1. Cartier duality

Let $R$ be a commutative ring, and let $G = \text{Spec } A$ be a commutative group scheme, where $A$ is a finite flat algebra over $R$. Let $A^\vee = \text{Hom}_{R-\text{mod}}(A, R)$ be the dual of $A$. Then $A^\vee$ has the structure of an $R$-module, given by

$$(rf)(a) = rf(a) = f(ra)$$

for $r \in R$ and $a \in A$.

If $A$ is a free $R$-algebra, then

$$\text{Hom}_{R-\text{mod}}(A \otimes A, R) \cong \text{Hom}_{R-\text{mod}}(A, R) \times \text{Hom}_{R-\text{mod}}(A, R),$$

so $(A \otimes A)^\vee \cong A^\vee \otimes A^\vee$.

If $A$ is a Hopf algebra, we have $R$-algebra maps

$$m : A \otimes A \to A$$
$$\Delta : A \to A \otimes A$$
$$\eta : R \to A$$
$$\varepsilon : A \to R$$
$$i : A \to A.$$

When we dualize these maps, we get maps

$$m^\vee : A^\vee \to A^\vee \otimes A^\vee$$
$$\Delta^\vee : A^\vee \otimes A^\vee \to A^\vee$$
$$\eta^\vee : A^\vee \to R$$
$$\varepsilon^\vee : R \to A^\vee$$
$$i^\vee : A^\vee \to A^\vee.$$

We can now state Cartier’s duality theorem.

**Theorem 1** (Cartier duality). With the maps given above, if $A$ is finite flat, then $A^\vee$ is again an $R$-Hopf algebra, with $A^\vee$ finite and flat over $R$. We call $G^\vee = \text{Spec } A^\vee$ the dual group scheme. Furthermore, for any $R$-algebra $S$,

$$G^\vee(S) = \text{Hom}_{S-\text{sch}}(G/S, \mathbb{G}_m/S) \cong \text{Hom}_{S-\text{Hopf}}(S[T^\pm 1], A \otimes S).$$

*Date: 27 October, 2010.*
We also have $G^\vee \cong G$ and $\#G^\vee = \#G$, and there’s also the usual duality pairing $G \times G^\vee \to \mathbb{G}_m$, given by $(g, \phi) \mapsto \phi(g)$.

Proof. We’ll check the bit about the functoriality of $S$-points. This amounts to checking that
\[
\text{Hom}_{R-\text{alg}}(\text{Hom}_{R-\text{mod}}(A, R), S) \cong \text{Hom}_{S-\text{Hopf}}(S[T^{\pm 1}], A \otimes S).
\]
By the universal property for tensor products, we have
\[
\text{Hom}_{S-\text{alg}}(\text{Hom}_{S-\text{mod}}(A \otimes S, S), S) \cong \text{Hom}_{R-\text{alg}}(\text{Hom}_{R-\text{mod}}(A, R), S),
\]
which means we can reduce to the case of $S = R$.

We want to show now that
\[
\text{Hom}_R(\text{Hom}_R(A, R), R) \cong \text{Hom}_R(R[T^{\pm 1}], A) = \{a \in A^\times : \Delta(a) = a \otimes a\}
\]
because of the compatibility conditions. The left side can be thought of as the set of $a \in A$ so that the assignment $\phi \mapsto \phi(a)$ is an $R$-Hopf algebra homomorphism (identifying $A^\vee$ with $A$). Thus, we need
\[
(\phi \psi)(a) = \phi(a)\psi(a)
\]
for all $\phi, \psi \in A^\vee$, but
\[
(\phi \psi)(a) = ((\phi \otimes \psi) \circ \Delta)(a) = \phi(a)\psi(a) = (\phi \otimes \psi)(a \otimes a)
\]
if and only if $\Delta(a) = a \otimes a$.

We need the unit element $\eta^\vee$ of $\text{Hom}(A, R)$ to map to the unit element $1$ of $R$, so $\eta^\vee(a) = 1$. The antipode property gives us that
\[
m \circ (id_A \otimes i) \circ \Delta = \eta,
\]
so $m(a \otimes i(a)) = ai(a) = 1$, so $a$ is a unit, so $G^\vee(R) \subset A^\times$, which finishes off the proof. 

