Ann. Sci. Math. Québec **36**, No 2, (2012), 559–575

THE AUTOMORPHISM GROUP OF FINITE ABELIAN p-GROUPS

ADOLF MADER

RÉSUMÉ. Les endomorphismes et les automorphismes d'un groupe abélien p-primaire fini sont concrètement représentés d'une manière efficace. L'ordre du groupe d'automorphismes est calculé et sa structure étudiée. Finalement, les sous-groupes caractéristiques sont décrits pour $p > 2$ ainsi que les sous-groupes complètement invariants pour tout p.

ABSTRACT. The endomorphisms and the automorphisms of a finite abelian p-group are presented in an efficient way. The order of the automorphism group is computed and its structure investigated. Finally the characteristic subgroups are described for $p > 2$ and the fully invariant subgroups for any p.

1. Introduction

In a recent article [HR07], the authors describe the automorphism group of an abelian group in terms of integer matrices and compute the order of the automorphism group. We use matrices whose entries are homomorphisms (they could be considered elements of the endomorphism ring) and employ much more algebra than the papers that enter deeper into the fine structure of the groups and must deal with integer matrices with entries modulo different powers p^n. In addition to computing the cardinality of the automorphism group, we describe the structure of the automorphism group of a finite abelian group. We describe all characteristic subgroups of G for $p > 2$, and show that there is an injective, but not necessarily surjective, correspondence between characteristic subgroups of G and normal subgroups of the automorphism group of G.

These results are not new but are special cases of results scattered in various papers on infinite abelian groups (see "Remarks on the Literature"). However, the proofs are new, elementary, and avoid all specialized terminology of infinite abelian group theory. The idea is that many people may need knowledge about finite abelian groups, but will never find it in specialized papers. This paper is self-contained and accessible to students with a basic knowledge of abstract algebra.

Reçu le 11 novembre 2011 et, sous forme définitive, le 20 mars 2012.

2. Background

We write our abelian groups additively. Maps on X to Y are defined by the scheme

$$f : X \ni x \mapsto f(x) \in Y,$$

thereby avoiding the tiresome phrase "where $x \in X$". The symbol ":=" stands for "by definition equals".

It is well known that every abelian torsion group is in a very canonical way the direct sum of its maximal primary subgroups, and therefore questions on torsion groups reduce to questions on primary groups. We therefore only consider finite p-groups G, where p is a fixed prime number.

Important subgroups of a group G are the fully invariant subgroups

$$G[p] := \{x \in G \mid px = 0\},$$

called *socle*, more generally

$$G[p^n] := \{x \in G \mid p^n x = 0\},$$

and

$$p^n G := \{p^n x \mid x \in G\}.$$

Observe that $G[p]$ may be considered a vector space over the prime field $\mathbb{Z}/p\mathbb{Z}$.

The following well-known lemma is fundamental.

Lemma 2.1. *Let G be an abelian group of exponent p^e. Then every element of order p^e generates a direct summand of G.*

Proof. Let $g \in G$ with $\operatorname{ord}(g) = p^e$. Let H be a subgroup of G that is maximal with respect to $H \cap \langle g \rangle = 0$. We claim that $G = \langle g \rangle \oplus H$.

We first establish an auxiliary result that also illustrates the further arguments. *Suppose that $x \in G$ and $px \in H$. Then there is $y \in H$ such that $px = py$.*

Here is the proof. If $x \in H$, then $y := x$ will do. So suppose that $x \notin H$. Then by maximality of H we have that $(\langle x \rangle + H) \cap \langle g \rangle \neq 0$. Hence there exist integers m, n and $h \in H$ such that $0 \neq mg = h + nx$ and we have $nx = mg - h$. We must have $\gcd(p, n) = 1$, or else $0 \neq mg = h + nx \in \langle g \rangle \cap H = 0$. Choose integers u, v such that $1 = un + vp^e$. Then $x = unx = umg - uh$ and it follows that $px = p(-uh)$.

