Compositio Math. 141 (2005) 1213–1237
doi:10.1112/S0010437X05001296

Automorphism groups for p-cyclic covers of the affine line

Claus Lehr and Michel Matignon

Abstract

Let k be an algebraically closed field of positive characteristic $p > 0$ and $C \to \mathbb{P}^1_k$ a p-cyclic cover of the projective line ramified in exactly one point. We are interested in the p-Sylow subgroups of the full automorphism group $\mathrm{Aut}_k C$. We prove that for curves C with genus 2 or higher, these groups are exactly the extensions of a p-cyclic group by an elementary abelian p-group. The main tool is an efficient algorithm to compute the p-Sylow subgroups of $\mathrm{Aut}_k C$ starting from an Artin–Schreier equation for the cover $C \to \mathbb{P}^1_k$. We also characterize curves C with genus $g_C \geqslant 2$ and a p-group action $G \subset \mathrm{Aut}_k C$ such that $2p/(p-1) < |G|/g_C$ and $4/(p-1)^2 \leqslant |G|/g_C^2$. Our methods rely on previous work by Stichtenoth whose approach we have adopted.

1. Introduction

When considering semi-stable models for p-cyclic covers of the projective line over a p-adic field K with an algebraically closed residue field k, we obtain as irreducible components of the special fiber p-cyclic étale covers of the affine line (see [Leh01, Mat03]). An interesting object in arithmetic geometry is the monodromy, i.e. the minimal Galois extension K'/K such that a semi-stable model is defined over K'. A general result (see [Des86, Liu02, Theorem 4.44, p. 551]) asserts that $\mathrm{Gal}(K'/K)$ acts faithfully on the special fiber of the semi-stable model as an automorphism group; so the complexity of the monodromy group is intimately related with the automorphism group of p-cyclic covers of the affine line over the residue field k. The aim of this paper is first to report on and then to complete the literature on the subject (cf. [Sti73a, Sti73b, Sin74, Hen78, BS86, Bra88, Nak87, vdGV92, Elk99]). We do this with the objective to use the results to study the monodromy group which occurs when considering p-cyclic covers of the projective line over a p-adic field (see [LM02, LM04]).

Our choice to disjoin this paper from the one on monodromy came from the new interest in automorphism groups of curves (see [CKK01, CK03, Gur03, Kon99, Leo96, Poo00a, Poo00b, vdPV03, vdPV04], etc.).

In the following theorem we have gathered the main results proved in the paper.

Theorem 1.1. *Let k be an algebraically closed field of characteristic $p > 0$ and $f(X) \in k[X]$ a polynomial of degree $m := \deg f$ prime to p. Let $k(X,W)/k(X)$ be an extension of degree p defined by $W^p - W = f(X)$ and denote by ∞ the place in $k(X,W)$ above $X = \infty$. We denote by $g(f) = (m-1)(p-1)/2$ the genus of $k(X,W)/k$ and assume $g(f) \geqslant 2$. Let $\mathrm{Aut}_k k(X,W)$ be the full automorphism group, $G_\infty(f) \subset \mathrm{Aut}_k k(X,W)$ the inertia group at ∞ and $G_{\infty,1}(f)$ the wild*

Received 11 December 2003, accepted in final form 1 July 2004, published online 1 September 2005.
2000 Mathematics Subject Classification 14H37, 14H10.
Keywords: automorphisms of curves, families of curves, Artin–Schreier covers, extraspecial groups.
Work supported in part by the European Community's Human Potential Programme under Contract HPRN-CT-2000-00114, GTEM.
This journal is © Foundation Compositio Mathematica 2005.

inertia group at ∞. Let $\rho \in G(f)$ be such that $\rho(X) = X$ and $\rho(W) = W + 1$; then ρ generates a p-cyclic subgroup in $G_\infty(f)$.

I. (a) *The group $G_{\infty,1}(f)$ is a p-Sylow subgroup of $\mathrm{Aut}_k k(X, W)$; moreover, outside of a small number of cases it is normal (see § 3).*

(b) *The group $G_{\infty,1}(f)$ is an extension*[1] *(necessarily central) of $\langle\rho\rangle \simeq \mathbb{Z}/p\mathbb{Z}$ by a elementary abelian p-group $(\mathbb{Z}/p\mathbb{Z})^t$ which is a subgroup of translations $X \to X + y$ of the affine line $\mathbb{A}^1_k$ (see § 3).*

(c) *Conversely any extension of $\mathbb{Z}/p\mathbb{Z}$ by an elementary abelian group $(\mathbb{Z}/p\mathbb{Z})^t$ with $t \geqslant 0$ is obtained in this way (see Theorem 7.1).*

II. (a) *$|G_{\infty,1}(f)| \leqslant p(m-1)^2$, i.e. $|G_{\infty,1}(f)|/g(f)^2 \leqslant 4p/(p-1)^2$ (see [Sti73b, Satz 4] and Proposition 6.6).*

(b) *If $(m-1, p) = 1$ then $|G_{\infty,1}(f)| = p$ (see [Sti73b, Satz 4] and Proposition 6.6).*

(c) *If $f(X) = X^m$ then $|G_{\infty,1}(f)| = p$ for $m - 1 \neq p^s$ and $|G_{\infty,1}(f)| = p^{2s+1}$ for $m - 1 = p^s$ (see [Sti73b, Satz 5] and Proposition 6.6).*

(d) *If $m - 1 = \ell p^s$, $s > 0$, $\ell > 1$, $(\ell, p) = 1$, then $|G_{\infty,1}(f)| \leqslant p^{s+1}$ for $p > 2$ and $|G_{\infty,1}(f)| \leqslant 2^s$ for $p = 2$; moreover, these bounds are optimal (see Proposition 6.6).*

(e) *One has $p/(p-1) < |G_{\infty,1}(f)|/g(f)$ ($\frac{2}{3}$ for $p = 2$) if and only if $f(X) = XS(X)$, where $S(X) - S(0)$ is an additive polynomial (see Proposition 8.3).*

(f) *Let C be a nonsingular projective curve over k of genus $g_C \geqslant 2$ and G a p-subgroup of $\mathrm{Aut}_k C$. We assume that $2p/(p-1) < |G|/g_C$. Then $4/(p-1)^2 \leqslant |G|/g_C^2$ if and only if C is birational to a curve $W^p - W = f(X)$ where $f(X) = XS(X)$ and $S(X) - S(0)$ is an additive polynomial. Moreover, either $|G|/g_C^2 = 4p/(p-1)^2$ and the group G is then equal to the group $G_{\infty,1}(f)$ or $|G|/g_C^2 = 4/(p-1)^2$ and the group G is then equal to an index p-subgroup of the group $G_{\infty,1}(f)$.*

This paper is organized as follows. In § 3 we give the structure of p-Sylow subgroups of $\mathrm{Aut}_k k(X, W)$. Section 4 is a group theoretic section: we give a description of extensions of a p-cyclic group by any elementary abelian p-group as a saturated subgroup of those extensions for which the center is p-cyclic; the latter extensions are the so-called extraspecial groups. This description seems to be missing in the literature and is adapted to the realization result we have in mind (see Theorem 1.1 I(c) above). Section 5 gives a lemma for the calculation of the group of translations of the affine line occurring in Theorem 1.1 I(b) and for the structure of $G_{\infty,1}(f)$. An algorithm is presented and then applied to a concrete example $f(X) \in \mathbb{F}_2[X]$ for which $G_{\infty,1}(f)$ is the dihedral group D_8 of order 8. In § 6 we develop the notion of modification of covers. One type, which corresponds to a base change by a cover of the affine line by itself, has the effect to enlarge the group $G_{\infty,1}(f)$. A second type of modification is presented which has the property to limit the order of the group. We then give bounds for the size of the group $G_{\infty,1}(f)$ and show that they are sharp. In § 7 we realize extensions of p-cyclic by elementary abelian p-groups as groups $G_{\infty,1}(f)$. It is noticeable that one type of extraspecial group (namely the central product of copies of D_8 in characteristic 2) is particularly difficult to realize explicitly. We apply the method to give a realization of D_8 with minimal conductor. Section 8 describes the p-cyclic covers of the line which maximalize the ratio $|G_{\infty,1}(f)|/g(f)^2$. They correspond to a special locus in the moduli spaces of curves describing the 'big' actions of p-groups on curves in characteristic $p > 0$, a first step towards a classification.

[1] Concerning extensions we use the terminology of [Suz82, ch. 2, § 7].

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

2. Notation

Throughout this paper we use the following notation.

- k is an algebraically closed field of characteristic $p > 0$.
- F denotes the Frobenius endomorphism for a k-algebra.
- $k\{\mathrm{F}\}$ denotes the k-subspace of $k[X]$ generated by the polynomials $\mathrm{F}^i(X), i = 0, 1, 2, \ldots$; it is a ring under the composition and for $\alpha \in k$, $\mathrm{F}\alpha = \alpha^p\mathrm{F}$. The elements in $k\{\mathrm{F}\}$ are the additive polynomials, i.e. those $P \in k[X]$ such that $P(\alpha + \beta) = P(\alpha) + P(\beta)$ for $\alpha, \beta \in k$. Moreover, a separable polynomial in $k[X]$ is additive if and only if the set of its roots $Z(P)$ is a subgroup of k (see [Gos96, ch. 1]).
- For $f(X) \in k[X]$ the equation $W^p - W = f(X)$ defines an étale cover of the affine line that we denote by C_f and each étale cover of the affine line can be presented like this. Let $f(X) \in k[X]$ then there is a unique polynomial $\mathrm{red}(f)(X) \in k[X]$ called the *reduced representative* of f which is p-power free, i.e. $\mathrm{red}(f)(X) \in \bigoplus_{(i,p)=1} kX^i$ and such that $\mathrm{red}(f)(X) = f(X) \bmod (\mathrm{F} - \mathrm{Id})k[X]$. By Artin–Schreier theory the covers C_f and $C_{\mathrm{red}(f)}$ are the same p-cyclic cover of the affine line. The curve C_f is irreducible if and only if $\mathrm{red}(f) \neq 0$. In what follows we always assume that $\mathrm{red}(f) \neq 0$. The degree of the reduced polynomial $\mathrm{red}(f)$ is called the *conductor* of the cover. It is prime to p and equal to the degree of f if $(\deg f, p) = 1$.
- By C_f we also denote the nonsingular projective curve with function field $k(X, W)$. If $m = \deg f$ is prime to p then the genus of C_f is $g(C_f) = ((m-1)(p-1))/2$.
- For $M \in C_f$ and $n \in \mathbb{N}$ let $L(nM) = \{\varphi \in k(C_f) \mid (\varphi) + nM \geqslant 0\}$. Then $\mathcal{P}(M) := \{-v_M(\varphi) \mid \varphi \in \bigcup_{n\in\mathbb{N}} L(nM) - \{0\}\}$ is called the *polar semi-group* at M.
- We denote by $\infty \in C_f$ the point $X = \infty$, $W = \infty$ and by $M_{x,w}$ the point $X = x$, $W = w$ with $w^p - w = f(x)$.
- Let $G(f) = \mathrm{Aut}_k C_f$, $G_\infty(f)$ the inertia group at ∞ and $G_{\infty,1}(f)$ the wild inertia group at ∞. Let $\rho \in G(f)$ be such that $\rho(X) = X$ and $\rho(W) = W + 1$. Then ρ generates a p-cyclic subgroup in $G_\infty(f)$.

3. p-Sylow subgroups of the group $G(f)$

With the above notation, Stichtenoth proved the following.

THEOREM 3.1 [Sti73b, Satz 6 and 7]. *Assume the genus $g(C_f) \geqslant 2$, i.e. $m \geqslant 2$ and $\{m, p\} \neq \{2, 3\}$. Then ∞ is the only point $M \in C_f$ such that $\mathcal{P}(M) = \deg f\mathbb{N} + p\mathbb{N}$; however, there are the following two exceptions.*

(a) *$m < p$, $m|1 + p$, $f(X) = X^m$. In this case, in addition to ∞, exactly the p zeros of X have the same semi-group $\mathcal{P}(M)$. More precisely for $i \in \mathbb{F}_p$ let σ_i be given by $\sigma_i(X) = X/(W - i)^\delta$ and $\sigma_i(W) = -1/(W - i)$, where $\delta = (1 + p)/m$. Then $\sigma_i \in G(f)$ and $\sigma_i(M_{0,i}) = \infty$. In particular, $G(f)$ acts transitively on the $p + 1$ points M such that $\mathcal{P}(M) = \mathcal{P}(\infty)$; $|G(f)| = pm(p^2 - 1)$ and $G_{\infty,1}(f)$ is a p-Sylow of $G(f)$.*

(b) *$f(X) = X^{1+p}$. Now exactly the p^3 points $M_{\alpha,\beta}$ where $\alpha^{p^2} = -\alpha$ and $\beta^p - \beta = \alpha^{1+p}$ have the same semi-group as the point ∞. Let $a \in k$ with $a^{p^2-1} = 1$,*

$$\sigma_{\alpha,\beta}(X) = \alpha + \frac{aX}{W} \quad \text{and} \quad \sigma_{\alpha,\beta}(W) = \beta - \frac{a^{1+p}}{W} - a\alpha^p\frac{X}{W}.$$

Then $\sigma_{\alpha,\beta} \in G(f)$ and $\sigma_{\alpha,\beta}(\infty) = M_{\alpha,\beta}$. In particular, $G(f)$ acts transitively on the $p^3 + 1$ points M such that $\mathcal{P}(M) = \mathcal{P}(\infty)$; $|G(f)| = p^3(p^3 + 1)(p^2 - 1)$ and $G_{\infty,1}(f)$ is a p-Sylow of $G(f)$.

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

Remark 3.2. Stichtenoth considers equations of the type $W^p + W = f(X)$. The expressions of the automorphisms σ_i and $\sigma_{\alpha,\beta}$ in cases (a) and (b) are then simpler. For a description of the full automorphism group in case (b) we refer to [Leo96].

We deduce the following.

Proposition 3.3. *Let $f \in Xk[X]$, $g \in Tk[T]$ and $C_g : V^p - V = g(T)$ such that $\deg f$, $\deg g$ are prime to p and $g(C_f) \geqslant 2$. We assume $\exists \varphi : C_f \to C_g$ a k-isomorphism. Then $\exists \sigma \in G(f)$ such that $\varphi \circ \sigma(\infty) = \infty$ and $\varphi \circ \sigma$ descends to $\mathbb{P}^1$, i.e. $\exists \tilde{\varphi} : \mathbb{P}^1 \to \mathbb{P}^1$ and a commutative diagram as follows.*

$$\begin{tikzcd}
C_f \arrow[r, "\varphi\circ\sigma"] \arrow[d, "X"'] & C_g \arrow[d, "T"] \\
\mathbb{P}^1 \arrow[r, "\tilde{\varphi}"] & \mathbb{P}^1
\end{tikzcd}$$

Moreover, $\exists (a,b) \in (k^\times, k)$ and $c \in \mathbb{F}_p^\times$ such that $\tilde{\varphi}^\sharp(T) = aX + b$ and $cf(X) - g(aX+b) \in (\mathrm{F} - \mathrm{Id})k[X]$. If f is not in case (a) or (b) of Theorem 3.1 we can take $\sigma = \mathrm{Id}$; then $G(f) = G_\infty(f)$ and so $G_{\infty,1}(f)$ is the unique p-Sylow subgroup. Conversely, any triple $(a,b,c) \in k^\times \times k \times \mathbb{F}_p^\times$ such that $cf(X) - g(aX+b) \in (\mathrm{F} - \mathrm{Id})(k[X])$ induces such a commutative diagram.

Proof. Let $m = \deg f$ then it is classical that $g(C_f) = (m-1)(p-1)/2$. Therefore, as $g(C_f) = g(C_g)$ it follows that $m = \deg f = \deg g$. The homomorphism $\varphi^\sharp : k(C_g) \to k(C_f)$ is a k-isomorphism which induces a graded isomorphism between the linear spaces $L(\infty\varphi(M))$ and $L(\infty M)$ and so the polar semi-groups are preserved. It follows that $\varphi^{-1}(\infty) \in C_f$ has a polar semi-group equal to that of $\infty \in C_f$. We deduce the existence of σ from Theorem 3.1 and can assume from now on that $\varphi(\infty) = \infty$.

Now we follow the discussion in Stichtenoth's paper [Sti73b, Satz 4].