Let’s write down the duality pairing explicitly. Write $\mathbb{G}_m(S) = \text{Spec } S[T^{\pm 1}]$, and let $U$ be a trivializing open subset of $S$ for the locally free sheaf $\mathcal{O}_G$. Let $e_1, \ldots, e_g$ be a basis for $\mathcal{O}_G | U$, and let $e_1^\vee, \ldots, e_g^\vee$ be the dual basis for $\mathcal{O}_{G^\vee} | U$. The corresponding map
\[
\mathcal{O}_S[T^{\pm 1}] | U \to \mathcal{O}_G | U \otimes_{\mathcal{O}_S} U \mathcal{O}_{G^\vee} | U
\]
is just
\[
T \mapsto \sum_{i=1}^g e_i \otimes e_i^\vee.
\]
This map is of course independent of the choice of basis $\{e_1, \ldots, e_g\}$.

Let’s now look at some examples of Cartier duality in action.

**Proposition 2.** Cartier duality commutes with base change. If $Y \to X$ is a map of schemes and $G$ is an $X$-group scheme, then $(G_Y)^\vee \cong (G^\vee)_Y$. 
Example. The dual of $\mu_n$ is $$\text{Hom}(\mu_n, \mathbb{G}_m) \cong \text{Hom}(R[T^\pm], R[X]/(X^n - 1)).$$

If $\phi : T \mapsto p(X)$ with $p(U)p(V) = p(UV)$, and $p(X) = \sum_{i=0}^{n-1} a_i X^i$, we have $$\sum_{i=0}^{n-1} a_i (UV)^i = \sum_{i=0}^{n-1} a_i U^i \sum_{i=0}^{n-1} a_i V^i \mod (U^n - 1, V^n - 1).$$

Comparing terms, we have $a_i a_j = 0$ for $i \neq j$ and $a_i = a_i^2$, and as $\phi$ takes 1 to 1, we have $\sum_{i=0}^{n-1} a_i = 1$. So, the $a_i$ are orthogonal idempotents. Thus, the $a_i$ correspond to a point in the constant scheme $(\mathbb{Z}/n\mathbb{Z})_R = \text{Spec } R^{(\mathbb{Z}/n\mathbb{Z})}$, and this is the Cartier dual to $\mu_n$.

If $R$ has positive characteristic $p > 0$ and $n = p$, we can write down the Cartier pairing map explicitly. This is a map $$R[T^\pm] \to R[X]/(X^p - X) \otimes R[Y]/(Y^p - 1).$$

We have $$(\mathbb{Z}/p\mathbb{Z})_R = \text{Spec } R[X]/(X^p - X), \quad \mu_p(R) = \text{Spec } R[Y]/(Y^p - 1).$$

We take $1, X, \ldots, X^{p-1}$ as a basis of $R[X]/(X^p - X)$, and let $f_0, f_1, \ldots, f_{p-1}$ be its dual basis. We find that $$f_i = \frac{f_1^i}{i!}.$$ Letting $\exp$ denote the truncated exponential function $$\exp(\xi) = 1 + \xi + \frac{\xi^2}{2!} + \cdots + \frac{\xi^{p-1}}{(p-1)!},$$ we see that $Y = \exp(f_1)$. By the construction of the Cartier pairing, we have $$T \mapsto \exp(X \otimes \log Y).$$

In slightly more down-to-earth language, if $\zeta \in \mu_p(U)$ and $a \in (\mathbb{Z}/p\mathbb{Z})(U)$, then the pairing $(\zeta, a)$ is given by $\zeta^a \in \mathbb{G}_m(U)$.

Example. Let’s now show that for $R$ of characteristic $p$, $\alpha_p$ is self-dual. Recall that for a ring $S$ over $R$, $\alpha_p(S) = \{ s \in S : s^p = 0 \}$. The dual is $$\text{Hom}_R(\alpha_p, \mathbb{G}_m) = \text{Hom}_R(R[T^\pm], R[X]/(X^p))$$
$$= \{ \phi(X) \in R[X]/(X^p) : \phi(U + V) = \phi(U)\phi(V) \}. $$

Write $\phi(X) = \sum_{i=0}^{p-1} a_i X^i$. Then, comparing coefficients in the equation $$\sum_{i=0}^{p-1} a_i (U + V)^i = \sum_{i=0}^{p-1} a_i U^i \sum_{i=0}^{p-1} a_i V^i$$
tells us that $a_0 = 1$, $a_1$ is a free parameter, and if $p$ is sufficiently large, then $a_2 = \frac{a_1^2}{2!}, a_3 = \frac{a_1^3}{3!}, \ldots, a_k = \frac{a_1^k}{k!}$ for $k \leq p - 1$. We also have $a_1^p = 0$, so $\phi(U) = \exp(aU)$ with $a^p = 0$, which corresponds to a point in $\alpha_p(R)$. Thus $\exp(aU)\exp(a'U) = \exp((a + a')U)$, so $\alpha_p$ is self-dual.

