Finite Flat Group Scheme

Hung Chiang

February 5, 2023

1 Finite Flat Group Schemes

1.1 Group Scheme

Definition 1. Let S be a Scheme. A group scheme G/S is a contravariant functor $G : (\mathrm{Sch}/S) \to (\mathrm{Groups})$ such that $(\mathrm{Sch}/S) \xrightarrow{G} (\mathrm{Groups}) \to (\mathrm{Sets})$ is a representable functor. A group scheme is commutative if it takes value in the full subcategory of abelian groups.

Equivalently, G is a scheme over S along with morphisms $m : G \times_S G \to G$, $\epsilon : S \to G$, $\iota : G \to G$ in the categories corresponding to multiplication, identity, inverse maps of groups. To be explicit, these morphisms should satisfies the following relations:

1. Assosiciativity:

$$m \circ (\mathrm{id}_G \times m) = m \circ (m \times \mathrm{id}_G) : G \times_S G \times_S G \to G.$$

2. Identity:

$$G = S \times_S G \xrightarrow{\epsilon \times \mathrm{id}_G} G \times_S G \xrightarrow{m} G$$

and

$$G = G \times_S S \xrightarrow{\mathrm{id}_G \times \epsilon} G \times_S G \xrightarrow{m} G$$

are both id_G.

3. Inverse:

$$G \xrightarrow{\Delta} G \times_S G \xrightarrow{\iota \times \mathrm{id}_G} G \times_S G \xrightarrow{m} G$$

and

$$G \xrightarrow{\Delta} G \times_S G \xrightarrow{\mathrm{id}_G \times \iota} G \times_S G \xrightarrow{m} G$$

are both the map $G \to S \xrightarrow{\epsilon} G$.

Once we have maps satisfying these relations, we can show that the representable functor h_G naturally lifts to a group functor.

Here are some examples of group schemes.

1. $\mathbb{G}_a : T \mapsto \Gamma(T, \mathcal{O}_T)$ is a group scheme, represented by $\mathbb{A}^1_S$.

2. $\mathbb{G}_m : T \mapsto \Gamma(T, \mathcal{O}_T^*)$ is a group scheme, represented by $S \times \operatorname{Spec}(\mathbb{Z}[t, t^{-1}])$. More generally, we have GL_n and many other subgroup schemes.

3. Let G be a group. The constant sheaf $\underline{G}$ defines a group scheme. It sends T to the group of locally constant functions from T to G. This is represented by the disjoint union of pieces of S indexed by elements of G. In particular, S it self represents the functor of trivial group.

4. Fiber products of group schemes over a group scheme is a group scheme. In particular, the kernel of a morphism of group schemes is a group scheme, represented by the fiber product

$$\begin{array}{ccc} \ker(\varphi) & \longrightarrow & S \\ \downarrow & & \downarrow{\scriptstyle \epsilon_H} \\ G & \xrightarrow{\varphi} & H \end{array} .$$

   However, in general, the cokernel of a morphism fails to be a group scheme.

5. Let $S' \to S$ be a S-scheme and G be a group scheme over S. Then $G \times_S S'$ is a group scheme over S'. The corresponding group functor is $T \mapsto G(T)$, where on RHS T is regarded as a S-scheme via $T \to S' \to S$.

Let G/S be a group scheme. G/S is separated iff $\epsilon : S \to G$ is a closed immersion.

1.2 Affine Group Schemes

Let $S = \operatorname{Spec}(R)$. We consider group schemes represented by affine schemes over S. That is, $G = \operatorname{Spec}(A)$ for some $A \in (\mathrm{Alg}_R)$. A should define a group functor on the category of (Alg_R), which is equivalent to that A is given a Hopf algebra structure, and once this is satisfied, $\operatorname{Spec}(A)$ actually becomes a group functor on $\mathrm{Sch} / \operatorname{Spec}(R)$. We denote by Δ the comultiplication, ϵ the counit, and S the antiinvolution. The counit is an surjective ring homomorphism $R \to A$, the kernel I called the argumentation ideal of G/R.

Proposition 1. $G = \operatorname{Spec}(A)$ is abelian group iff A is cocommutative.

