

CYCLIC MINIMAL GENERATING SETS FOR ABELIAN GROUPS

Elizabeth H. Kimber, John J. O'Connor, Edmund F. Robertson

Mathematical Institute, University of St Andrews,
North Haugh, St Andrews, KY16 9SS, Scotland

ABSTRACT. A finite group is said to be cyclically generated if it has an automorphism that cycles through a generating set for the group. Such a set will be called a cyclic generating set. We show that every finite abelian group is cyclically generated, and then present results concerning the existence of cyclic minimal generating sets for finite abelian groups of ranks 3, 4, and 5. Further results about cyclic generating sets of prime or square-free size are also included.

Definition 1. A finite group G is *cyclically generated* if it has an element x and an automorphism θ such that $\langle x, x\theta, x\theta^2, \dots, x\theta^{o(\theta)-1} \rangle = G$. The set $\{x, x\theta, x\theta^2, \dots, x\theta^{o(\theta)-1}\}$ is called a *cyclic generating set* and θ is called a *cyclic automorphism*.

Definition 2. A generating set X for a group G is *symmetric* if every permutation of the elements of X induces an automorphism of G .

As every symmetric generating set is also a cyclic generating set we can use results about symmetric generating sets to establish the existence of cyclic generating sets. In 2003 the following result was published:

Theorem (Miklós Abért, 2003) *Let G be a finite abelian group. Then G can be symmetrically generated by $n > 2$ elements if and only if there are positive integers a, b, c such that (i) $G = \mathbb{Z}_a \times \mathbb{Z}_{ab}^{n-2} \times \mathbb{Z}_{abc}$, and (ii) $(b, c) | n$.*

In the same paper Abért also notes that *Every finite abelian group of rank 2 is symmetrically generated by two generators*; see [?].

These results will be referred to as *Abért's Theorem* and conditions (i) and (ii) will be called *Abért's conditions*. We can use these results to give examples of finite abelian groups that have cyclic minimal generating sets and we now present further results that allow us to establish necessary and sufficient conditions for certain finite abelian groups to have cyclic minimal generating sets.

0.1. Notation. For consistency we use the (slightly unusual) notation used in [?], so an arbitrary finite abelian group will be written in the form $\mathbb{Z}_{a_0} \times \mathbb{Z}_{a_0 a_1} \times \dots \times \mathbb{Z}_{a_0 a_1 \dots a_{n-1}}$ where $a_i \geq 1$ for each i and the group operation is addition.

Automorphisms will usually be defined by matrices. Note that two matrices $A = [a_{ij}]$ and $B = [b_{ij}]$ represent the same map (with respect to the same basis) if their entries satisfy $a_{ij} \equiv b_{ij} \pmod{m_j}$ where m_j is the order of the j th basis element.

For every prime p dividing the order of an abelian group G , the p -primary part of G will be denoted by G_p .

1. PRELIMINARY RESULTS

Theorem 3. *Every finite abelian group is cyclically generated.*

Proof. Using the notation described previously, let $G = \mathbb{Z}_{a_0} \times \mathbb{Z}_{a_0 a_1} \times \cdots \times \mathbb{Z}_{a_0 a_1 \cdots a_{n-1}}$ where $a_i \geq 1$ for each i and let x_i be a generator of $\mathbb{Z}_{a_0 a_1 \cdots a_i}$. Define a map onto a generating set for G by $x_0 \mapsto x_0$ and $x_i \mapsto x_{i-1} + x_i$ for $i = 1, 2, \dots, n-1$. Note that this map is defined by the $n \times n$ matrix in which entries on the diagonal and sub-diagonal are 1 and all other entries are 0. As $o(x_{i-1}) \mid o(x_i)$, this map can be extended to an automorphism θ of G . Applying successive powers of θ to x_{n-1} gives

$$x_{n-1} \mapsto x_{n-2} + x_{n-1} \mapsto x_{n-3} + 2x_{n-2} + x_{n-1} \mapsto \cdots \mapsto x_0 + X + x_{n-1} \mapsto \cdots \mapsto x_{n-1}$$

where X is a sum of multiples of x_1, x_2, \dots, x_{n-2} and therefore the set $\{x_{n-1}\theta^j : j = 0, 1, \dots, o(\theta) - 1\}$ generates G . \square

Corollary 4. *If G is a finite abelian p -group then the order of the automorphism defined in the proof of Theorem ?? is a power of p .*

Lemma 5. *An automorphism θ cycles through a generating set for a group G if and only if every conjugate of θ in $\text{Aut } G$ cycles through a generating set.*

Proof. Suppose that θ has order n and x is such that $G = \langle x, x\theta, \dots, x\theta^{n-1} \rangle$. Let $\beta \in \text{Aut } G$. Then $\beta^{-1}\theta\beta$ cycles through a generating set containing $x\beta$. \square

Lemma 6. *If θ is a cyclic automorphism of a group G with $o(\theta) = n$, then for every characteristic subgroup K of G , the map $\hat{\theta}$ on G/K defined by $(gK)\hat{\theta} = g\theta K$ is a cyclic automorphism of order dividing n . It follows that if G has a characteristic subgroup K such that G/K is not cyclically generated by m generators for any m dividing n then G is not cyclically generated by n generators.*

Lemma 7. *A finite abelian group G is cyclically generated if and only if each of its primary parts is. Moreover, if the primary parts of G are $G_{p_1}, G_{p_2}, \dots, G_{p_k}$ and each G_{p_i} is cyclically generated by m_i generators then G has a cyclic generating set of size $\text{l.c.m.}(m_1, m_2, \dots, m_k)$.*

For a rank n abelian p -group with no repeated cyclic direct factors we determine necessary and sufficient conditions for a matrix to define an automorphism.