**Example.** If $G_1$ and $G_2$ are two group schemes, we have $(G_1 \times G_2)\vee \cong G_1^\vee \times G_2^\vee$. Hence, if $\Gamma$ is a finite abelian group, the diagonalizable group scheme $\text{Spec}(R[\Gamma])$ is Cartier dual to the constant scheme $\text{Spec}(R^\Gamma)$. Thus $\exp(aU)\exp(a'U) = \exp((a + a')U)$, so $\alpha_p$ is self-dual.

Here are the explicit maps for Cartier duality for the constant scheme for an abelian group $\Gamma$. Let $\{e_\gamma : \gamma \in \Gamma\}$ be the canonical basis for $R^\Gamma$. We have $e_\gamma : \Gamma \rightarrow R$ given by $\gamma' \mapsto \delta_{\gamma\gamma'}$. Then the Hopf algebra maps are given by

$$
\begin{align*}
m(e_\gamma \otimes e'_{\gamma'}) &= \begin{cases} e_\gamma & \text{if } \gamma = \gamma', \\
0 & \text{otherwise}. \end{cases} \\
\varepsilon(e_\gamma) &= \delta_{\gamma0}, \\
e(1) &= \sum_{\gamma \in \Gamma} e_{\gamma}, \\
\Delta(e_\gamma) &= \sum_{\gamma' \in \Gamma} e_{\gamma'} \otimes e_{\gamma - \gamma'}, \\
i(e_\gamma) &= e_{-\gamma}. 
\end{align*}
$$

To calculate the Cartier dual, we use the formulae

$$
\begin{align*}
m^\vee(e_\gamma^\vee) &= e_\gamma^\vee \otimes e_{\gamma'}^\vee, \\
\varepsilon^\vee(1) &= e_0^\vee, \\
e^\vee(e_\gamma^\vee) &= 1, \\
\Delta^\vee(e_\gamma^\vee \otimes e_{\gamma'}^\vee) &= e_{\gamma + \gamma'}^\vee, \\
i^\vee(e_\gamma^\vee) &= e_{\gamma}^\vee, 
\end{align*}
$$

where $\{e_\gamma^\vee : \gamma \in \Gamma\}$ is the dual basis. If $\Gamma = \mathbb{Z}/n\mathbb{Z}$ is the cyclic group of order $n$, the above formulae imply that $(R^\Gamma)^\vee \cong R[X]/(X^n - 1)$ with comultiplication $m^\vee(X) = X \otimes X$. Thus $(\mathbb{Z}/n\mathbb{Z})^\vee \cong \mu_n$.

1.1. **Group schemes of order 2.** A group scheme $G = \text{Spec} A$ of order 2 over $R$ is of the form $\text{Spec} R[X]/(X^2 + \alpha X + \beta)$. If we replace $X$ by $X - \varepsilon(X)$ if necessary, we may assume that $\beta = 0$ and that $\varepsilon(X) = 0$. Hence, up to isomorphism, a group scheme of order 2 is of the form $\text{Spec} R[X]/(X^2 + \alpha X)$. The group law is a morphism $R[T]/(T^2 + \alpha T) \rightarrow R[U, V]/(U^2 + \alpha U, V^2 + \alpha V)$.
given by $T \mapsto a + bU + cV + dUV$. The identity map tells us that $a = 0$, $b = 1$, $c = 1$, so the map is really of the form $T \mapsto U + V + \beta UV$ for some $\beta$. We need

$$(U + V + \beta UV)^2 + \alpha(U + V + \beta UV) = 0 \in A \otimes A.$$ 

Expanding this out shows up that $(2 - \alpha \beta)(1 - \alpha \beta) = 0$. the inverse map tells us that if $T \mapsto \gamma + \delta T$ under the inverse map, then $(1 - \alpha \beta)\delta = -1$ is a unit, so we must have $2 - \alpha \beta = 0$. Since $1 - \alpha \beta = -1$ already, we have $\delta = 1$ and hence $\gamma = 0$, so the inverse map is actually the identity (which shouldn’t be too surprising for a group scheme of order 2!). These conditions are also sufficient. We can now classify group schemes of order 2 completely.