Proof. G is abelian iff the diagram is commutative

$$\begin{array}{ccc} G \times_R G & \xrightarrow{\Phi} & G \times_R G \\ & {\scriptstyle m} \searrow & \downarrow{\scriptstyle m} \\ & & G \end{array}$$

where Φ interchange these two pieces of G. In terms of algebras, this diagram is

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes_R A \\ & {\scriptstyle \Delta} \searrow & \downarrow{\scriptstyle \Phi} \\ & & A \otimes_R A \end{array}$$

where Φ interchange these two pieces of A. This is exactly the cocommutativity. $\square$

1.3 Finite Flat Group Schemes

A finite flat groups scheme over S is a group scheme G/S of which the structure morphism is finite and flat. If the base is locally Noetherian, this is equivalent to that G/S is finite locally free. We always assume we are in this case. We can define the local rank, which is a locally constant function on the base, called the order of G, denoted by $|G|$.

If $S = \mathrm{Spec}(R)$, a group scheme G over S is finite flat iff $G = \mathrm{Spec}(A)$ where A is a finite flat R-Hopf algebra.

Example 1.

1. $\mu_n/S := S \times \mathrm{Spec}(\mathbb{Z}[X]/(X^n - 1))$ is finite free of order n.
2. Let G be a finite group. $\underline{G}$ is finite free.
3. If S is over $\mathbb{F}_p$, $\alpha_p := \ker(F_{G_a/S})$ is finite free of order p. It is represented by $S \times_{\mathbb{F}_p} \mathbb{F}_p[X]/(X^p)$.

If G is also smooth, G is a finite étale group scheme. Let S be a connected scheme and $\overline{s}$ be a geometric point. The fiber at $\overline{s}$ gives an equivalence of categories between the category of finite étale group schemes over S and the category of finite continuous $\pi_1(S, \overline{s})$-sets.

1.4 Cartier Duality

Let $S = \mathrm{Spec}(R)$ and G be a finite locally free group scheme over R. Then $G = \mathrm{Spec}(A)$ where A is a Hopf algebra over R, and is finite projective. It is possible to define $A^\vee := \mathrm{Hom}_R(A, R)$ as a Hopf algebra as $(A \otimes_R A)^\vee = A^\vee \otimes_R A^\vee$. It is cocommutative and is commutative iff A is cocommutative, namely, G is abelian. In this case, The corresponding group scheme is denoted by G^D, the Cartier dual of G. By construction, there is a natural isomorphism $(G^D)^D \cong D$.

Example 2. Let G be a finite group. $\underline{G}/R$ is represented by the Hopf algebra $\prod_{g \in G} Re_g$, where each e_g is the function taking 1 on the gth piece of $\mathrm{Spec}(R)$ and 0 on other pieces. The comultiplication is $\Delta(e_g) = \sum_{h \in G} e_{gh^{-1}} \otimes e_h$, the counit is $e_g \mapsto \delta(g)$, and the coinverse is $S : e_g \mapsto e_{g^{-1}}$. The algebra sturcture of $A^\vee$ is $R[G]$, where $\{g\}$ is the dual basis of $\{e_g\}$. In other words, g means taking value on the gth piece. Therefore, $\Delta(g) = g \otimes g$, $\epsilon(g) = 1$ for all g, and $S(g) = g^{-1}$.

Theorem 1. For every commutative R-algebra T,

$$\mathrm{Hom}_{\mathrm{Alg}/R}(A^\vee, T) = \mathrm{Hom}_T(G_T, \mathbb{G}_m / T).$$

In particular, when G is abelian, G^D represents the abelian group functor $\mathscr{H}om(G, \mathbb{G}_m)$, and we in turn use this as the definition of G^D.

