Glasgow Math. J. **49** (2007) 449–467. © 2007 Glasgow Mathematical Journal Trust.
doi:10.1017/S0017089507003801. Printed in the United Kingdom

NON-TAME AUTOMORPHISMS OF A FREE GROUP OF RANK 3 IN $\mathfrak{A}_p\mathfrak{A}$

A. I. PAPISTAS

Department of Mathematics, Aristotle University of Thessaloniki, GR 541 24, Thessaloniki, Greece
e-mail: apapist@math.auth.gr

(Received 5 May, 2006; revised 25 April, 2007; accepted 5 June, 2007)

TO PROFESSOR ROGER BRYANT ON HIS 60th BIRTHDAY

Abstract. We give a way of constructing non-tame automorphisms of a free group of rank 3 in the variety $\mathfrak{A}_p\mathfrak{A}$, with p prime.

2000 *Mathematics Subject Classification.* 20F28, 20H25

1. Introduction. For any group G, we write G' for the derived group of G. Let $\mathrm{IA}(G)$ denote the kernel of the natural mapping from $\mathrm{Aut}(G)$ into $\mathrm{Aut}(G/G')$. The elements of $\mathrm{IA}(G)$ are called IA-automorphisms of G. For a positive integer n, with $n \geq 2$, let F_n be a free group of rank n with a basis (in other words, a free generating set) $\{f_1, \ldots, f_n\}$. For any variety of groups $\mathfrak{V}$, let $\mathfrak{V}(F_n)$ denote the verbal subgroup of F_n corresponding to $\mathfrak{V}$. Also, let $F_n(\mathfrak{V}) = F_n/\mathfrak{V}(F_n)$: thus $F_n(\mathfrak{V})$ is a relatively free group of rank n and it has a basis $\{x_1, \ldots, x_n\}$, where $x_i = f_i\mathfrak{V}(F_n)$, $i = 1, \ldots, n$. If ϕ is an automorphism of $F_n(\mathfrak{V})$ then $\{x_1\phi, \ldots, x_n\phi\}$ is also a basis of $F_n(\mathfrak{V})$ and every basis of $F_n(\mathfrak{V})$ has this form. (For information concerning relatively free groups and varieties of groups see [**14**].) Since $\mathfrak{V}(F_n)$ is a characteristic subgroup of F_n, every automorphism φ of F_n induces an automorphism $\overline{\varphi}$ of $F_n(\mathfrak{V})$ in which $x_i\overline{\varphi} = (f_i\varphi)\mathfrak{V}(F_n)$ for $i = 1, \ldots, n$. Thus we obtain a homomorphism of automorphism groups

$$\alpha : \mathrm{Aut}(F_n) \longrightarrow \mathrm{Aut}(F_n(\mathfrak{V})).$$

An automorphism of $F_n(\mathfrak{V})$ which belongs to the image of α is called *tame*. The image of α is denoted by $T_{\mathfrak{V}}$ (or, briefly, T if no confusion is likely to arise). An element $h \in F_n(\mathfrak{V})$ is called *primitive* if h is contained in a basis of $F_n(\mathfrak{V})$. We say that h is induced by a primitive element of F_n if there exists a primitive element g of F_n such that $g\mathfrak{V}(F_n) = h$. For a non-negative integer m, $\mathfrak{A}_m$ denotes the variety of all abelian groups of exponent dividing m, interpreted in such a way that $\mathfrak{A}_0 = \mathfrak{A}$ is the variety of all abelian groups. Furthermore we write $\mathfrak{V}_m = \mathfrak{A}_m\mathfrak{A}$ for the variety of all extensions of groups in $\mathfrak{A}_m$ by groups in $\mathfrak{A}$.

Let R be a commutative ring with identity and m be a positive integer. We write $\mathrm{GL}_m(R)$ for the general linear group of degree m with entries in R and $\mathrm{SL}_m(R)$ for the corresponding special linear group. Let $\mathrm{E}_m(R)$ denote the subgroup of $\mathrm{SL}_m(R)$ that is generated by the elementary matrices. We say a matrix $(a_{ij}) \in \mathrm{SL}_m(R)$ is elementary if $a_{ii} = 1$ for $i = 1, \ldots, m$ and there exists at most one ordered pair of subscripts (i, j) with $i \neq j$ such that $a_{ij} \neq 0$. Furthermore we write $\mathrm{GE}_m(R)$ for the subgroup of $\mathrm{GL}_m(R)$ generated by the invertible diagonal matrices and $\mathrm{E}_m(R)$. A subset S of R is said to be *multiplicative closed* if $1 \in S$ and the product of any two elements of S is an element of S. We write $\mathcal{L}_S(R)$ for the localization of R at S. Let $R[a_1, \dots, a_r]$ be the polynomial ring in indeterminates $a_1, \dots, a_r$ with coefficients in R. Let S be the multiplicative monoid generated by the set $\{a_1, \dots, a_r\}$. Then $\mathcal{L}_S(R[a_1, \dots, a_r]) = R[a_1^{\pm 1}, \dots, a_r^{\pm 1}]$ is the Laurent polynomial ring in indeterminates $a_1, \dots, a_r$ with coefficients in R. Let $\mathbb{Z}$ denote the ring of integers. By a famous result of Suslin [**20**], $\mathrm{SL}_m(\mathbb{Z}[a_1^{\pm 1}, \dots, a_r^{\pm 1}]) = \mathrm{E}_m(\mathbb{Z}[a_1^{\pm 1}, \dots, a_r^{\pm 1}])$ for all integers $m \geq 3$ and $r \geq 1$. For $m = r = 2$, it is well-known that $\mathrm{SL}_2(\mathbb{Z}[a_1^{\pm 1}, a_2^{\pm 1}]) \neq \mathrm{E}_2(\mathbb{Z}[a_1^{\pm 1}, a_2^{\pm 1}])$ (see [**4**, **8**]).

Chein [**6**] gave an example of a non-tame automorphism of $F_3(\mathfrak{V}_0)$. Bachmuth and Mochizuki [**5**] have shown that $\mathrm{Aut}(F_3(\mathfrak{V}_0))$ is not finitely generated. Hence $\mathrm{IA}(F_3(\mathfrak{V}_0))$ is not finitely generated as a group on which T acts by conjugation. Thus there exist infinitely many non-tame automorphisms of $F_3(\mathfrak{V}_0)$. Roman'kov [**17**] has shown that there exists a primitive element of $F_3(\mathfrak{V}_0)$ that is not induced by a primitive element of F_3. Such a primitive element of $F_3(\mathfrak{V}_0)$ is called a non-induced primitive element. The existence of non-induced primitive element starts from the fact that $\mathrm{SL}_2(\mathbb{Z}[a_1^{\pm 1}, a_2^{\pm 1}]) \neq \mathrm{E}_2(\mathbb{Z}[a_1^{\pm 1}, a_2^{\pm 1}])$. Evans [**8**, Theorem C] has presented a method of constructing elements of $\mathrm{SL}_2(\mathbb{Z}[a_1^{\pm 1}, a_2^{\pm 1}])$ not in $\mathrm{E}_2(\mathbb{Z}[a_1^{\pm 1}, a_2^{\pm 1}])$. From the papers of Evans [**8**] and Roman'kov [**17**], it follows that there exists a way of constructing non-tame automorphisms of $F_3(\mathfrak{V}_0)$.

Our main purpose in this paper is to give a way of constructing non-tame automorphisms of $F_3(\mathfrak{V}_p)$ with p prime. In the next few lines we shall explain our method of how to construct non-tame automorphisms of $F_3(\mathfrak{V}_p)$: For each automorphism ϕ of $F_3(\mathfrak{V}_p)$ we define the Jacobian matrix J_ϕ over $\mathbb{F}_p A_3$, where $\mathbb{F}_p$ denotes the finite field with p elements, and A_3 is the free abelian group F_3/F_3' with a basis $\{s_1, s_2, s_3\}$, where $s_i = f_i F_3'$, $i = 1, 2, 3$. Let ζ be the Bachmuth representation of $\mathrm{IA}(F_3(\mathfrak{V}_p))$, that is, the group monomorphism $\zeta : \mathrm{IA}(F_3(\mathfrak{V}_p)) \to \mathrm{GL}_3(\mathbb{F}_p A_3)$ defined by $\phi\zeta = J_\phi$. Notice that the Bachmuth representation is essentially via Fox derivatives. Let S be the multiplicative monoid of $\mathbb{F}_p A_3$ generated by $s_1 - 1$, and let $\mathcal{L}_S(\mathbb{F}_p A_3)$ be the localization of $\mathbb{F}_p A_3$ at S. As in the paper of Bachmuth and Mochizuki [**5**], we conjugate $(\mathrm{IA}(F_3(\mathfrak{V})))\zeta$ by a specific element (c_{ij}) of $\mathrm{GL}_3(\mathcal{L}_S(\mathbb{F}_p A_3))$ to obtain a group homomorphism η from the image of ζ into $\mathrm{GL}_2(\mathcal{L}_S(\mathbb{F}_p A_3))$. Let H be a finitely generated subgroup of $\mathrm{IA}(F_3(\mathfrak{V}_p))$ containing $T \cap \mathrm{IA}(F_3(\mathfrak{V}_p))$. Let ρ be the mapping from H into A_3 defined by $\phi\rho = \det J_\phi = s_1^{\mu_1} s_2^{\mu_2} s_3^{\mu_3}$ where $\mu_1, \mu_2, \mu_3 \in \mathbb{Z}$. Since $T \cap \mathrm{IA}(F_3(\mathfrak{V}_p)) \subseteq H$, it is easily verified that ρ is a group epimorphism. We write N for the kernel of ρ. Since H/N is finitely presented and H is finitely generated, we obtain from a result of Hall [**10**, page 421] N is finitely generated as a group on which H acts by conjugation. Let $\mathcal{H}$ and $\mathcal{N}$ be the images of H and N, respectively, via η. We show in Lemma 3.2 that $\mathcal{N} \subseteq \mathrm{E}_2(\mathcal{L}_P(\mathbb{F}_p A_3))$ for some suitable multiplicative monoid P in $\mathbb{F}_p A_3$. The most difficult part of our method is to show that $\mathrm{SL}_2(\mathcal{L}_P(\mathbb{F}_p A_3)) \neq \mathrm{E}_2(\mathcal{L}_P(\mathbb{F}_p A_3))$ (see Lemma 3.6). We note that the multiplicative monoid P depends upon $\mathcal{H}$. Taking H to be $T \cap \mathrm{IA}(F_3(\mathfrak{V}_p))$ and an explicitly given multiplicative monoid P, we construct infinitely many non-tame automorphisms of $F_3(\mathfrak{V}_p)$ (see Theorem 4.2). That is, using Lemmas 3.3, 3.5 and 3.6, a particular 2×2 matrix, Δ, is constructed which is not a product of elementary matrices, which is nonetheless in the image of the automorphism group of M_3 (as is seen by explicitly writing an appropriate 3×3 matrix and conjugating it) and in the kernel of the map ρ. Lemma 3.2 then allows one to conclude that no tame automorphism can produce Δ, since tame automorphisms in the kernel of ρ are products of elementary matrices. The process of constructing these non-tame automorphisms is effective (see Examples 4.3).

2. Notation and preliminaries. We first fix some notation which is used throughout this paper. For any group G, we write G' for the derived group of G. Recall that IA(G) denotes the group of IA-automorphisms of G. If $a_1, \dots, a_c$ are elements of G then $[a_1, a_2] = a_1^{-1}a_2^{-1}a_1a_2$ and for $c \geq 3$, $[a_1, \dots, a_c] = [[a_1, \dots, a_{c-1}], a_c]$. For elements a and b of G, b^a denotes the conjugate $a^{-1}ba$. For a positive integer n, let F_n be a free group of rank n with a basis $\{f_1, \dots, f_n\}$. Let $A_n = F_n/F_n'$, the free abelian group of rank n. Thus $\{s_1, \dots, s_n\}$, with $s_i = f_iF_n'$ $(i = 1, \dots, n)$, is a basis for A_n. Fix a prime integer p. The variety $\mathfrak{V}_p$ is the class of all groups satisfying the laws $[[f_1, f_2], [f_3, f_4]]$ and $[f_1, f_2]^p$. Thus $\mathfrak{V}_p(F_3) = F_3''(F_3')^p$ and so, every element w of $\mathfrak{V}_p(F_3)$ is a product $w = w_1 \cdots w_k$, where for $i = 1, \dots, k$, either (i) $w_i \in F_3''$, or (ii) $w_i = [u, v]^p$ with $u, v \in F_3$. Let $M_3 = F_3(\mathfrak{V}_p)$ and let $x_i = f_i\mathfrak{V}_p(F_3)$, $i = 1, 2, 3$. Thus $\{x_1, x_2, x_3\}$ is a basis for M_3. Let $\mathbb{Z}$ and $\mathbb{F}_p$ be the ring of integers and the field of p elements, respectively. We write $\mathbb{Z}G$ (resp. $\mathbb{F}_pG$) for the integral group ring (resp. the group algebra over $\mathbb{F}_p$ and G).

