ur, "T\mapsto 1"'] &
\end{tikzcd}$$

commutes. But giving an R-algebra homomorphism $R[T] \to A$ is equivalent to giving the image a of T, so we obtain a bijection to the set

$$\big\{a \in A \;\big|\; m(a) = a \otimes a,\ \epsilon(a) = 1\big\}.$$

By biduality $A \cong A^{**}$ we can identify this with the set

$$\bigl\{\alpha \in \mathrm{Hom}_R(A^*, R) \;\big|\; \forall \ell, \ell' \in A^* \colon\ \alpha(m^*(\ell \otimes \ell')) = \alpha(\ell) \cdot \alpha(\ell'),\ \alpha(\epsilon^*(1)) = 1\bigr\}.$$

Finally, these conditions say precisely that $\alpha \colon A^* \to R$ is a homomorphism of R-algebras, i.e., corresponding to a point in $G^*(S)$. The additivity and functoriality are left to the reader. □

Proposition 24.3. If G' and G are both finite flat over S, then a bilinear morphism $\beta : G' \times_S G \to \mathbb{G}_{m,S}$ is nondegenerate at G' and G if and only if its adjoint $G' \to \underline{\mathrm{Hom}}_S(G, \mathbb{G}_{m,S}) = G^*$ is an isomorphism.

Proof. We have seen that β is nondegenerate at G' if and only if its adjoint $\varphi : G' \to G^*$ is a monomorphism. Similarly, β is nondegenerate at G if and only if its adjoint (after having swapped G' and G!) $\varphi' : G \to G'^*$ is a monomorphism. After the conscientious reader has checked that $\varphi' = \varphi^*$, she will see that the second fact is equivalent to φ being an epimorphism. □

§25 Cartier duality of finite Witt group schemes

From this section onwards we will again work over a perfect field k of characteristic $p > 0$. Our aim is to construct natural isomorphisms $(W_m^n)^* \cong W_n^m$ for all m and n and to describe their relation with the action of E and with all transition maps. The existence of an isomorphism $(W_m^n)^* \cong W_n^m$ alone can be proved without the following technicalities, merely by characterizing W_n^m up to isomorphism by a few simple properties. This makes a nice exercise for the interested reader.

By Proposition 24.3 it suffices to construct a nondegenerate pairing $W_n^m \times W_m^n \to \mathbb{G}_{m,k}$, and for this we use the multiplication of Witt vectors. Recall our notation $W_n = W/V^nW$ and $W_n^m = \ker(F^m|W_n)$. For all n and m consider the morphisms

$$\tau_n^m : W_n^m \to W,\ (x_0, \ldots, x_{n-1}) \mapsto (x_0, \ldots, x_{n-1}, 0, 0, \ldots).$$

Their images form a system of infinitesimal neighborhoods of 0 inside W, and we are interested in the formal scheme $\widehat{W} := \bigcup_{n,m} \tau_n^m(W_n^m)$. Its points over any k-algebra R are the elements $\underline{x} \in W(R)$ such that all components x_i are nilpotent and almost all are zero.

Lemma 25.1. (a) Addition in W induces a morphism $\widehat{W} \times \widehat{W} \to \widehat{W}$.
(b) Multiplication in W induces a morphism $W \times \widehat{W} \to \widehat{W}$.
In other words, $\widehat{W}(R)$ is an ideal in $W(R)$ for all R.

Proof. The phantom component $\Phi_n(\underline{x}) = x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^n x_n$ is an isobaric polynomial of degree p^n, if we set $\deg(x_i) = p^i$. Recall that addition in W is given by $\underline{x} + \underline{y} = \underline{s} = (s_0, s_1, \ldots)$, where the s_i are polynomials in $\mathbb{Z}[\underline{x}, \underline{y}]$ characterized by $\Phi_n(\underline{s}) = \Phi_n(\underline{x}) + \Phi_n(\underline{y})$, this last being the usual addition. Thus $\Phi_n(\underline{s})$ is isobaric of degree p^n when $\deg(x_i) = \deg(y_i) = p^i$, which in turn implies by induction that s_n is isobaric of degree p^n. Plugging in any $\underline{x}$, $\underline{y} \in \widehat{W}(R)$, we deduce that $s_i(\underline{x}, \underline{y})$ is nilpotent for all i and that it is zero for $i \gg 0$. This proves (a).

For (b) we similarly note that multiplication in W is given by $\underline{x} \cdot \underline{y} = \underline{p} = (p_0, p_1, \ldots)$, where $\Phi_n(\underline{p}) = \Phi_n(\underline{x}) \cdot \Phi_n(\underline{y})$. One finds that $p_n \in \mathbb{Z}[\underline{x}, \underline{y}]$ is isobaric of degree p^n when $\deg(y_i) = p^i$ and $\deg(x_i) = 0$, and then one concludes with the same argument. □

Note. Lemma 25.1 (a) defines an additive group structure on the formal scheme $\widehat{W}$, making it a "group formal scheme", that is, a group object in the category of formal schemes. However, the morphisms $\tau_n^m \colon W_n^m \to \widehat{W}$ are no group homomorphisms and their images no group subschemes, so $\widehat{W}$ should not be confused with the ind-object "$\varinjlim_{m,n} W_n^m$" from Proposition 23.9!

