Astérisque

BENEDICT H. GROSS

Ramification in p-adic Lie extensions

Astérisque, tome 65 (1979), p. 81-102

<http://www.numdam.org/item?id=AST_1979__65__81_0>

RAMIFICATION IN P-ADIC LIE EXTENSIONS

by

Benedict H. Gross

(Princeton)

-:-:-:-

Let $\mathcal{O}$ be a complete discrete valuation ring, with residue field k algebraically closed of characteristic $p > 0$. Let K be the field of fractions, $\overline{K}_s$ the separable closure of K, $\overline{K}$ the algebraic closure of K, and $\mathcal{G} = \mathrm{Aut}_K(\overline{K}) = \mathrm{Gal}(\overline{K}_s/K)$.

If G is a p-divisible group over $\mathcal{O}$, its general fibre determines a continuous Galois representation:

$$\rho : \mathcal{G} \longrightarrow \prod_{\lambda} GL(d_\lambda, D_\lambda)$$

where the D_λ are division algebras with center $\mathbb{Q}_p$. When K has characteristic zero this representation is well-known; it is given by the Galois action on the Tate module $T(G)$ [10]. When K has characteristic p, I will show how to define ρ as a Galois action on a generalized Tate module and will calculate its determinant.

In both cases the image of ρ is a closed subgroup of $\prod_{\lambda} GL(d_\lambda, D_\lambda)$ and inherits the structure of a p-adic Lie group. It carries two filtrations: an arithmetic filtration by the upper ramification subgroups of $\mathcal{G}$, and an analytic filtration by the p-saturated subgroups of Lie theory. When $\mathrm{char}(K) = 0$, Sen has shown that these two filtrations are related in a striking manner [7]; unfortunately, his results hold for <u>any</u> p-adic Galois representation and have nothing to do with the group G. When $\mathrm{char}(K) = p$ the ramification behavior of an <u>arbitrary</u> p-adic Galois representation can be quite random [11], but it seems that there <u>is</u> an interesting relation between the two filtrations when the representation comes from a p-divisible group over $\mathcal{O}$. Such a relation would reflect a favorable arithmetic property of ρ in the equicharacteristic case, much as $T(G)$ enjoys a Hodge-Tate decomposition in the case of mixed characteristic [10].

In this paper I will present evidence for such a filtration relation when G has dimension one. In this case the ramification calculations can be made quite explicitly, and one can appeal to the theory of formal A-modules when G has additional endomorphisms. It is a pleasure to express my appreciation to Jon Lubin and John Tate, who taught me this subject and offered many helpful suggestions.

§1. <u>Review of ramification theory</u> [8]

Let K be a local field, with algebraically closed residue field k of characteristic $p > 0$. Let v_K be the valuation on $\overline{K}$ with value group $\mathbb{Z}$ on K^*.

If E is a finite separable extension of K, we may filter the set

$$\Gamma = \Gamma_{E/K} = \mathrm{Hom}_K(E, \overline{K})$$

as follows. Since E is totally ramified over K, it is generated by any uniformizing parameter β. Let $e = [E:K]$ and define for $x \geq 0$ the subset

$$\Gamma_x = \{\sigma \in \Gamma : e v_K(\beta^\sigma - \beta) \geq x + 1\}$$

For large enough x, Γ_x consists only of the identity homomorphism; furthermore this filtration is independent of the choice of β.

We call x a <u>break</u> in the filtration if $\Gamma_x \neq \Gamma_{x+\varepsilon}$ for all $\varepsilon > 0$. When E is a Galois extension of K, the set Γ may be identified with the Galois group and the filtration we have defined coincides with the lower ramification filtration of $\mathrm{Gal}(E/K)$. In this case the breaks all occur at integers; in the general case the breaks may be rational, as $(\beta^{\sigma}-\beta)$ may ramify over E.

If $x = 0$ is the only break in the filtration of Γ then E/K is tamely ramified (hence cyclic). We shall henceforth assume there are further breaks. Define the Herbrand transition function:

$$\phi_{E/K}(x) = \frac{1}{e}\int_0^x \mathrm{Card}(\Gamma_t)dt \tag{1.1}$$

This is monotone increasing and piecewise linear. Let $\psi(x)$ be the inverse function on the interval $[0,\infty)$ and define the upper filtration of Γ by setting $\Gamma^y = \Gamma_{\psi(y)}$ for $y \geq 0$. The upper breaks are the values of y such that $\Gamma^{y+\varepsilon} \neq \Gamma^y$ for all $\varepsilon > 0$.

The lower numbering passes well to a subgroup, and the upper numbering to a quotient. To be precise: let L be a finite Galois extension of K containing E. Let $G = \mathrm{Gal}(L/K)$ and $H = \mathrm{Gal}(L/E)$, so $\Gamma \simeq G/H$. Then

$$H_x = H \cap G_x \qquad \text{for all } x \geq 0\,. \tag{1.2}$$

$$\Gamma^y = G^y H/H \qquad \text{for all } y \geq 0\,. \tag{1.3}$$

$$\phi_{L/K} = \phi_{E/K} \circ \phi_{L/E} \tag{1.4}$$

Using (1.3) we may define an upper filtration on the Galois group of an <u>infinite</u> Galois extension L/K by setting:

$$\mathrm{Gal}(L/K)^y = \{\sigma \in \mathrm{Gal}(L/K) : \text{ for all subfields } E \text{ of finite degree over } K,\ \sigma \in \Gamma^y_{E/K}\,\mathrm{Gal}(L/E)\}\,.$$

We say y is a break in this filtration if it occurs as a break in some finite quotient. Then every non-negative rational number occurs as a break in

$\mathrm{Gal}(\overline{K}_s/K)$; on the other hand, when $\mathrm{Gal}(L/K)$ is a p-adic Lie group, the breaks form a discrete subset of the reals [7], [11]. If L is the maximal abelian extension of K, the breaks occur exactly at the non-negative integers.