Lemma 8. *Let p be prime, let $G = \mathbb{Z}_{p^{\lambda_0}} \times \mathbb{Z}_{p^{\lambda_0+\lambda_1}} \times \cdots \times \mathbb{Z}_{p^{\lambda_0+\lambda_1+\cdots+\lambda_{n-1}}}$ where $\lambda_0, \lambda_1, \dots, \lambda_{n-1} \geq 1$, and let $\mathcal{E} = \{x_0, x_1, \dots, x_{n-1}\}$ be a canonical basis for G . Let $A = [a_{ij}]$ be an $n \times n$ matrix and let θ be the map defined by A with respect to \mathcal{E} . Then θ is an automorphism of G if and only if*

- (1) $p^{\lambda_i+\lambda_{i+1}+\cdots+\lambda_{j-1}}$ divides a_{ij} when $j > i$, and
- (2) $(a_{ii}, p) = 1$ for each i .

Proof. It is easy to verify that θ is a homomorphism if and only if condition (1) holds. Therefore, with the assumption that θ is a homomorphism, we prove that it is invertible if and only if condition (2) holds.

As θ is a homomorphism, condition (1) holds, so by expanding $\det A$ about the first column, we have $\det A \equiv a_{11}a_{22} \cdots a_{nn} \pmod{p}$. Therefore $\det A$ is coprime to p if and only if condition (2) holds. \square

This result has the following two useful corollaries. A simple counting argument gives the first (well known) corollary to Lemma ??.

Corollary 9. *The automorphism group of G has $p^\beta(p-1)^n$ elements for some β .*

Corollary 10. *Let $G = \mathbb{Z}_{p^{\lambda_0}} \times \mathbb{Z}_{p^{\lambda_0+\lambda_1}} \times \cdots \times \mathbb{Z}_{p^{\lambda_0+\lambda_1+\cdots+\lambda_{n-1}}}$ where $\lambda_i \geq 0$ for each i . A matrix satisfying conditions (1) and (2) in Lemma ?? defines an automorphism of G .*

Theorem 11. *If n is a square-free integer and p is a prime such that $p \equiv 1 \pmod{n}$ then every finite abelian p -group of rank $\leq n$ is cyclically generated by n generators.*

Proof. Let n be a product of distinct primes q_1, q_2, \dots, q_r . Let p be a prime with $p \equiv 1 \pmod{n}$, and let G be an abelian p -group with exponent p^λ and rank $\leq n$. As $p \equiv 1 \pmod{q_i}$ for each i , the group of units of \mathbb{Z}_{p^λ} contains an element α_i of order q_i for each i . Let $\alpha = \alpha_1\alpha_2 \cdots \alpha_r$. Then $\alpha^n \equiv 1 \pmod{p^\lambda}$. We use α to construct a cyclic automorphism of G .

If the rank of G is less than n we can extend G to the direct product of n cyclic subgroups by adding copies of the trivial group, and therefore we write $G = \mathbb{Z}_{p^{\lambda_0}} \times \mathbb{Z}_{p^{\lambda_0+\lambda_1}} \times \cdots \times \mathbb{Z}_{p^{\lambda_0+\lambda_1+\cdots+\lambda_{n-1}}}$ where $\lambda_0, \lambda_1, \dots, \lambda_{n-1} \geq 0$ and $\lambda_0 + \lambda_1 + \cdots + \lambda_{n-1} = \lambda$. Let $\mathcal{E} = \{x_1, x_2, \dots, x_n\}$ be a canonical basis for G and let $\theta : G \rightarrow G$ be the map defined with respect to \mathcal{E} by the matrix $\text{diag}\{\alpha, \alpha^2, \dots, \alpha^{n-1}, 1\}$. As α is coprime to p , the map θ is an automorphism, by Corollary ??, and it has order n by the definition of α . We need to show that θ cycles through a generating set for G .

Let $x = x_1 + x_2 + \cdots + x_n$. For every j in the range $j = 0, 1, \dots, n-1$, we have $x\theta^j = \sum_{i=1}^n \alpha^{ij}x_i$ and therefore

$$(1) \quad \sum_{j=0}^{n-1} x\theta^j = \sum_{j=0}^{n-1} \sum_{i=1}^n \alpha^{ij}x_i \equiv \sum_{i=1}^{n-1} x_i \left(\sum_{j=0}^{n-1} \alpha^{ij} \right) + nx_n \pmod{p^\lambda}.$$

For $i = 1, 2, \dots, n-1$, we will show that $\sum_{j=0}^{n-1} \alpha^{ij} \equiv 0 \pmod{p^\lambda}$, but we prove first that α^i satisfies $1 + \alpha^i + \alpha^{2i} + \dots + \alpha^{i(m_i-1)} \equiv 0 \pmod{p^\lambda}$ where m_i is the order of α^i . As $\alpha^{im_i} \equiv 1 \pmod{p^\lambda}$, we have $(\alpha^i - 1)(1 + \alpha^i + \alpha^{2i} + \dots + \alpha^{(m_i-1)i}) = \alpha^{m_i i} - 1 \equiv 0 \pmod{p^\lambda}$, so if we can show that $\alpha^i - 1$ is a unit in \mathbb{Z}_{p^λ} , then the result will follow.

