TORSION ELEMENTS OF THE NOTTINGHAM GROUP OF ORDER $p^2$ AND TYPE $\langle 2, m \rangle$

KRISHNA KISHORE

Abstract. We classify torsion elements of order $p^2$ and type $\langle 2, m \rangle$ in the Nottingham group defined over a prime field of characteristic $p > 0$.

1. Introduction

Let $p$ be a prime number, and $\mathbb{F}_p$ the prime field of characteristic $p$. Let $K := \mathbb{F}_p((t))$ be the field of Laurent-series in one variable $t$ over $\mathbb{F}_p$, and $\mathcal{O}_K := \mathbb{F}_p[t]$ its ring of integers. Let $U_1 := 1 + t\mathcal{O}_K$ be the group of principal units, and $U_k = 1 + t^k\mathcal{O}_K$, $k \geq 2$, be its higher unit subgroups. Consider the group $\text{Aut}(K)$ of automorphisms of $K$, and the subgroup $\text{Aut}^1(K)$ consisting of wild automorphisms of $K$, namely those which maps the uniformizer $t$ to the product $tz$ for some $z \in U_1$. The set $\{tz : z \in U_1\}$, corresponding to $\text{Aut}^1(K)$, equipped with composition of power series is a group, called the Nottingham group $\mathcal{N}$ over $\mathbb{F}_p$. [Je].

It is well-known that the Nottingham group $\mathcal{N}$, equipped with profinite topology, contains every countably based pro-$p$-groups as closed subgroups [Ca], whence interest in its study, as it offers a good model to test conjectures on pro-$p$-groups. The classification of elements of order $p$ in the Nottingham group defined over any finite field $\kappa$ is due to Klopsch [Kl], according to which they are classified in two steps. First, according to the depth, which may be any positive integer $d$ prime to $p$; second, when $d$ is given, these are only $|\kappa| - 1$ conjugacy classes, described by the coefficient of the series in degree $d + 1$. On the other hand, Lubin gave a different proof for the theorem of Klopsch using a different framework, namely that of associating characters $U_1 \to \mathbb{Z}/p^n\mathbb{Z}$ to conjugacy class of torsion elements in $\mathcal{N}$ and order $p^n$. The setup allows one to compute torsion elements of order $p^n$ for any integer $n \geq 1$.

2000 Mathematics Subject Classification. 11S31 (primary), 37P35, 20D15, 20E18 (secondary).

Key words and phrases. local class field theory, Nottingham group, torsion elements, ramification sequence.

This work was supported by Science and Engineering Research Board, Government of India [SERB-PDF/2016/004056].
In this paper we use this setup for the analysis of break sequences of strict equivalence classes. To state our main results, we now introduce some terminology.

Consider the $\mathbb{Z}_p$-module $\text{Hom}^{\text{cont}}_{\mathbb{Z}_p}(U_1, \mathbb{Z}/p^n\mathbb{Z})$ of continuous characters $\chi : U_1 \to \mathbb{Z}/p^n\mathbb{Z}$ on which the group $\mathfrak{N}$ acts on the right in a compatible manner with $\mathbb{Z}_p$-module structure:

$$w\chi(f(t)) := \chi(f \circ w(t))$$

for $f(t) \in U_1 = 1 + t\mathbb{F}_p[t]$ and $w \in \mathfrak{N}$. Two characters $\chi, \psi$ are called strictly equivalent, denoted $\chi \simeq \psi$, if there exists an $u \in \mathfrak{N}$ such that $\psi = u\chi$ and $u(t)/t \in \ker \chi$; if the former condition holds they are said to be weakly equivalent, and denoted $\chi \sim \psi$. To any surjective character $\chi : U_1 \to \mathbb{Z}/p^n\mathbb{Z}$ there corresponds a sequence of integers $\langle b(0), \ldots b(n-1) \rangle$, called the break sequence of $\chi$ or type of $\chi$, where $b(j-1)$ is the largest positive integer $b$ such that $\chi(1 + M^b + 1) \subset p^j\mathbb{Z}/p^n\mathbb{Z}$ but $\chi(1 + M^b) \not\subset p^j\mathbb{Z}/p^n\mathbb{Z}$.

Due to the work of Lubin [Lu], the conjugacy classes of torsion elements of order $p^2$ in $\mathfrak{N}$ corresponds to strict equivalence class of surjective continuous characters. Since two strictly equivalent characters have the same break sequence, one may pass onto the analysis of break sequences. In an unpublished work, Lubin classified torsion elements of order $p^2$ of break sequence type $\langle 1, m \rangle$ over any finite field. The main goal of this paper is to classify elements of order $p^2$ of type $\langle 2, m \rangle$ over any prime finite field. The number of classes depends on $m$. In particular we show that, given an odd prime $p$, for each $m \geq 2p$ there are at least $p(p-1)$, resp. $p(p-1)^2$, resp. $(p-1)^2$ number of conjugacy classes of elements of order $p^2$ corresponding to $m \equiv 0 \pmod{p}$, resp. $m \not\equiv 0$, resp. $m \equiv 1 \pmod{p}$.

Let $E_i$ be a topological basis of the principal unit group $U_1 = 1 + \mathfrak{N}$, and $\mathfrak{z}_i$ be the basis of $\text{Hom}^{\text{cont}}_{\mathbb{Z}_p}(1 + \mathfrak{N}, \mathbb{Z}/p^2\mathbb{Z})$ dual to $E_i$. Let $\chi$ be a character of type $\langle 2, m \rangle$ with the following expansion:

$$(1.1) \quad \chi = x_1 \mathfrak{z}_1 + x_2 \mathfrak{z}_2 + \sum_{1 \leq j \leq m \atop p \not| j} a_j \cdot p \mathfrak{z}_j,$$

where all the coefficients are in $\mathbb{F}_p$ and $x_2, a_m$ are nonzero; see Lemma 3.5. As it turns out, only some of these coefficients together with a relation among them determines the character up to strict equivalence. Accordingly we collect these coefficients into indicium of the character $\chi$, denoted $\text{ind} \chi$, and defined based on $m \pmod{p}$, namely that
\[ \chi = [x_2, \frac{x_1}{x_2} - \frac{a_m^{m-1}}{(m-1)x_2^2}], \quad \psi = [x_2, a_m, \frac{x_1}{x_2} - \frac{a_m^{m-1}}{(m-1)a_m}], \]

respectively. Now we can state our main results.