We now show how to calculate the upper breaks in $\Gamma_{E/K}$ when E is given as the root field of a separable Eisenstein polynomial. By (1.3) these breaks will also occur in the filtration of the Galois group of the normal closure of E.

Lemma 1.5 (Tate)

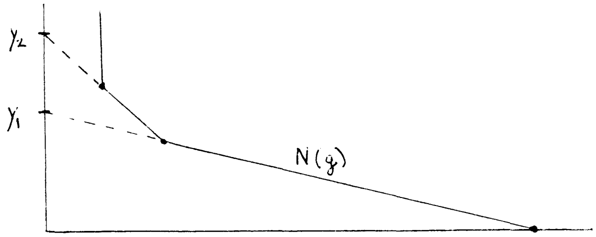
Assume $E = K(\beta)$, *where* β *satisfies the separable equation*:
$f(x) = x^e + a_{e-1}x^{e-1}+\ldots+a_0$ *with* $a_i \in K$, $v_K(a_i) \geq 1$, *and* $v_K(a_0) = 1$.

Let $g(x)$ *be the polynomial*:

$$g(x) = (\tfrac{1}{\beta})^e f(\beta x+\beta) = x^e + b_{e-1}x^{e-1}+\ldots+b_1 x$$

and let $N(g)$ *be its Newton polygon: the convex hull of the points* $(i,v_K(b_i))$ *in the plane*.

Then the upper breaks in the filtration of $\Gamma_{E/K}$ *occur at the y-intercepts of the non-trivial sides of* $N(g)$.



Proof. The roots of $g(x)$ are the values $a_\sigma = (\beta^\sigma/\beta) - 1$, where σ runs through $\mathrm{Hom}_K(E,\overline{K})$. Thus the distinct rational numbers in the set $S = \{ev_K(a_\sigma) : \sigma \neq 1\}$ give the lower breaks of Γ .

On the other hand, the numbers $-v_K(a_\sigma)$ are precisely the slopes of $N(g)$. Since the non-trivial sides of the polygon satisfy linear equations of the form

$$y + \lambda x = \phi_{E/K}(e\cdot\lambda)$$

we see that the y-intercepts give the upper breaks.

Corollary 1.6

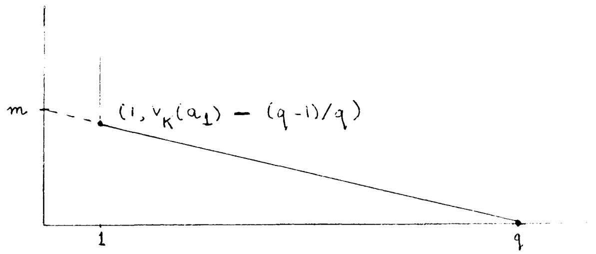
Suppose $\mathrm{char}(K) = p$ and $E = K(\beta)$ is a separable extension of degree $q = p^f$, where β satisfies $f(x)$ as in 1.5.

1) If $v_K(a_i) \geq v_K(a_1)$ for all $i \geq 1$ then $a_1 \neq 0$ and the upper and lower filtrations of $\Gamma_{E/K}$ have a unique break at the point

$$m = (qv_K(a_1)/q-1) - 1 .$$

2) If E/K is Galois then $q - 1$ divides $v_K(a_1)$ and $\mathrm{Gal}(E/K) \simeq \mathbb{F}_q^+$.

Proof. 1) The coefficient a_1 is non-zero as $f(x)$ is assumed separable. If we graph the Newton polygon of $g(x)$ as in (1.5) we find it has but one slope:



The y-intercept is at $(qv_K(a_1)/q-1) - 1$, which is the only upper break. By (1.1) it is also the only lower break.

2) If E/K is Galois the lower break must be integral. As there is only one break point and this point is positive, $\mathrm{Gal}(E/K)$ is an elementary abelian p-group [8].

§2. P-divisible groups and Galois representations

Let K be a field, and G a p-divisible group over K of height h. If $p \neq \mathrm{char}(K)$ then G is étale and is completely determined by its Tate module:

(2.1) $$T(G) = \mathrm{Hom}_{\overline{K}}(\mathbb{Q}_p/\mathbb{Z}_p, G) .$$

This module is free of rank h over $\mathbb{Z}_p = \mathrm{End}_K(\mathbb{Q}_p/\mathbb{Z}_p)$ and admits a left action of $\mathcal{G} = \mathrm{Aut}_K(\overline{K})$ which is continuous and $\mathbb{Z}_p$-linear:

(2.2) $$\rho : \mathcal{G} \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(T(G)) \simeq GL(h, \mathbb{Z}_p) .$$

The functor $G \longmapsto T(G)$ from étale groups to Galois modules is fully faithful [9], [10].

When $p = \mathrm{char}(K)$ the situation is more complicated as G need not be étale. The Tate module, as defined in (2.1), can only give information on the maximal étale quotient of G. To construct a more sensitive functor into the category of p-adic Galois modules, we need a larger supply of initial objects (like $\mathbb{Q}_p/\mathbb{Z}_p$).

