Raynaud on F-vector schemes and prolongation

Melanie Matchett Wood

November 7, 2010

1 Introduction and Motivation

Given a finite, flat commutative group scheme $\mathcal{G}$ killed by p over R of mixed characteristic and residue char p, we can describe action of Galois on generic fiber, in terms of data related to the R-scheme, even though Galois is happening over the generic fiber.

Theorem 1.1 (Theorem 4.1.1 of Raynaud's paper)**.** *Let R be strictly henselian, mixed characteristic, with residue field of characteristic p, with $v(p) = e$ (where the v of a uniformizer is 1). Let G be the generic fiber of a finite, flat, commutative R-group scheme $\mathcal{G}$ that is killed by p. Suppose $e \leq p-1$. The action of $\mathrm{Gal}(\bar{K}/K)$ on $\det(G)$ is given by the tame character $\tau_p^{v(\bar{\mathcal{D}}(\mathcal{G}))}$, where we will give τ_p explicitly later, and $\bar{\mathcal{D}}$ denotes the nonzero discriminant ideal in R.*

On the other hand, say we have a finite, commutative group scheme G over K (the fraction field of R) killed by p, when does it extend to a finite flat R-group scheme and when is such an extension unique? We will be able to (sometimes) answer these questions in terms of data about R (e.g. e), and in terms of the Galois action on G.

In order to develop this theory, we will first start by studying F-vector schemes, a basic object in their own right, and then study extensions of K-group schemes to R-group schemes. Rebecca's talks will bring the Galois theory into the picture.

2 F-vector schemes

Before we study the Galois actions (Rebecca's talk), we will first study group schemes killed by p. Let F be a finite field of order $q = p^r$. In particular, we will study F-vector schemes (think groups: group schemes :: F-vector spaces: F-vector schemes; probably the word "space" should be in there, but there are already so many words ...). In particular, just like F-vector spaces are commutative groups killed by p, we will have that F-vector schemes are commutative group schemes killed by p.

Definition. Let S be a scheme. An *F-vector S-scheme* is a representable contravariant functor from S-schemes to F-vector spaces.

We could also describe an F-vector S-scheme as an F-vector space object in the category of S-schemes, i.e. with the existence of certain maps satisfying certain commutative diagrams. After Samit's talk, constructing this definition should be an exercise. The only point worth mentioning is that F is just a plain old finite field, and not a "finite field scheme" or anything. Note that F-vector S-schemes are commutative S-group schemes killed by p.

We will start by studying "one dimensional F-vector space" schemes (defined below). Later, we will have to be in a strictly henselian DVR, and use Galois theory, to see that a group scheme killed by p, even a power of p, is built out of pieces that are "one dimensional F_i-vector space" schemes for some finite fields F_i (Proposition 3.2.1).

From now on we will work over a scheme S. Let G be an F-vector scheme over S that is finite, flat and of finite presentation on S, i.e. G is associated to a finite rank, locally free $\mathcal{O}_S$-Hopf algebra A. Let I be the augmentation ideal of A. We have the action of F^* on I, given by the F-vector space structure. We are going to use this action to decompose I into F^*-eigenspaces. To do this, we need to assume $\mu_{q-1}, \frac{1}{q-1} \in \mathcal{O}_S$ (more precisely, S is a scheme over $\mathrm{Spec}(D)$, where D is the ring,...). Then we can explicitly construction the projection operators that allow us to write

$$I = \bigoplus_{\chi \in \hat{F^*}} I_\chi$$

where $\lambda \in F^*$ acts on sections of I_χ by multiplication by $\chi(\lambda)$.

This decomposition is going to be really useful for figuring out the possible multiplication and co-multiplicaiton structures on A. Moreover, it will now allow us to define a kind of analog of "one-dimensional F-vector space".

Definition. An *F-line* G (over S) is a finite, flat, of finite presentation, F-vector S-scheme such that each I_χ is an invertible (locally free rank 1) $\mathcal{O}_S$-module.

Note F-lines are finite, flat, rank q, commutative, killed by p S-group schemes. If you wondered why the above definition is what we are thinking of as the analog of one-dimension F-vector spaces, the rank q fact should help. Further, we now see that in the cases we care about, rank q is sufficient to make an F-vector scheme an F-line.

