Raynaud's paper on F-vector schemes, part II

Rebecca Bellovin

1 Galois action

1.1 Review of tame ramification

Recall the notion of tame ramification for a discretely-valued henselian field K with residue characteristic $p > 0$: a finite extension L/K is said to be *tamely ramified* if it is separable and the extension of residue fields is separable with ramification degree coprime to p. Hence, tameness is preserved in towers and inherited by subextensions, so it is reasonable to define a general algebraic extension L/K to be *tame* when every finite subextension is tame (so L/K is separable).

We want to describe totally tame finite extensions in general, and for this purpose it will be convenient to pull down results from the more familiar complete case, so we now review the relationship between the Galois theory of K and its completion $\widehat{K}$ (which is implicitly used all the time in number theory when we identify decomposition groups in Galois groups of global fields with Galois groups of completions). For a finite separable extension L/K, the valuation on K uniquely extends to one on L. Indeed, the module-finite integral closure O_L in L of the discrete valuation ring O_K of K is a semi-local Dedekind domain, whence it must be local because the henselian property of O_K implies that O_L is a direct product of local rings). It follows that $\widehat{K} \otimes_K L$ is a field, and in fact it maps isomorphically to the completion $\widehat{L}$ of L relative to the valuation on L, so $\widehat{L}/\widehat{K}$ is separable with the same degree as L/K.

Brian Conrad heavily rewrote the section on tame ramification.

If L/K is Galois then we get a natural injective map

$$\mathrm{Gal}(L/K) \hookrightarrow \mathrm{Aut}(\widehat{L}/\widehat{K}),$$

forcing $\widehat{L}/\widehat{K}$ to be Galois, and then restriction to L defines an inverse map. This equality of Galois groups has two important consequences. First, by the Galois correspondence and the equalities among Galois groups, the functor $F \rightsquigarrow \widehat{F}$ from the category of intermediate fields in L/K (using K-maps) to the category of intermediate fields in $\widehat{L}/\widehat{K}$ (using $\widehat{K}$-maps) is an equivalence. That is, every intermediate field on the complete side has the form $\widehat{F}$ for a unique intemediate field F in L/K, with $\mathrm{Hom}_K(F', F) \to \mathrm{Hom}_{\widehat{K}}(\widehat{F}', \widehat{F})$ a bijection. The second property is that *every* finite separable extension L' of $\widehat{K}$ has the form $\widehat{L}$ for some finite separable extension L/K. Indeed, by separability and Krasner's Lemma, we can choose a primitive element and slightly change its minimal polynomial to have coefficients in K, and then the finite separable extension L/K defined by this polynomial has completion that is a *field* dense in L' and hence equal to L' due to closedness of all subfields over the complete $\widehat{K}$ (over which L' is finite).

To summarize, the functor $L \rightsquigarrow \widehat{K} \otimes_K L$ is a degree-preserving equivalence from the category of separable algebraic extensions of K to the category of separable algebraic extensions of $\widehat{K}$ (with this functor identified with completion on finite-degree extensions). In this sense, the Galois theories of K and $\widehat{K}$ are identified, and the absolute Galois groups of these two fields (relative to compatible choices of separable closures) are canonically isomorphic (as topological groups). Since the completion process has no effect on residue fields or ramification on finite-degree extensions, this correspondence respects unramifiedness, tameness, and total ramifiedness. Hence, from the familiar complete case (as in Serre's book "Local Fields") we obtain:

Proposition 1.1. *A finite extension L/K with maximal unramified subextension K'/K is tamely ramified if and only if $L = K'(\sqrt[m]{a})$ for an integer m not divisible by p and $a \in K'^{\times}$.*

It follows from this that if L/K and L'/K are finite separable extensions inside of a common extension and L/K is tame, then so is LL'/L'. Thus, the composite of two tamely ramified extensions (inside a fixed separable closure $\overline{K}/K$) is again tamely ramified, so there is a unique maximal tamely ramified extension K_t of K (inside of $\overline{K}$). This uniqueness forces K_t/K to be a Galois extension.