**Proposition 3.** The scheme $G_{\alpha, \beta} = \text{Spec } R[T]/(T^2 + \alpha T)$ with group law $T \mapsto U + V + \beta UV$ and $\alpha \beta = 2$ is a group scheme. The schemes $G_{\alpha, \beta}$ and $G_{\alpha', \beta'}$ are isomorphic if and only if $\alpha = u \alpha'$ and $\beta = u^{-1} \beta'$ for some $u \in R^\times$. The Cartier dual of $G_{\alpha, \beta}$ is $G_{\beta, \alpha}$.

Since Cartier duality is a functor, it is possible to dualize maps. If $k = \mathbb{F}_p$ and $G$ is a $k$-group scheme, we have a Frobenius map $\sigma : G \to G$ which is the identity on points and the $p^{th}$ power map on sections. Let $G^{(p)}$ be the fiber product

$$\begin{array}{ccc}
G^{(p)} & \longrightarrow & G \\
\downarrow & & \downarrow \\
\text{Spec } k & \underset{\sigma}{\longrightarrow} & \text{Spec } k
\end{array}$$

The induced map $F : G \to G^{(p)}$ coming from $\sigma : G \to G$ and $X \to \text{Spec } k$ is the (relative) Frobenius map.

Of course, we also have a Frobenius map on $G^\lor$, namely $F : G^\lor \to (G^{(p)})^\lor$. Dualizing this gives us a map $V : G^{(p)} \to G$, which we call the Verschiebung. The compositions $V \circ F$ and $F \circ V$ are both multiplication by $p$.

**Example.** (1) For $G = \alpha_p$, $F$ and $V$ are both zero.

(2) For $G = \mu_p$, $F$ is zero and $V$ is an isomorphism.

(3) For $G = \mathbb{Z}/n\mathbb{Z}$, $F$ is an isomorphism.

2. **Quotients for finite flat group schemes**

Let $R$ be a ring with $S = \text{Spec } R$, $G$ a finite flat (commutative) $R$-group scheme, and $H$ a finite flat $R$-subgroup scheme of $G$. We’d like to construct a quotient $G/H$ that has reasonable properties that quotients typically have.

In the finite flat case, there’s a neat trick that allows us to construct the quotient more easily than we would be able to do in full generality. We first prove a lemma:

**Lemma 4.** Let $f : H \to G$ be a map of $R$-group schemes. Then $f$ is a closed immersion if and only if the Cartier dual $f^\lor$ is faithfully flat.
Proof. Suppose that \( f \) is a closed immersion. We apply the fibral flatness theorem to show that \( f^\vee \) is flat.

**Theorem 5** (Fibral Flatness Theorem). Suppose \( g : X \to S \) and \( h : Y \to S \) are locally of finite presentation and \( \phi : X \to Y \) is an \( S \)-morphism. Then the following are equivalent:

1. \( g \) is flat and \( \phi_s : X_s \to Y_s \) is flat for all \( s \in S \).
2. \( h \) is flat at all points of \( \phi(X) \) and \( \phi \) is flat.

Hence we must show that \( f_s : H_s^\vee \to G_s^\vee \) is flat for all \( s \in S \). In other words, we’ve reduced to the case in which \( S \) is \( \text{Spec} \) of a field \( k \).

If \( G = \text{Spec} \ A \) and \( H = \text{Spec} \ B \), then the underlying ring map \( A \to B \) is surjective, so the map on duals \( \text{Hom}(B,k) \to \text{Hom}(A,k) \) is injective. Now, the desired result follows from a Theorem proven in Waterhouse’s *Introduction to Affine Group Schemes*:

**Theorem 6.** Let \( A \subset B \) be Hopf algebras over a field. Then \( B \) is faithfully flat over \( A \).  

Now, the construction of quotients is as follows. Let \( f : H \to G \) be a closed immersion of finite flat commutative group schemes. Then since \( f^\vee : G^\vee \to H^\vee \) is faithfully flat, its kernel \( K \) is also finite flat, so we have a sequence

\[
0 \to K \to G^\vee \to H^\vee
\]

of finite flat group schemes. We define \( K^\vee \), together with the map \( G \to K^\vee \), to be the cokernel of \( f \), and we write \( G/H \) instead of \( K^\vee \).