Proposition 2.1 (1.2.2)**.** *Let G be an F-vector S scheme defined by an $\mathcal{O}_S$ Hopf-algebra A locally free of rank q. Suppose S is connected, and there is an $s \in S$ such that G_s is étale (which is certainly the case when S is integral and with field of fractions characteristic 0). Then each I_χ is an invertible $\mathcal{O}_S$-module.*

Proof. Since each I_χ is locally free, it suffices to compute the rank at one point of S, even a geometric point. Over a geometric point, an étale F-vector scheme of rank q is just a 1-dimensional F-vector space, and one can easily compute each I_χ of the Hopf-algebra of functions has rank 1. □

If you are thinking about the situation in groups, you might wonder why we study $\mathbb{F}_{p^n}$-lines as our basic objects, since the groups that are $\mathbb{F}_{p^n}$-vector spaces break down into $\mathbb{F}_p$-vector spaces. This doesn't always happen for group schemes however. Even over a field,

you could have an étale group scheme of order 4, where there was an order 3 Galois element permuting the three non-identity geometric points. (This example would be better if I gave a concrete construction to show this was an $\mathbb{F}_4$-line, not just a commutative group scheme killed by 2 with an action of $\mathbb{F}_4^*$.)

2.1 Classification of F-lines

The I_χ decomposition will be very useful in order for us to determine the possible multiplication and co-multiplication maps in Hopf-algebras of F-lines. In particular, for $a \in I_\chi$, we have

$$c(a) = a \otimes 1 + 1 \otimes a + \sum_{\chi'\chi''=\chi} c_{\chi',\chi''}(a),$$

with $c_{\chi',\chi''}(a) \in I_{\chi'} \otimes I_{\chi''}$. The multiplication map d, restricted to $I_{\chi'} \otimes I_{\chi''}$ is

$$d_{\chi',\chi''} : I_{\chi'} \otimes I_{\chi''} \to I_{\chi'\chi''}.$$

This reduces us from having order of q^3 structure constants for our multiplication and co-multiplication to having order q^2 structure constants. The next real power comes from using the addition in F, and that for $\lambda, \lambda' \in F$ and v in an F-vector space $(\lambda + \lambda')v = \lambda v + \lambda' v$. This gives us lots of linear equations in the $w_{\chi',\chi''} = d_{\chi',\chi''} \circ c\chi', \chi''$ (note these are sections of $\mathcal{O}_S$), with coefficients and constants involving the characters of F evaluated at elements of F. We can use these equations to solve for the $w_{\chi',\chi''}$ purely in terms of F (in terms of some Jacobi sums of F). This is like in Simon's classification of group schemes of order 2 when he deduced that $ab = 2$.

The next (and hardest) step in the classification is to carefully evaluate these Gauss sums to deduce that various w's are units or p times a unit. In this step, Raynaud uses that S is over $\operatorname{Spec} D$, where D is as above and also has a unique prime above p. In particular, when $w_{\chi',\chi''}$ is a unit, we see that each of $d_{\chi',\chi''}$ and $c_{\chi',\chi''}$ is invertible and thus an isomorphism. This allows us to "relabel" so as to treat the isomorphism as and "equals." For example, suppose the I_χ are all free rank 1, and chose a basis y_χ. Then we can view the c's and d's as sections of $\mathcal{O}_S$. For example, just considering the structure coefficients for the multiplication, we have

$$y_\chi y_{\chi'} = d_{\chi,\chi'} y_{\chi\chi'}.$$

But if $d_{\chi,\chi'}$ is a unit then maybe we should have picked a different basis element so that $y_\chi y_{\chi'}$ is the basis element of $I_{\chi\chi'}$, to simplify the multiplication laws we have to work out (because there is now one fewer generator). Applying this idea systematically is a lot more subtle, and is how Raynaud reduces the number of unknown structure constants in the multiplcation and co-multiplication tables from the order of q^2 to order $r = \log q$. (Roughly, we write the characters in a p-adic notation, and we find the only non-unit w's come from "carries" when we do the p-adic addition.) Then Raynaud confirms that there are no further restrictions on the multiplication and co-multiplication structure constants by showing that anything satisfying the restrictions so far is a Hopf-algebra.

For simplicity, we will state the classification only in a special case.

Theorem 2.2 (Corollary 1.5.1)**.** *Let R be a local ring with residue characteristic p, and containing μ_{q-1}. Then an F-line over* $\operatorname{Spec} R$ *is determined by constants $\gamma_i, \delta_i \in R$ for $i = 1, \dots r$ such that $\gamma_i \delta_i = w$, where w is some (explicit) element in pR^*. Its Hopf algebra is*

$$R[X_1, \dots, X_r]/(X_i^p - \delta_i X_{i+1})$$

with indices in $\mathbb{Z}/r\mathbb{Z}$. The comultiplication is given explicitly in terms of the γ_i and unites in R that only depend on F. Two F-line are isomorphic (as F-vector S-schemes) if and only if there are units $u_i \in R^*$ such that

$$\delta_i' = u_i^p \delta_i u_{i+1}^{-1} \qquad \gamma_i = u_i^p \gamma_i' u_{i+1}^{-1}.$$

Raynuad's proof explicitly determines the possible structure constants, and the only ambiguity is the choice of bases of the r I_χ in which we chose a basis. A change of those bases if given by the u_i.