Now we specialize to the case where K has strictly henselian (discrete) valuation ring R, so K has separably closed residue field and no non-trivial unramified extensions. Thus, the Galois group $\mathrm{Gal}(\overline{K}/K)$ coincides with the inertia group I of K. We have a short exact sequence

$$1 \to I_p \to \mathrm{Gal}(\overline{K}/K) \to I_t \to 1$$

where I_t, the *tame inertia group*, is $\mathrm{Gal}(K_t/K)$. Every finite quotient of I_t has order prime to p, because it corresponds to a finite totally tamely ramified extension of K. So I_p is the maximal pro-p subgroup of $\mathrm{Gal}(\overline{K}/K)$, and is called the *wild inertia group*.

We will be primarily interested in the tame inertia group, and its representations. We can use the proposition above to study the structure of the tame inertia group. For m prime to p and u a unit of R, K contains all mth roots of u (because R is strictly henselian). Thus, the only tame extension of K of degree m is obtained by adjoining mth roots of the uniformizer π of R. In other words, there is a unique tame extension of K of degree m, and it is Galois over K with Galois group canonically isomorphic to $\mu_m(K)$. The surjection $I_t \to \mu_m(K)$ corresponding to this isomorphism is $\sigma \mapsto \frac{\sigma(\pi^{1/m})}{\pi^{1/m}}$ for any mth root of π. This isomorphism is independent of the choice of π and is compatible with change in m in the sense that if $n|m$, the diagram

$$\begin{array}{ccc} I_t & \longrightarrow & \mu_m(K) \\ \| & & \downarrow \\ I_t & \longrightarrow & \mu_n(K) \end{array}$$

commutes, where the righthand arrow is given by $\zeta \mapsto \zeta^{m/n}$. Thus, we have a canonical isomorphism $I_t \cong \varprojlim_{(m,p)=1} \mu_m(K) = \prod_{\ell \neq p} \mathbf{Z}_\ell(1)$. In particular, I_t is abelian, and even pro-cyclic.

1.2 Galois representations

Suppose R is a henselian discrete valuation ring with residue characteristic $p > 0$, and let G be an étale commutative K-group scheme killed by p. Then $G(\overline{K})$ is a finite-dimensional $\mathbf{F}_p$-vector space, equipped with a linear Galois action. Conversely, given a finite-dimensional $\mathbf{F}_p$-linear Galois representation

$\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(V)$, there is a commutative finite étale K-group scheme killed by p whose $\overline{K}$-points recover ρ.

Now suppose that G is simple as a K-group scheme (i.e., nontrivial with no nontrivial proper K-subgroup scheme), or equivalently that $\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(V)$ is irreducible as an $\mathbf{F}_p$-linear representation. Consider the restriction of ρ to the wild inertia group I_p. The subspace of I_p-invariants V^{I_p} is non-trivial, because I_p is a pro-p group acting (continuously) on a finite-dimensional $\mathbf{F}_p$-vector space (cf. lemma IX.1.2 in *Local Fields*). Because I_p is normal in $\mathrm{Gal}(\overline{K}/K)$, V^{I_p} is stable under the action of the full Galois group. But then the irreducibility of V as a $\mathrm{Gal}(\overline{K}/K)$ representation implies that V^{I_p} is all of V. This in turn implies that $\rho|_{I_p}$ is trivial, which justifies our earlier disregard of wild inertia.

If R is actually strictly henselian, then ρ is now an irreducible representation of the *commutative* group I_t. Now we use a form of Schur's lemma to say that the commutant of ρ in $\mathrm{Aut}(V)$ is a finite field F, and since I_t is commutative, $\rho(I_t)$ is contained in the commutant of ρ. Thus, I_t acts by homotheties on the F-vector space V. And since V is an irreducible representation, it is 1-dimensional as an F-vector space. This implies that G is actually an F-line.

