1 Recall

Assume we have a locally small category $C$ which admits finite products and has a final object $\star$, i.e. an object so that for every $Z \in \text{Ob}(C)$, there exists a unique morphism $Z \to \star$. Note that two morphisms $f, g : Z \to G$ can then be identified uniquely with a morphism $(f, g) : Z \to G \times G$.

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

There is an alternate description of commutative group objects which sheds more light on what associativity, commutativity, existence of identity and inverses means. Before we state the proposition, note that the existence of products implies the existence of a morphism $\sigma : G \times G \to G \times G$ interchanging the two factors.

**Proposition.** An object $G \in \text{Ob}(C)$ and a morphism $G \times G \xrightarrow{\mu} G$ constitute a commutative group object in $C$ if and only if the following properties hold:

- **Associativity:** The following diagram is commutative:

$$
\begin{array}{ccc}
G \times G \times G & \xrightarrow{\mu \times \text{id}} & G \times G \\
\downarrow{\text{id} \times \mu} & & \downarrow{\mu} \\
G \times G & \xrightarrow{\mu} & G.
\end{array}
$$

- **Commutativity:** The following diagram is commutative:

$$
\begin{array}{ccc}
G \times G & \xrightarrow{\mu} & G \\
\downarrow{\sigma} & & \downarrow{\mu} \\
G \times G & \xrightarrow{\sigma} & G.
\end{array}
$$

- **Identity element:** There exists a morphism $e : \star \to G$ such that the following diagram commutes

$$
\begin{array}{ccc}
\star \times G & \xrightarrow{e \times \text{id}} & G \times G \\
\downarrow{\text{pr}_2} & & \downarrow{\mu} \\
G & \xrightarrow{\mu} & G.
\end{array}
$$

- **Inverses:** There exists a morphism $i : G \to G$ such that the following diagram commutes

$$
\begin{array}{ccc}
G \times G & \xleftarrow{i \times \text{id}} & G \times G \\
\uparrow{\text{diag}} & & \downarrow{\mu} \\
G & \xrightarrow{e} & \star & \xrightarrow{e} & G
\end{array}
$$

where $e$ is the morphism from the previous bullet point.
2 Affine Group Schemes

Let $\text{Rings}$ be the category of commutative noetherian rings with 1. The morphisms of this category are ring homomorphisms preserving the identity. Recall that there is an (anti-)equivalence of categories between $\text{Rings}$ and the category $\text{Aff.Sch}$ of affine schemes.

Recall that an object $A$ of $\text{Rings}$ together with a morphism $R \to A$ constitutes a unitary $R$-algebra. Note that since $A$ is a ring and the multiplication $A \times A \to A$ is $R$-bilinear, it induces an $R$-module homomorphism $\mu : A \otimes_R A \to A$ as follows

\[
\begin{array}{ccc}
A & \leftarrow & A \\
\otimes & \downarrow & \mu \\
A \times A & \rightarrow & A
\end{array}
\]

This allows us to (equivalently) view a unitary $R$-algebra $A$ as an $R$-module with two homomorphisms of $R$-modules

\[
R \xleftarrow{\epsilon} A \xrightarrow{\mu} A \otimes_R A,
\]

satisfying $\mu(a \otimes a') = \mu(a' \otimes a)$ (corresponding to multiplication in $A$ being commutative) and $\mu(a \otimes \mu(a' \otimes a'')) = \mu(\mu(a \otimes a') \otimes a'')$ (corresponding to multiplication in $A$ being associative) and $\mu(e(1) \otimes a) = a$ (corresponding to $a \cdot e(1) = a$). Denote the category of $R$-algebras by $R\text{-Alg}$. Then the (anti-)equivalence of categories $\text{Rings}$ and $\text{Aff.Sch}$ restricts to an (anti-)equivalence of categories $R\text{-Alg}$ and $\text{Aff. R-Sch}$.

**Definition.** An **affine commutative group scheme over** $\text{Spec } R$ is a commutative group object in the category of affine schemes over $\text{Spec } R$.

Let $G = \text{Spec } A$ be an affine commutative scheme over $\text{Spec } R$. Then in particular $A$ is a unitary $R$-algebra. Combining the 'categorical' definitions for unitary $R$-algebras and commutative group object, we obtain the following diagram of $R$-module homomorphisms:

\[
\begin{array}{ccc}
R & \xleftarrow{\epsilon} & A \\
\otimes & \xrightarrow{\mu} & A \otimes_R A
\end{array}
\]

The axioms satisfied by all the morphisms above turn $A$ into a Hopf $R$-algebra.