Corollary 2.3 (Corollary 1.5.2)**.** *With the hypothesis of the above theorem, also say R is a strictly henselian DVR with field of fractions characteristic 0, uniformizer π, and $v(\pi) = 1$ and $e = v(p)$. Then isomorphism classes of F-line over R natural bijection with r-tuples $(n_1, /dots, n_r)$ of integers with $0 \leq n_i \leq e$.*

Proof. Let $n_i = v(\delta_i)$. Clearly this gives an invariant of F-lines. If two F-lines agree on these invariants, we can show they are isomorphic by funding units u_i as above, which we do by using the Henselian property. We find appropriate units in the residue field using the strictness, which says the residue field is separably closed. □

3 Prolongations

Let R be a Dedekind domain with fraction field K.

Definition. Let $\mathcal{X}$ be a flat R-scheme, and $X = \mathcal{X} \otimes_R K$. Let Y be a closed sub-scheme of X. Then the *schematic closure* $\mathcal{Y}$ of Y in $\mathcal{X}$ is given as follows. On an open affine U of $\mathcal{X}$ with ring $\mathcal{A}$, we have that $Y \cap U$ is given by an ideal I of $A := \mathcal{A} \otimes_R K$. Then $\mathcal{Y} \cap U$ is given by the inverse image $\mathcal{I}$ of I in $\mathcal{A}$.

We have that $\mathcal{A}/\mathcal{I} \to A/I$ is injective, and since A/I is a vector space over K, we have that $\mathcal{A}/\mathcal{I}$ is a torsion-free R-module. They key point is that over a Dedekind domain, torsion-free is equivalent to flat. Thus, we have that $\mathcal{A}/\mathcal{I}$ is flat. So the schematic closure is flat over R.

Proposition 3.1. *Schematic closure gives an inclusion preserving bijection between*

$$\{\textit{Closed subschemes } Y \textit{ of } X \qquad\} \longleftrightarrow \{\textit{Flat, closed subschemes } \mathcal{Y} \textit{ of } \mathcal{X} \qquad\}.$$

The inverse operation is given by $\mathcal{Y} \mapsto \mathcal{Y} \otimes_R K$.

Schematic closure is functorial in the following way. If we have $\mathcal{X} \to \mathcal{X}'$ over R, with $\mathcal{Y}, \mathcal{Y}'$ flat closed subschemes of $\mathcal{X}, \mathcal{X}'$ respectively, then the map $\mathcal{Y} \to \mathcal{X}'$ factors through $\mathcal{Y}'$ if and only if $\mathcal{Y} \otimes_R K \to \mathcal{Y}' \otimes_R K$.

If $\mathcal{X}$ is an R-group scheme and Y is a sub-K-group scheme of X, then $\mathcal{Y}$ is a closed sub-R-group scheme of $\mathcal{X}$. This follows from the above functorality and the fact that schematic closure commutes with fiber products.

Remark 3.2. We have worked with arbitrary flat $\mathcal{X}$ over R instead of just finite R-schemes (i.e. the ones of immediate interest) because this construction is useful in higher dimensional examples as well, such as divisors in 1-parameter families of varieties, or abelian subschemes of abelian schemes

An important special case is that we can define a notion of image. Let $f : GraG'$ be a morphism of finite, flat commutative group schemes such that f_K is a closed immersion. Then the schematic closure H of $f(G_K)$ in G' is a finite flat R-subgroup scheme of G', through which f factors. We call H the *schematic image* of f.

Definition. Let G be a finite, commutative K-group scheme. A *prolongation* $\mathcal{G}$ of G to $\operatorname{Spec} R$ is a finite, flat (necessarily commutative) R-group scheme such that $\mathcal{G} \otimes_R K \cong G$ (as group schemes).

If G is given by a K-Hopf-algebra A, then $\mathcal{G}$ is given by an R-sub-Hopf-algebra $\mathcal{A}$ of A such that $\mathcal{A} \otimes_R K = A$. Thus prolongations are partially ordered by containment.