These objects are furnished by Dieudonné theory. For any reduced rational number $\lambda = r/s$ in the interval $[0,1]$ there is a canonical p-divisible group G_λ defined over $\mathbb{F}_p$ of dimension r and height s. The group G_λ is specified by its Dieudonné module:

$$\mathbb{D}(G_\lambda) = \mathbb{Z}_p[F,V]/(F^{s-r}=V^r, FV=VF=p) .$$

All endomorphisms of G_λ are defined over $\mathbb{F}_{p^s}$, and

$$\mathrm{End}_{\mathbb{F}_{p^s}}(G_\lambda) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq D_\lambda ,$$

where D_λ is the central division algebra over $\mathbb{Q}_p$ with invariant $\lambda \pmod{\mathbb{Z}}$. The central assertion of the classical theory is that the category of p-divisible groups up to isogeny over $\overline{K}$ is semi-simple and that the groups G_λ represent the distinct simple objects [1]. If G is any group over K we therefore have

$$G \sim \prod_\lambda G_\lambda^{d_\lambda} \qquad \text{over } \overline{K} ,$$

where the d_λ are integers, almost all zero, determined by G. We can generalize the construction (2.1) by defining

$$V^\lambda(G) = \mathrm{Hom}_{\overline{K}}(G_\lambda, G) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \tag{2.3}$$

Then $V^\lambda(G)$ is a right module over D_λ of dimension d_λ, or a left module for the dual algebra D_λ°. It admits a continuous left action of $\mathcal{G}$; when K contains the field $\mathbb{F}_{p^s}$ this action is D_λ°-linear:

$$\rho^\lambda : \mathcal{G} \longrightarrow \mathrm{Aut}_{D_\lambda^\circ}(V^\lambda(G)) \simeq GL(d_\lambda, D_\lambda) .$$

If K contains the algebraic closure of the prime field we can thus define the representation $\rho = \bigoplus_\lambda \rho^\lambda$ on the generalized Tate module $V(G) = \bigoplus_\lambda V^\lambda(G)$.

Now suppose $\mathcal{O}$ is a complete discrete valuation ring, as in the introduction, with quotient field K and residue field k (algebraically closed of characteristic $p > 0$). Let G be a p-divisible group <u>defined over $\mathcal{O}$</u>. The special fibre G_k and the general fibre G_K are groups over a field; therefore

(2.5)
$$G_k \sim \Pi\, G_\lambda^{c_\lambda}$$
$$G_K \sim \Pi\, G_\lambda^{d_\lambda} \qquad \text{over } \overline{K} ,$$

where we accept the convention that $G_{0/1} = \mathbb{Q}_p/\mathbb{Z}_p$ and $d_{0/1} = h$ if $\mathrm{char}(K) = 0$. Consider the Galois representation arising from the general fibre:

(2.6)
$$\rho : \mathcal{G} \longrightarrow \prod_\lambda GL(d_\lambda, D_\lambda) .$$

How can we distinguish this from an arbitrary p-adic Galois representation?

First, we can compose ρ with the homomorphism

$$\det = \prod_\lambda \mathrm{Nm}_\lambda : \prod_\lambda GL(d_\lambda, D_\lambda) \longrightarrow \mathbb{Q}_p^*$$

where Nm_λ is the reduced norm in the algebra $\mathrm{Mat}(d_\lambda, D_\lambda)$ over $\mathbb{Q}_p$. We obtain a p-adic character $\varepsilon = \det(\rho)$ of $\mathcal{G}$.

<u>Theorem 2.7</u>

<u>If</u> $\mathrm{char}(K) = p$ <u>then</u> $\varepsilon = 1$ <u>in</u> $\mathrm{Hom}(\mathcal{G}, \mathbb{Q}_p^*)$.

<u>Proof</u>. The group G gives rise to an F-crystal $E(G)$ over the perfect closure of $\mathcal{O}$ [3]. The special fibre of this crystal is isogenous to the direct sum $\bigoplus E_\lambda^{c_\lambda}$, where $E_{r/s} = \mathbb{Z}_p[F]/(F^s = p^r)$. Over $\overline{K}$ the general fibre is isogenous

to $\oplus E_\lambda^{d_\lambda}$; over $K^{\mathrm{perf.}}$ it is isogenous to this crystal, twisted by the representation ρ .

The category of F-crystals has an exterior power operation which commutes with fibre products. If G has height h we find

$$(\textstyle\bigwedge^h E(G))_k \sim E_{\dim(G)/1}$$

$$(\textstyle\bigwedge^h E(G))_K \sim E_{\dim(G)/1} \quad \text{over } \overline{K} .$$

Over $K^{\mathrm{perf.}}$ the general fibre of $\bigwedge^h E(G)$ is isogenous to $E_{\dim(G)/1}$ twisted by the character $\varepsilon = \det(\rho)$. But the F-crystal $E_{\dim(G)/1}$ has only the <u>trivial</u> lifting from k to $\mathcal{O}$ [3]. As $\bigwedge^h E(G)$ is such a lifting, its general fibre is isomorphic to its special fibre and $\varepsilon = 1$.

<u>Notes</u>: 1) Suppose G has height h over $\mathcal{O}$ and its general fibre decomposes as in (2.5); then $\sum d_\lambda s_\lambda = h$ where $s_\lambda = \mathrm{denom}(\lambda)$. If C is the completion of the maximal unramified extension of $\mathbb{Q}_p$ (which splits all the algebras D_λ) , we have an embedding

$$\prod_\lambda GL(d_\lambda, D_\lambda) \hookrightarrow GL(h,C) .$$

Now let U be the open set $\mathrm{Spec}\,\mathcal{O} - \mathrm{Spec}\,k$, so $\mathcal{G} = \pi_1(U)$. Then (2.6) gives us a "monodromy representation"

$$\rho : \pi_1(U) \longrightarrow GL(h,C) . \tag{2.8}$$

In the geometric case when K has characteristic p , Theorem 2.7 asserts that the monodromy representation factors through $SL(h,C)$.

