Submitted exclusively to the London Mathematical Society
doi:10.1112/0000/000000

Torsion in the Nottingham group

Jonathan Lubin

Abstract

From local class-field theory and higher ramification theory one gets a classification up to conjugacy of the torsion elements of arbitrary order in the Nottingham group over a finite field, in terms of continuous characters on the multiplicative group of principal units in the ring of formal power series over the field. An essential part of this classification is to partition the torsion elements according to the depths of their successive p-power iterates. The classification described here is good enough to permit an independent proof of Klopsch's theorem on torsion elements of order p, but not good enough to give a full description of the finite set of classes of torsion elements with a given depth-sequence. The final section exhibits an efficient method of calculating the first few hundred terms of a series of order p^n, limited only by the capabilities of the computation package used, but gives no idea of any formula for describing the coefficients.

Introduction

This paper arises out of an appreciation of the Theorem of Klopsch [**5**], according to which the elements of the Nottingham group over a finite field κ of characteristic $p > 0$ that are of period p are classified in two steps: first according to the depth, which may be any positive integer d prime to p, but when d is given, there are only $|\kappa| - 1$ conjugacy classes, described neatly by the coefficient of the torsion series in degree $d + 1$.

There is little new mathematics in this paper. Rather, it makes direct use of standard results from local class field theory as may be found in [**7**] (English translation, [**8**]). And in Section 5 we use results from [**6**].

This paper is organized as follows: first I run through a very quick description of Klopsch's result, as a standard to reach for in the more complicated case of general order p^n. Next, the quickest and sketchiest possible précis of local class field theory, as it applies to the analysis of the situation at hand. Then I explain how a character of a certain type on the multiplicative group $1 + t\kappa[\![t]\!]$ describes and can be used to construct a torsion element of Nottingham, and discuss an equivalence relation among such characters that corresponds to conjugacy of the torsion elements in Nottingham; and I show how the ramification numbers of the character are related to the depths of successive p-power iterates of the torsion element. Then I give a proof of Klopsch's Theorem using these tools, to show how the method applies. The final application is a sketch of how to use symbolic computation to produce from a character of order p^n the essentially unique torsion element of Nottingham that corresponds.

1. *Notations, conventions, prior results*

We will work with a fixed finite constant field κ of characteristic p. Our discussions will deal mostly with extensions of Laurent-series fields over κ, and as much as possible I will call the larger field $K = \kappa(\!(x)\!)$, the smaller one $F = \kappa(\!(t)\!)$. The ring of integers of each of these fields will

---

2000 *Mathematics Subject Classification* 11S31 (primary), 37P35 (secondary). Please refer to `http://www.ams.org/msc/` for a list of codes.

be denoted $\mathcal{O}_K = \kappa[\![x]\!]$ and $\mathcal{O}_F = \kappa[\![t]\!]$, respectively, with maximal ideal $x\mathcal{O}_K = \mathfrak{M}_K$ and $\mathfrak{M}_F$ respectively. We also need to handle the groups of principal units of these, $1 + \mathfrak{M}_K$ and $1 + \mathfrak{M}_F$. Although the definitions here have depended on the choice of uniformizer x and t, the structures themselves are not so dependent. That is, any field automorphism $\varphi \in \mathrm{Aut}_\kappa(K)$ sends $\mathcal{O}_K$ and $\mathfrak{M}_K$ to themselves. An automorphism that sends a uniformizer x of K to xz, where $z \in 1 + \mathfrak{M}_K$, is called *wild*; again this does not depend on the choice of x. I will use x^φ to denote the image of x under the action of φ, so that $x^\varphi = u(x) = x\bigl(1 + \sum_{m\geq 1} a_m x^m\bigr) \in \mathcal{O}_K$. If d is the smallest index for which $a_d \neq 0$, we say that the *depth* of u is d, and write $\delta(u) = d$. The depth is a property of the automorphism φ, not merely the series u that describes it. The set of wild automorphisms of K is a group, which I will denote $\mathrm{Aut}^1_\kappa(K)$, and the corresponding series are all the $u(x) = x + \cdots \in x(1 + \mathfrak{M}_K)$, the *Nottingham group* over κ. I will write automorphisms and isomorphisms of fields on the right, as exponents: if $x^\varphi = u$ and $x^\psi = w$, then $x^{\varphi\psi}$ is the composition $u \circ w$, the result of substituting $w(x)$ for the variable in $u(x)$. I will use the notation $u^{\circ n}$ for the n-fold iterate of u, except when $n = -1$. And I will write $\langle * \rangle$ for the group generated by the element or set or list of objects represented by the asterisk.

The Nottingham group $\mathfrak{N}_\kappa$ is a pro-p group, and it has for each m prime to p a useful injective homomorphism that I will call *m-dispersal*, $\mathrm{Disp}_m \colon \mathfrak{N}_\kappa \to \mathfrak{N}_\kappa$, which takes $u(x) = xg(x)$, if $g \in 1 + \mathfrak{M}_K$, to $\bigl(u(x^m)\bigr)^{1/m} = x\bigl(g(x^m)\bigr)^{1/m}$, clearly a homomorphism from the first formula, clearly well-defined from the second formula, since any principal unit may always be raised to an exponent that is a p-adic integer. This is perhaps the first construct discussed here that depends on the choice of the uniformizer x. Its utility comes from the obvious relation $\delta\bigl(\mathrm{Disp}_m(u)\bigr) = m\delta(u)$.

For a nonzero constant $\alpha \in \kappa$, consider the fractional-linear series $j_{1,\alpha}(x) = x/(\alpha x + 1) = x - \alpha x^2 + \cdots$, a p-torsion element of $\mathfrak{N}_\kappa$. For m prime to p, let us define $j_{m,\alpha}$ to be $\mathrm{Disp}_m(j_{1,m\alpha}) = x - \alpha x^{m+1} + \cdots$, also a p-torsion element of $\mathfrak{N}_\kappa$, but now of depth m instead of 1. The Theorem of Klopsch [**5**] that was mentioned before states simply that every p-torsion element of $\mathfrak{N}_\kappa$ is the conjugate in that group of a unique $j_{m,\alpha}$. Since $\alpha \neq \beta$ implies that $x + \alpha x^{m+1} + \cdots$ is not conjugate to any $x + \beta x^{m+1} + \cdots$, Klopsch has given us a very clear vision of just what the p-torsion in $\mathfrak{N}_\kappa$ is.

2. *Local class-field theory*

In the incarnation of the subject presented here, class field theory deals with abelian extensions of local fields. But let us first examine some aspects of local fields that are quite general, not involving Galois theory in any way.

2.1. *The multiplicative structure of a local field*

For a local field in characteristic p such as F, we have two exact sequences:

$$1 \longrightarrow 1 + \mathfrak{M}_F \longrightarrow \mathcal{O}_F^* \longrightarrow \kappa^* \longrightarrow 1 \tag{1}$$

$$1 \longrightarrow \mathcal{O}_F^* \longrightarrow F^* \xrightarrow{V} \mathbb{Z} \longrightarrow 0 \tag{2}$$

In line (1), the sequence splits because the constants are in $\mathcal{O}_F$ already; in (2), the map V is the additive valuation on F, nonnegative on elements of $\mathcal{O}_F$, and describing a splitting is equivalent to choosing a uniformizer τ of F, that is an element with $V(\tau) = 1$. Subject to the choice of τ, then, we can write $F^* \cong \langle\tau\rangle \oplus \kappa^* \oplus (1 + \mathfrak{M}_F)$.

When we have a finite extension $K \supset F$ of fields, where F is complete and discretely valued, then it is a consequence of Hensel's Lemma that the unique $\mathbb{Z}$-valued valuation on K satisfies the formula $V_K(z) = V_F\bigl(\mathcal{N}_F^K(z)\bigr)/f$, where $\mathcal{N}_F^K \colon K^* \to F^*$ is the field-theoretic norm, and f is the residue-field extension degree, a number that is equal to 1 in the case of total ramification.