We have $G \supseteq \langle g \rangle \oplus H$. To establish equality, we note that $G[p^e] = G$ and show by induction on s that $G[p^s] \subseteq \langle g \rangle \oplus H$. So suppose that $x \in G$, $x \notin H$. By maximality of H, we have integers m, n and $h \in H$ such that $0 \neq mg = h + nx$ and so $nx = mg - h$. If $\gcd(n, p) = 1$, then it follows that $x \in \langle g \rangle \oplus H$. If $x \in G[p]$, then necessarily $\gcd(n, p) = 1$ and $x \in \langle g \rangle \oplus H$. Now suppose that $\operatorname{ord}(x) = p^s > p$ and $G[p^{s-1}] \subseteq \langle g \rangle \oplus H$ by induction. Then there exist $h \in H$ and an integer m such that $px = h + mg$. From $0 = p^s x = p^{s-1} h + p^{s-1} mg$, $\langle g \rangle \cap H = 0$, and $\operatorname{ord}(g) = p^e \geq p^s$, it follows that $m = pm'$ for some integer m'. Thus $p(x - m'g) = h$ and from the auxiliary result we get that $h = py$ for some $y \in H$. This says that $p(x - m'g - h') = 0$, *i.e.*, $x - m'g - h' \in G[p] \subseteq \langle g \rangle \oplus H$, and so $x \in \langle g \rangle \oplus H$. $\square$

Remark 2.2. It is an immediate corollary of Lemma 2.1 that every finite abelian p-group is the direct sum of cyclic subgroups: just peel off summand after summand using elements of largest order. Once it is known that a p-group G (finite or infinite) is the direct sum of cyclic subgroups, it is easily seen that the number of cyclic summands of order p^s is given by the so-called *Ulm invariant* of the group

$$\dim_{\mathbb{Z}/p\mathbb{Z}} \frac{(p^{s-1}G)[p]}{(p^s G)[p]}.$$

This then proves the Basis Theorem for finite abelian p-groups.

3. Endomorphisms and automorphisms

A p-group is *homocyclic of exponent* e if it is the direct sum of cyclic subgroups all of order p^e. The *rank* of a homocyclic p-group H, denoted $\operatorname{rk} H$, is the number of cyclic summands in an indecomposable decomposition of H, *i.e.*,

$$\operatorname{rk} H = \dim_{\mathbb{Z}/p\mathbb{Z}} \frac{(p^{e-1}H)[p]}{(p^e H)[p]} = \dim_{\mathbb{Z}/p\mathbb{Z}} H[p].$$

We will frequently use that

$$H \text{ homocyclic of exponent } p^e \Longrightarrow H[p^i] = p^{e-i}H. \tag{3.1}$$

Theorem 3.2 fully describes the automorphisms of a finite abelian p-group. We precede it with a special case.

Lemma 3.1. *Let H be a finite homocyclic group of exponent p^e. Then there is an exact sequence*

$$\operatorname{Hom}(H, pH) \overset{\sigma}{\rightarrowtail} \operatorname{Aut}(H) \overset{\rho}{\twoheadrightarrow} \operatorname{Aut}(H[p]),$$

where $\sigma : \operatorname{Hom}(H, pH) \ni \phi \mapsto 1 + \phi \in \operatorname{Aut}(H)$ and ρ is the restriction map. Consequently, $|\operatorname{Aut}(H)| = |\operatorname{Hom}(H, pH)| \cdot |\operatorname{Aut}(H[p])|$. Hence,

$$|\operatorname{Hom}(H, pH)| = \left(p^{e-1}\right)^{(\operatorname{rk} H)^2} \quad \textit{and} \quad |\operatorname{Aut}(H[p])| = \prod_{i=1}^{\operatorname{rk} H} \left(p^{\operatorname{rk} H} - p^{i-1}\right).$$

Proof. Note that $H[p] = p^{e-1}H$. We will show below (see Remark 4.2) that the restriction map $\operatorname{Aut}(H) \to \operatorname{Aut}(H[p])$ is surjective. We compute its kernel. Suppose that $\alpha \in \operatorname{Aut}(H)$ and $\alpha \restriction_{H[p]} = 1$. Let $0 \neq x \in H$. Then there is $m \in \mathbb{N}$ such that $0 \neq p^m x \in H[p] = p^{e-1}H$. Then $\alpha(p^m x) = p^m x$, hence $p^m(x - \alpha(x)) = 0$, and so $(1-\alpha)(x) = x - \alpha(x) \in H[p^m] \subseteq pH$. It follows that $\phi := \alpha - 1 \in \operatorname{Hom}(H, pH)$ and $\alpha = 1 + \phi$.

