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

$$R \xrightarrow{\ e\ } A \xleftarrow{\ \mu\ } A \otimes_R A,$$

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

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

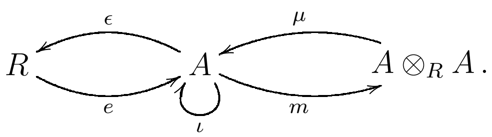
where $\mathfrak{aff}.R$-$\mathfrak{Sch}$ denotes the category of affine schemes over $\operatorname{Spec} R$. The object $* = \operatorname{Spec} R$ is a final object in $\mathfrak{aff}.R$-$\mathfrak{Sch}$.

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)



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.

<table>
<tr><th>meaning</th><th>axiom</th><th>axiom</th><th>meaning</th></tr>
<tr><td>μ associative</td><td>$\mu \circ (\mathrm{id} \otimes \mu) = \mu \circ (\mu \otimes \mathrm{id})$</td><td>$(m \otimes \mathrm{id}) \circ m = (\mathrm{id} \otimes m) \circ m$</td><td>$m$ coassociative</td></tr>
<tr><td>μ commutative</td><td>$\mu \circ \sigma = \mu$</td><td>$\sigma \circ m = m$</td><td>m cocommutative</td></tr>
<tr><td>e unit for μ</td><td>$\mu \circ (e(1) \otimes \mathrm{id}) = \mathrm{id}$</td><td>$(\epsilon \otimes \mathrm{id}) \circ m = 1 \otimes \mathrm{id}$</td><td>$\epsilon$ counit for m</td></tr>
<tr><td rowspan="2">m homomorphism
of unitary rings</td><td colspan="2">$m \circ \mu = (\mu \otimes \mu) \circ (\mathrm{id} \otimes \sigma \otimes \mathrm{id}) \circ (m \otimes m)$</td><td></td></tr>
<tr><td>$m(e(1)) = e(1) \otimes e(1)$</td><td>$\epsilon \circ \mu = \epsilon \otimes \epsilon$</td><td rowspan="2">$\epsilon$ homomorphism
of unitary rings</td></tr>
<tr><td></td><td colspan="2">$\epsilon \otimes e = \mathrm{id}$</td></tr>
<tr><td rowspan="2">ι homomorphism
of unitary rings</td><td>$\iota \circ \mu = \mu \circ (\iota \otimes \iota)$</td><td>$m \circ \iota = (\iota \otimes \iota) \circ m$</td><td>$(xy)^{-1} \overset{!}{=} x^{-1}y^{-1}$</td></tr>
<tr><td>$\iota \circ e = e$</td><td>$\epsilon \circ \iota = \epsilon$</td><td>$1 \overset{!}{=} 1^{-1}$</td></tr>
<tr><td>ι coinverse for m</td><td colspan="2">$e \circ \epsilon = \mu \circ (\mathrm{id} \otimes \iota) \circ m$</td><td></td></tr>
</table>

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)
$$\begin{array}{ccccc} R & \underset{e_A}{\overset{\epsilon_A}{\leftrightarrows}} & A & \underset{m_A}{\overset{\mu_A}{\leftrightarrows}} & A \otimes_R A \\ \Big| \,\text{id} & & \Big\uparrow \phi & & \Big\uparrow \phi\otimes\phi \\ R & \underset{e_B}{\overset{\epsilon_B}{\leftrightarrows}} & B & \underset{m_B}{\overset{\mu_B}{\leftrightarrows}} & B \otimes_R B\,. \end{array}$$

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

(3.3)
$$\begin{array}{ccc} G & \longrightarrow & G \times G \\ {\scriptstyle \Phi+\Psi}\Big\downarrow & & \Big\downarrow{\scriptstyle \Phi\times\Psi} \\ H & \longleftarrow & H \times H \end{array} \quad ,$$

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)
$$R \underset{\epsilon^*}{\overset{e^*}{\leftrightarrows}} A^* \underset{\mu^*}{\overset{m^*}{\leftrightarrows}} A^* \otimes_R A^*\,. \qquad (\iota^* : A^* \to A^*)$$

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 $\mathrm{id} \longrightarrow^{**}$ 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

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

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

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

Let $\{u_i\}_{0 \leq i < p}$ 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 $\underline{\mathbb{Z}/\mathbb{Z}p}_k$, $\mu\!\!\mu_{p,k}$, and $\boldsymbol{\alpha}_{p,k}$ are pairwise non-isomorphic.

Proof. The first one is étale, while both $\mu\!\!\mu_{p,k} = \operatorname{Spec} k[X]/(X^p - 1)$ 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. $\square$