OBSERVATION 1. Let $K \supset F$ be a totally ramified extension of local fields of characteristic p, and let $z \in K$. Then $\mathcal{N}_F^K(z) \in \mathcal{O}_F$ if and only if $z \in \mathcal{O}_K$; and if the extension is totally wild, i.e. the degree is a power of p, then $\mathcal{N}_F^K(z) \in 1 + \mathfrak{M}_F$ if and only if $z \in 1 + \mathfrak{M}_K$.

Little needs to be said about the proof except that for the second part, one needs to use the fact that when the norm is restricted to the constants, its kernel is trivial, because $|\kappa^*|$ is prime to p. Note that nothing in the preceding presumes that the extension is Galois or even separable.

COROLLARY 1. Let $K \supset F$ be a totally wildly ramified extension of local fields with constant field κ, let π_1, π_2 be uniformizers for K, and let $\tau_i = \mathcal{N}_F^K(\pi_i)$. If $\pi_1^\Phi = \pi_2$ and $\tau_1^\varphi = \tau_2$, with $\Phi \in \mathrm{Aut}_\kappa(K)$ and $\varphi \in \mathrm{Aut}_\kappa(F)$, then Φ is wild if and only if φ is also.

2.2. *Finite subgroups of Nottingham as Galois groups*

If u is a torsion element of $\mathfrak{N}_\kappa$ of period p^n, then we may apply the following general considerations to the group it generates. Any finite subgroup Γ of $\mathfrak{N}_\kappa$, whether cyclic or not, being a group of κ-automorphisms of $K = \kappa(\!(x)\!)$, will have a fixed field F over which K is Galois with group Γ. The smaller field certainly has the same constant field, so the extension is totally ramified, of degree $|\Gamma|$, and wildly ramified, since the degree is a power of p. Moreover, the norm of x, $t = \prod_{u\in\Gamma} u(x)$, is in F, and is a uniformizer for F. Any time we have a totally ramified extension $K \supset F$ with a pair of uniformizers (π, τ) such that $\mathcal{N}_F^K(\pi) = \tau$, I will refer to the coordinatizations as *consistent*.

But we have a situation where $K \supset F$ is a finite abelian extension of local fields with Galois group Γ. And for this situation there is the tool of local class-field theory, according to which there is an exact sequence

$$K^* \xrightarrow{\mathcal{N}_F^K} F^* \xrightarrow{\rho_F^K} \Gamma \longrightarrow 1\,,$$

where $\mathcal{N}_F^K$ is the norm, and ρ_F^K is the *norm residue map*. That is, ρ_F^K gives a canonical isomorphism between $F^*/\mathcal{N}_F^K(K^*)$ and Γ, the Galois group $\mathrm{Aut}_F(K)$. The norms from K are open in F^*, and indeed if U is any open subgroup of finite index in F^*, then there is a canonical abelian extension $K \supset F$ with $\mathcal{N}_F^K K^* = U$. The association $U \mapsto K$ is functorial: if $\psi\colon F \to F'$ is an isomorphism, then the corresponding extension $K' \supset F'$ has a corresponding isomorphism $\Psi\colon K \to K'$ such that for $z \in F$, $\rho_{F'}^{K'}(z^\psi) = \Psi^{-1}\rho_F^K(z)\Psi$ and as a result we have also the fact that for $\xi \in K^*$, $\left(\mathcal{N}_F^K(\xi)\right)^\psi = \mathcal{N}_{F'}^{K'}(\xi^\Psi)$. It should be pointed out here that to go from the data of F and the subgroup U to K and the map ρ_F^K is a procedure that is well-suited to calculation, at least with machine help, and we will do this in Section 5.

2.3. *Cyclic extensions*

Our concern in this paper is with cyclic extensions $K \supset F$, for which the Galois group Γ has a specified generator γ, and in this case we may use the isomorphism $\Gamma \cong \mathbb{Z}/p^n\mathbb{Z}$ induced by $\gamma \leftrightarrow 1$ to define a continuous character $\mathbf{X} = \mathbf{X}_\gamma\colon F^* \to \mathbb{Z}/p^n\mathbb{Z}$ with the property that for all $z \in F^*$, $\rho_F^K(z) = \gamma^{\mathbf{X}(z)}$, as summarized here:

$$\begin{array}{ccccc} F^* & \xrightarrow{\rho_F^K} & \Gamma & \ni & \gamma \\ & \searrow^{\mathbf{X}_\gamma} & \updownarrow\cong & & \updownarrow \\ & & \mathbb{Z}/p^n\mathbb{Z} & \ni & 1 \end{array} \tag{3}$$

When we've started with a coordinatization of K, in effect giving from γ a torsion element of the Nottingham group, there is additional information, summarized as:

OBSERVATION 2. Let $u(x) \in \mathfrak{N}_\kappa$ be a torsion element of period p^n; let $t = \prod_{i=0}^{p^n-1} u^{\circ i}(x)$; and let $F = \kappa(\!(t)\!)$. Then $K = \kappa(\!(x)\!)$ is cyclic, totally wildly ramified over F of degree p^n, and $U = \mathcal{N}_F^K(K^*)$ is open in F^*, containing t and κ^*, with F^*/U isomorphic via ρ_F^K to $\langle u \rangle$.

The group of norms contains κ^* because on the constants, the norm is the p^n-th power map, and $|\kappa^*|$ is prime to p.

2.4. *Characters on the principal units*

The character $\mathbf{X}\colon F^* \to \mathbb{Z}/p^n\mathbb{Z}$, where $F = \kappa(\!(t)\!)$, which came originally from a torsion element of Nottingham, can always be restricted to the principal units $1 + \mathfrak{M}_F$, losing some information in the process; but here, we look at the reverse process of starting with a character $\chi\colon 1 + \mathfrak{M}_F \to \mathbb{Z}/p^n\mathbb{Z}$ to get a torsion element of Nottingham.

Starting with a surjective continuous character $\chi\colon 1 + \mathfrak{M}_F \to \mathbb{Z}/p^n\mathbb{Z}$ and a uniformizer $t \in \mathfrak{M}_F$, we will construct a cyclic extension $K \supset F$ and a generator γ of $\mathrm{Gal}(K/F)$. Note that Corollary 1 tells us that when γ is described by a power series $u(x)$ dependent on a choice of uniformizer $x \in \mathfrak{M}_K$, the conjugacy class of u in $\mathfrak{N}_\kappa$ does not depend on the choice of x, as long as (x, t) is a consistent pair. Here is our procedure, then: the given character χ extends uniquely to all of $\mathcal{O}^*$, and we extend it to all of F^* by letting it be zero at t. Call the extended character $\mathfrak{X}$. If the kernel of χ is $U_0 \subset 1 + \mathfrak{M}_F$, then $\ker(\mathfrak{X}) = \langle t, \kappa^*, U_0 \rangle$. Call this subgroup U; it's open in F^*, and $F^*/U \cong \mathbb{Z}/p^n\mathbb{Z}$. We apply the existence theorem of local class-field theory to get the abelian extension field K, unique up to isomorphism, with $\mathcal{N}_F^K(K^*) = \ker(\rho_F^K) = U$, and take $\gamma = \rho_F^K\big(\mathfrak{X}^{-1}(1)\big)$. Since t is a norm from K, there are $x \in K$ that make (x, t) a consistent pair, to give a p^n-torsion element of $\mathfrak{N}_\kappa$ unique up to conjugacy in that group. I will refer to the above process, which starts with a character on $1 + t\kappa[\![t]\!]$ and ends with a torsion element $u(x)$ of $\mathfrak{N}_\kappa$, as the *standard procedure*.