**Definition.** A **homomorphism of group schemes** $\Phi : G \to H$ over $\text{Spec } R$ is a morphism in $\text{Aff. R-Sch}$, such that the induced morphism $\text{Mor}(Z, G) \to \text{Mor}(Z, H)$ is a homomorphism of groups for all $Z \in \text{Ob}(\text{Aff. R-Sch})$.

If $G = \text{Spec } A$ and $H = \text{Spec } B$, this morphism corresponds to a homomorphism of $R$-modules $\phi : B \to A$ such
that the following diagram commutes:

\[
\begin{array}{c}
\text{R} \\
\downarrow \phi \\
\text{B} \\
\downarrow \phi \otimes \phi \\
\text{B} \otimes_R \text{B},
\end{array}
\]

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

\[
\begin{array}{c}
G \\
\downarrow \Phi + \Psi \\
H \\
\downarrow \Phi \times \Phi \\
H \times H
\end{array}
\]

3 $\mu_{n,k}$ and $\alpha_{p,R}$

Let’s step aside from the course of the notes to define two objects of interest later. Recall that the multiplicative group over $k$ is $G_{m,k} \overset{\text{def}}{=} \text{Spec} k[T, T^{-1}]$. This is a group scheme, with co-multiplication $m : k[T, T^{-1}] \to k[T_1, T_1^{-1}] \otimes_k k[T_2, T_2^{-1}]$ given by $T \to T_1 \otimes T_2$. Consider the homomorphism $n \cdot \text{id} : G_{m,k} \to G_{m,k}$ induced by the map (on rings) $k[T, T^{-1}] \to k[T, T^{-1}]$ sending $t \mapsto t^n$. We are interested in the fiber produce $\mu_{n,k} = G_{m,k} \otimes_{G_{m,k}} \text{Spec} k$ in the diagram

\[
\begin{array}{c}
G_{m,k} \\
\downarrow n \cdot \text{id} \\
G_{m,k}
\end{array}
\]

where the map $\text{Spec} k \to G_{m,k}$ is induced from $k[S, S^{-1}] \to k$ sending $S \mapsto 1$.

For affine schemes, fiber products correspond to the tensor product of the corresponding rings, implying that $\mu_{n,k} = \text{Spec} A$, where $A = k[T, T^{-1}] \otimes_{k[S, S^{-1}]} k$. Using $T^n \otimes 1 = S(1 \otimes 1) = 1 \otimes S = 1 \otimes 1$, one concludes that $A = k[T]/(T^n - 1)$, hence $\mu_{n,k} = \text{Spec} k[T]/(T^n - 1)$. This is a group scheme with comultiplication $m$ sending, just like for $G_{m,k}$ (but in different rings) $T \mapsto T_1 \otimes T_2$.

The other object we introduce is $\alpha_{n,R} = \text{Spec} R[T]/(T^n)$. This is a group scheme with comultiplication $m : R[T]/(T^n) \to R[T_1]/(T_1^n) \otimes_R R[T_2]/(T_2^n)$ given by $m(T) = T_1 \otimes 1 + \otimes T_2$.

Note that over a field of positive characteristic $p$, with $n = p^s$, we have $T^{p^s} - 1 = (T - 1)^{p^s}$, and hence $\mu_{p^s,k} \simeq \text{Spec} k[U]/(U^{p^s}) \simeq \alpha_{p^s,k}$, where we identified $U = T - 1$. As a particular case, notice that we have established $\mu_{p,k} \simeq \alpha_{p,k}$ as schemes over $k$. By the end of the lecture, we shall see that $\mu_{p,k}$ and $\alpha_{p,k}$ are not isomorphic in the category of affine commutative finite flat group schemes over $\text{Spec} k$. 

3
4 Cartier Duality

Assume now that $G = \text{Spec} \, A$ is a group scheme, finite and flat over $R$ (i.e. that $A$ is a locally free, finitely-generated $R$-module). Let $A^* \overset{\text{def}}{=} \text{Hom}_R(A, R)$ be the $R$-dual of $A$. One can check that if we dualize the diagram following the definition of an affine commutative group scheme, one obtains the following diagram, under the identifications $R^* = R$ and $(A \otimes_R A)^* = A^* \otimes_R A^*$:

\[
\begin{array}{ccc}
R & \xrightarrow{e^*} & A^* \\
\downarrow{\epsilon^*} & & \downarrow{\mu^*} \\
A^* & \xleftarrow{i^*} & A^* \otimes_R A^*
\end{array}
\]

The morphisms $e^*, m^*, \mu^*, \epsilon^*$ and $i^*$ satisfy the axioms of a cocommutative Hopf algebra with antipodism, and therefore $G^* \overset{\text{def}}{=} \text{Spec} \, A^*$ is an affine commutative finite flat group scheme over $\text{Spec} \, R$.