**Theorem 1.1.** Let \( \chi, \psi \) be characters of order type \( \langle 2, m \rangle \). Then \( \chi \) is weakly equivalent to \( \psi \) if and only if \( \text{ind } \psi = \text{ind } \chi \).

**Theorem 1.2.** Let \( \chi, \psi \) be characters of order type \( \langle 2, m \rangle \) with standard expansions as in equation (1.1). Suppose \( \chi \) is strictly equivalent to \( \psi \), so that for some \( u = t(1 + \alpha t + \beta t^2 + \ldots) \in \mathfrak{N} \), one has \( \psi(f) = u\chi \).

Then

1. \( \text{ind } \chi = \text{ind } \psi \).
2. \( x_1\alpha + x_2\left(\beta - \binom{a}{2}\right) \equiv 0 \pmod{p} \).

Conversely, suppose \( \text{ind } \chi = \text{ind } \psi \), so that \( \chi \sim \psi \) by Theorem 1.1, i.e. \( \psi = u\chi \) for some \( u \in \mathfrak{N} \). Suppose among such \( u \in \mathfrak{N} \) there exists an \( u = t(1 + \alpha t + \beta t^2 + \ldots) \in \mathfrak{N} \) for which \( x_1\alpha + x_2\left(\beta - \binom{a}{2}\right) \equiv 0 \pmod{p} \), then \( \chi \simeq \psi \).

The proof of the theorem is briefly as follows. We choose the basis \( \{E_j := 1 + t^j\}, \ j \geq 1 \) and \( p \nmid j \), of the principal unit group \( U_1 \) and correspondingly the canonical basis \( \mathfrak{Z}_i \), dual to \( E_j \). Necessity of the conditions follow immediately upon evaluating the character at various basis elements \( E_j \). In order to prove the sufficiency condition, we use backwards induction and progressively build characters starting from \( \chi \) and at each stage we find appropriate \( u \in \mathfrak{N} \) such all the coefficients of \( u\chi \) and \( \psi \) with index \( k \) for all \( j \leq k \leq m \) are equal. The difficulty is in finding appropriate \( u \) that satisfies this criterion, so by a careful analysis of the relations among the coefficients we obtain the desired \( u \in \mathfrak{N} \).

As a consequence we have the following corollary:

**Corollary 1.3.** Let \( m \) be an integer \( \geq 2p \), where \( p \) an odd prime. For each such \( m \), let \( d_m \) denote the number of conjugacy classes of Nottingham elements of order \( p^2 \). Then,

\[
\begin{align*}
d_m & \geq \begin{cases} 
p(p-1) & \text{if } m \equiv 0 \pmod{p} \\
p(p-1)^2 & \text{if } m \equiv 1 \pmod{p} \\
p(p-1)^2 & \text{otherwise.}
\end{cases}
\end{align*}
\]

Finally, we refer the reader to an elegantly written article about Nottingham group by Sautoy and Fesenko [DF]. Also the reader may refer to a paper of Chinburg and Symonds, where in, the authors have computed an element of order 4 in the Nottingham group at the prime 2.
The outline of the paper is as follows. In §2 we explain the notation and conventions used in this paper. In §3 we describe Lubin’s framework which will be used later to classify torsion elements of order \( p^2 \); for more details of the approach, we recommend Lubin’s work in [Lu]. In §4 we discuss the topological structure of the principal unit group \( U_1 \) and a lemma of Lubin. In §5 we prove several computational lemmas that describe relations among the coefficients of the characters which are essential in §6 where we prove the main results of the paper, Theorem 1.1 and Theorem 1.2. In §7 we describe the limitations of the results of the paper, and the various generalities possible.

2. Notation and conventions

We adapt the following notation in this paper. The letter \( p \) always denotes a prime number, and \( \mathbb{F}_p \) the prime field of characteristic \( p > 0 \). By \( K \) we mean the field of Laurent-series \( \mathbb{F}_p((t)) \) over \( \mathbb{F}_p \), and \( \mathcal{O}_K := \mathbb{F}_p[[t]] \) its ring of integers with maximal ideal \( \mathfrak{M} = t\mathcal{O}_K \) where \( t \) is a fixed uniformizer of \( \mathcal{O}_K \). Then the group of principal units \( 1 + \mathfrak{M} \) is denoted by \( U_1 \), and its higher unit subgroups \( 1 + \mathfrak{M}^j, j \geq 1 \), by \( U_j \).

The Nottingham group over \( \mathbb{F}_p \) is always denoted by \( N \). The notation for strict equivalence is \( \simeq \), while that for weak equivalence is \( \sim \). Thus \( \chi \simeq \psi \) means that \( \chi \) and \( \psi \) are strictly equivalent, while \( \chi \sim \psi \) means that they are weakly equivalent.

The notation \( \binom{n}{k} \) for integers \( n, k > 0 \) is the usual combinatorial one. More importantly we write \( \binom{\alpha}{k} \) for \( \alpha \in \mathbb{F}_p \), to mean any \( \binom{n}{k} \) for \( n \equiv \alpha \pmod{p} \).

In this paper, we deal only with continuous characters \( \chi : U_1 \to \mathbb{Z}/p^n\mathbb{Z} \), with \( U_1 \) equipped with induced topology from that of topological group \( K^\times \), and \( \mathbb{Z}/p^n\mathbb{Z} \) with the discrete topology. So we omit the adjective ‘continuous’ while referring to the characters in the \( \mathbb{Z}_p \)-module \( \text{Hom}_{\mathbb{Z}_p}^{\text{cont}}(U_1, \mathbb{Z}/p^n\mathbb{Z}) \).

3. Lubin’s framework

3.1. Description of Lubin’s setup. In this section we describe Lubin’s framework to compute torsion elements of order \( p^n \) (in the Nottingham group \( \mathfrak{M} \)); for more details the reader may consult §2 of [Lu].

First, we describe how to associate a torsion element \( \gamma \in \mathfrak{M} \) of order \( p^n \) with a finite abelian extension \( K \supset \mathbb{F}_p((t)) \) with Galois group isomorphic to \( \mathbb{Z}/p^n\mathbb{Z} \) (where, recall, \( K = \mathbb{F}_p((t)) \) as in [2]). Given a torsion element \( \gamma \in \mathfrak{M} \) of order \( p^n \), considered as an element of \( \text{Aut}(K) \), let \( F \) denote...
be its fixed field in $K$. Then $K \supset F$ is a finite abelian extension with Galois group $\Gamma$ isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$. By the local class-field theory we have an exact sequence

$$K^* \xrightarrow{N_K^F} F^* \xrightarrow{\rho_K^F} \Gamma \to 1$$

such that the image of the norm map $N_K^F$ is an open subgroup in $F^*$, and for any open subgroup $U$ of finite index in $F^*$ there is a canonical abelian extension $L \subset F$ such that $N_L^F(L^*) = U$. Thus, with the aid of norm residue symbol $\rho_K^F$ we can obtain a character $X_\gamma : F^* \to \mathbb{Z}/p^n\mathbb{Z}$, via the canonical isomorphism $\Gamma \to \mathbb{Z}/p^n\mathbb{Z}$ sending the generator $\gamma$ to 1, and hence a character $U_1 \to \mathbb{Z}/p^n\mathbb{Z}$ by restriction; the latter character on $U_1$ is again denoted by $X_\gamma$, abusing notation.