Lemma 25.2. (a) The Artin-Hasse exponential induces a group homomorphism $\widehat{W} \to \mathbb{G}_{m,k}$, $\underline{x} \mapsto E(\underline{x}, 1)$.
(b) For all $\underline{x} \in W(R)$ and $\underline{y} \in \widehat{W}(R)$, we have $E\big((V\underline{x}) \cdot \underline{y}, 1\big) = E\big(\underline{x} \cdot (F\underline{y}), 1\big)$.
(c) For all $n \geq 1$, all $\underline{x}, \underline{x}' \in W(R)$ with the same image in $W_n(R)$, and all $\underline{y} \in \widehat{W}(R)$ such that $F^n\underline{y} = 0$, we have $E(\underline{x} \cdot \underline{y}, 1) = E(\underline{x}' \cdot \underline{y}, 1)$.

Proof. (a) By definition $E(\underline{x}, t) = \prod_{n \geq 0} F(x_n t^{p^n}) \in 1 + t\mathbb{Z}[\underline{x}][[t]]$, where $F(t) = 1 - t \pm \cdots \in 1 + t\mathbb{Z}_{(p)}[[t]]$. Thus for any $\underline{x} \in \widehat{W}(R)$ the series $E(\underline{x}, t)$ is actually a polynomial in t with constant term 1. In particular it can be evaluated at $t = 1$, yielding an element $E(\underline{x}, 1) \in \mathbb{G}_m(R)$. Thus the morphism in question is defined, and it is a homomorphism because E itself defines a group homomorphism from $W = W_k$ to the multiplicative group scheme $\Lambda_k =$ "$1 + t\mathbb{A}_k^1[[t]]$".

(b) follows from Proposition 21.1 (g) by setting $t = 1$.

(c) By assumption $\underline{x} - \underline{x}'$ maps to zero in $W_n(R)$, so it must be of the form $\underline{x} - \underline{x}' = V^n\underline{z}$ for some $\underline{z} \in W(R)$. Thus $\underline{x} = \underline{x}' + V^n\underline{z}$. We deduce that

$$E\big(\underline{x}\underline{y}, 1\big) = E\big((\underline{x}' + V^n\underline{z})\underline{y}, 1\big) = E\big(\underline{x}'\underline{y} + (V^n\underline{z})\underline{y}, 1\big) = E\big(\underline{x}'\underline{y}, 1\big) \cdot E\big((V^n\underline{z})\underline{y}, 1\big),$$

where we have also used the distributive law in W, Lemma 25.1, and the homomorphy of E. But (b) implies that the last factor is

$$E\big((V^n\underline{z})\underline{y}, 1\big) = E(\underline{z}(F^n\underline{y}), 1) = 1,$$

since $F^n\underline{y} = 0$ by assumption. □

Theorem 25.3. For all $n, m \geq 1$ there is a well-defined nondegenerate bilinear morphism

$$W_n^m \times W_m^n \to \mathbb{G}_{m,k}, \ (\underline{x}, \underline{y}) \mapsto \langle \underline{x}, \underline{y} \rangle := E\big(\tau_n^m(\underline{x}) \cdot \tau_m^n(\underline{y}), 1\big),$$

and it satisfies the following relations:
(a) $\langle \underline{x}, \underline{y} \rangle = \langle \underline{y}, \underline{x} \rangle$,
(b) $\langle v\underline{x}, \underline{y} \rangle = \langle \underline{x}, f\underline{y} \rangle$,
(c) $\langle r\underline{x}, \underline{y} \rangle = \langle \underline{x}, i\underline{y} \rangle$,
(d) $\langle V\underline{x}, \underline{y} \rangle = \langle \underline{x}, F\underline{y} \rangle$,
(e) $\langle \xi\underline{x}, \underline{y} \rangle = \langle \underline{x}, \xi\underline{y} \rangle$ for all $\xi \in W(k)$.
In particular, its adjoint is a canonical isomorphism $W_n^m \xrightarrow{\sim} (W_m^n)^*$.

Proof. Lemmas 25.1 (b) and 25.2 (a) imply that the morphism is well-defined. To see that it is bilinear, consider any $\underline{x}, \underline{x}' \in W_n^m(R)$ and $\underline{y} \in W_m^n(R)$. Then $\tau_n^m(\underline{x}+\underline{x}')$ and $\tau_n^m(\underline{x})+\tau_n^m(\underline{x}')$, even though they might be different in $\widehat{W}(R)$, have the same image in $W_n(R)$. Thus using Lemma 25.2 (a) and (c) one directly computes that $\langle \underline{x} + \underline{x}', \underline{y} \rangle = \langle \underline{x}, \underline{y} \rangle + \langle \underline{x}', \underline{y} \rangle$, as desired.

The same reasoning with $\tau_n^m(\xi\underline{x})$ and $\xi \cdot \tau_n^m(\underline{x})$ works for (e), and with $\tau_n^m(r\underline{x})$ and $\tau_{n+1}^m(\underline{x})$ for $\underline{x} \in W_{n+1}^m(R)$ it works for (c). Part (b) results from the calculation

$$\begin{aligned} \langle v\underline{x}, \underline{y} \rangle \ &= \ E\big(\tau_{n+1}^m(v\underline{x}) \cdot \tau_m^{n+1}(\underline{y}), 1\big) \ = \ E\big((V\tau_n^m(\underline{x})) \cdot \tau_m^{n+1}(\underline{y}), 1\big) \\ &\overset{25.2\,(b)}{=} E\big(\tau_n^m(\underline{x}) \cdot (F\tau_m^{n+1}(\underline{y})), 1\big) \ = \ E\big(\tau_n^m(\underline{x}) \cdot \tau_m^n(f\underline{y}), 1\big) \ = \ \langle \underline{x}, f\underline{y} \rangle \end{aligned}$$

for any $\underline{x} \in W_n^m(R)$ and $\underline{y} \in W_m^{n+1}(R)$. Moreover, (a) is obvious, and (d) follows from (b) and (c) and the relations $V = rv$ and $F = fi$ from §22.