OBSERVATION 3. The Nottingham group $\mathfrak{N}_\kappa$ acts on the group of characters defined on $1 + t\kappa[\![t]\!]$ with values in $\mathbb{Z}/p^n\mathbb{Z}$ in a natural way: if χ is such a character, and $w(t) \in \mathfrak{N}_\kappa$, then ${}_w\chi(f) = \chi(f \circ w)$, for $f \in 1 + t\kappa[\![t]\!]$. As one would expect, ${}_w\big({}_{w'}\chi\big) = {}_{ww'}\chi$.

When χ is a character on $1 + \mathfrak{M}_F$ and ψ is an isomorphism from F' to F, I will use the same notation, ${}_\psi\chi$, for the corresponding character on $1 + \mathfrak{M}_{F'}$.

DEFINITION 1. Let χ_1 and χ_2 be characters, $\chi_i\colon 1 + t\kappa[\![t]\!] \to \mathbb{Z}/p^n\mathbb{Z}$. We say that χ_1 is *strictly equivalent* to χ_2 and write $\chi_1 \simeq \chi_2$ if there is $w(t) \in \mathfrak{N}_\kappa$ such that $\chi_2 = {}_w\chi_1$ and $w(t)/t \in \ker(\chi_1)$.

One verifies without difficulty that strict equivalence is indeed symmetric and transitive. Note, however, that if $\chi_1 \simeq \chi_2$ and $\chi_2 = {}_w\chi_1$, it is not necessarily the case that $w(t)/t \in \ker(\chi_1)$. It is easily seen also that if $\psi \in \mathrm{Aut}_\kappa^1\big(\kappa(\!(t)\!)\big)$, with $\chi_2 = {}_\psi\chi_1$ and $t^\psi/t \in \ker(\chi_1)$, then ψ maps $\langle t, \kappa^*, \ker(\chi_2)\rangle$ onto $\langle t, \kappa^*, \ker(\chi_1)\rangle$.

LEMMA 2.1. *Let $K \supset F$ be a totally ramified cyclic extension of degree p^n, with $\mathrm{Gal}(K/F)$ generated by γ, let $\mathbf{X}_\gamma$ be the continuous character defined on F^* and onto $\mathbb{Z}/p^n\mathbb{Z}$ described in 2.3, and let π_1, π_2 be uniformizers of K for which $\pi_2/\pi_1 \in 1+\mathfrak{M}_K$. For $i = 1, 2$, let $\tau_i = \mathcal{N}_F^K(\pi_i)$; let $\psi_i \colon \kappa(\!(t)\!) \to F$ be the isomorphism taking t to τ_i; and let χ_i be the restriction to $1 + t\kappa[\![t]\!]$ of ${}_{\psi_i}\mathbf{X}_\gamma$. Then χ_1 and χ_2 are strictly equivalent characters on $1 + t\kappa[\![t]\!]$.*

$$\begin{array}{ccccccc} 1+t\kappa[\![t]\!] & \hookrightarrow & \kappa(\!(t)\!) & \overset{\psi_1}{\underset{\psi_2}{\rightrightarrows}} & F^* & \xleftarrow{\mathcal{N}_F^K} & K^* \\ & \searrow^{\chi_1} & & & \downarrow \mathbf{X}_\gamma & & \\ & \searrow_{\chi_2} & & & \mathbb{Z}/p^n\mathbb{Z} & & \end{array}$$

Proof. Because $\pi_2/\pi_1 \in 1+\mathfrak{M}_K$, we similarly have τ_2/τ_1 lying in $1+\mathfrak{M}_F$, which means that $\psi_2\psi_1^{-1} \in \mathrm{Aut}_\kappa^1\big(\kappa(\!(t)\!)\big)$. Thus $\chi_2 = {}_{\psi_2\psi_1^{-1}}\chi_1$, so that for $\chi_1 \simeq \chi_2$, it remains to show $t^{\psi_2\psi_1^{-1}}/t \in \ker(\chi_1)$. We have:

$$\chi_1\left(\frac{t^{\psi_2\psi_1^{-1}}}{t}\right) = \chi_1\left(\left(\frac{t^{\psi_2}}{t^{\psi_1}}\right)^{\psi_1^{-1}}\right) = \mathbf{X}_\gamma\left(\frac{t^{\psi_2}}{t^{\psi_1}}\right) = \mathbf{X}_\gamma\left(\frac{\tau_2}{\tau_1}\right),$$

which is zero because both τ_i are norms from K.

THEOREM 2.2. *If u_1 and u_2 are torsion elements of $\mathfrak{N}_\kappa$ that are conjugate in that group, then the characters on $1 + t\kappa[\![t]\!]$ that correspond are strictly equivalent. Conversely if χ_1 and χ_2 are strictly equivalent continuous characters on $1 + t\kappa[\![t]\!]$ with values in $\mathbb{Z}/p^n\mathbb{Z}$, the torsion power series that arise from them by the standard procedure are conjugate in $\mathfrak{N}_\kappa$.*

Proof. Starting with two conjugate elements of $\mathfrak{N}_\kappa$, we may as well treat them as descriptions of the same torsion element γ of $\mathrm{Aut}_\kappa^1(K)$ arising from coordinatizations by elements π_1 and π_2 of K. The hypothesis on the u_i implies that $\pi_2/\pi_1 \in 1+\mathfrak{M}_K$, so that we may apply Lemma 2.1 directly.

For the converse, let $F = \kappa(\!(t)\!)$ and let $\chi_1 \simeq \chi_2$, characters on $1 + t\kappa[\![t]\!]$, values in $\mathbb{Z}/p^n\mathbb{Z}$. We need to show that the standard procedure produces power series that are torsion elements of $\mathfrak{N}_\kappa$ conjugate in that group. Choose $u(t) \in \kappa[\![t]\!]$, then, corresponding to $\psi \in \mathrm{Aut}_\kappa^1(F)$, for which $\chi_2 = {}_u\chi_1$ and $u(t)/t \in \ker(\chi_1)$. In accordance with our procedure, we extend χ_i to a character $\mathfrak{X}_i$ defined on all of F^* by setting $\mathfrak{X}_i(t) = 0$.

$$\begin{array}{ccc} K_2^* & \overset{\Psi}{\dashrightarrow} & K_1^* \\ \downarrow \mathcal{N}_F^{K_2} & & \downarrow \mathcal{N}_F^{K_1} \\ F^* = \kappa(\!(t)\!)^* & \xrightarrow[t \mapsto u(t)]{\psi} & F^* \\ & \searrow^{\mathfrak{X}_2} & \downarrow \mathfrak{X}_1 \\ & & \mathbb{Z}/p^n\mathbb{Z} \end{array}$$

At this point, we have only the lower part of the diagram, and even need to verify that $\mathfrak{X}_1 \circ \psi = \mathfrak{X}_2$. This is certainly true on elements of $1+\mathfrak{M}_F$, since that is our hypothesis $\chi_2 = \chi_1 \circ \psi$. But $\mathfrak{X}_1(t^\psi) = \mathfrak{X}_1(t\, t^\psi/t) = \mathfrak{X}_1(t) + \chi_1(t^\psi/t) = 0$, which is enough to prove the claim. Let us call

$U_i = \ker(\mathfrak{X}_i)$; then we see that $U_2^{\psi} = U_1$, which was already remarked in the comments after Definition 1.

Now, class-field theory tells us that corresponding to U_1 and U_2 there are abelian field extensions, indeed cyclic extensions K_1 and K_2, such that each U_i is equal to $\mathcal{N}_F^{K_i}(K_i^*)$, and that there is $\Psi\colon K_2 \to K_1$ fitting into the preceding diagram: for each $z \in F^*$, $\Psi^{-1}\rho_F^{K_2}(z)\Psi = \rho_F^{K_1}(z^{\psi})$. Recall that the standard procedure specifies an element of $\mathrm{Gal}(K_i/F)$, $\gamma_i = \rho_F^{K_i}\big(\mathfrak{X}_i^{-1}(1)\big)$. Thus $\gamma_1 = \Psi^{-1}\gamma_2\Psi$. This does not yet prove anything: the desired conclusion involves power series, not automorphisms, and the standard procedure demands that we coordinatize the upper field in each case by a choice of uniformizer there that gives a consistent pair: $\pi_i \in K_i$ with $\mathcal{N}_F^{K_i}(\pi_i) = t$.