Case 1: $m > p$. Then $1, T$ (respectively $1, T, \ldots, T^{[m/p]}, V$) is a k-basis for $L(p\infty) \subset k(C_g)$ (respectively $L(m\infty) \subset k(C_g)$). Idem $1, X$ and $1, X, \ldots, X^{[m/p]}, W$ are a basis for $L(p\infty) \subset k(C_f)$ (respectively $L(m\infty) \subset k(C_f)$). As $\varphi^\sharp(L(p\infty)) = L(p\infty)$ (respectively $\varphi^\sharp(L(m\infty)) = L(m\infty)$) we get the existence of $a \in k^\times, b \in k$, such that $\varphi^\sharp(T) = aX + b$ and $\varphi^\sharp(V) = cW + Q(X)$ where $c \in k^\times$ and $Q(X) \in k[X]$ with $\deg Q(X) \leqslant [m/p]$. Then $(c^p - c)W + c^p f(X) + (Q(X)^p - Q(X)) = g(aX+b)$, so $c^p = c$ and $cf(X) - g(aX+b) \in (\mathrm{F} - \mathrm{Id})k[X]$. Conversely, these relations define an isomorphism.

Case 2: $m < p$. This works similarly; namely $1, V$ (respectively $1, V, \ldots, V^r, T$) with $rm < p < (r+1)m$ is a basis for $L(m\infty)$ (respectively $L(p\infty)$ in $k(C_g)$). Then $\varphi^\sharp(T) = aX + P(W)$, where $P(W) \in k[W]$ with $m \deg P < p$ and $\varphi^\sharp(V) = cW + Q$ where $c \in k^\times$ and $Q \in k$. We get the equation $(c^p - c)W + c^p f(X) + (Q^p - Q) = g(aX + P(W)) = a^m X^m + (ma^{m-1}P(W) + b_{m-1})X^{m-1} + \cdots + P(W)^m$, where $g(T) = T^m + b_{m-1}T^{m-1} + \cdots$. Comparing the W-degrees it follows that $P(W) = b \in k$ and $c^p = c$. Now we again get the condition $cf(X) - g(aX+b) \in (\mathrm{F} - \mathrm{Id})k[X]$. □

Corollary 3.4. *Let $f \in Xk[X]$ be such that $g(C_f) \geqslant 1$ and $S(f) := \{(a,b,c) \in k^\times \times k \times \mathbb{F}_p^\times \mid \exists P_{a,b,c}(X) \in k[X],\ cf(X) - f(aX+b) = P_{a,b,c}(X)^p - P_{a,b,c}(X)\}$. Such a polynomial $P_{a,b,c}$ in $k[X]$ is determined by these relation up to addition by an element in $\mathbb{F}_p$. For $(a,b,c) \in S(f)$ the formulas $\sigma_{a,b,c}(X) = aX + b$, $\sigma_{a,b,c}(W) = cW + P_{a,b,c}(X)$ define an automorphism of C_f which lies in $G_\infty(f)$. Further $G_\infty(f) = \langle \rho, \sigma_{a,b,c} \rangle$ for $(a,b,c) \in S(f)$ and $G_{\infty,1}(f) = \langle \rho, \sigma_{1,b,1} \rangle$ for $(1,b,1) \in S(f)$.*

Proof. If $g(C_f) > 1$ this follows from the proposition. If $g(C_f) = 1$ then $\{p, m\} = \{2, 3\}$. For $p = 2$ we have $f(X) = aX + X^3$ and if $p = 3$ then $f(X) = aX + X^2$. In each case we can give a basis for $L(m\infty)$ and $L(p\infty)$ of the same kind as given in the two cases of the proof of the proposition and we conclude in the same way. Note that if $g(C_f) = 0$, then $G_\infty(f) = k^\times X + k$. □

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

Now we can give the general structure of the wild automorphism group $G_{\infty,1}(f)$. In order to simplify the notations for $(1,y,1)\in S(f)$ we denote by σ_y the element $\sigma_{1,y,1}$ and by $P_f(X,y)$ the corresponding polynomial $P_{1,y,1}(X)$.

For $(1,y,1)$ and $(1,z,1)$ in $S(f)$ we define the following functions

$$\mathrm{Tr}_f(y) := P_f(X,y)+P_f(X+y,y)+P_f(X+2y,y)+\cdots+P_f(X+(p-1)y,y)$$
$$\epsilon_f(y,z) := P_f(X,y)+P_f(X+y,z)-P_f(X,z)-P_f(X+z,y).$$

Corollary 3.5. *With the above notation assume $g(C_f)>0$. Then $\rho\in Z(G_{\infty,1}(f))$ and $G_{\infty,1}(f)=\langle\rho,\sigma_y, y\in S(f)\rangle$. Further $\mathrm{Tr}_f(y)\in\mathbb{Z}/p\mathbb{Z}$ and $\sigma_y^p=\rho^{\mathrm{Tr}_f(y)}$. The commutation rule is given by $[\sigma_y,\sigma_z]=\rho^{\epsilon_f(y,z)}$ where $\epsilon_f(y,z)=P_f(X,y)+P_f(X+y,z)-P_f(X,z)-P_f(X+z,y)\in\mathbb{Z}/p\mathbb{Z}$. Moreover, we have the following exact sequence $0\to\langle\rho\rangle\simeq\mathbb{Z}/p\mathbb{Z}\to G_{\infty,1}(f)\xrightarrow{\pi}k$, where $\pi(\sigma_y)=y\in k$ and the image of π is finite dimensional as $\mathbb{F}_p$-vector space, i.e. a finite elementary abelian p-group.*

Proof. From $\sigma_y(X)=X+y$ and $\sigma_y(W)=W+P_f(X,y)$ we get $\sigma_y^p(W)=W+\mathrm{Tr}_f(y)$. As $\sigma_y^p(X)=X$ it follows that $\mathrm{Tr}_f(y)\in\mathbb{Z}/p\mathbb{Z}$ and $\sigma_y^p=\rho^{\mathrm{Tr}_f(y)}$. For the commutation rule we remark that $[\sigma_y,\sigma_z](X)=X$. From this it follows that $[\sigma_y,\sigma_z]=\rho^{\epsilon_f(y,z)}$ for some $\epsilon_f(y,z)\in\mathbb{Z}/p\mathbb{Z}$. In order to determine $\epsilon_f(y,z)$ we calculate $\sigma_y\circ\sigma_z(W)=W+P_f(X,y)+P_f(X+y,z)$ which is equal to $W+P_f(X,z)+P_f(X+z,y)+\epsilon_f(y,z)$. □

4. Extensions of a p-cyclic group by an elementary abelian p-group

In Corollary 3.5 we saw that the groups $G_{\infty,1}(f)$ belong to the following class of p-groups.

Definition 4.1. We denote by C_1 the set of finite groups G which are extensions of a p-cyclic group N by a finite elementary abelian p-group G/N. We remark that the induced homomorphism $G/N\to\mathrm{Aut}\,N$ is necessarily trivial for order reasons and so such an extension is central.

Conversely, in § 7, we prove that any group in C_1 is a group $G_{\infty,1}(f)$. To this end we need a group theoretic classification in terms of a special class of such groups.

4.1 Extraspecial groups

We refer to [Hup67, Suz82, Suz86] for the structure of finite p-groups.

If G lies in C_1 then necessarily $N\subset Z(G)$. Those nonabelian groups in C_1 for which $Z(G)$ is itself p-cyclic are called extraspecial. In particular, a nonabelian group G of order p^3 is always extraspecial:

- if $p>2$, then G is isomorphic to either $E(p^3)$ or $M(p^3)$, where
$$E(p^3)=\langle x,y|x^p=y^p=[x,y]^p=1,[x,y]\in Z(E(p^3))\rangle \text{ with exponent } p,$$
$$M(p^3)=\langle x,y|x^{p^2}=y^p=1,y^{-1}xy=x^{1+p}\rangle \text{ with exponent } p^2;$$
- if $p=2$, then G is either isomorphic to the dihedral group D_8 or to the quaternion group Q_8. These two groups both have exponent 2^2.

More generally let G be an extraspecial p-group; then (see [Suz86, Theorem 4.18]) $|G|=p^{2n+1}$ for some $n>0$ and the following four types occur.

I. If $p>2$, then either:
   (a) exponent$(G)=p$ and G is a central product of n groups $E(p^3)$ (i.e. the direct product where the p-cyclic centers of each factor are amalgamated);
   (b) exponent$(G)=p^2$ and G is a central product of $M(p^3)$ and $n-1$ groups $E(p^3)$.

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

II. If $p = 2$, then either:

(a) G is a central product of n groups D_8. Let $q_a(n)$ (respectively $d_a(n)$) be the number of elements of order 4 (respectively of order at most 2); or

(b) G is a central product of a group Q_8 and $n-1$ groups D_8. Let $q_b(n)$ (respectively $d_b(n)$) be the number of elements of order 4 (respectively of order at most 2).

We have the following:

- $q_a(n) = -2^n + 2^{2n}$ and so $d_a(n) = 2^n + 2^{2n}$;
- $q_b(n) = 2^n + 2^{2n}$ and so $d_b(n) = -2^n + 2^{2n}$.

In each case the structure of the central product is uniquely determined by the structure of the factors. In the following when speaking of the isomorphism type of an extraspecial group we will refer to the four types above, namely type I(a), I(b), II(a) and II(b).

The class C_1 has been described in the following result (cf. [Suz86, ch. 4, Theorem 4.16]).

Proposition 4.2. *Any $G \in C_1$ is isomorphic to one of the groups in the following list.*

(a) *An elementary abelian p-group.*

(b) *An abelian group of type $(p, p, \ldots, p, p^2)$.*

(c) *A central product of an extraspecial p-group E and an abelian group A. If A is not elementary abelian, then*

$$E \cap A = Z(E) = A^p.$$

4.2 Saturated subgroups of extraspecial groups

Definition 4.3. Let E be an extraspecial group and $\pi : E \to E/Z(E)$ the canonical homomorphism. A *saturated subgroup* of E is a group $\pi^{-1}(V)$, for V a subgroup of $E/Z(E)$. We denote

$$C_2 := \{G \text{ which are saturated subgroup of some extraspecial group}\}.$$

From the description of an extraspecial group as a central product of copies of those of order p^3 given in § 4.1, it follows that for $p > 2$ (respectively $p = 2$) any extraspecial group of type I(a) (respectively type II(a)) is a saturated subgroup of an extraspecial group of type I(b) (respectively type II(b)).

We need the following result from group theory. Although it is possible to give a proof using the classification of extraspecial groups and Proposition 4.2, we give a direct proof which deals with factor systems and fits well with the realization result we intend to prove.

Proposition 4.4. *The two classes C_i for $i = 1, 2$ are equal.*

Proof. Let $G \in C_1$, then $G' \subset N \subset Z(G)$ (see Definition 4.1). This last condition allows to define a skew-symmetric bilinear form on the $\mathbb{F}_p$-vector space G/N: if $\overline{x}, \overline{y} \in G/N$, then $[x, y] \in G' = \langle \rho \rangle \subset N$, i.e. $[x, y] = \rho^{\epsilon}$ where $\epsilon \in \mathbb{Z}/p\mathbb{Z}$. Note that $[x, y]$ is independent of the lifts of $\overline{x}$ and $\overline{y}$ to G as $N \subset Z(G)$. We define $\langle \overline{x}, \overline{y} \rangle := \epsilon$. Note that $x \in Z(G)$ if and only if $\langle \overline{x}, \overline{y} \rangle = 0$ for all $y \in G$. Therefore, $\langle \cdot, \cdot \rangle$ is nondegenerate if and only if $G' = N = Z(G)$, i.e. G is extraspecial. We call $\langle \cdot, \cdot \rangle$ the form associated to $G \in C_1$.

Consider the extension of groups

$$1 \to N \to G \overset{\overset{s}{\curvearrowleft}}{\longrightarrow} V := G/N \to 1.$$

Let s be a set theoretical section. To any two $v_1, v_2 \in V$ we have a $c(v_1, v_2) \in N$ such that $s(v_1)s(v_2) = s(v_1 v_2)c(v_1, v_2)$ and $c(\cdot, \cdot)$ is the 2-cocycle corresponding to the equivalence class of the above extension in $H^2(V,N) = H^2(V,\mathbb{F}_p)$. Note that N has trivial action by V (cf. Definition 4.1). From $c(\cdot,\cdot)$ we recover G in the following way: on the set $V \times \mathbb{F}_p$ one defines a group structure via

$$(v_1,\alpha)(v_2,\beta) = (v_1+v_2, \alpha+\beta+c(v_1,v_2)).$$

The form associated to G, i.e. $\langle\cdot,\cdot\rangle$ on V, can be expressed in terms of c:

$$\begin{aligned}\langle v_1,v_2\rangle &= [s(v_1),s(v_2)] = s(v_1)^{-1}s(v_2)^{-1}s(v_1)s(v_2) = (s(v_2)s(v_1))^{-1}s(v_1)s(v_2)\\ &= c(v_2,v_1)^{-1}s(v_2v_1)^{-1}s(v_1v_2)c(v_1,v_2) = c(v_2,v_1)^{-1}c(v_1,v_2).\end{aligned}$$

Identifying N with $\mathbb{F}_p$ we write $\langle v_1,v_2\rangle = c(v_1,v_2) - c(v_2,v_1)$. We distinguish the cases $p > 2$ and $p = 2$.

Case $p > 2$. Let $V \hookrightarrow W := V \bigoplus V$ be the embedding that identifies V with the first factor of W and $\mathrm{pr}_1 : W \to V$ the projection on the first factor. We denote by c a cocycle corresponding to the given group extension and we extend the corresponding 2-form $\langle v_1,v_2\rangle = c(v_1,v_2) - c(v_2,v_1)$ from V to W to a nondegenerate skew form given by the $2n \times 2n$-block matrix

$$\begin{pmatrix} A & -\mathbb{I} \\ \mathbb{I} & 0 \end{pmatrix} \in M_{2n}(\mathbb{F}_p)$$

where $A \in M_n(\mathbb{F}_p)$ is the matrix of $\langle\cdot,\cdot\rangle$ on the n-dimensional vector space V and $\mathbb{I} \in M_n(\mathbb{F}_p)$ the identity.

Now we obtain a 2-cocycle $d : W \times W \to \mathbb{F}_p$ via $(w_1,w_2) \to \langle w_1,w_2\rangle + c(\mathrm{pr}_1(w_2),\mathrm{pr}_1(w_1))$. We remark that $d_{|V}$ maps (v_1,v_2) to $\langle v_1,v_2\rangle + c(v_2,v_1) = c(v_1,v_2) - c(v_2,v_1) + c(v_2,v_1) = c(v_1,v_2)$. So $d_{|V} = c$ and the group extension E corresponding to d therefore contains G as a subgroup.

It remains to show that $|Z(E)| = p$. This amounts to the skew-form $\langle\langle\cdot,\cdot\rangle\rangle$ associated to d on W to be nondegenerate. We compute on W:

$$\begin{aligned}\langle\langle w_1,w_2\rangle\rangle &= d(w_1,w_2) - d(w_2,w_1)\\ &= \langle w_1,w_2\rangle + c(\mathrm{pr}_1(w_2),\mathrm{pr}_1(w_1)) - \langle w_2,w_1\rangle - c(\mathrm{pr}_1(w_1),\mathrm{pr}_1(w_2))\\ &= 2\langle w_1,w_2\rangle - \langle \mathrm{pr}_1(w_1),\mathrm{pr}_1(w_2)\rangle.\end{aligned}$$

Therefore, $\langle\langle\cdot,\cdot\rangle\rangle$ has the $2n \times 2n$-block matrix

$$\begin{pmatrix} 2A & -2\mathbb{I} \\ 2\mathbb{I} & 0 \end{pmatrix} - \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} A & -2\mathbb{I} \\ 2\mathbb{I} & 0 \end{pmatrix} \in M_{2n}(\mathbb{F}_p)$$

which has maximal rank as $p > 2$. We conclude that E is extraspecial. We have obtained G as subgroup of the extraspecial group E and $N = Z(E) \subset G$ follows from the fact that in the construction above the second factor of $V \times \mathbb{F}_p$ and $W \times \mathbb{F}_p$ correspond to N and $Z(E)$, respectively.

Case $p = 2$. Using the above notation, let $n := \dim V$ and $M_n(\mathbb{F}_2)$ the $\mathbb{F}_2$-vector space of $n \times n$ matrices. Any such matrix defines a bilinear form (hence a 2-cocycle) on V. Therefore, we have a map of $\mathbb{F}_2$-vector spaces

$$M_n(\mathbb{F}_2) \xrightarrow{\varphi} H^2(V,\mathbb{F}_2). \qquad (1)$$

Moreover, a matrix A is in the kernel K of φ if and only if its associated 2-cocycle c defines the split extension, which is the elementary abelian 2-group of rank $n+1$.