Conversely, suppose that $\phi \in \operatorname{Hom}(H, pH)$. Then $\phi^e = 0$ and therefore $1 + \phi$ is invertible in $\operatorname{End}(H)$, so $\alpha := 1+\phi \in \operatorname{Aut}(H)$. It remains to show that $1+\phi \restriction_{H[p]} = 0$. Let $x \in H[p]$. Then $x \in p^{e-1}H$, say $x = p^{e-1}y$, and we get that $\alpha(x) = x + \phi(x)$ where $\phi(x) = p^{e-1}\phi(y) = 0$ because $\phi(y) \in pH$ and $p^{e-1}(pH) = 0$.

Each of the $\operatorname{rk} H$ generators of H can be mapped to any element of pH and $|pH| = (p^{e-1})^{\operatorname{rk} H}$. To do the other count, recall that $H[p]$ is just a $\mathbb{Z}/p\mathbb{Z}$-vector space. Thus counting the automorphisms is equivalent to counting the non-singular matrices of size $\operatorname{rk} H \times \operatorname{rk} H$. This is done in the well-known fashion. There are $p^{\operatorname{rk} H}$ possible first rows from which the 0-row must be omitted, leaving $p^{\operatorname{rk} H} - 1$ possibilities. From the $p^{\operatorname{rk} H}$ possibilities of the second row, the linear multiples of the first row must be omitted, leaving $p^{\operatorname{rk} H} - p$ possibilities, and so on. □

We can now offer the main result of this section.

Theorem 3.2. *Let $G = G_1 \oplus G_2 \oplus \cdots \oplus G_e$ be a finite abelian p-group such that $G_i = 0$ or G_i is homocyclic of exponent p^i.*

(1) *Every endomorphism of G can be identified with a matrix*

$$U = \begin{bmatrix} u_{11} & u_{21} & \cdots & u_{e1} \\ u_{12} & u_{22} & \cdots & u_{e2} \\ \vdots & \vdots & \ddots & \vdots \\ u_{1e} & u_{2e} & \cdots & u_{ee} \end{bmatrix},$$

where $u_{ij} \in \operatorname{Hom}(G_i, G_j)$. The action is given by

$$U\, x^{\downharpoonleft} = \begin{bmatrix} u_{11}x_1 + u_{21}x_2 + \cdots + u_{e1}x_e \\ u_{12}x_1 + u_{22}x_2 + \cdots + u_{e2}x_e \\ \vdots \\ u_{1e}x_1 + u_{2e}x_2 + \cdots + u_{ee}x_e \end{bmatrix},$$

where $x^{\downharpoonleft} = [x_1, \ldots, x_e]^{tr}$ for $x_i \in G_i$. This action can be interpreted as matrix multiplication and the composite of two endomorphisms is the product matrix.

(2) *The endomorphism $U = [u_{ij}]$ is an automorphism if and only if we have that $u_{ii} \in \operatorname{Hom}(G_i, G_i)$ is an automorphism for all i.*

(3) *We have*

$$|\operatorname{Aut}(G)| = \left(\prod_{(i,j):\, i>j} \left(p^j\right)^{2(\operatorname{rk} G_i)(\operatorname{rk} G_j)} \right) \prod_{G_i \neq 0} \left(\left(p^{i-1}\right)^{(\operatorname{rk} G_i)^2} \prod_{j=1}^{\operatorname{rk} G_i} \left(p^{\operatorname{rk} G_i} - p^{j-1}\right) \right).$$

Note that the notation u_{ij} is so chosen that the first index indicates the domain G_i of the homomorphism and the second index the codomain G_j. Also by preceding the u_{ij} by the projection onto G_i and following it by the insertion of G_j, matrix U could be turned into a matrix with entries in $\operatorname{End}(G)$.

Proof. (1) This is a standard fact resulting from the isomorphism

$$\operatorname{Hom}(G, G) \cong \bigoplus_{i,j} \operatorname{Hom}(G_i, G_j).$$

(2) Consider the restriction map

$$^{-} : \operatorname{End}(G) \to \operatorname{End}(G[p]).$$

It is clear that $\overline{\operatorname{Aut}(G)} \subseteq \operatorname{Aut}(G[p])$. Suppose that $U \in \operatorname{End}(G)$, $\overline{U} \in \operatorname{Aut}(G[p])$, and, by way of contradiction, assume that $0 \neq x \in G$ such that $U(x) = 0$. Then there exists an m such that $0 \neq p^m x \in G[p]$. Then

$$\overline{U}(p^m x) = U(p^m x) = p^m U(x) = 0,$$

contradicting the fact that $\overline{U}$ is injective. So U is injective, and therefore bijective because G is finite. We have $\overline{U} = [\overline{u_{ij}}]$. We have shown that

$$U \in \operatorname{End}(G) \text{ is an automorphism if and only if } \overline{U} \text{ is an automorphism.} \tag{3.2}$$