Put $\pi_i^{\gamma_i} = w_i(\pi_i)$, where $w_i(x) \in \kappa[\![x]\!]$, x being an indeterminate; also put $\varpi = \pi_2^{\Psi}$. Then the relations so far established give $\varpi^{\gamma_1} = \big(w_2(\pi_2)\big)^{\Psi} = w_2\big(\pi_2^{\Psi}\big) = w_2(\varpi)$; that is, the automorphism γ_1 of K_1 is represented by the power series w_1 when the uniformizer π_1 is used, but by w_2 when ϖ is used. To show that the the two series are conjugate in $\mathfrak{N}_\kappa$, we need only show that ϖ/π_1 is a principal unit. But one easily sees that $\mathcal{N}_F^{K_1}(\varpi/\pi_1) = \big(\mathcal{N}_F^{K_2}(\pi_2)\big)^{\psi}/t = t^{\psi}/t$, which is a principal unit; and so by using Observation 1, we see that w_1 and w_2 are conjugate in $\mathfrak{N}_\kappa$.

3. *The ramification data of a character*

In view of Theorem 2.2, our attention passes from torsion elements of the Nottingham group to continuous characters on $1 + t\kappa[\![t]\!]$. Such characters are easy to construct in bewildering profusion, and in Section 5 I will show how to use the explicit formulas of local class field theory to write down as many terms as desired of the torsion element of Nottingham that comes from a given character, subject only to the computing capability at our disposal.

In this section, we use a stripped-down version of higher ramification theory to give a coarse classification of continuous characters $\chi\colon 1 + t\kappa[\![t]\!] \to \mathbb{Z}/p^n\mathbb{Z}$. I will quote many results from Chapter 4 of [**7**] (or [**8**]), but will attempt to make the exposition comprehensible to readers not familiar with this material.

3.1. *The multiplicative fine-structure of a local field*

Unlike the situation in characteristic zero, where the existence of the logarithm shows that the principal units $1 + \mathfrak{M}_F$ in the field F have a subgroup of finite index isomorphic to $\mathcal{O}_F^+$, the situation in positive characteristic is much more interesting. The simplest case here is $\mathbb{F}_p(\!(t)\!)$, with constant field the prime field. One easily sees that the group $1 + t\mathbb{F}_p[\![t]\!]$ is topologically generated by the series $\{1 + t^m\}$ for m prime to p, so that $1 + t\mathbb{F}_p[\![t]\!] \cong \prod_m (1 + t^m)^{\mathbb{Z}_p}$, the indices ranging over those same values of m—because of the topology on the underlying group, that's a direct product, not sum. But the basis I've specified is arbitrary, far from natural; the best basis is one related to the Artin-Hasse exponential—for a complete treatment of this matter, one may refer to [**4**], Chapter III, Section 17. But all of these descriptions of $1 + t\mathbb{F}_p[\![t]\!]$ are based on the coordinatization by way of the uniformizer t: they are not in any sense absolute.

When the constant field is not the prime field, the general picture is just as clear: if $[\kappa\colon \mathbb{F}_p] = f$, then a basis $\{\zeta_1, \cdots, \zeta_f\}$ of κ over the prime field gives us a topological basis $\{1 + \zeta_j t^m\}$ with all (j, m) satisfying $1 \le j \le f$ and $\gcd(p, m) = 1$. Once again, the Artin-Hasse exponential comes into its own, telling us that for each m prime to p, there is a factor of $1 + t\kappa[\![t]\!]$ naturally isomorphic to $W_\infty(\kappa)$, the ring of Witt vectors over κ. But while the action of $\mathfrak{N}_\kappa$ on $1 + t\kappa[\![t]\!]$ is $\mathbb{Z}_p = W_\infty(\mathbb{F}_p)$-linear, this action does not respect the structure of $1 + t\kappa[\![t]\!]$ as $W_\infty(\kappa)$-module. Thus we will not benefit from the use of Artin-Hasse. Suffice it to say that to describe a

continuous character χ on $1+t\kappa[\![t]\!]$ with values in $\mathbb{Z}/p^n\mathbb{Z}$, it is enough to specify the value at each $1+\zeta_j t^m$, the indices as above, though all but finitely many of these values will be zero.

3.2. *The break sequence of a character*

Definition 2. Let F be a local field in which the maximal ideal of the ring of integers is $\mathfrak{M}$, and let χ be a continuous character from $1+\mathfrak{M}$ onto $\mathbb{Z}/p^n\mathbb{Z}$. Then the *break sequence* of χ is $\langle b^{(0)}, b^{(1)}, \cdots, b^{(n-1)}\rangle$, where for each j, $b^{(j)}$ is the largest integer b for which there is $z \in 1+\mathfrak{M}^b$ such that $\chi(z) = p^j$.

Alternatively, $p^{n-j-1}\chi$ is trivial on $1+\mathfrak{M}^{b^{(j)}+1}$ but not on $1+\mathfrak{M}^{b^{(j)}}$. A more important way of looking at the break sequence is the following:

Observation 4. Let $\mathfrak{X}\colon F^* \to \mathbb{Z}/p^n\mathbb{Z}$ be a continuous surjective character, and let K be the corresponding extension of F, with Galois group generated by γ. If $\langle b^{(0)}, \cdots, b^{(n-1)}\rangle$ is the ramification sequence of $\mathfrak{X}$, then for each j, $\rho_F^K(1+\mathfrak{M}_F^{b^{(j)}}) = \langle \gamma^{p^j}\rangle$, while $\rho_F^K(1+\mathfrak{M}_F^{b^{(j)}+1}) = \langle \gamma^{p^{j+1}}\rangle$.

As an example over $\mathbb{F}_3$ with $n=2$, suppose $\chi(1+t) = 2 \in \mathbb{Z}/9\mathbb{Z}$, $\chi(1+t^2) = 3$, and $\chi(1+t^5) = 6$, but all for all other values of m prime to 3, $\chi(1+t^m) = 0$. Then $b^{(0)} = 1$ and $b^{(1)} = 5$.

Observation 5. Let F be a local field of characteristic p, and χ a character from $1+\mathfrak{M}_F$ onto $\mathbb{Z}/p^n\mathbb{Z}$. Then the ramification sequence $\langle b^{(0)}, \cdots, b^{(n-1)}\rangle$ of χ satisfies the conditions:
(1) $\gcd(p, b^{(0)}) = 1$;
(2) For each $i > 0$, $b^{(i)} \geq pb^{(i-1)}$; and
(3) If the above inequality is strict, then $\gcd(p, b^{(i)}) = 1$.
Conversely, every sequence $\langle b^{(0)}, \cdots, b^{(n-1)}\rangle$ satisfying the above three conditions is the ramification sequence of some character χ on $1+\mathfrak{M}_F$.

This is easily seen, when the structure of $1+\mathfrak{M}_F$ is taken into account. Among the possible forms for the sequence $\langle b\rangle$, one may be pointed out as most special: the one where $b^{(i)} = p^i$; we can call these characters *minimally ramified*.

We will see in the next section that the classification of characters according to their ramification sequences is the appropriate generalization to cyclic subgroups of $\mathfrak{N}_\kappa$ of nonprime order of the rough classification by depth in Klopsch's Theorem. But at this stage, we merely make:

Observation 6. There are only finitely many different characters χ with the ramification sequence $\langle b^{(0)}, b^{(1)}, \cdots, b^{(n-1)}\rangle$, and, *a fortiori*, only finitely many strict equivalence classes of such characters.

