Covering Groups of Rank 1 of Elementary Abelian Groups

R. Gow and R. Quinlan

Abstract: Covering groups of elementary abelian groups of odd exponent p can be classified according to the rank of their p–th power homomorphisms, which may be regarded as linear transformations of $\mathbb{F}_p$–vector spaces. This paper contains a description of the isomorphism types and the automorphism groups of those covering groups in which this rank is 1. Analogous considerations of elementary abelian 2–groups and their covering groups are included in the final section.

Let p be an odd prime, let n be a positive integer and let Q denote the elementary abelian group of order p^n. In this paper we associate to every covering group of Q its *rank*, which is an integer in the range $0, \ldots, n$. We begin by constructing a group H of order $p^{n(n+1)/2}$ which has every covering group of Q as a central quotient. In Section 1 we describe the automorphism group of H and use it to derive a formula of P. Hall involving the orders of the automorphism groups of all the non–isomorphic covering groups of Q. In Section 2 we define the *rank* of a covering group and prove a modified version of Hall's formula for covering groups of fixed rank. Sections 3 and 4 are devoted to a detailed investigation of the rank 1 case, using tools from linear algebra. In Section 5 we consider related questions about elementary abelian 2–groups and their covering groups, but here the information available is combinatorial rather than algebraic in nature.

We begin with the basic definitions.

For any group G and elements x, y of G, we let $[x, y]$ denote the commutator $x^{-1}y^{-1}xy$. As usual we denote the commutator subgroup and centre of G by G' and $Z(G)$ respectively.

Suppose for now that p is any prime and n is a positive integer and let Q be an elementary abelian p–group of order p^n. A group $\tilde{Q}$ is said to be a *covering group* (or *stem cover*) of Q if $\tilde{Q}$ contains a subgroup Z with the following properties :

- $Z \subseteq Z(\tilde{Q}) \cap \tilde{Q}'$;
- Z is an elementary abelian group of order $p^{n(n-1)/2}$;
- $\tilde{Q}/Z \cong Q$.

Any such covering group $\tilde{Q}$ is a central quotient of a larger finite p–group H whose structure allows us to investigate the properties of all the covering groups in a uniform way. The group H is defined as follows, see also [3]. Let F be a free group of rank n with free generators $a_1, \ldots, a_n$. Let R be the fully invariant subgroup of F generated by

$$x^{p^2},\ [x,y]^p,\ [x^p,y] \quad \text{and } [[x,y],z]$$

for all x, y and z in F, and let $H = F/R$. H is a finite p–group generated by the n elements $h_i = a_i R$ for $1 \leq i \leq n$. Let $\Phi(H)$ denote the Frattini subgroup of H. This is clearly a central subgroup of H. Higman shows in [3] that $\Phi(H)$ is an elementary abelian p–group of order $p^{n(n+1)/2}$ generated by the $n(n+1)/2$ independent elements $h_1^p, \ldots, h_n^p$ and $[h_i, h_j]$ for $1 \leq i < j \leq n$. Let C be any complement of H' in $\Phi(H)$. Then H/C is a covering group of Q and all covering groups $\tilde{Q}$ are obtained in this way as central quotients of H. Since there are $p^{n^2(n-1)/2}$ complements of H' in $\Phi(H)$, we obtain $p^{n^2(n-1)/2}$ such central quotients but, of course, different complements may give rise to isomorphic covering groups. In this paper we will distinguish a special class of covering groups and investigate the automorphism groups of the members of this class.

1 On the automorphisms of the group H

The group H is a quotient of a free group by a fully invariant subgroup. As Higman observes, this means that H enjoys the following special property with respect to its automorphism group. Let M and N be subgroups of $\Phi(H)$ and suppose that there is an isomorphism between H/M and H/N. Then there exists an automorphism τ of H which satisfies $\tau(M) = N$ and induces the isomorphism between H/M and H/N. Conversely, it is clear that, given any subgroup M of $\Phi(H)$ and any automorphism σ of H, $\sigma(M)$ is then also a subgroup of $\Phi(H)$ and σ induces an isomorphism between H/M and $H/\sigma(M)$. This phenomenon allows us to relate the automorphisms of covering groups $\tilde{Q}$ to the group $\mathrm{Aut}(H)$ of all automorphisms of H.

We first determine some information about $\mathrm{Aut}(H)$. In general if G is a group and $\sigma \in \mathrm{Aut}(G)$, we say that σ is a *central* automorphism of G if σ induces the identity on $G/Z(G)$, or equivalently if σ fixes every coset of $Z(G)$ in G.

Lemma 1.1 *The group* $\mathrm{Aut}(H)$ *contains a normal elementary abelian subgroup of order* $p^{n^2(n+1)/2}$ *consisting of central automorphisms and the quotient is isomorphic to* $\mathrm{GL}(n,p)$ *(the group of all automorphisms of* Q*).*

Proof: We note that $H/\Phi(H) \cong Q$ and thus we have a homomorphism from $\mathrm{Aut}(H)$ to $\mathrm{Aut}(Q) = \mathrm{GL}(n,p)$. Now the discussion above about lifting isomorphisms of quotients of H implies that the homomorphism considered above is surjective. We have therefore only to

determine the kernel of this automorphism. Suppose then that for some automorphism σ of H we have $\sigma(x)\Phi(H) = x\Phi(H)$ for all x in H. It follows then that

$$\sigma(x) = x\tau(x),$$

where $\tau(x) \in \Phi(H)$. Thus σ is a central automorphism of H. It is straightforward to see that τ defines a homomorphism from H into $\Phi(H)$. Conversely, any such homomorphism from H into $\Phi(H)$ determines a central automorphism. Thus the number of central automorphisms is the number of homomorphisms from H into $\Phi(H)$. Now $\Phi(H)$ is an elementary abelian group of order $p^{n(n+1)/2}$ and the largest elementary abelian quotient group of H is $H/\Phi(H)$ of order p^n. It follows that there are $p^{n^2(n+1)/2}$ central automorphisms, as claimed. □

We now prove a theorem of P. Hall, [2], formula (18), p.202. While several proofs can be found in the literature, we include this proof, as it illustrates the utility of the group H, and also as we intend to extend the formula in the next section.