Suppose that $i > j$ and $x \in G_i[p]$. Then $x = p^{i-1}x'$ for some $x' \in G_i$, and

$$\overline{u_{ij}}(x) = \overline{u_{ij}}(p^{i-1}x') = u_{ij}(p^{i-1}x') = p^{i-1}u_{ij}(x') = 0$$

because $i - 1 \geq j$ and $p^j G_j = 0$. We therefore have

$$\overline{U} = \begin{bmatrix} \overline{u_{11}} & 0 & \cdots & 0 \\ \overline{u_{12}} & \overline{u_{22}} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \overline{u_{1e}} & \overline{u_{2e}} & \cdots & \overline{u_{ee}} \end{bmatrix}.$$

Suppose first that $\overline{U}$ is an automorphism of $G[p]$. By a routine computation, it is found that the inverse $V = [v_{ij}]$ of $\overline{U}$ must also be lower triangular:

$$V = \begin{bmatrix} v_{11} & 0 & \cdots & 0 \\ v_{12} & v_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ v_{1e} & v_{2e} & \cdots & v_{ee} \end{bmatrix}.$$

It now follows from $\overline{U}V = I_e$ that $\overline{u_{ii}}v_{ii} = 1$ for $i = 1, \dots, e$, showing that $\overline{u_{ii}}$ is invertible.

Conversely, assume that $(\overline{u_{ii}})^{-1}$ exists for every i. Then the product matrix $\operatorname{diag}\left((\overline{u_{11}})^{-1}, \dots, (\overline{u_{ee}})^{-1}\right)\overline{U}$ is a subdiagonal matrix with 1 along the diagonal. So

$$V := \operatorname{diag}\left((\overline{u_{11}})^{-1}, \dots, (\overline{u_{ee}})^{-1}\right)\overline{U} - I_e$$

is a subdiagonal matrix with 0 on the diagonal and therefore it is nilpotent, say $V^n = 0$. Then

$$(I_e + V)(I_e + (-V) + (-V)^2 + \cdots + (-V)^{n-1}) = I_e.$$

Thus $I_e + V = \operatorname{diag}\left((\overline{u_{11}})^{-1}, \dots, (\overline{u_{ee}})^{-1}\right)\overline{U}$ is invertible and hence so is $\overline{U}$. Finally, by (3.2) applied with $G = G_i$, we have that u_{ii} is an automorphism if and only if $\overline{u_{ii}}$ is an automorphism.

(3) The matrix representation of the automorphisms of G and (2) tell us that

$$|\operatorname{Aut}(G)| = \left(\prod_{(i,j)\colon i \neq j} |\operatorname{Hom}(G_i, G_j)|\right)\left(\prod_{i=1}^{e} |\operatorname{Aut}(G_i)|\right).$$

Suppose that $i < j$. Then $p^i G_i = 0$, so $u_{ij}(G_i) \subseteq G_j[p^i] = p^{j-i}G_j$. Thus $\operatorname{Hom}(G_i, G_j) = \operatorname{Hom}(G_i, p^{j-i}G_j)$ and

$$|\operatorname{Hom}(G_i, G_j)| = |p^{j-i}G_j|^{\operatorname{rk} G_i} = (p^i)^{(\operatorname{rk}(G_j)(\operatorname{rk} G_i)}. \tag{3.3}$$

Suppose that $i > j$. Then $p^j G_j = 0$, hence $p^j G_i \subseteq \operatorname{Ker} u_{ij}$. Thus

$$\operatorname{Hom}(G_i, G_j) = \operatorname{Hom}(G_i/p^j G_i, G_j)$$

and

$$|\operatorname{Hom}(G_i, G_j)| = |G_j|^{\operatorname{rk} G_i} = (p^j)^{(\operatorname{rk} G_j)(\operatorname{rk} G_i)}. \tag{3.4}$$

For $i \neq j$, we know $|\operatorname{Hom}(G_i, G_j)|$ by (3.3) and (3.4) and $|\operatorname{Aut} G_i|$ for $G_i \neq 0$ is obtained from Lemma 3.1. We obtain the final formula by observing the bijective correspondence $(i, j) \leftrightarrow (j, i)$ for $i \neq j$, for which we get the same value $(p^m)^{(\operatorname{rk} G_i)(\operatorname{rk} G_j)}$ in (3.3) and (3.4), where m is the larger of i and j. □

4. Dissecting $\operatorname{Aut}(G)$

In this section we will exhibit a chain of normal subgroups of $\operatorname{Aut}(G)$ and precisely describe the quotients of consecutive normal subgroups.