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

If we have homomorphism $\Phi : G \to H$ of affine commutative finite flat group schemes over $\text{Spec} \, R$ corresponding to a homomorphism $\phi : B \to A$, then $\phi$ induces $\phi^* : A^* \to B^*$ and thus a homomorphism of group schemes $H^* \to G^*$. Hence Cartier duality gives a contravariant functor from the category of affine group schemes to itself.

This functor is additive, i.e. given $\Psi, \Phi : G \to H$, then $(\Psi + \Phi)^* = \Psi^* + \Phi^*$.

5 Constant Group Schemes

Let $G$ be an additive finite abelian group. We want to exhibit a finite commutative group scheme associated to $G$. For that we take the disjoint union of $|G|$ copies of the final object $\text{Spec} \, R = \ast$ in the category of affine schemes over $\text{Spec} \, R$. Let $G_R$ (standard notation for group schemes) be

\[G_R = \coprod_{g \in G} \text{Spec} \, R.\]

**Notation:** Write $(\text{Spec} \, R)_g = \text{Spec} \, R$ for the $g$-component of $G_R$.

**Exercise:** Why is this a scheme over $\text{Spec} \, R$? What is the unique morphism to the terminal object $\text{Spec} \, R$?

**Exercise:** $G_R$ is finite and flat over $\text{Spec} \, R$.

As written, it is not obvious that this is a commutative group scheme over $\text{Spec} \, R$. For that, note first that

\[G_R \times G_R \cong \coprod_{g, g' \in G} \text{Spec} \, R.\]

This follows from the fact that the product of two disjoint unions $X = \coprod X_\alpha$ and $Y = \coprod Y_\beta$ of $R$-schemes is the disjoint union of the products $X_\alpha \times_R Y_\beta$ (EGA, I.3.2.8) and from $(\text{Spec} \, R \times_R \text{Spec} \, R) \subseteq \text{Spec} \, R$ (EGA Chapter I.3.2.2).

Define then the morphism $\mu : G \times G \to G$ by sending the component $(\text{Spec} \, R)_g \times (\text{Spec} \, R)_{g'}$ of $G_R \times G_R$ to the $(\text{Spec} \, R)_{g+g'}$ component of $G_R$. 

4
Exercise: The scheme $G_R$ and the morphism $\mu$ define a commutative group scheme over $\text{Spec } R$.

The scheme $G_R$ is also called the constant group scheme over $R$ with fiber $G$.

Lemma. Let

$$R^G \overset{\text{def}}{=} \{ f : G \to R | f \text{ is a map of sets} \}.$$  

This is a ring, with addition and multiplication defined componentwise. The zero and the identity are the constant maps with value 0, respectively 1. Then $G_R \cong \text{Spec}(R^G)$.

Proof. This follows by induction from EGA I.3.1.1.

However, as it is necessary in the subsequent discussion, we can describe the isomorphisms between the two sides in the following way:

As a convenience of notation, let $R_g$ be a copy of the ring $R$, and assume the $g$-component of $G_R$ is $(\text{Spec } R)_g = \text{Spec } R_g$. For every such component we have a morphism $\text{Spec } R_g \to \text{Spec}(R^G)$ induced by the ring homomorphism $R^G \to R_g$ sending $f$ to $f(g) \in R = R_g$. This then induces a morphism $\phi : G_R \to \text{Spec}(R^G)$.

Conversely, we have a morphism $\psi : \text{Spec}(R^G) \to G_R$, induced by the ring homomorphisms $R_g \to R^G$ sending an element $r \in R = R_g$ to the map $f : G \to R$ satisfying $f(g) = r$ and $f(g') = 0$ for $g \neq g'$.

Exercise: $\phi$ and $\psi$ are isomorphisms, inverse to each other. \qed

In particular $G_r \times G_r$ is $\text{Spec}(R^G \times G^G)$ and thus the map $G_R \times G_R \to G_R$ is induced by the the comultiplication map $m : R^G \to R^G \otimes R^G \cong R^G \times G^G$. Let’s explicitly define this map. Let $f \in R^G$. From the map on components $G_R \times G_R \to G_R$ defined above, one can deduce that $m(f)$ is the map of $R^G \times G^G$ sending $(g, g')$ to $f(g + g')$. The counit $R^G \to R$ is defined by $\epsilon(f) = f(0)$. The coinverse $i : R^G \to R^G$ is, as expected, the map sending $g \mapsto f(-g)$.