Proposition 1.2. *Suppose R is strictly henselian, with fraction field K, and let G be a commutative finite group scheme over K killed by a power of p. If G is étale or multiplicative and $\{G_i\}_{i\in I}$ is the family of successive quotients of a Jordan-Hölder filtration for G, then there is a family of finite fields $\{F_i\}_{i\in I}$ such that G_i is an F_i-line.*

Proof. We begin by filtering G by powers of p, so that we may assume that G is killed by p itself. Then if G is étale, we can apply the argument above to the (étale) quotients in a Jordan-Hölder filtration of G. If G is multiplicative, we can take the Cartier dual to get something étale, apply the preceding argument, and dualize back. □

Corollary 1.3. *Suppose R is strictly henselian with $e \le p-1$, and let $\mathcal{G}$ be a finite flat commutative group scheme over R, killed by a power of p. Then $\mathcal{G}$ has a composition series $\{\mathcal{G}_i\}_i$ such that the successive quotients $\mathcal{G}_i/\mathcal{G}_{i+1}$ are F_i-vector schemes for a family of finite fields $\{F_i\}_i$.*

Proof. Let $\{G_i\}_i$ be the composition series on the generic fiber obtained from the previous proposition, and for each i let $\mathcal{G}_i$ be the schematic closure of

G_i. Then $\mathcal{G}_i/\mathcal{G}_{i+1}$ is a prolongation of G_i/G_{i+1}, which is an F_i-vector scheme. Since $e \leq p-1$, we may apply the theorem on prolongations that Melanie proved to conclude that $\mathcal{G}_i/\mathcal{G}_{i+1}$ is also an F_i-vector scheme. □

1.3 Galois actions on F-vector schemes

In this section, we let R be strictly henselian of mixed characteristic $(0,p)$, and let K be its fraction field. Let F be a finite field of size $q = p^r$.

Suppose that G is an F-line over K, described by the equations

$$X_i^p = \delta_i X_{i+1}$$

By combining these equations, we find that $\overline{K}$-points of G correspond to solutions to the equations

$$X_i^q = a_i X_i$$

where $a_i = \delta_i^{p^{r-1}} \delta_{i+1}^{p^{r-2}} \cdots \delta_{i+r-1}$. So for any extension L/K, finding L-points of G depends on L containing $q-1$st roots of a_i. Note that $a_{i+1} = a_i^p/\delta_i^{p^r-1} = a_i^p/\delta_i^{q-1}$, so if L contains the $q-1$st roots of one a_i, it contains the $q-1$st roots of all the a_i. So all of the $\overline{K}$-points of G appear over a tame extension L/K of degree dividing $q-1$.

Thus, the tame inertia group I_t acts on $G(L)$ by a character of the form

$$I_t \to \mu_{q-1}(K) \xrightarrow{\psi} \mathbf{F}_q^\times$$

Here the first map is the canonical projection from the structure of tame inertia, and $\psi : \mu_{q-1}(K) \to \mathbf{F}_q^\times$ depends on the Galois action on $G(L)$.

In order to better understand this Galois action, we will express ψ in terms of certain distinguished characters $\chi_i : \mathbf{F}_q^\times \to \mu_{q-1}(K)$. Namely, every character $\chi : \mathbf{F}_q^\times \to \mu_{q-1}(K)$ can be extended to a map $\mathbf{F}_q \to R$ by sending 0 to 0. We will say that χ is *distinguished* if the composition $\mathbf{F}_q \to R \to k$ is a homomorphism of fields (Raynaud calls these characters "fundamental"). Note that if χ is a distinguished character, the distinguished characters are precisely those of the form χ^{p^h} for some integer h. Since $\chi^{p^r} = \chi$ with r minimal as such, we can view the distinguished characters as a set $\{\chi_i\}_{i \in \mathbf{Z}/r\mathbf{Z}}$ such that $\chi_{i+1} = \chi_i^p$. We define $\psi_i : \mu_{q-1}(K) \to F^\times$ to be the inverse of χ_i.

When Melanie derived the equations for G, that is, $K[X_i]/(X_i^p - \delta_i X_{i+1})$, she actually chose the X_i so that F acts on them via distinguished characters, that is, $[\lambda]X_i = \chi_i(\lambda)X_i$ for $\lambda \in F^\times$ and $[\lambda]$ the endomorphism of the Hopf algebra induced by the action of λ on $\mathcal{G}$.