2.1. Fox derivatives. We use the partial derivatives introduced by Fox [**9**]. In our notation these are defined as follows : For $j = 1, 2, 3$, the (left) Fox derivative associated with f_j is the linear map $D_j : \mathbb{Z}F_3 \longrightarrow \mathbb{Z}F_3$ satisfying the conditions

$$D_j(f_j) = 1, \quad D_j(f_i) = 0 \ \text{ for } \ i \neq j \tag{1}$$

and

$$D_j(uv) = D_j(u) + uD_j(v) \ \text{ for all } \ u, v \in F_3. \tag{2}$$

It follows that $D_j(1) = 0$ and $D_j(u^{-1}) = -u^{-1}D_j(u)$ for all $u \in F_3$. Let ε be the unit augmentation map $\varepsilon : \mathbb{Z}F_3 \to \mathbb{Z}$. It is well-known (see, for example, [**7**, page 5]) that the kernel of ε (i.e., the augmentation ideal of $\mathbb{Z}F_3$) is a free left $\mathbb{Z}F_3$-module with basis $\{f_j - 1 : j = 1, 2, 3\}$. If $u \in \mathbb{Z}F_3$ then $u - u\varepsilon = \sum_{i=1}^{3} u_i(f_i - 1)$, with $u_i \in \mathbb{Z}F_3$, $i = 1, 2, 3$. By applying D_j, we obtain $D_j(u) = u_j$ and so, we get the following Fox's fundamental formula

$$u - u\varepsilon = \sum_{i=1}^{3} D_i(u)(f_i - 1) \tag{3}$$

for all $u \in \mathbb{Z}F_3$.

There is a natural group epimorphism $\kappa : F_3 \to A_3$ which extends to a ring epimorphism $\kappa : \mathbb{Z}F_3 \to \mathbb{Z}A_3$. Furthermore we write γ for the natural ring epimorphism from $\mathbb{Z}A_3$ into $\mathbb{F}_pA_3$ which agrees on $\mathbb{Z}$ with the natural ring homomorphism from $\mathbb{Z}$ onto $\mathbb{F}_p$. Set $\delta = \kappa \circ \gamma$ and let λ be the natural group epimorphism $\lambda : M_3 \to A_3$ which extends to a ring epimorphism $\lambda : \mathbb{F}_pM_3 \to \mathbb{F}_pA_3$. Note that, for all $f \in F_3$,

$$f\delta = (f\kappa)\gamma = (fF_3')\gamma = fF_3' = (f\mathfrak{V}_p(F_3))\lambda. \tag{4}$$

The equation (4) is really a statement about a rather natural commuting triangle. By an easy calculation, for all $u, v \in F_3$ and $j = 1, 2, 3$,

$$D_j([u, v]) = u^{-1}(v^{-1} - 1)D_j(u) + u^{-1}v^{-1}(u - 1)D_j(v). \tag{5}$$

Let $u = u_1u_2 \cdots u_k$, with $u_1, u_2, \ldots, u_k \in F_3$ and $k \geq 2$. It follows from (2) and an inductive argument on k that

$$D_j(u) = D_j(u_1) + u_1D_j(u_2) + \cdots + u_1 \cdots u_{k-1}D_j(u_k) \tag{6}$$

for $j = 1, 2, 3$. We may deduce from (6) that

$$D_j([u, v]^p) = (1 + [u, v] + \cdots + [u, v]^{p-1})D_j([u, v]) \tag{7}$$

for all $u, v \in F_3$ and $j = 1, 2, 3$. Every element w of $\mathfrak{V}_p(F_3)$ is a product $w = w_1 \cdots w_k$, where for $i = 1, \ldots, k$, either (i) $w_i \in F_3''$, or (ii) $w_i = [u, v]^p$ with $u, v \in F_3$. It follows from (4)–(7) that

$$(D_j(w))\delta = 0 \tag{8}$$

for $j = 1, 2, 3$ and $w \in \mathfrak{V}_p(F_3)$.

For j, with $j \in \{1, 2, 3\}$, we define

$$d_j(f\mathfrak{V}_p(F_3)) = (D_j(f))\delta$$

for all $f \in F_3$. It is easily verified that d_j is well-defined. Since D_j is a linear map and δ is a ring homomorphism, we obtain d_j extends to a linear map from $\mathbb{F}_pM_3$ into $\mathbb{F}_pA_3$ for $j = 1, 2, 3$. From (1), we obtain

$$d_j(x_j) = 1, \quad d_j(x_i) = 0 \quad \text{for} \quad i \neq j.$$

Furthermore $d_j(u^{-1}) = -(u\lambda)^{-1}d_j(u)$ for all $u \in M_3$. Let $u, v \in M_3$, with $u = f\mathfrak{V}_p(F_3)$, $v = g\mathfrak{V}_p(F_3)$ and $f, g \in F_3$. We may deduce from (2) and (4) that

$$d_j(uv) = d_j(u) + (u\lambda)d_j(v). \tag{9}$$

Note that if $u \in M_3'$ and $v \in M_3$ then (9) becomes

$$d_j(uv) = d_j(u) + d_j(v). \tag{10}$$

Furthermore, by (5), (9) and since δ is a ring homomorphism, we obtain

$$d_j([u, v]) = (u^{-1}\lambda)(v^{-1}\lambda - 1)d_j(u) + (u^{-1}\lambda)(v^{-1}\lambda)(u\lambda - 1)d_j(v). \tag{11}$$

Let ϕ be an automorphism of M_3. The *Jacobian matrix* J_ϕ is defined to be the 3×3 matrix over $\mathbb{F}_pA_3$ whose (i, j) entry is $d_j(x_i\phi)$ for $i, j = 1, 2, 3$. Since δ is a ring homomorphism, it follows from (3) that

$$u\lambda - 1 = \sum_{i=1}^{3} d_i(u)(s_i - 1) \tag{12}$$

for all $u \in M_3$. Since M_3' is a vector space over $\mathbb{F}_p$, it may be regarded as a right $\mathbb{F}_p(M_3/M_3')$-module in the usual way, where the module action comes from conjugation in M_3. The group epimorphism $\lambda : M_3 \to A_3$ induces an isomorphism from M_3/M_3' to A_3. So, we may regard M_3' as a right $\mathbb{F}_pA_3$-module. For $w \in M_3'$ and $s \in \mathbb{F}_pA_3$, we write w^s to denote the image of w under the action of s. For $s \in \mathbb{F}_pA_3$ write $s = \sum_i m_i r_i$, where $m_i \in \mathbb{F}_p$ and $r_i \in A_3$ for each i and define

$$s^* = \sum_i m_i r_i^{-1}.$$

Thus $s \mapsto s^*$ is an involutary linear mapping from $\mathbb{F}_pA_3$ to $\mathbb{F}_pA_3$. For $w \in M_3'$ and $s \in \mathbb{F}_pA_3$, it is easily verified that

$$d_j(w^s) = s^* d_j(w). \tag{13}$$

The proof of the following result is elementary.

Lemma 2.1. *Let M_3 be the free group of rank 3 in the variety $\mathfrak{V}_p$, with p prime.*

(i) *For $u \in M_3'$, $[x_i, x_j]^u = [x_i, x_j]$ for all i, j.*

(ii) *For all $u \in M_3$ such that $u \equiv u' \pmod{M_3'}$,*

$$[x_i, x_j]^u = [x_i, x_j]^{u'}.$$

(iii) *For all $u, v \in M_3$,*

$$[x_i, x_j]^{uv} = [x_i, x_j]^{vu}.$$

(iv) $d_i(x_i[x_i, x_j]) = s_j^{-1}$, $\quad d_j(x_i[x_i, x_j^{-1}]) = 1 - s_i$ $\quad$ *and* $\quad d_j(x_i[x_i, x_j]) = s_j^{-1}(s_i - 1)$ *for $i \neq j$.*

(v) *Let $w \in M_3'$. Then we may write*

$$w = \prod_{\substack{i,j \\ 1 \le j < i \le 3}} [x_i, x_j]^{v_{ij}}$$

where $v_{ij} \in \mathbb{F}_pA_3$ for all i, j.

By Lemma 2.1, $[x_i, x_j]^u$ is *really* determined by the congruence classes of u modulo M_3'.

2.2. Ihara's Theorem. If R is a unique factorization domain (UFD) and $S \subseteq R \setminus \{0\}$ is a multiplicative closed subset then $\mathcal{L}_S(R)$ is a UFD (see, for example, [**1**, Chapter 2]). Recall that $\mathbb{F}_p[s_1, s_2, s_3]$ is a UFD. Let C be the monoid generated by $\{s_1, s_2, s_3\}$. It is easily verified that $\mathbb{F}_pA_3 = \mathcal{L}_C(\mathbb{F}_p[s_1, s_2, s_3])$ and so $\mathbb{F}_pA_3$ is a UFD. Let Q denote the quotient field of $\mathbb{F}_pA_3$. The field Q has a discrete valuation determined by the powers of s_3. More precisely, if $v \in \mathbb{F}_pA_3 \setminus \{0\}$, then v can be uniquely written as

$$v = \sum_{i=t}^{r} v_i s_3^i = s_3^t \sum_{i=0}^{r-t} v_{i+t} s_3^i, \quad t < r,$$

where $v_{i+t} \in \mathbb{F}_pA_2$, $i = 0, \ldots, r-t$. Define the s_3-value of v to be $\nu v = t$. If $u, v \in \mathbb{F}_pA_3 \setminus \{0\}$, then we define $(u/v)\nu = u\nu - v\nu$. Let $\mathcal{O}$ be the valuation ring of ν i.e., $\mathcal{O}$

https://doi.org/10.1017/S0017089507003801 Published online by Cambridge University Press

is the ring consisting of 0 and all $w \in Q \setminus \{0\}$ such that $wv \geq 0$. For the proof of the following result, we refer to [**19**, Corollary 1, page 79].

LEMMA 2.2. $\mathrm{SL}_2(Q)$ *is the free product of* $\mathrm{SL}_2(\mathcal{O})$ *and* $\mathrm{SL}_2(\mathcal{O})^{\left(\begin{smallmatrix}1 & 0\\ 0 & s_3\end{smallmatrix}\right)} = \left(\begin{smallmatrix}1 & 0\\ 0 & s_3\end{smallmatrix}\right)^{-1}\mathrm{SL}_2(\mathcal{O})\left(\begin{smallmatrix}1 & 0\\ 0 & s_3\end{smallmatrix}\right)$ *with their intersection D amalgamated.*

2.3. Irreducible polynomials over finite fields. We recall a general principle of obtaining new irreducible polynomials from known ones (see, for example, [**12**, Chapter 3]). Let $f \in \mathbb{F}_p[x]$ be a non-zero polynomial. If f has a non-zero constant term, then the least positive integer e for which $f(x)$ divides $x^e - 1$ is called the *order* of f and denoted by $\mathrm{ord}(f)$. Let f be an irreducible polynomial in $\mathbb{F}_p[x]$ of degree m, with a non-zero constant term. Then $\mathrm{ord}(f)$ is equal to the order of any root of f in the multiplicative group $\mathbb{F}_{p^m}^*$, where $\mathbb{F}_{p^m}$ denotes the field with p^m elements. Let $f(x)$ be a monic irreducible polynomial in $\mathbb{F}_p[x]$ of degree m and order e, and let $t \geq 2$ be an integer whose prime factors divide e but not $(p^m - 1)/e$. Furthermore if $t \equiv 0 \bmod 4$ then $p^m \equiv 1 \bmod 4$. Then $f(x^t)$ is a monic irreducible polynomial in $\mathbb{F}_p[x]$ of degree mt and order et (see [**12**, Theorem 3.35]). The following lemma is probably well-known.