Proof. $\mathrm{Hom}_R(A^\vee, T) = A \otimes_R T$. Let $g \in A \otimes_R T$. g is an R-algebra homomorphism iff $g(1_{A^\vee}) = 1_T$ and the diagram

$$\begin{array}{ccc} A^\vee \otimes_R A^\vee & \xrightarrow{m^\vee} & A^\vee \\ \downarrow{\scriptstyle g\otimes g} & & \downarrow{\scriptstyle g} \\ T \otimes_R T & \xrightarrow{m_T} & T \end{array}$$

is commutative. RHS is identified as the group of units in $u \in (A \otimes_R T)^\times$ satisfying that $\Delta_T(u) = u \otimes u \in A \otimes_R T \otimes_T A \otimes_R T = A \otimes_R A \otimes_R T$. We should equate these two groups. By replacing A with A_T and R-alg with T-alg we may assume that $R = T$.

Suppose g is in LHS. The identity in $A^\vee$ is the map $\epsilon : A \to R$. Therefore, $g(1_{A^\vee}) = \epsilon(g) = 1$. The commutative diagram

$$\begin{array}{ccc} A^\vee \otimes_R A^\vee & \xrightarrow{m^\vee} & A^\vee \\ \downarrow{\scriptstyle g\otimes g} & & \downarrow{\scriptstyle g} \\ R \otimes_R R & \xrightarrow{m_R} & R \end{array}$$

is equivalent to that for every $\phi, \psi \in A^\vee$, $\phi(g)\psi(g) = (\phi \otimes \psi)(\Delta(g))$. This is equivalent to that $\Delta(g) = g \otimes g$. Now We prove that g is a unit by showing that $S(g)g = 1$. Since S corresponds to the inverse, we have that

$$m \circ (S \otimes \mathrm{id}_A) \circ \Delta = \epsilon : A \to R \to A.$$

Putting g and we have

$$S(g)g = 1.$$

Suppose $u \in A^\times$ satisfying that $\Delta(u) = u \otimes u$. This u makes the diagram above commutative. Moreover, the counit gives that equation

$$\mathrm{id}_A = (\epsilon \otimes \mathrm{id}_A) \circ \Delta : A \to A.$$

Putting u and we have $\epsilon(u) = 1$.

We look at group structures of both sides. RHS is exactly the multiplication in $A^\times$. Therefore, we should show that if g_1, g_2 are in LHS, the map

$$A^\vee \xrightarrow{\Delta^\vee} A^\vee \otimes_R A^\vee \xrightarrow{g_1 \otimes g_2} R$$

is $g_1 g_2$. This is true as the map sends a to $(g_1 \otimes g_2)(\Delta(a)) = m(g_1, g_2)(a) = (g_1 g_2)(a)$. $\square$

The universal family is $1_{A^\vee} \in A^\vee \otimes_R A$. The morphism $G^D \times G \to \mathbb{G}_m$ is given by the R-algebra homomorphism determined by $t \mapsto 1_{A^\vee}$.

We see that G^D commute with base extension and direct product. When the base is not affine, G^D exists locally and glue into a global solution.

Example 3. Let $G = \underline{\mathbb{Z}/n\mathbb{Z}}_R$. $A^\vee = R[\mathbb{Z}/n\mathbb{Z}] = R[X]/(X^n - 1)$ where $X = [1]$. We have $\Delta(X) = X \otimes X$, $\epsilon(X) = 1$, and $S(X) = [n-1] = X^{n-1} = X^{-1}$. Therefore, $G^D = \mu_n$ and the pairing $G(T) \times G^D(T) \to G_m(T)$ is $(a, f) \mapsto f^a$.

Example 4. Let R be a $\mathbb{F}_p$-algebra and $G = \alpha_p = R[X]/(X^p)$. α_p is self-dual and the pairing $\alpha_p(T) \times \alpha_p(T) \to \mathbb{G}_m(T)$ is

$$(a, b) \mapsto \exp(a + b) := 1 + \sum_{n=1}^{p-1} \frac{(a+b)^n}{n!}.$$

In particular, $\underline{\mathbb{Z}/p\mathbb{Z}}_R$, μ_n/R, and α_p are mutually non-isomorphic: Take a geometric fiber and we have that $\underline{\mathbb{Z}/p\mathbb{Z}}$ is reduced while μ_p and α_p are non-reduced.