Theorem 1.2 *Let $\Gamma_1, \ldots, \Gamma_r$ be representatives of all the non–isomorphic covering groups of Q. Then*

$$\frac{1}{|\mathrm{GL}(n,p)|} = \sum_{i=1}^{r} \frac{1}{|\mathrm{Aut}(\Gamma_i)|}$$

Proof: $\mathrm{Aut}(H)$ acts on the $p^{n^2(n-1)/2}$ complements of H' in $\Phi(H)$, and it follows from Higman's argument that two complements are in the same orbit precisely when their corresponding central quotient groups are isomorphic covering groups of Q. Suppose for each i that

$$\Gamma_i \cong H/C_i$$

for some complement C_i and let A_i be the subgroup of $\mathrm{Aut}(H)$ that fixes C_i. We have then a homomorphism from A_i into $\mathrm{Aut}(\Gamma_i)$, and Higman's argument implies that this homomorphism is surjective. Furthermore, the kernel of the homomorphism consists of those automorphisms of H that satisfy $\sigma(x)C_i = xC_i$ for all $x \in H$. It is easy to see that there are p^{n^2} such central automorphisms.

The orbit–stabilizer theorem implies that

$$\begin{aligned} p^{n^2(n-1)/2} &= \sum_{i=1}^{r} |\mathrm{Aut}(H) : A_i| \\ &= \sum_{i=1}^{r} p^{n^2(n+1)/2} |\mathrm{GL}(n,p)| / p^{n^2} |\mathrm{Aut}(\Gamma_i)|, \end{aligned}$$

and this gives us the required result. □

We note that Hall gives an illustration of this formula when considering the ten non–isomorphic covering groups of an elementary abelian group of order 8, [2], p. 203.

Each covering group Γ_i considered above has $p^{n^2(n-1)/2}$ central automorphisms, which form a normal elementary abelian subgroup of $\mathrm{Aut}(\Gamma_i)$. Thus in the formula of Theorem 1.2, $p^{n^2(n-1)/2}$ divides each term $|\mathrm{Aut}(\Gamma_i)|$. U. Webb shows in [6], Theorem 2, that for odd p, as $n \to \infty$, the proportion of covering groups Γ_i for which $|\mathrm{Aut}(\Gamma_i)| = p^{n^2(n-1)/2}$ approaches 1. Clearly, any attempt to classify such groups by conventional invariants such as automorphisms is unlikely to succeed.

2 The p–th power homomorphism

Since H is nilpotent of class 2, we have

$$(xy)^p = x^p y^p [x,y]^{p(p-1)/2}$$

for all x and y in H. Now H' has exponent p and we deduce that

$$(xy)^p = x^p y^p$$

if p is odd. We assume henceforth that p is odd. Thus $x \mapsto x^p$ is a homomorphism and the p–th powers of elements in H form a subgroup H^p, generated by $h_1^p, \ldots, h_n^p$, which is a canonical complement to H' in $\Phi(H)$. The corresponding quotient H/H^p is distinguished by the fact that it is the unique covering group $\tilde{Q}$ of exponent p. It is straightforward to see that this covering group admits a subgroup Γ, say, of automorphisms isomorphic to $\mathrm{GL}(n,p)$ and the full automorphism group is the semi–direct product of the group of central automorphisms with the subgroup Γ.

Let now C be a complement of H' in $\Phi(H)$ and let $G = H/C$ be the corresponding covering group of Q. $G/\Phi(G)$ is an elementary abelian group of order p^n and $\Phi(G)$ is an elementary abelian group of order $p^{n(n-1)/2}$. We switch to additive notation and consider $G/\Phi(G)$ as a vector space V of dimension n over $\mathbb{F}_p$. Then $G' = \Phi(G)$ is naturally isomorphic to the exterior square $V \wedge V$ under the identification $[x_1, y_1] \leftrightarrow x \wedge y$, where x and y are elements of V that have preimages x_1 and y_1, respectively, in G. This is well defined, as G' is central. In this vector space context, the p–th power map of G into itself determines an $\mathbb{F}_p$–linear transformation, ϕ, say, from V into $V \wedge V$. It is this linear transformation that determines the structure of G, since this structure depends only on knowing the p–th powers of the generators of G in terms of products of commutators.

Let k be the rank of ϕ as a linear transformation. Then p^k is the order of the group of p–th powers in G, and if G_p denotes the subgroup of elements of order dividing p in G, $|G : G_p| = p^k$. We also have $|H^p : C \cap H^p| = p^k$. We will say that G has rank k as a covering group. Thus the covering group of exponent p has rank 0. In Sections 3 and 4 of this paper we will classify the covering groups of rank 1 and give a description of their automorphism groups. This is largely a problem in the theory of skew–symmetric forms.

We feel that it might just be feasible to classify covering groups of rank 2, although this is probably a difficult problem of linear algebra. We doubt if covering groups of rank greater than 2 can be classified in any reasonable way.

Before starting on our classification of the covering groups of rank 1, we pause to extend Hall's automorphism formula for all covering groups to those of rank k.