Lemma 4.1. *Let G be a finite p-group. Then every endomorphism of pG extends to an endomorphism of G, and every automorphism of pG extends to an automorphism of G.*

Proof. Write $G = G_1 \oplus H$ such that $pG_1 = 0$ and $H[p] \subseteq pH$. This can be done by starting with a direct decomposition of G with cyclic summands, collecting the summands of order p to form G_1, and combining the other summands to form H. Let $H = \langle h_1 \rangle \oplus \cdots \oplus \langle h_n \rangle$. Then

$$\forall\, i \in \{1, \ldots, n\}, \operatorname{ord}(h_i) = p \operatorname{ord}(ph_i).$$

Let $\xi \in \operatorname{End}(pH)$. Then

$$\xi(ph_i) = \sum_{j=1}^{n} pm_{ij} h_j,$$

with $\operatorname{ord}(ph_i) \sum_{j=1}^{n} pm_{ij} h_j = 0$. We define $\eta \in \operatorname{End}(G)$ by letting η be the identity on G_1 and setting $\eta(h_i) := \sum_{j=1}^{n} m_{ij} h_j$. This is a well-defined endomorphism because

$$\operatorname{ord}(h_i) \sum_{j=1}^{n} m_{ij} h_j = \operatorname{ord}(ph_i) \sum_{j=1}^{n} pm_{ij} h_j = 0.$$

If ξ is an automorphism of $pG = pH$, then ξ is injective on $H[p] \subseteq pH$, η is injective on $G_1 \oplus H[p] = G[p]$, and hence is an automorphism of G. □

Remark 4.2. Lemma 4.1 says that the restriction maps

$$\operatorname{End}(G) \to \operatorname{End}(pG) \quad \text{and} \quad \operatorname{Aut}(G) \to \operatorname{Aut}(pG)$$

are surjective. If we apply these maps repeatedly, it follows that the restriction maps

$$\operatorname{End}(G) \to \operatorname{End}(p^n G) \quad \text{and} \quad \operatorname{Aut}(G) \to \operatorname{Aut}(p^n G)$$

are also surjective.

Proposition 4.3. *Let G be a finite abelian p-group. There is a short exact sequence*

$$\operatorname{Aut}_{pG} G \overset{\iota}{\rightarrowtail} \operatorname{Aut}(G) \overset{\rho}{\twoheadrightarrow} \operatorname{Aut}(pG)$$

where ι is insertion, ρ is the restriction map, and

$$\operatorname{Aut}_{pG}(G) := \{\alpha \in \operatorname{Aut}(G) \mid \alpha \restriction_{pG} = 1\}.$$

Proof. By Lemma 4.1 the restriction map ρ is surjective and clearly

$$\operatorname{Ker}(\rho) = \operatorname{Aut}_{pG}(G). \qquad \square$$

We will now investigate $\operatorname{Aut}_{pG}(G)$ more closely.

Lemma 4.4. *Let $\varphi : G \to G/pG$ be the natural epimorphism. There is an exact sequence*

$$\operatorname{Hom}(G/pG, pG) \overset{\sigma}{\rightarrowtail} \operatorname{Aut}_{pG}(G) \overset{-}{\to} \operatorname{Aut}(G/pG)$$

where $\sigma :\ \operatorname{Hom}(G/pG, pG) \ni \xi \mapsto 1 + \xi\varphi \in \operatorname{Aut}_{pG}(G)$ *and*

$$^{-} :\ \operatorname{Aut}_{pG}(G) \ni \alpha \mapsto \overline{\alpha} \in \operatorname{Aut}(G/pG)$$

is given by $\varphi\alpha = \overline{\alpha}\varphi$.