Conversely, given a surjective continuous character $X : U_1 \to \mathbb{Z}/p^n\mathbb{Z}$, we construct a cyclic extension $L \supset K$ and a generator $\gamma$ of the Galois group $\text{Gal}(L/K)$ of order $p^n$. Given such a character $X$, clearly it has a unique extension to $\mathcal{O}_L^*$ and then to $K^*$ by letting to be 0 at $t$. Thus we obtain a continuous surjective character $\widetilde{X} : K^* \to \mathbb{Z}/p^n\mathbb{Z}$ with the kernel generated by $t, \ker(X)$, and $\kappa^*$ (the subgroup $\kappa^*$ is contained in the kernel because its order is $p-1$ which is relatively prime to $p^n$.) The kernel is clearly an open subgroup and hence, by the existence part of local class-field theory, there is a finite abelian extension $L \supset K$, unique up to isomorphism, with Galois group isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$ such that the image of $L^*$ under the norm map $N_L^K$ is $\ker(\widetilde{X})$. Furthermore, we have an exact sequence

$$L^* \xrightarrow{N_L^K} K^* \xrightarrow{\rho_L^K} \text{Gal}(L/K) \xrightarrow{} 1$$

The generator $\gamma$ of $\text{Gal}(L/K)$ is obtained by $\gamma := \rho_L^K \circ \widetilde{X}^{-1}(1)$.

Let us note here that the description of $\gamma \in \mathfrak{N}$ in terms of power series $u(t)$ depends on the choice of the uniformizer $t$, but, the conjugacy class of $u(t)$ in $\mathfrak{N}$ does not provided $N_L^K(x) = t$ for a choice of uniformizer $x \in \mathcal{O}_L$ (which is used to construct back $\widetilde{X}$.)

**Remark 3.1.**

(1) Note that the extensions $K/F$ and $L/K$ are totally wildly ramified, whence the terminology ‘wild’ automorphism associated to the elements of Nottingham group $\mathfrak{N}$.

(2) Let us observe that given a torsion element $\gamma$ the construction yields a subfield $F$ of $K$ such that Galois group $\text{Gal}(F/K)$ is cyclic of order $p^n$. On the other hand, given a character $X :
$U_1 \to \mathbb{Z}/p^n\mathbb{Z}$ the construction gives an extension $L$ of $K$ such that $\text{Gal}(L/K)$ is cyclic of order $p^n$.

(3) In the terminology of Lubin [Lu], the procedure by which one obtains a torsion series $u(x)$ of order $p^n$ in the Nottingham group from a continuous surjective character $U_1 \to \mathbb{Z}/p^n\mathbb{Z}$ is called the standard procedure.

The Nottingham group $\mathfrak{N}$ acts on the group of characters $U_1 \to \mathbb{Z}/p^n\mathbb{Z}$ as follows. For $w \in \mathfrak{N}$ and $\chi$ such a character, one has

$$w\chi(f(t)) := \chi(f \circ w(t))$$

for $f(t) \in U_1 = 1 + t\mathbb{F}_p[[t]]$. Hence $w(w'\chi) = ww'\chi$. Now, we impose certain equivalence relation on these group of characters, which, as it turns out, characterizes conjugacy classes of order $p^n$ elements in $\mathfrak{N}$.

**Definition 3.2.** Two characters $\chi, \psi : U_1 \to \mathbb{Z}/p^n\mathbb{Z}$ are said to be strictly equivalent, denoted $\chi \simeq \psi$, if there exists an element $w \in \mathfrak{N}$ such that $\psi = w\chi$ and $w(t)/t \in \ker(\chi)$. They are said to weakly equivalent, denoted $\chi \sim \psi$, if there exists an element $w \in \mathfrak{N}$ such that $\chi_2 = w\chi_1$.

As it turns out, strict equivalence is indeed an equivalence relation and is the right relation, in contrast to weak equivalence, one needs to impose to characterize conjugacy classes of torsion elements in the Nottingham group: [Lu, pp. 5]:

**Theorem 3.3.** (Lubin) If two elements in $\mathfrak{N}$ are conjugate (in that group), then their corresponding characters are strictly equivalent. Conversely, if two characters are strictly equivalent continuous characters of $U_1$ with values in $\mathbb{Z}/p^n\mathbb{Z}$, the torsion power series that arise from them by the standard procedure (Remark 3.1) are conjugate in $\mathfrak{N}$.

This result allows one to pass from the analysis of conjugacy classes of torsion elements of order $p^n$, to the analysis of strict equivalence continuous characters $U_1 \to \mathbb{Z}/p^n\mathbb{Z}$; the structure of the $\mathbb{Z}_p$-module of continuous characters can be stratified according to the following definition:

**Definition 3.4.** Let $\chi : U_1 \to \mathbb{Z}/p^n\mathbb{Z}$ be a surjective continuous character. The break sequence of the character $\chi$ is the tuple $\langle b(0), \ldots, b(n-1) \rangle$ where for each $j$, the number $b(j)$ is the largest integer $b$ for which there is a $z \in 1 + \mathfrak{M}^b$ such that $\chi(z) = p^j$.

**Lemma 3.5.** (Lubin) Let $\chi : U_1 \to \mathbb{Z}/p^n\mathbb{Z}$ be a surjective continuous character. Let $\langle b(0), \ldots, b(n-1) \rangle$ be its break sequence. Then the following conditions hold:
(a) \( \gcd(p, b^{(0)}) = 1 \).
(b) For each \( i > 0 \), \( b^{(i)} \geq pb^{(i-1)} \), and
(c) If the above inequality is strict, then \( \gcd(p, b^{(i)}) = 1 \).

