Lecture 6

November 25, 2004
Notes by Charles Mitchell

§14 Frobenius and Verschiebung

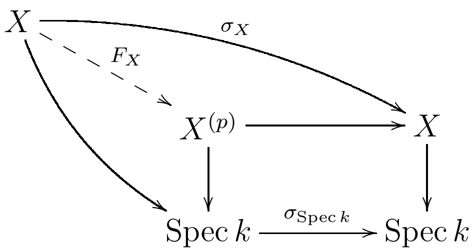
Definition. The *absolute Frobenius morphism* $\sigma_X : X \to X$ of a scheme over $\mathbb{F}_p$ is the identity on points and the map $a \mapsto a^p$ on sections. Note that this is functorial: for all morphisms $\varphi : X \to Y$ of schemes over $\mathbb{F}_p$, the diagram

$$\begin{CD} X @>{\varphi}>> Y \\ @V{\sigma_X}VV @VV{\sigma_Y}V \\ X @>{\varphi}>> Y \end{CD}$$

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:



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:

$$\begin{CD} X @>{F_X}>> X^{(p)} = X \otimes_{k,\sigma} k \\ @V{\varphi}VV @VV{\varphi^{(p)} = \varphi \otimes id}V \\ Y @>{F_Y}>> Y^{(p)} = Y \otimes_{k,\sigma} k \end{CD}$$

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

$$\begin{array}{ccc}
X \times_k Y & \xrightarrow{F_X \times F_Y} & X^{(p)} \times_k Y^{(p)} \\
& \searrow^{F_{X\times Y}} & \wr\| \\
& & (X \times_k Y)^{(p)}
\end{array}$$

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

$$\begin{array}{ccc}
X_{k'} & \xrightarrow{F_{X_{k'}}} & (X_{k'})^{(p)} \\
& \searrow^{(F_X)_{k'}} & \wr\| \\
& & (X^{(p)})_{k'}
\end{array}$$

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

$$\begin{array}{ccccc}
x \cdot a^p & \longleftarrow\!\shortmid & [x(a \otimes \cdots \otimes a)] & \longleftarrow\!\shortmid & a \otimes x \\
A & \twoheadleftarrow & \operatorname{Sym}^p A & \hookleftarrow & A \otimes_{k,\sigma} k \\
& \nwarrow^{\text{mult}} & \uparrow & & \\
& & A^{\otimes p} & &
\end{array}$$

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 $\mathrm{Sym}^p A$, 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

$$\begin{array}{ccccc} A & \hookrightarrow & (A^{\otimes p})^{S_p} & \xrightarrow{\lambda_A} & A \otimes_{k,\sigma} k \\ & \searrow^{\text{comult}} & \big\downarrow & & \\ & & A^{\otimes p} & & \end{array}$$

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 $G = \mathrm{Spec}\, A$. 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:

$$\begin{array}{ccc} G^{(p)} & \xrightarrow{V_G} & G \\ {\scriptstyle \varphi^{(p)}}\big\downarrow & & \big\downarrow{\scriptstyle \varphi} \\ H^{(p)} & \xrightarrow[V_H]{} & H \end{array}$$

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

$$\begin{array}{ccc} (G \times H)^{(p)} & \cong & G^{(p)} \times H^{(p)} \\ & \searrow_{V_{G\times H}} & \big\downarrow{\scriptstyle V_G \times V_H} \\ & & G \times H \end{array}$$

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

$$\begin{array}{ccc} (G_{k'})^{(p)} & \cong & (G^{(p)})_{k'} \\ & \searrow_{V_{(G_{k'})}} & \big\downarrow{\scriptstyle (V_G)_{k'}} \\ & & G \end{array}$$

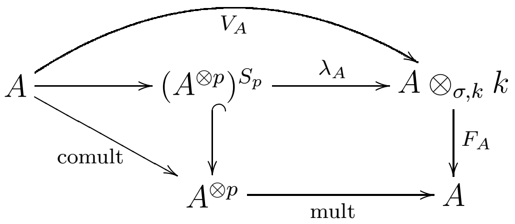
We are now in a position to tackle the above question (b).

Theorem 14.4. For any affine commutative group scheme G,

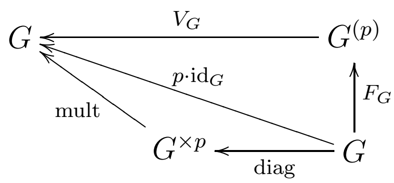
(a) $V_G \circ F_G = p \cdot \mathrm{id}_G$,

(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:

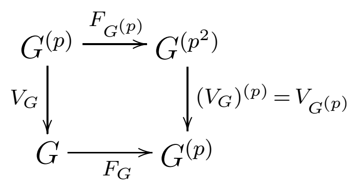


The definition of λ_A implies that the right hand square commutes. In terms of group schemes, this diagram becomes



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



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) $G_{k^{\text{sep}}}$ 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) $G_{k^{\text{sep}}}$ is a direct sum of $\mu_{n_i,k^{\text{sep}}}$ 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 $G^{\mathrm{red}} \subset G$ with the same support as G is a closed subgroup scheme, and the map $(g, g') \mapsto g + g'$ defines an isomorphism $G^0 \oplus G^{\mathrm{red}} \xrightarrow{\sim} G$.

Proof. As k is perfect, all residue fields of G^{red} are separable over k, implying that $G^{\mathrm{red}} \times G^{\mathrm{red}} \subset G \times G$ is again reduced. Therefore the restriction to $G^{\mathrm{red}} \times G^{\mathrm{red}}$ 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 $G^{\mathrm{red}} \to G/G^0$ is an isomorphism. Since the formation of both sides is compatible with base extension, we may assume that k is separably closed. Then $G^{\mathrm{red}} \to G/G^0$ is a bijective homomorphism between constant group schemes and hence an isomorphism. □

Example. Regard an inseparable field extension $k' = k(\sqrt[p]{u}) \supsetneq k$. 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

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

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

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

This sequence is non-split, because $G_i \cong \operatorname{Spec} k' \ncong G_0$ 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 $G^0 = G_0 \cong \alpha_{p,k}$, and we have a short exact sequence

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

This sequence is non-split, because $G_i \cong \operatorname{Spec} k' \ncong G_0$ for $i \neq 0$.

Definition. A finite commutative group scheme G is called *local* if $G = G^0$ and *reduced* if $G = G^{\mathrm{red}}$. 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

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

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 $1 \le i \le n$, and therefore A is a quotient of $k[X_1, \ldots, X_n]/(X_1^p, \ldots, X_n^p)$. In particular $|G| = \dim_k A \le p^n$.

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 $0 \le i < n$. 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 $|G| \le p^n$, 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. □