It remains to prove nondegeneracy, and for this we begin with the case $n = m = 1$. Since $W_1^1 = \boldsymbol{\alpha}_p$ is simple, it suffices to prove that the pairing is nontrivial. But in this case we have

$$\langle x, y \rangle \ = \ E\big(\tau_1^1(x) \cdot \tau_1^1(y), 1\big) \overset{20.7}{=} E\big(\tau_1^1(xy), 1\big) \ = \ F(xy) \ = \ 1 - xy \pm \ldots,$$

which is not identically 1 for (x, y) in $\boldsymbol{\alpha}_p \times \boldsymbol{\alpha}_p$, as desired.

The general case can be deduced from this in two ways. One way is to perform induction over n and m, by relating the short exact sequences from the beginning of §22 and their Cartier duals, using the adjunctions in (b) and (c), and then applying the five lemma. Another way is to first show that every non-zero subgroup scheme $G \subset W_n^m$ contains $i^{m-1}v^{n-1}(W_1^1)$. Indeed, this follows at once from Lemma 22.1 and the fact that G must possess a subgroup scheme isomorphic to $\boldsymbol{\alpha}_p \cong W_1^1$. By symmetry, it is then enough to show that $\langle -, - \rangle$ is non-trivial on $i^{m-1}v^{n-1}(W_1^1) \times W_m^n$, which follows from the special case $n = m = 1$ by (b) and (c). □

Lecture 12

Januar 28, 2005
Notes by Alexander Caspar

§26 Duality and the Dieudonné functor

Let k be a perfect field of characteristik $p > 0$ and $W(k)$ its ring of Witt vectors, and consider the torsion $W(k)$-module

$$T := W(k)\big[\tfrac{1}{p}\big]/W(k).$$

Proposition 26.1. The functor

$$N \mapsto N^* := \mathrm{Hom}_{W(k)}(N, T)$$

defines an anti-equivalence from the category of finite length $W(k)$-modules to itself, and there is a functorial isomorphism

$$N \cong (N^*)^*.$$

Proof. The biduality homomorphism $N \to (N^*)^*$ is obtained by resolving the evaluation pairing $N \times N^* \to T$. It suffices to prove that this homomorphism is an isomorphism; everything else then follows. Since the functor is additive, and every N is a direct sum of cyclic modules, it suffices to prove the isomorphy in the case $N = W(k)/p^n\, W(k)$. But that is straightforward. □

We denote by σ the endomorphism of T that is induced by F, the Frobenius on $W(k)$. Let E be the ring of "noncommutative polynomials" over $W(k)$ in the two variables F and V with the relations as defined in §23. For any left E-module N we define maps $F, V : N^* \to N^*$ by

$$\ell \mapsto F\ell,\ n \mapsto (F\ell)(n) := \sigma(\ell(Vn)),$$

$$\ell \mapsto V\ell,\ n \mapsto (V\ell)(n) := \sigma^{-1}(\ell(Fn)).$$

As F is σ-linear and V is σ^{-1}-linear with respect to $W(k)$, the twists by $\sigma^{\pm 1}$ on the right hand side are precisely those necessary to make $F\ell$ and $V\ell$ again $W(k)$-linear. One easily calculates that together with the usual $W(k)$-action on N^*, this turns N^* into a left E-module.

Proposition 26.2. The functor $N \mapsto N^*$ defines an anti-equivalence from the category of finite length left E-modules to itself, and there is a functorial isomorphism

$$N \cong (N^*)^*.$$

Proof. This is a direct consequence of Proposition 26.1. □

The aim of this section is to show:

Theorem 26.3. For any local-local commutative group scheme G there is a functorial isomorphism of E-modules

$$M(G^*) \cong M(G)^*.$$

Note. The idea behind the proof is to reduce the general case to the case $G = W_n^n$ and to use the isomorphism $(W_n^n)^* \cong W_n^n$ from Theorem 25.3.

We start with the isomorphisms from Proposition 23.3 (a)

$$E_n^n := E/(EF^n + EV^n) \cong \mathrm{End}(W_n^n) \cong M(W_n^n). \tag{26.4}$$

We denote the residue class of $e \in E$ in E_n^n by $[e]$.