**Definition 7.** Let

\[
0 \to G' \xrightarrow{f} G \xrightarrow{g} G'' \to 0
\]

be a sequence of finite flat group schemes. We say that this sequence is exact if

1. \( f \) is a closed immersion, and
2. \( G'' \) is the cokernel of \( f \).

It’s important to verify that \( G/H \) has the desired properties of quotients. In particular, it should satisfy the universal mapping property of quotients, and we should have \( |G/H| \times |H| = |G| \).

**Proposition 8.** The composite map \( H \to G \to G/H \) is zero. The group scheme \( G/H \) satisfies the universal mapping property for quotient, namely that if \( G \to M \) is a map of group schemes so that \( H \to G \to M \) is the zero map, then \( G \to M \) factors through \( G/H \).
Proof. By construction, \((G/H)^\vee\) is the kernel of \(G^\vee \to H^\vee\), so the composite map \((G/H)^\vee \to G^\vee \to H^\vee\) is zero. Dualizing, we see that \(H \to G \to G/H\) is also zero. Now suppose we have a map \(G \to M\) so that \(H \to G \to M\) is zero. Dualizing, we have that \(M^\vee \to G^\vee \to H^\vee\) is zero. Hence \(M^\vee \to G^\vee\) factors through \((G/H)^\vee\), as \((G/H)^\vee\) is the kernel of \(G^\vee \to H^\vee\). Dualizing again, \(G \to M\) factors through \(G/H\). ■

Proposition 9. \(H = \ker(\pi : G \to G/H)\).

Proof. It suffices to check the result on \(\mathbb{Z}\)-points. In this case, the proof is virtually identical to that for abelian groups. ■

Proposition 10. If \(f : H \to G\) is a closed immersion, then \(\pi : G \to G/H\) is faithfully flat.


Theorem 11. \(|G/H| \times |H| = |G|\).

Proof. Consider the map \(G \times_{G/H} G \to G \times H\) given by \((x, y) \mapsto (x, x^{-1}y)\). (This map does actually land in \(G \times H\) because \(x\) and \(y\) must be in the same coset modulo \(H\) if \((x, y) \in G \times_{G/H} G\).) This map is an isomorphism, whose inverse is given by \((a, b) \mapsto (a, ab)\). Hence, by counting ranks in this isomorphism, we have

\[
\frac{|G|^2}{|G/H|} = |G| \times |H|,
\]

or

\[
|G/H| \times |H| = |G|,
\]

as desired. ■

Proposition 12. Suppose we have an exact sequence

\[0 \to G_1 \to G_2 \to G_3 \to 0,\]

where the \(G_i\) are finite flat commutative group schemes. Then Cartier duality gives us another exact sequence

\[0 \to G_3^\vee \to G_2^\vee \to G_1^\vee \to 0.\]

3. The connected-étale sequence

Let \(G = \text{Spec} A\) be a finite flat group scheme over \(k\). Then \(A\) is a product of local \(k\)-algebras, \(A = \prod_i A_i\), so \(G = \text{Spec} A = \bigsqcup_i \text{Spec} A_i\). The unit section \(A \to k\) factors through some \(A_0\) as \(A \to A_0 \to k\).

Definition 13. For \(\varepsilon : A \to A_0 \to k\), \(G^0 = \text{Spec} A_0\) is called the connected component of the identity.
If $G^0$ is the connected component of $G$, then $G^0$ is a finite flat subgroup scheme of $G$.

If $G = \text{Spec } A$ is finite flat over a henselian local ring $R$, we can still define the connected component $G^0$ in a similar manner. In this situation, $G^0$ is the spectrum of a henselian local $R$-algebra with the same residue field as $R$ and is a finite flat subgroup scheme of $G$.

We'll now discuss étale algebras and schemes. First, we'll work over a field $k$.

**Definition 14.** A finite $k$-algebra $A$ is said to be étale if $A = \prod_i k_i$, where each $k_i/k$ is a finite separable field extension. A finite affine $k$-group scheme $G = \text{Spec } A$ is étale if $A$ is an étale algebra.

Let $\Gamma$ be the absolute Galois group of $k$. We have a functor

$$\{\text{finite étale algebras}\} \to \{\text{finite } \Gamma\text{-sets}\}$$

given by

$$A \mapsto \text{Hom}_k(A, \bar{k})$$

(or $\text{Hom}_k(A, k^{\text{sep}})$). In fact, this functor induces an equivalence of categories. Similarly, we have an equivalence of categories between the category of finite étale affine commutative $k$-group schemes and finite $\Gamma$-modules.