Example 5. Let A, B be abelian schemes and $\varphi : A \to B$ be an isogeny. The exact sequence

$$0 \to \ker(\varphi) \to A \to B \to 0$$

induces the long exact sequence

$$\begin{aligned} 0 &\to \mathscr{H}om(B, \mathbb{G}_m) \to \mathscr{H}om(A, \mathbb{G}_m) \to \mathscr{H}om(\ker(\varphi), \mathbb{G}_m) = \ker(\varphi)^D \\ &\to \mathscr{E}xt^1(B, \mathbb{G}_m) \to \mathscr{E}xt^1(A, \mathbb{G}_m). \end{aligned}$$

$\mathscr{H}om(A, \mathbb{G}_m)$, $\mathscr{H}om(B, \mathbb{G}_m)$ are trivial and $\mathscr{E}xt^1(B, \mathbb{G}_m) \to \mathscr{E}xt^1(A, \mathbb{G}_m)$ is naturally identified with $B^\vee \xrightarrow{\varphi^\vee} A^\vee$. Hence $\ker(\varphi)^D$ is naturally identified with $\ker(\varphi^\vee)$. The pairing $\ker(\varphi) \times \ker(\varphi^\vee) \to \mathbb{G}_m$ is the Weil pairing.

1.5 Connected-étale Sequence

We assume here that $S = \operatorname{Spec}(R)$ where R is a Henselian local ring.

Proposition 2. Let G be a finite flat group scheme over S and G^0 be the connected component of G containing the image of the unit section. Then G^0 is a closed finite flat group subgroup scheme, G/G^0 is étale, denoted by $G^{\text{ét}}$, and every morphism from G to a finite étale group scheme factors through $G^{\text{ét}}$.

Proof. For every finite scheme over S has the form $\operatorname{Spec}(T)$ where $T = T_1 \times \cdots \times T_r$ a product of Henselian local rings. Let k be the residue field of R and k_i be the residue field of T_i. We have $\operatorname{Spec}(T_i)(\overline{k}) = \operatorname{Hom}_k(k_i, \overline{k})$, which is exact a $G_k = \operatorname{Aut}(\overline{k}/k)$-orbit in $\operatorname{Spec}(T)(\operatorname{Spec}(k))$. Therefore, T is connected if and only if $\operatorname{Spec}(T)(\overline{k})$ is a transitive G_k-set.

Let G be a finite flat group scheme over S, say $G = \operatorname{Spec}(T)$, $T = T_1 \times \cdots \times T_r$ as in the previous paragraph. Then each T_i is finite flat over T. Say $G^0 = \operatorname{Spec}(T_1)$. Since the unit section is a closed immersion, we have a surjective map $T_0 \to R$. This identifies k_1 and k. Therefore, the product of G^0 with any component G_i of G is again connected. In particular, $G^0 \times G^0$ is connected. This says that $m(G^0 \times G^0)$ has image in G^0. As the inverse map on G^0 also has image in G^0, G^0 is a finite flat subgroup scheme of G. $G_i \times G^0$ is connected implies $(g, g_0) \mapsto g g_0 g^{-1}$ also has image in G^0, so G^0 is normal.

The quotient $G^{\text{ét}} := G/G^0$ exists as a group scheme. Since G is finite flat, $G^{\text{ét}}$ is also finite flat $|G| = |G^0||G^{\text{ét}}|$. Since G^0 is open, the unit section of $G^{\text{ét}}$ has open image. We conclude that $G^{\text{ét}}$ is étale. □

Proposition 3. If R is a perfect field k, $G \to G^{\text{ét}}$ has a section by G^{red} and G is a semi-direct product $G = G^0 \rtimes G^{\text{ét}}$.

Proof. Again we write $G = \text{Spec}(T)$, $T = T_1 \times \cdots \times T_r$ a product of Artinian local rings. G^{red} is the product of $\text{Spec}(k_i)$. Since k is perfect, G^{red} is étale and $k_i \times_k k_j$ is a product of finite extensions of k. We have that $G^{\text{red}} \times G^{\text{red}}$ is also reduced and a similar argument shows that G^{red} is a closed subgroup of G. The intersection $G^0 \cap G^{\text{red}}$ is trivial by explicit computation. $G^{\text{red}} \to G^{\text{ét}}$ is an isomorphism because $G^{\text{red}}(\overline{k}) = G(\overline{k}) = G^{\text{ét}}(\overline{k})$. □

Example 6. Since $\mu_{p^n}(k) = 1$ if k is a field of characteristic p, for every Henselian local ring R with residue field k of characteristic p, μ_{p^n} is connected.

