BULL. AUSTRAL. MATH. SOC. 20K10, 20F28
VOL. 67 (2003) [511–519]

DETERMINATION OF TORSION ABELIAN GROUPS BY THEIR AUTOMORPHISM GROUPS

P. SCHULTZ, A. SEBELDIN AND A.L. SYLLA

An Abelian torsion group is determined by its automorphism group if and only if its locally cyclic component is determined by its automorphism group. We describe the locally cyclic groups that are determined by their automorphism groups.

1. INTRODUCTION AND NOTATION

The Baer–Kaplansky Theorem ([**2**]) states that two torsion Abelian groups are isomorphic when their endomorphism rings are isomorphic. Leptin [**3**] showed that for $p > 3$, two Abelian p-groups are isomorphic when their automorphism groups are isomorphic. This result was extended by Liebert [**4**] to $p = 3$ and eventually Schultz [**5**] found a proof for all p, including $p = 2$. The purpose of this paper is to determine the groups that are determined by their automorphism groups in the class of all torsion Abelian groups.

We say that a group G of a class Ω is determined by its automorphism group in this class if there does not exist a non-isomorphic group H in Ω with $\operatorname{Aut} G \cong \operatorname{Aut} H$. Let $\Omega(\operatorname{Aut})$ be the subclass of Ω consisting of groups determined in Ω by their automorphism groups.

We denote by

A	the class of torsion Abelian groups
C	the class of torsion cyclic groups
D	the class of torsion locally cyclic groups
P	the set of all prime numbers
$\mathbb{Z}^+$	the set of positive integers 1, 2, ...
$\mathbb{N}$	the set of natural numbers 0, 1, ...
$\mathbb{Z}(n)$	the additive cyclic group of order n
$\mathbb{Z}_n$	the multiplicative cyclic group of order n
GF(p)	the field of order p

Received 11th November, 2002
The main results in this paper were presented at the Borevich Conference in St Petersburg, September, 2002.

$J(p)$	the ring of p-adic integers
J_p	the multiplicative group of p-adic units
$\mathcal{Z}(X)$	the centre of the group X.

If G is a torsion Abelian group, let G_p be the p-component of G and $P(G)$ the set $\{p \in \mathbf{P} : G_p \neq 0\}$ of relevant primes for G. Let $P_a = P_a(G)$, $P_b = P_b(G)$ and $P_c = P_c(G)$ be the sets of primes for which G_p is not bounded, bounded but not cyclic, and cyclic respectively. Finally, let $G_a = \bigoplus_{p \in P_a} G_p$, $G_b = \bigoplus_{p \in P_b} G_p$ and $G_c = \bigoplus_{p \in P_c} G_p$. Other notation is conventional or taken from [**2**].

2. Basic Results

We begin by reviewing some well-known results and their immediate consequences.

Lemma 2.1.

1. $\operatorname{Aut} G \cong \prod_{p \in \mathbf{P}} \operatorname{Aut} G_p$.
2. *If* $p \geqslant 3 \in \mathbf{P}$ *and* $k \geqslant 1$, *then* $\operatorname{Aut} \mathbb{Z}(p^k) \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{k-1}}$.
3. $\operatorname{Aut} \mathbb{Z}(2) = \{1\}, \operatorname{Aut} \mathbb{Z}(4) \cong \mathbb{Z}_2$ *and* $\operatorname{Aut} \mathbb{Z}(2^k) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$ *for* $k \geqslant 3$. *It follows that if* $G_2 = 0$ *then* $\operatorname{Aut} G \cong \operatorname{Aut}(G \oplus \mathbb{Z}(2))$.
4. (See [**3**].) *If* G *is a p-group and* H *is a q-group for primes* $3 \leqslant p < q$, *then* $\operatorname{Aut} G \cong \operatorname{Aut} H$ *if and only if* $G \cong \mathbb{Z}(p^k)$, $H \cong \mathbb{Z}(q)$ *and* $p^{k-1}(p-1) = q-1$.
5. *If* G *and* $H \in \mathbf{A}$ *such that* $\operatorname{Aut} G \cong \operatorname{Aut} H$, *then* $P_a(G) = P_a(H)$. *In fact, according to* [**2**, Theorem 115.1], $\mathcal{Z}(\operatorname{Aut} G)$ *contains* J_p *as a direct factor if and only if* G_p *is unbounded.*