Conversely, every sequence \( \langle b^{(0)}, \ldots, b^{(n-1)} \rangle \) satisfying the above three conditions is the break sequence of some character \( \chi \) on \( U_1 \). There are only finitely many different characters \( \chi \) with the break sequence \( \langle b^{(0)}, \ldots, b^{(n-1)} \rangle \), and a fortiori, only finitely many strict equivalence classes of such characters.

4. Topological structure of \( U_1 \) and consequences

In this section, we describe the topological structure of \( U_1 \), then analyze the structure of the \( \mathbb{Z}_p \)-module \( \text{Hom}_{\mathbb{Z}_p}(U_1, \mathbb{Z}/p^n\mathbb{Z}) \) in which the characters \( \chi : U_1 \to \mathbb{Z}/p^n\mathbb{Z} \) live. We obtain a coarse classification of the equivalence classes of strict equivalent characters which will be refined in the next section.

4.1. Topological structure of \( U_1 \). Let us begin by recalling the topological structure of the multiplicative group \( U_1 \) [Iw, Chap. 2]. The principal unit group \( U_1 \) has a \( \mathbb{Z}_p \)-module structure as follows. More generally any finite abelian \( p \)-group has a structure of a \( \mathbb{Z}/p^n\mathbb{Z} \)-module for any \( n \) sufficiently large. Indeed, the canonical isomorphism \( \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p \) together with the natural projection map \( \mathbb{Z}_p \to \mathbb{Z}_p/p^n\mathbb{Z}_p \) gives a canonical structure of \( \mathbb{Z}_p \)-module. Hence any abelian pro-\( p \)-group \( G \) has also a canonical \( \mathbb{Z}_p \)-module structure; let us recall any abelian pro-\( p \)-group is the projective limit of a family \( \{G_i\} \) of finite abelian \( p \)-groups. In particular, since \( U_1 \) is the projective limit of finite abelian \( p \)-groups \( U_1/U_n \) with respect to the canonical maps \( U_1/U_m \to U_1/U_n \) for \( m \geq n \geq 0 \), we have:

\[
U_1 = \lim_{\leftarrow n} U_1/U_n.
\]

Alternatively, we have the following topological isomorphism [Iw, Prop. 2.8]

**Proposition 4.1.** The \( \mathbb{Z}_p \)-module \( U_1 \) is topologically isomorphic to the direct product of countably infinite copies of \( \mathbb{Z}_p \). In fact,

\[
U_1 \cong \prod_{n \geq 1} (1 + t^m)\mathbb{Z}_p
\]

Let us note that the family \( \{1 + t^m\} \) is a topological basis of \( U_1 \). This basis serves well while working over a prime field of characteristic \( p > 0 \), and not so well over arbitrary finite fields. In the latter case
the basis constructed with the aid of Artin-Hasse exponential is almost mandatory; the reader may refer to [Ha, §17.5] for a full treatment of the topic.

4.2. Description of the module $\Hom_{\mathbb{Z}/p^n\mathbb{Z}}^\cont(U_1, \mathbb{Z}/p^n\mathbb{Z})$. The principal unit group $U_1$ is equipped with two actions, namely that of Nottingham group $\mathfrak{N}$ and that of $\mathbb{Z}/p$. The action of Nottingham group $\mathfrak{N}$ via $(z, u) \mapsto z \circ u$ (where the $\circ$ denotes composition of power series) for $z \in U_1$ and $u \in \mathfrak{N}$. (Recall, that if $u = t(1 + \sum_{i \geq 1} a_i t^i)$, and $z = 1 + \sum_{j \geq 1} b_j t^j$ then $z \circ u := 1 + \sum_{j \geq 1} b_j u^j$.) On the other hand, by means of exponentiation by a $p$-adic integer we have the natural action of $\mathbb{Z}/p$ on $U_1$; this action is well-defined since for $z \in U_1$ the $(t)$-adic limit of the sequence $\{z^p^n\}$ is 1. These two actions on $U_1$ are compatible, i.e. for $a \in \mathbb{Z}/p$, $u \in \mathfrak{N}$, we have

$$(z^a) \circ u = (z \circ u)^a,$$

which can be readily verified by replacing $a$ with approximation by integers $(a_n)$ for $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ converging to $a$.

From the description of $U_1$ as a $\mathbb{Z}/p$-module, it follows that we have a $\mathbb{Z}/p^n\mathbb{Z}$-module structure on $\Hom_{\mathbb{Z}/p^n\mathbb{Z}}^\cont(U_1, \mathbb{Z}/p^n\mathbb{Z})$ with basis $3_m$ dual to the basis $\{1 + t^m\}$ of $U_1$, where $m \geq 1$ and $(m, p) = 1$: with the notation $E_j := 1 + t^j$, we have $3_i(E_j) = \delta_{ij}$ where $\delta_{ij}$ is the Kronecker delta function. In other words, the set of continuous characters from $U_1 \to \mathbb{Z}/p^n\mathbb{Z}$ is the direct sum (not product) of the character groups on the factors $(1 + t^m)$ into $\mathbb{Z}/p^n\mathbb{Z}$ for $p \nmid m$. It follows that a character $\chi \in \Hom_{\mathbb{Z}/p}(U_1, \mathbb{Z}/p^n\mathbb{Z})$ has the following form

$$\chi = \sum_{j \geq 1} a_j 3_j \quad a_j \in \mathbb{Z}/p^n\mathbb{Z}.$$}

Now, let $\chi : U_1 \to \mathbb{Z}/p^n\mathbb{Z}$ be a surjective (continuous) character with break sequence $\langle b^{(0)}, \ldots, b^{(n-1)} \rangle$. From the definition of the break sequence [Def. 3.4] it follows that the kernel of $\chi$ contains $U_{b^{(n-1)}+1}$. Therefore all characters with this break sequence are in $\Hom_{\mathbb{Z}/p^n\mathbb{Z}}(U_1/U_{b^{(n-1)}+1}, \mathbb{Z}/p^n\mathbb{Z})$, which is a direct sum of cyclic $\mathbb{Z}/p^n\mathbb{Z}$-modules, one for each integer $j \leq m$ prime to $p$.

4.3. Strict equivalence condition.
Lemma 4.2. Let $\chi, \psi : U_1 \rightarrow \mathbb{Z}/p^n\mathbb{Z}$ be two continuous characters. Then $\chi$ is strictly equivalent to $\psi$ if and only if there an $u \in \mathfrak{N}$ such that $\psi = u\chi$ and $\chi(u(t)/t) \equiv 0 \pmod{p^{n-1}}$.