Given integers k and n with $1 \leq k \leq n$, we define f_k^n by

$$f_k^n = (p^n - 1) \cdots (p^n - p^{k-1}).$$

We note then that the number of subspaces of dimension k in a vector space of dimension n over $\mathbb{F}_p$ is

$$\frac{f_k^n}{|\mathrm{GL}(k,p)|}.$$

Moreover, if $k \leq \min(n,m)$, it is straightforward to show that the number of linear transformations of rank k from a vector space of dimension n over $\mathbb{F}_p$ into a vector space of dimension m over $\mathbb{F}_p$ is

$$\frac{f_k^n f_k^m}{|\mathrm{GL}(k,p)|}.$$

Theorem 2.1 *Let $\Gamma_1, \ldots, \Gamma_t$ be representatives of all the non–isomorphic covering groups of Q of rank k, where $0 \leq k \leq n$. Then*

$$\frac{f_k^n f_k^{\binom{n}{2}}}{p^{n^2(n-1)/2}|\mathrm{GL}(k,p)||\mathrm{GL}(n,p)|} = \sum_{i=1}^{t} \frac{1}{|\mathrm{Aut}(\Gamma_i)|}.$$

Proof: A covering group of rank k is determined by a complement C of H' in $\Phi(H)$ satisfying $|H^p : C \cap H^p| = p^k$. It is an easy argument of linear algebra to show that the number of such complements equals the number of linear transformations of rank k from a vector space of dimension n over $\mathbb{F}_p$ into a vector space of dimension $n(n-1)/2$ over $\mathbb{F}_p$. (We remark that this equality also follows from our discussion of the way that covering groups of rank k arise when the p–th power map determines a linear transformation of rank k.) Thus the number of complements that determine covering groups of rank k is

$$\frac{f_k^n f_k^{\binom{n}{2}}}{|\mathrm{GL}(k,p)|}.$$

$\mathrm{Aut}(H)$ acts on these complements and Higman's argument shows that two complements are in the same orbit precisely when their corresponding central quotient groups are isomorphic covering groups of rank k. If we follow the rest of the proof of Theorem 1.2, we obtain

$$\frac{f_k^n f_k^{\binom{n}{2}}}{|\mathrm{GL}(k,p)|} = \sum_{i=1}^{t} |\mathrm{Aut}(H) : A_i|,$$

where as before A_i is the stabilizer in $\mathrm{Aut}(H)$ of a complement C_i for which $H/C_i \cong \Gamma_i$. This formula may be rearranged to give

$$\frac{f_k^n f_k^{\binom{n}{2}}}{p^{n^2(n-1)/2}|\mathrm{GL}(k,p)||\mathrm{GL}(n,p)|} = \sum_{i=1}^{t} \frac{1}{|\mathrm{Aut}(\Gamma_i)|},$$

as required. □

3 The rank 1 case

Let V be a vector space of dimension $n \geq 2$ over $\mathbb{F}_p$, and let $\phi : V \longrightarrow V \wedge V$ be a linear transformation of rank 1. Choose a generator r of $\mathrm{Im}\,\phi$, and choose a basis $\mathcal{B} = \{x_1, \ldots, x_n\}$ of V. Then r and $\mathcal{B}$ together determine an alternating bilinear form $f : V \times V \longrightarrow \mathbb{F}_p$ by

$$r = \sum_{1 \leq i < j \leq n} f(x_i, x_j) x_i \wedge x_j.$$

Thus for elements x_s, x_t of $\mathcal{B}$, $f(x_s, x_t)$ is defined as the coefficient of $x_s \wedge x_t$ in the expression for r as a linear combination of the elements of the basis $\{x_i \wedge x_j\}_{1 \leq i < j \leq n}$ of $V \wedge V$; f is of course extended to all of $V \wedge V$ by bilinearity.

The form f depends both on the choice of generator r of $\mathrm{Im}\,\phi$ and on the choice of a basis of V. Since $\mathrm{Im}\,\phi$ has dimension 1, replacing r by another generator simply amounts to replacing f by af for some $a \in \mathbb{F}_p^\times$. Let $\mathcal{B}' = \{x_1', \ldots, x_n'\}$ be another basis of V and let f' be the alternating form on V defined by writing r in terms of the basis $\{x_i' \wedge x_j'\}$ of $V \wedge V$. If A and A' are the matrices of f and f' with respect to $\mathcal{B}$ and $\mathcal{B}'$ respectively, then it is easily checked that $A = RA'R^t$, where R is the change of basis matrix from $\mathcal{B}'$ to $\mathcal{B}$, defined by $x_i' = \sum_{j=1}^{n} (R)_{ji} x_j$, for $i = 1, \ldots, n$. Thus we have the following result.

Lemma 3.1 *Let $\{y_1, \ldots, y_n\}$ be a basis of V and let $r \in V \wedge V$ be fixed. If*

$$r = \sum_{1 \leq i < j \leq n} b_{ij} y_i \wedge y_j,$$

and $C = (c_{ij})$ is a matrix which is congruent in $M_n(\mathbb{F}_p)$ to $B = (b_{ij})$, then there exists a basis $\{y_1', \ldots, y_n'\}$ of V with

$$r = \sum_{1 \leq i < j \leq n} c_{ij} y_i' \wedge y_j'.$$

The forms f and f' on V are generally different, since the matrix of f with respect to $\mathcal{B}'$ is $R^t AR$ which is typically not equal to A'. However f and f' certainly have the same rank. This rank is even and at most equal to n, and is an invariant of the covering group of Q determined by ϕ.

It is not the case that the rank of f fully determines this covering group, but we now show that the number of isomorphism types of covering group corresponding to a given possibility for rank$f$ is at most 2.