Under this equivalence, the constant group schemes correspond to the $\Gamma$ modules with trivial Galois action.

**Example.** Take $k = \mathbb{R}$, and look at $\mu_3 = \text{Spec } A$, where $A = \mathbb{R}[X]/(X^3 - 1) \cong \mathbb{R} \times \mathbb{C}$. Then $\mu_3(\mathbb{C}) = \text{Hom}_\mathbb{R}(\mathbb{R} \times \mathbb{C}, \mathbb{C}) = \{f_1, f_2, f_3\}$, where $f_1 : \mathbb{R} \to \mathbb{C}, \mathbb{C} \to 0$, $f_2 : \mathbb{R} \to 0, \mathbb{C} \to \mathbb{C}$, and $f_3 : \mathbb{R} \to 0, \mathbb{C} \to \mathbb{C}$. If $\sigma$ is complex conjugation, then $\sigma$ fixes $f_1$ and switches $f_2$ and $f_3$.

**Theorem 15 (Cartier).** If $k$ is a field of characteristic 0, then every finite group scheme is étale.

We also need to discuss étale group schemes over a ring. Let $R$ be a connected noetherian base ring, and let $G$ be a finite $R$-group scheme. Then $G = \text{Spec } A$ is étale if it is flat, and $A \otimes k$ is étale for any residue field $R \to k \to 0$. Equivalently, $G$ is étale if the discriminant of $A$ is a unit, or if it is nonzero on any special fiber.

**Theorem 16.** Let $R$ be a henselian local ring or a field with $S = \text{Spec } R$, and let $G$ be a commutative affine group scheme, flat and of finite type over $R$. Then there is an exact sequence

$$0 \to G^0 \to G \to G^\text{ét} \to 0,$$

where $G^0$ is a connected, finite flat subgroup scheme over $R$, and $G^\text{ét} = G/G^0$ is an étale finite group scheme over $R$. 
Proof. We’ll start with some generalities. Let \( T \) be a scheme finite over \( S \). Then \( T = \text{Spec} \ B \) for some finite \( R \)-algebra \( B \). Then \( B = \prod B_i \), where each \( B_i \) is a local henselian ring. Hence \( T = \bigsqcup T_i \) is a finite disjoint union of connected open subschemes \( T_i = \text{Spec} \ B_i \). The \( T_i \) are the connected components of \( T \). For each \( i \), let \( t_i \) be the closed point of \( T_i \) with residue field \( k_i \). Let \( s \in S \) be the closed point with residue field \( k \). Let \( \alpha \) be the geometric point of \( S \) corresponding to an algebraic closure \( \overline{k} \) of \( k \). Let \( \Gamma \) be the absolute Galois group of \( k \). Then \( \Gamma \) acts on 
\[
T(\alpha) = \text{Hom}(A, \overline{k}) = \bigoplus \text{Hom}_k(k_i, \overline{k})
\]
by its action on \( \overline{k} \). The functor \( T \mapsto T(\alpha) \) from finite \( S \)-schemes to finite \( \Gamma \)-sets commutes with products and disjoint unions. From this, we can deduce a few things:

1. The \( T_i(\alpha) \) are the orbits for the action of \( \Gamma \) on \( T(\alpha) \), so \( T \) is connected if and only if \( \Gamma \) acts transitively on \( T(\alpha) \).
2. \( T_i \times_S T_j \) is connected if and only if at least one of \( T_i(\alpha) \) and \( T_j(\alpha) \) is a singleton
   if and only if at least one of \( k_i \) and \( k_j \) is purely inseparable over \( k \).
3. The connected components of the closed fiber \( T_s \) are the closed fibers \( (T_i)_s \) of the connected components of \( T \).

Now, suppose \( G \) is a finite \( S \)-group scheme. Let \( G^0 \) be the connected component of \( G \) which contains the image of the identity section \( \varepsilon : S \to G \). Then \( S \) is a closed subscheme of the connected scheme \( G^0 \) so they have the same residue field \( k \). By (2) from the above, we see that for each connected component \( G_i \) of \( G \), \( G_i \times_S G^0 \) is connected. Its image \( G_i G^0 \) under the multiplication map \( G \times_S G \to G \) is connected and contains \( G_i S = G_i \), so it’s equal to \( G_i \). Hence, \( G^0 G^0 = G^0 \). The inverse map also preserves \( G^0 \) because it is an automorphism of \( S \) preserving the identity section. Thus \( G^0 \) is an open and closed subgroup scheme of \( G \).