Let μ be the largest power of p dividing $(\lambda-1)!$. If we suppose that $\alpha^i = 1 + kp$ then $(\alpha^i)^{p^{\lambda+\mu}} \equiv 1 \pmod{p^\lambda}$ and hence the order of α^i must be a power of p , but this is a contradiction because p and n are coprime.

Now let $q = (i, n)$ and note that if $q > 1$ then without loss of generality we can assume that for each i there is some k_i such that $q = q_1 q_2 \dots q_{k_i}$ and $i = lq$ for some l . Let $\hat{q} = n/q$, so α^i has order \hat{q} , and $1 + \alpha^i + \dots + \alpha^{i(\hat{q}-1)} \equiv 0 \pmod{p^\lambda}$. If $j \equiv j' \pmod{\hat{q}}$ then $\alpha^{ij} \equiv \alpha^{ij'} \pmod{p^\lambda}$. Therefore $\sum_{j=0}^{n-1} \alpha^{ij} \equiv q \sum_{j=0}^{\hat{q}-1} \alpha^{ij} \equiv 0 \pmod{p^\lambda}$ as required.

From equation (??) we now have $\sum_{j=0}^{n-1} x\theta^j \equiv nx_n \pmod{p^\lambda}$ and therefore x_n is in the subgroup generated by the $x\theta^j$ s. By replacing i by $i-t \pmod{n}$ in the argument above it can be shown that x_t is also in this subgroup for every t in the range $1, 2, \dots, n-1$. \square

2. ABELIAN GROUPS OF RANKS 3 AND 4 WITH CYCLIC MINIMAL GENERATING SETS

The results in the previous section will now be used to prove classification results for abelian groups of rank 3 or rank 4 with cyclic minimal generating sets. We begin with the rank 3 result.

Theorem 12. *Let $G = \mathbb{Z}_a \times \mathbb{Z}_{ab} \times \mathbb{Z}_{abc}$ where $a \geq 2$ and let \mathcal{A} be the set consisting of 1 and all products of primes of the form $6\lambda + 1$. Then G is cyclically generated by 3 generators if and only if either (b, c) is in \mathcal{A} or $\frac{1}{3}(b, c)$ is in \mathcal{A} .*

Proof. Let $G = \mathbb{Z}_a \times \mathbb{Z}_{ab} \times \mathbb{Z}_{abc}$. By Lemma ??, G is cyclically generated by 3 generators if and only if each of its p -primary parts is either cyclic or cyclically generated by 3 generators.

For every prime p dividing the order of G , we write G_p as $\mathbb{Z}_{p^\lambda} \times \mathbb{Z}_{p^{\lambda+\mu}} \times \mathbb{Z}_{p^{\lambda+\mu+\nu}}$ where $\lambda, \mu, \nu \geq 0$, and we assume that G_p is not cyclic. If $\lambda = \nu = 0$, or $\mu = \nu = 0$, or $\mu = 0$ or $\nu = 0$ then G_p satisfies Abért's conditions for $n = 3$, and hence it is cyclically generated by 3 generators by Abért's Theorem, [?].

It therefore remains to consider the case $\mu, \nu \geq 1$ and $\lambda \geq 0$. If $p \equiv 1 \pmod{6}$ then by Theorem ??, G_p has a cyclic automorphism of order 3, while if $p \equiv -1 \pmod{6}$ or $p = 2$ then by Corollary ??, G_p has no automorphism of order 3.

If $p = 3$ and at least one of μ and ν is 1, then G_3 is cyclically generated by 3 generators by Abért's Theorem. Finally we show that G_3 is not cyclically generated by 3 generators if $\mu \geq 2$ and $\nu \geq 2$.

Let $\mu = 2 + \mu'$ and $\nu = 2 + \nu'$ where $\mu', \nu' \geq 0$, and let $H = G_3/G_3(3^{\lambda+\mu'})$ and $K = H/3^4H$, so $K = \mathbb{Z}_9 \times \mathbb{Z}_{81}$. We prove that K is not cyclically generated by 3 generators.

Suppose that K has a cyclic automorphism θ of order 3. If θ is represented (with respect to the canonical basis $\{v, w\}$ for K) by the matrix A , then by Lemma ??, $a_{12} \equiv 0 \pmod{9}$ and $(a_{11}, 3) = (a_{22}, 3) = 1$. We consider the automorphisms induced by θ on two factor groups of K to obtain further information about the entries of A .