LEMMA 2.3. *Let* $\mathbb{N}$ *be the set of positive integers. There exists an injective mapping* ω *from* $\mathbb{N}$ *into itself and a monic irreducible polynomial* $\pi(x)$ *in* $\mathbb{F}_p[x]$ *such that* $\pi(x^{n\omega})$ *is a monic irreducible polynomial in* $\mathbb{F}_p[x]$ *for all* $n \geq 1$.

Proof. Let $p = 2$. Then $x^{2\,3^n} + x^{3^n} + 1$ is irreducible in $\mathbb{F}_2[x]$ for all $n \geq 1$ (see [**12**, Chapter 3, page 146]). Thus we may assume that p is an odd prime. Let q be an odd prime divisor of $p - 1$. Then there exists $a \in \{2, \dots, p-1\}$ such that $a^{\frac{p-1}{q}} \neq 1$. Since $x^q - a$ has no root in $\mathbb{F}_p$, we obtain $x^{q^n} - a$ is irreducible in $\mathbb{F}_p[x]$ for all $n \geq 1$ (see [**12**, Theorem 3.75 and page 145]). Thus we may assume that p has the form $1 + 2^r$, with $r \geq 1$, and so p is a Fermat prime and $r = 2^\beta$, with $\beta \in \{0, 1, 2, \dots\}$. Let $\beta = 0$. Since $x^3 - x - 1$ is irreducible in $\mathbb{F}_3[x]$ and $\mathrm{ord}(x^3 - x - 1) = 13$, we obtain $x^{3\,13^n} - x^{13^n} - 1$ is irreducible in $\mathbb{F}_3[x]$ for all $n \geq 1$. Finally, we assume that $\beta \geq 1$. Recall that $(\frac{3}{p}) = 1$ if and only if $p \equiv 1, -1 \bmod 12$ (see [**15**, page 139]). Since $p \equiv 5 \bmod 12$, we obtain $(\frac{3}{p}) = -1$ and so $x^2 - 3$ is irreducible in $\mathbb{F}_p[x]$. Since $\mathrm{ord}(x^2 - 3) = 2^{r+1}$ and $\frac{p^2-1}{2^{r+1}} = 1 + 2^{r-1}$, we obtain $x^{2^n} - 3$ is irreducible in $\mathbb{F}_p[x]$ for all $n \geq 1$ (see, also, [**12**, Theorem 3.75]). Therefore there exists an irreducible polynomial $\pi(x)$ in $\mathbb{F}_p[x]$ and an injective mapping ω from $\mathbb{N}$ into itself such that $\pi(x^{n\omega})$ is irreducible for all n.

REMARK 2.4. It is well-known that, for a prime power q, the number of monic irreducible polynomials of degree n over $\mathbb{F}_q$ is given by $\frac{1}{n}\sum_{d|n}\mu(\frac{n}{d})q^d$. Thus there are infinitely many monic irreducible polynomials over $\mathbb{F}_q$ of different degree. The proof of Lemma 2.3 is needed in Section 4 for constructing non-tame automorphisms of $F_3(\mathfrak{B}_p)$.

It is elementary to show that if R is a principal ideal domain (PID), which is not a field, and $a \in R \setminus \{0\}$ is a non-unit of R then, $\mathcal{L}_S(R)$ is a PID, where $S = \{a^n : n \geq 0\}$.

LEMMA 2.5. *Let* π *be a monic irreducible polynomial of a positive degree with a non-zero constant term in* $\mathbb{F}_p[s_1]$, *J the ideal of* $\mathbb{F}_p[s_1]$ *generated by* π *and I the ideal of* $\mathbb{F}_pA_1$ *generated by* π. *Then* $\mathbb{F}_p[s_1]/J$ *is isomorphic to* $\mathbb{F}_pA_1/I$.

https://doi.org/10.1017/S0017089507003801 Published online by Cambridge University Press

Proof. Let $\pi = s_1^n + c_{n-1}s_1^{n-1} + \cdots + c_1s_1 + c_0$, with $n \geq 1$ and $c_0 \neq 0$, be a monic irreducible element in $\mathbb{F}_p[s]$. Let I be the ideal in $\mathbb{F}_pA_1$ generated by π. Let $E = I \cap \mathbb{F}_p[s]$. We claim that $E = J$. Since E is an ideal in $\mathbb{F}_p[s_1]$ and $\mathbb{F}_p[s_1]$ is a PID, E is generated by an element d, say. Since $\pi \in \mathbb{F}_p[s_1]$, $\pi \in E$ and so $J \subseteq E$. To show that $E \subseteq J$ it is enough to prove that $d \in J$. But $d \in I$ and so $d = \pi u$ for some $u \in \mathbb{F}_pA_1$. Write $u = s_1^m v$, where $v = a_0 + a_1s_1 + \cdots + a_\mu s_1^\mu \in \mathbb{F}_p[s_1]$ and $a_0 \neq 0$. Suppose that $m < 0$. Since $c_0a_0 \neq 0$, we obtain a contradiction. Thus $m \geq 0$ and $d \in J$. Therefore $E = J$. Observe that π is irreducible in $\mathbb{F}_pA_1$. Since both $\mathbb{F}_p[s_1]$ and $\mathbb{F}_pA_1$ are PID, we obtain $\mathbb{F}_p[s_1]/J$ and $\mathbb{F}_pA_1/I$ are fields. Let δ be the natural ring homomorphism from $\mathbb{F}_p[s_1]$ into $\mathbb{F}_pA_1/I$ defined by $v\delta = v + I$ for all $v \in \mathbb{F}_p[s_1]$. It is easily verified that $\ker\delta = J$ and so δ induces a ring monomorphism $\bar\delta$ from $\mathbb{F}_p[s_1]/J$ into $\mathbb{F}_pA_1/I$ such that $(v + J)\bar\delta = v\delta$. We claim that $\bar\delta$ is surjective. Let $u = w + I$, where $w \in \mathbb{F}_pA_1$, and write $w = s_1^m w_1$ where $w_1 \in \mathbb{F}_p[s_1]$. If $m \geq 0$, we obtain $(w + J)\bar\delta = u$. Suppose that $m < 0$. Then, since $(\mathbb{F}_p[s_1] + I)/I$ is a field, there exists $x \in \mathbb{F}_p[s_1]$ such that $(s_1 + I)(x + I) = 1 + I$. Also, $(s_1 + I)(s_1^{-1} + I) = 1 + I$. Therefore $x + I = s_1^{-1} + I$ and so, $(x^{-m}w_1 + J)\bar\delta = x^{-m}w_1 + I = s_1^m w_1 + I = w + I = u$. Thus $\bar\delta$ is surjective and so, $\mathbb{F}_p[s_1]/J$ is isomorphic to $\mathbb{F}_pA_1/I$.

3. A method. We denote by Ω a free left $\mathbb{F}_pA_3$-module with a basis $\{t_1, t_2, t_3\}$. The set $A_3 \times \Omega$ becomes a group by defining a multiplication

$$(\bar u, m_1)(\bar v, m_2) = (\bar u\,\bar v, m_1 + \bar u m_2) = (\overline{uv}, m_1 + \bar u m_2)$$

for all $\bar u, \bar v \in A_3$, where $\bar u = uF_3'$ and $\bar v = vF_3'$, with $u, v \in F_3$, and $m_1, m_2 \in \Omega$. Let χ be the mapping from F_3 into $A_3 \times \Omega$ defined by $f\chi = (\bar f, d_1(u)t_1 + d_2(u)t_2 + d_3(u)t_3)$, with $u = f\mathfrak{V}_p(F_3)$. It is easily verified that χ is a group homomorphism. But $\ker\chi = \mathfrak{V}_p(F_3)$ (see, for example, [**11**, Proposition 1]). Hence M_3 is embedded into $A_3 \times \Omega$ by χ satisfying the conditions $x_i\chi = (s_i, t_i)$, $i = 1, 2, 3$. The proof of the following result is elementary.

Lemma 3.1. For $u \in M_3'$,

$$u\chi = (1, d_1(u)t_1 + d_2(u)t_2 + d_3(u)t_3).$$

Let ϕ be an IA-automorphism of M_3 satisfying the conditions $x_i\phi = x_iu_i$, where $u_i \in M_3'$, $i = 1, 2, 3$, and let $\widehat\phi = \chi^{-1}\phi\chi$. It is easily verified that $\widehat\phi$ is an IA-automorphism of $M_3\chi$. Thus, for $i \in \{1, 2, 3\}$,

$$\begin{aligned}
(s_i, t_i)\widehat\phi = (x_i\phi)\chi &= (x_i\chi)(u_i\chi) \\
\text{(Lemma 3.1)} \qquad &= (s_i, t_i)(1, d_1(u_i)t_1 + d_2(u_i)t_2 + d_3(u_i)t_3) \\
\text{(Equation (9))} \qquad &= (s_i, d_1(x_iu_i)t_1 + d_2(x_iu_i)t_2 + d_3(x_iu_i)t_3) \\
&= (s_i, a_{i1}t_1 + a_{i2}t_2 + a_{i3}t_3),
\end{aligned} \tag{14}$$

where $a_{ij} = d_j(x_iu_i)$ for $i, j \in \{1, 2, 3\}$, and

$$a_{i1}(s_1 - 1) + a_{i2}(s_2 - 1) + a_{i3}(s_3 - 1) = s_i - 1 \tag{15}$$

for $i = 1, 2, 3$. The equation (15) is just a restatement of Fox's fundamental formula, as stated in equation (12). Notice that equations (14) give $J_\phi = (a_{ij})$. The mapping ζ from $\mathrm{IA}(M_3)$ into $\mathrm{GL}_3(\mathbb{F}_pA_3)$ given by $\phi \longmapsto J_\phi = (a_{ij})$ is a faithful representation of $\mathrm{IA}(M_3)$. (Indeed, write $\gamma_{ij} = d_j(x_i\phi\psi)$, $a_{ij} = d_j(x_i\phi)$ and $b_{ij} = d_j(x_i\psi)$. By Lemma 2.1

and equations (9), (10), (13) and (11), we get $\gamma_{ij} = \sum_{\kappa=1}^{3} a_{i\kappa} b_{\kappa j}$ for $i, j = 1, 2, 3$ and so, ζ is a group homomorphism. If $x_i\phi = x_i u_i$, with $u_i \in M_3'$, $i = 1, 2, 3$, and $d_j(x_i\phi) = d_j(x_i u_i) = \delta_{ij}$, where δ_{ij} is the Kronecker's delta, then $d_j(u_i) = 0$ for $i, j = 1, 2, 3$. Hence $u_i \in \mathfrak{V}_p(F_3)$ with $i = 1, 2, 3$ (see, for example, [**11**, Proposition 1]). Therefore ζ is a group monomorphism.) Suppose that $(a_{ij}) \in \mathrm{Im}\zeta$. Thus the determinant of (a_{ij}) is a unit in $\mathbb{F}_pA_3$, and its rows satisfy equations (15). Since the units of $\mathbb{F}_pA_3$ are of the form $q\,a$ (see, for example, [**18**, Lemma 3.2, page 55]), where $q \in \mathbb{F}_p \setminus \{0\}$ and $a \in A_3$, we obtain

$$\det(a_{ij}) = q s_1^{\mu_1} s_2^{\mu_2} s_3^{\mu_3} \tag{16}$$

where $q \in \mathbb{F}_p \setminus \{0\}$ and $\mu_1, \mu_2, \mu_3 \in \mathbb{Z}$. For the next few lines, for each $u \in \mathbb{F}_pA_3$, we write $\widehat{u}$ for the element of $\mathbb{F}_p$ obtained from u substituting s_1, s_2, s_3 by 1. For $s_2 = s_3 = 1$, equations (15) give $a_{11}(s_1^{\pm 1})(s_1 - 1) = s_1 - 1$ and $a_{i1}(s_1^{\pm 1})(s_1 - 1) = 0$ with $i = 2, 3$. Since $\mathbb{F}_pA_3$ is an integral domain, we get $a_{11}(s_1^{\pm 1}) = 1$ and $a_{21}(s_1^{\pm 1}) = a_{31}(s_1^{\pm 1}) = 0$. Thus $\widehat{a}_{11} = 1$ and $\widehat{a}_{21} = \widehat{a}_{31} = 0$. Similarly, $\widehat{a}_{22} = \widehat{a}_{33} = 1$ and $\widehat{a}_{ij} = 0$ for $i \neq j$. Thus equation (16) (for $s_1 = s_2 = s_3 = 1$) gives $q = 1$. Therefore, for an element $(a_{ij}) \in \mathrm{Im}\zeta$, its determinant is equal to $s_1^{\mu_1} s_2^{\mu_2} s_3^{\mu_3}$, with $\mu_1, \mu_2, \mu_3 \in \mathbb{Z}$, and its rows satisfy equations (15). For the converse, the proof of Lemma 1 in [**2**] carries over with minor changes apart from some obvious misprints. We note that the aforementioned equivalent statements are stated in [**3**, Proposition 2]. This is the *Bachmuth representation* of $\mathrm{IA}(M_3)$.