Proposition 3.3 (2.2.2)**.** *Let $\mathscr{G}$ and $\mathscr{G}'$ be prolongations of a finite, commutative K-group scheme G. Then $\mathscr{G}$ and $\mathscr{G}'$ have a sup prolongation and an inf prolongation.*

Proof. To obtain a sup, we take the R-algebra generated by the two R-algebras. To obtain an inf, we use Cartier duality. □

Corollary 3.4 (2.2.3)**.** *If K is characteristic 0, there is a maximum and minimum among all prlongations of a finite, commutative K-group scheme G.*

Proof. Since G is étale, we have that A is an étale K-algebra. All the prolongations are contained in the maximal order of A, which is a finitely generated R-module. We use Cartier duality for the minimum. □

Note that for non-étale K-algebras, there isn't necessarily a maximal order, e.g. $\mathbb{Q}[x]/x^2$ contains $\mathbb{Z}[x/n]$ for all n.

3.1 Extending F-vector structure to prolongations

Proposition 3.5 (3.3.1)**.** *Suppose that K is characteristic zero, and let $\mathscr{G}$ be a fintie flat R-group scheme, such that the generic fiber G is an F-vector scheme. Then the F-vector structure extends to the maximal and minimal prolognations of G.*

Proof. Automorphisms of A preserve the maximal and minimal "Hopf-orders." □

Proposition 3.6 (3.3.2)**.** *Let R be a DVR of mixed characteristic, with residue characteristic p, containing μ_{q-1}. Let G be a F-vector K-scheme, of rank q, which has a prolongnation $\mathscr{G}$ to R.*

1. *The maximal prolongnation $\mathscr{G}^+$ of G is characterized by:*
   (a) *$v(\delta_i) \leq p-1$ for all i*
   (b) *there exists an i with $v(\delta_i) < p-1$*
2. *If $e < p-1$, then $\mathscr{G}$ is, up to isomorphism, the unique prologonation of G to R, and it is an F-vector scheme.*
3. *If $e = p-1$, if G is simple and R is henselian, then either $\mathscr{G}$ is the unique prolongation of G, or there are two prolongations. In any case, all the prolongations of F-vector schemes.*

Remark 3.7. We will see in Section **??** that we can remove the condition that $\mu_{q-1} \subset R$ from the above, as in Remark **??**.

Proof. Recall that if $\mathscr{G}, \mathscr{G}'$ are F-vector R-schemes prolonging G, then we have

$$0 \leq v(\delta_i) \leq e = v(p)$$

and

$$0 \leq v(\delta_i') \leq e$$

for some $\delta_i, \delta_i' \in R$. Since $\mathscr{G}$ and $\mathscr{G}'$ have the same generic fiber, there are elements $u_i \in K^*$ such that

$$\delta_i' = u_i^p \delta_i u_{i+1}^{-1}$$

We have $\mathcal{A}' \subset \mathcal{A}$ if and only if

$$v(u_i) \geq 0$$

for all i.

Suppose $\mathcal{A}' \subset \mathcal{A}$ and that some u_i has positive valuation (i.e. $\mathscr{G} \neq \mathscr{G}'$). The consider the u_i with the largest valuation, and we see that $v(\delta_i') \geq p-1$. Thus if $e < p-1$, there is a unique F-vector prolongation. However, the maximal and minimal prolongations are both F-vector prolongations, and thus they are equal, proving 2.

Now to prove 1. If all $v(\delta_i)$ are all at least $p-1$, we can take all $u_i = \pi^{-1}$ and get a bigger F-vector prolongation. If the $v(\delta_i)$ are not all equal, let $v(\delta_i)$ be the greatest. If $v(\delta_i) \geq p$, then we can take $u_i = \pi^{-1}$ and $u_j = 1$ for all other j and get a bigger F-vector prolongation. Suppose $v(\delta_i) \geq p$ for some i. Then we see either they are all equal and at least $p-1$ or they are not all equal, and in either of the two cases above we have a bigger F-vector prolongation. This shows that a maximal prolongation has these equations. Conversely, an F-vector prolongation with such δ_i cannot have a strictly bigger prolongation. Suppose it did. Then if all the u_i have the same valuation, then we see that $v(\delta_i) \geq p-1$ for all i. If some u_i has a larger valuation than u_{i+1}, then $v(\delta_i) \geq p$.

□

4 Remarks on lattices

We have used various hypotheses on our DVR in some of the above, but we'd like to see that the results about unique prolognations don't require these hypotheses.