2) Theorem 2.7 may be formulated for K of arbitrary characteristic. Let χ be the cyclotomic character giving the action of $\mathcal{G}$ on p-power roots of unity in $\overline{K}$. Then

$$\varepsilon = \chi^{\dim(G)} \quad \text{in } \mathrm{Hom}(\mathcal{G}, \mathbb{Q}_p^*) . \tag{2.9}$$

For K of characteristic zero this is due to Raynaud [6]; for K of characteristic p it is a restatement of (2.7) .

§3. Formal A-modules of dimension 1 .

Let G be a connected p-divisible group of dimension 1 over $\mathcal{O}$. Then G can be identified with a formal group on one parameter, and we can make the representation ρ of (2.6) more explicit by using Lazard's one-dimensional theory. When G has additional endomorphisms it is convenient to analyse this situation using the language of formal A-modules [2] [4].

Let A be the ring of integers in a finite extension F of $\mathbb{Q}_p$, let π be a prime of A and $q = \mathrm{Card}(A/\pi A)$. Suppose R is a ring over A and $\gamma : A \longrightarrow R$ is the natural morphism. Then a formal A-module of dimension n over R is a pair $G = (\hat{G},i)$, where $\hat{G}$ is a formal group of dimension n over R and $i : A \longrightarrow \mathrm{End}_R(\hat{G})$ is an injective ring homomorphism such that $i(a)$ induces multiplication by $\gamma(a)$ on $\mathrm{Lie}\ (\hat{G})$. We write $[a]_G$ for the element $i(a)$ in $\mathrm{End}_R(\hat{G})$. If G and H are two formal A-modules over R , we define

$$\mathrm{Hom}_R(G,H) = \{\phi \in \mathrm{Hom}_R(\hat{G},\hat{H}) : \phi \circ [a]_G = [a]_H \circ \phi \quad \text{all } a \in A\} .$$

We shall henceforth only consider formal A-modules and formal groups of dimension one.

It is quite easy to describe the category of formal A-modules over a field K of characteristic p ; if $A = \mathbb{Z}_p$ this is equivalent to the category of formal groups. Choosing a model for $\hat{G}$ over K we have

$$[\pi]_G\ (x) = f(x^{q^h})$$

where $f(x)$ is a power series over K with $f'(0) \neq 0$, and h is a strictly positive integer, the <u>height</u> of G . (The height of $\hat{G}$, as a formal group, is then $h\cdot[A:\mathbb{Z}_p]$, and we shall assume the height is finite.) If K is separably closed there is one isomorphism class of formal A-modules for each finite height.

As a representative, we can take the formal A-module $G_{1/h}$, which is defined over $A/\pi A$ and characterized by

$$[\pi]_{G_{1/h}}(x) = x^{q^h} . \tag{3.1}$$

This formal A-module achieves all of its endomorphisms over the field $\mathbb{F}_{q^h}$; there we have

$$\mathrm{End}_{\mathbb{F}_{q^h}}(G_{1/h}) = B_{1/h}$$

where $B_{1/h}$ is the maximal order in the central division algebra over $F = A\otimes\mathbb{Q}_p$ with invariant $1/h \pmod{\mathbb{Z}}$. When K is not separably closed G is classified over K by its height and a representation

$$\rho : \mathrm{Gal}(\overline{K}_s/K) \longrightarrow B^*_{1/h}$$

as in §2.

We can now apply this to formal A-modules G over $\mathcal{O}$ whose special fibre is isomorphic to $G_{1/h}$ over k. Let $G_{0/1}$ denote the constant étale A-module F/A. When $\mathrm{char}(K) = 0$ we have $G_K \underset{\overline{K}}{\simeq} (G_{0/1})^h$. When $\mathrm{char}(K) = p$ the general fibre of G must also have dimension 1, therefore

$$G_K \underset{\overline{K}}{\sim} G_{1/g} \times (G_{0/1})^d$$

where $1 \leq g \leq h$ and $g + d = h$. Define the Tate modules

$$\begin{aligned} T^{1/g}(G) &= \mathrm{Hom}_{\overline{K}}(G_{1/g}, G_K) \quad \text{of rank 1 over } B_{1/g} \\ T^{0/1}(G) &= \mathrm{Hom}_{\overline{K}}(G_{0/1}, G_K) \quad \text{of rank } d \text{ over } A . \end{aligned} \tag{3.2}$$

These afford Galois representations:

$$\begin{aligned} \rho^{1/g} &: \mathcal{G} \longrightarrow B^*_{1/g} = B^* \\ \rho^{0/1} &: \mathcal{G} \longrightarrow GL(d,A) \end{aligned} \tag{3.3}$$

as in (2.4). We shall restrict our study to the equicharacteristic case ($g \geq 1$), as the ramification of $\rho^{0/1}$ when $\mathrm{char}(K) = 0$ is well-known [7].

Choosing a model for $\hat{G}$ over $\mathcal{O}$ we have

$$[\pi]_G\,(x) = f(x^{q^g}) \tag{3.4}$$

where $f(x) = a_1 x + a_2 x^2 + \ldots$ has coefficients in $\mathcal{O}$ and $a_1 \neq 0$. If we insist on a model lifting the standard model of $G_{1/h}$, then all the a_i lie in the maximal ideal except for a_{q^d}. The integer $e = v_K(a_1)$ is independent of the model chosen; it is zero if and only if $d = 0$. In that case the representation $\rho = \rho^{1/g} \oplus \rho^{0/1}$ is <u>trivial</u> [5]. The simplest nontrivial case is when $d = e = 1$; **here** we have complete results.