Indeed, if $r = b^{(n-1)} + 1$, then χ vanishes on $1+\mathfrak{M}_F^r$, so that χ is effectively a character on the group $(1+\mathfrak{M})/(1+\mathfrak{M}^r)$, finite because κ is finite.

3.3. *Upper and lower numberings: breaks and depths*

Consider a character χ of the type we've been discussing, and the torsion element $u \in \mathfrak{N}_\kappa$ of period p^n that has come from χ by application of the standard procedure. Since the depths of

u and its several p^j-power iterates are clearly invariant under conjugation, and similarly the break sequence of χ is invariant under the action of $\mathfrak{N}_\kappa$, one would hope for a way of relating these two sequences. In this paragraph, I do just that.

DEFINITION 3. Let $K \supset F$ be a totally ramified Galois extension of local fields, with $\mathrm{Gal}(K/F) = G$. If $\pi \in \mathfrak{M}_K$ is a uniformizer for K, set $G_j = \{\gamma \in G\colon v_\pi(\pi^\gamma/\pi - 1) \geq j\}$.

OBSERVATION 7. The filtration $G = G_0 \supset G_1 \supset \cdots$ does not depend on the choice of π, and the subgroups G_j all are normal in G.

PROPOSITION 3.1. *Let $K \supset F$ be a totally ramified Galois extension of local fields with group G, and let κ be their common constant field. Then G_0/G_1 is injected into κ^*, and for $i > 0$, G_i/G_{i+1} is injected into κ^+. In particular, if G is cyclic of degree p^n, then $(G_i : G_{i+1}) \leq p$ and there are precisely n values of i for which $G_i \neq G_{i+1}$.*

The proof is easy, and I refer the reader not familiar with this matter to a standard reference such as Chapter IV of [**7**] ([**8**]).

DEFINITION 4. For a Galois totally ramified extension $K \supset F$, the *lower breaks* are the finitely many values of i for which $G_i \neq G_{i+1}$. When we denote them in ascending order b_0, b_1, …, b_{s-1}, the *upper breaks* $b^{(0)}$, $b^{(1)}$, …, $b^{(s-1)}$ are defined as follows:

$$\left.\begin{aligned} b^{(0)} &= b_0 \\ b^{(j)} &= b^{(j-1)} + \frac{b_j - b_{j-1}}{(G\colon G_{b_j})}\,, \text{ for } j > 0 \end{aligned}\right\} \tag{4}$$

OBSERVATION 8. When u is a torsion element of $\mathfrak{N}_\kappa$ of period p^n, the n lower breaks of the Galois group $\Gamma = \langle u \rangle$ are exactly the depths of u, $u^{\circ p}$, …, $u^{\circ p^{n-1}}$.

Let us return to Definition 4 for a moment: it is by no means obvious that the upper breaks are integers, and indeed they usually are not. But the Hasse-Arf Theorem says that when the Galois group is abelian, the upper breaks are integral. Its background and proof can be found in §3 of Chapter IV and §7 of Chapter V, respectively, of [**7**].

Another result that we need, and that I can only quote and not attempt to prove here, is to be found at the very end of [**7**]: it is that when an extension $K \supset F$ is totally ramified and abelian with group G, then $G_{b_j} = \rho_F^K(1 + \mathfrak{M}_F^{b^{(j)}})$. The precise reference is [**7**], Chapter XV, §3, Theorem 2. The upshot is:

PROPOSITION 3.2. *If γ is an element of $\mathrm{Aut}_\kappa(K)$ of period p^n, with fixed field F, and $\mathbf{X}_\gamma$ is the associated character defined on F^*, then the upper breaks of the group $\langle\gamma\rangle$ are the breaks $\langle b^{(0)}, \cdots, b^{(n-1)}\rangle$ of $\mathbf{X}_\gamma$.*

For the case that we are most interested in, where the Galois group is cyclic and $(G\colon G_{b_j}) = p^j$, we have the relatively simple relation of Formula 4 connecting the depths of the successive p-power iterates of the torsion element u of $\mathfrak{N}_\kappa$ to the breaks of the associated character. In

particular, for the minimally ramified case where $b^{(j)} = p^j$, the corresponding torsion series u has $\delta\big(u^{\circ p^j}\big) = \big(p^{2j+1}+1\big)/(p+1)$.

4. *Klopsch's Theorem*

Recall that the theorem from [**5**] that has prompted this paper, namely Proposition 3.3 there, states that the conjugacy classes of p-torsion elements of $\mathfrak{N}_\kappa$ of depth m are represented by the series that I called $j_{m,a}(x) \in \kappa[\![x]\!]$ in Section 1. Since these are indexed by the nonzero elements of κ, an equivalent way of stating Klopsch's Theorem is to say that there are precisely $|\kappa|-1$ strict equivalence classes of continuous characters χ defined on $1+t\kappa[\![t]\!]$ and onto $\mathbb{Z}/p\mathbb{Z}$. That the two statements are equivalent follows from Theorem 2.2, Observation 8, and Proposition 3.2.

4.1. *The proof*

Our proof here of Klopsch's Theorem is Theorem 4.2 below, and we prepare the ground with the computational Lemma 4.1.

We call $\kappa(\!(t)\!) = F$, as usual, and note that for a character χ to have its break sequence simply $\langle m\rangle$ means precisely that χ is trivial on $1+\mathfrak{M}_F^{m+1}$ but not on $1+\mathfrak{M}_F^m$, and that thus χ restricts to a nonzero linear function $\widetilde{\chi}$ on the κ-one-dimensional space $\big(1+\mathfrak{M}^m\big)\big/\big(1+\mathfrak{M}^{m+1}\big)$. Note also that for any $u \in \mathfrak{N}_\kappa$, $\widetilde{{}_u\chi} = \widetilde{\chi}$.

LEMMA 4.1. *Let χ and ψ be characters on $1+\mathfrak{M}_F$, both with break sequence $\langle m\rangle$. Then there is $u \in \mathfrak{N}_\kappa$ with $\psi = {}_u\chi$ if and only if $\widetilde{\chi} = \widetilde{\psi}$.*

Proof. Let us suppose first that $\widetilde{\chi} = \widetilde{\psi}$. Our hypotheses imply that χ and ψ agree on $1+\mathfrak{M}^m$. We will need to use the nondegeneracy of the trace pairing, which implies that if $\sigma\colon \kappa \to \mathbb{F}_p$ is $\mathbb{F}_p$-linear, there is a unique $a \in k$ such that for every $\lambda \in \kappa$, $\sigma(\lambda) = \mathrm{Tr}(a\lambda)$, where Tr is the field-theoretic trace from κ to $\mathbb{F}_p$. We may use the series $1+t^m$ as the basis element for the one-dimensional κ-space $\big(1+\mathfrak{M}^m\big)\big/\big(1+\mathfrak{M}^{m+1}\big)$, and we now let $a \in \kappa$ be such that for every $\lambda \in \kappa$, $\chi(1+\lambda t^m) = \psi(1+\lambda t^m) = \mathrm{Tr}(a\lambda)$. Let us show inductively, starting with $n=0$, that there is $u_n(t) \in \mathfrak{N}_\kappa$ with $\chi_n := {}_{u_n}\chi$ and ψ agreeing on $1+\mathfrak{M}^{m-n}$; we take $u_0(t) = t$, the identity element of $\mathfrak{N}_\kappa$. Now, in case $m-n-1$ is a multiple of p, it must be that no matter what λ is in κ, $\chi_n(1+\lambda t^{m-n-1}) = 0$, since χ_n is being evaluated at a p-th power. So in this case, we may accomplish the inductive step by taking $u_{n+1} = u_n$, $\chi_{n+1} = \chi_n$. In the general case that $m-n-1$ is not a multiple of p, set $U(t) = t + \beta t^{n+2}$, for $\beta \in \kappa$ to be determined. For $j \geq m-n$, $(1+\lambda t^j)\circ U(t) \equiv 1+\lambda t^j \bmod (t^{m+1})$, so that for these values of j, ${}_U(\chi_n)$ and ψ agree when evaluated at $1+\lambda t^j$. Thus we need only adjust β so that for all λ, ${}_U\chi_m(1+\lambda t^{m-n-1}) = 0$. Now, since χ_s and ψ agree on $1+\mathfrak{M}^{m-n}$, the character $\chi_s - \psi$ induces a linear map from $\big(1+\mathfrak{M}^{m-n-1}\big)\big/\big(1+\mathfrak{M}^{m-n}\big)$ to $\mathbb{F}_p$, so there is $c \in \kappa$ such that for all λ, $\big(\chi_n - \psi\big)(1+\lambda t^{m-n-1}) = \mathrm{Tr}(c\lambda)$. Now we have