Lemma 3.2 *Let $\mathcal{B} = \{x_1, \ldots, x_n\}$ and $\mathcal{B}' = \{x'_1, \ldots, x'_n\}$ be bases for V having the property that $\ker \phi = \langle x_2, \ldots, x_n \rangle = \langle x'_2, \ldots, x'_n \rangle$. Let r be a generator for $\operatorname{Im} \phi$ and let f and f' be the alternating forms on V defined as above by r and by $\mathcal{B}$ and $\mathcal{B}'$ respectively. Then $x_1 \in \operatorname{rad} f$ if and only if $x'_1 \in \operatorname{rad} f'$.*

Proof : Let A and A' denote the matrices of f with respect to $\mathcal{B}$ and f' with respect to $\mathcal{B}'$ respectively, and let R be the change of basis matrix from $\mathcal{B}'$ to $\mathcal{B}$. Then the first row of R has a non–zero entry as its first entry, but otherwise consists entirely of zeroes. Then since $A = RA'R^t$ and R is invertible, the first row and first column of A consist entirely of zeroes if and only if the same is true of A'. □

Lemma 3.3 *Let G be a covering group of Q of rank 1 for which the alternating forms on V associated to the p–th power map have rank $2t$. Then exactly one of the following holds :*

1. *V has a basis $\{x_1, x_2, \ldots, x_n\}$ with $\ker \phi = \langle x_2, \ldots, x_n \rangle$ and $\phi(x_1) = \sum_{i=1}^{t} x_{2i-1} \wedge x_{2i}$.*

2. *V has a basis $\{x_1, x_2, \ldots, x_n\}$ with $\ker \phi = \langle x_2, \ldots, x_n \rangle$ and $\phi(x_1) = \sum_{i=1}^{t} x_{2i} \wedge x_{2i+1}$.*

Proof : Choose a basis $\{y_1, \ldots, y_n\}$ for V with $\phi(y_1) = r \neq 0$ and $\phi(y_i) = 0$ for $i \geq 2$. Let f be the alternating bilinear form on V defined by r and this basis.
Case 1 Suppose $y_1 \notin \operatorname{rad} f$. After reordering the elements $y_2, \ldots, y_n$ if necessary, we may assume that $f(y_1, y_2) \neq 0$. Define $a_i = f(y_1, y_i)$ for $i \geq 2$, and define $x_2 = \sum_{i=2}^{n} a_i y_i$. Then $\{y_1, x_2, y_3, \ldots, y_n\}$ is a basis of V, and

$$r = y_1 \wedge x_2 + \sum_{j=3}^{n} b_{2j} x_2 \wedge y_j + \sum_{3 \leq i < j \leq n} b_{ij} y_i \wedge y_j.$$

Define

$$x_1 = y_1 - \sum_{j=3}^{n} b_{2j} x_j.$$

Then

$$r = x_1 \wedge x_2 + \sum_{3 \leq i < j \leq n} b_{ij} y_i \wedge y_j.$$

Thus if f' is the form on V determined by r and the basis $\{x_1, x_2, y_3, \ldots, y_n\}$, we have $f'(x_1, x_2) = 1$ and $V_1 = \langle y_3, \ldots, y_n \rangle \subseteq \ker \phi$ is the orthogonal complement of $\langle x_1, x_2 \rangle$ with

respect to f'. It now follows from Lemma 3.1 that we can find a basis $\{x_3, \ldots, x_n\}$ of V_1 so that

$$\phi(x_1) = x_1 \wedge x_2 + \cdots + x_{2t-1} \wedge x_{2t}.$$

Then $\{x_1, \ldots, x_n\}$ is a basis of V satisfying 1.
Case 2 Suppose $y_1 \in \operatorname{rad} f$. Then it follows immediately from Lemma 3.1 that $V_1 = \langle y_2, \ldots, y_n \rangle$ has a basis $\{x_2, \ldots, x_n\}$ with

$$r = x_2 \wedge x_3 + \cdots + x_{2t} \wedge x_{2t+1}.$$

Setting $x_1 = y_1$ produces a basis $\{x_1, \ldots, x_n\}$ of V satisfying 2.

Finally, Lemma 3.2 shows that 1. and 2. cannot both be satisfied for the same covering group of Q. □

For $2t < n$ we will denote the groups described in 1. and 2. of Lemma 3.3 by $G^0_{n,2t}$ and $G^1_{n,2t}$ respectively. In the case where n is even and the bilinear form determined by a generator of $\operatorname{Im}\phi$ has rank n, $\operatorname{rad} f = 0$ and there is only one possible covering group; otherwise two covering groups correspond to each possibility for rank f. We have proved the following result.

Theorem 3.4 *Let Q be a non–cyclic elementary abelian group of odd order p^n. Then the number of isomorphism types of covering group of Q in which the p–th power map has rank 1 is $n-1$.*

4 Groups of Automorphisms

As in previous sections, let Q denote the elementary abelian group of order p^n, for an odd prime p and integer $n \geq 2$. If G is a covering group of Q, then the automorphism group of G contains an elementary abelian normal subgroup of order $p^{n^2(n-1)/2}$, consisting of central automorphisms. We denote the group of central automorphisms of G by $\mathrm{CAut}(G)$. The quotient $\mathrm{Aut}(G)/\mathrm{CAut}(G)$ is isomorphic to a subgroup of $\mathrm{GL}(n,p)$. We will denote this group by $\overline{\mathrm{Aut}}(G)$ and refer to it as the *essential* automorphism group of G. In this section we describe the essential automorphism groups of the covering groups of rank 1 of Q discussed in Section 3.

Let V be a vector space of dimension n over $\mathbb{F}_p$ and let $\phi : V \longrightarrow V \wedge V$ be a linear transformation of rank 1. Let G be the associated covering group of Q, and let $\sigma \in \mathrm{GL}(V)$. Then σ induces $\sigma^* \in \mathrm{GL}(V \wedge V)$, defined for x and y in V by $\sigma^*(x \wedge y) = \sigma(x) \wedge \sigma(y)$. Suppose that σ is induced by an automorphism $\tilde{\sigma}$ of G (in this case σ is said to *lift* to G). Then from the fact that $\tilde{\sigma}$ commutes with the p–th power homomorphism in G and the identification of G' with $V \wedge V$ it follows that $\sigma^*\phi = \phi\sigma$.