Proof. Necessity of the condition follows from the definition: if $u(t)/t \in \ker(\chi)$, i.e. $\chi(u(t)/t) \equiv 0 \pmod{p^n}$ then obviously $\chi(u(t)/t) \equiv 0 \pmod{p^{n-1}}$. As for the sufficiency of the condition, let $(b^{(0)}, \ldots, b^{(n-1)})$ be the break sequence of the character $\chi$. Let $m = b^{(n-1)}$. By definition, $U_{m+1} \subset \ker(\chi)$. We claim that if $z \in U_m$ and $w = tz \in \mathfrak{N}$ then $w\chi = \chi$. Indeed, evaluating at the basis elements $E_j := 1 + t^j$, we have

$$w\chi(E_j) = \chi(E_j \circ w) = \chi(1 + w^j) \equiv \chi((1 + t^j)) \pmod{U_{m+1}}$$

$$= \chi(E_j)$$

since

$$1 + w^j = 1 + t^j z' = 1 + t^j(1 + t^m z')$$

$$= 1 + t^j + t^{j+m} z' \equiv (1 + t^j)(1 + t^{m+j})z' \pmod{U_{m+1}}$$

for some $z' \in \mathcal{O}$.

Let $u \in \mathfrak{N}$ be the element given by the condition, i.e. that $\psi = u\chi$ and $\chi(u(t)/t) \equiv 0 \pmod{p^{n-1}}$. This implies, in particular, that $p^{-a-1}\chi(u(t)/t) = \lambda \in \mathbb{F}_p$. More generally, we have an $\mathbb{F}_p$-linear map

$$\overline{\chi} : \mathbb{F}_p \rightarrow \mathbb{F}_p$$

defined by $\overline{\chi}(a) = \chi(1 + at^m)/p^{n-1} \in \mathbb{F}_p$. In particular, there is an $a \in \mathbb{F}_p$ such that $\overline{\chi}(a) = \chi(1 + at^m)/p^{n-1} = -\lambda \in \mathbb{F}_p$.

Put $w(t) = t + at^{m+1} \in \mathfrak{N}$. Then $w\chi = u(w\chi) = u\chi = \psi$, so that the first condition still holds. We now calculate $\chi(u \circ w(t))/t$. Since $(u \circ w(t)) \equiv u(t) + at^{m+1} \pmod{(t^{m+2})}$, we have

$$(u \circ w(t))/t \equiv \frac{u(t)}{t} + at^{m} \equiv \frac{1}{t}u(t)(1 + at^{m}) \pmod{(t^{m+1})},$$

therefore

$$\chi((u \circ w(t))/t) \equiv \chi(u(t)/t)/p^{n-1} + \chi(1 + at^{m}) = \lambda - \lambda = 0.$$ 

Thus, $\chi((u \circ w(t))/t) \equiv 0 \pmod{p^n}$ so that, by definition, $\psi$ is strictly equivalent to $\chi$. □

---

I thank Jonathan Lubin for sharing this proof with me; the lemma and its proof appears in an unpublished paper of Lubin, that deals with torsion elements of order $p^2$ and type $(1, m)$. 
5. Structure of characters

Now we begin the classification of strict equivalent classes of type \(\langle 2, m \rangle\) corresponding to Nottingham elements of order \(p^2\). Up to conjugacy in \(N\), they correspond to strict equivalence classes of characters of type \(\langle b^{(0)}, b^{(1)} \rangle\) [Thm. 3.3]. From Lemma 3.5 it follows that \(b^{(0)}\) is prime to \(p\), and \(b^{(1)} \geq pb^{(0)}\) which, if strict, implies that \(b^{(1)}\) is prime to \(p\), otherwise \(b^{(1)} = 2p\). In this paper, we classify strict equivalence classes where \(b^{(0)} = 2\). Then since \(p \nmid b^{(0)}\), the prime \(p \neq 2\). The classification depends on whether \(b^{(1)}\) is prime to \(p\) or not, and if it is prime to \(p\) then whether it is congruent to 1 (mod \(p\)) or not. Note that there is only one case for \(m \equiv 0 \pmod{p}\), namely that \(m = 2p\); thus we have only ‘exceptional’ case \(\langle 2, 2p \rangle\). Also note that a character of certain type \(\langle b^{(0)}, b^{(1)} \rangle\) is automatically surjective by definition. So when we talk of characters ‘of type...’ we do not explicitly mention that the character is surjective. Recall that further we omit the adjective ‘continuous’, as no other kind is considered in this paper; see §2.

Consider the \(\mathbb{Z}/p^2\mathbb{Z}\)-module \(\text{Hom}^{\text{cont}}_{\mathbb{Z}/p^2\mathbb{Z}}(U_1, \mathbb{Z}/p^2\mathbb{Z})\) of characters, \(\chi : 1 + \mathfrak{N} \to \mathbb{Z}/p^2\mathbb{Z}\). For \(p \nmid j\), let \(\mathfrak{3}_j\) be the canonical basis dual to \(E_j := 1 + t^j\), i.e. \(\mathfrak{3}_j(E_i) = \delta^i_j\), the Kronecker delta function. Let \(\mathcal{A} = \{0, 1, \ldots, p^2 - 1\}\) be a fixed choice of representatives of \(\mathbb{Z}/p^2\mathbb{Z}\). Then any character \(\chi\) of type \(\langle 2, m \rangle\) has the expression of the form

\[
\chi = \sum_{1 \leq j \leq m \atop p \nmid j} a_j \mathfrak{3}_j.
\]

with the coefficients \(a_j \in \mathcal{A}\). From the definition of break sequence [Def. 3.4], it follows that

1. \(a_1 \in \mathbb{Z}/p^2\mathbb{Z}\)
2. \(a_2 \in (\mathbb{Z}/p^2\mathbb{Z})^*\)
3. For all \(3 \leq j \leq m\) such that \(p \nmid j\), the coefficient \(a_j \in \{0, p, 2p, \ldots, (p - 1)p\}\)
4. If \((m, p) = 1\), then \(a_m \neq 0\).

Writing \(a_1, a_2\) in the form \(x + p.y\) where \(x, y \in \{0, 1, \ldots, p - 1\}\), and changing the notation, the above expansion takes the following form

\[
\chi = x_1 \mathfrak{3}_1 + x_2 \mathfrak{3}_2 + \sum_{1 \leq j \leq m \atop p \nmid j} a_j.p \mathfrak{3}_j,
\]

where now \(x_1, x_2, a_1, \ldots, a_m \in \{0, 1, \ldots, p - 1\}\), and \(x_2 \neq 0\), and if \((m, p) = 1\) then \(a_m \neq 0\) too. We call this expansion of \(\chi\) as in equation standard expansion.
Let $\chi, \psi$ be two characters of type $(2, m)$ with standard expansions:

$$\chi = x_1 \beta_1 + x_2 \beta_2 + \sum_{1 \leq j \leq m} a_j \cdot p \beta_j, \quad \psi = y_1 \beta_1 + y_2 \beta_2 + \sum_{1 \leq j \leq m} b_j \cdot p \beta_j.$$  

The following lemma will be used throughout the paper; its motivation will be apparent while proving the main result.