Lemma 2.1, 5. implies that $\operatorname{Aut} G$ determines the set P_a of primes p for which G_p is unbounded. The next Proposition likewise shows that $\operatorname{Aut} G$ also determines the set P_b of primes p for which G_p is bounded but not cyclic.

Proposition 2.2. *Let* $G \in \mathbf{A}$. *Then* $p \in P_b$ *if and only if* $\operatorname{Aut} G$ *contains a non-commutative normal p-subgroup but no direct factor* $\cong J_p$.

Proof: Suppose G_p is non-zero and bounded. Then by Lemma 2.1, 5., $\operatorname{Aut} G$ has no direct factor $\cong J_p$. It was shown in [**5**, Theorem A] that $\operatorname{Aut} G_p$, which is a direct factor of $\operatorname{Aut} G$, has a non-trivial maximal normal p-subgroup Δ_p. It is easy to see that Δ_p is commutative if and only if G_p is cyclic.

Conversely, suppose $\operatorname{Aut} G$ contains a non-commutative normal p-subgroup Δ_p but no direct factor $\cong J_p$. By Lemma 2.1, 5., $p \notin P_a$. Each projection of Δ_p onto the direct factor $\operatorname{Aut} G_q$ of $\operatorname{Aut} G$ is a normal p-subgroup, so at least one is non-commutative. But by [**5**] again, $\operatorname{Aut} G_q$ contains a non-commutative normal p-subgroup if and only if $p = q$. ∎

PROPOSITION 2.3. *Let $G \in \mathbf{A}$. If $p \in P_a \cup P_b$, then G_p is determined by* $\operatorname{Aut} G$.

PROOF: Let $p \in P_a \cup P_b$. It was shown in [**5**, Theorem A] that except for the exceptional groups described below, G_p is determined by its maximal normal p-subgroup Δ_p. Now if G_p is not cyclic and $p > 2$, then Δ_p has no commutative direct factor so Δ_p is the unique normal p-subgroup of $\operatorname{Aut} G$ which is maximal with respect to having no commutative direct factor. If $p = 2$ then $\Delta_2 = \langle -1 \rangle \times \Delta_2'$ and Δ_2' is the unique normal 2-subgroup of of $\operatorname{Aut} G$ which is maximal with respect to having no commutative direct factor.

It remains to consider the exceptional case ([**5**, Theorem B]), in which $G_p = D_p \oplus B_p$ where D_p is divisible of rank r_p and B_p is elementary of rank s_p say. In that case, $\operatorname{Aut} G/\Delta_p$ contains as a direct factor $\operatorname{Aut} D_p \times \operatorname{Aut} B_p$. The first term is the general linear group of degree r_p over $J(p)$, and the second is the general linear group of degree s_p over $\mathrm{GF}(p)$. Since $\operatorname{Aut} G/\Delta_p$ contains no other factors of these two types if $s_p > 1$, we are done. ∎

COROLLARY 2.4. *Let G and $H \in \mathbf{A}$ with $\operatorname{Aut} G \cong \operatorname{Aut} H$. Then $G_a \oplus G_b \cong H_a \oplus H_b$.*

We can now settle the case of p-groups in $\mathbf{A}(\mathrm{Aut})$.