Let t, r and the basis $\{x_1, \ldots, x_n\}$ of V be defined as in the statement of Lemma 3.3. Let Γ be the subgroup of $\mathrm{GL}(V)$ consisting of those transformations which lift to automorphisms of G, so $\sigma \in \Gamma$. Since σ^* must preserve the image of ϕ we have $\sigma^*(r) = ar$ for some $a \in \mathbb{F}_p^\times$. Since the subspace $\langle x_2, \ldots, x_n \rangle = \ker\phi$ of V must be σ–invariant we must have $\sigma(x_1) \in a'x_1 + \ker\phi$, where $a' \in \mathbb{F}_p^\times$. Finally since $\phi(x_1) = r$ and $ar = \sigma^*\phi(x_1) = \phi\sigma(x_1) = a'r$ we see that $a' = a$.

Case 1: $G \cong G^0_{n,2t}$. In this case

$$r = x_1 \wedge x_2 + \cdots + x_{2t-1} \wedge x_{2t},$$

and $\sigma^*(r) = ar$ means

$$ar = \sigma(x_1) \wedge \sigma(x_2) + \cdots + \sigma(x_{2t-1}) \wedge \sigma(x_{2t}).$$

Let R and S denote respectively the matrices of σ and f with respect to the basis $\{x_1, \ldots, x_n\}$ of V. Then $aS = RSR^t$ by the comments preceding Lemma 3.1, and $(R^t)^t SR^t = aS$. Thus the element σ' of $\mathrm{GL}(V)$ whose matrix with respect to $\{x_1, \ldots, x_n\}$ is R^t sends x_1 to ax_1 and satisfies $f(\sigma'(u), \sigma'(v)) = af(u, v)$, for $u, v \in V$. Thus σ' induces on $V/\mathrm{rad}\, f$ an element of the conformal symplectic group $\mathrm{CSp}(2t, p)$. Hence $\Gamma \cong \overline{\mathrm{Aut}}\left(G^0_{n,2t}\right)$ is isomorphic (via the transpose-inverse mapping on $\mathrm{GL}(n, p)$) to some subgroup of that subgroup of $\mathrm{GL}(V)$ consisting of transformations τ with the following properties

- $\tau.f = af$ for some $a \in \mathbb{F}_p^\times$, and
- $\tau(x_1) = ax_1$ (for the same a).

For each of the $p - 1$ choices for a, the number of elements of $\mathrm{GL}(V/\mathrm{rad}f)$ satisfying these two conditions is

$$\frac{1}{p^{2t} - 1} \left|\mathrm{Sp}(2t, p)\right|.$$

Each element of Γ must restrict to an invertible linear transformation of $\mathrm{rad}f$, a space of dimension $n - 2t$. We conclude

$$\left|\overline{\mathrm{Aut}}\left(G^0_{n,2t}\right)\right| \leq \frac{p-1}{p^{2t} - 1} \left|\mathrm{Sp}(2t, p)\right| \left|\mathrm{GL}(n - 2t, p)\right| p^{(2t-1)(n-2t)}. \tag{1}$$

Case 2: $G \cong G^1_{n,2t}$. In this case

$$r = x_2 \wedge x_3 + \cdots + x_{2t} \wedge x_{2t+1}.$$

As above $\sigma^*(r) = ar$ for some $a \in \mathbb{F}_p^\times$, $\sigma'(x_1) = ax_1$ for the same a, and $\sigma'.f = af$. Furthermore σ' restricts on $\mathrm{rad}\, f = \langle x_1, x_{2t+2}, \ldots, x_n \rangle$ to an invertible linear transformation preserving the subspace $\langle x_1 \rangle$. Thus

$$\left|\overline{\mathrm{Aut}}\left(G^1_{n,2t}\right)\right| \leq \frac{p-1}{p^{n-2t} - 1} \left|\mathrm{Sp}(2t, p)\right| \left|\mathrm{GL}(n - 2t, p)\right| p^{2t(n-2t)}. \tag{2}$$

The next theorem employs Hall's formula for covering groups of rank 1 to replace the inequalities (1) and (2) above with equalities.

Theorem 4.1 *For $t \leq n/2$,*

1. $\left|\overline{\mathrm{Aut}}\left(G^0_{n,2t}\right)\right| = \dfrac{p-1}{p^{2t}-1}\left|\mathrm{Sp}(2t,p)\right|\left|\mathrm{GL}(n-2t,p)\right|p^{(2t-1)(n-2t)}$.

2. $\left|\overline{\mathrm{Aut}}\left(G^1_{n,2t}\right)\right| = \dfrac{p-1}{p^{n-2t}-1}\left|\mathrm{Sp}(2t,p)\right|\left|\mathrm{GL}(n-2t,p)\right|p^{2t(n-2t)}$.

Proof: By Theorem 2.1, we have

$$\frac{f_1^n f_1^{\binom{n}{2}}}{|\mathrm{GL}(1,p)||\mathrm{GL}(n,p)|} = \sum_{t=1}^{\lceil n/2\rceil-1}\frac{1}{|\overline{\mathrm{Aut}}(G^1_{n,2t})|} + \sum_{t=1}^{\lfloor n/2\rfloor}\frac{1}{|\overline{\mathrm{Aut}}(G^0_{n,2t})|}.$$

Thus, by (1) and (2)

$$\begin{aligned}\frac{f_1^n f_1^{\binom{n}{2}}}{|\mathrm{GL}(1,p)||\mathrm{GL}(n,p)|} \quad \geq \quad & \sum_{t=1}^{\lceil n/2\rceil-1}\frac{p^{n-2t}-1}{(p-1)p^{(2t)(n-2t)}\left|\mathrm{Sp}(2t,p)\right|\left|\mathrm{GL}(n-2t,p)\right|} \\ & + \sum_{t=1}^{\lfloor n/2\rfloor}\frac{p^{2t}-1}{(p-1)p^{(2t-1)(n-2t)}\left|\mathrm{Sp}(2t,p)\right|\left|\mathrm{GL}(n-2t,p)\right|}.\end{aligned}$$