Example 7. Let k be an algebraically closed field of characteristic p such that $|E[p](k)| = p$. Then we have

$$0 \to E[p]^0 \to E[p] \to E[p]^{\text{ét}} \to 0$$

and both $E[p]^0$, $E[p]^{\text{ét}}$ have order p, Since G_k is trivial, $E[p]^{\text{ét}} \cong \underline{\mathbb{Z}/p\mathbb{Z}}$. Since $E[p] \cong E[p]^D$, taking dual of the exact sequence and we have

$$0 \to \mu_p \to E[p] \to (E[p]^0)^D \to 0.$$

Since μ_p is connected and of order p, we have $E[p]^0 \cong \mu_p$, hence the split exact sequence

$$0 \to \mu_p \to E[p] \to \underline{\mathbb{Z}/p\mathbb{Z}} \to 0.$$

1.6 Deligne's Theorem

Now we assume G/S is a commutative finite flat group scheme with constant rank n.

Theorem 2. $n : G \to G$ is the trivial map.

If the base is a field, the theorem is also true: For every $g \in G(T)$, $g^n = 1$.

Let C be a finite locally free algebra over B with constant rank $n > 0$. Then $\det_B(C) := \bigwedge_B^n C$ is an invertible module over B. For every $c \in C$, $c\cdot \in \text{End}_B(C)$ induces $\det(c) \in \text{End}_B(\det_B(C)) = B$ is well-defined, called the norm map.

Let G be a finite locally free group scheme over $\text{Spec}(R)$, represented by A, and $f : B \to C$ as above. We would like to define a trace map

$$\text{Tr}_f : G(C) \to G(B).$$

Lemma 1. The norm map $N : A^\vee \otimes_R C \to A^\vee \otimes_R B$ restrict to a map $\text{Tr}_f : G(C) \to G(B)$, and if $g \in \text{im}(G(B) \xrightarrow{G(f)} G(C))$, $\text{Tr}_f(g) = g^n$.

Proof. Let $g \in A^\vee \otimes_R C$. $g \in G(C)$ iff $\epsilon^\vee(g) = 1 \in C$ and $\Delta^\vee(g) = g \otimes g$. This gives corresponding properties for $\det(g)$ as det commutes with comultiplication and counit.

In particular, if $g \in \operatorname{im}(A^\vee \otimes_R B \to A^\vee \otimes_R C)$, $N(g) = g^n \in A^\vee \otimes_R B$, which is g^n when regarded as characters of G^D. $\square$

We can now prove the theorem when $S = \operatorname{Spec}(R)$ and G is finite locally free of constant rank n, represented by A. We first show that every element in $G(R)$ is annihilated by n. Let $u \in G(R)$, identified with its image in $G(A)$. Let $\operatorname{Tr} : G(A) \to G(R)$ be induced by the structure map $R \to A$. Consider $\lambda_u : A \to A$ given by $A \xrightarrow{\Delta} A \otimes_R A \xrightarrow{u \otimes \mathrm{id}_A} A$. This is an R-automorphism, and also corresponds to $u\xi$ where $\xi = \mathrm{id}_A \in G(A)$ is the universal family. Therefore, we have

$$u^n \operatorname{Tr}(\xi) = \operatorname{Tr}(u\xi) = \operatorname{Tr}(\lambda_u(\xi)) = \operatorname{Tr}(\xi) \operatorname{Tr}(\lambda_u).$$

Therefore, $\operatorname{Tr}(\lambda_u) = u^n \in A^\vee$, which is a unit in $R \subset \mathbb{A}^\vee$. Since it is a character, it is also an idempotent. This gives that the element is $1_{A^\vee}$, which is the unit element in $G(R)$.