Note that E_n^n is an algebra quotient of E, that is noncommutative in general. We will always consider E_n^n as a *left* E-module. Multiplication on the right by any $e \in E$ induces an endomorphism of left E-modules, which we denote by $\rho_e : E_n^n \to E_n^n$. Recall that by definition any $\xi \in W(k)$ acts on W_n^n through multiplication by $\sigma^{-n}(\xi)$; we denote this endomorphism by $\mu_{\sigma^{-n}(\xi)} : W_n^n \to W_n^n$. For the later use we observe that under the isomorphisms (26.4) the following endomorphisms correspond:

(26.5)

action on \ of	$\xi \in W(K)$	F	V
$M(W_n^n)$	$M(\mu_{\sigma^{-n}(\xi)})$	$M(F)$	$M(V)$
$\wr\|$			
$\mathrm{End}(W_n^n)$	$(\_) \circ \mu_{\sigma^{-n}(\xi)}$	$(\_) \circ F$	$(\_) \circ V$
$\wr\|$			
E_n^n	ρ_ξ	ρ_F	ρ_V

Next we determine the relation with the epimorphism $fr : W_{n+1}^{n+1} \to W_n^n$.

Lemma 26.6. The following diagram commutes:

$$\begin{tikzcd}
M(W_n^n) \arrow[r, hook, "M(fr)"] & M(W_{n+1}^{n+1}) \\
\wr\| & \wr\| \\
\mathrm{End}(W_n^n) \arrow[r, hook, "iv\circ(\_)\circ fr"] & \mathrm{End}(W_{n+1}^{n+1}) \\
\wr\| & \wr\| \\
E_n^n \arrow[r, hook, "{[p]: [e]\mapsto[pe]}"] & E_{n+1}^{n+1}.
\end{tikzcd}$$

Proof. The top square commutes, because $iv : W_n^n \hookrightarrow W_{n+1}^{n+1}$ induces the transition map in the direct system defining M. For the bottom square, since all arrows are E-module homomorphisms, it suffices to prove the commutativity for the generator [1]. But this follows from:

$$\begin{tikzcd}
\mathrm{id} \arrow[r, mapsto] & ivfr = VF = p \cdot \mathrm{id} \\
{[1]} \arrow[u, mapsto] \arrow[r, mapsto] & {[p].} \arrow[u, mapsto]
\end{tikzcd}$$

□

By the self-duality $(W_n^n)^* \cong W_n^n$ and the isomorphisms 26.4, Theorem 26.3 in the special case $G = W_n^n$ amounts to an isomorphism of left E-modules $(E_n^n)^* \cong E_n^n$. Our next job is to construct such an isomorphism directly. First we decompose E_n^n as a left $W(k)$-module as

$$E_n^n = \bigoplus_{|i|<n} W(k)/p^{n-|i|}W(k) \cdot \begin{cases} [F^{|i|}], & i \geq 0, \\ [V^{|i|}], & i \leq 0. \end{cases} \tag{26.7}$$

We define a left $W(k)$-bilinear pairing

$$\langle \_, \_ \rangle_n : E_n^n \times E_n^n \to T,$$

by setting

$$\langle [F^i], [F^i] \rangle_n := \langle [V^i], [V^i] \rangle_n := [p^{-(n-i)}],$$

for any $0 \leq i \leq n$ and mapping all the other pairs of generators to zero.

Lemma 26.8. This is a symmetric, perfect bilinear pairing of left $W(k)$-modules, and it satisfies the following relations for all $e, e' \in E$ and $\xi \in W(k)$:

(a) $\langle [Fe], [e'] \rangle_n = \sigma\left(\langle [e], [Ve'] \rangle_n\right)$

(b) $\langle [eF], [e'] \rangle_n = \langle [e], [e'V] \rangle_n$

(c) $\langle [e\xi], [e'] \rangle_n = \langle [e], [e'\xi] \rangle_n$

(d) $\langle [pe], [e'] \rangle_{n+1} = \langle [e], [e'] \rangle_n$

Proof. The first statement follows directly from the construction. It is enough to prove the remaining formulas when e and e' are $W(k)$-multiples of classes of generators. For example, for $\alpha, \beta \in W(k)$ and $0 \leq i \leq n$ we have

$$\langle [F\alpha F^i], [\beta F^{i+1}] \rangle_n = \langle [\sigma(\alpha) F^{i+1}], [\beta F^{i+1}] \rangle_n = [\sigma(\alpha)\beta p^{-(n-i-1)}] \text{ and}$$

$$\sigma\left(\langle[\alpha F^i],[V\beta F^{i+1}]\rangle_n\right) = \sigma\left(\langle[\alpha F^i],[\sigma^{-1}(\beta)pF^i]\rangle_n\right) = \sigma\left([\alpha\sigma^{-1}(\beta)pp^{-(n-i)}]\right),$$

which are equal. Together with similar calculations this proves (a). (b) is proved in the same way, except that no twist by σ occurs, because F and V are multiplied from the right. What happens in (c) is illustrated by the typical case:

$$\begin{aligned}\langle[F^i\xi],[F^i]\rangle_n &= \langle[\sigma^i(\xi)F^i],[F^i]\rangle_n = [\sigma^i(\xi)p^{-(n-i)}] \\ &= \langle[F^i],[\sigma^i(\xi)F^i]\rangle_n = \langle[F^i],[F^i\xi]\rangle_n.\end{aligned}$$

Finally, (d) is also straightforward. □

Lemma 26.9. The pairing $\langle\_,\_\rangle_n$ induces a left E-linear isomorphism

$$E_n^n \cong (E_n^n)^*.$$

Proof. By the first assertion of Lemma 26.8 only the compatility with F and V needs to be checked. But that follows at once from 26.8 (a), from the symmetry of the pairing, and the definition of the action of F and V on $(E_n^n)^*$. □