PROPOSITION 2.5. *Let G be an Abelian p-group. Then G is in $\mathbf{A}(\mathrm{Aut})$ if and only if $p = 2$ and*

1. *$G \cong \mathbb{Z}(2^k)$ with $k \geqslant 2$ and $2^{k-2} + 1$ is composite; or*
2. *G is bounded but not cyclic; or*
3. *G is unbounded and $G \not\cong \mathbb{Z}(2^\infty) \oplus \mathbb{Z}(2)$.*

PROOF: ($\Rightarrow$) If G is a p-group in $\mathbf{A}(\mathrm{Aut})$ then $p = 2$ by Lemma 2.1, 3.

1. Suppose G is cyclic. Since $\operatorname{Aut} \mathbb{Z}(2) \cong \operatorname{Aut} 0$ and $\operatorname{Aut} \mathbb{Z}(4) \cong \operatorname{Aut} \mathbb{Z}(3)$ we have that $G \cong \mathbb{Z}(2^k)$ for some $k \geqslant 3$. If $2^{k-2} + 1 = q$ is prime, then by Lemma 2.1, 4., $\operatorname{Aut}(G) \cong \operatorname{Aut}(\mathbb{Z}(q) \oplus \mathbb{Z}(4))$, a contradiction, so $2^{k-2} + 1$ is composite.
2. If G is bounded but not cyclic, there is nothing to prove.
3. Suppose then that G is unbounded. If $G \cong \mathbb{Z}(2^\infty) \oplus \mathbb{Z}(2)$, then an easy computation shows that $\operatorname{Aut} G \cong \operatorname{Aut}(\mathbb{Z}(2^\infty) \oplus \mathbb{Z}(3))$, so 3. holds.

($\Leftarrow$) Conversely, let G be a 2-group and suppose H is a torsion Abelian group with $\operatorname{Aut} G \cong \operatorname{Aut} H$. We consider the three conditions in turn.

1. $G \cong \mathbb{Z}(2^k)$ with $k \geqslant 2$ and $2^{k-2} + 1$ composite. Then $k \geqslant 5$, so $\operatorname{Aut} G \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$. In particular, $\operatorname{Aut} G$ is commutative so by [**2**, Theorem 115.1], H is cyclic.

If there exists $p \neq 2$ such that $H_p \neq 0$, and $H_p \cong \mathbb{Z}(p^m)$ with $m > 1$ then by Lemma 2.1, 1., $\operatorname{Aut} H$ has a direct factor which is a p-group, a contradiction. Hence $H_p \cong \mathbb{Z}(p)$

for every $p \in P(H) \setminus \{2\}$. Hence $\operatorname{Aut} H \cong \operatorname{Aut} H_2 \times K$, where $K = \prod_{p \in P(H)\setminus\{2\}} \mathbb{Z}_{p-1}$. Thus each $\mathbb{Z}_{p-1}$ is a 2-group, so $P(H) = \{2\}$, $\{2,p\}$, $\{2,p,q\}$ or $\{p,q\}$ for distinct primes p and $q \neq 2$.

If $P(H) = \{2\}$ then by [**5**], $H \cong G$.

In the remaining cases, H_p or $H_q \cong \mathbb{Z}(2^{k-2}+1)$, contradicting Condition 1.

2. G is bounded but not cyclic with $2^k G = 0, 2^{k-1}G \neq 0$.

   (a) If $k = 1$ then G is a vector space of dimension $n \geqslant 2$ and $\operatorname{Aut}(G) \cong \operatorname{GL}(n,2)$. It is well-known that this implies $H \cong G$.

   (b) If $k = 2$, then $G = \bigoplus_\alpha \mathbb{Z}(2) \oplus \bigoplus_\beta \mathbb{Z}(4)$ where $\alpha + \beta > 1$ and $\beta \neq 0$. In this case, $\mathcal{Z}(\operatorname{Aut} H) \cong \mathcal{Z}(\operatorname{Aut} G) \cong \mathbb{Z}_2$, so by [**2**, Theorem 115.1], if $H \neq H_2$ then $H_3 \cong \bigoplus_\gamma \mathbb{Z}(3)$. Since $\operatorname{Aut} H$ is not commutative, $\gamma > 1$ and hence $\operatorname{Aut} H$ contains an element of order 3, a contradiction. Thus $H = H_2$ and $H \not\cong \mathbb{Z}(2)$, so by [**5**], $H \cong G$.