Let $\Phi(K)$ denote the Frattini subgroup of K and let φ be the natural homomorphism $K \rightarrow K/\Phi(K) = \mathbb{Z}_3 \times \mathbb{Z}_3$. Let θ_F denote the automorphism induced by θ on $K/\Phi(K)$ as defined in the proof of Lemma ?. Then θ_F must cycle through a generating set of size 3 for $K/\Phi(K)$ and, if B is the matrix that represents θ_F with respect to the basis $\{v\varphi, w\varphi\}$, then $b_{ij} \equiv a_{ij} \pmod{3}$. Therefore $b_{11}, b_{22} \in \{1, -1\}$ and $b_{12} = 0$, so $\det B = b_{11}b_{22} = \pm 1$. As θ_F has order 3, we must have $b_{11} = b_{22} = 1$ and hence $b_{21} = \pm 1$. It follows that $a_{11}, a_{22} \equiv 1 \pmod{3}$, and $a_{21} \equiv \pm 1 \pmod{3}$.

Now let ψ be the natural homomorphism $K \rightarrow K/9K$ and let θ' denote the automorphism of $K/9K$ induced by θ . We know that θ' is a cyclic automorphism of order 3 and, if C is the matrix that represents θ' with respect to the basis $\{v\psi, w\psi\}$, then $c_{ij} \equiv a_{ij} \pmod{9}$. From the information we have about the entries of A we know that $c_{12} = 0$, $c_{11}, c_{22} \equiv 1 \pmod{3}$ and $c_{21} \not\equiv 0 \pmod{3}$. By the assumption that θ' has order 3, we must therefore have $c_{11}^2 + c_{11}c_{22} + c_{22}^2 \equiv 0 \pmod{9}$. Completing the square gives $(c_{11} + 5c_{22})^2 \equiv 6c_{22}^2 \pmod{9}$, from which it follows that $3|c_{22}$, which is a contradiction. Therefore θ' cannot have order 3 and this proves that K and hence G_3 cannot be cyclically generated by 3 generators. \square

Theorem 13. *Let $G = \mathbb{Z}_a \times \mathbb{Z}_{ab} \times \mathbb{Z}_{abc} \times \mathbb{Z}_{abcd}$ where $a \geq 2$ and let \mathcal{B} be the set consisting of 1 and all products of primes of the form $4\lambda + 1$. Then G is cyclically generated by 4 generators if and only if either (b, c, d) is in \mathcal{B} or $\frac{1}{2}(b, c, d)$ is in \mathcal{B} .*

Proof. By Lemmas ?? and ??, we are looking for cyclic automorphisms of order 4 or 2 for each of the primary parts of G and as every finite abelian group of rank 2 is symmetrically generated by 2 generators, we only need to consider the primary parts that have rank 3 or 4. That is, those primary parts of G that correspond to primes that divide ab .

For every prime p dividing ab , we write G_p as $\mathbb{Z}_{p^\lambda} \times \mathbb{Z}_{p^{\lambda+\mu}} \times \mathbb{Z}_{p^{\lambda+\mu+\nu}} \times \mathbb{Z}_{p^{\lambda+\mu+\nu+\sigma}}$ where $\lambda, \mu, \nu, \sigma \geq 0$ and λ and μ are not both zero. We prove that the existence of a cyclic generating set of size four depends on the choice of p only if $\mu, \nu, \sigma \geq 1$.

If $\nu = \sigma = 0$ or if $\mu = \nu = 0$ then G_p satisfies Abért's conditions for $n = 4$ and is therefore cyclically generated by 4 generators.

If $\lambda = 0$, then for any $\beta > 0$, let $H_p = \mathbb{Z}_{p^\beta} \times \mathbb{Z}_{p^{\beta+\mu}} \times \mathbb{Z}_{p^{\beta+\mu+\nu}} \times \mathbb{Z}_{p^{\beta+\mu+\nu+\sigma}}$. Then $G_p \cong H_p/H_p(p^\beta)$, so if H_p is cyclically generated by 4 generators then G_p is cyclically generated by 2 or 4 generators. Therefore without loss of generality we can assume that $\lambda \geq 1$. With respect to a canonical basis $\{w, x, y, z\}$, the following matrices define automorphisms of order 4 that cycle through a generating set for G_p when applied to z in the cases $\mu = 0$, $\nu = 0$, and $\sigma = 0$ respectively.

$$\begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}.$$

We now show that if $\mu, \nu, \sigma \geq 1$ then G_p is cyclically generated by 4 generators if and only if $p \equiv 1 \pmod{4}$ or $p = 2$ and one of μ, ν, σ is at most 1.

We begin with the case that p is odd. Let $\{w, x, y, z\}$ be a canonical basis for G_p , where once again we can assume that $\lambda \geq 1$.

As $p \equiv 1 \pmod{4}$, -1 is a quadratic residue modulo p and hence modulo p^n for any n , see [?] p.69. Therefore there exists some α in $\mathbb{Z}_{p^{\lambda+\mu+\nu+\sigma}}$ such that $\alpha^4 \equiv -1 \pmod{p^{\lambda+\mu+\nu+\sigma}}$. With respect to the basis $\{w, x, y, z\}$, let θ be represented by the matrix $\text{diag}\{\alpha, -1, -\alpha, 1\}$. By construction, θ is an automorphism of order 4 and the set produced when θ is repeatedly applied to $w + x + y + z$ is $\{w + x + y + z, \alpha w - x - \alpha y + z, -w + x - y + z, -\alpha w - x + \alpha y + z\}$, which is a generating set for G_p .