Now we can construct the isomorphism in Theorem 26.3. Fix a local-local G and take any $n \gg 0$ such that F^n and V^n annihilate G. Then they also annihilate G^* and $M(G^*)$ and $M(G)^*$. We obtain the following sequence of isomorphisms

$$\begin{aligned}M(G^*) &\cong \operatorname{Hom}(G^*, W_n^n) \\ &\overset{25.3}{\cong} \operatorname{Hom}(G^*, (W_n^n)^*) \\ &\overset{\text{Cartier duality}}{\cong} \operatorname{Hom}(W_n^n, G) \\ &\overset{23.2}{\cong} \operatorname{Hom}_E(M(G), M(W_n^n)) \\ &\overset{26.4}{\cong} \operatorname{Hom}_E(M(G), E_n^n) \\ &\overset{26.2}{\cong} \operatorname{Hom}_E((E_n^n)^*, M(G)^*) \\ &\overset{26.9}{\cong} \operatorname{Hom}_E(E_n^n, M(G)^*) \\ &\overset{\text{evaluate at }[1]\in E_n^n}{\cong} \{\ell \in M(G)^* | F^n\ell = V^n\ell = 0\} \\ &= M(G)^*.\end{aligned}$$

Clearly the composite isomorphism is functorial in G. It remains to show that it is E-linear and independent of n. To prove that it is E-linear we trace the action through the whole sequence of isomorphisms:

action on \ of	$\xi \in W(K)$	F	V	explanation
$\mathrm{Hom}(G^*, W_n^n)$	$\mu_{\sigma^{-n}(\xi)} \circ (\_)$	$F \circ (\_)$	$V \circ (\_)$	
$\wr\Vert$				Theorem 25.3 (a,d,e)
$\mathrm{Hom}(G^*, (W_n^n)^*)$	$\mu^*_{\sigma^{-n}(\xi)} \circ (\_)$	$V^* \circ (\_)$	$F^* \circ (\_)$	
$\wr\Vert$				Functoriality of Cartier duality
$\mathrm{Hom}(W_n^n, G)$	$(\_) \circ \mu_{\sigma^{-n}(\xi)}$	$(\_) \circ V$	$(\_) \circ F$	
$\wr\Vert$				Functoriality of M
$\mathrm{Hom}_E(M(G), M(W_n^n))$	$M(\mu_{\sigma^{-n}(\xi)}) \circ (\_)$	$M(V) \circ (\_)$	$M(F) \circ (\_)$	
$\wr\Vert$				Table (26.5)
$\mathrm{Hom}_E(M(G), E_n^n)$	$\rho_\xi \circ (\_)$	$\rho_V \circ (\_)$	$\rho_F \circ (\_)$	
$\wr\Vert$				Functoriality of $(\_)^*$ from Lemma 26.2
$\mathrm{Hom}_E((E_n^n)^*, M(G)^*)$	$(\_) \circ \rho^*_\xi$	$(\_) \circ \rho^*_V$	$(\_) \circ \rho^*_F$	
$\wr\Vert$				Lemma 26.8 (b,c)
$\mathrm{Hom}_E(E_n^n, M(G)^*)$	$(\_) \circ \rho_\xi$	$(\_) \circ \rho_F$	$(\_) \circ \rho_V$	
$\wr\Vert$				explicit calculation, see below
$M(G)^*$	ξ	F	V	

The explicit calculation verifying the last step is the commutativity of the following diagram for any $\varphi \in \mathrm{Hom}_E(E_n^n, M(G)^*)$ and any $e \in E$:

$$\begin{tikzcd}
\varphi \arrow[r, mapsto] \arrow[d, mapsto] & \varphi(\_ \cdot e) \arrow[d, mapsto] \\
\varphi([1]) \arrow[r, mapsto] & e \cdot \varphi([1]) \ = \ \varphi([e]).
\end{tikzcd}$$

Finally, the following commutative diagram gives the independence of n:

$$\begin{tikzcd}
\mathrm{Hom}(G^*, W_n^n) \arrow[r, hook, "iv\circ(\cdot)"] & \mathrm{Hom}(G^*, W_{n+1}^{n+1}) & \\
\wr\Vert & \wr\Vert & \text{Theorem 25.3 (b,c)} \\
\mathrm{Hom}(G^*, (W_n^n)^*) \arrow[r, hook, "(fr)^*\circ(\cdot)"] & \mathrm{Hom}(G^*, (W_{n+1}^{n+1})^*) & \text{Functoriality of} \\
\wr\Vert & \wr\Vert & \text{Cartier duality} \\
\mathrm{Hom}(W_n^n, G) \arrow[r, hook, "(\cdot)\circ fr"] & \mathrm{Hom}(W_{n+1}^{n+1}, G) & \\
\wr\Vert & \wr\Vert & \text{Functoriality of } M \\
\mathrm{Hom}_E(M(G), M(W_n^n)) \arrow[r, hook, "M(fr)\circ(\cdot)"] & \mathrm{Hom}_E(M(G), M(W_{n+1}^{n+1})) & \\
\wr\Vert & \wr\Vert & \text{Lemma 26.6} \\
\mathrm{Hom}_E(M(G), E_n^n) \arrow[r, hook, "{[p]\circ()}"] & \mathrm{Hom}_E(M(G), E_{n+1}^{n+1}) & \\
\wr\Vert & \wr\Vert & \text{Functoriality of } (\_)^* \\
\mathrm{Hom}_E((E_n^n)^*, M(G)^*) \arrow[r, hook, "{(\cdot)\circ[p]^*}"] & \mathrm{Hom}_E((E_{n+1}^{n+1})^*, M(G)^*) & \\
\wr\Vert & \wr\Vert & \text{Lemma 26.8 (d)} \\
\mathrm{Hom}_E(E_n^n, M(G)^*) \arrow[r, hook, "{(\cdot)\circ[1]}"] & \mathrm{Hom}_E(E_{n+1}^{n+1}, M(G)^*) & \\
\wr\Vert & \wr\Vert & \text{evaluation at [1]} \\
M(G)^* \arrow[r, "\mathrm{id}"] & M(G)^* &
\end{tikzcd}$$