This is equivalent to $c(v_1,v_2) = c(v_2,v_1)$ for all $v_1,v_2 \in V$ and $c(v,v) = 0$ for all $v \in V$ (here we use $p = 2$). In other words $A = A^t$ and A has only zeros on its diagonal. We conclude $\dim\ker\varphi = n-1+n-2+\cdots+1 = n(n-1)/2$. It is known that $\dim H^2(V,\mathbb{F}_2) = n(n+1)/2$ (see [Joh76, p. 168]).

Therefore,

$$1 \to K \to M_n(\mathbb{F}_2) \xrightarrow{\varphi} H^2(V,\mathbb{F}_2) \to 1$$

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

is exact. In particular φ is onto, so every element of $H^2(V,\mathbb{F}_2)$ can be represented by a 2-cocycle that is a bilinear form.

Again we let the given extension correspond to the cocycle $c \in Z^2(V,\mathbb{F}_2)$ and by the above we may assume c is bilinear corresponding to a matrix A.

Let $V \hookrightarrow W := V \oplus V$ be the first factor and consider $d \in Z^2(V,\mathbb{F}_2)$ corresponding to the block matrix

$$\begin{pmatrix} A & \mathbb{I} \\ 0 & 0 \end{pmatrix} \in M_{2n}(\mathbb{F}_p).$$

Then $d_{|V} = c$, so the group defined by d contains G.

Claim. E is an extraspecial group, i.e. the 2-form $\langle\langle\cdot,\cdot\rangle\rangle$ defined by d on W is nondegenerate.

We calculate $\langle\langle w_1, w_2\rangle\rangle = d(w_1,w_2) - d(w_2,w_1) = w_1^tBw_2 + w_2^tBw_1 = w_1^tBw_2 + (w_2^tBw_1)^t = w_1^tBw_2 + w_1^tB^tw_2 = w_1^t(B+B^t)w_2$ and

$$B + B^t = \begin{pmatrix} A + A^t & \mathbb{I} \\ \mathbb{I} & 0 \end{pmatrix} \in M_{2n}(\mathbb{F}_p)$$

has rank $2n$ (independently of what A is).

Conversely (for any characteristic $p > 0$) let $G \in C_2$. Then $G \hookrightarrow E$ is a saturated subgroup of an extraspecial group E. Therefore, $G/Z(E) \hookrightarrow E/Z(E)$, both are elementary abelian and hence we have an exact sequence

$$1 \longrightarrow Z(E) \longrightarrow G \longrightarrow G/Z(E) \longrightarrow 1$$

showing that $G \in C_1$. □

Remark 4.5. Let $p > 2$ and let $G \in C_1$ with exponent p. We have realized G as a saturated subgroup of an extraspecial group E. A calculation using the extended cocycle c to W, then shows that E has the same exponent as G.

5. Computation of $G_{\infty,1}(f)$: an algorithm

5.1 Universal family

Notation. In order to be able to treat families of covers it is useful for a given conductor m, prime to p, to work over the ring $A := \mathbb{F}_p[t_i, 1 \leqslant i \leqslant m]$ and consider $f(X) = \sum_{1\leqslant i\leqslant m} t_iX^i$.

A specialization homomorphism is an homomorphism $\varphi : A \to k$, where k is an algebraically closed field of characteristic $p > 0$; then $\varphi(f)(X) = \sum_{1\leqslant i\leqslant m} \varphi(t_i)X^i \in k[X]$. Note that the conductor of the cover is preserved if and only if $\varphi(t_m) \neq 0$.

Let $i < m$ and $(i,p) = 1$ and denote by $n(i) := \max\{n \in \mathbb{N} \mid ip^n < m\}$. The following lemma is the key tool; for this we introduce $\Delta(f)(X,Y) := f(X+Y) - f(X) - f(Y)$.

Lemma 5.1 (Compare with [Sti73b, p. 621]). *With the above notation there is a unique polynomial $R(X,Y) \in \bigoplus_{1\leqslant i<m,(i,p)=1} A[Y]X^{ip^{n(i)}}$ and a unique polynomial $P_f(X,Y) \in XA[Y][X]$ such that*

$$\Delta(f)(X,Y) = R(X,Y) + (\mathrm{Id} - \mathrm{F})P_f(X,Y). \tag{2}$$

The polynomial $P_f(X,Y)$ is characterized by the following:

$$P_f(X,Y) = (\mathrm{Id} + \mathrm{F} + \cdots + \mathrm{F}^{n-1})\Delta(f) \mod (X^{[(m-1)/p]+1}) \tag{3}$$

for any n such that $p^n > [(m-1)/p]$.

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

Proof. Existence: note that $\deg_X \Delta(f) = m-1$ and $\Delta(f) \in (X,Y)A[X,Y]$. Let $(i,p)=1$ with $1 \leqslant i < m$ and $0 \leqslant j \leqslant n(i)$. For a monomial $\delta_{ip^j}(Y)X^{ip^j}$ of $\Delta(f)$ where $\delta_{ip^j}(Y) \in A[Y]$ and of total degree less than m we write $\delta_{ip^j}(Y)X^{ip^j} = (\delta_{ip^j}(Y))^{p^{n(i)-j}}X^{ip^{n(i)}} + (\mathrm{Id}-\mathrm{F})(P_{ip^j}(X))$ with $P_{ip^j}(X) = (\mathrm{Id}+\mathrm{F}+\cdots+\mathrm{F}^{n(i)-j-1})(\delta_{ip^j}(Y)X^{ip^j})$.

For the unicity we remark that if $P_f(X,Y)$ satisfies the formula (2), then $\deg_X P_f(X,Y) \leqslant [(m-1)/p]$ and so it suffices to prove formula (3) in the lemma. We have the identity

$$(\mathrm{Id}+\mathrm{F}+\cdots+\mathrm{F}^{n-1})\Delta(f) = (\mathrm{Id}+\mathrm{F}+\cdots+\mathrm{F}^{n-1})R(X,Y) + (\mathrm{Id}-\mathrm{F}^n)P_f(X,Y)$$

for any n. Now $R(X,Y) \in (X^{[(m-1)/p]+1})$ as $ip^{n(i)} < m < ip^{n(i)+1}$ and $P_f(X,Y) \in XA[Y][X]$. Then for $p^n > [(m-1)/p]$ we obtain the formula (3). □

DEFINITION 5.2. Let $\varphi : A \to k$ be a specialization homomorphism with $\varphi(t_m) \neq 0$. We denote by the same letter the induced homomorphism on polynomials via the action on the coefficients. Let $\mathrm{Ad}_{\varphi(f)}(Y) \in k[Y]$ be the monic generator of the ideal generated by the coefficients of $\varphi(R)(X,Y) \in k[Y]$. As usual we denote by $Z(\mathrm{Ad}_{\varphi(f)}(Y))$ the set of zeros in the algebraically closed field k. For $i=1,2$ let φ_i be two specialization homomorphisms with $\varphi_i(t_m) \neq 0$. If $\mathrm{red}\,\varphi_1(f) = \mathrm{red}\,\varphi_2(f)$, then $\varphi_1(R)(X,Y) = \varphi_2(R)(X,Y)$ and so $\mathrm{Ad}_{\varphi_1(f)} = \mathrm{Ad}_{\varphi_2(f)}$. It follows that for $g \in k[x]$, $\deg g = m$ and $\varphi : A \to k$ a specialization homomorphism with $\varphi(t_m) \neq 0$ and such that $g = \varphi(f)$ we can define $\mathrm{Ad}_g := \mathrm{Ad}_{\varphi(f)}$. Moreover, one has $\mathrm{Ad}_g = \mathrm{Ad}_{\mathrm{red}\,g}$.

COROLLARY 5.3. *Let $m-1 = \ell p^s$ with $(\ell,p)=1$ (i.e. $s = v_p(m-1)$). Write $R(X,Y) = \sum_j a_j(Y)X^j = \sum_{1\leqslant i<m,\,(i,p)=1} a_{ip^{n(i)}}(Y)X^{ip^{n(i)}}$.*

(i) *The coefficient $a_{m-1}(Y) \in mt_mY + (YA[Y])^p$ and $\deg a_{m-1}(Y) \leqslant (m-1)^2$.*

(ii) *If $\ell > 1$, let $j_0 = 1 + (\ell-1)p^s$. Then j_0 is prime to p (also if $s=0$) and $n(j_0)=0$. Moreover, the coefficient $a_{j_0}(Y) = \ell t_m Y^{p^s} + \cdots + 2t_{j_0+1}Y$ if $p>2$ and if $p=2$ one has $a_{j_0}(Y) = \ell t_m Y^{2^s} + \cdots + t_{j_0+2}Y^2$. In particular, if $(p,m-1)=1$ (so $s=0$ and $p>2$) one has $j_0 = m-1$ and $a_{j_0}(Y) = mt_mY$.*

Proof. For (i) we remark that $m-1 = \ell p^s = \ell p^{n(\ell)}$ is the highest representative less than m of ℓ modulo multiplication by a power of p. Now $\Delta(X^m) = mYX^{m-1} +$ lower degree terms and, as the lower degree monomials have coefficients in $YA[Y]$ which give contributions in the coefficient of the monomial X^{m-1} of $R(X,Y)$ after we raise to some p-power, the result follows. Concerning the degree, we remark that $\Delta(f)(X,Y) = \sum_{t\leqslant m-1}\delta_t(Y)X^t$ and $\deg\delta_t(Y) \leqslant m-1$. Now, as in the proof of Lemma 5.1, we can write $t = ip^j$ where $(i,p)=1$, $1 \leqslant i < m$ and $0 \leqslant j \leqslant n(i)$. Then the contribution of $\delta_{ip^j}(Y)X^{ip^j}$ in $R(X,Y)$ is $(\delta_{ip^j}(Y))^{p^{n(i)-j}}X^{ip^{n(i)}}$ whose Y-degree is $\leqslant (m-1)^2$.

For (ii) we remark that $j_0 > (m-1)/p + 1$ and j_0 is prime to p. So the coefficient of the monomial X^{j_0} in $R(X,Y)$ is the same as that of $\Delta(f)$ and so equal to $\sum_{j_0<i\leqslant m,(i,p)=1}\binom{i}{j_0}t_iY^{i-j_0} = \ell t_m Y^{p^s} + \cdots + (j_0+1)t_{j_0+1}Y$. The result follows. □

Remark 5.4. In [Hen78, p. 114] one can find a discussion of the equation $W^p - W = f(X)$ and our system of representatives modulo $p^{\mathbb{N}}$ as well as j_0 as it occurs above.

PROPOSITION 5.5. *Let $\varphi : A \to k$ be a specialization homomorphism with $\varphi(t_m) \neq 0$. Then $\mathrm{Ad}_{\varphi(f)}(Y)$ is a separable and additive polynomial (§ 2) and its set of zeros $Z(\mathrm{Ad}_{\varphi(f)})$ is equal to $\{y \in k \mid \Delta(\varphi\circ f)(X,y) \in (\mathrm{Id}-\mathrm{F})k[X]\}$. Moreover if $y \in Z(\mathrm{Ad}_{\varphi(f)})$ then there is a unique $P(X) \in Xk[X]$ such that $\Delta(\varphi(f))(X,y) = (\mathrm{Id}-\mathrm{F})P(X)$ and $P(X) = \varphi(P_f)(X,y)$. Further $Z(\mathrm{Ad}_{\varphi(f)}) = \{y \in k \mid \sigma_y \in G_{\infty,1}(f)\}$ where $\sigma_y(X) = X+y$ and $\sigma_y(W) = W + \varphi(P_f)(X,y)$ (for notation see Corollary 3.5). In particular, $|G_{\infty,1}(\varphi(f))| = p\deg\mathrm{Ad}_{\varphi(f)}(Y)$ and for $y,z \in Z(\mathrm{Ad}_{\varphi(f)})$ the commutation rule for $\sigma_y,\sigma_z \in G_{\infty,1}(\varphi(f))$ is determined by $\epsilon_{\varphi(f)}(y,z) = \varphi(P_f)(X,y) + \varphi(P_f)(X+y,z) - \varphi(P_f)(X,z) - \varphi(P_f)(X+z,y)$.*

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

Proof. The additive polymonial $\mathrm{Ad}_{\varphi(f)}(Y)$ is separable because from Corollary 5.3(i) we know that it divides the polynomial $\varphi(a_{m-1}(Y)) \in m\varphi(t_m)Y + (Yk[Y])^p$ which is separable. To prove that it is additive, it suffices to show that its set of roots is stable under addition (§ 2). We first remark that $Z(\mathrm{Ad}_{\varphi(f)}) \subset \{y \in k \mid \sigma_y \in G_{\infty,1}(f)\}$ (cf. Corollary 3.4). For the reverse inclusion we remark that in the equality

$$\Delta\varphi(f)(X,y) = (\mathrm{Id} - \mathrm{F})P(X), \tag{4}$$

for suitable $P(X) \in k[X]$, we can assume that $P(X) \in Xk[X]$ as $\Delta(\varphi(f))(0,y) = 0$. Note that $\deg P \leqslant [(m-1)/p]$. Then for $n \gg 0$ we have $(\mathrm{Id}+\cdots+\mathrm{F}^n)\Delta(\varphi(f))(X,y) = P(X) \bmod X^{[(m-1)/p]+1}$, so $P(X) = \varphi(P_f)(X,y)$ (cf. Corollary 3.4). Then from Lemma 5.1 and (4) it follows that $\varphi(R)(X,y) = 0$, i.e. $\mathrm{Ad}_{\varphi(f)}(y) = 0$.

Let $y,z \in k$ such that $\Delta(\varphi(f))(X,y), \Delta(\varphi(f))(X,z) \in (\mathrm{Id} - \mathrm{F})k[X]$. We have the following general identity: $\Delta(\varphi(f))(X,y+z) = \Delta(\varphi(f))(X+z,y) + \Delta(\varphi(f))(X,z) - \Delta(\varphi(f))(y,z)$ and for our choice of y,z each term on the right-hand side is in $(\mathrm{Id} - \mathrm{F})k[X]$, so $\mathrm{Ad}_{\varphi(f)}(y+z) = 0$. □

Remark 5.6. In Definition 5.2 we saw that if $\varphi : A \to k$ is a specialization homomorphism with $\varphi(t_m) \neq 0$ and such that $g = \varphi(f)$ then $\mathrm{Ad}_{\varphi(f)}$ does not depend on φ. It follows from Proposition 5.5 that $\epsilon_{\varphi(f)}(y,z)$ does not depend on φ. This is also a consequence of the identity for $h \in k[X]$: $\Delta(h)(X,Y) + \Delta(h)(X+Y,Z) - \Delta(h)(X,Z) - \Delta(h)(X+Z,Y) = 0$.

Corollary 5.7. *We denote by* $\mathrm{Id} : A \to \mathrm{Fr}A$ *the inclusion homomorphism.*

A. (i) *If* $p = 2$ *and* $m = 3$, *then* $\mathrm{Ad}_{\mathrm{Id}(f)}(Y) = t_3^{-2}(t_3^2Y^4 + t_3Y)$.
(ii) *If* $p = 2$ *and* $m = 5$, *then* $\mathrm{Ad}_{\mathrm{Id}(f)}(Y) = t_5^{-4}(t_5^4Y^{16} + t_3^4Y^8 + t_3^2Y^2 + t_5Y)$.
(iii) *If* $p = 3$ *and* $m = 4$, *then* $\mathrm{Ad}_{\mathrm{Id}(f)}(Y) = t_4^{-3}(t_4^3Y^9 + 2t_2^3Y^3 + t_4Y)$.

B. *Outside case A one has* $\mathrm{Ad}_{\mathrm{Id}(f)}(Y) = Y$. *Moreover,* $\exists D(\underline{t}) \in \mathbb{F}_p[\underline{t}] - \{0\}$ *such that for any specialization* $\varphi : A \to k$ *with* $\varphi(D(\underline{t})) \neq 0$ *one has* $\mathrm{Ad}_{\varphi(f)}(Y) = Y$ *and so* $G_{\infty,1}(\varphi(f)) \simeq \mathbb{Z}/p\mathbb{Z}$.

Proof.

A. A direct calculation gives the formulas.

B. In order to simplify the proof we can assume that $t_m = 1$. If p does not divide $m-1$ the result follows from Corollary 5.3(ii). Therefore we can write $m = 1 + \ell p^s$ with $(\ell, p) = 1$, $s > 0$. We distinguish two cases.