Let R be a DVR and K be its fraction field. Let V be a finite dimensional K vector space. *An R-lattice L of V* is a finite, free R-sub-module of V such that $L \otimes_R K = V$.

Proposition 4.1. *Let $R \to R'$ be a local extension of DVR's with the same residue field and a common uniformizer (e.g., R' may be the completion or henselization of R). There is an inclusion-preserving bijection*

$$\{R\text{-lattices in } V \qquad\} \longleftrightarrow \{R'\text{-lattices in } V \otimes_K K' \qquad\}$$

given by $L \mapsto L \otimes_R R'$.

Proof. The interesting part is to prove surjectivity. Given an R' lattice L', we pick an arbitrary R-lattice L, and compare L' to $L_{R'}$. The change of bases matrices over K' only have finite denominators, so we can assume, for a uniformizer π that

$$\pi^N L_{R'} \subset L' \subset L_{R'}.$$

It remains to show that every $R'/\pi^N R'$-submodule of $L_{R'}/\pi^N L_{R'}$ arises from a $R/\pi^N R$-submodule of $L/\pi^N L$, but $R/\pi^N R \cong R'/\pi^N R'$. □

Proposition 4.2. *Let R' be a unramified extension of R, with R henselian (e.g., complete) There is an inclusion preserving bijection*

$$\{R\text{-lattices in } V \qquad\} \longleftrightarrow \left\{\begin{matrix}\mathrm{Gal}(K'/K) \text{ invariant } R'\text{-lattices in} \\ V \otimes_K K'\end{matrix}\right\}$$

given by $L \mapsto L \otimes_R R'$.

Remark 4.3. Notice that the unramified condition is absolutely necessary. If $R' = R[\sqrt{\pi}]$, then the maxmimal ideal of R' is an R'-lattice in K', but it definitely does not arise as a base change from R.

Proof. The henselian condition ensures that the integral closure of R in each finite extension (and hence each algebraic extension) of K is *local*, so R' is the integral closure of R in K'. We can reduce to the case of finite extensions since every lattice only uses finitely many elements to write down. Again, the interesting part is surjectivity. If we have some Galois invariant R'-lattice L', we wish to find a basis for it with vectors whose entries are in R. For a vector $v \in L'$, and a basis $\alpha_1, \ldots, \alpha_n$ for R' over R, we write w_i for the sum of the conjugates of $\alpha_i v$, which is an R-vector. Since the extension is unramfied, the discriminant is a unit, and we can invert the matrix of the conjugates of the α_i's to write v as a linear combination of the w_i. If we do this for a basis of R', we have a collection of R-vectors that span L' as an R'-module. (See II.Lemma 5.8.1 in Silverman's book "Arithmetic of elliptic curves" for further details in the analogous case of Galois descent relative to field extensions rather than unramified dvr extensions.) □

Remark 4.4. We can now fill in the missing step in the group scheme proof of Nagell-Lutz from Samit's lecture, we would like to prove that for odd p, there are no finite, flat *local* group schemes of order p with constant (cyclic) generic fiber over $\mathbb{Z}_{(\ell)}$ (ℓ-prime). As Simon discussed, if $\ell \neq p$ then the group scheme must be etale and thus can't be non-reduced at the special fiber. So let $\ell = p$, and suppose that the constant group scheme $\mathbb{Z}/p\mathbb{Z}$ over $\mathbb{Q}$ (say $\operatorname{Spec} A$) had more than one prolongation to $\mathbb{Z}_{(p)}$. These prolongations are $\mathbb{Z}_{(p)}$ lattices in A. We can base change to add μ_{p-1} to our DVR without introducing any ramification, so as to apply Proposition **??**, part 2. The prolongations are still prolongations after base change, and must be the same. Thus they were the same over $\mathbb{Z}_{(p)}$.

As another application, let R be a mixed characteristic DVR, and K its fraction field. Let G be a finite commutative K-group scheme. Let R', K' denote the maximal unramified extension. If $G \otimes_K K'$ has a prolongation $\mathcal{G}$ to R', then we claim that G has a prolongation to R. Now $\mathcal{G}$ corresponds to a lattice in the Hopf-algebra of $G \otimes_K K'$. It may not be Galois stable, however. But since we have one prolongation, we have a maximal one, and the maximal one is Galois stable. Thus, it is the base change from a R-lattice. We can see that the R-lattice is closed under multiplication and comultiplication because the lattice bijections commute with tensor product and are functorial in the sense that we can check that in a map of K-vector spaces, one lattice lands inside the other if and only if it does after base extension.