   (c) If $k = 3$, then $\mathcal{Z}(\operatorname{Aut} H) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Thus if $H \neq H_2$ then $H \cong \bigoplus_{\delta(3)} \mathbb{Z}(3) \oplus \bigoplus_{\delta(2)} \mathbb{Z}(2) \oplus \bigoplus_{\delta(4)} \mathbb{Z}(4)$ where $\delta(3) + \delta(2) + \delta(4) > 2$, $\delta(3) > 0$ and $\delta(4) > 0$. If $\delta(3) > 1$, then $\operatorname{Aut} H$ has elements of order 3, a contradiction, so $\delta(3) = 1$. Hence $\delta(2) + \delta(4) > 1$. Since $k = 3$, $G \cong \bigoplus_{\alpha(2)} \mathbb{Z}(2) \oplus \bigoplus_{\alpha(4)} \mathbb{Z}(4) \oplus \bigoplus_{\alpha(8)} \mathbb{Z}(8)$, where $\alpha(8) \geqslant 1$. It follows that for any choice of $\alpha(i)$, $i = 2, 4, 8$ and $\delta(j)$, $j = 2, 4$, we have $\operatorname{Aut} H \not\cong \operatorname{Aut} G$, a contradiction. Thus $H = H_2$, so by [**5**], $H \cong G$.

   (d) If $k \geqslant 4$, then $\mathcal{Z}(\operatorname{Aut} H) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$ and hence H has a direct summand H_p where $r(H_p) > 1$ and $p > 3$. Hence H is a bounded 2-group such that $\operatorname{Aut} G \cong \operatorname{Aut} H$, so by [**5**], $H \cong G$.

3. G is not bounded, and $G \neq \mathbb{Z}(2^\infty) \oplus \mathbb{Z}(2)$. Then $\operatorname{Aut} G \neq \mathcal{Z}(\operatorname{Aut} G) \cong \mathbb{Z}_2 \times J_2$ or $\operatorname{Aut} G \cong J_2$. Hence H is an unbounded 2-group such that $\operatorname{Aut} G \cong \operatorname{Aut} H$, so by [**5**], $H \cong G$. ∎

REMARK 2.6. It is well-known that if $2^k + 1$ is prime, then k is a power of 2 and $F_i = 2^{2^i} + 1$ is a so-called Fermat prime. Only five Fermat primes are known, $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$.

3. Locally cyclic groups

Let G and H be Abelian torsion groups with $\operatorname{Aut} G \cong \operatorname{Aut} H$. By Corollary 2.4, we know that $G \cong H$ if and only if $G_c \cong H_c$, so we now assume that $G \in \mathbf{D}$, the class of direct sums of cyclic groups of distinct prime power orders, known as locally cyclic groups because $\mathbf{D}$ is the class of groups for which every finite subset is contained in a cyclic summand.

From now on, $G = \bigoplus_{p\in\mathbf{P}(G)} G_p$ with $G_p \cong \mathbb{Z}(p^{n_p})$ for some $n_p \in \mathbb{Z}^+$. It follows that $\operatorname{Aut} G = \prod_{p\in\mathbf{P}(G)} \operatorname{Aut} G_p$ where $\operatorname{Aut} G_p$ is described in Lemma 2.1. In particular, $\operatorname{Aut} G$ is a direct product of cyclic groups. Furthermore, for any reduced $H \in \mathbf{A}$, $\operatorname{Aut} H$ is Abelian if and only if $H \in \mathbf{D}$.