1. $\ell > 1$. Let $j_0 = 1 + (\ell - 1)p^s$ and write $R(X,Y) = \sum_j a_j(Y)X^j$. Then $a_{j_0}(Y) = \ell Y^{p^s} +$ lower degree terms whose leading coefficient is a unit in A. The ring A is factorial hence it follows that $\mathrm{Ad}_{\mathrm{Id}(f)}(Y)$ is also a gcd in $A[Y]$ of the coefficients of $R(X,Y)$ and so lies in $A[Y]$. Let $\varphi : A \to k$ be a specialization morphism. Then $\varphi(\mathrm{Ad}_{\mathrm{Id}(f)})$ is monic and $\deg \varphi(\mathrm{Ad}_{\mathrm{Id}(f)}) = \deg \mathrm{Ad}_{\mathrm{Id}(f)}(Y)$. Now we remark that $\varphi(\mathrm{Ad}_{\mathrm{Id}})$ divides $\varphi(a_{m-1}(Y)) \in mY + (Yk[Y])^p$ and so is still separable in $k[X]$ (cf. Corollary 5.3(i)). Let us consider the specialization homomorphism $\varphi_0 : A \to \mathbb{F}_p$ defined by $\varphi_0(t_i) = 0$ for $i = 1, \ldots, m-1$. Then $\varphi_0(f)(X) = X^m$ and $\mathrm{Ad}_{\varphi_0(f)}(Y)$ divides ℓY^{p^s} (see the proof of Corollary 5.3(ii)). It follows that $\mathrm{Ad}_{\mathrm{Id}(f)}(Y) = Y$.
2. $\ell = 1$. Then $m = 1 + p^s$ with $s > 0$. A look at the monomials in $\Delta(f)(X,Y)$ shows that the highest contribution in $a_{m-1}(Y)$ comes from $(X+Y)^{1+p^s}$ and more precisely from the linear term $Y^{p^s}X$ which we need to raise to the power p^s. So finally $a_{m-1}(Y) = Y^{p^{2s}} +$ lower degree monomials and so $\mathrm{Ad}_{\mathrm{Id}(f)}(Y) \in A[Y]$. Now, as in case 1, we look for good specialization morphisms.

For $p > 3$ we consider $\varphi_0(f)(X) = X^3 + X^m$; then $\mathrm{Ad}_{\varphi_0(f)}(Y) | \varphi_0(a_{2p^{s-1}}(Y)) = 3^{p^{s-1}}Y^{p^{s-1}}$ and we conclude as in case 1.

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

For $p = 2$ and $s > 2$ we consider $\varphi_0(f)(X) = X^7 + X^m$; then $\mathrm{Ad}_{\varphi_0(f)}(Y) | \varphi_0(a_{3p^{s-2}}(Y)) = Y^{p^{s-2}}$ and we conclude as in case 1.

For $p = 3$ and $s > 1$ we consider $\varphi_0(f)(X) = X^5 + X^m$; then $\mathrm{Ad}_{\varphi_0(f)}(Y) | \varphi_0(a_{4p^{s-2}}(Y)) = (2Y)^{p^{s-2}}$ and we conclude as in case 1.

In order to exhibit a polynomial $D(\underline{t})$ we recall that Y is the content of the polynomial $R(X,Y) = \sum_j a_j(Y)X^j$ in $A[Y][X]$. Therefore, there exist elements $b_j(Y) \in (\mathrm{Fr}A)[Y]$ such that $\sum_j b_j(Y)a_j(Y) = Y$. Any $D(\underline{t}) \in \mathbb{F}_p[\underline{t}] - \{0\}$ such that $D(\underline{t})b_j(Y) \in A[Y]$ for all j works. □

Remark 5.8. As A is a unique factorization domain it is a natural question to ask for the best $D(\underline{t})$.

5.2 The algorithm

Let k be an algebraically closed field of characteristic $p > 0$ and $f \in k[X]$ such that $\mathrm{red}(f) \neq 0$. We are interested in the set $S(f) := \{y \in k \mid \Delta(f)(X,y) \in (\mathrm{F} - \mathrm{Id})k[X]\}$. Note that the two endomorphisms $\tau_y : X \to X + y$ and F of $k[X]$ commute. From this it follows that $S(f)$ only depends of the class of $f \bmod (\mathrm{F} - \mathrm{Id})k[X]$ and, in particular, $S(f) = S(\mathrm{red}(f))$. If $\deg f$ is prime to p then f is a specialization (in many ways) of the universal family considered in § 5.1. Consequently, Ad_f is well defined and $S(f) = Z(\mathrm{Ad}_f(Y))$.

The following procedure has been written in Maple; we comment on some steps and then present a concrete example.

Let $d := \deg f$ and assume for simplicity that $(d,p) = 1$. Then d is the conductor m of the cover C_f. If $(d,p) \neq 1$ the algorithm still works but needs to be adapted.

Step 1. Replace f by $f - f(0)$.

Step 2. Define $\delta_0 := f(X+Y) - f(X) - f(Y)$.

Step 3. Define inductively $\delta_{n+1} := \delta_0 + \delta_n^p \bmod (p, X^{[(d-1)/p]+1})$.

Step 4. Iterate until it is stationary and define $P(X,Y)$ to be the limit.

Step 5. Define $R := \delta_0 - P(X,Y) + P(X,Y)^p \in k[Y][X]$. This polynomial depends only on the class of f modulo $(\mathrm{F} - \mathrm{Id})k[X]$; moreover, the occurring X-monomials have degrees between $[(d-1)/p]$ and d.

Step 6. Define $\mathrm{Ad}_f(Y) :=$ gcd of the polynomials in $k[Y]$ which are the coefficients of $R \in k[Y][X]$.

Step 7. Calculate $\mathrm{Tr}_f(Y) := P(X,Y) + P(X+Y,Y) + \cdots + P(X+(p-1)Y,Y) \bmod \mathrm{Ad}_f(Y)$. Then for $y \in Z(\mathrm{Ad}_f)$ we have $\mathrm{Tr}_f(y) \in \mathbb{F}_p$. If $\mathrm{Tr}_f(y) = 0$, then y induces automorphisms of order dividing p. Otherwise it induces automorphisms of order p^2 (see Corollary 3.5).

Step 8. Calculate $\epsilon(Y,Z) := P(Y,Z) - P(Z,Y) \bmod (\mathrm{Ad}_f(Y), \mathrm{Ad}_f(Z))$. For a given $y \in Z(\mathrm{Ad}_f(Y))$ the roots of $\epsilon(y,Z)$ correspond to those automorphisms that commute with the ones corresponding to y. This is the commutation rule (see Corollary 3.5).

5.3 Illustration of the algorithm

Here we illustrate the algorithm which, for a given f, gives the structure of the group $G_{\infty,1}(f)$. This example is a realization of D_8 with $f \in \mathbb{F}_2[X]$. We use Maple and include some comments.

```
 > restart;
 > f:=X^(1+2)+X^(1+2+2^2)+X^(1+2+2^4)+X^(1+2+2^5)+X^(1+2^3+2^5):
 > delta0:=collect(subs(X=X+Y,f),X) -f-subs(X=Y,f),[X,Y]) mod 2:
 > delta1:=rem(collect(delta0+delta1^2-subs(X=0,delta0+delta1^2),[X,Y])
mod 2,X^21,X) mod 2:
```

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

Note that $21 = 40/2 + 1$. Here one reiterates the command until it is stationary.

```
 > P:=delta1:
 > F:=collect(delta0-P-P^2,[X,Y]) mod 2;
F :=
(Y^24+Y^80+Y^132+Y^528+Y^192+Y^64+Y^576+Y^1280+Y^1088+Y^6+Y^3+Y^16+Y^9
+Y^272)*X^32+(Y^256+Y^128+Y^4+Y^32)*X^24+(Y^128+Y^2)*X^36+(Y^4+Y)*X^34
+(Y+Y^16)*X^40+(Y^8+Y^2)*X^33
```

Here we remark that $\mathrm{Ad}_f(Y)$ divides the coefficient of X^{34}.

```
 > F:=collect(rem(F,Y^4+Y,Y)mod 2,X);
F := 0
```

Conclusion: $\mathrm{Ad}_f(Y) = Y^4 + Y$.

```
 > Tr_f(Y):=rem(collect(P+subs(X=X+Y,P),X),Y^4+Y,Y)  mod 2;
Y^3+Y^2+Y
 > Gcd(Y^4+Y,Y^3+Y^2+Y) mod 2;
Y^3+Y^2+Y
```

It follows that the three roots of $Y^3 + Y^2 + Y$ induce six elements of order 2 and the last root $Y = 1$ induces two elements of order 4.

```
 > epsilon:=subs([X=Y,Y=Z],P)-subs([X=Z],P) mod 2:
 > epsilon:=collect(rem(epsilon,Y^4+Y,Y) mod 2,Z);
 > epsilon:=collect(rem(epsilon,Z^4+Z,Z) mod 2,Y);
epsilon:= Z^2*Y+Z*Y^2
```

The group is nonabelian of order 8 with two elements of order 4; this is D_8.

Note that $f := X^3 + X^7 + X^{19} + X^{35} + X^{41}$ is reduced with conductor greater than 25. More generally it is a good question to ask for realizations over $\mathbb{F}_2$ (we mean $f \in \mathbb{F}_2[X]$) for groups in the class C_1.

6. Bounds for $|G_{\infty,1}(f)|$

6.1 Modifications of covers

In § 5.1, we fixed the conductor which is equivalent to fixing the genus of the cover. Here we study how for $f(X) \in k[X]$, the additive polynomial $\mathrm{Ad}_{\mathrm{red}(f)}(Y)$ changes through natural algebraic transformations which do not necessarily preserve the genus. We use these transformations in order to produce elements $f \in k[X]$ for which the bounds on $G_{\infty,1}(f)$, given in § 6.2, are attained. In § 7 we use the same transformations to obtain groups $G_{\infty,1}(f)$ with a given structure.

Definition 6.1. Let $S(X)$ be an additive polynomial $\in k[X]$. We say that the cover $C_{f\circ S}$ is a *modification of type 1* of C_f.

Note that if $(\deg f, p) = 1$ in general $(\deg f \circ S, p) \neq 1$. This explains why in the formulas below we work with $\mathrm{red}(f \circ S)$. Geometrically the p-cyclic cover $C_{f\circ S} \to \mathbb{P}^1$ is obtained from the p-cyclic cover $C_f \to \mathbb{P}^1$ after base change with the cover $\mathbb{A}^1 \to \mathbb{A}^1$ defined by the additive polynomial S.

Proposition 6.2. *Let $f \in k[X]$ be any polynomial with $(\deg f, p) = 1$ and $S(X) \in k[X]$ be a separable and additive polynomial. Then $\mathrm{Ad}_f(S(Y))$ divides $\mathrm{Ad}_{\mathrm{red}(f\circ S)}(Y)$. Further for $y, z \in Z(\mathrm{Ad}_f(S(Y)))$ we have $y, z \in Z(\mathrm{Ad}_{\mathrm{red}(f\circ S)}(Y))$ and $\epsilon_f(S(y), S(z)) = \epsilon_{\mathrm{red}(f\circ S)}(y, z)$ (see Proposition 5.5).*

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

Proof. One can write $\Delta(f)(X,Y) = \mathrm{Ad}_f(Y)G(X,Y) + P_f(X,Y) - P_f(X,Y)^p$, where $G(X,Y) \in k[Y][X]$ has content equal to 1 and $P_f(X,Y) \in k[Y][X]$. Then $\Delta(f\circ S)(X,Y) = \Delta(f)(S(X),S(Y)) =$

$$\mathrm{Ad}_f(S(Y))G(S(X),S(Y)) + P_f(S(X),S(Y)) - P_f(S(X),S(Y))^p.$$

If $y \in Z(\mathrm{Ad}_f(S(Y)))$ then $\Delta(f\circ S)(X,y) = P(S(X),S(y)) - P(S(X),S(y))^p$ and as $\mathrm{red}(f\circ S)(X) = f\circ S(X) + Q(X) - Q(X)^p$ for some $Q(X) \in k[X]$ we can write $\Delta(\mathrm{red}(f\circ S))(X,y) = (\mathrm{Id} - \mathrm{F})(P(S(X),S(y)) + \Delta(Q)(X,y))$ which, by Proposition 5.5, gives $\mathrm{Ad}_{\mathrm{red}(f\circ S)}(y) = 0$. The divisibility follows as $S(Y)$ and so $\mathrm{Ad}_f(S(Y))$ is separable. Moreover, by the same proposition for $y \in Z(\mathrm{Ad}_f(S(Y)))$ we have $P_{\mathrm{red}(f\circ S)}(X,y) = P(S(X),S(y)) + \Delta(Q)(X,y)$. We remark that $\Delta(Q)(X,y) + \Delta(Q)(X+y,z) - \Delta(Q)(X,z) - \Delta(Q)(X+z,y) = 0$ implies that $\epsilon_f(S(y),S(z)) = \epsilon_{\mathrm{red}(f\circ S)}(y,z)$ for $y,z \in Z(\mathrm{Ad}_f(S(Y)))$. □

Remark 6.3. In Proposition 6.2, it can happen that $\mathrm{Ad}_f(S(Y))$ strictly divides $\mathrm{Ad}_{\mathrm{red}(f\circ S)}(Y)$. For example, if $f(X) = X^{1+p^n}$ then $\mathrm{Ad}_f(Y) = Y + Y^{p^{2n}}$ (see Proposition 8.1). If $S(X) = X + X^p$ then $f\circ S(X) = (X+X^p)(X^{p^n} + X^{p^{n+1}}) = X^{1+p^n} + X^{1+p^{n+1}} + X^{p+p^n} + X^{p+p^{n+1}}$ and so $\mathrm{red}(f\circ S) = X^{1+p^{n-1}} + 2X^{1+p^n} + X^{1+p^{n+1}}$. Further $\mathrm{Ad}_{\mathrm{red}(f\circ S)}(Y) = Y + \cdots + Y^{p^{2(n+1)}}$ (see Proposition 8.1) and $\mathrm{Ad}_f(S(Y)) = Y + Y^p + Y^{p^{2n}} + Y^{p^{2n+1}}$ strictly divides $\mathrm{Ad}_{\mathrm{red}(f\circ S)}(Y)$.

Definition 6.4. Let $g(X), h(X) \in k[X]$ and assume that none of $\mathrm{red}(g), \mathrm{red}(h), \mathrm{red}(g+h)$ is zero. If $\mathrm{Ad}_{\mathrm{red}(h)}(Y) | \mathrm{Ad}_{\mathrm{red}(g)}(Y)$ we say that the cover C_{g+h} is a *modification of type 2* of C_g.

Proposition 6.5. *Let g,h be as above and assume that C_{g+h} is a modification of type 2 of C_g. Then $\mathrm{Ad}_{\mathrm{red}(h)}(Y) | \mathrm{Ad}_{\mathrm{red}(g+h)}(Y)$. Further for $y,z \in Z(\mathrm{Ad}_{\mathrm{red}(h)}(Y))$ we have $y,z \in Z(\mathrm{Ad}_{\mathrm{red}(g+h)}(Y))$ and $\epsilon_{\mathrm{red}(g+h)}(y,z) = \epsilon_{\mathrm{red}(g)}(y,z) + \epsilon_{\mathrm{red}(h)}(y,z)$ (see Proposition 5.5).*

Proof. This is clear from Proposition 5.5. □

6.2 Bounds

For fixed conductor we give bounds for $|G_{\infty,1}(f)|$.