Since $p^{n-2t}-1=0$ if $n=2t$, this implies that

$$\frac{f_1^n f_1^{\binom{n}{2}}}{|\mathrm{GL}(1,p)||\mathrm{GL}(n,p)|} \geq \sum_{t=1}^{\lfloor n/2\rfloor}\frac{p^n-1}{(p-1)p^{2t(n-2t)}\left|\mathrm{Sp}(2t,p)\right|\left|\mathrm{GL}(n-2t,p)\right|},$$

with equality if and only if the statement of the theorem holds.

Since

$$\frac{f_1^n f_1^{\binom{n}{2}}}{|\mathrm{GL}(1,p)|} = \frac{\left(p^{\binom{n}{2}}-1\right)\left(p^n-1\right)}{p-1},$$

we need to show that

$$\frac{p^{\binom{n}{2}}-1}{|\mathrm{GL}(n,p)|} = \sum_{t=1}^{\lfloor n/2\rfloor}\frac{1}{p^{2t(n-2t)}\left|\mathrm{Sp}(2t,p)\right|\left|\mathrm{GL}(n-2t,p)\right|}.$$

Let S denote the set of non–zero alternating bilinear forms on $V\times V$. Then $|S| = p^{\binom{n}{2}}-1$ (this is the number of non–zero skew–symmetric matrices in $M_n(\mathbb{F}_p)$). We have an action of $\mathrm{GL}(V)$ on S defined by

$$\sigma.f(u,v) = f(\sigma^{-1}(u),\sigma^{-1}(v)),\ \text{for } f\in S,\ \sigma\in GL(V) \text{ and } u,v\in V.$$

If f has rank $2t$, then $\operatorname{rad} f$ has dimension $n-2t$, and the stabilizer of f under this action has order $|\mathrm{Sp}(2t,p)|\,|\mathrm{GL}(n-2t,p)|\,p^{2t(n-2t)}$. Thus

$$p^{\binom{n}{2}}-1=\sum_{t=1}^{\lfloor n/2\rfloor}\frac{|\mathrm{GL}(n,p)|}{p^{2t(n-2t)}|\mathrm{Sp}(2t,p)|\,|\mathrm{GL}(n-2t,p)|},$$

as required. □

5 Uniform covering groups in the case $p=2$

In this section we let Q_2 denote an elementary abelian group of order 2^n, where we assume $n\geq 2$. The squaring map in a covering group G of Q_2 is not a homomorphism, but satisfies the identity

$$(xy)^2=x^2y^2[x,y],$$

for $x,y\in G$. Thus we cannot define the rank of these covering groups as we did in the case of odd prime exponents. However, if (for p odd) we characterize the rank 1 covering groups of elementary abelian groups as those that possess a basis consisting of elements all having the same p–th power, we might by analogy consider those covering groups of Q_2 having a generating set consisting of n elements all having the same square. We will describe such covering groups as *uniform*, and such generating sets as *uniform bases*.

Suppose now that $n\geq 3$ and that G is a uniform covering group of Q_2 with uniform basis $\mathcal{B}=\{x_1,\ldots,x_n\}$, where $x_i^2=r\in G'$ for $i=1,\ldots,n$. We note the following facts, of which proofs can be found in [5].

Theorem 5.1 *1. If $s\in G'$ and $s\neq r$, then s cannot be the square of elements from three different cosets of G' in G.*

2. If $x\in G$ and $x^2=r$, then one of the following holds :

- *$x\in x_iG'$ for some $x_i\in\mathcal{B}$,* or
- *$r=\prod_{1\leq j<l\leq k}[x_{i_j},x_{i_l}]$ for some subset $\{i_1,\ldots,i_k\}$ of $\{1,\ldots,n\}$, with $k\geq 2$ even, and $x\in x_{i_1}\ldots x_{i_k}G'$,* or
- *$r=1$ and $x\in G'$.*

It follows from 2. in Theorem 5.1 that the number of cosets of G' in G consisting of elements of square r is either n (in which case every uniform basis consists of a representative of each of these cosets) or $n+1$. In this latter case, if $r=1$ we again have a unique uniform basis up to a choice of coset representatives. If $r\neq 1$ we can replace one of $x_{i_1},\ldots,x_{i_k}$ in $\mathcal{B}$ with a representative of $x_{i_1}\ldots x_{i_k}G'$ and so G has $k+1$ essentially different uniform bases.

We associate to G a graph $\Gamma(G)$ on vertex set $\{X_1, \ldots, X_n\}$ as follows. We have

$$r = \prod_{1 \le i < j \le n} [x_i, x_j]^{\alpha_{ij}},$$

where $\alpha_{ij} = 0$ or 1 for each choice of i and j. We declare the vertices X_l and X_m to be adjacent in $\Gamma(G)$ if and only if $a_{lm} = 1$, i.e. if and only if the commutator $[x_l, x_m]$ appears in the expression for r in terms of the basis elements $[x_i, x_j],\ 1 \le i < j \le n$ of G'. It is easily verified that the isomorphism type of the graph $\Gamma(G)$ does not depend on a particular choice of uniform basis; the only case to check is the one where G has a uniform basis $\{y_1, \ldots, y_n\}$ with $y_l^2 = r = \prod_{1 \le i < j \le k} [y_i, y_j]$ for $l = 1, \ldots, n$, where k is even and $2 \le k \le n$. In this case there is more than one choice of uniform basis, and every choice determines a graph consisting of $n - k$ isolated vertices and a complete subgraph on the remaining k vertices. Again see [5] for the details. We have the following result (compare Theorem 3.4):

Theorem 5.2 *The number of isomorphism types of uniform covering group of Q_2 is equal to the number of isomorphism types of graph of order n.*

We now turn our attention to the automorphisms of uniform covering groups of Q_2. As in Section 4 we consider the essential automorphism group $\overline{\mathrm{Aut}}(G)$ instead of the full automorphism group. The first result is that $\overline{\mathrm{Aut}}(G)$ is isomorphic to the automorphism group of the graph $\Gamma(G)$, except in those special cases where $n + 1$ cosets of G' consist of elements having the same (non–identity) square.