Suppose now that $p \equiv -1 \pmod{4}$. We show that $G_p/G_p(p^\lambda)$ is not cyclically generated by 4 generators and it then follows by Lemma ?? that if $\lambda \geq 0$ then G_p is also not cyclically generated by 4 generators. As $p \equiv -1 \pmod{4}$, the Sylow 2-subgroup of each of $\text{Aut } \mathbb{Z}_{p^\mu}$, $\text{Aut } \mathbb{Z}_{p^{\mu+\nu}}$, and $\text{Aut } \mathbb{Z}_{p^{\mu+\nu+\sigma}}$, is \mathbb{Z}_2 , see [?] p.83 and therefore we have

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \leq \text{Aut } \mathbb{Z}_{p^\mu} \times \text{Aut } \mathbb{Z}_{p^{\mu+\nu}} \times \text{Aut } \mathbb{Z}_{p^{\mu+\nu+\sigma}} \leq \text{Aut } (G_p/G_p(p^\lambda)).$$

But by Corollary ??, the size of $\text{Aut } (G_p/G_p(p^\lambda))$ is $p^r(p-1)^3$ for some r , so the Sylow 2-subgroup of $\text{Aut } (G_p/G_p(p^\lambda))$ must be $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, and hence $G_p/G_p(p^\lambda)$ has no automorphism of order 4.

It remains to consider the case $p = 2$. If one of μ, ν, σ is 1 then we define cyclic automorphisms of order 4 in each of the three cases $\mu = 1, \nu = 1$, and $\sigma = 1$. As before, we can assume that $\lambda \geq 1$ and with respect to the usual basis $\{w, x, y, z\}$ for G_2 , the following matrices define automorphisms

of order 4 in the cases $\mu = 1, \nu = 1$, and $\sigma = 1$ respectively.

$$\begin{pmatrix} -1 & -2 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 & 0 \\ 1 & 1 & -2 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & -1 & -2 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

The automorphisms defined by these matrices cycle through a generating set for G_2 when applied to z .

Finally we show that G_2 cannot be cyclically generated by 4 generators if $\mu, \nu, \sigma \geq 2$.

As $\mu \geq 2$, we can write $\mu = \mu' + 2$, so

$$G_2 = \mathbb{Z}_{2^\lambda} \times \mathbb{Z}_{2^{\lambda+\mu'+2}} \times \mathbb{Z}_{2^{\lambda+\mu'+\nu+2}} \times \mathbb{Z}_{2^{\lambda+\mu'+\nu+\sigma+2}}.$$

If G_2 is cyclically generated by 4 generators then so is $G_2/G_2(2^{\lambda+\mu'})$, by Lemma ??, so we consider $G_2/G_2(2^{\lambda+\mu'})$. The proof is similar to the proof that $\mathbb{Z}_9 \times \mathbb{Z}_{81}$ has no cyclic automorphism of order 3.

Let $H = G_2/G_2(2^{\lambda+\mu'})$, so

$$H = \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^{\nu+2}} \times \mathbb{Z}_{2^{\nu+\sigma+2}}.$$

Suppose that H has a cyclic automorphism of order 4 and let A be the matrix that represents θ with respect to the usual basis for H . By Lemma ??, a_{11}, a_{22}, a_{33} must be odd and $2^\nu | a_{12}$, $2^{\nu+\sigma} | a_{13}$, and $2^\sigma | a_{23}$.

We first consider the automorphism θ_F induced by θ on $H/\Phi(H)$, which is $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Let this be defined, with respect to the usual basis, by the matrix B where $b_{ij} \equiv a_{ij} \pmod{2}$, so by Lemma ??, $b_{ij} = 0$ if $i < j$, $b_{ij} = 1$ if $i = j$, and there is no restriction on the choice of b_{21}, b_{31} and b_{32} . Therefore $B \in D_8 < \text{Aut}(H/\Phi(H))$, and since it must have order 4, we can assume without loss of generality that

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Now let C be the matrix produced when the entries of A are reduced modulo 4. This is the matrix that defines the automorphism induced by θ on the factor group $H/4H$. We know that $4 | a_{12}, 4 | a_{13}$, and $4 | a_{23}$ because $\nu, \sigma \geq 2$, and hence $c_{12} = c_{13} = c_{23} = 0$. Moreover, we know that the diagonal entries of C must be ± 1 , and from the form of B we know that $c_{31} = 2u$ for some u . Therefore C is conjugate to the matrix ,

$$\hat{C} = \begin{pmatrix} c_{11} & 0 & 0 \\ 1 & c_{22} & 0 \\ 2u & 1 & c_{33} \end{pmatrix}.$$

By noting that the entries on the sub-diagonal of \hat{C}^2 must be even, it follows that $\hat{C}^4 \neq I_4$, which is a contradiction. The result follows by Lemma ??. \square

3. RANK 5 ABELIAN GROUPS WITH CYCLIC MINIMAL GENERATING SETS

Unlike the rank 3 and 4 cases, we do not have a single classification result for finite abelian groups of rank 5 with cyclic minimal generating sets because we only have partial results for abelian 5-groups. We do, however, have the following result which, by Lemma ??, gives a classification for finite abelian groups of rank 5 and order not divisible by 5.