Proof. Let $\xi \in \operatorname{Hom}(G/pG, pG)$. Then $(1 + \xi\varphi)(1 - \xi\varphi) = 1$ and

$$(1 + \xi\varphi)(px) = px$$

for every $x \in G$. So $\operatorname{Hom}(G/pG, pG)$ maps into $\operatorname{Aut}_{pG}(G)$ and

$$\{1 + \xi\varphi \mid \xi \in \operatorname{Hom}(G/pG, pG)\} \subseteq \operatorname{Ker}(^{-}).$$

Suppose that $\alpha \in \operatorname{Aut}_{pG}(G)$ and $\overline{\alpha} = 1$. Then $\varphi\alpha = \varphi$ and $\varphi(\alpha - 1) = 0$. Hence $\alpha - 1 \in \operatorname{Hom}(G, pG)$ and $(1 - \alpha)(pG) = 0$. Hence $\alpha = 1 + \xi\varphi$ for some $\xi \in \operatorname{Hom}(G/pG, pG)$. $\square$

There remains the problem of determining $\operatorname{Im}(^{-})$ and the precise structure of $\operatorname{Aut}_{pG}(G)$. A special case is very simple.

Proposition 4.5. *Suppose that $G[p] \subseteq pG$ and let $\varphi : G \to G/pG$ be the natural epimorphism. Then*

$$\operatorname{Aut}_{pG}(G) = \left\{1 + \xi\varphi \,\middle|\, \xi \in \operatorname{Hom}\left(\tfrac{G}{pG}, pG\right)\right\} \cong \operatorname{Hom}\left(\tfrac{G}{pG}, pG\right).$$

Proof. We only need to check that every $\alpha \in \operatorname{Aut}_{pG}(G)$ induces the identity on G/pG. This is the case because $p(1 - \alpha)(G) = (1 - \alpha)(pG) = 0$, and so

$$(1 - \alpha)(G) \subseteq G[p] \subseteq pG. \qquad \square$$

The hypothesis of Proposition 4.5 is equivalent to saying that G has no direct summands of order p. This necessitates looking at $G = G_1 \oplus H$, where G_1 is the direct sum of all summands of order p in some decomposition of G as a direct sum of cyclic subgroups. Again, we will understand endomorphisms of G as matrices

$$\begin{bmatrix} \alpha_{11} & \alpha_{21} \\ \alpha_{12} & \alpha_{22} \end{bmatrix} \qquad \begin{cases} \alpha_{11} \in \operatorname{Hom}(G_1, G_1), & \alpha_{21} \in \operatorname{Hom}(H, G_1), \\ \alpha_{12} \in \operatorname{Hom}(G_1, H), & \alpha_{22} \in \operatorname{Hom}(H, H), \end{cases}$$

with the action ($x \in G_1$, $y \in H$)

$$\begin{bmatrix} \alpha_{11} & \alpha_{21} \\ \alpha_{12} & \alpha_{22} \end{bmatrix}(x + y) = \begin{bmatrix} \alpha_{11} & \alpha_{21} \\ \alpha_{12} & \alpha_{22} \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \alpha_{11}(x) + \alpha_{21}(y) \\ \alpha_{12}(x) + \alpha_{22}(y) \end{bmatrix}.$$

Proposition 4.6. *Write $G = G_1 \oplus H$, where $pG_1 = 0$ and $H[p] \subseteq pG$. Then $\mathrm{Aut}_{pG}(G)$ contains the subgroups*

$$\begin{aligned} A_1 &:= \left\{ \begin{bmatrix} 1 & 0 \\ \xi\varphi & 1+\xi\varphi \end{bmatrix} \middle| \xi \in \mathrm{Hom}\left(\frac{G}{pG}, pG\right) \right\}, \\ A_2 &:= \left\{ \begin{bmatrix} 1 & \xi \\ 0 & 1 \end{bmatrix} \middle| \xi \in \mathrm{Hom}(H, G_1) \right\}, \\ A_3 &:= \left\{ \begin{bmatrix} \alpha_{11} & 0 \\ 0 & 1 \end{bmatrix} \middle| \alpha_{11} \in \mathrm{Aut}(G_1) \right\}. \end{aligned}$$

(1) $A_1 = \mathrm{Ker}(^-)$ *and* $\mathrm{Hom}\left(\frac{G}{pG}, pG\right) \ni \xi \mapsto 1 + \xi\varphi = \begin{bmatrix} 1 & 0 \\ \xi\varphi & 1+\xi\varphi \end{bmatrix} \in A_1$ *is an isomorphism.*