We consider the base extension G_A and we have that every element in $G_A(A) = G_A$ is annihilated by n. In particular, ξ is annihilated by n, and hence $nG(T) = 0$ for all $T \in \operatorname{Sch}/R$.

Now we prove the case where S is arbitrary and G/S is finite locally free of constant rank n. Let $U \subset S$ be an open subset. We have the commutative diagram

$$\begin{array}{ccccc} G_U & \xrightarrow{n\cdot} & G_U & \longrightarrow & U \\ \downarrow & & \downarrow & & \downarrow \\ G & \xrightarrow{n\cdot} & G & \longrightarrow & S \end{array}$$

as in Sch/S, $G_U(T) = G(T)$ if $T \to S$ has image in U and is the empty set for otherwise. Therefore, the restriction of $n\cdot : G \to G$ on G_U is $n\cdot : G_U \to G_U$. Note that

$$\begin{array}{ccccc} U & \xrightarrow{\epsilon_{G_U}} & G_U & \longrightarrow & U \\ \downarrow & & \downarrow & & \downarrow \\ S & \xrightarrow{\epsilon_G} & G & \longrightarrow & S \end{array}$$

is also commutative. If there is an open cover $\{U_i\}_{i \in I}$ such that $n\cdot : G_{U_i} \to G_{U_i}$ factors through $\epsilon_{G_{U_i}}$ for all i, then $n \cdot G \to G$ factors through ϵ_G, namely, G is annihilated by n. This is verified for all $U \subset S$ affine, so is true for S.

We would like to finally lift the restriction that G/S is locally free. Suppose only that G/S is finite flat of constant rank n. We compare tow morphisms $n\cdot : G \to G$ and $G \to S \xrightarrow{\epsilon_G} G$. For every $s \in S$, these tow maps are the same when restricted to the fiber at s, for that G_s is locally free of rank n. This reduces to an algebraic problem that if A is a R-algebra and R-algebra homomorphisms $\phi_1, \phi_2 : A \to A$ induces the same map on A_s for all $s \in \operatorname{Spec}(R)$, then $\phi_1 = \phi_2$. This is true as $(\phi_1 - \phi_2)_s = 0$ for all $s \in \operatorname{Spec}(R)$, and hence is $\phi_1 - \phi_2 = 0$.

Corollary 1. Let G be a commutative finite flat group scheme over S of order n. If n is invertible in $\mathcal{O}(S)^\times$, G is étale. In particular, if S is over a characteristic 0 field, every commutative finite flat group scheme is étale.

Proof. Multiplication by n has effect $n\cdot$ on $\Omega^1_{G/S}$, which is invertible. However n kills G, so $n\cdot$ on $\Omega^1_{G/S}$ is trivial. This says that $\Omega^1_{G/S} = 0$, namely, G is étale. $\square$

1.7 Frobenius Morphism

Let T be a scheme over $\mathbb{F}_p$. We define the absolute Frobenius morphism $F_T : T \to T$ as follows: The map on the underlying space is the identity map, and for every $U \subset T$ open subset, the map on structure sheaves $\mathcal{O}_T(U) \to \mathcal{O}_T(U)$ is given by $x \mapsto x^p$.

Example 8. Let $T = \mathrm{Spec}(R)$. F_T is the morphism induced by the absolute Frobenius map on R.

Let S be a scheme over $\mathbb{F}_p$ and T be a S-scheme. We define $T^{(p)}$ as the fiber product

$$\begin{array}{ccc} T^{(p)} & \longrightarrow & T \\ \downarrow & & \downarrow \\ S & \xrightarrow{F_S} & S \end{array}$$

and define the relative Frobenius $F_{T/S}$ as $(T \to S) \times F_T : T \to T^{(p)}$. Note that both $T^{(p)}$ and $F_{T/S}$ depends on S. We often assume that S is a field of characteristic p. For every $r \in \mathbb{N}$, we define inductively $T^{(p^{r+1})} := (T^{(p^r)})^{(p)}$ and $F^{r+1}_{T/S} : T \to T^{(p^{r+1})} := F_{T^{(p^r)}/S} \circ F^r_{T/S}$.