Now we can prove the following result relating the constants δ_i to the Galois action:

Theorem 1.4. *With the above hypotheses on R, K, and G, the Galois group* $\mathrm{Gal}(\overline{K}/K)$ *acts on the F-vector space $G(L)$ via the character $I_t \to \mu_{q-1}(K) \xrightarrow{\psi} F^\times$, where $\psi = \psi_{i+1}^{v(\delta_i)} \cdots \psi_{i+r}^{v(\delta_{i+r-1})}$.*

Proof. Note first of all that if $x \in G(L)$ given by $x = (x_1, \ldots, x_r)$ (where x_i is the value of X_i at x), then $[\lambda]x = (\chi_i(\lambda)x_i)$ for $\lambda \in F$. This is because x can be given by solutions $x_i \in L$ to the r equations $X_i^q = a_i X_i$, satisfying $x_{i+1} = x_i^p/\delta_i$, so applying $[\lambda]X_i = \chi_i(\lambda)X_i$ yields a new point $\chi_i(\lambda)x_i$.

On the other hand, if $\sigma \in I_t$, $\sigma(x) = (j_q(\sigma)^{v(a_i)}x_i)$ by the definition of the Galois action on $L = K(\sqrt[q-1]{a_1}, \ldots, \sqrt{q-1}a_r)$.

Combining these two facts, we see that the action of $\sigma \in I_t$ on $G(L)$ coincides with the action of $\psi_i(j_q(\sigma))^{v(a_i)} \in F^\times$ on the ith component. This element of $F^\times$ is actually independent of i, since the conditions $v(a_{i+1}) = pv(a_i) - (q-1)v(\delta_i)$ and $\psi_{i+1}^p = \psi_i$ imply

$$\begin{aligned} \psi_{i+1}(j_q(\sigma))^{v(a_{i+1})} = \psi_{i+1}(j_q(\sigma))^{pv(a_i)-(q-1)v(\delta_i)} &= \frac{\psi_i(j_q(\sigma))^{v(a_i)}}{\psi_{i+1}(j_q(\sigma))^{(q-1)v(\delta_i)}} \\ &= \psi_i(j_q(\sigma))^{v(a_i)} \end{aligned}$$

(using that $\psi^{q-1} = 1$ for any character ψ of $\mu_{q-1}(K)$). □

This theorem lets us read off the structure constants of an F-line over K from the Galois representation on the geometric points. We can use it to give a criterion for an F-line over K to extend to an F scheme over R.

Theorem 1.5. *Suppose R is a strictly henselian discrete valuation of mixed characteristic $(0, p)$. Let G be an F-line over K associated to a character $\psi = \psi_{i+1}^{n_i} \cdots \psi_{i+r}^{n_{i+r-1}} : \mu_{q-1}(K) \to F^\times$. Then G has a prolongation if and only if $0 \leq n_j \leq e$ for all j.*

Example 1.6. Let $R = \mathbf{Z}_p$ and let $\mathcal{E}/R$ be an elliptic curve with supersingular reduction. Let $\mathcal{G}/R$ be the p-torsion $\mathcal{E}[p]$, and let G be its generic fiber. Then

G is simple, because any subgroup scheme H would have étale or multiplicative schematic closure, contrary to $\mathcal{G}$ having supersingular reduction (to see this, let $\mathcal{H}$ be the schematic closure of H, so that $\mathcal{G}$ is an $\mathbf{F}_p$-line. Then by the classification, $\mathcal{H} = \operatorname{Spec} R[X]/(X^p - \delta X)$, where $v(\delta) = 0$ or 1; in the first case, $\mathcal{H}$ is étale, and in the second case, $\mathcal{H}$ is dual to something étale).