<u>Theorem 3.5</u>

Let G be a formal A-module of dimension 1 and height $h = g + d$ over $\mathcal{O}$. Assume $d = e = 1$ and for $n \geq 0$ define the rational numbers

$$a(n) = \frac{q^h - 1}{(q^g-1)(q^d-1)}\,(q^n - 1)$$

1) a) *The representation $\rho^{1/g} : \mathcal{G} \longrightarrow B^*$ is surjective, so B^* inherits an upper ramification filtration.*

   b) *The upper breaks in this filtration are precisely at the points $a(n)$, $n \geq 0$ (or $n \geq 1$ if $q^g = 2$).*

   c) *For $n \geq 1$ $(B^*)^{a(n)} = 1 + \pi_B^n B$, where π_B is a prime of B.*

2) a) *The representation $\rho^{0/1} : \mathcal{G} \longrightarrow A^*$ is surjective, so A^* inherits an upper ramification filtration.*

   b) *The upper breaks in this filtration are precisely at the points $a(gn)$, $n \geq 0$ (or $n \geq 1$ if $q = 2$).*

   c) *For $n \geq 1$ $(A^*)^{a(gn)} = 1 + \pi_A^n A$.*

We will prove this result in the following section. First we shall make a few remarks on its contents and provide a concrete example.

Example: Let E be the elliptic curve over $\mathcal{O} = \overline{\mathbb{F}}_2[[t]]$ with plane equation

$$y^2 + txy + y = x^3$$

and origin at the inflection point $(x,y) = (0,0)$. Then E_K is ordinary, but E_k is supersingular. The formal group $\hat{E}$ associated to this model, using x as a local parameter at the origin, gives a formal A-module G with $A = \mathbb{Z}_2$ and

$$[-2]_G(x) = tx^2 + (1+t^3)x^4 + \ldots + (t^{2n-4}+t^{2n-1})x^{2n} + \ldots.$$

Thus $h = 2$ and $g = d = e = 1$. Applying (3.5) we see the upper breaks in $\rho^{0/1}(\mathcal{G}) = A^*$ occur at the points $a(gn) = 3(2^n-1)$, and $(A^*)^{3(2^n-1)} = 1 + 2^n A$ for $n \geq 1$. These are the breaks in the separable quotient of the 2-division field of E_K.

Notes: 1) The breaks in the upper filtration of $\rho^{1/g}(\mathcal{G})$ are integral if and only if $g = 1$, i.e. if and only if $B^*_{1/g}$ is abelian.

2) Since $(\pi_B)^g = (\pi_A)$ in $B_{1/g}$, we find

$$(B^*)^{a(gn)} = 1 + \pi_A^n B \quad \text{for } n \geq 1$$

and the function $a(gn)$ relates the ramification filtration to the π_A-filtration in both $\rho^{0/1}$ and $\rho^{1/g}$. Let H^* denote the elements in $B^* \times A^*$ whose reduced norm down to A^* is 1, and H_n the elements of H^* congruent to 1 $(\text{mod } \pi_A^n)$. I suspect that $\rho = \rho^{1/g} \oplus \rho^{0/1}$ maps $\mathcal{G}$ surjectively onto H^* and that for $n \geq 1$,

$$(H^*)^{a(gn)} = H_n .$$

Theorem 2.7, combined with (3.5), shows that this holds at least when $A = \mathbb{Z}_p$.

3) When $d = 1$ but $e > 1$ we can prove a slightly weaker result. Let e_s be the separable degree of K over $L = k((a_1))$. Then there are positive constants c and N such that, for all $n > N$,

$$(3.6) \qquad \begin{aligned} \rho^{1/g}(\mathcal{G})^{e_s a(n)+c} &\subseteq 1 + \pi_B^n B \subseteq \rho^{1/g}(\mathcal{G})^{e_s a(n)-c} \\ \rho^{0/1}(\mathcal{G})^{e_s a(gn)+c} &\subseteq 1 + \pi_A^n A \subseteq \rho^{0/1}(\mathcal{G})^{e_s a(gn)-c} \end{aligned} .$$

Indeed, by Drinfeld's moduli theory [2], we can find a model for G over $k[[a_1]]$ where we can apply (3.5). Then (3.6) follows from a comparison of the upper numbering on $\mathrm{Gal}(\overline{L}_s/L)$ with that on its subgroup $\mathcal{G} = \mathrm{Gal}(\overline{K}_s/K)$ of index e_s.

Thus the breaks in the π_A-filtration of $\rho(\mathcal{G})$ occur near the upper breaks $e_s \cdot a(gn)$. The breaks in the p-saturated filtration therefore occur near the upper breaks $e_s \cdot a(g \cdot e_F \cdot n)$, where $F = A \otimes \mathbb{Q}_p$ and $e_F = v_F(p)$. This result bears an eerie formal relation to a theorem of Sen in characteristic zero. By definition

$$\begin{aligned} e_s a(g e_F n) &= e_s \frac{(q^h-1)}{(q^g-1)(q^d-1)} (q^{g e_F n}-1) \\ &= e_s \frac{q^h-1}{q^d-1} (1 + q^g + q^{2g} + \dots + q^{(e_F n-1)g}) . \end{aligned}$$

When $\mathcal{O}$ has mixed characteristic, $g = 0$, $d = h$, and $e_s = v_K(\pi_A)$. Thus, arguing <u>purely formally</u>, we might expect that in this case the breaks in the p-saturated filtration of $\rho(\mathcal{G})$ would be near the upper breaks $e_s e_F n = e_K n$. But this is precisely Sen's result [7] : is there a general theory which can obtain both results simultaneously?

4) When $d > 1$ the situation becomes more complicated. It seems that the upper breaks in $\rho(\mathcal{G})$ are determined by the valuations of the d moduli that classify the lifting of G over $G_{1/h}$ [2], [5]. When $d = 1$, a_1 is the unique modulus of the lifting; it might be interesting to study maximal 1-dimensional families in general.