Theorem 14. *Let $p \neq 5$ be prime and let G be a noncyclic finite abelian p -group of rank ≤ 5 . Then G is cyclically generated by 5 generators if and only if*

- (i) G satisfies Abért's conditions for $n = 5$, or
- (ii) $p \equiv 1 \pmod{10}$, or
- (iii) $p \equiv -1 \pmod{10}$ and G can be written in the form $\mathbb{Z}_{p^\alpha} \times \mathbb{Z}_{p^\beta} \times \mathbb{Z}_{p^\beta} \times \mathbb{Z}_{p^\gamma} \times \mathbb{Z}_{p^\gamma}$ where $\alpha, \beta \geq 0$ and $\gamma \geq 1$.

We split all primes other than 5 into three classes: 2 and primes of the form $10k \pm 3$, primes of the form $10k - 1$, and primes of the form $10k + 1$. If p is in the last class then every noncyclic finite abelian p -group of rank at most 5 is cyclically generated by 5 generators by Theorem ??. We now present classification results for primes from the other classes.

Theorem 15. *Let G be a noncyclic finite abelian p -group of rank at most 5. If $p = 2$ or $p \equiv \pm 3 \pmod{10}$ then G has a cyclic automorphism of order 5 if and only if G satisfies Abért's conditions for $n = 5$.*

The proof uses the following lemma.

Lemma 16. *Let p be a prime and let G be an abelian p -group of rank 4 with precisely three repeated direct cyclic factors of order p^α . Then for some β , $|\text{Aut } G| = p^\beta(p-1)|GL(3, \mathbb{Z}_{p^\alpha})|$.*

Proof. There are two cases to consider; either the exponent of G is greater than the order of the repeated direct factors, or they are equal. In the first case a matrix A represents an automorphism of G (with respect to a canonical basis) if and only if the submatrix $[a_{ij}]_{i,j=1}^3$ is in $GL(3, \mathbb{Z}_{p^\lambda})$, $p^\mu | a_{i4}$ for $i = 1, 2, 3$, and $(a_{44}, p) = 1$, while in the second case A represents an automorphism if and only if the submatrix $[a_{ij}]_{i,j=2}^4$ is in $GL(3, \mathbb{Z}_{p^{\lambda+\mu}})$, $p^\mu | a_{1j}$ for $j = 2, 3, 4$, and $(a_{11}, p) = 1$. \square

We now prove Theorem ??:

Proof. We write $G = \mathbb{Z}_{p^\lambda} \times \mathbb{Z}_{p^{\lambda+\mu}} \times \mathbb{Z}_{p^{\lambda+\mu+\nu}} \times \mathbb{Z}_{p^{\lambda+\mu+\nu+\sigma}} \times \mathbb{Z}_{p^{\lambda+\mu+\nu+\sigma+\tau}}$. Assume that $p = 2$ or $p \equiv \pm 3 \pmod{10}$ and that G does not satisfy Abért's conditions for $n = 5$. If G has rank 2 or 3 then $G/\Phi(G)$ is an elementary abelian p -group of rank 2 or 3. However, if $p = 2$ or $p \equiv \pm 3 \pmod{10}$ then neither $GL(2, p)$ or $GL(3, p)$ has an element of order 5 and hence G is not cyclically generated by 5 generators by Lemma ??. Similarly, if ν or σ is non-zero then G has a characteristic subgroup K such that G/K is an

elementary abelian p -group of rank 2 or 3, and therefore G is not cyclically generated by 5 generators.

It only remains to prove that if $G = \mathbb{Z}_{p^\lambda} \times \mathbb{Z}_{p^{\lambda+\mu}} \times \mathbb{Z}_{p^{\lambda+\mu}} \times \mathbb{Z}_{p^{\lambda+\mu}} \times \mathbb{Z}_{p^{\lambda+\mu+\tau}}$ where $\lambda \geq 0$ and $\sigma, \tau \geq 1$ then G has no cyclic automorphism of order 5.

In this case G has a characteristic subgroup K such that $G/K = \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^{1+\tau}}$ and by Lemma ?? the automorphism group of this factor group has no element of order 5. Therefore G is not cyclically generated by 5 generators. \square

Theorem 17. *Let G be a noncyclic finite abelian p -group of rank at most 5. If $p \equiv -1 \pmod{10}$ then G is cyclically generated by 5 generators if and only if G is cyclic or satisfies Abért's conditions for $n = 5$, or, by a suitable rearrangement of the order of the direct factors, it can be written in the form $\mathbb{Z}_{p^\alpha} \times \mathbb{Z}_{p^\beta} \times \mathbb{Z}_{p^\beta} \times \mathbb{Z}_{p^\gamma} \times \mathbb{Z}_{p^\gamma}$ where $\alpha, \beta \geq 0$ and $\gamma \geq 1$.*

Again, before we prove the theorem we need the result of the following Lemma.