Lecture 13

February 03, 2005
Notes by Stefan Gille

§27 The Dieudonné functor in the étale case

Let E act on W_n from the left hand side, where F and V act as such and $\xi \in W(k)$ through multiplication by $\sigma^{-n}(\xi)$. Then the monomorphisms $v : W_n \hookrightarrow W_{n+1}$ are E-equivariant (compare Prop. 23.1). Also, the W_n^m form a fundamental system of infinitesimal neighborhoods of zero in all W_n. Thus for G local-local the functor M of §23 can be described equivalently as $M(G) = \varinjlim_n \mathrm{Hom}(G, W_n)$. Using this latter description we now prove a similar result for reduced-local groups:

Theorem 27.1. The functor $G \longmapsto M(G) = \varinjlim_n \mathrm{Hom}(G, W_n)$ induces an anti-equivalence of categories:

$$\left\{\!\!\left\{ \begin{array}{l} \text{finite commutative} \\ \text{étale group schemes} \\ \text{over } k \text{ of } p\text{-power order} \end{array} \right\}\!\!\right\} \xrightarrow{\sim} \left\{\!\!\left\{ \begin{array}{l} \text{left } E\text{-modules of} \\ \text{finite length with} \\ F \text{ an isomorphism} \end{array} \right\}\!\!\right\}.$$

Moreover, $\mathrm{length}_{W(k)} M(G) = \log_p |G|$.

Remark. The target category can be identified with the category of finite length $W(k)$-modules N together with a σ-linear automorphism $F : N \to N$, because V is determined by the relation $V = pF^{-1}$.

Remark. In [DG70] and [Fo77] the above theorem is proved jointly with the local-local case and using the same kind of reductions. But it also ties up nicely with descent and Lang's theorem, which have an independent interest, and which I want to describe.

Theorem 27.2 (Lang's Theorem). Let k be an algebraically closed field of positive characteristic. Let G be a connected algebraic group of finite type over k, and $F : G \to G$ a homomorphism with $dF = 0$. Then the map

$$G(k) \longrightarrow G(k), \qquad g \longmapsto g^{-1} \cdot F(g)$$

is surjective.

Proof. For any $g \in G(k)$ the morphism $G \to G$, $h \mapsto h^{-1}gF(h)$ has derivative $-\,\mathrm{id}$ everywhere, which is surjective; hence this morphism is dominant. As G is connected, the image contains an open dense subset $U_g \subseteq G$. The same holds in particular with $g = 1$. It follows that $U_g \cap U_1 \neq \emptyset$, and therefore there exist $h, \tilde{h} \in G(k)$ with $h^{-1}gF(h) = \tilde{h}^{-1}F(\tilde{h})$. Thus $g = h\tilde{h}^{-1}F(\tilde{h})F(h)^{-1} = (\tilde{h}h^{-1})^{-1} \cdot F(\tilde{h}h^{-1})$, as desired. □

Proposition 27.3. Let k be an algebraically closed field of positive characteristic. Let N be a $W(k)$-module of finite length together with a σ-linear automorphism $F : N \to N$. Then

$$N^F \;:=\; \{\, n \in N \,|\, Fn = n \,\}$$

is a finite commutative p-group, and the natural homomorphism

$$W(k) \otimes_{\mathbb{Z}_p} N^F \;\longrightarrow N\,, \quad x \otimes n \;\longmapsto\; xn$$

is an isomorphism. In particular $\operatorname{length}_{W(k)} N \;=\; \log_p |N^F|$.

Proof. Consider first the special case $N = W_n(k)$ with $F = \sigma$. In this case we have

$$N^F = W_n(k^F) = W_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z},$$

from which the claim obviously follows. The same follows for direct sums of modules of this type. In the general case, the proposition amounts to showing that every N is isomorphic to such a direct sum, because the desired isomorphism $W(k) \otimes_{\mathbb{Z}_p} N^F \to N$ is equivariant with respect to $\sigma \otimes \mathrm{id}$ on the source and F on the target.