§4. The proof of Theorem 3.5

To prove part 1) we start with the representation

$$\rho^{1/g} : \mathcal{G} \longrightarrow B^* .$$

Recall that the prime π_B gives a filtration on the image:

$$B^* \supsetneq 1 + \pi_B B \supset 1 + \pi_B^2 B \supset \ldots$$

with successive quotients:

$$B^* / 1 + \pi_B B \simeq \mathbb{F}_{q^g}^*$$

$$1 + \pi_B^n B / 1 + \pi_B^{n+1} B \simeq \mathbb{F}_{q^g}^+ \quad \text{for } n \geq 1 .$$

For $n \geq 0$ let H_n be the kernel of the composed homomorphism:

$$\rho_n : \mathcal{G} \longrightarrow B^* \longrightarrow (B^*/1+\pi_B^{n+1}B) \simeq (B/\pi_B^{n+1}B)^* ,$$

and let K_n be the fixed field of H_n in $\overline{K}_s$. Then $(\mathcal{G}/H_n) \simeq \mathrm{Gal}(K_n/K)$ and we have a tower of fields:

$$\begin{array}{l} \overline{K}_s \\ \quad \ddots \\ \qquad K_1 \\ \qquad | \\ \qquad K_0 \\ \qquad | \\ \qquad K = K_{-1} \end{array}$$

If we choose an isomorphism of formal A-modules over $\overline{K}_s$:

$$\phi : G \longrightarrow G_{1/g}$$

we have, for $\sigma \in \mathcal{G}$,

$$\rho^{1/g}(\sigma) = \phi \circ \phi^{-\sigma} \in \mathrm{Aut}(G_{1/g}) \simeq B^* .$$

Choosing models for G and $G_{1/g}$ over $\mathcal{O}$, we may write ϕ as a power series:

$$\phi(x) = k_1 x + k_2 x^2 + \dots$$

with coefficients in $\overline{K}_s$. Similarly, we have the power series over $\mathcal{O}$:

$$[\pi]_G(x) = a_1 x^{q^g} + a_2 x^{2q^g} + \dots$$

$$[\pi]_{G_{1/g}}(x) = x^{q^g} .$$

Since ϕ is an isomorphism of formal A-modules, these series satisfy:

$$\phi \circ [\pi]_G(x) = [\pi]_{G_{1/g}} \circ \phi(x) = \phi^{q^g}(x^{q^g}) . \tag{4.1}$$

Lemma 4.2

1) *The coefficients* k_j *in* $\phi(x)$ *are integral in* $\overline{K}_s$.

2) *One has* $k_j \in K_{n-1}$ *for all* $j < q^n$, *and* $K_n = K_{n-1}(k_{q^n})$.

Proof. The integrality of the k_j follows from the identity (4.1), which may be used to define them successively. Since $\sigma \in H_0$ if and only if $k_1^\sigma = k_1$, we have $K_0 = K(k_1)$. But for $\sigma \in H_0$:

$$\phi \circ \phi^{-\sigma}(x) = x + kx^{q^m} + \dots ;$$

furthermore, $\sigma \in H_n$ if and only if $m > n$. This gives part 2) .

Lemma 4.3

Assume that $d = e = 1$. *Then for* $n \geq 0$,

1) ρ_n *induces an isomorphism* $\mathrm{Gal}(K_n/K) \simeq (B/\pi_B^{n+1}B)^*$.

2) k_{q^n} *is a uniformizing parameter of* K_n .

3) $\mathrm{Gal}(K_n/K_{n-1})$ *has a unique upper and lower break at the point* $m = q^{hn} - 1$.

4) *The lower filtration of* $G = \mathrm{Gal}(K_n/K)$ *is given by:*

$$\begin{aligned}
G_0 &= G \\
G_x &= \mathrm{Gal}(K_n/K_0) && \text{for} \quad 0 < x \le q^h - 1 \\
G_x &= \mathrm{Gal}(K_n/K_1) && \text{for} \quad q^h - 1 < x \le q^{2h} - 1 \\
&\vdots \\
G_x &= \mathrm{Gal}(K_n/K_{n-1}) && \text{for} \quad q^{(n-1)h} - 1 < x \le q^{nh} - 1 \\
G_x &= (1) && \text{for} \quad q^{nh} - 1 < x .
\end{aligned}$$

5) The upper filtration of $G = \mathrm{Gal}(K_n/K)$ is given by:

$$\begin{aligned}
G^0 &= G \\
G^x &= \mathrm{Gal}(K_n/K_0) && \text{for} \quad 0 < x \le a(1) \\
G^x &= \mathrm{Gal}(K_n/K_1) && \text{for} \quad a(1) < x \le a(2) \\
&\vdots \\
G^x &= \mathrm{Gal}(K_n/K_{n-1}) && \text{for} \quad a(n-1) < x \le a(n) \\
G^x &= (1) && \text{for} \quad a(n) < x ,
\end{aligned}$$

where $a(1), a(2), \dots, a(n)$ are defined in Theorem 3.5.

Proof. We use an induction on n. For $n = 0$ look at the coefficient of x^{q^g} in the identity (4.1). This gives the equation:

$$k_1 a_1 = k_1^{q^g} .$$

Since $e = v_K(a_1) = 1$, this shows that $K_0 = K(k_1)$ has degree $q^g - 1$ over K and that k_1 is a uniformizing parameter. By counting we see that the injection

$$\rho_0 : \ \mathrm{Gal}(K_0/K_1) \longrightarrow (B/\pi_B B)^*$$

is an isomorphism. The only upper and lower break is at 0, as K_0 is a tamely ramified extension of K.