**Lemma 5.1.** Let $\chi, \psi$ be two characters of type $(2, m)$ with standard expansions as in equation (5.1). Let $u(t) = t(1 + \alpha t + \beta t^2 + \ldots) \in \mathfrak{H}$. Then,

(a) $u \chi(E_1(t)) = x_1 + \alpha x_2 \pmod{p}$, and $u \chi(E_2(t)) = x_2 \pmod{p}$.
(b) If $p \nmid m$ then $u \chi(E_m(t)) = p a_m \pmod{p^2}$.
(c) If $m \equiv 0,1 \pmod{p}$ then $u \chi(E_{m-1}) = p (a_{m-1} + (m - 1) \alpha a_m)$ \pmod{p^2}.
(d) If $m \equiv 0 \pmod{p}$, so that $m = 2p$, then $u \chi(E_{m-1}) = p (a_{m-1} + \eta x_2)$ \pmod{p^2} where $\eta^p = (m - 1) \alpha$.

**Proof.** (a) Since $E_1 \circ u(t) = 1 + u(t) = 1 + t(1 + \alpha t + \beta t^2 + \ldots) = 1 + t + \alpha t^2 + \beta t^3 + \ldots = (1 + t)(1 + t^2)\alpha \ldots$ we have, modulo $p$,

$$u \chi(E_1(t)) = \chi(E_1 \circ u(t)) = \chi((1 + t)(1 + t^2)\alpha)$$

$$= \chi(E_1(t)) + \chi(E_2(t)) = x_1 + \alpha x_2.$$  

Similarly, the other relation is obtained by evaluating at $E_2$, and using the expansion $1 + u(t)^2 = 1 + t^2(1 + \alpha t + \beta t^2 + \ldots)^2 = 1 + t^2 + \ldots = (1 + t^2) \ldots$ Thus, modulo $p$,

$$u \chi(E_2(t)) \equiv \chi(E_2 \circ u(t)) \equiv \chi(1 + t^2) = x_2.$$  

(b) If $p \nmid m$ then, modulo $p^2$,

$$u \chi(E_m(t)) = \chi(E_m \circ u(t)) = \chi(1 + t^m) = \chi(E_m(t)) = p a_m.$$  

(c) First note that $E_{m-1} \circ u(t) = 1 + u(t)^{m-1} = 1 + t^{m-1} + (m - 1) \alpha t^m + \ldots$, then the conclusion follows by evaluating $u \chi$ at $E_{m-1}$.

(d) First observe that $1 + \alpha t^m = (1 + \eta t^2)\alpha^p$ with $\eta^p = \alpha$. Then we have

$$E_{m-1} \circ u(t) = 1 + t^{m-1} + (m - 1) \alpha t^m + \ldots$$

$$= (1 + t^{m-1})(1 + (m - 1) \alpha t^m)$$

$$= (1 + t^{m-1})(1 + \eta t^2)^p \quad \text{where } \eta^p = (m - 1) \alpha$$

$$= E_{m-1} E_2^{\eta p},$$

and therefore, modulo $p^2$,

$$u \chi(E_{m-1}(t)) = p a_{m-1} + p \eta(x_2 + p a_2)$$

$$= p (a_{m-1} + \eta x_2).$$
As noted in the introduction, only some of the coefficients in the standard expansion of characters together with a relation among them, determines the character up to strict equivalence. Accordingly we collect these coefficients into indicium of the character \( \chi \):

**Definition 5.2.** Let \( \chi \) be a character of type \( \langle 2, m \rangle \), and \( \chi = x_1 \zeta_1 + x_2 \zeta_2 + \sum_{1 \leq j \leq m} a_j p \zeta_j \) be its standard expansion. The indicium of \( \chi \), denoted \( \text{ind} \chi \), is defined as follows:

(i) If \( m \equiv 0 \pmod{p} \), so that \( m = 2p \), then

\[
\text{ind} \chi = [x_2, x_1, x_2 - \frac{a_{m-1}}{(m-1)x_2}].
\]

(ii) If \( m \not\equiv 0, 1 \pmod{p} \), then

\[
\text{ind} \chi = [x_2, a_m, x_1, x_2 - \frac{a_{m-1}}{(m-1)a_m}].
\]

(iii) If \( m \equiv 1 \pmod{p} \), then

\[
\text{ind} \chi = [x_2, a_m, 0].
\]

Let us denote the last coordinate of \( \text{ind} \chi \) by \( \text{ind}_0 \chi \).

**Lemma 5.3.** Let \( \chi, \psi \) be two characters of type \( \langle 2, m \rangle \) with standard expansions as in equation (5.1). Suppose \( \psi = u \chi \) for some \( u(t) = t(1 + \alpha t + \beta t^2 \ldots) \in \mathfrak{N} \). Then \( \text{ind}_0 u \chi = \text{ind}_0 \psi \).

**Proof.** There is nothing to show in the case where \( m \equiv 1 \pmod{p} \). Consider the case where \( m \not\equiv 0, 1 \pmod{p} \). Since

\[
E_{m-1} \circ u(t) = 1 + t^{m-1}(1 + \alpha t + \beta t^2 + \ldots) = 1 + t^{m-1} + \alpha t^m + \beta t^{m+1} + \ldots
\]

\[
= (1 + t^{m-1})(1 + t^m)^{\alpha} \ldots = E_{m-1}(t)E_m^\alpha(t)
\]

we see that, modulo \( p^2 \),

\[
\psi(E_{m-1}(t)) = u \chi(E_{m-1}(t)) = \chi(E_{m-1} \circ u(t)) = \chi(E_{m-1}(t)E_m^\alpha(t)) = p a_{m-1} + p \alpha a_m,
\]

and hence \( \alpha = b_{m-1} - a_{m-1}/(m-1)a_m \). From the relations (a), (b) of Lemma 5.1, it follows that \( a_m = b_m, y_1 = x_1 + \alpha x_2 \), and consequently
we have

\[
\frac{x_1}{x_2} - \frac{a_{m-1}}{(m-1)a_m} = \frac{x_1 - y_1}{x_2} + \frac{y_1}{x_2} - \frac{b_{m-1}}{(m-1)a_m} = \frac{b_{m-1} - a_{m-1}}{(m-1)a_m}
\]