Case 1: Suppose G has a uniform basis $\mathcal{B} = \{x_1, \ldots, x_n\}$, $x_i^2 = r$, and that $\cup_{i=1}^n x_i G'$ is the full set of elements of G having square r. Let $\sigma \in \mathrm{Aut}(G)$. It follows from Theorem 5.1 that σ must permute the cosets $x_i G'$ and fix $r \in G'$. Thus associated to σ is a permutation π_σ of $\{1, \ldots, n\}$ defined by

$$\sigma(x_i G') = x_{\pi_\sigma(i)} G'.$$

Suppose $r = \prod_{1 \le i < j \le n} [x_i, x_j]^{\alpha_{ij}}$. Then since σ fixes r we must have

$$r = \prod_{1 \le i < j \le n} [x_{\pi_\sigma(i)}, x_{\pi_\sigma(j)}]^{\alpha_{ij}}$$

also. Thus the permutation σ_Γ of the vertex set $\{X_1, \ldots, X_n\}$ of $\Gamma(G)$ defined by $\sigma_\Gamma(X_i) = X_{\pi_\sigma(i)}$ is a graph automorphism. The mapping ψ from $\mathrm{Aut}(G)$ to $\mathrm{Aut}(\Gamma(G))$ sending σ to σ_Γ is clearly a group homomorphism whose kernel is the group $\mathrm{CAut}(G)$ of central automorphisms of G. To show that ψ induces an isomorphism between $\overline{\mathrm{Aut}}(G)$ and $\mathrm{Aut}(\Gamma(G))$, it remains to show that it is surjective.

Let F be a free group of rank n with generators $a_1, \ldots, a_n$, and as before let R be the fully invariant subgroup of F generated by elements of the form $x^4,\ [x, y]^2,\ [x^2, y]$ and $[[x, y], z]$

for $x, y, z \in F$. Let $H = F/R$ and for $i = 1, \ldots, n$ let $h_i = a_i R$. Define

$$r' = \prod_{1 \le i < j \le n} [h_i, h_j]^{\alpha_{ij}},$$

and let C be the subgroup of H generated by $\{h_i^2 r'\}_{i=1,\ldots,n}$. Then $H/C \cong G$. Suppose π is a permutation of $\{1, \ldots, n\}$ for which the function τ_Γ sending X_i to $X_{\pi(i)}$ is an automorphism of $\Gamma(G)$. Then the automorphism τ' of H defined on generators by $\tau'(h_i) = h_{\pi(i)}$ fixes r' and permutes the h_i^2, hence fixes C. Thus τ' induces an automorphism τ of G with $\psi(\tau) = \tau_\Gamma$. We conclude that ψ is surjective and $\overline{\mathrm{Aut}}(G) \cong \mathrm{Aut}(\Gamma(G))$; in particular $\overline{\mathrm{Aut}}(G)$ is isomorphic to a subgroup of S_n.

It was proved by R. Frucht in [1] that every finite group can be realized as the automorphism group of a graph. Thus by contrast with Theorem 4.1 we obtain the following result.

Theorem 5.3 *If $\tilde{G}$ is a finite group then there exists a uniform covering group G of an elementary abelian 2-group for which $\overline{\mathrm{Aut}}(G) \cong \tilde{G}$.*

Proof: The groups described in Case 1 are those represented by non–exceptional graphs, where an exceptional graph is defined to be one consisting of a complete subgraph on a positive even number of vertices, with any remaining vertices isolated. The automorphism group of an exceptional graph of order n is isomorphic to $S_k \times S_{n-k}$ where $2 \le k \le n$ and k is even. Frucht's theorem shows that every finite group not of this form can be realized as the automorphism group of a non–exceptional graph and therefore as the essential automorphism group of a uniform covering group of an elementary abelian 2–group. It remains to show that for any positive integers k and n with $2 \le k \le n$ and k even, $S_k \times S_{n-k}$ can also be realized as the full group of automorphisms of a non–exceptional graph. To see this let Γ be the graph on vertex set $\{X_1, \ldots, X_{n+2}\}$ consisting of a complete subgraph on $\{X_1, dots, X_{k+1}\}$ and the edge $X_{k+1}X_{k+2}$, with the remaining vertices isolated. Then $\mathrm{Aut}(\Gamma) \cong S_k \times S_{n-k}$ since any permutation of $\{X_1, \ldots, X_k\}$ can be combined with any permutation of $\{X_{k+3}, \ldots, X_{n+2}\}$ to produce an automorphism of Γ, and every automorphism of Γ arises in this way. Finally since Γ is non–exceptional it describes a covering group (of the elementary abelian group of order 2^{n+2},) whose essential automorphism group is isomorphic to $S_k \times S_{n-k}$. □