We write $\mathcal{A}$ for the image of $\mathrm{IA}(M_3)$ via ζ. Let S be the multiplicative monoid of $\mathbb{F}_pA_3$ generated by $s_1 - 1$. Since $\mathbb{F}_pA_3$ is a UFD and $S \subseteq \mathbb{F}_pA_3 \setminus \{0\}$, we obtain $\mathcal{L}_S(\mathbb{F}_pA_3)$ is a UFD. We conjugate $\mathcal{A}$ by the element

$$(c_{ij}) = \begin{pmatrix} s_1 - 1 & 0 & 0 \\ s_2 - 1 & (s_1 - 1)^{-1} & 0 \\ s_3 - 1 & 0 & 1 \end{pmatrix}.$$

Using equation (15) it is easy to verify that

$$(c_{ij})^{-1}(a_{ij})(c_{ij}) = \begin{pmatrix} 1 & a_{12}(s_1 - 1)^{-2} & a_{13}(s_1 - 1)^{-1} \\ 0 & b_{11} & b_{12} \\ 0 & b_{21} & b_{22} \end{pmatrix}, \tag{17}$$

where $b_{11} = [a_{22}(s_1 - 1) - a_{12}(s_2 - 1)](s_1 - 1)^{-1}$, $b_{12} = a_{23}(s_1 - 1) - a_{13}(s_2 - 1)$, $b_{21} = [a_{32}(s_1 - 1) - a_{12}(s_3 - 1)](s_1 - 1)^{-2}$ and $b_{22} = [a_{33}(s_1 - 1) - a_{13}(s_3 - 1)](s_1 - 1)^{-1}$. It is easily verified that the map η from $\mathcal{A}$ into $\mathrm{GL}_2(\mathcal{L}_S(\mathbb{F}_pA_3))$ defined by $(a_{ij})\eta = (b_{k\ell})$ is a group homomorphism.

Let H be a finitely generated subgroup of $\mathrm{IA}(M_3)$ containing $T \cap \mathrm{IA}(M_3)$. Let ρ be the mapping from H into A_3 defined by $\phi\rho = \det J_\phi = s_1^{\mu_1} s_2^{\mu_2} s_3^{\mu_3}$, where $\mu_1, \mu_2, \mu_3 \in \mathbb{Z}$. Since $T \cap \mathrm{IA}(M_3) \subseteq H$, it is easily verified that ρ is an epimorphism. Thus we obtain the following short exact sequence

$$1 \to N \to H \xrightarrow{\rho} A_3 \to 1,$$

where N denotes the kernel of ρ. Since H/N is finitely presented and H is finitely generated, we obtain from a result of Hall [**10**, page 421] N is finitely generated as a group on which H acts by conjugation. The proof of the following result is based on some ideas given in the proof of Lemma 5 in [**5**].

LEMMA 3.2. *Let $\mathcal{H}$ and $\mathcal{N}$ be the images of H and N, respectively, in* $\mathrm{GL}_2(\mathcal{L}_S(\mathbb{F}_pA_3))$ *via the group homomorphism η. Let $(a_{ij1}),\ldots,(a_{ijr})$ be a generating set of $\mathcal{H}$, and let $(b_{ij1}),\ldots,(b_{ijs})$ be a generating set of $\mathcal{N}$ as a group on which $\mathcal{H}$ acts by conjugation. Then there exist irreducible elements $\alpha_1,\ldots,\alpha_q\in\mathbb{F}_pA_3$ such that if P is the multiplicative monoid generated by $\mathbb{F}_p\setminus\{0\}$, $\{s_1^{\pm1},s_2^{\pm1},s_3^{\pm1}\}$, s_1-1 and α_j, $j=1,\ldots,q$, then $(d_{ij})\in$ $\mathrm{E}_2(\mathcal{L}_P(\mathbb{F}_pA_3))$ for all $(d_{ij})\in\mathcal{N}$.*

Proof. From (17), $a_{12k},b_{12\ell}\in\mathbb{F}_pA_3$ for $k=1,\ldots,r$ and $\ell=1,\ldots,s$. Let $\alpha_1,\ldots,\alpha_q$ be the irreducible elements in $\mathbb{F}_pA_3$ which appear as a factor of a_{12k} or $b_{12\ell}$, $k=1,\ldots,r$, $\ell=1,\ldots,s$. Let P be the multiplicative monoid generated by $\mathbb{F}_p\setminus\{0\}$, $\{s_1^{\pm1},s_2^{\pm1},s_3^{\pm1}\}$, s_1-1 and α_j, $j=1,\ldots,q$. Since P is a multiplicative closed set not containing the zero element and $\mathbb{F}_pA_3$ is a UFD, we obtain $\mathcal{L}_P(\mathbb{F}_pA_3)$ is a UFD and

$$\mathbb{F}_pA_3\subseteq\mathcal{L}_S(\mathbb{F}_pA_3)\subseteq\mathcal{L}_P(\mathbb{F}_pA_3)\subseteq Q.$$

Let $(d_{ij})\in\mathcal{H}$. We claim that $(d_{ij})\in\mathrm{GE}_2(\mathcal{L}_P(\mathbb{F}_pA_3))$. By (17), $a_{11k}a_{22k}-a_{12k}a_{21k}$ is a unit in $\mathcal{L}_P(\mathbb{F}_pA_3)$ for $k=1,\ldots,r$. Fix k, $k=1,\ldots,r$, and write e_{ij} for a_{ijk}, $i,j=1,2$. Let $e_{12}=0$. Then

$$\begin{pmatrix}e_{11}&0\\e_{21}&e_{22}\end{pmatrix}=\begin{pmatrix}e_{11}&0\\0&e_{11}^{-1}\end{pmatrix}\begin{pmatrix}1&0\\e_{11}e_{21}&1\end{pmatrix}\begin{pmatrix}1&0\\0&e_{11}e_{22}\end{pmatrix}\in\mathrm{GE}_2(\mathcal{L}_P(\mathbb{F}_pA_3)).$$

Thus we may assume that $e_{12}\neq0$. Since $e_{12}\in P$, we obtain $e_{21}=e_{12}^{-1}(e_{11}e_{22}-u)$, where $u=e_{11}e_{22}-e_{21}e_{12}$. Then

$$\begin{pmatrix}e_{11}&e_{12}\\e_{21}&e_{22}\end{pmatrix}=\begin{pmatrix}e_{12}&0\\0&e_{12}^{-1}\end{pmatrix}\begin{pmatrix}1&0\\e_{12}e_{22}&1\end{pmatrix}\begin{pmatrix}u^{-1}&0\\0&1\end{pmatrix}$$
$$\begin{pmatrix}1&-e_{11}e_{12}^{-1}\\0&1\end{pmatrix}\begin{pmatrix}0&u\\-u&0\end{pmatrix}\in\mathrm{GE}_2(\mathcal{L}_P(\mathbb{F}_pA_3)).$$

Thus (d_{ij}) is a product of the (a_{ijk}), whence $(d_{ij})\in\mathrm{GE}_2(\mathcal{L}_P(\mathbb{F}_pA_3))$. For the next few lines, we write $E(x)$ for the matrix $\left(\begin{smallmatrix}x&1\\-1&0\end{smallmatrix}\right)$ for $x\in\mathcal{L}_P(\mathbb{F}_pA_3)$. Note that, for invertible element x,

$$\begin{pmatrix}x&0\\0&x^{-1}\end{pmatrix}=E(0)^{-1}E(x^{-1})E(x)E(x^{-1})E(0)^{-1},$$

$$E(0)=\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&0\\-1&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}$$

and

$$E(x)=\begin{pmatrix}1&-x\\0&1\end{pmatrix}E(0).$$

Thus $\left(\begin{smallmatrix}x&0\\0&x^{-1}\end{smallmatrix}\right)\in\mathrm{E}_2(\mathcal{L}_S(\mathbb{F}_pA_3))$. Applying similar arguments as above, we obtain $(b_{ij\ell})\in$ $\mathrm{E}_2(\mathcal{L}_P(\mathbb{F}_pA_3))$ for all $\ell=1,\ldots,s$. The group $\mathcal{N}$ is generated as a group by the elements

$$(a_{ij})^{-1}(b_{ij\ell})(a_{ij}),$$

where $\ell = 1, \dots, s$, and $(a_{ij}) \in \mathcal{H}$. Since $\mathrm{E}_2(\mathcal{L}_P(\mathbb{F}_p A_3))$ is a normal subgroup of $\mathrm{GE}_2(\mathcal{L}_P(\mathbb{F}_p A_3))$, we obtain $(a_{ij})^{-1}(b_{ij\ell})(a_{ij}) \in \mathrm{E}_2(\mathcal{L}_P(\mathbb{F}_p A_3))$. Thus $(d_{ij}) \in \mathrm{E}_2(\mathcal{L}_P(\mathbb{F}_p A_3))$ if $(d_{ij}) \in \mathcal{N}$.

We need some notation and auxiliary lemmas before we prove a result (namely, Lemma 3.6) which is the key ingredient of our method of constructing non-tame automorphisms of $F_3(\mathfrak{V}_p)$.

First we recall some elementary facts about unique factorization domains (UFD) (see, for example, [**1**, Chapter 2]). Let R be a UFD. Two elements u and v in R are said to be associates if $u = cv$, where c is a unit. Define a relation $\equiv$ on R as follows : $u \equiv v$ if u and v are associates. It is an equivalence relation on R. Denote by $[u]$ the equivalence class of u. An element $a \in R$ is irreducible if and only if it is prime. For a non-empty subset X of $R \setminus \{0\}$ we write $\mathrm{Irr}(X)$ for the set of equivalence classes $[u]$, where u is an irreducible element of R which appears in the factorization of some element of X. Let $u, v \in R \setminus \{0\}$. If $v = ua$ for some $a \in R$ we say u divides v (written $u \mid v$); otherwise we write $u \nmid v$. Any set Y of nonzero elements of R has a greatest common divisor (gcd). Note that any two gcds of Y are associates. If 1 is a gcd of Y, then we say that the set Y is relatively prime.