If $S = \mathrm{Spec}(R)$ and $T = \mathrm{Spec}(A)$, $T^{(p^r)} = \mathrm{Spec}(A \otimes_{R,F_R^r} R)$ and the relative Frobenius $F^r_{T/S}$ corresponds to the map

$$A \otimes_{R,F_R^r} R \to A, \ a \otimes r \mapsto ra^{p^r}.$$

Since $T \mapsto T^{(p)}$ is a base change, it defines a covarint functor, commutes with fiber product, and we have the commutative diagram

$$\begin{array}{ccc} T & \xrightarrow{\varphi} & U \\ \downarrow{\scriptstyle F_{T/S}} & & \downarrow{\scriptstyle F_{U/S}} \\ T^{(p)} & \xrightarrow{\varphi^{(p)}} & U^{(p)} \end{array}.$$

Let G be a group scheme over S. $G^{(p)}$ is a group scheme over S because it is a base change. Let $F_S^* T = T \to S \xrightarrow{F_S} S$ for every S-scheme T. Then $G^{(p)}(T) = G(F_S^* T)$. $F_{G/S} : G \to G^{(p)}$ defines a morphism over S. In terms of functors, the map is $G(T) \to G(F_S^* T)$ via $T \to G \xrightarrow{F_G} G$. This is a group homomorphism because $m \circ (F_G \times F_G) = F_G \circ m$.

Example 9. Let $S = \mathrm{Spec}(R)$ and $G = \mathbb{G}_a/R$. Then $G = G^{(p)} = \mathbb{G}_a/R$ while $F_{G/R}$ is induced by the map $X \mapsto X^p$. The kernel of the relative Frobenius is $\mathrm{Spec}(R[X]/(X^p))$ as the identity map on $\mathbb{G}_a$ is induced by $R[X] \to R$, $X \mapsto 0$, which is surjective with kernel (X), and the image of (X) in $R[X]$ via the relative Frobenius map is (X^p). The relative Frobenius sends a function to its pth power.

Assume that G is a finite flat group scheme over k. Then $G^{(p)}$ is also finite flat group scheme.

Definition 2. The Verschiebung map $V_{G/S}$ is defined as the dual of $F_{G^D/S}$.

Since base change commutes with Cartier dual, we have the natural isomorphism $G^{D,(p),D} \cong G^{(p),D,D} \cong G^{(p)}$ and we write $V_{G/k} : G^{(p)} \to G$. Verschiebung also commutes with fiber products and gives the commutative diagram

$$\begin{array}{ccc} T^{(p)} & \xrightarrow{\varphi^{(p)}} & U^{(p)} \\ \downarrow V_{T/S} & & \downarrow V_{U/S} \\ T & \xrightarrow{\varphi} & U \end{array}.$$

Example 10. $F_{G/S}$ is trivial if $G = \alpha_p$ or μ_p. $F_{G/S}$ is an isomorphism on $\underline{\mathbb{Z}/p\mathbb{Z}}$. Taking dual and we have the statements for $V_{G/S}$.

Let k be a field of characteristic p. We have the following propositions regarding $F_{G/k}$:

Proposition 4.

1. $F_{G/k} \circ V_{G/k} = [p]_{G^{(p)}}$, $V_{G/k} \circ F_{G/k} = [p]_G$.
2. G is connected iff $F^r_{G/k}$ is trivial for some r. G is étale iff $F_{G/k}$ is an isomorphisms.
3. The order of a connected finite flat group scheme over k has order of the form p^d. In particular, if $F_{G/k}$ is trivial, $d = \dim_k(I/I^2)$, where I is the augmentation ideal.

References

[Hon] Serin Hong. Notes on p-adic hodge theory. http://www-personal.umich.edu/~serinh/Notes%20on%20p-adic%20Hodge%20theory.pdf.

[Pin] Richard Pink. Finite group schemes. https://people.math.ethz.ch/~pink/ftp/FGS/CompleteNotes.pdf.

[Tat97] John Tate. Finite flat group schemes. *Modular forms and Fermat's last theorem*, pages 121–154, 1997.