To study the action of inertia on $G(\overline{\mathbf{Q}}_p)$, we replace R with its strict henselization, so that G is an F-line, where $F = \mathbf{F}_{p^2}$, and so $\mathcal{G}$ is as well. Then we know (from the classification) that $\mathcal{G} = \operatorname{Spec} R[X_1, X_2]/(X_1^p - \delta_1 X_2, X_2^p - \delta_2 X_1)$ where $0 \leq v(\delta_i) \leq 1$. If $v(\delta_1) = v(\delta_2) = 0$, then $\mathcal{G}$ is étale, which is false. If $v(\delta_1) = v(\delta_2) = 1$, then $\mathcal{G}$ is multiplicative, again contrary to our assumptions (as the torsion-levels of an elliptic curve over any ring are Cartier self-dual). Thus, $v(\delta_1\delta_2) = 1$ and $\mathcal{G} = \operatorname{Spec} R[X]/(X^{p^2} - pX)$ (we can change coordinates to get rid of a unit) and the character $\psi : \mu_{p^2-1}(K) \to F^\times$ associated to the character describing the action of inertia $I_t \to \mu_{p^2-1}(K) \to F^\times$ is the inverse to one of the two distinguished characters ψ_1,ψ_2. If we change the choice of F-action through composition with the p-power automorphism of F then we swap which of the ψ_i's appears. In this sense, neither of the two tame characters is “preferred”.

In addition, we know from the theory of abelian varieties that the full Galois group $G_{\mathbf{Q}_p}$ acts on the determinant of p-torsion by the cyclotomic character. In other words, if we look at the Galois representation $\rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(\mathbf{F}_p)$ on p-torsion, we know its determinant and we know its restriction to inertia $\rho|_I$. So we actually know ρ up to an unramified quadratic character (which is “best possible”), since an unramified quadratic twist on the elliptic curve preserves good reduction and induces the corresponding twist on the Galois representations.

1.4 Main result

The main result we promised to prove is the following theorem, which describes the Galois action on the generic fiber of a finite flat group scheme over a base with low ramification.

Theorem 1.7. *Let R be a strictly henselian discrete valuation ring with mixed characteristic $(0, p)$ and fraction field K, and let τ_p denote the tame character $\tau_p : I_t \to \mu_{p-1}(K) \to \mathbf{F}_p^\times$.*

Let G be the generic fiber of a commutative R-group scheme $\mathcal{G}$ which is finite, flat, and killed by p. Let $\mathfrak{d}_{\mathcal{G}/R}$ denote the discriminant ideal of $\mathcal{G}$ over R.

If $e \leq p-1$ then $\#G$ divides $v(\mathfrak{d}_{\mathcal{G}/R})$ and $\mathrm{Gal}(\overline{K}/K)$ acts on $\det(G)$ via the character $\tau_p^{v(\mathfrak{d}_{\mathcal{G}/R})/\#G}$.

To clarify the meaning of the discriminant ideal, note that the coordinate ring A of $\mathcal{G}$ is a finite free R-module, so it is well-posed to define $\mathfrak{d}_{\mathcal{G}/R} = (\det(\mathrm{Tr}_{A/R}(a_j a_k)))$ where $\{a_j\}$ is any ordered R-basis for A. This makes sense more generally for any ring extension that is locally free of finite rank as a module.

We will need a few properties of discriminant ideals later, so we record them here:

- $\mathfrak{d}_{A' \otimes_A A''} = (\mathfrak{d}_{A'/A})^{n''}(\mathfrak{d}_{A''/A})^{n'}$ where A' and A'' are free of respective ranks n' and n'' as A-modules. This lets us computes discriminants of fiber products $\mathcal{G}' \times_{\mathcal{G}} \mathcal{G}''$.
- If we have a tower of rings $A/A'/R$, each finite free over the next, then $\mathfrak{d}_{A/R} = \mathfrak{d}_{A'/R}^{\mathrm{rk}_{A'} A} \mathrm{Nm}_{A'/R}(\mathfrak{d}_{A/A'})$. This will let us compute relative discriminants of R-group schemes $\mathcal{G} \to \mathcal{G}'$.

Before we begin the proof of the theorem, we will calculate the discriminant $\mathfrak{d}_{\mathcal{G}/R}$.

Lemma 1.8. *Suppose $\mathcal{G}$ is an F-line, with Hopf algebra*

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

Then we have $\mathfrak{d}_{\mathcal{G}/R} = (\prod_{i=1}^r \delta_i)^{p^r}$. In particular, $v(\mathfrak{d}_{\mathcal{G}/R}) = p^r \sum_{i=1}^r v(\delta_i)$, so $\frac{v(\mathfrak{d}_{\mathcal{G}/R})}{p^r}$ is an integer.