To identify N with such a direct sum, we begin with any isomorphism of $W(k)$-modules

$$\varphi : \bigoplus_{i=1}^{r} W_{n_i}(k) \xrightarrow{\sim} N.$$

Via this the endomorphism ring

$$\underline{\mathrm{End}}_{W(k)}\, N \cong \bigoplus_{i,j=1}^{r} W_{\min\{n_i,n_j\}\,,\,k}$$

can be viewed as a unitary ring scheme over k. As a scheme it is isomorphic to an affine space of some dimension over k; in particular it is irreducible. Its group of units $G := \underline{\mathrm{Aut}}_{W(k)}\, N$ is an open subscheme in it; hence G is a connected algebraic group over k. The given σ-linear automorphism F then has the form $\varphi g \sigma \varphi^{-1}$ for some $g \in G(k)$. By Lang's theorem applied to the Frobenius on G we can write $g = h^{-1} \cdot \sigma(h)$ for some $h \in G(k)$. Thus

$$F = \varphi h^{-1} \sigma(h) \sigma \varphi^{-1} \;=\; (\varphi h^{-1}) \sigma(h \varphi^{-1}) \;=\; (\varphi h^{-1}) \sigma(\varphi h^{-1})^{-1}\,,$$

which means that φh^{-1} is the desired F-equivariant isomorphism. $\square$

Proof of Theorem 27.1 for k algebraically closed: In this case the source category is equivalent to the category of finite commutative p-groups Γ, and the functor gives:

$$\Gamma \longmapsto \underline{\Gamma}_k \longmapsto \varinjlim_n \operatorname{Hom}(\underline{\Gamma}_k, W_n)\,.$$

The latter group is equal to $\varinjlim_n \operatorname{Hom}(\Gamma, W_n(k))$, which in turn is isomorphic to

$$\operatorname{Hom}\bigl(\Gamma, W(k)\bigl[\tfrac{1}{p}\bigr]/W(k)\bigr) \;\cong\; W(k) \otimes_{\mathbb{Z}_p} \operatorname{Hom}(\Gamma, \mathbb{Q}_p/\mathbb{Z}_p).$$

We note that $\operatorname{Hom}(\Gamma, \mathbb{Q}_p/\mathbb{Z}_p)$ is the Pontrjagin dual of Γ, and the action of F corresponds to the action of $\sigma \otimes \mathrm{id}$ on $W(k) \otimes_{\mathbb{Z}_p} \operatorname{Hom}(\Gamma, \mathbb{Q}_p/\mathbb{Z}_p)$. By Proposition 27.3 this gives the desired anti-equivalence and the formula for the length.

Proof of Theorem 27.1 in general: Let $\bar{k}$ be an algebraic closure of k. Then we have (anti-)equivalences of categories:

$$\begin{tikzcd}
\left\{\left\{\begin{array}{l}\text{finite commutative}\\ \text{étale group schemes}\\ \text{over } k \text{ of } p\text{-power order}\end{array}\right\}\right\} \arrow[r, "G\mapsto M(G)"] \arrow[d, "\cong"', "G\mapsto G_{\bar{k}}"] & \left\{\left\{\begin{array}{l}\text{finite length } W(k)\text{-}\\ \text{modules with a } \sigma\text{-linear}\\ \text{automorphism } F\end{array}\right\}\right\} \\
\left\{\left\{\begin{array}{l}\text{finite commutative étale}\\ \text{group schemes over } \bar{k} \text{ of}\\ p\text{-power order with a con-}\\ \text{tinuous } \mathrm{Gal}(\bar{k}/k)\text{-action}\end{array}\right\}\right\} \arrow[r, "\cong", "G_{\bar{k}}\mapsto M(G_{\bar{k}})"'] & \left\{\left\{\begin{array}{l}\text{finite length } W(\bar{k})\text{-mod-}\\ \text{ules with a } \sigma\text{-linear auto-}\\ \text{morphism } F \text{ and a con-}\\ \text{tinuous } \mathrm{Gal}(\bar{k}/k)\text{-action}\end{array}\right\}\right\} \arrow[u, "\cong", "N\mapsto N^{\mathrm{Gal}(\bar{k}/k)}"']
\end{tikzcd}.$$

In fact, the vertical arrows are equivalences by descent, and the lower horizontal arrow is an anti-equivalence by Theorem 27.1 for $\bar{k}$, where it is proven already, and the functoriality of $M(\ )$ under automorphisms of $\bar{k}$. Since

$$M(G_{\bar{k}})^{\mathrm{Gal}(\bar{k}/k)} \;=\; \varinjlim_n \operatorname{Hom}(G_{\bar{k}}, W_{n,\bar{k}})^{\mathrm{Gal}(\bar{k}/k)} \;=\; \varinjlim_n \operatorname{Hom}(G, W_n) \;=\; M(G),$$

the whole diagram commutes, and therefore the upper horizontal arrow is an anti-equivalence, too. Finally the formula for the length is preserved by descent, because

$$\operatorname{length}_{W(k)} M(G) \;=\; \operatorname{length}_{W(\bar{k})} W(\bar{k}) \otimes_{W(k)} M(G) \;=\; \operatorname{length}_{W(\bar{k})} M(G_{\bar{k}})\,,$$

and we are done.

Caution. In general $\mathrm{length}_{W(k)} M(G) \neq \mathrm{length}_E M(G)$, although for local-local G the equality does hold. The point is that all simple local-local G have order p, but not the simple étale ones.

Example. Let $G(\bar{k}) \cong \mathbb{F}_p^r$ with an irreducible action of the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$. Then $M(G)$ must be a simple E-module, i.e., we have $M(G) \cong k^r$ with an irreducible F-action.