$$\begin{aligned}
\big({}_U(\chi_n)\big)(1+\lambda t^{m-n-1}) &= \chi_n\big[1+\lambda(t+\beta t^{n+2})^{m-n-1}\big] \\
&= \chi_n\big[1+\lambda(t^{m-n-1}+(m-n-1)\beta t^m)\big] \\
&= \chi_n(1+\lambda t^{m-n-1}) + \chi_n\big(1+\lambda(m-n-1)\beta t^m\big) \\
&= \psi(1+\lambda t^{m-n-1}) + \mathrm{Tr}(c\lambda) + \mathrm{Tr}\big((m-n-1)a\beta\lambda\big)\,,
\end{aligned}$$

which necessitates $c + (m-n-1)a\beta = 0$, possible because a and $m-n-1$ both are nonzero in κ. Consequently, we take $u_{n+1} = U \circ u_n$, and $\psi_{n+1} = {}_U(\psi_n)$ to complete the induction and the "if" part of the Lemma. The "only if" statement is much easier. Indeed, suppose that

${}_u\chi = \psi$ for $u(t) = xg(t) \in \mathfrak{N}_\kappa$, and therefore $\big(g(t)\big)^m = 1 + \mu t + \cdots$. Then

$$\psi(1+\lambda t^m) = \chi(1+\lambda u^m) = \chi(1+\lambda t^m + \lambda\mu t^{m+1} + \cdots) = \chi(1+\lambda t^m)\,,$$

so that $\widetilde{\psi} = \widetilde{\chi}$.

THEOREM 4.2. *Let χ and ψ be continuous characters from $1 + t\kappa[\![t]\!]$ onto $\mathbb{Z}/p\mathbb{Z}$, and with their unique break at m. Then $\chi \simeq \psi$ if and only if $\widetilde{\chi} = \widetilde{\psi}$.*

Proof. There are only $|\kappa| - 1$ linear functions $\widetilde{\chi}$ because each of them is of the form $1 + \lambda t^m \mapsto \mathrm{Tr}(a\lambda)$ for an $a \in \kappa^*$ that is determined by $\widetilde{\chi}$. If now $\widetilde{\chi} = \widetilde{\psi}$, we know from Lemma 4.1 that there's a $u(t) \in \mathfrak{N}_\kappa$ such that $\psi = {}_u\chi$, but it remains to adjust this u to a $\bar{u}$ such that $\psi = {}_{\bar{u}}\chi$ and $\bar{u}(t)/t \in \ker(\chi)$. Consider $\chi\big(u(t)/t\big) = \nu \in \mathbb{F}_p$. Because $\widetilde{\chi} \neq 0$, there is $c \in \kappa$ such that $\chi(1 + ct^m) = -\nu$. Now we simply set $\bar{u}(t) = (1 + ct^m)u(t)$, which certainly satisfies the second condition on $\bar{u}$ above; and since $u(t)$ and $\bar{u}(t)$ are congruent modulo (t^{m+1}), the first condition is satisfied as well.

The converse follows from the easy half of Lemma 4.1.

4.2. *Connecting the present approach with Klopsch's*

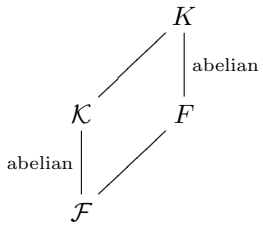
Let us call $\omega_b \colon \kappa \to \mathbb{F}_p$ the linear map $\lambda \mapsto \mathrm{Tr}(\lambda/b)$. It is still incumbent on us to see which series $j_{m,a}$ is conjugate to an element of $\mathfrak{N}_\kappa$ that comes, via the standard procedure, from a character $\chi \colon 1 + \mathfrak{M}_F \to \mathbb{F}_p$ with ramification data $\langle m \rangle$, and for which $\widetilde{\chi} = \omega_b$. The answer is that $a = b^{1/p}$, and the proof comes from an explicit description of the class field theory of a ramified cyclic extension of degree p to be found in [**7**]. It is Proposition 5 in § 3 of Chapter XV. I quote it here, with only light rephrasing.

PROPOSITION 4.3. *Let K/F be a cyclic, totally ramified extension of degree p equal to the characteristic of F; let G be its Galois group, and s a generator of G. Let π be a uniformizer of K, and let $m = v_K(M)$, where $M = (\pi^s/\pi) - 1$. Let $x \in 1 + {\mathfrak{M}_F}^m$, and let $c(z) = (z - 1)/\mathrm{Tr}_F^K(M)$. Then $c(z) \in \mathcal{O}_F$, and if $\bar{c}$ denotes its image in the residue field κ, one has $\rho_F^K(z) = s^{\mathrm{Tr}(\bar{c})}$.*

The trace map mentioned at the very end is the κ-over-$\mathbb{F}_p$ trace, as has been the established notation for this paper. The Proposition in [**7**] makes use of a "super-trace" that's definable for any quasifinite field κ, but in our case Serre's function boils down to the ordinary trace.

Although in principle the above Proposition could be used for a direct proof of the desired result, it seems most efficient to use it only for the case where the unique break is at $m = 1$, and use another result in local class field theory, also standard but more general, to get the general case. This is the Norm Relation, extractable from Property (1) of § 3, Chapter XI of [**7**]. It says that if $K \supset \mathcal{F}$ is a finite extension of local fields, and $\mathcal{K}$ and F are intermediate fields with K abelian over F and $\mathcal{K}$ abelian over $\mathcal{F}$, then for $z \in \mathcal{K}$ and $\alpha \in F^*$, the relation $\big(\rho_F^K(\alpha)\big)(z) = \big\{\rho_{\mathcal{F}}^{\mathcal{K}}\big(\mathcal{N}_{\mathcal{F}}^F(\alpha)\big)\big\}(z)$ holds: as seen in the diagram below, restriction of elements of

$\mathrm{Gal}(K/F)$ to $\mathcal{K}$ corresponds to taking the norm from F to $\mathcal{F}$.



THEOREM 4.4. *Let $a \in \kappa$, and let $u(x) = j_{m,a}(x) = x/(1+max^m)^{1/m}$. Let $K = \kappa(\!(x)\!)$ and $F = \kappa(\!(t)\!)$, where $t = \prod_{i=0}^{p-1} u^{\circ i}(x)$. Then the associated character $\chi\colon 1+\mathfrak{M}_F \to \mathbb{Z}/p\mathbb{Z}$ has $\widetilde{\chi}(\lambda) = \mathrm{Tr}(\lambda/a^p)$ for all $\lambda \in \kappa$.*

Proof. Remember that since χ has $\langle m \rangle$ for its unique break, we need to show that $\chi(1+\lambda t^m) = \mathrm{Tr}(\lambda/a^p)$, in other words that $\rho_F^K(1+\lambda t^m)$ acts on x to give $u^{\circ n}(x)$, where $n = \mathrm{Tr}(\lambda/a^p)$.