Case 2: Suppose G has a uniform basis $\{x_1, \ldots, x_n\}$ with $x_i^2 = r$ for $i = 1, \ldots, n$ and $r = \prod_{1 \le i < j \le k} [x_i, x_j]$ with $k \ge 2$ even. Then if we define $y = x_1 x_2 \ldots x_k$, we have $y^2 = r$ also and by Theorem 5.1 we have

$$\{x \in G : x^2 = r\} = \left(\bigcup_{i=1}^{n} x_i G' \right) \cup y G'.$$

If σ is an automorphism of G then as above σ must permute the $n + 1$ cosets of G' represented by $x_1, \ldots, x_n, y$. In addition σ must fix r and from this requirement it follows

that σ must permute the cosets $x_{k+1}G', \ldots, x_nG'$. Now suppose that σ maps the set $S = \{x_1G', \ldots, x_kG'\}$ into a subset of $S_1 := \{x_1G', \ldots, x_kG', yG'\}$ with k elements. Then it is easily verified that $\sigma(yG')$ is that element of S_1 not belonging to $\sigma(S)$. In the case where $\sigma(S) = S$ it is clear that σ fixes r. On the other hand suppose $\sigma(x_lG') = yG'$ for some $l \in \{1, \ldots, k\}$, and suppose $S_1 - \sigma(S) = x_mG'$. Then $\sigma(y) \in x_mG'$ and

$$\begin{aligned}
\sigma(r) &= \sigma([x_l, y]) \prod_{\substack{1 \le i < j \le k \\ i,\, j \ne l}} \sigma([x_i, x_j]) \\
&= [y, x_m] \prod_{\substack{1 \le i < j \le k \\ i,\, j \ne m}} [x_i, x_j] \\
&= \prod_{1 \le i < j \le k} [x_i, x_j] \\
&= r.
\end{aligned}$$

Thus σ fixes r. We conclude that every automorphism of G permutes the cosets $x_1G', \ldots, x_kG', yG'$ and also permutes the cosets $x_{k+1}G', \ldots, x_nG'$. Hence $\overline{\mathrm{Aut}}(G)$ is isomorphic to a subgroup of $S_{k+1} \times S_{n-k}$.

Now let H be defined as before and let $r' = \prod_{1 \le i < j \le k} [h_i, h_j]$. Define C to be the subgroup of H generated by $h_1^2 r', \ldots, h_n^2 r'$. Then $H/C \cong G$ and we can define a automorphism τ of H on generators as follows :

- τ permutes the elements $h_{k+1}, \ldots, h_n$, and
- τ maps each of $h_1, \ldots, h_k$ to a different element of the set $\{h_1, \ldots, h_k, h\}$, where h is defined to be the product $h_1 \ldots h_k$.

Then it easily checked that τ fixes r'. Also τ fixes C, for suppose $\tau(h_l) = h$ for some $l \in \{1, \ldots, k\}$. Then

$$\begin{aligned}
\tau(h_l^2 r') &= h^2 r' \\
&= h_1^2 \ldots h_k^2 \prod_{1 \le i < j \le k} [x_i, x_j] r' \\
&= h_1^2 \ldots h_k^2 (r')^2 \\
&= h_1^2 \ldots h_k^2.
\end{aligned}$$

That this element belongs to C follows from the fact that k is even and $r' \in Z(H)$.

Since τ fixes C it induces an automorphism of G. It follows that an automorphism of G may involve any permutation of $\{x_1G', \ldots, x_nG', yG'\}$ combined with any permutation of $\{x_{k+1}G', \ldots x_nG'\}$. Thus we obtain the following theorem.

Theorem 5.4 *Let G be a uniform covering group of Q_2 for which $\Gamma(G)$ consists of a complete subgraph on an even number $k \geq 2$ of vertices, and $n-k$ isolated vertices. Then*

$$\overline{\mathrm{Aut}}(G) \cong S_{k+1} \times S_{n-k}.$$

We conclude this section with the following observations.

1. If n is odd, then the maximum possible order of $\overline{\mathrm{Aut}}(G)$ for a uniform covering group G of Q_2 is $n!$, and this occurs in the following three different cases :

   - G is generated by n involutions; $\Gamma(G)$ is the null graph on n vertices.
   - $G = \langle x_1, \ldots, x_n : x_i^2 = \prod_{1 \leq i < j \leq n} [x_i, x_j] \rangle$; $\Gamma(G)$ is the complete graph on n vertices.
   - $G = \langle x_1, \ldots, x_n : x_i^2 = \prod_{1 \leq i < j \leq n-1} [x_i, x_j] \rangle$; $\Gamma(G)$ consists of a complete graph on $n-1$ vertices and a single isolated vertex.

   In each of these cases $\overline{\mathrm{Aut}}(G) \cong S_n$.

2. If n is even, then the maximum possible order of $\overline{\mathrm{Aut}}(G)$ is $(n+1)!$, and this occurs in the case where $\Gamma(G)$ is a complete graph on n vertices, so

   $$G = \langle x_1, \ldots, x_n : x_i^2 = \prod_{1 \leq i < j \leq n} [x_i, x_j] \rangle.$$

   In this case $\overline{\mathrm{Aut}}(G) \cong S_{n+1}$.

References

[1] R. Frucht, *Herstellung von Graphen mit vorgegebener abstrakten Gruppe*, Compositio Math. **6** (1938), 239–250.

[2] P. Hall, *On groups of automorphisms*, J. Reine Angew. Math. **182** (1940) 194–204.

[3] G. Higman, *Enumerating p-groups. I: Inequalities*, Proc. London Math. Soc. **10** (1960) 24–30.

[4] B. Huppert, *Endliche Gruppen*, Springer–Verlag, Berlin–Heidelberg–New York, 1967.

[5] R. Quinlan, *Real elements and real-valued characters of covering groups of elementary abelian 2-groups*, J. Algebra **275** (2004), 191–211.

[6] U. Webb, *The number of stem covers of an elementary abelian p–group*, Math. Z. **182**, (1983), no. 3, 327–337.

Mathematics Department, University College Dublin, Belfield, Dublin 4, Ireland
E-mail : rod.gow@ucd.ie, rachel.quinlan@ucd.ie