Since \( G \) is finite flat over \( S \), every component of \( G \) is finite flat, so we can take the quotient \( S \)-group scheme \( G^{\text{ét}} = G/G^0 \), and \( G^{\text{ét}} \) is again finite flat, and \( |G| = |G^{\text{ét}}| \times |G^0| \). Since \( G^0 \) is open in \( G \), the unit section \( G^0 \cap G^0 = S \) is open in \( G/G^0 = G^{\text{ét}} \), so \( G^{\text{ét}} \) is étale.

Note now that there are no nontrivial homomorphisms from a connected \( S \)-group scheme to an étale one, because such a map would factor through the identity component of the étale one, which is the unit section. Hence, a map of \( G \) into an étale \( S \)-group \( H \) has kernel containing \( G^0 \) and hence factors through \( G/G^0 \).

Suppose \( R \) is a henselian local ring with fraction field \( K \), and let \( G \) be a finite flat commutative group scheme. Then we have the connected-étale sequence
\[
0 \to G^0 \to G \to G^{\text{ét}} \to 0.
\]
If we make a local base change \( R'/R \), then \( G^0_{R'} = G^0 \times_R R' \) and \( G^{\text{ét}}_{R'} = G^{\text{ét}} \times_R R' \), so in this case, the connected-étale sequence is well-behaved. Under non-local base changes, however, the story is much more complicated.
**Proposition 17.** If the residue characteristic of $R$ is zero, then $G^0 = S$, and $G = G^{\text{ét}}$. If it’s $p > 0$, then $[G^0 : S]$ is a power of $p$. Furthermore, if $|G|$ is invertible in $S$, then $G = G^{\text{ét}}$ and $G^0 = S$.

*Proof.* See Tate, §3.7.II, pages 138–141. ■

**Definition 18.** An affine finite group scheme $G = \text{Spec } A$ over a field $k$ is called an infinitesimal group scheme if $A$ is a local $k$-algebra with maximal ideal $m$, and there is some $r \in \mathbb{N}$ so that $x^{p^r} = 0$ for all $x \in m$.

**Proposition 19.** If $R = k$ is a perfect field, the map $G \to G^{\text{ét}}$ has a unique section, so that $G$ is a semidirect product $G = G^0 \rtimes G^{\text{ét}}$.

*Proof.* The only interesting case is that of $\text{char } k = p > 0$, for the characteristic zero case is taken care of by the previous result. Let $G = \text{Spec } A$ be a finite $k$-group scheme. Let $N$ be the nilradical of $A$, so that $G_{\text{red}} = \text{Spec } (A/N)$. Since $k$ is assumed perfect, $G_{\text{red}}$ is étale over $k$. Then $G_{\text{red}} \times G_{\text{red}}$ is reduced, so the map

$$G_{\text{red}} \times G_{\text{red}} \hookrightarrow G \times G \to G$$

factors through $G_{\text{red}}$ and hence induces the structure of a $k$-group scheme on $G_{\text{red}}$. Let $\alpha = \text{Spec } (\overline{k})$ be a geometric point of $S$. Then the isomorphisms $G_{\text{red}}(\alpha) = G(\alpha) = G^{\text{ét}}(\alpha)$ show that the restriction to $G_{\text{red}}$ of the map $G \to G^{\text{ét}}$ is an isomorphism. Thus we have a section $G^{\text{ét}} \to G$ and thus a semidirect product decomposition $G \cong G^0 \rtimes G^{\text{ét}}$. Uniqueness of the section follows because a map from an étale scheme to an infinitesimal scheme with a rational point is constant. ■

We sometimes call a group scheme local rather than connected. We say $G$ is of type $(l,e)$ (and so forth) if $G$ is local and $G^\vee$ is étale (and so forth). For any such $G$ over a perfect field $k$, there is a unique decomposition

$$G = G_{e,e} \times G_{e,l} \times G_{l,e} \times G_{l,l},$$

where the notation is what one would expect it to be.

**Example.** Let $k$ be algebraically closed of characteristic $p > 0$. Then we can partially classify the four basic types of commutative groups.

1. The $\alpha_{p^n}$ are local-local. (There are others as well.)
2. The only étale-étale groups are reduced of order prime to $p$.
3. Étale-local groups are direct products of $\mathbb{Z}/p^n\mathbb{Z}$’s.
4. Local-étale groups are the duals of $p$-groups, and hence direct products of $\mu_{p^n}$’s.