Lemma 18. *If $p \equiv -1 \pmod{10}$ then any element of order 5 in $GL(3, p)$ is conjugate to one of two block diagonal matrices $(1, v_x)$ where*

$$v_x = \begin{pmatrix} 0 & 1 \\ -1 & x \end{pmatrix}, \text{ and } x^2 + x - 1 \equiv 0 \pmod{p}.$$

Proof. As $p \equiv -1 \pmod{10}$, 5 is a quadratic residue modulo p^n for any $n \geq 1$, see [?], p.76, Theorem 97, and therefore, $x^2 + x - 1 \equiv 0 \pmod{p}$ has two distinct solutions, which we will denote by j and k . By choice of j and k , $v_j^5 = v_k^5 = 1$, and as the Sylow 5-subgroups of $GL(3, p)$ and $GL(2, p)$ have the same order, any matrix of order 5 in $GL(3, p)$ is conjugate to a block diagonal matrix $(1, X)$ where X has order 5 in $GL(2, p)$. It therefore follows from the representatives of the conjugacy classes of $GL(2, p)$ given in [?] p.326 and the fact that any element of order 5 in $GL(2, p)$ must lie in $SL(2, p)$, that the only matrices of order 5 in $GL(3, p)$ must be conjugate either to $(1, v_j)$ or to $(1, v_k)$. \square

We now prove Theorem ??:

Proof. Assume that $p \equiv -1 \pmod{10}$ and G can be written in the form $\mathbb{Z}_{p^\alpha} \times \mathbb{Z}_{p^\beta} \times \mathbb{Z}_{p^\beta} \times \mathbb{Z}_{p^\gamma} \times \mathbb{Z}_{p^\gamma}$ where $\alpha, \beta \geq 0$ and $\gamma \geq 1$, and $\{v, w, x, y, z\}$ is a canonical basis for G when it is written in this form. Let p^λ be the exponent of G and let j and k be the distinct roots of $x^2 + x - 1$ in \mathbb{Z}_{p^λ} . With respect to $\{v, w, x, y, z\}$, let θ be the automorphism defined by the block diagonal matrix $(1, v_j, v_k)$. As j and k are distinct and their difference is coprime to p , applying successive powers of θ to $v + w + y$ gives a generating set for G .

Now suppose that G is not cyclic, does not satisfy Abért's conditions for $n = 5$, and cannot be written in the form in the statement of the theorem. If $\sigma, \tau \geq 1$ then G has a characteristic subgroup K such that $G/K = \mathbb{Z}_{p^\sigma} \times \mathbb{Z}_{p^{\sigma+\tau}}$, which has no automorphism of order 5 by Corollary ?. The only

other cases to consider are $\nu = \sigma = 0$, $\sigma = \tau = 0$, $\sigma = 0$, and $\tau = 0$, where we assume $\lambda \geq 0$, but $\mu, \nu, \sigma, \tau \geq 1$ unless stated otherwise. In the first case, either G or $G/G(p^\lambda)$ is $\mathbb{Z}_{p^\mu} \times \mathbb{Z}_{p^\mu} \times \mathbb{Z}_{p^\mu} \times \mathbb{Z}_{p^{\mu+\tau}}$ and in the other cases either G or $G/G(p^\lambda)$ is $\mathbb{Z}_{p^\mu} \times \mathbb{Z}_{p^{\mu+\nu}} \times \mathbb{Z}_{p^{\mu+\nu}} \times \mathbb{Z}_{p^{\mu+\nu}}$ or has a characteristic subgroup K such that G/K or $(G/G(p^\lambda))/K$ is of this form. We show! that a group of the second form has no cyclic automorphism of order 5. The proof for a group of the first form is similar.

Let $H = \mathbb{Z}_{p^\mu} \times \mathbb{Z}_{p^{\mu+\nu}} \times \mathbb{Z}_{p^{\mu+\nu}} \times \mathbb{Z}_{p^{\mu+\nu}}$ and let $\{w, x, y, z\}$ be a canonical basis for H . Note that every basis \mathcal{B}' for the subgroup $\mathbb{Z}_{p^{\mu+\nu}} \times \mathbb{Z}_{p^{\mu+\nu}} \times \mathbb{Z}_{p^{\mu+\nu}}$ can be extended to a basis $\mathcal{B} = \{w\} \cup \mathcal{B}'$ for H . Suppose that H has a cyclic automorphism θ of order 5 and θ is represented with respect to \mathcal{B} by the matrix A . By Lemma ??, θ induces a cyclic automorphism θ_F of order 5 on $H/\Phi(H)$, and if ϕ is the natural homomorphism $H \rightarrow H/\Phi(H)$ then by the proof of Lemma ??, θ_F is represented with respect to the basis $\mathcal{B}\phi$ by the matrix C where $c_{ij} \equiv a_{ij} \pmod{p}$ and

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ c_{21} & & & \\ c_{31} & C' & & \\ c_{41} & & & \end{pmatrix} \quad \text{where } C' \in GL(3, p) \text{ has order 5.}$$