Recall from the proof of Lemma 3.2 that P is the multiplicative monoid generated by $\mathbb{F}_p \setminus \{0\}$, $\{s_1^{\pm 1}, s_2^{\pm 1}, s_3^{\pm 1}\}$, $s_1 - 1$, and α_j, $j = 1, \dots, q$. A typical element of $P \setminus \{1\}$ has the form

$$d\, a\, (s_1 - 1)^n\, \alpha_{j_1} \cdots \alpha_{j_\mu},$$

where $d \in \mathbb{F}_p \setminus \{0\}$, $a \in A_3$, n a non-negative integer, and $\alpha_{j_k} \in \{\alpha_1, \dots, \alpha_q\}$, $k = 1, \dots, \mu$. Each α_j, $j = 1, \dots, q$, has a unique expression as an element in $\mathbb{F}_p A_3$

$$\alpha_j = s_3^{m_j} \left(\sum_{i_j = m_j}^{n_j} u_{i_j} s_3^{i_j - m_j} \right),$$

where $m_j \le n_j$, $u_{i_j} \in \mathbb{F}_p A_2$, $i_j = m_j, \dots, n_j$, $u_{m_j} \ne 0$ and $u_{n_j} \ne 0$. Write $h_j = s_3^{-m_j} \alpha_j$ for $j = 1, \dots, q$. Let P_{s_3} be the submonoid of P generated by $\mathbb{F}_p \setminus \{0\}$, $\{s_1^{\pm 1}, s_2^{\pm 1}\}$, $s_1 - 1$ and $h_1, \dots, h_q$. Thus an element of $P_{s_3} \setminus \{1\}$ has the form

$$d\, h\, (s_1 - 1)^n\, h_{j_1} \cdots h_{j_\mu},$$

where $d \in \mathbb{F}_p \setminus \{0\}$, $h \in A_2$, n a non-negative integer, and $h_{j_k} \in \{h_1, \dots, h_q\}$, $k = 1, \dots, \mu$. Note that $P_{s_3} \subseteq \mathbb{F}_p A_2[s_3]$ and $\mathcal{L}_P(\mathbb{F}_p A_3) \cap \mathcal{O} = \mathcal{L}_{P_{s_3}}(\mathbb{F}_p A_2[s_3])$. Let Ψ be the ring epimorphism from $\mathbb{F}_p A_2[s_3]$ onto $\mathbb{F}_p A_2$ satisfying the conditions $u\Psi = u$ for all $u \in \mathbb{F}_p A_2$ and $s_3 \Psi = 0$. Thus $P_{s_3}\Psi$ is the monoid generated by $\mathbb{F}_p \setminus \{0\}$, $\{s_1^{\pm 1}, s_2^{\pm 1}\}$, $s_1 - 1$ and $u_{m_1}, \dots, u_{m_q}$. An element of $P_{s_3}\Psi \setminus \{1\}$ is written as

$$d\, h\, (s_1 - 1)^n\, u_{j_1} \cdots u_{j_\mu},$$

where $d \in \mathbb{F}_p \setminus \{0\}$, $h \in A_2$, n is a non-negative integer, and $u_{j_1}, \dots, u_{j_\mu} \in \{u_{m_1}, \dots, u_{m_q}\}$. Hence $\mathrm{Irr}(P_{s_3}\Psi)$ is finite. Since $0 \notin P_{s_3}\Psi$, the epimorphism Ψ induces a ring epimorphism $\widetilde{\Psi}$ from $\mathcal{L}_{P_{s_3}}(\mathbb{F}_p A_2[s_3])$ onto $\mathcal{L}_{P_{s_3}\Psi}(\mathbb{F}_p A_2)$ such that $\frac{f}{t}\widetilde{\Psi} = \frac{f\Psi}{t\Psi}$.

LEMMA 3.3. *Let $\pi(s_1)$ and ω be as in the statement of Lemma 2.3. Then, for infinitely many n, $\pi(s_1^{n\omega})$ is not invertible in $\mathcal{L}_{P_{s_3}\Psi}(\mathbb{F}_p A_2)$.*

https://doi.org/10.1017/S0017089507003801 Published online by Cambridge University Press

Proof. Let $\pi(s_1)$ and ω be as in the statement of Lemma 2.3. Then $\pi(s_1^{n\omega})$ is an irreducible polynomial in $\mathbb{F}_pA_2$ for all $n \geq 1$. Suppose that $\pi(s_1^{n\omega})$ is invertible in $\mathcal{L}_{P_{s_3}\Psi}(\mathbb{F}_pA_2)$ for some n. Then there exists $u \in \mathcal{L}_{P_{s_3}\Psi}(\mathbb{F}_pA_2)$ such that $\pi(s_1^{n\omega})u = 1$. Write $u = \frac{v}{t}$ where $v \in \mathbb{F}_pA_2$ and $t \in P_{s_3}\Psi$. Thus $\pi(s_1^{n\omega})v = t$ in $\mathbb{F}_pA_2$. Since $\mathbb{F}_pA_2$ is a UFD, we obtain there exists t_1 an irreducible element in $\mathbb{F}_pA_2$ which appears in the factorization of t such that $\pi(s_1^{n\omega}) \in [t_1]$. Observe that if $\pi(s_1^{n\omega}) \in [t_1]$ then $\pi(s_1^{m\omega})$ does not belong to $[t_1]$ for $m \neq n$. Indeed, if $\pi(s_1^{m\omega}) \in [t_1]$ then $\pi(s_1^{n\omega}) = \pi(s_1^{m\omega})c$, where c is a unit in $\mathbb{F}_pA_2$. Since the only units in $\mathbb{F}_pA_2$ are the elements of $\mathbb{F}_p \setminus \{0\}$ and the elements of A_2, we obtain a contradiction. Thus $\pi(s_1^{m\omega})$ does not belong to $[t_1]$ for $m \neq n$. Since $\mathrm{Irr}(P_{s_3}\Psi)$ is finite whereas $\pi(s_1^{n\omega})$ is irreducible for all $n \geq 1$, we obtain $\pi(s_1^{n\omega})$ is not invertible in $\mathcal{L}_{P_{s_3}\Psi}(\mathbb{F}_pA_2)$ for infinitely many n.

REMARK 3.4. Let π be a monic irreducible polynomial in $\mathbb{F}_p[s_1]$ subject to π is not invertible in $\mathcal{L}_{P_{s_3}\Psi}(\mathbb{F}_pA_2)$. Then $\pi \nmid x$ for all $x \in P_{s_3}\Psi$. Indeed, suppose that there exists $x \in P_{s_3}\Psi$ such that $\pi | x$. Thus $x = \pi x'$ for some $x' \in \mathbb{F}_pA_2$. Since $x \in P_{s_3}\Psi$, we obtain x is invertible in $\mathcal{L}_{P_{s_3}\Psi}(\mathbb{F}_pA_2)$. Therefore π is invertible in $\mathcal{L}_{P_{s_3}\Psi}(\mathbb{F}_pA_2)$ which is a contradiction. By Remark 2.4, there are infinitely many irreducible polynomials of different degrees in $\mathbb{F}_p[s_1]$. Thus there are infinitely many irreducible polynomials in $\mathbb{F}_pA_2$. The arguments given in the proof of Lemma 3.3 guarantee that there are infinitely many irreducible elements in $\mathbb{F}_pA_2$ which are not invertible in $\mathcal{L}_{P_{s_3}\Psi}(\mathbb{F}_pA_2)$.

By the proof of Lemma 3.3 (and Remark 3.4), we may choose a monic irreducible polynomial π of degree m in $\mathbb{F}_p[s_1]$ subject to $\pi \nmid x$ for all $x \in P_{s_3}\Psi$, and there exists an odd prime divisor q of $p^m - 1$. Let I be the ideal of $\mathbb{F}_pA_1$ generated by π. By Lemma 2.5, $\mathbb{F}_pA_1/I$ is a field of p^m elements.

From now on, we fix π and write K for $\mathbb{F}_pA_1/I$. The natural mapping ϑ from $\mathbb{F}_pA_1$ onto K induces a ring epimorphism ϑ_1 from $\mathbb{F}_pA_2$ onto $K[s_2^{\pm 1}]$ in a natural way. Since $P_{s_3}\Psi$ is a multiplicative closed subset of $\mathbb{F}_pA_2$, we obtain $P_{s_3}\Psi\vartheta_1$ is a multiplicative closed subset of $K[s_2^{\pm 1}]$. Suppose that $0 \in P_{s_3}\Psi\vartheta_1$. Then there exists $v \in P_{s_3}\Psi$ such that $v\vartheta_1 = 0$. Since $v \in P_{s_3}\Psi$, we obtain v is invertible in $\mathcal{L}_{P_{s_3}\Psi}(\mathbb{F}_pA_2)$. Write $v = \sum v_\ell s_2^\ell$, with $v_\ell \in \mathbb{F}_pA_1$. By applying ϑ_1, we obtain

$$v\vartheta_1 = \sum (v_\ell\vartheta)s_2^\ell = 0$$

and so, $v_\ell \in \ker\vartheta$ for all ℓ. Since $\ker\vartheta$ is the ideal in $\mathbb{F}_pA_1$ generated by π, we obtain π divides v_ℓ for all ℓ and so, π divides v in $\mathbb{F}_pA_2$ which is a contradiction by the choice of π. Therefore $0 \notin P_{s_3}\Psi\vartheta_1$ and so, $\mathcal{L}_{P_{s_3}\Psi\vartheta_1}(K[s_2^{\pm 1}]) \neq \{0\}$. Observe that $\mathrm{Irr}(P_{s_3}\Psi\vartheta_1)$ is finite. The epimorphism ϑ_1 induces a ring epimorphism $\widetilde{\vartheta}_1$ from $\mathcal{L}_{P_{s_3}\Psi}(\mathbb{F}_pA_2)$ onto $\mathcal{L}_{P_{s_3}\Psi\vartheta_1}(K[s_2^{\pm 1}])$ by defining $\frac{u}{t}\widetilde{\vartheta}_1 = \frac{u\vartheta_1}{t\vartheta_1}$ for all $u \in \mathbb{F}_pA_2$ and $t \in P_{s_3}\Psi$.

Let b be an element of $K \setminus \{0\}$ such that $b^{\frac{p^m-1}{q}} \neq 1$. Since $s_2^q - b$ has no root in K, we obtain $s_2^{q^n} - b$ is irreducible in $K[s_2]$ for all $n \geq 1$ (see [**12**, Theorem 3.75 and page 145]). Since $\mathrm{Irr}(P_{s_3}\Psi\vartheta_1)$ is finite whereas $s_2^{q^n} - b$ is irreducible in $K[s_2^{\pm 1}]$ for all $n \geq 1$, we obtain $s_2^{q^n} - b$ is not invertible in $\mathcal{L}_{P_{s_3}\Psi\vartheta_1}(K[s_2^{\pm 1}])$ for infinitely many n. Thus we obtain the following result.

LEMMA 3.5. *There exists $b \in K$ such that $s_2^{q^n} - b$ is irreducible in $K[s_2^{\pm 1}]$ for all $n \geq 1$. Furthermore, for infinitely many n, $s_2^{q^n} - b$ is not invertible in $\mathcal{L}_{P_{s_3}\Psi\vartheta_1}(K[s_2^{\pm 1}])$.*

Choose $s_2^{q^n} - b$ an irreducible element in $K[s_2]$ subject to $s_2^{q^n} - b$ is not invertible in $\mathcal{L}_{P_{s_3}\Psi\vartheta_1}(K[s_2^{\pm 1}])$. Let c be an element of $\mathbb{F}_pA_1$ such that $c\vartheta = b$. Then $s_2^{q^n} - c$ is an irreducible element in $\mathbb{F}_pA_1[s_2]$. Hence $s_2^{q^n} - c$ is irreducible in $\mathbb{F}_pA_2$. It is easy to verify that $s_2^{q^n} - c$ is not invertible in $\mathcal{L}_{P_{s_3}\Psi}(\mathbb{F}_pA_2)$. Furthermore $s_2^{q^n} - c \nmid y$ for all $y \in P_{s_3}\Psi$, and π, $s_2^{q^n} - c$ are relatively prime elements in $\mathbb{F}_pA_2$.

Next we shall construct an element Δ of $\mathrm{SL}_2(\mathcal{L}_P(\mathbb{F}_pA_3)) \setminus \mathrm{E}_2(\mathcal{L}_P(\mathbb{F}_pA_3))$. The proof of the following result is based on some ideas given in the proof of Theorem C in [**8**].

LEMMA 3.6. *Let π be an irreducible element in $\mathbb{F}_pA_1$ subject to $\pi \nmid x$ for any element $x \in P_{s_3}\Psi$. Let $K = \mathbb{F}_pA_1/I$, where I is the ideal of $\mathbb{F}_pA_1$ generated by π. Let σ be an irreducible element in $\mathbb{F}_pA_2$ such that* (i) *π and σ are relatively prime in $\mathbb{F}_pA_2$,* (ii) *$\sigma \nmid x$ for any element $x \in P_{s_3}\Psi$ and* (iii) *$\sigma\widetilde{\vartheta}_1$ is not invertible in $\mathcal{L}_{P_{s_3}\Psi\vartheta_1}(K[s_2^{\pm 1}])$. Then, for $t \in \mathcal{L}_{P_{s_3}}(\mathbb{F}_pA_2[s_3])$ with $t\nu = 0$ and $t\widetilde{\Psi} \neq 0$, the matrix*

$$\Delta = \begin{pmatrix} 1 + \sigma\pi t^2 s_3^{-1} & -\sigma^2 t^2 s_3^{-1} \\ \pi^2 t^2 s_3^{-1} & 1 - \sigma\pi t^2 s_3^{-1} \end{pmatrix}$$

is an element of $\mathrm{SL}_2(\mathcal{L}_P(\mathbb{F}_pA_3)) \setminus \mathrm{E}_2(\mathcal{L}_P(\mathbb{F}_pA_3))$.