Proposition 6.6. *Let k be an algebraically closed field of positive characteristic p and $f(X) \in k[X]$ a polynomial of degree m prime to p. Let $g(f) = (m-1)(p-1)/2$ be the genus of C_f and assume $g(f) \geqslant 2$. We write $m - 1 = \ell p^s$ with $\ell \geqslant 1$, $(\ell,p) = 1$ and $s \geqslant 0$. Then*

I. *$|G_{\infty,1}(f)| \leqslant p(m-1)^2$, i.e. $|G_{\infty,1}(f)|/g(f)^2 \leqslant 4p/(p-1)^2$ and we have equality for $f(X) = X^{1+p^s}$.*

II. *If $s = 0$, i.e. $(m-1,p) = 1$ then $|G_{\infty,1}(f)| = p$.*

III. *If $s > 0$:*

(i) *let $\ell > 1$ and $p = 2$, then $|G_{\infty,1}(f)| \leqslant 2^s$ and $|G_{\infty,1}(f)|/g(f) \leqslant \frac{2}{3}$; the two inequalities are equalities for $f(X) = \mathrm{red}((X + X^{2^{s-1}})^7)$ and $s > 1$;*

(ii) *let $\ell > 1$ and $p > 2$, then $|G_{\infty,1}(f)| \leqslant p^{s+1}$ and $|G_{\infty,1}(f)|/g(f) \leqslant (2/\ell)p/(p-1) \leqslant p/(p-1)$; the three inequalities are equalities for $f(X) = X^{1+2p^s} - X^{2+p^s}$;*

(iii) *let $\ell = 1$, i.e. $m = 1 + p^s$, then $|G_{\infty,1}(f)| \leqslant p^{2s+1}$, i.e. $|G_{\infty,1}(f)|/g(f) \leqslant 2p^s p/(p-1)$ and the two inequalities are equalities for $f(X) = X^{1+p^s}$.*

Proof. I. This follows from Corollary 5.3(i). For the example $f(X) = X^{1+p^s}$ we refer to III(iii). The last part of Corollary 5.3 gives II. For III(i) and(ii) we can assume that $f(X) = \sum_{1\leqslant i<m} t_i X^i + X^m \in k[X]$. Let $j_0 = 1 + (\ell - 1)p^s$. We have seen in Corollary 5.3 that $a_{j_0}(Y) = \ell Y^{p^s} + \cdots + 2t_{j_0+1}Y$, so $\deg \mathrm{Ad}_f(Y) \leqslant \deg a_{j_0}(Y) = p^s$ if $p > 2$ and $\deg \mathrm{Ad}_f(Y) \leqslant (1/2)\deg a_{j_0}(Y) = 2^{s-1}$ if $p = 2$. The result follows from Proposition 5.5.

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

Now we discuss the examples in which the bounds are attained. Let $p = 2$, $(\ell, 2) = 1$ and $f(X) = X^{1+\ell 2}$. In this case it is an easy consequence of Corollary 5.3 that $\mathrm{Ad}_f(Y) = Y$. Let $S(X) = X + X^{2^{s-1}}$ where $s > 1$. Then $f \circ S(X) = (X + X^{2^{s-1}})(X^2 + X^{2^s})^\ell = X(X^2 + X^{2^s})^\ell + X^{2^{s-2}}(X + X^{2^{s-1}})^\ell \bmod (\mathrm{Id} - \mathrm{F})k[X]$ has conductor $1 + \ell 2^s = m$. From Proposition 6.2 we know that $\mathrm{Ad}_f(S(Y))$ $= Y + Y^{2^{s-1}} | \mathrm{Ad}_{f \circ S}(Y)$ and from the first part of the proposition we get $\deg \mathrm{Ad}_{f \circ S}(Y) \leqslant 2^{s-1}$. Consequently we have equality $\mathrm{Ad}_{f \circ S}(Y) = Y + Y^{2^{s-1}} = \mathrm{Ad}_f(S(Y))$. Therefore, we conclude $|G_{\infty,1}(f \circ S)|/g(f) = 2/\ell \leqslant \frac{2}{3}$. This yields equality for $l = 3$, i.e. $f(S(X)) = (X + X^{2^{s-1}})^7$.

Let $p > 2$ we give an example for $\ell = 2$. As $a_{j_0}(Y) = \ell Y^{p^s} + \cdots + 2t_{j_0+1}Y$ we need $t_{j_0+1} \neq 0$. Now $j_0 + 1 = 2 + (\ell - 1)p^s = 2 + p^s$, so we consider $f(X) = X^{1+2p^s} - X^{2+p^s}$ and show that $\mathrm{Ad}_f(Y) = Y^{p^s} - Y$. The first part of the proposition yields $\deg \mathrm{Ad}_f(Y) \leqslant p^s$ so it suffices to prove a divisibility. Let $y \in k$ be such that $y^{p^s} = y$. Then $\Delta(f)(X, y) = (X + y)(X^{p^s} + y)^2 - (X + y)^2(X^{p^s} + y) - f(X) - f(y) = (X + y)(X^{2p^s} + 2yX^{p^s} + y^2) - (X^2 + 2yX + y^2)(X^{p^s} + y) - f(X) - f(y) = 0 \bmod (\mathrm{Id} - \mathrm{F})k[X]$.

(iii) The inequality is a special case of I. Let $f(X) = X^{1+p^s}$ and write $q = p^s$. Then $\Delta(f)(X, Y) = Y^q X + Y X^q = (Y^{q^2} + Y)X^q + P(X, Y) - P(X, Y)^p$. It follows that $\mathrm{Ad}_f(Y) = Y^{q^2} + Y$ and we obtain equalities. □

Remark 6.7. In general, for a given curve C in order to bound the automorphism group one considers a prime $\ell > 2$ not equal to p and uses the injective homomorphism

$$\mathrm{Aut}\, C \hookrightarrow \mathrm{Gl}(2g(C), \mathbb{F}_\ell)$$

where $g(C)$ is the genus. Let us, for example, consider the case $p = 2$ and $C = C_f$ with $\deg f = 1 + 2^k$. Then $2g(C_f) = 2^k$ and $|G_{\infty,1}(f)|$ divides the order of a 2-Sylow of $\mathrm{Gl}(2^k, \mathbb{F}_\ell)$ which is equal to $2^{g(C_f)F(1)-1}$, where $F(1) = 1 + v_2(\ell^2 - 1) + v_2(\ell - 1)$ (see [CF64] for the structure of 2-Sylow subgroups of $\mathrm{Gl}(2^k, \mathbb{F}_\ell)$). From this one also obtains bounds for $\mathrm{Aut}\, C_f$, but they are far from being as good as those in Proposition 6.6.

7. Group theoretic characterization of $G_{\infty,1}(f)$

7.1 Realization of groups as $G_{\infty,1}(f)$

In Corollary 3.5, we saw that the groups $G_{\infty,1}(f)$ belong to the class C_1 of p-groups (see Definition 4.1). Moreover, in § 4.2 we saw that $C_1 = C_2$, the class of saturated subgroups of the extraspecial groups. We define a third class

$$C_3 := \{G \mid \exists f \in Xk[X], (\deg f, p) = 1 \text{ such that } G \simeq G_{\infty,1}(f)\}.$$

Theorem 7.1. *The three classes $C_i, i = 1, 2, 3$ are equal.*

Proof. It is sufficient for G in C_1 to give a recipe to get an $f \in k[X]$ such that $G \simeq G_{\infty,1}(f)$. The method is the following: as G belongs to C_2, there is E an extraspecial group such that $G \simeq \pi^{-1}(V \subset E/Z(E))$, a saturated subgroup. Moreover, if $p > 2$ (respectively $p = 2$), we can choose E of type I(b) (respectively type II(b)); see Definition 4.3. Realizations of the extraspecial groups of type I(a) and II(b) occur naturally. In order to produce extraspecial groups of type I(b) we first consider a realization of the extraspecial group with the same order but of type I(a). Then we do a modification using the cocycle which occurs for the Witt vectors of length 2. For E an extraspecial group of type I(b) (respectively type II(b)) consider $G_{\infty,1}(f_E)$ a realization. Now to a subspace $V \subset E/Z(E)$ we associate an additive polynomial S_V which we use in order to produce a convenient modification of the cover C_{f_E}. The key point is that our modification will not change the commutation rule. □

Case $p > 2$. Let E be an extraspecial group of order pq^2 where $q = p^n$ and $n > 0$.

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

Step 1. Realization of E with exponent p (type I(a)).

CLAIM. If $f_1(X) := X^{1+q}$, then $E \simeq G_{\infty,1}(f_1)$ and $2p/(p-1) < |G_{\infty,1}(f_1)|/g(f_1) = (2p/(p-1))q$.

Proof. One has $\Delta(f_1)(X,Y) = Y^qX + YX^q = (Y^{q^2}+Y)X^q + P(X,Y) - P(X,Y)^p$, where $P(X,Y) = \sum_{0\leqslant i\leqslant n-1}(Y^qX)^{p^i}$. It follows that $\mathrm{Ad}_{f_1}(Y) = Y^{q^2} + Y$ and for $y \in Z(\mathrm{Ad}_{f_1})$, $P_{f_1}(X,y) = P(X,y)$ (Proposition 5.5). We remark that the polynomial $P(X,Y)$ is an additive polynomial. Therefore, if $y \in Z(\mathrm{Ad}_{f_1})$ and if $\sigma_y \in G_{\infty,1}(f_1)$ is such that $\sigma_y(X) = X + y$, then $\sigma_y(W) = W + P(X,y) + c$, for $c \in \mathbb{F}_p$ (Proposition 5.5), then $\sigma_y^p(W) = W + P(X,y) + P(X+y,y) + \cdots + P(X+(p-1)y,y) = W + (p(p-1)/2)P(y,y)$. So if $p > 2$ then $\sigma_y^p = \mathrm{Id}$ and consequently the exponent of $G_{\infty,1}(f_1)$ is p. If $y,z \in Z(\mathrm{Ad}_{f_1})$ then (Proposition 5.5) $\epsilon_{f_1}(y,z) = P(X,y) + P(X+y,z) - P(X,z) - P(X+z,y) = P(y,z) - P(z,y) = \sum_{0\leqslant i\leqslant n-1}(yz^q)^{p^i} - \sum_{0\leqslant i\leqslant n-1}(y^qz)^{p^i}$. Assume that $y \neq 0$ is such that σ_y is in the center of $G_{\infty,1}(f_1)$ (this condition does not depend on $c \in \mathbb{F}_p$ with $\sigma_y(W) = W + P(X,y) + c$). Then $\epsilon_{f_1}(y,z)$ as a polynomial in z should have p^{2n} roots which is a contradiction. So the center is $\langle\rho\rangle$ where $\rho(X) = X$ and $\rho(W) = W + 1$. □

Step 2. Realization of E with exponent p^2 (type I(b)).

We will use the Witt vectors of length 2 and modifications of the cover built for type I(a). Let

$$c(X,Y) = \frac{(X+Y)^p - X^p - Y^p}{p} = \sum_{1\leqslant i\leqslant p-1} \frac{(-1)^{i-1}}{i} X^iY^{p-i}$$

and

$$f_0(X) := c(X^p, -X) = \sum_{1\leqslant i\leqslant p-1} \frac{1}{i} X^{p+(p-1)i}.$$

A straightforward calculation in $W_2(\mathbb{F}_p)$ shows that $\Delta(f_0)(X,Y) = c((\mathrm{F}-\mathrm{Id})X, (\mathrm{F}-\mathrm{Id})Y) + (\mathrm{F}-\mathrm{Id})c(X,Y)$. As $c((\mathrm{F}-\mathrm{Id})X, (\mathrm{F}-\mathrm{Id})Y) = (Y^p - Y)(X^p - X)^{p-1} +$ lower X-degree terms $\in (Y^p - Y)\mathbb{F}_p[X,Y]$ it follows that $\mathrm{Ad}_{f_0}(Y) = Y^p - Y$ and for $y \in Z(\mathrm{Ad}_{f_0}(Y))$ (i.e. $y \in \mathbb{F}_p$) $P_{f_0}(X,y) = -c(X,y) = \sum_{1\leqslant i\leqslant p-1}((-1)^i/i)y^{p-i}X^i$ (cf. Proposition 5.5). One can prove that $G_{\infty,1}(f_0)$ is p^2-cyclic; in order to get an extraspecial group of exponent p^2 we use modifications of f_0. Let $q := p^n$, $f_1(X) = X^{1+q}$, θ a (q^2-1)th root of -1 (so that $\theta^{q^2} + \theta = 0$) and $A(X) := \theta X^q - \theta^q X$. Then $S(X) := A(X) + A(X)^p + \cdots + A(X)^{q/p}$ is an additive polynomial and $S(X)^p - S(X) = A(X)^q - A(X) = \theta^q(X + X^{q^2})$.

CLAIM. If $f_2(X) := \mathrm{red}(f_0(S(X))) + f_1(X)$, then $E \simeq G_{\infty,1}(f_2)$ and $|G_{\infty,1}(f_2)|/g(f_2) = 2p/(p-1)^2 < p/(p-1)$.

Proof. We have

$$\begin{aligned}\Delta(f_0)(S(X),S(Y)) &= c(S(X)^p - S(X), S(Y)^p - S(Y)) + (\mathrm{Id}-\mathrm{F})(-c(S(X),S(Y)))\\ &= c(A(X)^q - A(X), A(Y)^q - A(Y)) + (\mathrm{Id}-\mathrm{F})(-c(S(X),S(Y))) \qquad (5)\end{aligned}$$

and $\Delta(f_1)(X,Y) = Y^qX + YX^q$. We now show that $\mathrm{Ad}_{\mathrm{red}(f_0\circ S)}(Y) = \theta^{-q}\mathrm{Ad}_{f_0}(S(Y)) = Y + Y^{q^2}$ for $y + y^{q^2} = 0$. To this end, note that $f_0(S(X)) = c(S(X)^p, -S(X)) = \sum_{1\leqslant i\leqslant p-1}(1/i)S(X)^{p+(p-1)i}$ has conductor $1 + (p-1)q^2$ hence, by Proposition 6.6 III(ii), $\deg \mathrm{Ad}_{\mathrm{red}(f_0\circ S)} \leqslant q^2$. As, by Proposition 6.2, $\mathrm{Ad}_{f_0}(S(Y)) = S(Y)^p - S(Y) = A(Y)^q - A(Y) = \theta^q(Y + Y^{q^2})|\mathrm{Ad}_{\mathrm{red}(f_0\circ S)}(Y)$, we get the equality.

Note that $\mathrm{red}(f_0 \circ S)$ and f_1 have the same additive polynomial so, due to the property of second type modifications (Proposition 6.5), we obtain $Y + Y^{q^2}|\mathrm{Ad}_{f_2}(Y)$. As f_2 and $\mathrm{red}(f_0 \circ S)$ have the same conductor, the same argument as above gives $\deg \mathrm{Ad}_{f_2}(Y) \leqslant q^2$. Finally, we conclude that $\mathrm{Ad}_{f_2}(Y) = Y + Y^{q^2}$ showing the claim.

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

Next we show that $G_{\infty,1}(f_2)$ has exponent p^2. Let y be such that $\mathrm{Ad}_{f_2}(y)=\mathrm{Ad}_{\mathrm{red}(f_0\circ S)}(y)=\mathrm{Ad}_{f_1}(y)=0$. We need to calculate $\sum_{0\leqslant i\leqslant p-1}P_{f_2}(X+iy,y)$ (see Corollary 3.5). One has $P_{f_2}(X,y)=P_0(X,y)+P_1(X,y)$, where $P_1(X,Y):=P_{f_1}(X,Y)=y^qX+(y^qX)^p+\cdots+(y^qX)^{q/p}$ (Step 1) and $P_0(X,Y):=P_{\mathrm{red}(f_0\circ S)}(X,Y)$ can be deduce from (5) in the following way: for $y\in Z(\mathrm{Ad}_{f_2})$ we have $S(y)^p-S(y)=\theta^q(y+y^{q^2})=0$, so (5) gives $\Delta(f_0)(S(X),S(y))=(\mathrm{Id}-\mathrm{F})(-c(S(X),S(y)))$. As we can write $\mathrm{red}(f_0\circ S)(X)=f_0(X)+(\mathrm{Id}-\mathrm{F})h(X)$ it follows that

$$P_0(X,y)=-c(S(X),S(y))+\Delta(h)(X,y). \tag{6}$$

We easily see that $\sum_{0\leqslant i\leqslant p-1}\Delta(h)(X+iy,y)=0$, so we need to calculate $\sum_{0\leqslant i\leqslant p-1}c(S(X+iy),S(y))$. Note that $c(S(X),S(y))=\sum_{1\leqslant i\leqslant p-1}((-1)^{i-1}/i)S(y)^iS(X)^{p-i}$ and that S is an additive polynomial. If we set $Z:=S(y)S(X)^p-S(y)^pS(X)$ then

$$\sum_{0\leqslant i\leqslant p-1}P_0(X+iy,y)=\mathrm{Tr}_{k(S(X))/k(Z)}(-c(S(X),S(y)))=S(y)^p\quad\text{where } k=\mathbb{F}_p^{alg}.$$

For the contribution of P_1 we remark that f_1 induces an extraspecial group of exponent p so $\sum_{1\leqslant i\leqslant p-1}P_1(X+iy,y)=0$.

Finally, we have shown that $\sum_{0\leqslant i\leqslant p-1}P_{f_2}(X+iy,y)=S(y)^p$ and so for $y\in Z(\mathrm{Ad}_{f_2}(Y))-Z(S(Y))$ the element $\sigma_y\in G_{\infty,1}(f_2)$ has order p^2.

Now we show that the center is $\langle\rho\rangle$. If $y,z\in Z(\mathrm{Ad}_{f_2}(Y))$ then $\epsilon_j(y,z)=P_j(X,z)+P_j(X+z,y)-P_j(X,y)-P_j(X+y,z)$ for $j=1,2$.