We need some more notation. Let $\mathbb{S}N$, the set of *supernatural numbers*, be the set of all formal products

$$\mathbf{n} = \prod_{p\in\mathbf{P}} p^{n_p} \text{ where } n_p \in \mathbb{N}.$$

A prime p is *relevant* for $G \in \mathbf{D}$ or for $\mathbf{n} \in \mathbb{S}N$ if $n_p > 0$. Thus $G \in \mathbf{D}$ is completely determined by a supernatural number $\mathbf{n}$, and we denote G by $\mathbb{Z}(\mathbf{n})$. The correspondence $\mathbb{Z}(\mathbf{n}) \leftrightarrow \mathbf{n}$ from $\mathbf{D}$ to $\mathbb{S}N$ is a bijection. If $\mathbf{n} \in \mathbb{S}N$, let $\mathbf{P}(\mathbf{n})$ denote the set of primes relevant for $\mathbf{n}$.

Let $\mathbb{Z}(\mathbf{n}) \in \mathbf{D}$, and let $M(\mathbf{n})$ be the multiset consisting of the orders of all the prime power direct summands of $\operatorname{Aut} \mathbb{Z}(\mathbf{n})$. We begin with the simplest case in which $\mathbf{n}$ is a prime power. A finite multiset M of prime powers is called *allowable* if $M = M(p^k)$ for some prime power p^k.

The following Lemma is a mild extension of Leptin's Theorem, since it includes the case $p = 2$.

LEMMA 3.1. *Let M be a non-empty finite multiset of prime powers and let m be the product of the terms in M. Then $M = M(p^k)$ for some prime power if and only if either*

(a) *$M = \{2, 2^\ell\}$ for some $\ell \in \mathbb{Z}^+$, or*

(b) *p^ℓ is the largest term in M for some $\ell \in \mathbb{Z}^+$ and M consists of the prime power factors of $m = p^\ell(p-1)$, or*

(c) *$m + 1 = q$ is prime and M consists of the prime power factors of m.*

There are two distinct prime powers p^k and q for which $M = M(p^k) = M(q)$ if and only if M satisfies both (b) *and* (c).

PROOF: Suppose $M = M(p^k)$. If $p = 2$ and $k > 2$, then $\operatorname{Aut} \mathbb{Z}(p^k) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$ and we have case (a).

If $p^k = 4$, or if $p > 2$ and $k > 1$, then $\operatorname{Aut} \mathbb{Z}(p^k) \cong \mathbb{Z}_{p^{k-1}} \times \mathbb{Z}_{p-1}$ and we have case (b).

Finally, if $p > 2$ and $k = 1$, then $\operatorname{Aut} \mathbb{Z}(p^k) \cong \mathbb{Z}_{p-1}$ and we have case (c).

Conversely, if M satisfies (a), then $M = M(2^{\ell+2})$. If M satisfies (b), then $M = M(p^{\ell+1})$. If M satisfies (c), then $M = M(q)$.

It follows that if M satisfies both (b) and (c) then $M = M(p^k) = M(q)$ with $p^k \neq q$. Conversely, if $M = M(p^k) = M(q^\ell)$ with $p^k \neq q^\ell$, then M does not satisfy (a) so M satisfies both (b) and (c). ∎

https://doi.org/10.1017/S0004972700037308 Published online by Cambridge University Press

Examples of a multiset M satisfying both (b) and (c) of Lemma 3.1 include $M(9) = \{2, 3\} = M(7)$ given already by Leptin's Theorem, and $M(4) = \{2\} = M(3)$.

We now consider the next simplest case, in which $\mathbf{n}$ is finite. Let $G = \mathbb{Z}(n)$, $n = \prod_{p \in \mathbf{P}(n)} p^{n_p} \in \mathbb{Z}^+$.

The multiset $M(n)$ has a partition $\{M_p : p \in \mathbf{P}(n)\}$ where M_p is an allowable multiset consisting of the orders of the prime power summands of $\operatorname{Aut} \mathbb{Z}(p^{n_p})$. Thus each part of the partition determines one or two primes p such that $M_p = M(p^k)$ for some k. Distinct partitions determine distinct n, but a given partition may determine several different n.