Proof. Throughout the proof, we write X for $\left(\begin{smallmatrix} 1 & 0 \\ 0 & s_3 \end{smallmatrix}\right)$. By Lemma 2.2, $\mathrm{SL}_2(Q) = \mathrm{SL}_2(\mathcal{O}) *_D \mathrm{SL}_2(\mathcal{O})^X$, where $D = \mathrm{SL}_2(\mathcal{O}) \cap \mathrm{SL}_2(\mathcal{O})^X$. Clearly $\Delta \in \mathrm{SL}_2(Q)$. Now,

$$\Delta = \begin{pmatrix} 1 & \sigma/\pi \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \pi^2 t^2 s_3^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & -\sigma/\pi \\ 0 & 1 \end{pmatrix}.$$

It is easily verified that $\left(\begin{smallmatrix} 1 & \pm\sigma/\pi \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}) \setminus D$ and $\left(\begin{smallmatrix} 1 & 0 \\ \pi^2 t^2 s_3^{-1} & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O})^X \setminus D$. The normal form theorem for the free products with amalgamation (see [**13**, Corollary 4.4.2]) implies that if $\Delta = g_1 g_2 \cdots g_r$, where the g_i are alternately in $\mathrm{SL}_2(\mathcal{O}) \setminus D$ and $\mathrm{SL}_2(\mathcal{O})^X \setminus D$, then $r = 3$, $g_1, g_3 \in \mathrm{SL}_2(\mathcal{O}) \setminus D$, and $g_2 \in \mathrm{SL}_2(\mathcal{O})^X \setminus D$. Note that π is not invertible in $\mathcal{L}_P(\mathbb{F}_pA_3)$. Indeed, let $w \in \mathcal{L}_P(\mathbb{F}_pA_3)$ such that $\pi w = 1$. Write $w = s_3^{w\nu} \frac{u}{\underset{\sim}{v}}$ for some $u \in \mathcal{L}_P(\mathbb{F}_pA_2[s_3])$ and $v \in P_{s_3}$. Since $\pi\nu = 0$, we obtain $w\nu = 0$. By applying $\widetilde{\Psi}$, we obtain π is invertible in $\mathcal{L}_{P_{s_3}\Psi}(\mathbb{F}_pA_2)$ which is a contradiction by our hypothesis. Let $B = \mathrm{SL}_2(\mathcal{L}_P(\mathbb{F}_pA_3)) \cap \mathrm{SL}_2(\mathcal{O})$, $\Gamma = \mathrm{SL}_2(\mathcal{L}_P(\mathbb{F}_pA_3)) \cap \mathrm{SL}_2(\mathcal{O})^X$ and $G = \langle B, \Gamma \rangle$. We claim that $\mathrm{E}_2(\mathcal{L}_P(\mathbb{F}_pA_3)) \leq G$. But

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in B,$$

and so

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -f & 1 \end{pmatrix},$$

for all $f \in \mathcal{L}_P(\mathbb{F}_pA_3)$. To show our claim, it is enough to prove that

$$\begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix} \in G$$

for all $f \in \mathcal{L}_P(\mathbb{F}_pA_3)$. Furthermore

$$\begin{pmatrix} 1 & 0 \\ s_3^{-1} & 1 \end{pmatrix} \in \Gamma \quad \text{and} \quad \begin{pmatrix} 1 & -s_3 \\ 0 & 1 \end{pmatrix} \in B,$$

and so

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ s_3^{-1} & 1 \end{pmatrix}\begin{pmatrix} 1 & -s_3 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ s_3^{-1} & 1 \end{pmatrix} = \begin{pmatrix} -s_3^{-1} & 0 \\ 0 & -s_3 \end{pmatrix} \in G.$$

Let $f \in \mathcal{L}_P(\mathbb{F}_pA_3)$ and let r be a positive integer such that $s_3^{2r}f \in \mathcal{L}_P(\mathbb{F}_pA_2[s_3])$. Since

$$\begin{pmatrix} 1 & s_3^{2r}f \\ 0 & 1 \end{pmatrix} \in G$$

we obtain

$$\begin{pmatrix} -s_3^{-r} & 0 \\ 0 & -s_3^{r} \end{pmatrix}\begin{pmatrix} 1 & s_3^{2r}f \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -s_3^{r} & 0 \\ 0 & -s_3^{-r} \end{pmatrix} = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix} \in G.$$

Thus $\mathrm{E}_2(\mathcal{L}_P(\mathbb{F}_pA_3)) \leq G$. Suppose that $\Delta \in \mathrm{E}_2(\mathcal{L}_P(\mathbb{F}_pA_3))$. Note that $B \cap D = \Gamma \cap D$. Since $\mathrm{E}_2(\mathcal{L}_P(\mathbb{F}_pA_3)) \leq G$, we may write $\Delta = g_1g_2\cdots g_r$ where the g_i are alternately in B and Γ, and no g_i lies in D. Thus by the normal form theorem for free products with amalgamation, we may write

$$\Delta = \begin{pmatrix} d & e \\ f & g \end{pmatrix}\begin{pmatrix} h & is_3 \\ js_3^{-1} & k \end{pmatrix}\begin{pmatrix} \ell & m \\ n & q \end{pmatrix},$$

where $d, e, f, g, h, i, j, k, \ell, m, n, q \in \mathcal{L}_{P_{s_3}}(\mathbb{F}_pA_2[s_3])$. Making the calculations, we obtain

$$\Delta = \begin{pmatrix} dh\ell + ejs_3^{-1}\ell + is_3dn + ekn & dhm + ejs_3^{-1}m + is_3dq + ekq \\ fh\ell + gjs_3^{-1}\ell + fis_3n + gkn & fhm + gjs_3^{-1}m + fis_3q + gkq \end{pmatrix}.$$

Therefore

$$1 + \sigma\pi t^2 s_3^{-1} = dh\ell + ejs_3^{-1}\ell + is_3dn + ekn \tag{18}$$

and so, we obtain from (18)

$$\sigma\pi t^2 = (-1 + dh\ell + ekn)s_3 + ej\ell + is_3^2dn. \tag{19}$$

By applying $\widetilde{\Psi}$ on (19), we obtain

$$\sigma\pi(t^2\widetilde{\Psi}) = (e\widetilde{\Psi})(j\widetilde{\Psi})(\ell\widetilde{\Psi}). \tag{20}$$

Similarly,

$$\pi^2(t^2\widetilde{\Psi}) = (g\widetilde{\Psi})(j\widetilde{\Psi})(\ell\widetilde{\Psi}). \tag{21}$$

Since $\mathcal{L}_{P_{s_3}\Psi}(\mathbb{F}_pA_2)$ is an integral domain, and by the choice of t, we obtain from (20) and (21)

$$\sigma(g\widetilde{\Psi}) = \pi(e\widetilde{\Psi}). \tag{22}$$

Write $g\widetilde{\Psi} = \frac{u}{t_1}$ and $e\widetilde{\Psi} = \frac{v}{t_1'}$, where $u, v \in \mathbb{F}_pA_2$ and $t_1, t_1' \in P_{s_3}\Psi$. Thus (22) becomes

$$\sigma u t_1' = v t_1 \pi.$$

By our hypothesis, (i) and (ii), and since $\mathbb{F}_pA_2$ is a UFD, we obtain σ divides v and π divides u. Therefore $g\widetilde{\Psi} = \pi e_1$ and $e\widetilde{\Psi} = \sigma e_2$, where $e_1, e_2 \in \mathcal{L}_{P_{s_3}\Psi}(\mathbb{F}_pA_2)$. Since $dg - ef = 1$, we have

$$(d\widetilde{\Psi})(g\widetilde{\Psi}) - (e\widetilde{\Psi})(f\widetilde{\Psi}) = 1$$

and so

$$(d\widetilde{\Psi})\pi e_1 - \sigma e_2(f\widetilde{\Psi}) = 1. \tag{23}$$

By applying $\widetilde{\vartheta}_1$ on (23), we obtain $\sigma\widetilde{\vartheta}_1$ is invertible in $\mathcal{L}_{P_{s_3}\Psi\vartheta_1}(K[s_2^{\pm 1}])$ which is a contradiction by (iii). Therefore $\Delta \in \mathrm{SL}_2(\mathcal{L}_P(\mathbb{F}_pA_3)) \setminus \mathrm{E}_2(\mathcal{L}_P(\mathbb{F}_pA_3))$.

4. A construction of non-tame automorphisms. It is well-known (see, for instance, [**13**, Section 3.6, Theorem N4]) that $\mathrm{IA}(F_3)$ is generated by the following automorphisms K_{ij} and K_{ijk}, where $i, j, k \in \{1, 2, 3\}$, satisfying the conditions

$$\begin{aligned} (f_i)K_{ij} &= f_j^{-1} f_i f_j && \text{for } i \neq j \\ (f_m)K_{ij} &= f_m && \text{if } m \neq i \end{aligned}$$

and

$$\begin{aligned} (f_i)K_{ijk} &= f_i[f_j, f_k] && \text{for } i \neq j < k \neq i \\ (f_m)K_{ijk} &= f_m && \text{if } m \neq i. \end{aligned}$$

The natural mapping from F_3 onto M_3 induces a group homomorphism, say α, from $\mathrm{Aut}(F_3)$ into $\mathrm{Aut}(M_3)$. We write τ for the restriction of α on $\mathrm{IA}(F_3)$. It is easily verified that the image of τ is equal to $T \cap \mathrm{IA}(M_3)$. It is generated by $\tau_{ij} = K_{ij}\tau$ for all $i \neq j$ and $\tau_{ijk} = K_{ijk}\tau$ for $i \neq j < k \neq i$. Thus $x_i\tau_{ij} = x_j^{-1}x_ix_j$ for $i \neq j$, $x_m\tau_{ij} = x_m$ if $m \neq i$, and $x_i\tau_{ijk} = x_i[x_j, x_k]$ for $i \neq j < k \neq i$ and $x_m\tau_{ijk} = x_m$ if $m \neq i$. Note that $\tau_{ijk}^{-1} = \tau_{ikj}$. Define $\mathcal{T} = \{\tau_{ij}, \tau_{ijk} : i \neq j < k \neq i\}$. Thus $\mathcal{T}$ is a generating set of $T \cap \mathrm{IA}(M_3)$. Recall that we have the following short exact sequence

$$1 \to \ker\rho_1 \to T \cap \mathrm{IA}(M_3) \xrightarrow{\rho_1} A_3 \to 1,$$

where $\phi\rho_1 = \det J_\phi = s_1^{\mu_1}s_2^{\mu_2}s_3^{\mu_3}$, $\mu_1, \mu_2, \mu_3 \in \mathbb{Z}$. Note that $\tau_{31}^{-1}\tau_{21}, \tau_{32}^{-1}\tau_{12}, \tau_{23}^{-1}\tau_{13} \in \ker\rho_1$. Write $\mathcal{Q} = \{\tau_{123}, \tau_{213}, \tau_{312}, \tau_{31}^{-1}\tau_{21}, \tau_{32}^{-1}\tau_{12}, \tau_{23}^{-1}\tau_{13}, (\tau_{ij}, \tau_{\mu\nu}), (\tau_{\alpha\beta\gamma}, \tau_{\kappa\ell m}), (\tau_{\alpha\beta\gamma}, \tau_{ij}) : i \neq j, \mu \neq \nu, \alpha \neq \beta < \gamma \neq \alpha, \kappa \neq \ell < m \neq \kappa\}$.