We also saw that $\mathrm{Ad}_{f_0}(Y)=Y^p-Y$ and $G_{\infty,1}(f_0)$ is abelian (in fact cyclic), so $\epsilon_{\mathrm{red}(f_0\circ S)}(y,z)=\epsilon_{f_0}(S(y),S(z))=0$ (see Corollary 3.5 and Proposition 6.5). Finally $\epsilon_{f_2}(y,z)=\epsilon_1(y,z)=(z^qy+z^{qp}y^p+\cdots+z^{q^2/p}y^{q/p})-(zy^q+z^py^{pq}+\cdots+z^{q/p}y^{q^2/p})$. For $z\neq0$ this is a polynomial in y of degree q^2/p, so it has at most q^2/p roots and hence $z\in Z(G_{\infty,1}(f_2))$ if and only if $z=0$. □

Step 3. Realization of saturated subgroups of an extraspecial group E of exponent p^2 (type I(b)).

Note that $E/Z(E)$ is the group of automorphisms of $k[X]$ whose elements are $\sigma_y(X)=X+y$ where $y\in\mathrm{Ad}_{f_2}(Y)$. Then a subgroup $V\subset E/Z(E)$ corresponds to a monic additive polynomial S_V which divides $\mathrm{Ad}_{f_2}(Y)$ (see § 2). Note that necessarily S_V has distinct roots so $S_V=s_0X+s_1X^p+\cdots+X^{p^r}$ and $s_0\neq0$. As $\pi^{-1}(E/Z(E))=E$ we can assume that $0<r<2n$. We consider $\ell>1$ such that $(\ell(\ell+1),p)=1$ and $f(X):=\mathrm{red}(S_V(X)^{\ell+1})+f_2(X)=\mathrm{red}(S_V(X)^{\ell+1})+\mathrm{red}(f_0(S(X)))+f_1(X)$.

Our aim is first to find ℓ such that $\mathrm{Ad}_f(Y)=S_V(Y)$.

We remark that the conductors for these three contributions are, respectively, $1+\ell p^r$, $1+(p-1)q^2$ and $1+q$. We adopt the notation of Lemma 5.1 and, as in the proof of Corollary 5.3, we consider $j_0=1+(\ell-1)p^r$ and we calculate the coefficient of $X^{j_0p^{n(j_0)}}$ in $R(X,Y)$.

- We show that the contribution from $\Delta(S_V^{\ell+1})(X,Y)$ is $[((\ell+1)!/1!\dots1!(\ell-1)!)S_V(Y)s_0]^{p^{n(j_0)}}$. One has $pj_0>(\ell+1)p^r$, so the only contribution comes from the monomial X^{j_0} and we claim that its coefficient is $((\ell+1)!/1!\dots1!(\ell-1)!)S_V(Y)s_0$. Namely one has $\Delta(S_V^{\ell+1})(X,Y)=(S_V(Y)+s_0X+\cdots+X^{p^r})^{\ell+1}-S_V(Y)^{\ell+1}-S_V(X)^{\ell+1}$, so one needs to solve the following system of equations $i+i_0+\cdots+i_r=\ell+1$ and $i_0+i_1p+i_2p^2+\cdots+i_rp^r=j_0$ where $i\in\{1,2,\dots,\ell\}$. We get $p^r-1=(i-1)p^r+i_0(p^r-1)+i_1(p^r-p)+\cdots+i_{r-1}(p^r-p^{r-1})$. It follows that $p|i_0-1$ and $i_0\leqslant1$ so $i_0=1$ and $i=1$, $i_1=i_2=\cdots=i_{r-1}=0$ and so $i_r=\ell-1$. This proves the claim.
- For the contribution from $\Delta(\mathrm{red}(f_0\circ S))(X,Y)$ we distinguish two cases.

Case $p>3$. If ℓ is such that $((\ell-1)\ell(\ell+1),p)=1$ (for example $\ell=2$) then there is no contribution of $\Delta(\mathrm{red}(f_0\circ S))(X,Y)$.

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

Proof. We have (Step 2) $\Delta(f_0 \circ S)(X,Y) = c(A(X)^q - A(X), A(Y)^q - A(Y)) + (\mathrm{F} - \mathrm{Id})c(S(X), S(Y))$ and $c(A(X)^q - A(X), A(Y)^q - A(Y)) = c(\theta^q(X^{q^2} + X), \theta^q(Y^{q^2} + Y)) = \theta^{pq} \sum_{1 \leqslant i \leqslant p-1}((-1)^{i-1}/i)$ $(Y^{q^2} + Y)^{p-i}(X^{q^2} + X)^i$. We remark that the equation $i_0 + i_1 q^2 = p^\alpha j_0$ with $i_0 + i_1 = i$, $1 \leqslant i \leqslant p-1$ and $\alpha \in \mathbb{N}$ is equivalent to $\alpha = 0$, $i_0 = 1$ and $\ell - 1 = i_1 p^{2n-r}$. Hence, if $((\ell-1)\ell(\ell+1), p) = 1$ there is no contribution. □

Case $p = 3$. Take $\ell = 4$. Then the equation above gives $i_1 3^{2n-r} = 3$ which has a solution if and only if $r = 2n-1$ and then $i_1 = 1$ and $i = i_0 + i_1 = 2$. Let us assume that $r = 2n-1$. Then the contribution to the coefficient of $X^{j_0 p^{n(j_0)}}$ is $[2\theta^{3q}(Y^{q^2} + Y)]^{p^{n(j_0)}}$.

Clearly there is no contribution from $\Delta(f_1)(X,Y)$.

Let us now show that $\mathrm{Ad}_f(Y) = S_V(Y)$.

If $p > 3$ and $((\ell-1)\ell(\ell+1), p) = 1$, it follows that $\mathrm{Ad}_f(Y)$ divides $S_V(Y)$ which itself divides $\mathrm{Ad}_{f_2}(Y) = Y + Y^{q^2}$ and so $\mathrm{Ad}_f(Y) = S_V(Y)$.

If $p = 3$ take $\ell = 4$ then the same proof works unless $r = 2n-1$ and then $\mathrm{Ad}_f(Y)$ divides $T(Y)^{p^{n(j_0)}}$ where $T(Y) := 2S_V(Y)s_0 + 2\theta^{pq}(Y^{q^2} + Y)$. We can write $Y^{q^2} + Y = (Y - \alpha)S_V(Y)$. Then $s_0\alpha = -1$ and $T(Y) = 2\theta^{pq}S_V(Y)(Y - \beta)$, with $\beta = \alpha - \theta^{-pq}s_0$. We remark that $s_0^{q^2} + s_0 = 0$ and $\theta^{q^2} + \theta = 0$, so $\beta^{q^2} + \beta = -2\theta^{-pq}s_0 \neq 0$. In particular, β is not a root of $Y^{q^2} + Y$ (and so of $S_V(Y)$). As $\mathrm{Ad}_f(Y)$ is an additive polynomial we still get that it divides $S_V(Y)$.

We remark that, by Corollary 5.3, $\mathrm{Ad}_{X^{\ell+1}}(Y) = Y$ and so $\mathrm{Ad}_{S_V^{\ell+1}(Y)} = S_V(Y)$ by Proposition 6.2. Then, by Proposition 6.5, for $y, z \in Z(S_V(Y))$ one has $\epsilon_f(y,z) = \epsilon_{S_V^{\ell+1}}(y,z) + \epsilon_{f_2}(y,z)$. As $\epsilon_{S_V^{\ell+1}}(y,z) = 0$ (Proposition 6.2), the commutation rule is that of E.

Case $p = 2$. Let E be the extraspecial group of type II(b) and order pq^2, i.e. it is the central product of Q_8 and $n-1$ copies of D_8.

Step 1. Realization of E.

Claim. Let $f_1(X) := X^{1+q}$ then $E \simeq G_{\infty,1}(f_1)$ and $|G_{\infty,1}(f_1)|/g(f_1) = (2p/(p-1))q > 2p/(p-1)$.

The proof is the same as for type I(a). We use the same calculation up to the point where we used specifically that $p = 2$. We have seen that $\sigma_y^p(W) = W + P(X,y) + P(X+y,y) + \cdots + P(X + (p-1)y, y) = W + (p(p-1)/2)P(y,y)$. So this time as $p = 2$, $\sigma_y^2(W) = W + P(y,y)$ where $P(Y,Y) = \sum_{0 \leqslant i \leqslant n-1} Y^{(q+1)p^i}$ and $Q(Y) := P(Y,Y)Y^{-q} = \sum_{0 \leqslant i \leqslant n-1} Y^{(q+1)p^i - q}$ is a separable polynomial of degree $2^{2n-1} + 2^{n-1} - 2^n$. Define $d(n)$ to be the number of elements of order at most 2, they correspond to those $y \in Z(\mathrm{Ad}_{f_1})$ such that $P(y,y) = 0$ (this condition does not depend on c). Moreover $P(Y,Y)^2 - P(Y,Y) = Y^{2^n}(Y^{2^{2n}} + Y)$, hence the roots of $Q(Y)$ are simple and among those of Ad_{f_1}. It follows that $d(n) = 2(2^{2n-1} + 2^{n-1} - 2^n) = 2^{2n} - 2^n = d_b(n)$ and so $G_{\infty,1}(f_1)$ is an extraspecial group of type II(b) (see § 4.1).

Step 2. Realization of saturated subgroups in E.

If $S_V(Y)$ is the additive polynomial corresponding to a saturated subgroup we take $f(X) = (\mathrm{red}S_V(X))^7 + X^{1+2^n}$. The conductor is $1 + 6 * 2^{2(n-1)}$. We look at the contribution of $\Delta(S_V^7)(X,Y) = (S_V(Y) + s_0X + \cdots + X^{2^r})^7 - S_V(Y)^7 - S_V(X)^7$. The contribution $S_V(Y)^2 s_0 X^{1+2^{r+2}}$ is the only one in degrees $(1 + 2^{r+2})2^{\mathbb{N}}$ and we conclude as in the $p > 2$ case.

Remark 7.2. Let $p > 2$ and G be a p-group belonging to the class C_1. The proof of the theorem above gives a realization of this group as a group $G_{\infty,1}(f)$ through an embedding in an extraspecial group of type I(b) hence of exponent p^2. In the case that the group G has exponent p one gets simpler realizations in considering G as a saturated subgroup of an extraspecial group of the same

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

exponent p, i.e. of type I(a) (see Remark 4.5). Following the same line as in Step 3 for $p > 2$, one can show that $f(X) = \mathrm{red}(S_V(X)^{\ell+1}) + f_1(X)$ gives a realization for G.

7.2 An application: realization of extraspecial groups of type II(a)

We have not yet given an explicit realization of extraspecial groups of type II(a) (see Definition 4.3). Such a group with cardinality $2^{2(n-1)+1}$ is the central product $D_8 * \cdots * D_8$ ($n-1$ times). Let us explain how we get such a realization using the method above. This group is a saturated subgroup of the extraspecial group of type II(b), $Q_8 * D_8 * \cdots * D_8$ of cardinality 2^{2n+1}. The construction above gives the existence of $f(X) = S_V(X)^7 + X^{1+2^n}$ where S_V is an additive polynomial of degree 2^{n-1} such that the automorphism group $G_{\infty,1}(f)$ is the saturated subgroup $D_8 * \cdots * D_8$ ($n-1$ times). Note that the conductor is $1 + 6 * 2^{2(n-1)}$ and so $|G_{\infty,1}(f)|/g(f) = \frac{2}{3}$ gives the sharp bound for such a conductor (Proposition 6.6). More concretely we now give an explicit realization of D_8 ($n = 2$) with conductor 25 which is the minimal one (see B(ii) below and compare with the realization given in § 5.3).

We view D_8 as a saturated subgroup $\pi^{-1}(V)$ of the extraspecial group $E := Q_8 * D_8$ where $\pi : E \to E/Z(E) = W$ for which we know that $f_1(X) = X^{1+2^2}$ gives a realization. The corresponding additive polynomial is $\mathrm{Ad}_{f_1}(Y) = Y^{2^4} + Y$ and $W = Z(\mathrm{Ad}_{f_1}) \subset \mathbb{F}_2^{alg}$. Then V is a subgroup of order 4 and $V = Z(S_V)$, where S_V is an additive polynomial dividing Ad_{f_1}. Therefore, we can write $S_V(Y) = Y^4 + aY^2 + bY$ where $b \neq 0$.

The remainder of the division of $Y^{16} + Y$ by $Y^4 + aY^2 + bY$ is $(1 + b^5 + ba^6)Y + (b^2a^4 + ab^4 + a^7)Y^2$. Consequently we get the two equations $1 + b^5 + ba^6 = 0$ and $b^2a^4 + ab^4 + a^7 = 0$. For each couple (a, b) satisfying these equations we consider $f_{a,b} := (X^4 + aX^2 + bX)^7 + X^5$ and then we get $\mathrm{Ad}_{f_{a,b}}(Y) = Y^4 + aY^2 + bY$. If $y \in W(= E/Z(E))$ then $P_{f_1}(X, y) + P_{f_1}(X + y, y) = y^4(y^6 + y)$. We remark that $Y^6 + Y$ divides $\mathrm{Ad}_{f_1}(Y) = Y^{16} + Y$ and the quotient is $Y^{10} + Y^5 + 1$. This gives a partition of W into two sets. W_2: the roots of $Y^6 + Y$ corresponding to the 12 elements of $G_{\infty,1}(f_1)$ of order at most 2 and W_4: the roots of $Y^{10} + Y^5 + 1$ corresponding to the 20 elements of $G_{\infty,1}(f_1)$ of order 4. Now $V := Z(\mathrm{Ad}_{f_{a,b}})$ is a subgroup of W and for $y \in V$ one has $P_{f_1}(X, y) = P_{f_{a,b}}(X, y)$ and so $P_{f_{a,b}}(X, y) + P_{f_{a,b}}(X + y, y) = y^4(y^6 + y)$. Concerning the commutation rule for $y, z \in V \subset W$ we have $\epsilon_{f_{a,b}}(y, z) = \epsilon_{f_1}(y, z) = z^2y^8 + zy^4 + z^8y^2 + z^4y = yz(y + z)(y^2 + zy + z^2)(zy^4 + z^4y + 1)$.

A. $a = 0$ and $1 + b^5 = 0$. Note that in this case $\mathrm{Ad}_{f_{a,b}}(Y) = Y^4 + bY$ and only the roots $y = 0$ and $y = b^2$ are in W_2. Moreover for $y, z \in V$ one has $yz(y + z)(y^2 + zy + z^2) = yz(y^3 + z^3) = 0$. It follows that the group $G_{\infty,1}(f_{a,b})$ is abelian, isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

B. Let $A := b^5 + a^6b + 1$ and $B := b^4 + a^3b^2 + a^6$. Then the resultant of A and B in b is $(b^5+1)(b^{10}+b^5+1)^2$. The case $b^5+1 = 0$ is Case 1 above. Now we can assume that $b^{10}+b^5+1 = 0$, i.e. b is a primitive 15th root of 1. The equations $A = B = 0$ give three sets of covers.

   (i) $ab = 1$, i.e. $a = b^{14}$. In this case $Y^4 + aY^2 + bY$ divides $Y^6 + Y$. Then the group has exponent 2 and it is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$.

   (ii) $ab = b^5$ i.e. $a = b^4$. In this case $Y^4 + aY^2 + bY$ has only one root (b^7) in common with $Y^{10} + Y^5 + 1$. It follows that the group $G_{\infty,1}(f_{a,b})$ has two elements of order 4 and so it is D_8. We can write $\mathrm{red}(f_{a,b}) = (b^{14} + b^5)X + (b + b^8)X^3 + (1 + b^{14} + b^{13})X^5 + (b^7 + 1)X^7 + (b^{13} + b^{10})X^9 + (b^4 + b + b^6)X^{11} + (b^2 + 1)X^{13} + b^2X^{17} + b^3X^{19} + b^9X^{21} + bX^{25}$, which is defined over $\mathbb{F}_{16}$.

   (iii) $ab = b^{10}$, i.e. $a = b^9$. In this case $(Y^4 + aY^2 + bY)/Y$ divides $Y^{10} + Y^5 + 1$ and it follows that the group $G_{\infty,1}(f_{a,b})$ has six elements of order 4, so this is Q_8.

Remark 7.3. We could also obtain families. For this it suffices to deal with f_1 giving a family, for example $f_1 = tX^3 + X^5$ (see Proposition 8.1 A(ii)). However, the corresponding discussion is more delicate than the above.