Now assume that the lemma holds for K_{n-1}/K. Look at the coefficient of $x^{q^{g+n}}$ in the identity (4.1). This gives the equation:

$$k_1 a_{q^n} + \ldots + k_{q^{n-1}} a_q^{q^{n-1}} + \ldots + k_{q^n} a_1^{q^n} = (k_{q^n})^{q^g} .$$

But I claim this is an Eisenstein equation:

$$b + a_1^{q^n} y = y^{q^g} \tag{4.4}$$

for $y = k_{q^n}$ over K_{n-1}. It is clear that b is integral, by (4.2). Since G lifts $G_{1/h}$ and $d = 1$, we know $v_K(a_i) \geq 1$ for $i \neq q$. Consequently, $v_{K_{n-1}}(a_i) > 1$ for $i \neq q$ and

$$v_{K_{n-1}}(b) = v_{K_{n-1}}(k_{q^{n-1}} a_q^{q^{n-1}}) = 1$$

by our inductive hypothesis that $k_{q^{n-1}}$ is a uniformizing parameter in K_{n-1}. Therefore $K_n = K_{n-1}(k_{q^n})$ has degree q^g over K_{n-1} and uniformizing parameter k_{q^n}. By induction, we know that $[K_{n-1}:K] = (q^g-1)q^{g(n-1)}$; hence the injection

$$\rho_n : \operatorname{Gal}(K_n/K) \longrightarrow (B/\pi_B^{n+1}B)^*$$

is surjective by counting. By applying corollary (1.6) to the equation (4.4) we see that $\operatorname{Gal}(K_n/K_{n-1})$ has a unique upper and lower break at the point:

$$m = v_{K_{n-1}}(a_1^{q^n})\, q^g/q^g-1 - 1 = q^{hn} - 1 .$$

The calculation of the filtrations on $\operatorname{Gal}(K_n/K)$ is now accomplished using the identity $\phi_{K_n/K} = \phi_{K_{n-1}/K} \circ \phi_{K_n/K_{n-1}}$, the inductive hypothesis, and the fact that

$$\phi_{K_n/K_{n-1}}(x) = x \qquad \text{for } x \leq q^{nh} - 1 .$$

This lemma yields part 1) of Theorem 3.5 as an immediate corollary. Given an adequate theory of π-divisible A-modules, we can see how part 2) of this Theorem would follow formally from part 1). We can define the character:

$$\varepsilon_A = \det_A(\rho) : \mathcal{G} \longrightarrow A^*$$

where $\det_A : B^*_{1/g} \times GL(d,A) \longrightarrow A^*$ is the reduced norm in the category of F-algebras. In analogy with (2.7) one would expect:

$$\varepsilon_A \overset{?}{=} 1 \quad \text{in } \mathrm{Hom}(\mathcal{G}, A^*) . \tag{4.5}$$

When $d = 1$ this would imply:

$$\rho_{0/1} \overset{?}{=} (\mathrm{Nm}_{1/g} \circ \rho_{1/g})^{-1} , \tag{4.6}$$

from which we could easily derive its ramification filtration. Since the full theory of "A-crystals" is not available to prove (4.5), we shall prove part 2) independently, and check that the results are consistent with (4.6).

First we must identify the representation

$$\rho_{0/1} : \mathcal{G} \longrightarrow GL(d,A) = M^*$$

where $M = \mathrm{Mat}(d,A)$. We appropriate our previous notation: for $n \geq 0$ let H_n be the kernel of the composed homomorphism:

$$\rho_n : \mathcal{G} \longrightarrow M^* \longrightarrow M^*/\, 1 + \pi^{n+1}M \simeq (M/\pi^{n+1}M)^*$$

and let K_n be the fixed field of H_n in $\overline{K}_s$.

If $\overline{m} = \{x \in \overline{K} : v_K(x) > 0\}$, then the set of points of G in $\overline{m}$ give a genuine A-module $G(\overline{m})$. Let $G(\overline{m})_{\pi^{n+1}}$ be the finite submodule of π^{n+1}-torsion. This module is free of rank d over $A/\pi^{n+1}A$ and is stable under the action of $\mathcal{G}$. The resulting representation:

$$\mathcal{G} \longrightarrow \mathrm{Aut}_{A/\pi^{n+1}A}(G(\overline{m})_{\pi^{n+1}}) \simeq (M/\pi^{n+1}M)^*$$

may be identified with ρ_n . Consequently, K_n is just the separable subfield of the field of π^{n+1}-division points.

<u>Lemma 4.14</u>

<u>Assume that</u> $d = e = 1$. <u>Then for</u> $n \geq 0$,

1) ρ_n induces an isomorphism $\mathrm{Gal}(K_n/K) \simeq (A/\pi^{n+1}A)^*$.

2) If $\alpha_n \in G(\overline{m})_{\pi^{n+1}}$ and $[\pi^n]_G(\alpha) \neq 0$, then $\beta_n = \alpha_n^{q^{g(n+1)}}$ is a uniformizing parameter in K_n .

3) $\mathrm{Gal}(K_n/K_{n-1})$ has a unique upper and lower break at the point $m = q^{hn} - 1$.