Lemma 4.1. *The kernel of ρ_1 is finitely generated by $\mathcal{Q}$ as a group on which $T \cap \mathrm{IA}(M_3)$ acts by conjugation.*

Proof. Let $N_{\mathcal{Q}}$ be the normal closure of $\mathcal{Q}$ in $T \cap \mathrm{IA}(M_3)$, that is, the intersection of all normal subgroups of $T \cap \mathrm{IA}(M_3)$ containing $\mathcal{Q}$. It is easy to show that $N_{\mathcal{Q}}$ is generated by the set $\{\gamma^{-1}x\gamma : x \in \mathcal{Q}, \gamma \in T \cap \mathrm{IA}(M_3)\}$. We claim that $N_{\mathcal{Q}} = \ker\rho_1$. Since $\mathcal{Q} \subseteq \ker\rho_1$ and $\ker\rho_1$ is normal in $T \cap \mathrm{IA}(M_3)$, it is enough to show that $\ker\rho_1 \subseteq N_{\mathcal{Q}}$. For the next few lines, we set $E = T \cap \mathrm{IA}(M_3)$. Since E/E' is finitely presented and E is finitely generated, we obtain E' is finitely generated as a group on which E acts by conjugation. In fact, E' is generated by the set $\{(\tau_{ij}, \tau_{\mu\nu}), (\tau_{\alpha\beta\gamma}, \tau_{\kappa\ell m}), (\tau_{\alpha\beta\gamma}, \tau_{ij}) : i \neq j, \mu \neq \nu, \alpha \neq \beta < \gamma \neq \alpha, \kappa \neq \ell < m \neq \kappa\}$ as a group on which E acts by conjugation. Thus $E' \subseteq N_{\mathcal{Q}}$. Note that $E/N_{\mathcal{Q}}$ is an abelian group generated by 3 elements. Since

$$(E/N_{\mathcal{Q}})/(\ker\rho_1/N_{\mathcal{Q}}) \cong E/\ker\rho_1$$

and $E/\ker\rho_1$ is a free abelian group of rank 3, we obtain $\ker\rho_1 \subseteq N_{\mathcal{Q}}$. Therefore $\ker\rho_1 = N_{\mathcal{Q}}$.

In the Appendix, we write down all $J_\phi = (a_{ij})$ for $\phi \in \mathcal{T} \cup \mathcal{Q}$ subject to $a_{13} \neq 0$ or $a_{23} \neq 0$. For simplicity, we write (J_ϕ, a_{13}, a_{23}) for $\phi \in \mathcal{T} \cup \mathcal{Q}$. Let P be the multiplicative monoid generated by $\mathbb{F}_p \setminus \{0\}$, $\{s_1^{\pm1}, s_2^{\pm1}, s_3^{\pm1}\}$, $s_1 - 1, s_2 - 1, s_3 - 1$, and $\delta_1, \ldots, \delta_5$ (see Appendix). Recall that for any element $u = \sum_i m_i r_i \in \mathbb{F}_p A_3$, with $m_i \in \mathbb{F}_p$ and $r_i \in A_3$, $u^* = \sum_i m_i r_i^{-1}$, and $(u^*)^* = u$. Furthermore, for $w \in M_3'$ and $u \in \mathbb{F}_p A_3$, $d_j(w^u) = u^* d_j(w)$ for $j = 1, 2, 3$. Notice that $P_{s_3}\Psi$ is the multiplicative monoid generated by $\mathbb{F}_p \setminus \{0\}$, $\{s_1^{\pm1}, s_2^{\pm1}\}$, $s_1 - 1, s_2 - 1$.

THEOREM 4.2. *Let π be an irreducible element in $\mathbb{F}_p A_1$ subject to $\pi \nmid x$ for any element $x \in P_{s_3}\Psi$. Let $K = \mathbb{F}_p A_1/I$, where I is the ideal of $\mathbb{F}_p A_1$ generated by π. Let σ be an irreducible element in $\mathbb{F}_p A_2$ such that* (i) *π and σ are relatively prime in $\mathbb{F}_p A_2$,* (ii) *$\sigma \nmid x$ for any element $x \in P_{s_3}\Psi$ and* (iii) *$\sigma\widetilde{\vartheta}_1$ is not invertible in $\mathcal{L}_{P_{s_3}\Psi\vartheta_1}(K[s_2^{\pm1}])$. Then, for $t \in \mathcal{L}_{P_{s_3}}(\mathbb{F}_p A_2[s_3])$ with $tv = 0$ and $t\widetilde{\Psi} \neq 0$, the automorphism ϕ of M_3 satisfying the conditions*

$$\begin{aligned}
x_1\phi &= x_1\\
x_2\phi &= x_2\ \ [x_3, x_1]^{(s_1 s_2^{-1}\sigma^2)^*}\ \ [x_2, x_1]^{(-s_1 s_3^{-1}(s_1-1)\sigma\pi)^*}\\
x_3\phi &= x_3\ \ [x_3, x_1]^{(s_1 s_3^{-1}(s_1-1)\sigma\pi)^*}\ \ [x_2, x_1]^{(-s_1 s_2 s_3^{-2}(s_1-1)^2\pi^2)^*}
\end{aligned}$$

is non-tame.

Proof. Since M_3 is a free group in the variety $\mathfrak{V}_p$ with a free generating set $\{x_1, x_2, x_3\}$, ϕ extends uniquely to a group homomorphism of M_3. Write $b_i = s_i - 1$ for $i = 1, 2, 3$. Using the equations (9), (10), (11) and (13), we calculate $d_j(x_i\phi)$, with $i, j \in \{1, 2, 3\}$, and so, the Jacobian matrix J_ϕ becomes

$$J_\phi = \begin{pmatrix} 1 & 0 & 0\\ \sigma^2 b_3 s_3^{-1} - \sigma\pi b_1 b_2 s_3^{-1} & 1 + \sigma\pi b_1^2 s_3^{-1} & -\sigma^2 b_1 s_3^{-1}\\ -\pi^2 b_1^2 b_2 s_3^{-1} + \sigma\pi b_1 b_3 s_3^{-1} & \pi^2 b_1^3 s_3^{-1} & 1 - \sigma\pi b_1^2 s_3^{-1} \end{pmatrix}.$$

Since $\det J_\phi = 1$ and the rows of J_ϕ satisfy the conditions (15), we obtain $J_\phi \in \mathrm{Im}\zeta$. Since ζ is a group monomorphism, we get $\phi \in \mathrm{IA}(M_3)$. To get a contradiction, we assume that ϕ is tame. Since $\phi \in T \cap \mathrm{IA}(M_3)$ and $\det J_\phi = 1$, we obtain $\phi \in \ker\rho_1$. To get its image in $\mathrm{GL}_2(\mathcal{L}_S(\mathbb{F}_p A_3))$ we conjugate it by

$$(c_{ij}) = \begin{pmatrix} b_1 & 0 & 0\\ b_2 & b_1^{-1} & 0\\ b_3 & 0 & 1 \end{pmatrix}$$

which implies that

$$\Delta = \begin{pmatrix} 1+\sigma\pi b_1^2 s_3^{-1} & -\sigma^2 b_1^2 s_3^{-1} \\ \pi^2 b_1^2 s_3^{-1} & 1-\sigma\pi b_1^2 s_3^{-1} \end{pmatrix} \in (\ker\rho_1)\eta.$$

By Lemma 3.2 (for $H = T \cap \mathrm{IA}(M_3)$ and $N = \ker\rho_1$), $\Delta \in \mathrm{E}_2(\mathcal{L}_P(\mathbb{F}_p A_3))$. But, by Lemma 3.6, $\Delta \in \mathrm{SL}_2(\mathcal{L}_P(\mathbb{F}_p A_3)) \setminus \mathrm{E}_2(\mathcal{L}_P(\mathbb{F}_p A_3))$ and so, ϕ is a non-tame automorphism of M_3.

Examples 4.3. We shall give a family of examples of non-tame automorphisms of M_3 for $p=3$. It is enough to construct irreducible elements π and σ in $\mathbb{F}_3 A_2$ subject to all conditions of Theorem 4.2 are satisfied. The polynomial $\pi = s_1^3 - s_1 - 1$ is irreducible in $\mathbb{F}_3[s_1]$. It is easily verified that $\pi \notin P_{s_3}\Psi$. By Remark 3.4, $\pi \nmid x$ for all $x \in P_{s_3}\Psi$. Let I be the ideal in $\mathbb{F}_3 A_1$ generated by π, and let $K = \mathbb{F}_3 A_1/I$. Then K is a field of 27 elements. Let $q = 13$. It is easily verified that $s_1^2 - 1 \notin I$. Let $b = s_1 + I$. Since the polynomial $s_2^{13} - b$ has no root in K, we obtain $s_2^{13^n} - b$ is irreducible in $K[s_2]$ for all $n \geq 1$ (see [**12**, Theorem 3.75 and page 145]). The natural mapping ϑ from $\mathbb{F}_3 A_1$ onto K induces a ring epimorphism ϑ_1 from $\mathbb{F}_3 A_2$ onto $K[s_2^{\pm 1}]$ in a natural way. Since $P_{s_3}\Psi\vartheta_1$ is a multiplicative closed subset of $K[s_2^{\pm 1}]$, and $0 \notin P_{s_3}\Psi\vartheta_1$, the epimorphism ϑ_1 induces a ring epimorphism $\widetilde{\vartheta}_1$ from $\mathcal{L}_{P_{s_3}\Psi}(\mathbb{F}_3 A_2)$ onto $\mathcal{L}_{P_{s_3}\Psi\vartheta_1}(K[s_2^{\pm 1}])$ by defining $\frac{u}{v}\widetilde{\vartheta}_1 = \frac{u\vartheta_1}{v\vartheta_1}$ for all $u \in \mathbb{F}_3 A_2$ and $v \in P_{s_3}\Psi$. But $s_2^{13^n} - b \notin P_{s_3}\Psi\vartheta_1$ and $s_2^{13^n} - b$ is not invertible in $\mathcal{L}_{P_{s_3}\Psi\vartheta_1}(K[s_2^{\pm 1}])$ for all n. Write $\sigma_n = s_2^{13^n} - s_1$. It is easy to verify that σ_n is irreducible in $\mathbb{F}_3 A_2$. In addition, $\sigma_n \nmid y$ for all $y \in P_{s_3}\Psi$, and π and σ_n are relatively prime in $\mathbb{F}_3 A_2$. Thus, for all $n \geq 1$, π and σ_n satisfy all the conditions of Theorem 4.2.

In the next few lines, we shall prove that the IA-automorphism group of M_3 is not finitely generated. Although the aforementioned result was stated in [**16**], we shall apply the aforementioned method to fill a gap to complete the proof. To get a contradiction, we assume that $\mathrm{IA}(M_3)$ is finitely generated. We have the following short exact sequence

$$1 \to \ker\rho_2 \to \mathrm{IA}(M_3) \xrightarrow{\rho_2} A_3 \to 1,$$

where $\phi\rho_2 = \det J_\phi = s_1^{\mu_1} s_2^{\mu_2} s_3^{\mu_3}$, $\mu_1, \mu_2, \mu_3 \in \mathbb{Z}$. Applying Lemma 3.2 for $H = \mathrm{IA}(M_3)$ and $N = \ker\rho_2$, there exists a multiplicative monoid P of $\mathbb{F}_p A_3$ such that $(d_{ij}) \in \mathrm{E}_2(\mathcal{L}_P(\mathbb{F}_p A_3))$ for all $(d_{ij}) \in (\ker\rho_2)\eta$. By the proof of Lemma 3.2 (and Remark 3.4), we may choose a (monic) irreducible polynomial π of degree m in $\mathbb{F}_p[s_1]$ subject to $\pi \nmid x$ for all $x \in P_{s_3}\Psi$, and there exists q an odd prime divisor of $p^m - 1$. Let I be the ideal of $\mathbb{F}_p A_1$ generated by π. By Lemma 2.5, $K = \mathbb{F}_p A_1/I$ is a field of p^m elements. By Lemma 3.5, there exists $b \in K$ such that $s_2^{q^n} - b$ is irreducible in $K[s_2^{\pm 1}]$ for all $n \geq 1$, and, for infinitely many n, $s_2^{q^n} - b$ is not invertible in $\mathcal{L}_{P_{s_3}\Psi\vartheta_1}(K[s_2^{\pm 1}])$. The natural mapping ϑ from $\mathbb{F}_p A_1$ onto K induces a ring epimorphism ϑ_1 from $\mathbb{F}_p A_2$ onto $K[s_2^{\pm 1}]$ in a natural way. Since $P_{s_3}\Psi\vartheta_1$ is a multiplicative closed subset of $K[s_2^{\pm 1}]$, and $0 \notin P_{s_3}\Psi\vartheta_1$, the epimorphism ϑ_1 induces a ring epimorphism $\widetilde{\vartheta}_1$ from $\mathcal{L}_{P_{s_p}\Psi}(\mathbb{F}_p A_2)$ onto $\mathcal{L}_{P_{s_3}\Psi\vartheta_1}(K[s_2^{\pm 1}])$ by defining $\frac{u}{v}\widetilde{\vartheta}_1 = \frac{u\vartheta_1}{v\vartheta_1}$ for all $u \in \mathbb{F}_p A_2$ and $v \in P_{s_3}\Psi$. Choose $s_2^{q^n} - b$ an irreducible element in $K[s_2]$ subject to $s_2^{q^n} - b$ is not invertible in $\mathcal{L}_{P_{s_3}\Psi\vartheta_1}(K[s_2^{\pm 1}])$. Let