The following properties characterise the multisets $M(n)$:

PROPOSITION 3.2. *Let M be a multiset of prime powers. Then*

(a) *$M = M(n)$ for some positive integer n if and only if M has a partition $Q = \{M_p : p \in \mathbf{P}(n)\}$ into allowable multisets M_p such that $M_p = M(p^{n_p})$.*

(b) *Let Q be a partition of M into allowable multisets. If two parts of Q are identical, then one satisfies* (b) *and the other* (c) *of Lemma 3.1 and no other part of Q is identical to them.*

(c) *Let $\mathcal{P}(M)$ be the set of partitions of M into allowable multisets. For each partition $Q \in \mathcal{P}(M)$, let Q_1 be the set of parts of Q satisfying only one of* (a), (b) *or* (c) *of Lemma 3.1, and let Q_2 be the multiset of parts satisfying both (b) and (c) such that both M_p and M_q are parts of Q. Let $Q_3 = Q \setminus (Q_1 \cup Q_2)$ be the remaining parts of Q. If some $\{2, 2^\ell\}$ occurs in Q_1 or if $\{2\}$ occurs in Q_2, let $N(Q) = |Q_4|$. otherwise, let $N(Q) = |Q_4 + 1|$. Then $\left|\{n \in \mathbb{Z}^+ : M = M(n)\}\right| = \sum_{Q \in \mathcal{P}(M)} 2^{N(Q)}$.*

PROOF: We have seen that n determines a multiset $M = M(n)$ and a partition Q of M into allowable parts satisfying (a) and (b). Part (c) counts the number of partitions Q having a part which determines two prime powers, only one of which appears in Q, or for which no part determines a positive power of 2.

Conversely, suppose M is a multiset having a partition Q into allowable parts satisfying (a) and (b). Then the parts determine distinct prime powers whose product is n such that $M = M(n)$.

Finally, if $M = M(n)$ for k distinct n, then k is the power of 2 determined in (c). $\square$

COROLLARY 3.3. *Let $n = \prod_{p \in \mathbf{P}(n)} p^{n_p}$ and let $M = M(n)$. For all $p \in \mathbf{P}(n)$ let m_p be the product of the terms in the finite set M_p and let p^k be the largest element of M_p. Then $\mathbb{Z}(n) \in \mathbf{A}(\mathrm{Aut})$ if and only if M has a unique partition $Q = \{M_p : p \in \mathbf{P}(n)\}$ into allowable multisets M_p and:*

(a) *$4 \mid n$; and*

(b) *Whenever both $m_p = p^k(p-1)$ and $m_p + 1 = q$ is prime, then $q \in \mathbf{P}(n)$ and M_p and M_q both occur in Q.*

PROOF: ($\Leftarrow$) Since M has only one partition into allowable parts and the conditions of Proposition 3.2, (c) are satisfied with $N(Q) = 0$, n is unique.

($\Rightarrow$) Conversely, if $\mathbb{Z}(n)$ is determined by its automorphism group then M has only one partition Q into allowable parts and in Proposition 3.2, (c), $N(Q) = 0$. Hence n has a non-zero 2-component not equal to 2, so conditions (a) and (b) of the Corollary hold. ∎

As an illustration of Corollary 3.3, here is an example of a cyclic group determined by its automorphism group:

EXAMPLE 3.4.

$$\operatorname{Aut}\mathbb{Z}(252) \cong \operatorname{Aut}\mathbb{Z}(4) \times \operatorname{Aut}\mathbb{Z}(7) \times \operatorname{Aut}\mathbb{Z}(9) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3,$$

so $M(252) = \{2, 2, 2, 3, 3\}$.