Now consider the case \( m \equiv 0 \pmod{p} \). From Lemma 5.1 (a), and the hypothesis that \( \psi = u\chi \), it follows that \( b_{m-1} = a_{m-1} + \eta x_2 \) where \( \eta = (b_{m-1} - a_{m-1})/x_2 \) and \( \eta \equiv (m-1)\alpha \) so that \( \alpha = (b^p_{m-1} - a^p_{m-1})/(m-2)x^p_2 \). As previously, \( y_1 = x_1 + \alpha x_2 \). Equating these expressions for \( \alpha \) and rearranging the terms we obtain the desired conclusion.

\[ \Box \]

6. Classification of strict equivalence classes

In this section we prove the main result of the paper. Let us fix characters \( \chi, \psi \) of type \( \langle 2, m \rangle \) with standard expansions

\[
(6.1) \quad \chi = x_1 \overline{3}_1 + x_2 \overline{3}_2 + \sum_{1 \leq j \leq m \atop p \nmid j} a_j p \overline{3}_j, \quad \psi = y_1 \overline{3}_1 + y_2 \overline{3}_2 + \sum_{1 \leq j \leq m \atop p \nmid j} b_j p \overline{3}_j.
\]

**Theorem 6.1.** Let \( \chi, \psi \) be characters of type \( \langle 2, m \rangle \). Then \( \chi \sim \psi \) if and only if \( \text{ind} \psi = \text{ind} \chi \).

**Proof.** Let \( \chi, \psi \) have standard expansions as in equation (6.1). Necessity of the condition follows from the already established results. Indeed, from Lemma 5.1 (a) it follows that \( a_2 = b_2 \) in all cases and \( a_m = b_m \) if \( m \not\equiv 0 \pmod{p} \). The remaining equality that \( \text{ind}_0 \chi = \text{ind}_0 \psi \) follows from Lemma 5.3.

The hard part is to prove the sufficiency of the condition, namely that \( \text{ind} \chi = \text{ind} \psi \) implies \( \chi \sim \psi \). First observe that Lemma 5.1 can be applied with \( u = t(1 + \alpha t^2) \), for some \( \alpha, \beta \in \mathbb{F}_p \), since terms of degree \( \geq 4 \) in \( t \) do not affect the conclusions of the lemma. The strategy of the proof is to use backwards induction, beginning with index \( m - 1 \) in the case where \( m \not\equiv 0, 1 \pmod{p} \), with index \( m - 2 \) in the case where \( m \equiv 1 \pmod{p} \), and with index \( m - 1 \) in the case where \( m \equiv 0 \pmod{p} \).

First consider the case where \( m \not\equiv 0, 1 \pmod{p} \). By hypothesis \( \text{ind} \chi = \text{ind} \psi \), hence in particular \( a_m = b_m \). Let \( u = t(1 + \alpha t^2) \) where \( \alpha = (b_{m-1} - a_{m-1})/(m-1)a_m \). Then the coefficients of \( u\chi, \psi \) with index \( m - 1 \), resp. \( m \) are equal. Moreover since \( \text{ind}_0 \chi = \text{ind}_0 \psi \), we obtain

\[
\alpha = \frac{y_1 - x_1}{x_2} = \frac{b_{m-1} - a_{m-1}}{(m-1)a_m}.
\]
Consequently by Lemma 5.1(a), \( u\chi(E_1) = y_1 = \psi(E_1) \) and \( u\chi(E_2) = y_2 = \psi(E_2) \). Thus, together with the hypothesis that \( x_2 = y_2 \), we have

\[
u\chi = y_1\bar{3}_1 + y_2\bar{3}_2 + \sum_{1 \leq j \leq m-2, \ell \neq j} a_j p \bar{3}_j + b_{m-1} p \bar{3}_{m-2} + b_m p \bar{3}_m.
\]

We now assume, inductively, that there is an integer \( N \), where \( 3 < N < m-1 \), such that for all \( j \), \( N \leq j < m \), we have \( b_j = a_j \). To complete the induction then, we need to construct \( w \in \mathfrak{N} \) such that the coefficients of \( w\chi \) and \( \psi \) with index \( 3 \leq j-1 \leq k \leq m, p \nmid k \) are equal. If \( p \mid (j-1) \) then the coefficient with index \( j-1 \) does not occur in the standard expansion of \( \chi \), so then there is nothing to prove. Otherwise, let \( w = t(1 + \alpha t^{m-(j-1)}) \) with \( \alpha = (b_{j-1} - a_{j-1})/(j-1)a_m \), then clearly \( b_{j-1} = \psi(E_{j-1}(t)) = (w\chi)(E_{j-1}(t)) \), and the \( b_k = a_k \) for all \( j-1 \leq k < m, p \nmid k \). The induction is complete, and we may assume \( \chi \) to be of the following form

\[
\chi = y_1\bar{3}_1 + y_2\bar{3}_2 + a'_1 p \bar{3}_1 + a'_2 p \bar{3}_2 + \sum_{3 \leq j \leq m, \ell \neq j} b_j p \bar{3}_j
\]

for some \( a'_1, a'_2 \in \mathbb{F}_p \). Note that at each stage of the induction after the base case the coefficients \( y_1, y_2 \) do not change. Furthermore, it is evident that indicum of the characters do not change either.

Now it remains to deal with the coefficients \( a'_1, a'_2 \). Let \( u = t(1 + \alpha t^{m-2}) \) with \( \alpha = (b_2 - a'_2)/2b_m \). Then,

\[
u\chi(E_2(t)) = \chi(E_2 \circ u(t)) = \chi(1 + t^2(1 + 2\alpha t^{m-2}))
\]

\[
= \chi(E_2 \cdot E_m^2) = y_2 + p(a'_2 + 2\alpha b_m)
\]

\[
= y_2 + pb_2 = \psi(E_2(t))
\]

It remains to consider the coefficient with index 1 case. Let \( u = t(1 + \alpha t^{m-1}) \) where \( \alpha = (b_1 - a'_1)/b_m \), where \( a'_1 \) is the altered coefficient \( a_1' \) in \( u\chi \), where \( u \) is the element chosen in the previous step. Then, modulo \( p^2 \),

\[
u\chi(E_1(t)) = \chi((1+t)(1+t^m)^\alpha) = y_1 + pa'_1 + p\alpha b_m
\]

\[
= y_1 + p \left( a_1 + \frac{b_1 - a'_1}{b_m} b_m \right)
\]

\[
= y_1 + p b_1 = \psi(E_1(t)).
\]

This completes the proof in the case where \( m \equiv 1 \pmod{p} \).
where \( \alpha \) is an \((m-2)\)th root of unity. Consider the composite \( U = u \circ (1 + \alpha t) \) where \( \alpha = (y_1 - x_1)/x_2 \). Then \( U\chi \) has the following form

\[
U\chi = y_1\zeta_1 + y_2\zeta_2 + \sum_{1 \leq j \leq m-1, p \nmid j} a_j p\zeta_j + b_m p\zeta_m.
\]

Now we proceed as in the previous case to complete the induction.