**Definition 20.** We say that the Frobenius (resp. Verschiebung) is nilpotent if some iterate $F^n$ (resp. $V^n$) is zero.

**Proposition 21.** Let $G$ be a finite flat commutative group scheme, and let $F$ and $V$ be the Frobenius and Verschiebung maps, respectively.
(1) $G$ is étale-étale if and only if $F$ and $V$ are both isomorphisms.
(2) $G$ is étale-local if and only if $F$ is an isomorphism and $V$ is nilpotent.
(3) $G$ is local-étale if and only if $F$ is nilpotent and $V$ is an isomorphism.
(4) $G$ is local-local if and only if $F$ and $V$ are both nilpotent.

4. Torsion in abelian varieties

Let $A$ be an abelian scheme. We consider the group scheme $G = A[n]$. It fits into a connected-étale sequence

$$0 \to G^0 \to G \to G^{\text{ét}} \to 0.$$ 

Let’s investigate the connected component and the étale quotient. Suppose we’re working over a complete dvr $R$ with fraction field $K$, residue field $k$, and with $n$ invertible in $K$. Then every $\overline{K}$-point of $G$ lives in some finite extension $K'/K$ with valuation ring $R'/R$ and residue field $k'/k$, and integrality considerations show that actually $G(R') = G(K')$. Since $\text{Spec } R'$ is connected, a point in $G(R')$ lies in $G^0(R')$ if and only if its specialization in $G_k(k')$ vanishes. Hence $G^0(\overline{K})$ consists of those points in $G(\overline{K})$ whose specializations into the geometric points of $A_k$ are 0.

So, that’s the story for the connected component of the identity. Now we need to understand the étale quotient.

The geometric points of the $n$-torsion of $A_k$ are in bijection with the geometric points of the special fiber of the maximal étale quotient $A[n]^\text{ét}$. If $n$ is not divisible by the characteristic of $K$ and $K'/K$ is a large enough finite extension to contain all the coordinates of $A_K[n]$, then $A[n]^\text{ét}_{R'}$ is a constant scheme.

Suppose $E$ is an elliptic curve over a $p$-adic dvr $R$. If $E$ has supersingular reduction, then $E[p] = E[p]^0$, and the étale quotient is trivial.

If $E$ has ordinary reduction, then $E[p]^0$ and $E[p]^\text{ét}$ each have order $p$. To see that the connected part has order $p$, note that the connected part commutes with passage to the geometric special fiber, where the connected part has order $p$. On the other hand, $E[p]$ has order $p^2$ since $[p] : E \to E$ is finite flat of degree $p^2$.

Now, let $E_0$ be an ordinary elliptic curve over a finite field $k$ of characteristic $p$, and let $G = E_0[p]$. Then $G = G^0 \times G^{\text{ét}}$ with $G^0$ local of order $p$ and $G^{\text{ét}}$ étale of order $p$. Passing to a finite extension $k'/k$ if necessary so that $G^{\text{ét}}$ as a Galois module has trivial Galois action, we have $G^{\text{ét}} = (\mathbb{Z}/p\mathbb{Z})$. By a result of Cartier and Nishi, the $N$-torsion of an elliptic curve is always self-dual (in any characteristic), so the local Cartier dual $(G^{\text{ét}})^\vee = (\mathbb{Z}/p\mathbb{Z})^\vee = \mu_p$ must be $G^0$. Mike and Brandon will discuss how to lift $E_0$ to an elliptic curve $E$ over $W(k)$ so that $E[p] \cong \mu_p \times \mathbb{Z}/p\mathbb{Z}$ as $W(k)$-group schemes. If $F$ is the fraction field of $W(k)[\mu_p]$, we get a point $E[p](F)$ defining $(\mathbb{Z}/p\mathbb{Z})_F \to E_F$ whose scheme-theoretic closure in $E_{W(k)[\mu_p]}$ is $\mu_p$, which is local.

5. References

Here are some further references for this material:
(1) Schoof’s “Introduction to finite group schemes,” at www.cems.uvm.edu/~voight/notes/274-Schoof.pdf.
(2) Shatz’s “Group schemes, formal groups, and $p$-divisible groups,” in Arithmetic geometry by Cornell and Silverman.
(3) Tate’s “Finite flat group schemes,” in Modular forms and Fermat’s last theorem by Cornell, Silverman, and Stevens.
(4) Waterhouse’s Introduction to affine group schemes.