AN ELEMENT OF ORDER 4 IN THE NOTTINGHAM GROUP AT THE PRIME 2

T. CHINBURG AND P. SYMONDS

1. Introduction

The Nottingham group $\mathcal{N}(k)$ over a field k of characteristic $p > 0$ is the group of continuous automorphisms of the ring $k[[t]]$ which are equal to the identity modulo t^2. The object of this paper is to construct for $p = 2$ an explicit element of order 4 in $\mathcal{N}(k)$. After giving the proof we will discuss the relation of this construction to some of the literature concerning elements of order p^2 in $\mathcal{N}(k)$.

Theorem 1.1. *Suppose k has characteristic $p = 2$. An automorphism $t \mapsto \sigma(t)$ of order 4 of $k[[t]]$ is given by setting*

$$\begin{aligned} \sigma(t) &= t + t^2 + (t^6) + (t^{12} + t^{14}) + (t^{24} + t^{26} + t^{28} + t^{30}) + (t^{48} + \cdots + t^{62}) + \cdots \\ &= t + t^2 + \sum_{j=0}^{\infty} \sum_{\ell=0}^{2^j-1} t^{6\cdot 2^j + 2\ell} \qquad (1.1) \end{aligned}$$

Proof. Let $A = k[[t, w]]/(w + (1 + t)w^2 + t^3)$. We may define a continuous automorphism σ of A over k by

$$\sigma(t) = (t + w)/(1 + t) \quad \text{and} \quad \sigma(w) = w/(1 + t). \qquad (1.2)$$

It is easily verified that σ has order 4.

Set $v = w(1 + t)$ so that $A = k[[t, v]]/(v^2 + v + t^3 + t^4)$ and let

$$s = \sum_{i=0}^{\infty} (t^3 + t^4)^{2^i}. \qquad (1.3)$$

Then $s^2 + s = t^3 + t^4$, so $v^2 + v + t^3 + t^4 = (v + s)(v + s + 1)$. The second factor is invertible, so $A = k[[t, v]]/(v + s)$. Thus $v = s \in A$ and $w = s/(1+t)$. Substituting this into the expression for $\sigma(t)$ in (1.2) leads to

$$\sigma(t) = \frac{t}{1+t} + \frac{s}{(1+t)^2} = \frac{t}{1+t} + \frac{t^3+t^4}{(1+t)^2} + \frac{\sum_{i=1}^{\infty} (t^3(1+t))^{2^i}}{(1+t)^2}.$$

This leads to the formula in the Theorem on setting $j = i - 1$ in the last sum on the right. □

Date: September 28, 2010.

2000 *Mathematics Subject Classification.* Primary 20F29; Secondary 11G05, 14H37.

Supported by NSF Grant DMS05-00106.

Remark 1.2. Let $(x : y : z)$ be homogeneous coordinates for the projective space $\mathbb{P}^2_k$. We may define an order 4 automorphism σ of $\mathbb{P}^2_k$ by $\sigma(x) = x + y$, $\sigma(y) = y$ and $\sigma(z) = x + z$. This σ stabilizes the curve E with homogeneous equation $z^2y + (z + x)y^2 + x^3 = 0$ as well as the point $Q = (0 : 0 : 1)$ on E. By [8, Appendix A], E is a supersingular elliptic curve with origin Q and j-invariant 0. The completion of the local ring of E at Q is isomorphic to the ring $A \cong k[[t]]$ above when we let $t = x/z$ and $v = (1 + x/z)(y/z)$, and the action of σ on A results from the action of σ on E.

We now discuss some literature pertaining to Theorem 1.1.

Camina has shown in [2] that $\mathcal{N}(k)$ contains every countably based pro-p group as a subgroup [2], so in particular $\mathcal{N}(k)$ contains every finite p-group. In [6], Klopsch shows that representatives for the conjugacy classes of elements of order p are given by the automorphisms $t \mapsto t(1 - at^m)^{-1/m}$ as m ranges over positive integers prime to p and a ranges over elements of k^*. In [3], Camina wrote concerning explicitly described subgroups of $\mathcal{N}(k)$ that "An element of order p^2 is still not known." Order p^2 automorphisms of $k[[t]]$ over k have been extensively studied by Green and Matignon [4], and their work contains implicit formulas for elements of $\mathcal{N}(k)$ of order p^2. Barnea and Klopsch mention in the introduction of [1] that the subgroups of the Nottingham group they consider contain elements of arbitrarily large p-power order. In [7], Lubin uses formal groups of height 1 to give an explicit construction iterative construction of an element

$$t \to \sigma(t) = \sum_{i=1} a_i t^i \tag{1.4}$$

of $\mathcal{N}(k)$ of order p^n for each integer $n \geq 2$. Related constructions of such elements have been considered recently by Green in [5].

The formula in Theorem 1.1 is of interest because it does not require an iterative procedure to produce the a_i in (1.4), and because the height of the formal group associated to the elliptic curve E in Remark 1.2 is 2. It would be very interesting if formal groups of height greater than 1 lead to similar formulas for all primes p.

References

[1] Barnea, Y. and Klopsch, B.: Index-subgroups of the Nottingham group, Adv. Math. **180** no. 1, 187-221 (2003).

[2] Camina, R.: Subgroups of the Nottingham group, J. Algebra **196**, 101-113 (1997).

[3] Camina, R.: The Nottingham group, in New horizons in pro-p groups, Progr. Math. **184**, Birkhäuser Boston, Boston, Mass. (2000).

[4] Green, B. and Matignon, M.: Liftings of Galois covers of smooth curves Compositio Mathematica **113**, 237272,= (1998).

[5] Green, B.: Realizing deformations of curves using Lubin-Tate formal groups. Israel J. Math. **139** (2004), 139–148.

[6] Klopsch, B.: Automorphisms of the Nottingham group, J. Algebra **223**, 37-56 (2000).

[7] Lubin, J.: Torsion in the Nottingham group, doi:10.1112/0000/000000 (2010).

[8] Silverman, J.: The Arithmetic of Elliptic Curves. Springer, New York (1986).

T.C.: Department of Mathematics, University of Pennsylvania, Philadelphia, Pennsylvania 19104-6395, U. S. A.

E-mail address: `ted@math.upenn.edu`

P.S.:, School of Mathematics, University of Manchester, Oxford Road, Manchester M13 9PL, Manchester M13 9PL United Kingdom

E-mail address: `Peter.Symonds@manchester.ac.uk`