4) The lower filtration of $G = \mathrm{Gal}(K_n/K)$ is given by:

$$\begin{array}{lll} G_0 = G & & \\ G_x = \mathrm{Gal}(K_n/K_0) & \text{for} & 0 < x \leq q^h - 1 \\ G_x = \mathrm{Gal}(K_n/K_1) & \text{for} & q^h - 1 < x \leq q^{2h} - 1 \\ \vdots & & \\ G_x = \mathrm{Gal}(K_n/K_{n-1}) & \text{for} & q^{(n-1)h} - 1 < x \leq q^{nh} - 1 \\ G_x = (1) & \text{for} & q^{nh} - 1 < x . \end{array}$$

5: The upper filtration of $G = \mathrm{Gal}(K_n/K)$ is given by:

$$\begin{array}{lll} G^0 = G & & \\ G^x = \mathrm{Gal}(K_n/K_0) & \text{for} & 0 < x \leq a(g) \\ G^x = \mathrm{Gal}(K_n/K_1) & \text{for} & a(g) < x \leq a(2g) \\ \vdots & & \\ G^x = \mathrm{Gal}(K_n/K_{n-1}) & \text{for} & a(g(n-1)) < x \leq a(gn) \\ G^x = (1) & \text{for} & a(gn) < x , \end{array}$$

where $a(g), a(2g), \ldots, a(ng)$ are defined in Theorem 3.5.

Proof. We use an induction on n . For $n = 0$ the extension K_0 is generated by the non-zero roots of the polynomial $f(x)$, where

$$[\pi]_G(x) = f(x^{q^g}) .$$

Since $d = e = 1$ each non-zero root β_0 has K-valuation $1/(q-1)$. Consequently the injection:

$$\rho_0 : \mathrm{Gal}(K_0/K) \longrightarrow (A/\pi A)^*$$

is an isomorphism, and β_0 is a uniformizing element. The break sequence is obvious as K_0 is tamely ramified over K.

Now assume the result holds for the layer K_{n-1}/K. Let α_n be an element in $G(\bar{m})_{\pi^{n+1}}$ not killed by π^n, and put

$$\alpha_{n-1} = [\pi]_G(\alpha_n) = f(\alpha_n{}^{q^g}) .$$

Raising this identity to the q^{ng} power, we obtain:

$$\beta_{n-1} = \alpha_{n-1}^{q^{ng}} = f^{q^{ng}}(\alpha_n^{q^{(n+1)g}}) = f^{q^{ng}}(\beta_n) .$$

By our induction hypothesis, β_{n-1} is a uniformizing parameter in K_{n-1}. Applying the Weierstrass preparation theorem to the power series

$$f^{q^{ng}}(x) = a_1^{q^{ng}} x + a_2^{q^{ng}} x^2 + \ldots + a_q^{q^{ng}} x^q + \ldots$$

we see that β_n satisfies an Eisenstein polynomial over K_{n-1} :

$$g(x) = x^q + b_{q-1}x^{q-1} + \ldots + b_1 x + b_0$$

with

$$v_{K_{n-1}}(b_0) = 1 \quad v_{K_{n-1}}(b_i) \geq v_{K_{n-1}}(b_1) .$$

We may therefore apply corollary (1.6) to conclude that $K_{n-1}(\beta_n)$ has degree q over K_{n-1} and a unique upper break at the point

$$m = qv_{K_{n-1}}(b_1)/q\text{-}1 - 1 = q^{nh} - 1 ,$$

as

$$v_{K_{n-1}}(b_1) = v_{K_{n-1}}(a_1^{q^{ng}}) = q^{ng}(q-1)q^{n-1} .$$

Clearly β_n is a uniformizing parameter in $K_{n-1}(\beta_n)$; counting degrees shows that $K_n = K_{n-1}(\beta_n)$ and that the injection

$$\rho_n : \mathrm{Gal}(K_n/K) \longrightarrow (A/\pi A)^*$$

is an isomorphism. One can now calculate the entire break sequence using the induction hypothesis and the identity

$$\phi_{K_n/K} = \phi_{K_{n-1}/K} \circ \phi_{K_n/K_{n-1}} .$$

This lemma immediately yields part 2) of Theorem 3.5 as a corollary. It is easy to check that **parts** 1) and 2) are consistent with (4.6) using the identities:

$$\mathrm{Nm}_A(1+\pi_B^{gn}B) = 1 + \pi_A^n A$$

$$\mathrm{Nm}_A(1+\pi_B^{gn+1}B) = 1 + \pi_A^{n+1}A .$$

-:-:-

Bibliography.

1. Demazure, M. Lectures on p-divisible groups. Lecture notes in mathematics No. 302, Springer-Verlag, Berlin-New York, 1972.

2. Drinfel'd, V. G. Elliptic modules. (Russian) Math. Sbornik, 94, 1974; English translation: Math. USSR-Sb., 23, 1976.

3. Grothendieck, A. Groupes de Barsotti-Tate et cristaux de Dieudonné. Séminaire de mathématiques supérieures No. 45, Beaverton, Oregon, 1974.

4. Lubin, J. Formal A-modules defined over A . Symposia math. inst. naz. di alta matematica, 1970.

5. Lubin, J. and Tate, J. Formal moduli for one-parameter formal Lie groups. Bull. soc. math. France (1), 94, 1966.

6. Raynaud, M. Schémas en groups de type (p,..,p). Bull. soc. math. France, 102, 1974.

7. Sen, S. Ramification in p-adic Lie extensions. Invent. math. (1), 17, 1972.

8. Serre, J.-P. Corps locaux. Publications de l'Institut de Mathématique de l'Université de Nancago, Actualités Sci. Indust. No. 1296, Hermann, Paris, 1962.

9. Serre, J.-P. Groupes p-divisibles(d'après J. Tate). Séminaire Bourbaki No. 318, 1966/67.

10. Tate, J. p-divisible groups. Proc. conf. on local fields, Springer, Berlin, 1967.

11. Wintenberger, J.-P. Automorphismes et extensions galoisiennes de corps locaux. Thesis, Grenoble, 1978.

-:-:-:-

Benedict H. GROSS
Department of Mathematics
Princeton University
Princeton, NJ 08540
U.S.A.