First, we prove the Theorem in the case that $m = 1$. Since t expands as $x^p/(1-a^{p-1}x^{p-1})$, the minimal polynomial for x over F is $x^p + a^{p-1}tx^{p-1} - t$, and $\mathrm{Tr}_F^K(x) = -a^{p-1}t$. So, in Proposition 4.3, we have the dictionary: s is the automorphism induced by u, $\pi = x$, $m = 1$, $M = -1 + u(x)/x = -au(x)$, and $\mathrm{Tr}_F^K(M) = -a\mathrm{Tr}_F^K(x) = a^p t$. If $z = 1+\lambda t$, then $\rho_F^K(z) = u^{\circ n}(x)$, where $n = \mathrm{Tr}(\lambda/a^p) \in \mathbb{F}_p$, as desired.

For the case of general m, we form the subfield $\mathcal{K} = \kappa(\!(\xi)\!)$ of K, where $\xi = x^m$, and note that the automorphism of K induced by the power series $u(x)$ restricts to $\mathcal{K}$ to send ξ to $w(\xi) = \xi/(1+ma\xi)$: in other words, as series, $u = \mathrm{Disp}_m(w)$. We put $\tau = \prod_i w^{\circ i}(\xi)$, so that $\tau = t^m$ as well, and we set $\mathcal{F} = \kappa(\!(\tau)\!)$.

Say that $\rho_F^K(1+\lambda t^m)$ acts on x to give $u^{\circ n}(x)$. Then by the construction of w it acts on ξ to give $w^{\circ n}(\xi)$, and by the Norm Relation, it acts on ξ by application of $\sigma = \rho_{\mathcal{F}}^{\mathcal{K}}\big(\mathcal{N}_{\mathcal{F}}^F(1+\lambda t^m)\big)$. But $\mathcal{N}_{\mathcal{F}}^F(1+\lambda t^m) = (1+\lambda\tau)^m$, which is congruent modulo $\mathfrak{M}_{\mathcal{F}}{}^2$ to $1+m\lambda\tau$. Then the case where $m = 1$ applies to tell us that $\xi^\sigma = w^{\circ\nu}(\xi)$ where $\nu = \mathrm{Tr}(m\lambda/m^p a^p)$, so that $n = \mathrm{Tr}(\lambda/a^p)$, as claimed.

5. *Explicit computations*

In this section, we will see how the explicit description of the norm residue mapping, first described in work of Carlitz from the 1930's (for example [**1**], [**2**], [**3**]), can be used to calculate as many terms as one might like of the torsion series in $\mathfrak{N}_\kappa$ corresponding to a given continuous character on $1 + t\kappa[\![t]\!]$. Rather than go back to Carlitz, however, I will use the techniques and notation from [**6**], explaining these as rapidly as I can before working out any examples.

5.1. *Explicit local class field theory*

We work with a finite field $\kappa \cong \mathbb{F}_q$, and a local field $F = \kappa(\!(t)\!)$, where t is an indeterminate. We fix a polynomial $f(X) = tX + X^q$, and note (Lemma 1 of [**6**]) that for every $z \in \mathcal{O} = \kappa[\![t]\!]$, there is a unique series $[z](X) \in \mathcal{O}[\![X]\!]$ that satisfies the condition $[z]'(0) = z$ and that commutes with f: $[z]\big(f(X)\big) = f\big([z](X)\big)$. In fact, if $z = \sum_i c_i t^i$, where the coefficients c_i are in κ, then $[z](X) = \sum_i c_i f^{\circ i}(X)$, where as usual the exponent on f denotes i-fold iteration. In particular, for $c \in \kappa$, $[c](X) = cX$, and $[t^n] = f^{\circ n}$. One calculates easily that $[t^2](X)$ expands out to $t^2X + (t+t^q)X^q + X^{q^2}$, and the reader may find it instructive to work out what $[t^3](X)$ is, as well.

The merit of the polynomials $[t^m](X)$ is this:

PROPOSITION 5.1. *The field $\mathcal{F}_t$ gotten by adjoining all roots of all $[t^m]$ to F enjoys the following properties:*

1. *The extension $\mathcal{F}_t \supset F$ is abelian and totally ramified; and among all abelian totally ramified extensions of F, $\mathcal{F}_t$ is maximal.*
2. *The uniformizer t is a norm from every finite extension $K \supset F$ contained in $\mathcal{F}_t$, and no other uniformizer of F has this property.*
3. *If $\mathcal{U}$ is the maximal unramified extension of F in an algebraic closure of $\mathcal{F}_t$, then $\mathcal{F}_t\mathcal{U}$ is the maximal abelian extension of F.*
4. *Let $n \geq 1$. The abelian extension F_n of F for which $\mathcal{N}_F^{F_n}(F_n^*) = \langle t \rangle \cdot (1 + \mathfrak{M}_F^n)$ is the field gotten by adjoining all the roots of $[t^i]$ for $i \leq n$, equivalently all the roots of $[t^n]$, equivalently one root of the F-Eisenstein polynomial $[t^n]/[t^{n-1}] = f^{\circ n}(X)/f^{\circ(n-1)}(X)$, where $f^{\circ 0}(X)$ is understood to be X.*
5. *Furthermore, $\mathrm{Gal}(F_n/F) \cong \mathcal{O}^*/(1+\mathfrak{M}^n)$. It is also the case that for $z \in \mathcal{O}^*$, $\rho_F^{F_n}(z)$ sends any root ζ of $[t^n]$ to $[z^{-1}](\zeta)$, $\rho_F^{F_n}$ being the the norm residue mapping.*

These properties may be found in [**6**], mostly in Theorems 2 and 3 there. The extension $F_n \supset F$ has a tame degree of $q-1$, thus is not totally wildly ramified unless $q = 2$. It may be worthwhile to observe that the breakpoints $(b_i, b^{(i)})$, for $0 \leq i < n$, are $b_i = q^i - 1$, $b^{(i)} = i$.

5.2. *How to proceed*

With the facts from Proposition 5.1, we can build torsion elements of Nottingham. Take a continuous character $\chi\colon 1 + t\kappa[\![t]\!] \to \mathbb{Z}/p^m\mathbb{Z}$, and assume χ surjective, so that it is of order p^m. If the breaks of χ are $\langle b^{(0)}, \cdots, b^{(m-1)} \rangle$, set $n = b^{(m-1)} + 1$. Then $1 + \mathfrak{M}^n = 1 + t^n\kappa[\![t]\!]$ is the largest subgroup of this shape contained in $\ker(\chi)$, i.e. n is the smallest integer for which $\mathrm{Im}(\chi)$ appears naturally as a quotient of $\mathcal{O}^*/(1+\mathfrak{M}^n)$. We extend χ to be a character on $\mathcal{O}^*$ by setting it to be zero on κ^* (necessary, because $|\kappa^*|$ is prime to p); this gives an intermediate field K between F and F_n, namely the fixed field of $\ker(\chi)$, as in Diagram 5 below:

$$\begin{array}{ccc} & F_n & \\ & \diagup \;\big|\; & \\ & \diagup \;\big|\; & \ker(\chi) \\ \mathcal{O}^*/(1+\mathfrak{M}^n) & \big| \quad K & \\ & \diagdown \;\big|\; & \\ & \diagdown \;\big|\; & \mathbb{Z}/p^m\mathbb{Z} \\ & F & \end{array} \tag{5}$$

We have $\mathrm{Gal}(K/F) \cong \mathbb{Z}/p^n\mathbb{Z}$, with K being a local field, say $K = \kappa(\!(x)\!)$ for some uniformizer x of K. And the automorphism of K that we seek is the restriction to K of the automorphism of F_n corresponding to $\chi^{-1}(1)$ via the norm residue mapping.