§28 The Dieudonné functor in the general case

Recall from Theorems 15.5 and 17.1 that any finite commutative group scheme of p-power order has a unique decomposition

$$G \;=\; G_{r\ell} \,\oplus\, G_{\ell r} \,\oplus\, G_{\ell\ell}\,.$$

In §23 and §27 we have already defined $M(G_{\ell\ell})$ and $M(G_{r\ell})$. Since $G_{\ell r}^*$ is of reduced-local type, we can define:

$$M(G) \;:=\; M(G_{r\ell}) \,\oplus\, M(G_{\ell r}^*)^* \,\oplus\, M(G_{\ell\ell})\,. \tag{28.1}$$

By construction this is a finite length left E-module, and by combining Theorem 27.1 and Propositions 23.3 (b) and 26.2, we deduce that

$$\mathrm{length}_{W(k)} M(G) = \log_p |G|.$$

Also, F and V are nilpotent on $M(G_{\ell\ell})$, and F is an isomorphism on $M(G_{r\ell})$. Since $FV = p$ in E, it follows that V is nilpotent on $M(G_{r\ell})$. The same holds for $M(G_{\ell r}^*)$, and so V is an isomorphism and F is nilpotent on $M(G_{\ell r}^*)^*$. In fact, such a decomposition exists for any finite length E-module:

Lemma 28.2. *Every finite length left E-module has a unique and functorial decomposition*

$$\begin{array}{lccccccc}
 & M \;= & M_{r\ell} & \oplus & M_{\ell r} & \oplus & M_{\ell\ell} \\
\text{where } F \text{ is} & & \text{isom.} & & \text{nilpot.} & & \text{nilpot.} \\
\text{where } V \text{ is} & & \text{nilpot.} & & \text{isom.} & & \text{nilpot.}
\end{array}$$

Proof. The images of $F^n : M \to M$ form a decreasing sequence of E-submodules of M. Since M has finite length, this sequence stabilizes, say with $F^n M = M'$ for all $n \gg 0$. Then $F : M' \to M'$ is an isomorphism; hence $M' \cap \ker(F^n|_M) = 0$; and so by looking at the length we find that $M = M' \oplus \ker(F^n|_M)$. Repeating the same with V on $\ker(F^n|_M)$ we obtain the desired decomposition. Uniqueness and functoriality are clear. □

Recall from Theorem 26.3 that there is a functorial isomorphism $M(G_{\ell\ell}^*) \cong M(G_{\ell\ell})^*$. By construction this isomorphism extends to G. Altogether we have now proven:

Theorem 28.3. The functor M defined by (28.1) induces an anti-equivalence of categories

$$\left\{\left\{\begin{array}{c}\text{finite commutative}\\ \text{group schemes over}\\ k \text{ of } p\text{-power order}\end{array}\right\}\right\} \xrightarrow{\sim} \left\{\left\{\begin{array}{c}\text{left } E\text{-modules}\\ \text{of finite length}\end{array}\right\}\right\}.$$

Moreover $\text{length}_{W(k)} M(G) = \log_p |G|$, and there is a functorial isomorphism $M(G^*) \cong M(G)^*$.

Note. The definition $M(G_{\ell r}) := M(G_{\ell r}^*)^*$ looks somewhat artificial and cheap. But it is a fact that often one does need special arguments for $G_{\ell r}$ or $G_{r\ell}$. Nevertheless Fontaine [Fo77] uses a uniform definition of $M(G)$ for all cases, basically using a combination of the W_n with the formal group scheme $\widehat{W}$ from §25.

In principle, since M is an equivalence of categories, all properties of G can be read off from $M(G)$. We end with an example:

Proposition 28.4. There is a natural isomorphism

$$T_{G,0} \cong \big(M(G)/FM(G)\big)^*.$$

Proof. It suffices to show this in each of the cases $G = G_{r\ell}$, $G_{\ell r}$, and $G_{\ell\ell}$. In the first case $T_{G,0} = 0$ and F is an isomorphism on $M(G)$, and so both sides vanish. In the other two cases we have by Proposition 13.1

$$T_{G,0} \cong \text{Hom}(G^*, \mathbb{G}_{a,k}) = \text{Hom}(G^*, W_1).$$

Since $M(G^*) = \varinjlim_n \text{Hom}(G^*, W_n)$ and $W_1 = \ker(V|_{W_n})$ for all $n \geq 1$, the latter is

$$\ker(V|_{M(G^*)}) = \ker(V|_{M(G)^*}) = \text{coker}(F|_{M(G)})^*,$$

as desired. □

References

[De72] M. Demazure: *Lectures on p-divisible groups*, Springer-Verlag, Berlin etc., 1972

[DG70] M. Demazure, P. Gabriel: *Groupes Algébriques, Tome I*, Masson et Cie, 1970

[Fo77] J.-M. Fontaine: *Groupes p-divisibles sur les corps locaux,* Astérisque, No. 47-48. Paris: Société Mathématique de France, 1977

[Mu70] D. Mumford: *Abelian varieties*, Oxford University Press, 1970

[Oo66] F. Oort: *Commutative group schemes,* Lecture Notes in Mathematics 15, Berlin: Springer, 1966

[SGA3] *Schémas en groupes, I–III,* Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3), Dirigé par M. Demazure et A. Grothendieck, Lecture Notes in Mathematics 151–153, Berlin: Springer, 1970

[Wa79] W.C. Waterhouse: *Introduction to affine group schemes*, Springer-Verlag, New York etc., 1979

[We94] C.A. Weibel: *An introduction to homological algebra*, Cambridge University Press, 1994