c be an element of $\mathbb{F}_pA_1$ such that $c\vartheta = b$. Then $\sigma = s_2^{q^n} - c$ is an irreducible element in $\mathbb{F}_pA_1[s_2]$. Hence σ is irreducible in $\mathbb{F}_pA_2$. Furthermore $\sigma \nmid y$ for all $y \in P_{s_3}\Psi$. It is easily verified that π and σ are relatively prime elements in $\mathbb{F}_pA_2$. Let

$$(a_{ij}) = \begin{pmatrix} 1 & 0 & 0 \\ \sigma^2 b_3 s_3^{-1} - \sigma\pi b_1 b_2 s_3^{-1} & 1 + \sigma\pi b_1^2 s_3^{-1} & -\sigma^2 b_1 s_3^{-1} \\ -\pi^2 b_1^2 b_2 s_3^{-1} + \sigma\pi b_1 b_3 s_3^{-1} & \pi^2 b_1^3 s_3^{-1} & 1 - \sigma\pi b_1^2 s_3^{-1} \end{pmatrix}.$$

Since $\det(a_{ij}) = 1$ and the rows of (a_{ij}) satisfy the conditions (15), we obtain $(a_{ij}) \in (\ker\rho_2)\zeta$. Since ζ is a group monomorphism, there exists $\phi \in \ker\rho_2$ such that $(a_{ij}) = J_\phi$. To get its image in $\mathrm{GL}_2(\mathcal{L}_S(\mathbb{F}_pA_3))$, we conjugate it by

$$(c_{ij}) = \begin{pmatrix} b_1 & 0 & 0 \\ b_2 & b_1^{-1} & 0 \\ b_3 & 0 & 1 \end{pmatrix}$$

which implies that

$$\Delta = \begin{pmatrix} 1 + \sigma\pi b_1^2 s_3^{-1} & -\sigma^2 b_1^2 s_3^{-1} \\ \pi^2 b_1^2 s_3^{-1} & 1 - \sigma\pi b_1^2 s_3^{-1} \end{pmatrix} \in (\ker\rho_2)\eta.$$

Thus, by Lemma 3.2, Δ is an element of $\mathrm{E}_2(\mathcal{L}_P(\mathbb{F}_pA_3))$. By Lemma 3.6, $\Delta \in \mathrm{SL}_2(\mathcal{L}_P(\mathbb{F}_pA_3)) \setminus \mathrm{E}_2(\mathcal{L}_P(\mathbb{F}_pA_3))$ which is a contradiction. Therefore $\mathrm{IA}(M_3)$ is not a finitely generated group.

Appendix

$\big(J_{\tau_{13}}, s_3^{-1}(s_1-1), 0\big)$, $\big(J_{\tau_{23}}, 0, s_3^{-1}(s_2-1)\big)$, $\big(J_{\tau_{123}}, s_1 s_2^{-1} s_3^{-1}(s_2-1), 0\big)$,

$\big(J_{\tau_{213}}, 0, s_1^{-1} s_2 s_3^{-1}(s_1-1)\big)$, $\big(J_{\tau_{23}^{-1}\tau_{13}}, s_3^{-1}(s_1-1), 1-s_2\big)$, $(J_{(\tau_{12},\tau_{13})}, (1-s_1)(s_2-1), 0)$,

$\big(J_{(\tau_{12},\tau_{23})}, s_3^{-1}(s_1-1)(s_2-1), 0\big)$, $\big(J_{(\tau_{12},\tau_{123})}, -s_1 s_2^{-1} s_3^{-1}(s_2-1)^2, 0\big)$,

$\big(J_{(\tau_{12},\tau_{213})}, s_1^{-1} s_2 s_3^{-1}(s_1-1)^2\big(1-(s_1^{-1}-1)(s_3^{-1}-1)\big), s_1^{-2} s_2 s_3^{-2}(s_1-1)^2(s_3-1)\big)$,

$\big(J_{(\tau_{13},\tau_{21})}, 0, s_3^{-1}(s_1-1)(1-s_2)\big)$, $\big(J_{(\tau_{13},\tau_{31})}, -s_1^{-1} s_3^{-1}(s_1-1)^2, 0\big)$,

$\big(J_{(\tau_{13},\tau_{32})}, -s_2^{-1}(s_1-1)(s_2-1), 0\big)$, $\big(J_{(\tau_{13},\tau_{123})}, s_1 s_2^{-1} s_3^{-1}(1-s_2)(s_3-1), 0\big)$,

$\big(J_{(\tau_{13},\tau_{213})}, 0, s_1^{-1} s_2 s_3^{-2}(s_3-1)(s_1-1)\big)$, $\big(J_{(\tau_{13},\tau_{312})}, -s_1^{-1} s_2^{-1}(s_1-1)^2(s_2-1), 0\big)$,

$(J_{(\tau_{21},\tau_{23})}, 0, -(s_1-1)(s_2-1))$,

$\big(J_{(\tau_{21},\tau_{123})}, s_1 s_2^{-2} s_3^{-2}(s_2-1)^2(s_3-1), s_1 s_2^{-1} s_3^{-1}(s_2-1)^2(1-(s_2^{-1}-1)(s_3^{-1}-1)\big)\big)$,

$\big(J_{(\tau_{21},\tau_{213})}, 0, -s_1^{-1} s_2 s_3^{-1}(s_1-1)^2\big)$, $\big(J_{(\tau_{23},\tau_{31})}, 0, s_1^{-1}(s_2-1)(1-s_1)\big)$,

$\big(J_{(\tau_{23},\tau_{32})}, 0, -s_2^{-1} s_3^{-1}(s_2-1)^2\big)$,

$\big(J_{(\tau_{23},\tau_{123})}, s_1 s_2^{-1} s_3^{-2}(s_2-1)(s_3-1), 0\big)$, $\big(J_{(\tau_{23},\tau_{213})}, 0, s_1^{-1} s_2 s_3^{-1}(s_1-1)(1-s_3)\big)$,

$\big(J_{(\tau_{23},\tau_{312})}, 0, s_1^{-1} s_2^{-1}(s_1-1)(s_2-1)^2\big)$,

https://doi.org/10.1017/S0017089507003801 Published online by Cambridge University Press

$$\big(J_{(\tau_{31},\tau_{123})}, s_1 s_2^{-1} s_3^{-1}(1-s_2)\big(s_1^{-1}(1-s_1)+s_2^{-1}s_3^{-1}(s_2-1)(s_3-1)\big), 0\big),$$
$$\big(J_{(\tau_{31},\tau_{213})}, 0, s_1^{-2}s_2 s_3^{-1}(s_1-1)^2\big), \big(J_{(\tau_{32},\tau_{123})}, s_1 s_2^{-2} s_3^{-1}(s_2-1)^2, 0\big),$$
$$\big(J_{(\tau_{32},\tau_{213})}, 0, s_1^{-1}s_2 s_3^{-1}(1-s_1)\big(s_2^{-1}(1-s_2)+s_1^{-1}s_3^{-1}(s_1-1)(s_3-1)\big)\big),$$
$$\big(J_{(\tau_{123},\tau_{213})}, -s_3^{-2}(s_1-1)(s_3-1)+s_1 s_2^{-1}s_3^{-3}(s_2-1)(s_3-1)^2-s_3^{-4}(s_1-1)(s_3-1)^3,$$
$$-s_1^{-1}s_2 s_3^{-3}(s_3-1)^2(s_1-1)+s_3^{-2}(s_2-1)(s_3-1)\big)$$
$$\big(J_{(\tau_{123},\tau_{312})}, -s_1 s_2^{-3}s_3^{-1}(s_2-1)^3, 0\big), \big(J_{(\tau_{213},\tau_{312})}, 0, s_1^{-3}s_2 s_3^{-1}(s_1-1)^3\big),$$

Set

$$\delta_1 = 1+s_3,$$
$$\delta_2 = s_2(s_1-1)(s_3-1)-s_1 s_3(s_2-1),$$
$$\delta_3 = s_2 s_3(1-s_1)+s_1(s_2-1)(s_3-1),$$
$$\delta_4 = s_1 s_3(1-s_2)+s_2(s_1-1)(s_3-1)$$

and

$$\delta_5 = 2s_1 s_2 s_3^2(s_1-1)(s_2-1)-s_1^2 s_3(s_2-1)^2(s_3-1)$$
$$+s_1 s_2(s_1-1)(s_2-1)(s_3-1)^2-s_2^2 s_3(s_1-1)^2(s_3-1).$$

REFERENCES

1. W. A. Adkins and S. H. Weintraub, *Algebra: an approach via module theory*, Graduate Texts in Mathematics No. 136 (Springer-Verlag 1992).

2. S. Bachmuth, Automorphisms of free metabelian groups, *Trans. Amer. Math. Soc*. **118** (1965), 93–104.

3. S. Bachmuth, Automorphisms of a class of metabelian groups, *Trans. Amer. Math. Soc*. **127** (1967), 284–293.

4. S. Bachmuth and H. Y. Mochizuki, $E_2 \neq SL_2$ for most Laurent polynomial rings, *Amer. J. Math. (6)* **104** (1981), 1181–1189.

5. S. Bachmuth and H. Y. Mochizuki, The nonfinite generation of Aut(G), G free metabelian of rank 3, *Trans. Amer. Math. Soc.* **270** (1982), 693–700.

6. O. Chein, IA-automorphisms of free and free metabelian groups, *Comm. Pure Appl. Math.* **21** (1968), 605–629.

7. N. D. Gupta, *Free group rings*, Contemp. Math. No. 66 (American Mathematical Society 1987).

8. M. J. Evans, Primitive elements in the free metabelian group of rank 3, *J. Algebra* **220** (1999), 475–491.

9. R. H. Fox, Free differential calculus I, *Annals of Math* **57** (1953), 547–560.

10. P. Hall, Finiteness conditions for soluble groups, *Proc. London Math. Soc. (3)* **4** (1954), 419–436.

11. A. F. Krasnikov, Nilpotent subgroups of relatively free groups, (Russian) *Algebra i Logika (4)* **17** (1978), 389–401; translation in *Algebra and Logic (4)* **17** (1978), 263–270.

12. R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications Vol. 20 (Addison-Wesley Publ. Company 1983).

13. W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory* (Dover Publications, Inc., New York 1976).

14. H. Neumann, *Varieties of groups* (Springer-Verlag 1967).

15. I. Niven, H. Zuckerman and H. Montgomery, *An introduction to the theory of numbers*, Fifth Edition (John Wiley & Sons, 1991).

16. A. I. Papistas, Automorphisms of metabelian groups, *Canad. Math. Bull*. **41** (1998), 98–104.

17. V. A. Roman'kov, Primitive elements of free groups of rank 3, *Math. Sb.* **182** (1991), 1074–1085; (English transl.) Math. USSR-Sb. **73** (1992), 445–454.

18. S. K. Sehgal, *Topics in group rings*, Pure and Applied Mathematics, Vol. 50 (Marcel Dekker 1978).

19. J-P. Serre, *Trees* (Springer-Verlag, 1980).

20. A. A. Suslin, On the structure of the special linear group over polynomial rings, *Izv. Akad. Nauk*. **11** (1974), 221–238.