Finally consider the case where \( m \equiv 0 \pmod{2} \). As already noted, we have \( m = 2p \). In this case, the basis of induction begins at index \( m - 1 \), and by Lemma 5.1 (d) the basis step holds for appropriate \( \alpha \), and the induction proceeds as in the \( m \neq 0,1 \pmod{2} \) case.

This finishes the proof the sufficiency of the condition \( \text{ind } \chi = \text{ind } \psi \) to imply that \( \chi \) is weakly equivalent to \( \psi \). \( \square \)

**Corollary 6.2.** Let \( m \) be an integer \( \geq 2p \), where \( p \) an odd prime. For each such \( m \), let \( d_m \) denote the number of conjugacy classes of Nottingham elements of order \( p^2 \). Then,

\[
d_m \geq \begin{cases} 
p(p-1) & \text{if } m \equiv 0 \pmod{p} \\
(p-1)^2 & \text{if } m \equiv 1 \pmod{p} \\
(p-1)^2 & \text{otherwise.}
\end{cases}
\]

**Proof.** Recall that the only break sequence with \( p \mid m \) is \((2,2p)\). The corollary follows immediately from the definition of indicium 5.2, and the properties of the coefficients \( x_1, x_2 \) and \( a_j \) for \( 1 \leq j \leq m, p \nmid j \). [Referto the discussion before Lemma 5.1, namely that \( x_2, a_m \in \{1, \ldots, p - 1\} \), and \( x_1 \in \{0, \ldots, p - 1\} \); these coordinates of indicium can be chosen independent of each other. \( \square \)

**Theorem 6.3.** Let \( \chi, \psi \) be characters of order type \((2,m)\) with standard expansions as in equation 6.1. Suppose \( \chi \simeq \psi \), so that for some \( u = t(1 + \alpha t + \beta t^2 + \ldots) \in \mathfrak{N} \), one has \( \psi = u\chi \). Then

1. \( \text{ind } \chi = \text{ind } \psi \).
2. \( x_1 \alpha + x_2 \left( \beta - \left(\frac{\alpha}{2}\right) \right) \equiv 0 \pmod{p} \).

Conversely, suppose \( \text{ind } \chi = \text{ind } \psi \), so that \( \chi \sim \psi \) by Theorem 6.1, i.e. \( \psi = u\chi \) for some \( u \in \mathfrak{N} \). Suppose among such \( u \in \mathfrak{N} \) there exists an \( u = t(1 + \alpha t + \beta t^2 + \ldots) \in \mathfrak{N} \) for which \((2)\) holds, then \( \chi \simeq \psi \).

**Proof.** Suppose \( \chi \simeq \psi \), so that for some \( u = t(1 + \alpha t + \beta t^2 + \ldots) \in \mathfrak{N} \), one has \( \psi = u\chi \), in other words \( \chi \sim \psi \). By Theorem 6.1 \( \text{ind } \chi = \text{ind } \psi \). Furthermore since by definition we have \( \chi(u(t)/t) \equiv 0 \pmod{p} \) it follows that \( (x_1 \alpha + x_2 (\beta - \left(\frac{\alpha}{2}\right))) \equiv 0 \pmod{p} \). Indeed, since \( u(t)/t = \).
\[ 1 + \alpha t + \beta t^2 + \ldots = (1 + t)^\alpha(1 + t^2)^{\beta - \binom{\alpha}{2}} \ldots, \]
it follows that, modulo \( p \),
\[ 0 = \chi(u(t)/t) = x_1\alpha + x_2\left(\beta - \binom{\alpha}{2}\right). \]
The converse implication is again a consequence of Theorem 6.1 and
the above computation. \( \square \)

7. Final remarks

The strict equivalence classes given by the proof of Theorem 6.1
corresponds to some conjugacy classes of Nottingham elements of order
\( p^2 \) [Theorem 3.3]. A complete account of number of strict equivalence
classes of arbitrary type \( \langle a, m \rangle \) where \( a \neq 1, 2 \) needs to be determined.
Moreover, in this paper we considered only the case where the base
field is a prime field \( \mathbb{F}_p \). One might wonder about the the results in the
general case of arbitrary finite field.

Acknowledgments

I remain grateful to Jonathan Lubin for his patience in responding
to numerous emails, and his enthusiasm in clarifying various notions in
the theory.

References

[Ca] Camina, R.: Subgroups of the Nottingham Group, Journal of Algebra, Vol. 196, Issue 1, Po. 101-113, October 1997.
[Ch] Chinburg, T., Symonds, P.: An element of order 4 in the Nottingham group at the prime 2, preprint. [https://arxiv.org/abs/1009.5135.]
[DF] du Sautoy M., Fesenko I. Where the Wild Things Are: Ramification Groups and the Nottingham Group. In: du Sautoy M., Segal D., Shalev A. (eds) New Horizons in pro-p Groups. Progress in Mathematics, vol 184. Birkhuser, Boston, MA, 2000.
[Ha] Hazewinkel, M.: Formal Groups and Applications. Number 78 in Pure and Applied Mathematics. Academic Press, 1978.
[Iw] Iwasawa, K: Local class field theory, Oxford University Press Inc., 1986.
[Je] Jennings, S.A.: Substitution groups of formal power series under substitution, Canad. J. Math., 6 , pp 325-340, 1954.
[Kl] Klopsch, B: Automorphisms of the Nottingham group, J. Algebra 223, pp 37–56, 2000.
[Lu] Lubin J: Torsion in the Nottingham group. Bull. London Math. Soc., pp 547–560, 2011.

E-mail address: venkatakrishna@iiserpune.ac.in

Venkata Krishna Kishore Gangavarapu, Department of Mathematics, Indian Institute of Science Education and Research, Pune, India, 411 008.