The recipe for doing this consists of the following steps:

(1) Get a uniformizer y for F_n, in fact y must be a root of $f^{\circ n}/f^{\circ(n-1)}$, which may also be seen as $g \circ f^{\circ(n-1)}$, where $g(X) = f(X)/X = t + x^{q-1}$. Then express $t \in F$ as a power series in y, $t = G(y)$. The initial degree of G will be $(q-1)q^{n-1} = [F_n\colon F]$. This series will be calculated up to a degree N that is suitably large. This may look like a daunting computational task, but if we consider the relation $t + \left(f^{\circ(n-1)}(y)\right)^{q-1} = 0$ as a polynomial equation in $\kappa[\![y]\!][t]$ for which we seek a root in $\kappa[\![y]\!]$, then we see that the derivative is a unit in $\kappa[\![y]\!]$, and Newton's method can be utilized. In fact, in the example in §5.3 below, only six iterations were needed to get accuracy modulo (y^{1601}).

(2) Choose $z \in \kappa[t] \cap 1 + \mathfrak{M}_F$ for which $\chi(z) = -1$ (to take account of the exponent in rule (5) of Proposition 5.1), and expand $[z](X) \in \kappa[t][X]$. It will be a polynomial, not an infinite series. Then make the substitution $t \mapsto G(y)$, $X \mapsto y$, to get an invertible series in y, say $U(y)$, which in fact will be a torsion element of Nottingham, valid up to degree N.

(3) List the elements of $\ker(\chi)$ modulo $1 + \mathfrak{M}^n$, there will be $(q-1)q^{n-1}/p^m$ of them, call this number s, and say that the list is $\{1 = a_0, a_1, \cdots, a_{s-1}\}$. Then write $\prod_i [a_i](X)$, again a polynomial in t and X, and again substitute $G(y)$ for t, y for X, to get $\mathcal{N}(y)$, a power series in y that in fact is the norm of y down to K. As a power series in y, its initial degree is s.

(4) Call $\mathcal{N}(y) = x \in K$. The automorphism of F_n described by U restricts to an automorphism of K, taking x to $u(x) \in \kappa[\![x]\!]$. This is the desired element of Nottingham, and as a power series, it satisfies the relation $u \circ \mathcal{N} = \mathcal{N} \circ U$. Notice that since $\mathcal{N}$ is not an invertible series, it is not routine to find u from the data of $\mathcal{N}$ and U. I should also point out at this stage that the final product u is now known only up to degree N/s.

5.3. *An example*

As an example, let us construct an element of period 8 in characteristic two that's a little more interesting than a minimally ramified one. Take the ramification data $\langle 1, 3, 6\rangle$, with the constant field $\kappa = \mathbb{F}_2$, and let F be $\kappa(\!(t)\!)$, with the character $\chi\colon 1 + \mathfrak{M}_F \to \mathbb{Z}/8\mathbb{Z}$ the one for which $\chi(1+t) = -1$, $\chi(1+t^3) = 2$, and $\chi(1+t^5) = 0$. Since χ will vanish on $1 + \mathfrak{M}_F^7$, the number n in the recipe in the previous section is 7, $[F_7\colon F] = 64$, and $s = 8$.

If we want accuracy in our explicitly computed torsion series u to be 200, we need to do our computations in $F_7 = \kappa(\!(y)\!)$ to degree 1600. The first thing to compute is the expression for t in terms of the uniformizer y of F_7. In the notation of §5.2, $f(X) = tX + X^2$, and we need to use the relation $t + f^{\circ 6}(y) = 0$ to get an expression $t = G(y)$, and what we get is

$$t \equiv G(y) = y^{64} + y^{96} + y^{128} + \cdots + y^{1593} + y^{1594} + y^{1596} \bmod (y^{1601})\,.$$

Next step is to list the elements of $\ker(\chi)$ as a homomorphism defined on $(1 + \mathfrak{M}_F)/(1 + \mathfrak{M}_F^7)$. The kernel is of order eight, generated by $(1+t^2)(1+t^3)$ and $1+t^5$. These eight elements must be expanded as described in the previous section, and then the eight are to be multiplied together to give a series for $\mathcal{N}(y) = x$. We get

$$x = \mathcal{N}(y) \equiv y^8 + y^{20} + y^{36} + \cdots + y^{1594} + y^{1596} + y^{1599} \bmod (y^{1601})\,.$$

The series $\mathcal{N} \circ U$ may be computed simply by composition of power series, but I found that it was much more direct to list the elements of the coset $(1+t)\ker(\chi)$, expand and multiply the eight results, just as $\mathcal{N}(y)$ was calculated immediately above. In any event, the result is

$$(\mathcal{N} \circ U)(y) \equiv y^8 + y^{16} + y^{20} + \cdots + y^{1593} + y^{1599} + y^{1600} \bmod (y^{1601})\,.$$

From the givens of $\mathcal{N}$ and $\mathcal{N} \circ U$, getting the unique u such the $u \circ \mathcal{N} = \mathcal{N} \circ U$ is most likely not available as a preexisting routine in a computation package, but is easily programmed and presents no problem. In our specific case, we get $u = u_{100} + u_{200}$, where

$$\begin{aligned} u_{100}(x) = {} & x + x^2 + x^3 + x^5 + x^8 + x^{11} + x^{13} + x^{14} + x^{16} + x^{17} + x^{18} + x^{19} + x^{20} \\ & + x^{21} + x^{24} + x^{26} + x^{27} + x^{29} + x^{30} + x^{31} + x^{33} + x^{34} + x^{35} + x^{36} + x^{37} + x^{39} \\ & + x^{42} + x^{44} + x^{45} + x^{47} + x^{48} + x^{49} + x^{51} + x^{52} + x^{55} + x^{58} + x^{59} \\ & + x^{63} + x^{65} + x^{68} + x^{71} + x^{72} + x^{73} + x^{76} + x^{78} \\ & + x^{81} + x^{82} + x^{83} + x^{84} + x^{85} + x^{86} + x^{89} + x^{90} + x^{92} + x^{93} + x^{95} + x^{96} + x^{100}\,, \end{aligned}$$

and

$$\begin{aligned} u_{200}(x) = {} & x^{104} + x^{106} + x^{109} + x^{110} + x^{113} + x^{114} + x^{115} + x^{116} + x^{117} + x^{118} + x^{120} \\ & + x^{122} + x^{123} + x^{124} + x^{125} + x^{127} + x^{129} + x^{135} + x^{136} + x^{139} \\ & + x^{141} + x^{144} + x^{145} + x^{146} + x^{147} + x^{148} + x^{153} + x^{157} + x^{158} \\ & + x^{162} + x^{165} + x^{166} + x^{167} + x^{168} + x^{169} + x^{171} + x^{172} + x^{175} + x^{176} + x^{180} \\ & + x^{184} + x^{185} + x^{189} + x^{190} + x^{194} + x^{195} + x^{197} + x^{199} + x^{200}\,, \end{aligned}$$

and I leave it to the reader to check not only that the depths of $u^{\circ 2}$ and $u^{\circ 4}$ are 5 and 17 respectively, as predicted, but also that $u^{\circ 8}(x) \equiv x \bmod (x^{201})$.

References

1. L. Carlitz, 'The arithmetic of polynomials in a finite field', *American J. Math.* 54 (1932) 39–50.
2. L. Carlitz, 'The arithmetic of polynomials in a finite field', *Duke Math. J.* 1 (1935) 137–168.
3. L. Carlitz, 'The arithmetic of polynomials in a finite field', *Trans. American Soc.* 43 (1938) 167–182.
4. M. Hazewinkel, *Formal groups and applications* (Academic Press, New York, 1978) No. 78 in the series Pure and Applied Mathematics
5. B. Klopsch, 'Automorphisms of the Nottingham group', *J. Algebra* 223 (2000) 37–56.
6. J. Lubin and J. Tate, 'Formal complex multiplication in local fields', *Ann. Math.* 81 (1965) 380–387.
7. J-P. Serre, *Corps locaux* (Hermann, Paris, 1965).
8. J-P. Serre, *Local fields* (Springer, New York, 1979). Translation of the preceding by M. J. Greenberg.

Jonathan Lubin
Mathematics Department, Box 1917
Brown University
Providence, RI 02912-1917
USA

lubinj@math.brown.edu