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

8. Maximal curves

8.1 Universal family

We have seen that if $g(C_f) \geqslant 2$ then $|G_{\infty,1}(f)|/g(f)^2 \leqslant 4p/(p-1)^2$ and we have equality for $f = X^{1+p^n}$. In fact this equality characterizes the f with $\mathrm{red}(f) \neq 0$ and of the form $S_1(X)S_2(X)$ where for $i = 1, 2$ the S_i are additive polynomials. Namely for a given genus there is a universal family given in the following.

Proposition 8.1. *Let $n > 1$, $A_n := \mathbb{F}_p^{alg}[t_i, 0 \leqslant i \leqslant n]$ and $f := t_0X^{1+p^0} + t_1X^{1+p} + \cdots + t_{n-1}X^{1+p^{n-1}} + t_nX^{1+p^n} \in A_n[X]$. Let k be an algebraically closed field and $\varphi : A_n \to k$ a specialization homomorphism such that $\varphi(t_n) \neq 0$. Then $\mathrm{Ad}_{\varphi(f)}(Y) = \varphi(\sum_{0\leqslant i\leqslant n}(t_i^{p^{n-i}}Y^{p^{n-i}} + t_i^{p^n}Y^{p^{n+i}})) = \varphi(t_n)Y + \cdots + (\varphi(t_n))^{p^n}Y^{p^{2n}}$ and $|G_{\infty,1}(\varphi(f))| = p^{2n+1}$. Furthermore we have the following.*

A. (i) *If $p > 2$, then $\varphi(f)$ is reduced and $G_{\infty,1}(\varphi(f))$ is an extraspecial group of type I(a).*
   (ii) *If $p = 2$, and $t_0 = 0$, then $\varphi(f)$ is reduced and $G_{\infty,1}(\varphi(f))$ is an extraspecial group of type II(b).*

B. *Let $\pi : \mathcal{X} = \mathrm{Spec}(A_n[t_n^{-1}][X, W]/(W^p - W - f)) \to \mathrm{Spec}A_n[t_n^{-1}]$ be the structure morphism. This is a flat family of curves and the fibers are highly singular. Let us consider the normalization $\tilde{\pi} : \tilde{\mathcal{X}} \to \mathrm{Spec}A_n[t_n^{-1}]$. As the fibers have the same conductor, and flatness is an open condition, after a suitable localization we get a smooth family over some nonempty open $\mathrm{Spec}A_n[Q^{-1}] \subset \mathrm{Spec}A_n[t_n^{-1}]$. Each geometric fiber of this family has genus $g_n := p^n(p-1)/2$. The geometric generic fiber is the curve $C_{\mathrm{Id}(f)}$. The group $G_{\infty,1}(\mathrm{Id}(f))$ acts faithfully on each fiber $\tilde{C}_{\varphi(f)}$ and is identified with the group $G_{\infty,1}(\varphi(f))$.*

Proof. A. In Theorem 7.1 (Case $p > 2$, Step 1 and Case $p = 2$, Step 1) we have shown A for $\varphi = \varphi_0$ where $\varphi_0(t_i) = 0$ for $i < n$ and $\varphi_0(t_n) = 1$. In the general case, for the convenience of the reader, we repeat the argument in detail. Write $f_i = t_iX^{1+p^i}$ with $t_0 = 0$ for $p = 2$. Then $\Delta(f)(X, Y) = \sum_{0\leqslant i\leqslant n}\Delta(f_i)$, where $\Delta(f_i) = A_i + B_i$, $A_i = t_iYX^{p^i}$, $B_i = t_iY^{p^i}X$. We can write $\Delta(f_i) = (t_i^{p^{n-i}}Y^{p^{n-i}} + t_i^{p^n}Y^{p^{n+i}})X^{p^n} + P_i - P_i^p$ where $P_i = A_i + \cdots + A_i^{p^{n-i-1}} + B_i + \cdots + B_i^{p^{n-1}}$ for $i \leqslant n-1$ and $B_i + \cdots + B_i^{p^{n-1}}$ for $i = n$. One obtains $\mathrm{Ad}_{\varphi(f)}(Y) = \sum_{0\leqslant i\leqslant n}((\varphi(t_i))^{p^{n-i}}Y^{p^{n-i}} + (\varphi(t_i))^{p^n}Y^{p^{n+i}}) = \varphi(t_n)Y + \cdots + (\varphi(t_n))^{p^n}Y^{p^{2n}}$ is a separable, additive polynomial with constant degree p^{2n}; it follows that $|G_{\infty,1}(\varphi(f))| = p^{2n+1}$ is constant.

Now we can describe the isomorphism class of the group $G_{\infty,1}(\varphi(f))$. We remark that $P(X, Y) = \sum_{0\leqslant i\leqslant n}P_i(X, Y)$ is an additive polynomial. When considering $P(X, Y)$ as a polynomial in X and with coefficients in $A_n[Y]$, the monomial of highest X-degree is

$$(\varphi(t_n)^{p^{n-1}}Y^{p^{2n-1}} + \sum_{0\leqslant i\leqslant n-1}((\varphi(t_i))^{p^{n-1-i}}Y^{p^{n-1-i}} + (\varphi(t_i))^{p^{n-1}}Y^{p^{n-1+i}}))X^{p^{n-1}}.$$

When considering $P(X, Y)$ as a polynomial in Y and with coefficients in $A_n[X]$, the monomial of highest Y-degree is $(\varphi(t_n))^{p^{n-1}}X^{p^{n-1}}Y^{p^{2n-1}}$. Now if $y, z \in Z(\mathrm{Ad}_{\varphi(f)})$ then (cf. Proposition 5.5) $\epsilon_{\varphi(f)}(y, z) = \varphi(P_f)(X, y) + \varphi(P_f)(X + y, z) - \varphi(P_f)(X, z) - \varphi(P_f)(X + z, y) = \varphi(P_f)(y, z) - \varphi(P_f)(z, y)$. Assume $y \neq 0$ is such that σ_y (see Proposition 5.5) is in the center of $G_{\infty,1}(\varphi(f))$ then $\epsilon_{\varphi(f)}(y, z)$ as a polynomial in z should have p^{2n} roots which is a contradiction as the polynomial $\varphi(P)(Y, Z) - \varphi(P)(Z, Y)$ has Z-degree p^{2n-1}. So the center is $\langle\rho\rangle$ where $\rho(X) = X$ and $\rho(W) = W + 1$ and so $G_{\infty,1}(\varphi(f))$ is an extraspecial group of order p^{2n+1}. In order to determine the type we look at the exponent. If $y \in Z(\mathrm{Ad}_{\varphi(f)})$ then $P(X, y) + P(X + y, y) + \cdots + P(X + (p-1)y, y) = W + p(p-1)/2P(y, y)$. Hence (see Proposition 5.5) if $p > 2$ then $\sigma_y^p = \mathrm{Id}$ and consequently the exponent of $G_{\infty,1}(\varphi(f))$ is p; this ends the proof when $p > 2$. If $p = 2$ then $\sigma_y^2(W) = W + P(y, y)$

where $P(Y,Y) = \sum_{1\leqslant i\leqslant n}(B_i^{2^{n-i}} + \cdots + B_i^{2^{n-1}}) \in A_n[Y]$. Its lowest degree monomial is B_n and the one of highest degree is $B_n^{2^{n-1}}$. It follows that $Q(Y) := P(Y,Y)Y^{-2^n}$ is a separable polynomial of degree $2^{2n-1} + 2^{n-1} - 2^n$. Define $d(n)$ to be the number of elements of order at most 2 in $G_{\infty,1}(\varphi(f))$; they correspond to those $y \in Z(\mathrm{Ad}_{\varphi(f)})$ such that $P(y,y) = 0$. Moreover one checks easily that $P(Y,Y)^2 - P(Y,Y) = Y^{2^n}\mathrm{Ad}_{\varphi(f)}$, hence the roots of $Q(Y)$ are simple and among those of $\mathrm{Ad}_{\varphi(f)}$. It follows that $d(n) = 2(2^{2n-1} + 2^{n-1} - 2^n) = 2^{2n} - 2^n = d_b(n)$ and so $G_{\infty,1}(\varphi(f))$ is an extraspecial group of type II(b) (see § 4.1).

B. This is a special case of the following ([Liu02, Corollary 2.13, p. 224, and Proposition 8.3.11, p. 352 (Proof)]). Let $f : X \longrightarrow T$ be a proper dominant morphism with T irreducible. If the generic fiber is smooth then there is a nonempty open $U \subset T$ such that $f^{-1}(U) \longrightarrow U$ is smooth. □

Remark 8.2. Such a family was previously considered in the literature in connection with coding theory. Namely in [vdGV92] the specialization morphisms φ taking values in $\mathbb{F}_{p^{2n}}$ are studied. The additive polynomial $\mathrm{Ad}_{\varphi(f)}$ is then their polynomial $E_n(Y) = S(Y)^{p^n} + \sum_{0\leqslant i\leqslant n}(t_iY)^{p^{n-i}}$ where $S(X) = \sum_{0\leqslant i\leqslant n} t_iY^{p^i}$. The zeros are interpreted as the $\mathbb{F}_p$-vector space which is the kernel of the $\mathbb{F}_p$-bilinear form $\mathrm{Tr}_{\mathbb{F}_{p^{2n}}/\mathbb{F}_p}(xS(y) + yS(x))$ (which is symmetric if $p > 2$ and alternating if $p = 2$). In case $p = 2$, they also prove a factorization of $E_n(Y) = YE_n^-(Y)E_n^+(Y)$ which corresponds to a partition of the roots depending on the order of the corresponding automorphism of C_f. Such a decomposition works in general. They give the structure of the groups $G_{\infty,1}(\varphi(f))$.

An approach more closely related to ours can be found in [Elk99] (notably, paragraph 5). There the polynomials $\mathrm{Ad}_{\varphi(f)}(Y) = \varphi(\sum_{0\leqslant i\leqslant n}(t_i^{p^{n-i}}Y^{p^{n-i}} + t_i^{p^n}Y^{p^{n+i}}))$ are studied on their own. They form the class of 'the palindromic polynomials'.

8.2 Application to the moduli space of curves

We keep the notations of Proposition 8.1. For a fixed $n > 1$ let $A_n := \mathbb{F}_p^{alg}[t_i, 0 \leqslant i \leqslant n-1]$ and $f := t_0X^{1+p^0} + t_1X^{1+p} + \cdots + t_{n-1}X^{1+p^{n-1}} + t_nX^{1+p^n} \in A_n[X]$ with $t_n = 1$. (As soon as $t_n \neq 0$, after a change of variable, this condition is satisfied.) For $p = 2$ we take $t_0 = 0$ (in order to have f be reduced) and set $g_n := p^n(p-1)/2$. Let $\theta \in \mathbb{F}_p^{alg}$ be a primitive $(p-1)(p^n+1)$th root of 1. Then $\Theta : (t_0, \dots, t_{n-1}) \to (\theta^{p^n-p^0}t_0, \theta^{p^n-p^1}t_1, \dots, \theta^{p^n-p^{n-1}}t_{n-1})$ induces an $\mathbb{F}_p^{alg}$-automorphism of $\mathrm{Spec}A_n$ of order p^n+1. Let $B_n := A_n^{\langle\Theta\rangle}$ be the quotient of the affine space by the cyclic group of automorphisms $\langle\Theta\rangle$. The structure morphism $\pi : \tilde{C}_f \to \mathrm{Spec}A_n[Q^{-1}]$ is a family of curves of genus g_n (Proposition 8.1). Moreover, by Proposition 3.3 two specialization morphisms $\varphi_i : A_n \to k$, for $i = 1,2$ will give isomorphic k-curves if and only if $\exists c \in \mathbb{F}_p^\times$ and $(a,b) \in (k^\times, k)$ such that $\sum_{0\leqslant i\leqslant n-1}\varphi_2(t_i)(aX+b)^{1+p^i} + (aX+b)^{1+p^n} = c(\sum_{0\leqslant i\leqslant n-1}\varphi_1(t_i)X^{1+p^i} + X^{1+p^n}) \bmod (\mathrm{Id} - \mathrm{F})k[X]$. It follows that $a^{1+p^n} = c \in \mathbb{F}_p^\times$ and for $i \geqslant 0$ one has $\varphi_2(t_i) = ca^{-(1+p^i)}\varphi_1(t_i) = a^{p^n-p^i}\varphi_1(t_i)$. (Note that for $p = 2$ we have assumed $t_0 = 0$ and so f is reduced.) Conversely these conditions (take $b = 0$) define two specialization morphisms which give isomorphic k-curves which are in the same orbit under the action of the group Θ. By the definition of the coarse moduli space M_{g_n}, we deduce from the existence of the family $\tilde{C}_f \to \mathrm{Spec}A_n[Q^{-1}]$ a map from $\mathrm{Spec}A_n[Q^{-1}]$ to M_{g_n}. This map factors through $\mathrm{Spec}B_n[N(Q)^{-1}]$ (where $N(Q) := \prod_{0\leqslant i\leqslant p^n}\Theta^i(Q)$) in an injective morphism. The image is an algebraic subset of M_{g_n} of the same dimension as that of $\mathrm{Spec}B_n$. A measure of the size of families of curves which are étale covers of the affine line, and with given extraspecial group of type I(a) and order p^{2n+1} as an automorphism group, is given by the dimension of this image, which is $O(\log(g_n))$.

8.3 Characterization of maximal p-cyclic covers of the affine line

It is remarkable that these families for varying n can be characterized by the following Hurwitz-type bound.

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

PROPOSITION 8.3. *Let k be an algebraically closed field, $p = \operatorname{char}(k) > 0$ and $f(X) \in Xk[X]$ a polynomial of degree $m := \deg f$ prime to p. We assume f is reduced. If $|G_{\infty,1}(f)|/g(f) > p/(p-1)$ ($\frac{2}{3}$ for $p = 2$) then $f(X) = XS(X)$, where $S(X) - S(0)$ is an additive polynomial. Moreover, if $\deg S = p^n$ then $|G_{\infty,1}(f)|/g(f) = 2p^n p/(p-1)$ and $|G_{\infty,1}(f)|/g(f)^2 = 4p/(p-1)^2$ (see Proposition 8.1).*

Proof. The proof works by elimination of bad monomials. We saw in Proposition 6.6 that only for $m = 1 + p^s$ with $s > 0$, $|G_{\infty,1}(f)|/g(f)$ can be greater than $p/(p-1)$ ($\frac{2}{3}$ if $p = 2$). Now we show that any other monomial in $f(X)$ has exponent 1 or $1 + p^t$ with $t < s$.

Let us assume that this is not the case and denote by X^a the monomial of highest degree which is not of the above form. We first assume that p does not divide $a - 1$ (such a case does not occur if $p = 2$) and consider the integer k such that $p^{k-1} < a - 1 < p^k$. Then $k \leqslant s$ and $p^{s-1} < (a-1)p^{s-k} < p^s$. Further the monomial in X^a has a contribution in $R(X, Y)$ (defined in Lemma 5.1) which is equal to $a^{p^{s-k}}Y^{p^{s-k}}X^{(a-1)p^{s-k}} +$ other terms. Moreover, as for $\alpha > 0$ we have $p^\alpha(a-1) > (a-1)$, it follows that $a^{p^{s-k}}Y^{p^{s-k}}$ is exactly the coefficient of $X^{(a-1)p^{s-k}}$ in R. This would imply that $|G_{\infty,1}(f)| \leqslant p$ and $|G_{\infty,1}(f)|/g(f) \leqslant 2p/((p-1)p^s) \leqslant p/(p-1)$, a contradiction.