There is only one partition of $M(252)$ satisfying Proposition 3.2, namely $\{\{2\}, \{2,3\}, \{2,3\}\}$. Since the prime indices of the parts must be distinct, the only possibilities are $M_2 = \{2\}$, $n_2 = 4$, $M_3 = \{2,3\}$, $n_3 = 9$ and $M_7 = \{2,3\}$, $n_7 = 7$. Thus $\mathbb{Z}(252)$ is determined by its automorphism group in $\mathbf{A}$.

We have already seen how a given partition of M may give rise to distinct n. Here is an example of a multiset M having different partitions into allowable parts:

EXAMPLE 3.5. Let $n = 4 \times 3 \times 67$. Then $M = M(n) = \{2, 2, 2, 3, 11\}$. M has partitions $\{\{2\}, \{2\}, \{2, 3, 11\}\}$ corresponding to the original n and $M = \{\{2\}, \{2, 3\}, \{2, 11\}\}$ corresponding to both $n = 4 \times 7 \times 23$ and $n = 4 \times 9 \times 23$.

There are no other possibilities for n.

The problem of finding explicitly all $m \in \mathbb{Z}^+$ such that $\operatorname{Aut}\mathbb{Z}(n) \cong \operatorname{Aut}\mathbb{Z}(m)$ for any given n is difficult, but we have an algorithmic solution based on the following Lemma.

LEMMA 3.6. *For any $2 \neq n \in \mathbb{Z}^+$, $|\operatorname{Aut}\mathbb{Z}(n)| < n \leqslant |\operatorname{Aut}\mathbb{Z}(n)|^2$, with equality on the right if and only if $n = 4$.*

PROOF: By Lemma 2.1, 1., it suffices to consider the case $n = p^k$ for any prime p. If $p^k = 4$ we have $4 = |\operatorname{Aut}\mathbb{Z}(4)|^2$ and if $p = 2$ and $k \geqslant 3$ then $|\operatorname{Aut}\mathbb{Z}(2^k)| = 2^{k-1} < 2^k < 2^{2k-2}$.

Suppose that $p \geqslant 3$. Then

$$|\operatorname{Aut}\mathbb{Z}(p^k)| = p^{k-1}(p-1) < p^k \leqslant p^{2k-2}p < p^{2k-2}(p-1)^2 = |\operatorname{Aut}\mathbb{Z}(p^k)|^2.$$ ∎

The suggested algorithm is: given the multiset $M(n)$, let N be the product of its elements. Compute $M(m)$ for all m with $N < m \leqslant N^2$ and compare it with $M(n)$.

https://doi.org/10.1017/S0004972700037308 Published online by Cambridge University Press

REMARK 3.7. The problem of finding all $n \in \mathbb{Z}^+$ such that $\mathbb{Z}(n)$ is determined by its automorphism group is related to an unresolved number theoretic conjecture of Carmichael [1], that there is no positive integer n for which $|\mathrm{Aut}\,\mathbb{Z}(n)| = |\mathrm{Aut}\,\mathbb{Z}(m)|$ implies $n = m$. Our results throw no light on Carmichael's conjecture, since we lack criteria for a unique partition of $M(n)$, which seems to involve some delicate problems of Number Theory.

Now we deal with the general case of $\mathbf{n} \in \mathbb{S}N$. Let $G = \mathbb{Z}(\mathbf{n})$. Then G determines a multiset $M(\mathbf{n})$ which has a partition into finite allowable parts, but now there may be infinitely many parts. Once again, each allowable part of such a partition determines one or two prime powers as in Lemma 3.1, but the problem of sorting out different partitions of a multiset is no easier than in the finite case.

