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:

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

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

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

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

Then we have the following isomorphisms

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

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 $p \neq \mathrm{char}(k)$ and k is finitely generated over its prime field, then the natural homomorphism

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

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 $A(\mathbb{C}) \cong (\mathrm{Lie}\, A_{\mathbb{C}})/\,\mathrm{H}_1\left(A(\mathbb{C}), \mathbb{Z}\right)$ induces an isomorphism $T_p A \cong \mathrm{H}_1\left(A(\mathbb{C}), \mathbb{Z}\right) \otimes \mathbb{Z}_p$.

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

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

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 $\boldsymbol{\mu}_{m,k}$. This is defined as the fiber product

in the following commutative diagram

$$\begin{array}{ccc} \mathbb{G}_{m,k} & \xrightarrow{m\cdot\mathrm{id}} & \mathbb{G}_{m,k} \\ \uparrow & & \uparrow{\scriptstyle 1} \\ \boldsymbol{\mu}_{m,k} & \longrightarrow & \operatorname{Spec} k\,. \end{array}$$

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

$$\begin{array}{ccc} k[T,T^{-1}] & \xleftarrow{T^m \leftarrow\!\shortmid S} & k[S,S^{-1}] \\ \downarrow & & \downarrow \\ k[T]/(T^m-1) & \longleftarrow & k. \end{array}$$

Thus we get the equality $\boldsymbol{\mu}_{m,k} = \operatorname{Spec} k[T]/(T^m-1)$ with the group operation $(t,t') \mapsto t \cdot t'$. If $p = \operatorname{char}(k)$, we have $T^{p^n} - 1 = (T-1)^{p^n}$ and therefore $\boldsymbol{\mu}_{p^n,k} \cong \operatorname{Spec} k[U]/(U^{p^n})$ 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 $\boldsymbol{\mu}_{p^n,k}$, 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:

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

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

$$\begin{array}{ccc} G \times G & \xrightarrow{\mu} & G \\ {\scriptstyle \sigma}\downarrow & \nearrow_{\mu} & \\ G \times G\,, & & \end{array}$$

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:

$$\begin{array}{ccc} * \times G & \xrightarrow{e \times \mathrm{id}} & G \times G \\ {\scriptstyle pr_2}\downarrow \wr & \swarrow_{\mu} & \\ G\,. & & \end{array}$$

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

$$\begin{array}{ccccc} G \times G & & \xrightarrow{\mathrm{id} \times i} & & G \times G \\ {\scriptstyle \mathrm{diag}}\uparrow & & & & \downarrow{\scriptstyle \mu} \\ G & \longrightarrow & * & \xrightarrow{e} & G \end{array} ,$$

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.