Let us now assume that $a - 1 = \ell p^t$, where $\ell > 1$, $(\ell, p) = 1$ and $t > 0$. Let $j_0 = 1 + (\ell - 1)p^t$ and say $p^{k-1} < j_0 < p^k$. Then $p^{s-1} < j_0 p^{s-k} < p^s$ and $pj_0 < a$ if and only if $\ell < p/(p-1) - 1/p^t$ but this is not the case. Hence the monomial X^a contributes to $R(X, Y)$ in the monomial $X^{j_0 p^{s-k}}$ with only one term which is equal to $(\ell Y^{p^t})^{p^{s-k}}X^{j_0 p^{s-k}}$. Any other contribution to R in the monomial $X^{j_0 p^{s-k}}$ can only occur from a monomial X^b with $j_0 < b < a$. Now such a contribution will be $(\binom{b}{j_0}Y^{b-j_0})^{p^{s-k}}$ whose degree is at most $(b - j_0)p^{s-k} < (a - j_0)p^{s-k} = p^{t+s-k}$. Finally we get that $\deg \mathrm{Ad}_f(Y) \leqslant p^{t+s-k}$. From this we get $|G_{\infty,1}(f)|/g(f) \leqslant 2p^{t+s-k+1}/p^s(p-1)$ and so $1 < 2p^{t-k}$, i.e. $t \geqslant k$ for $p > 2$ ($\frac{1}{3} < 2^{t-k+1}$ and $t \geqslant k - 1$ for $p = 2$). On the other hand, $(\ell - 1)p^t < p^k$, so $(\ell - 1) < 1/p^{t-k}$, a contradiction. □

8.4 Maximal p-group actions

In [Sti73a], Stichtenoth proved that if C is a nonsingular projective curve over k with genus $g_C \geqslant 2$ then $|\mathrm{Aut}_k(C)| \leqslant 16g_C^4$ unless C is birational to a curve $W^{p^n} + W = X^{1+p^n}$ ($p = \operatorname{char} k$). In fact he obtained this general bound as a corollary to his study of p-cyclic (étale) covers of the affine line with conductor m. Namely it follows from the bound for p-Sylow subgroups $|G_{\infty,1}(f)| \leqslant p(m-1)^2$ for $f \in k[X]$ of degree m prime to p (see [Sti73b, Satz 4] and Corollary 5.3(i)). In the same spirit, Proposition 8.3 has a corollary on automorphisms groups of curves. Namely we can describe the curves C with a 'big' p-group of automorphisms G. First we need to define what we mean by 'big'.

For this we use Nakajima's extension of Stichtenoth's work in order to circumvent group actions on curves contradicting Hurwitz-type bounds. Namely in [Nak87, Theorem 1] he concentrated on p-group actions and gave bounds on the size of the group in terms of the Hasse–Witt invariant of the curve. The following proposition is a translation of his results. Let us first make a definition.

DEFINITION 8.4. Let C be a nonsingular projective curve over k and G a p-subgroup of $\mathrm{Aut}_k C$. We say that (C, G) satisfies condition (N) if $g_C > 0$ and $|G|/g_C > 2p/(p-1)$.

PROPOSITION 8.5. *Assume (C, G) with $g_C \geqslant 2$ satisfies condition (N). Then there is a point, say $\infty \in C$, such that G is the wild inertia subgroup of G at ∞. Moreover C/G is isomorphic to $\mathbb{P}^1_k$ and the ramification locus (respectively branch locus) of the cover $\pi : C \to C/G$ is the point ∞ (respectively $\pi(\infty)$). We define the ramification groups in lower notation G_i ($i \geqslant 0$) by*

$$G_0 := \{\sigma \in G \mid \sigma(\infty) = \infty\} = G$$

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

and for $i \geqslant 1$

$$G_i := \{\sigma \in G_0 \mid \mathrm{ord}_\infty(\sigma(\pi_\infty) - \pi_\infty) \geqslant i+1\},$$

where π_∞ *is a uniformizing parameter at* $\infty \in C$ *and* ord *is the order function at* ∞. *Let* i_0 *be the integer such that* $G_2 = G_3 = \cdots = G_{i_0} \supsetneqq G_{i_0+1}$.

(i) *Then* $G_2 \neq G_1$ *and the quotient curve* C/G_2 *is isomorphic to* $\mathbb{P}^1_k$.

(ii) *Let* H *be a subgroup which is normal in* G *and such that* $g_{C/H} > 0$. *Then* G/H *is a* p*-subgroup of* $\mathrm{Aut}_k C/H$ *and* $|G|/g_C \leqslant |G/H|/g_{C/H}$. *In particular* $(C/H, G/H)$ *satisfies condition (N). Moreover if* $M \leqslant |G|/g_C^2$ *for some* M *one gets* $|H| \leqslant (1/M)|G/H|/g_{C/H}^2$.

(iii) *Let* H *be a subgroup which is normal in* G *and* $G_2 \supsetneqq H \supset G_{i_0+1}$. *Then* $g_{C/H} = (|G_2/H| - 1)(i_0 - 1)/2 > 0$ *and* $(C/H, G/H)$ *satisfies condition (N).*

Proof. (i) When we compare the condition $|G|/g_C > 2p/(p-1)$ to [Nak87, Theorem 1], we see that C has Hasse–Witt invariant zero; moreover, it follows from the proof that the branch locus is reduced to one point and the ramification is total. Now we apply the Hurwitz formula to the cover $C \to C/G$. We have

$$2(g_C - 1) = |G|2(g_{C/G} - 1) + \sum_{0 \leqslant i}(|G_i| - 1). \tag{7}$$

As $G = G_0 = G_1$ we get

$$g_C \geqslant |G| g_{C/G}. \tag{8}$$

This together with the assumption $|G|/g_C > 2p/(p-1)$ implies $g_{C/G} = 0$. Now if $G_2 = G_1$ then (7) yields $2(g_C - 1) \geqslant |G|2(0-1) + 3(|G| - 1)$ which is a contradiction.

(ii) Let H be a normal subgroup of G then G/H is a p-subgroup of $\mathrm{Aut}_k C/H$ so, as in (8), we have

$$g_C \geqslant |H| g_{C/H}. \tag{9}$$

If $g_{C/H} \neq 0$ we get $|G|/g_C \leqslant |G/H|/g_{C/H}$. Now if $M \leqslant |G|/g_C^2$, one has

$$|H| \leqslant \frac{1}{|H|}\frac{g_C^2}{g_{C/H}^2} \leqslant \frac{1}{M}\frac{|G/H|}{g_{C/H}^2}.$$

(iii) Under the condition $G_2 \supsetneqq H \supset G_{i_0+1}$ we can calculate $g_{C/H}$. For this we remark that the cover $C/H \to C/G_2$ is Galois with group G_2/H which is elementary abelian. The ramification groups are $G_2/H = (G_2/H)_0 = (G_2/H)_1 = \cdots = (G_2/H)_{i_0} \supset (G_2/H)_{i_0+1} = \{0\}$ (exercise). It follows from (7) that $2(g_{C/H} - 1) = |G_2/H|(0-2) + (i_0+1)(|G_2/H| - 1)$. Hence, $g_{C/H} = (|G_2/H| - 1)(i_0 - 1)/2 > 0$ and so $2p/(p-1) < |G|/g_C \leqslant |G/H|/(g_{C/H})$. □

For the action of a p-group G on a curve C with genus $g_C \geqslant 2$, we calculate $|G|/g_C$. If it is greater than $2p/(p-1)$ we will see that, to a certain degree, the values of $|G|/g_C^2$ classify the actions at least when $|G|/g_C^2$ is big enough. Here we concentrate on the case of 'maximal curves' and in a sequel paper we will go further in the classification.

Theorem 8.6. *Let* C *be a nonsingular projective curve over* k *of genus* $g_C \geqslant 2$ *and* G *a* p*-subgroup of* $\mathrm{Aut}_k C$. *We assume that* (C, G) *satisfies condition (N) and keep the notation of Proposition 8.5.*

(i) *There is a normal subgroup* H *of* G *with* $G_2 \supsetneqq H \supset G_{i_0+1}$ *and* $|G_2/H| = p$. *For any such* H $g_{C/H} = (p-1)(i_0-1)/2 > 0$ *and there is a polynomial* $f(X) = XS(X) \in k[X]$, *where* $S(X) - S(0)$ *is an additive polynomial of degree* $i_0 - 1 = p^{n_0} \in p^{\mathbb{N}^*}$, *such that* C/H *is birational to the curve* C_f. *Moreover,* $g_{C/G_{i_0+1}} = \frac{1}{2}(|G_2/G_{i_0+1}| - 1)(i_0 - 1)$ *and* $|G/G_2| = (1/p)|G/H| \leqslant (i_0 - 1)^2$.

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

(ii) *Let $M_1 := 4p/(p-1)^2$. Then $M_1 \leqslant |G|g_C^2$ if and only if C is birational to a curve $C_f\colon W^p - W = f(X) := XS(X)$ where $S(X) - S(0) = \sum_{0\leqslant i\leqslant\mu} t_i X^{p^i}$ is an additive polynomial $\in k[X]$ with $\mu \geqslant 1$ and $t_\mu \neq 0$. In this case $G = G_{\infty,1}(f)$ is an extraspecial group of type I(a) (respectively type II(b)) if $p > 2$ (respectively $p = 2$), $M_1 = |G|/g_C^2$, and $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$.*

(iii) *Let $M_2 := 4/(p-1)^2$. Then $M_2 \leqslant |G|/g_C^2 < M_1$ if and only if C is as in (ii). In this case G has index p in $G_{\infty,1}(f)$ and $M_2 = |G|/g_C^2$. Note that $G \supset [G_{\infty,1}(f), G_{\infty,1}(f)] = Z(G_{\infty,1}(f))$.*

Proof. (i) The existence of such a group H is a classical fact for p-groups [Suz82, Theorem 1.12, ch. 2]. The assertion follows from Propositions 8.5(iii), 8.3 and 6.6 I.

One common ingredient for (ii) and (iii) is that a lower bound $M \leqslant |G|/g_C^2$ will produce, following (i) and Proposition 8.5(ii), an upper bound for G_{i_0+1}; namely

$$|G_{i_0+1}| \leqslant \frac{1}{M}\frac{|G/G_{i_0+1}|}{g_{C/G_{i_0+1}}^2} \leqslant \frac{1}{M}\frac{4|G_2/G_{i_0+1}|}{(|G_2/G_{i_0+1}|-1)^2}.$$

(ii) We have

$$1 \leqslant |G_{i_0+1}| \leqslant \frac{1}{M_1}\frac{4|G_2/G_{i_0+1}|}{(|G_2/G_{i_0+1}|-1)^2}.$$

Observe that $4p^n/(p^n-1)^2$ as a function in n is strictly decreasing and hence it follows that $|G_{i_0+1}| = 1$ and $|G_2/G_{i_0+1}| = p$. Finally this gives $|G_2| = p$ and the result follows from Proposition 8.3.

(iii) If $|G_2/G_{i_0+1}| = p^{2+n}$ with $n \in \mathbb{N}$, then

$$\frac{1}{M_2}\frac{4p^{2+n}}{(p^{2+n}-1)^2} \leqslant \frac{1}{M_2}\frac{4p^2}{(p^2-1)^2} < 1;$$

so $1 \leqslant |G_{i_0+1}| < 1$, a contradiction. It follows that $|G_2/G_{i_0+1}| = p$ and $|G_{i_0+1}| = 1$ or p. Assuming that $|G_{i_0+1}| = p$ we obtain that there is $i_1 > 0$ such that $G = G_0 = G_1 \supseteq G_2 = \cdots = G_{i_0} \supsetneqq G_{i_0+1} = \cdots = G_{i_0+i_1} \supsetneqq G_{i_0+i_1+1} = 1$. Furthermore, one has $|G_2| = p^2$ and $2(g_C - 1) = |G_2|2(0-1) + \sum_{0\leqslant i}(|G_i| - 1) = -2p^2 + (i_0+1)(p^2-1) + i_1(p-1)$. In particular, as $i_1 > 0$, we get $g_C > (i_0-1)(p^2-1)/2$ and so $|G|/g_C^2 < 4p^2/(p^2-1)^2 < M_2$, a contradiction! We therefore have proven that $|G_{i_0+1}| = 1$ and $G_2 \simeq \mathbb{Z}/p\mathbb{Z}$ and conclude that G is a subgroup of index p of an extraspecial group by 8.1. □

Acknowledgements

We would like to thank Aristides Kontogeorgis for his correspondence along the elaboration of this paper. Its final version was written while the second author was a guest of the Max-Planck-Institut in Bonn.

References

Bra88 R. Brandt, *Über die Automorphismengruppen von algebraischen Funktionenkörpern*, PhD thesis, University of Essen (1988).

BS86 R. Brandt and H. Stichtenoth, *Die Automorphismengruppe hyperelliptischer Kurven*, Manuscripta Math. **55** (1986), 83–92.

CF64 R. Carter and P. Fong, *The Sylow 2-subgroups of the finite classical groups*, J. Algebra **1** (1964), 139–151.

CKK01 G. Cornelissen, F. Kato and A. Kontogeorgis, *Discontinuous groups in positive characteristic and automorphisms of Mumford curves*, Math. Ann. **320** (2001), 55–85.

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

CK03 G. Cornelissen and F. Kato, *Equivariant deformation of Mumford curves and of ordinary curves in positive characteristic*, Duke Math. J. **116** (2003), 431–470.

Des86 M. Deschamps, *Réduction semi-stable*, in *Pinceaux de courbes de genre au moins deux*, ed. L. Szpiro, Astérisque **86** (1981), 1–34.

Elk99 N. Elkies, *Linearized algebra and finite groups of Lie type. I. Linear and symplectic groups*, in *Applications of curves over finite fields* (Seattle, WA, 1997), Contemporary Mathematics, vol. 245 (American Mathematical Society, Providence, RI, 1999), 77–107.

Gos96 D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 35 (Springer, Berlin, 1996).

Gur03 R. Guralnick, *Monodromy groups of coverings of curves*, in *Galois groups and fundamental groups*, Mathematical and Scientific Research Institute Publications, vol. 41 (Cambridge University Press, Cambridge, 2003), 1–46.

Hen78 H-W. Henn, *Funktionenkörper mit grosser Automorphismengruppe*, J. reine angew. Math. **302** (1978), 96–115.

Hup67 B. Huppert, *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenschaften, vol. 134 (Springer, Berlin, 1967).

Joh76 D. L. Johnson, *Presentation of groups*, London Mathematical Society Lecture Note Series, vol. 22 (Cambridge University Press, Cambridge, 1976).

Kon99 A. Kontogeorgis, *The group of automorphisms of cyclic extensions of rational function fields*, J. Algebra **216** (1999), 665–706.

LM02 C. Lehr and M. Matignon, *Wild monodromy and automorphisms of curves*, Conference Proceedings, Tokyo, 2002, eds T. Sekiguchi and N. Suwa, to appear.
Available at: http://www.math.u-bordeaux.fr/∼matignon/.

LM04 C. Lehr and M. Matignon, *Wild monodromy and automorphisms of curves*, math.AG/0412294.

Leh01 C. Lehr, *Reduction of p-cyclic covers of the projective line*, Manuscripta Math. **106** (2001), 151–175.

Leo96 H.-W. Leopoldt, *Über die Automorphismengruppe des Fermatkörpers*, J. Number Theory **56** (1996), 256–282.

Liu02 Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6 (Oxford University Press, Oxford, 2002).

Mat03 M. Matignon, *Vers un algorithme pour la réduction stable des revêtements p-cycliques de la droite projective sur un corps p-adique*, Math. Ann. **325** (2003), 323–354.

Nak87 S. Nakajima, *p-ranks and automorphism groups of algebraic curves*, Trans. Amer. Math. Soc. **303** (1987), 595–607.

Poo00a B. Poonen, *Varieties without extra automorphisms I: Curves*, Math. Res. Lett. **7** (2000), 67–76.

Poo00b B. Poonen, *Varieties without extra automorphisms II: Hyperelliptic curves*, Math. Res. Lett. **7** (2000), 77–82.

Sin74 B. Singh, *On the group of automorphisms of function field of genus at least two.* J. Pure Appl. Algebra **4** (1974), 205–229.

Sti73a H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe*, Arch. Math. (Basel) **24** (1973), 527–544.

Sti73b H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein spezieller Typ von Funktionenkörpern*, Arch. Math. (Basel) **24** (1973), 615–631.

Suz82 M. Suzuki, *Group theory I*, Grundlehren der Mathematischen Wissenschaften, vol. 247 (Springer, New York, 1982).

Suz86 M. Suzuki, *Group theory II*, Grundlehren der Mathematischen Wissenschaften, vol. 248 (Springer, New York, 1986).

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press

vdGV92 G. van der Geer and M. van der Vlugt, *Reed–Muller codes and supersingular curves I*, Compositio Math. **84** (1992), 333–367.

vdPV03 M. van der Put and H. Voskuil, *Mumford coverings of the projective line*, Arch. Math. (Basel) **80** (2003), 98–105.

vdPV04 M. van der Put and H. Voskuil, *Discontinuous subgroups of* $\mathrm{PGL}_2(K)$, J. Algebra **271** (2004), 234–280.

Claus Lehr lehr@math.unipd.it
Università di Padova, Dipartimento di Matematica Pura ed Applicata, Via Belzoni 7, 35131 Padova, Italy

Michel Matignon matignon@math.u-bordeaux1.fr
Laboratoire de Théorie des Nombres et d'Algorithmique Arithmétique, UMR 5465 CNRS, Université de Bordeaux I, 351 cours de la Libération, 33405 Talence cedex, France

https://doi.org/10.1112/S0010437X05001296 Published online by Cambridge University Press