Proof. Define $A_1 = R[X_1]/(X_1^q - a_1 X_1)$, and inductively define

$$A_i := A_{i-1}[X_i]/(\delta_{i-1} X_i - X_{i-1}^p),$$

so that $A = A_r$. In other words, we have a rising chain of rank-q R-sublattices of A.

We start by computing $\mathfrak{d}_{A_1/R}$. The basis for $R[X_1]/(X_1^q - a_1X_1)$ over R will be $\{1, X_1, \ldots, X_1^{q-1}\}$, so that $\mathrm{Tr}(X_1^k)$ will be zero unless $q-1$ divides k, in which case it will be q if $k = 0$ and $(q-1)a_1^{k/(q-1)}$ if $k \neq 0$. So to compute $\mathfrak{d}_{A_1/R}$ we need to compute the determinant of the matrix with an q in the upper left corner, $(q-1)a_1$ on the anti-diagonal, and $(q-1)a_1^2$ in the lower right corner. This determinant is easily seen to be $(q-1)^{q-1}a_1^q$, and since $(q-1, p) = 1$, $\mathfrak{d}_{A_1/R} = (a_1^q)$.

Next we note that, starting with $\{1, X_1, \ldots, X_1^{q-1}\}$ and working inductively, to obtain an R-basis of A_i from the basis for A_{i-1}, we simply divide the basis elements which are multiples of X_{i-1}^{pj}, $1 \leq j \leq p^{r-i+1} - 1$, by δ_{i-1}^j (and there are p^{i-1} of each of these). Since $\delta_{i-1} \in R$, $\mathrm{Tr}(\delta_i X_1^k) = \delta_i \,\mathrm{Tr}(X_1^k)$ for any k. Therefore,

$$\begin{aligned}
\mathfrak{d}_{A_i/R} &= \mathfrak{d}_{A_{i-1}/R} \,/ (\delta_{i-1}^{p^{i-1}(1+2+\cdots+(p^{r-i+1}-1))})^2 \\
&= \mathfrak{d}_{A_{i-1}/R} \,/ \delta_{i-1}^{p^{i-1}p^{r-i+1}(p^{r-i+1}-1)} \\
&= \mathfrak{d}_{A_{i-1}/R} \,/ \delta_{i-1}^{p^r(p^{r-i+1}-1)}
\end{aligned}$$

Recall that $a_1 = \delta_1^{p^{r-1}} \delta_2^{p^{r-2}} \cdots \delta_r = \prod_{i=1}^r \delta_i^{p^{r-i}}$, so

$$\mathfrak{d}_{A_1/R} = (\prod_{i=1}^r \delta_i^{p^{r-i}(p^r)}).$$

So to calculate $\mathfrak{d}_{\mathcal{G}/R}$, we need to divide $\prod_{i=1}^r \delta_i^{p^{r-i}(p^r)}$ by $\prod_{i=1}^{r-1} \delta_i^{p^r(p^{r-i}-1)}$. We get

$$\mathfrak{d}_{\mathcal{G}/R} = \left(\prod_{i=1}^r \delta_i^{p^r} \right) = \left(\prod_{i=1}^r \delta_i \right)^{p^r}$$

□

We also describe the behavior of the discriminant in exact sequences of finite flat group schemes (which is where we need to allow the base to be the product of local rings).

Proposition 1.9. *Suppose we have an exact sequence* $0 \to \mathcal{G}' \to \mathcal{G} \to \mathcal{G}''$ *of finite flat group schemes over* R *of orders* n', n, *and* n'' *(so* $n = n'n''$*). Then* $\mathfrak{d}_{\mathcal{G}/R} = (\mathfrak{d}_{\mathcal{G}'/R})^{n''}(\mathfrak{d}_{\mathcal{G}''/R})^{n'}$. *In particular,* $v(\mathfrak{d}_{\mathcal{G}/R})/\#\mathcal{G} = v(\mathfrak{d}_{\mathcal{G}'/R})/\#\mathcal{G}' + v(\mathfrak{d}_{\mathcal{G}''/R})/\#\mathcal{G}''$, *so the integrality property of* $v(\mathfrak{d}_{\mathcal{G}/R})/\#\mathcal{G}$ *holds if it does for the other two terms.*

Proof. We have an isomorphism $\mathcal{G} \times_R \mathcal{G}' \cong \mathcal{G} \times_{\mathcal{G}''} \mathcal{G}$ given by $(g, g') \mapsto (g, gg')$. We will take discriminants of both sides.