By Lemma ??, C' is conjugate to $(1, v_j)$ or $(1, v_k)$, and we can assume that \mathcal{B}' was chosen so that $C' = (1, v_j)$ or $C' = (1, v_k)$. Assume therefore that $C' = (1, v_j)$. Now we prove that C is conjugate to the block diagonal matrix $T = (1, 1, v_j)$. The assumption that $C^5 = I_4$ means that $c_{21} = 0$, but does not restrict the choice of c_{31} and c_{41} , and if Y is the 4×4 matrix with diagonal entries 1 and all other entries 0 except $y_{31} = \frac{c_{31}(1-j)-c_{41}}{2-j}$ and $y_{41} = \frac{c_{31}+c_{41}}{2-j}$, then $Y^{-1}CY = T$. Therefore there is a basis $\mathcal{E} = \{e_1, e_2, e_3, e_4\}$ for $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ such that T is the matrix defining θ_F with respect to \mathcal{E} . However, because of the form of T , we know that $\langle e_3, e_4 \rangle$ is θ_F invariant and θ_F acts as the identity on $\langle e_1, e_2 \rangle$. Therefore θ_F cannot cycle through a generating set. The result follows by Lemma ??. \square

4. CYCLIC GENERATING SETS OF PRIME SIZE FOR ABELIAN GROUPS OF RANK 2

We present a result about the non-existence of a cyclic generating set of prime size p for a certain p -group of rank 2 and this leads to a classification of rank 2 abelian p -groups with cyclic generating sets of size p .

Theorem 19. *Let p be a prime. The group $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ is cyclically generated by p generators if and only if $p = 2$ or $p = 3$.*

Proof. The reason for this result is that for $p \geq 5$, the cyclic automorphisms of $\mathbb{Z}_p \times \mathbb{Z}_p$ that have order p are induced by cyclic automorphisms of $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ of order p^2 . Any automorphism of $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ of order p induces only the identity map on $\mathbb{Z}_p \times \mathbb{Z}_p$.

Let $G = \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$. The matrices $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 6 & 1 \end{pmatrix}$ define cyclic automorphism of order p for $p = 2$ and $p = 3$ respectively.

Now suppose $p \geq 5$ and suppose that G has a cyclic automorphism θ of order p . By Lemma ??, θ induces a cyclic automorphism θ_F of order p on $G/\Phi(G)$, and if A is a matrix representing θ then (with respect to the relevant basis for $G/\Phi(G)$) the induced automorphism θ_F is represented by the matrix $A' = [a_{ij} \pmod{p}]$, where A' has order p in $GL(2, p)$. Without loss of generality we can therefore assume that the basis of G was chosen so that $A' = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and $A = \begin{pmatrix} 1 + ip & 1 + jp \\ kp & 1 + lp \end{pmatrix}$. We show that the 1,2 entry of A^p is not 0 when reduced modulo p^2 and therefore A^p does not represent the identity map.

The 1,2 entry of A^p is $(1 + jp)y_{p-1}$ where

$$y_{p-1} = \sum_{s=0}^{\lfloor (p-1)/2 \rfloor} \binom{p-1-s}{s} T^{p-1-2s} (-D)^s$$

and T and D are the trace and determinant of A ; see Theorem 1 of [?]. By using equation (7.1) in the same paper we can prove that

$$y_{p-1} \equiv p \left(1 - k \underbrace{\sum_{s=0}^{\lfloor (p-1)/2 \rfloor} \binom{p-1-s}{s} 2^{p-1-2s} (-1)^s s}_{\Delta} \right) \pmod{p^2}$$

and therefore $(1 + jp)y_{p-1} \equiv y_{p-1} \pmod{p^2}$. It is therefore sufficient to show that $y_{p-1} \not\equiv 0 \pmod{p^2}$. We do this by showing that the sum labelled Δ is divisible by p for $p \geq 5$. Note that for $p \geq 5$, $\lfloor (p-1)/2 \rfloor = (p-1)/2 \geq 2$. By Corollary 2 on page 4 of [?] we have

$$\binom{p-1-s}{s} = 2^{-p+1+2s} \sum_{t=s}^{(p-1)/2} \binom{p}{2t+1} \binom{t}{s}$$

and for $1 \leq s \leq t < (p-1)/2$ it follows that

$$\binom{p-1-s}{s} \equiv 2^{-p+1+2s} \binom{(p-1)/2}{s} \pmod{p}.$$

Therefore

$$\begin{aligned}
\Delta &\equiv \sum_{s=1}^{(p-1)/2} \binom{(p-1)/2}{s} (-1)^s s \pmod{p} \\
&= \frac{p-1}{2} \sum_{s=1}^{(p-3)/2} \binom{(p-3)/2}{s-1} (-1)^s \\
&= -\frac{p-1}{2} \sum_{s=0}^{(p-3)/2} \binom{(p-3)/2}{s} (-1)^s,
\end{aligned}$$

which is 0 by the Binomial Theorem because $(p-3)/2 \geq 1$ and hence $y_{p-1} \equiv p \pmod{p^2}$, as required. \square

Finally we state a classification result, the proof of which follows from Abért's Theorem, Theorems ?? and ??, and Corollary ??.

Theorem 20. *A rank 2 abelian p -group, $\mathbb{Z}_{p^\lambda} \times \mathbb{Z}_{p^{\lambda+\mu}}$, is cyclically generated by p generators if and only if λ , μ , and p satisfy one of the following conditions:*

- (i) $p = 2$, or
- (ii) $p = 3$ and either $\lambda = 1$ or $\mu \leq 1$, or
- (iii) $p \geq 5$ and $\lambda = 1$.