The conditions for $\mathbb{Z}(\mathbf{n})$ to be determined by its automorphism group are the same as those in Corollary 3.3, as is the proof:

THEOREM 3.8. *Let* $\mathbf{n} = \prod_{p \in \mathbf{P}(n)} p^{n_p}$ *and let* $M = M(\mathbf{n})$. *For all* $p \in \mathbf{P}(n)$ *let* m_p *be the product of the terms in the finite set* M_p *and let* p^k *be the largest element of* M_p. *Then* $\mathbb{Z}(\mathbf{n}) \in \mathbf{A}(\mathrm{Aut})$ *if and only if* M *has a unique partition* $Q = \{M_p : p \in \mathbf{P}(n)\}$ *into allowable parts* M_p *and:*

(a) $n_2 \geqslant 2$; *and*

(b) *Whenever both* $m_p = p^k(p-1)$ *and* $m_p + 1 = q$ *is prime, then* $q \in \mathbf{P}(\mathbf{n})$ *and* M_p *and* M_q *both occur in* Q.

However, as in the finite case, the difficulty lies in the condition that M has a unique partition. Here is a putative example of an infinite group in $\mathbf{D}$ which is determined by its automorphism group.

EXAMPLE 3.9. Suppose there are infinitely many Fermat primes F_i and let $\mathbf{n} = 8\prod F_i$. Then $M(\mathbf{n})$ consists of two copies of 2, and countably many distinct powers of 2 greater than 2. Hence the only partition of $M(\mathbf{n})$ into allowable parts is $\{\{2, 2\}, \{F_i - 1\} : F_i \text{ is a Fermat prime}\}$ so $\mathbb{Z}(\mathbf{n}) \in \mathbf{D}(\mathrm{Aut})$.

Since the conjecture that there are infinitely many Fermat primes is not considered likely, here is another example based on a more reasonable conjecture.

CONJECTURE 3.10. There is an infinite sequence $\{p_i\}$ of primes such that $p_1 = 3$, $p_2 = 5$ and for all $i \geqslant 3$, $p_i = 2^i q_i + 1$, where q_i is a prime such that $q_i \neq 2^k m + 1$ for any $k < i$ and any product m of primes p_j with $j < i$.

EXAMPLE 3.11. Let $\mathbf{n} = 16 p_1 p_2 \dots$ where $\{p_i\}$ is a sequence of primes satisfying Conjecture 3.10. Let M be the multiset of $\mathbb{Z}(\mathbf{n})$. Then $M(\mathbf{n})$ has a unique partition into allowable parts, each of which determines a unique cyclic summand of prime order, namely

$$M(\mathbf{n}) = \{\{2, 4\}, \{2\}, \{4\}, \{2^i, q_i\} : i \geqslant 3\}.$$

Theorem 3.8 implies that $\mathbb{Z}(\mathbf{n}) \in \mathbf{A}(\mathrm{Aut})$.

References

[1] R.D. Carmichael, 'On Euler's ϕ-function', *Bull. Amer. Math. Soc.* **13** (1906-07), 241–243.

[2] L. Fuchs, *Infinite Abelian groups*, 2 Vols. (Academic Press, New York, London, 1970–1973).

[3] H. Leptin, 'Abelsche p-Gruppen und ihre Automorphismengruppen', *Math. Z.* **73** (1960), 235–253.

[4] W. Liebert, 'Isomorphic automorphism groups of primary Abelian groups', in *Abelian group theory*, (R. Göbel and E. A. Walker, Editors) (Gordon and Breach, 1987), **pp.** 9–31.

[5] P. Schultz, 'Automorphisms which determine an abelian p-group', in *Abelian groups, module theory and topology*, Marcel Dekker Lecture Notes in Pure and Applied Mathematics **201**, 1998, **pp.** 373–379.

Department of Mathematics and Statistics
The University of Western Australia
Nedlands W.A. 6907
Australia
e-mail: schultz@math.uwa.edu.au

Department of Mathematics
University of Conakry
Guinea-Conakry
West Africa
e-mail: amseb@mail.ru

Department of Mathematics
University of Conakry
Guinea-Conakry
West Africa
e-mail: sebeldin@gn.refer.org

https://doi.org/10.1017/S0004972700037308 Published online by Cambridge University Press