By our basic properties of discriminants, we have $\mathfrak{d}_{\mathcal{G}\times_R \mathcal{G}'/R} = (\mathfrak{d}_{\mathcal{G}'/R})^n (\mathfrak{d}_{\mathcal{G}/R})^{n'}$ and $\mathfrak{d}_{\mathcal{G}\times_{\mathcal{G}''}\mathcal{G}/\mathcal{G}''} = \left((\mathfrak{d}_{\mathcal{G}/\mathcal{G}''})^{n'}\right)^2$, so

$$\begin{aligned} \mathfrak{d}_{\mathcal{G}\times_{\mathcal{G}''}\mathcal{G}/R} &= (\mathfrak{d}_{\mathcal{G}''/R})^{n'^2} \operatorname{Nm}_{\mathcal{G}''/R}(\mathfrak{d}_{\mathcal{G}\times_{\mathcal{G}''}\mathcal{G}/\mathcal{G}''}) \\ &= (\mathfrak{d}_{\mathcal{G}''/R})^{n'^2} \operatorname{Nm}_{\mathcal{G}''/R}\left((\mathfrak{d}_{\mathcal{G}/\mathcal{G}''})^{2n'}\right) \end{aligned}$$

Moreover, $\mathfrak{d}_{\mathcal{G}/R} = (\mathfrak{d}_{\mathcal{G}''/R})^{n'} \operatorname{Nm}_{\mathcal{G}''/R}(\mathfrak{d}_{\mathcal{G}/\mathcal{G}''})$, so the right side is actually

$$(\mathfrak{d}_{\mathcal{G}''/R})^{-n'^2} (\mathfrak{d}_{\mathcal{G}/R})^{2n'}.$$

Thus, we have

$$\begin{aligned} (\mathfrak{d}_{\mathcal{G}'/R})^n (\mathfrak{d}_{\mathcal{G}/R})^{n'} &= (\mathfrak{d}_{\mathcal{G}''/R})^{-n'^2} (\mathfrak{d}_{\mathcal{G}/R})^{2n'} \\ (\mathfrak{d}_{\mathcal{G}'/R})^n (\mathfrak{d}_{\mathcal{G}''/R})^{n'^2} &= (\mathfrak{d}_{\mathcal{G}/R})^{n'} \end{aligned}$$

Then extracting n' roots, we get

$$(\mathfrak{d}_{\mathcal{G}'/R})^{n''} (\mathfrak{d}_{\mathcal{G}''/R})^n = \mathfrak{d}_{\mathcal{G}/R}$$

□

Now we can prove the theorem.

Proof. If $\mathcal{G}$ is actually an F-line, we know that the Galois group $\operatorname{Gal}(\overline{K}/K)$ acts on $G(\overline{K})$ via the tame character

$$I_t \to \mu_{q-1} \xrightarrow{\psi} F^\times,$$

where $\psi = \psi_{i+1}^{v(\delta_i)} \cdots \psi_{i+r}^{v(\delta_{i+r-1})}$. More precisely, this character describes the Galois action on the 1-dimensional F-vector space $G(\overline{K})$. But we can also view it as giving the Galois action on the r-dimensional $\mathbf{F}_p$-vector space $G(\overline{K})$. Taking the determinant of the action is the same as composing with the norm map $\operatorname{Nm}_{F/\mathbf{F}_p}$.