Consider now the canonical basis $\{ e_g \}$ of $R^G$ given by $e_g : G \to R$ such that $e_g(g) = 1$ and $e_g(g') = 0$ for $g' \neq g$. Using the above, one can check that we have

$$\mu(e_g \otimes e_{g'}) = (e_g \text{ if } g = g') \text{ and } (0 \text{ otherwise})$$
$$\epsilon(e_g) = (1 \text{ if } g = 0) \text{ and } (0 \text{ otherwise})$$
$$\epsilon(1) = \sum_{g \in G} e_g$$
$$m(e_g) = \sum_{g' \in G} e_g' \otimes e_{g-g'}$$
$$i(e_g) = e_{-g}.$$  

To see what the Cartier dual of $G_R$ is, let $(\hat{e}_g)_{g \in G}$ be the basis of $(R^G)^*$ dual to the above basis, i.e. $\hat{e}_g(g') = 1$
if \( g' = g \) and 0 if \( g' \neq g \). Then the dual maps are given by

\[
\begin{align*}
\mu^*(\hat{e}_g) &= \hat{e}_g \otimes \hat{e}_g \\
e^*(1) &= \hat{e}_0 \\
e^*(\hat{e}_g) &= 1 \\
m^*(\hat{e}_g \otimes \hat{e}_g') &= \hat{e}_{g+g'} \\
i^*(\hat{e}_g) &= \hat{e}_{-g}.
\end{align*}
\]

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

**Example 1:** \( G = \mathbb{Z}/n\mathbb{Z} \)

Denote \( X \overset{\text{def}}{=} \hat{e}^1 \). Then \((R^G)^* \simeq R[G] = R[\mathbb{Z}/n\mathbb{Z}] = R[X]/(X^n-1)\). The comultiplication \( \mu^* : (R^G)^* \to (R^G)^* \otimes_R (R^G)^* \) is \( \mu^*(X) = X \otimes X \), which we note is the same as what holds for \( \mu_{n,R} \). Thus

\[
(\mathbb{Z}/n\mathbb{Z})^*_R \simeq \mu_{n,R}.
\]

**Dual of \( \alpha_{p,R} \):**

Assume \( R \) has characteristic \( p \) and let \( A = R[T]/(T^p) \). Recall \( \alpha_{p,R} = \text{Spec} A \) is a group scheme with comultiplication \( m(T) = T \otimes 1 + 1 \otimes T \). Let \( e_i \) be the basis \((T_i)_{0 \leq i < p}\). Then we have

\[
\begin{align*}
\mu(T^i \otimes T^j) &= (T^{i+j} \text{ if } i + j < p) \text{ and } (0 \text{ otherwise}) \\
\epsilon(T^i) &= (1 \text{ if } i = 0) \text{ and } (0 \text{ otherwise}) \\
\epsilon(1) &= T^0 \\
m(T^i) &= \sum_{0 \leq j \leq i} \binom{i}{j} \cdot T^j \otimes T^{i-j} \\
i(T^i) &= (-1)^i T^i.
\end{align*}
\]

If \( \{u_i\} \) is the dual basis of \( A^* \). Then one can check that the \( R \)-linear map \( A^* \to A \) sending \( u_i \) to \( T^i/i! \) is an isomorphism of Hopf algebras, and therefore

\[
(\alpha_{p,R})^* \simeq \alpha_{p,R}.
\]

We finish the talk with the following

**Proposition.** Let \( k \) be any field with char \( k = p > 0 \). Then the group schemes \( \mathbb{Z}/p\mathbb{Z}_k \), \( \mu_{p,k} \) and \( \alpha_{p,k} \) are pairwise non-isomorphic.

**Proof.** The group scheme \( \mathbb{Z}/p\mathbb{Z}_k \) is isomorphic to \( \text{Spec} k^p \), so it is a reduced scheme, while \( \mu_{p,k} = \text{Spec} k[T]/(T^p-1) \) and \( \alpha_{p,k} = \text{Spec} k[T]/(T^p) \) are non-reduced, so they are distinct.

As we have seen before \( \mu_{p,k} \) and \( \alpha_{p,k} \) are isomorphic as schemes. However as affine group schemes, they are not, for their Cartier duals are different from the previous two examples.

\[ \square \]
Bibliography