We find that the Galois action on the 1-dimensional $\mathbf{F}_p$-vector space $\det G(\overline{K})$ is given by the composition $I_t \to \mu_{q-1}(K) \xrightarrow{\mathrm{Nm}_{F/\mathbf{F}_p}(\psi)} \mathbf{F}_p^\times$ where

$$\begin{aligned}
\mathrm{Nm}_{F/\mathbf{F}_p}(\psi) &= \psi \cdot \psi^p \cdots \psi^{p^{r-1}} \\
&= \prod_{k=0}^{r-1} \left(\psi_{i+1-k}^{v(\delta_i)} \cdots \psi_{i+r-k}^{v(\delta_{i+r-1})} \right) \text{ since } \psi_i^p = \psi_{i-1} \\
&= (\psi_{i+1} \cdots \psi_{i+r})^{v(\delta_i)+\cdots v(\delta_{i+r-1})}
\end{aligned}$$

To check that the composition $I_t \to \mu_{q-1} \xrightarrow{\psi_{i+1}\cdots\psi_{i+r}} \mathbf{F}_p^\times$ is actually the character $\tau_p : I_t \to \mu_{p-1} \to \mathbf{F}_p^\times$, consider $(\psi_{i+1} \cdots \psi_{i+r})(\zeta)$ for $\zeta \in \mu_{q-1}(K)$:

$$(\psi_{i+1} \cdots \psi_{i+r})(\zeta) = \mathrm{Nm}_{F/\mathbf{F}_p} \psi_{i+1}(\zeta) = \psi_{i+1}(\zeta^{1+p+\cdots+p^{r-1}}) = \psi_{i+1}(\zeta^{(q-1)/(p-1)})$$

In other words, in the diagram

$$\begin{array}{ccccc}
I_t & \longrightarrow & \mu_{q-1}(K) & \xrightarrow{\psi_{i+1}\cdots\psi_{i+r}} & \mathbf{F}_p^\times \\
\| & & \downarrow & & \| \\
I_t & \longrightarrow & \mu_{p-1}(K) & \xrightarrow{\psi_{i+1}} & \mathbf{F}_p^\times
\end{array}$$

the right-hand square commutes. Here the middle arrow is raising elements of $\mu_{q-1}(K)$ to the power $\frac{q-1}{p-1}$. The composition along the bottom is τ_p, because there is only one distinguished character of $\mathbf{F}_p^\times$. But we know the left-hand square commutes, from our earlier study of the structure of the tame inertia group, so $I_t \to \mu_{q-1} \xrightarrow{\psi_{i+1}\cdots\psi_{i+r}} \mathbf{F}_p^\times$ is actually the character τ_p.

Thus, we have shown that the Galois action on $\det(G)$ coincides with the action of $\tau_p^{v(\delta_i \cdots \delta_{i+r-1})}$ if $\mathcal{G}$ is an F-vector scheme. Combining this with lemma 1.8, we are done in this case.

In the general case, we may filter $\mathcal{G}$ so that the successive quotients $\mathcal{G}_i$ are F_i-vector schemes for suitable finite fields F_i. Then it is enough to check how the Galois action on $\det(G)$ and $\frac{1}{\#G} v(\mathfrak{d}_{\mathcal{G}/R})$ behave in exact sequences. Proposition 1.9 showed that $\frac{1}{\#G} v(\mathfrak{d}_{\mathcal{G}/R})$ is additive in exact sequences, so we only need to check that the Galois action on $\det(G)$ is multiplicative in exact sequences.

So suppose we have an exact sequence $1 \to \mathcal{G}' \to \mathcal{G} \to \mathcal{G}'' \to 1$, and let ρ', ρ, and ρ'' denote the corresponding Galois representations on $G'(\overline{K})$, $G(\overline{K})$, and $G''(\overline{K})$. Then we have the exact sequence of Galois representations

$$0 \to G'(\overline{K}) \to G(\overline{K}) \to G''(\overline{K}) \to 0$$

and abstract properties of the top exterior product show that

$$\det \rho = \det \rho' \cdot \det \rho''$$

as desired. This may be seen more concretely by writing $\rho = \left(\begin{smallmatrix} \rho' & * \\ 0 & \rho'' \end{smallmatrix}\right)$ and taking the determinant. $\square$