(2) $\mathrm{Hom}(H, G_1) \ni \xi \mapsto \begin{bmatrix} 1 & \xi \\ 0 & 1 \end{bmatrix} \in A_2$ *is an isomorphism.*

(3) $\mathrm{Aut}(G_1) \ni \alpha_{11} \mapsto \begin{bmatrix} \alpha_{11} & 0 \\ 0 & 1 \end{bmatrix} \in A_3$ *is an isomorphism.*

(4) *The group $\mathrm{Aut}_{pG}(G)$ is the iterated semi-direct product of the groups A_i, i.e., $\mathrm{Aut}_{pG}(G) = (A_1 \rtimes A_2) \rtimes A_3$.*

Proof. (1) We must write $1 + \xi\varphi$ in terms of its components $G_1 \to G_1$, $H \to G_1$, $G_1 \to H$, and $H \to H$. Let $x \in G_1$. Then $(1 + \xi\varphi)(x) = x + \xi\varphi(x)$, where $\xi\varphi(x) \in H$. This shows that the entry in position $(1, 1)$ in the matrix representation of $1 + \xi\varphi$ must be 1. It also shows that the entry in position $(2, 1)$ must be $\xi\varphi$. Now let $x \in H$. Then $(1 + \xi\varphi)(x) = x + \xi\varphi(x) \in H$, hence the component in G_1 is 0 which shows that the entry in position $(1, 2)$ of the matrix must be 0, and the entry in position $(2, 2)$ must be $1 + \xi\varphi$. This proves (1) because it is already known that $\xi \mapsto 1 + \xi\varphi$ is an isomorphism.

(2) and (3). It is readily seen that the A_2, A_3 are subgroups of $\mathrm{Aut}_{pG}(G)$ and isomorphic to $\mathrm{Hom}(H, G_1)$ and $\mathrm{Aut}(G_1)$ respectively.

(4) We remark that $A_1 = \mathrm{Ker}(^-)$ is normal in $\mathrm{Aut}_{pG}(G)$, A_3 normalizes A_2, and $A_1 \cap A_2 = \{1\}$. The elements of A_1A_2 are matrices of the form $\begin{bmatrix} 1 & \alpha_{21} \\ \alpha_{12} & \alpha_{22} \end{bmatrix}$, where $\alpha_{21} \in \mathrm{Hom}(H, G_1) = \mathrm{Hom}(H/pH, G_1)$, $\alpha_{12} \in \mathrm{Hom}(G_1, H) = \mathrm{Hom}(G_1, H[p])$, and $\alpha_{22} \in \mathrm{Aut}_{pH} H$. Hence $A_3 \cap (A_1A_2) = \{1\}$. This establishes that $\mathrm{Aut}_{pG}(G)$ contains the subgroup $(A_1 \rtimes A_2) \rtimes A_3)$. It remains to show that the iterated semi-direct product $(A_1 \rtimes A_2) \rtimes A_3$ exhausts $\mathrm{Aut}_{pG}(G)$.

Let $\alpha = \begin{bmatrix} \alpha_{11} & \alpha_{21} \\ \alpha_{12} & \alpha_{22} \end{bmatrix} \in \mathrm{Aut}_{pG}(G)$. We show first that $\alpha_{11} \in \mathrm{Aut}(G_1)$. Let $x \in G_1$. Then

$$\alpha(x) = \begin{bmatrix} \alpha_{11} & \alpha_{21} \\ \alpha_{12} & \alpha_{22} \end{bmatrix} \begin{bmatrix} x \\ 0 \end{bmatrix} = \begin{bmatrix} \alpha_{11}x \\ \alpha_{12}x \end{bmatrix}, \text{ where } \alpha_{12}x \in H[p] \subseteq pH = pG.$$

Therefore $\alpha^{-1}(\alpha_{12}x) = \alpha_{12}(x)$. Suppose that $\alpha_{11}(x) = 0$. Then $\alpha(x) = \alpha_{12}(x)$, and hence $\alpha^{-1}(\alpha_{12}x) = x$. We now have that $\alpha_{12}(x) = \alpha^{-1}(\alpha_{12}x) = x \in G_1 \cap H = 0$,

α_{11} is injective, and hence an automorphism of G_1. We compute that

$$\begin{bmatrix} \alpha_{11} & \alpha_{21} \\ \alpha_{12} & \alpha_{22} \end{bmatrix} \begin{bmatrix} \alpha_{11}^{-1} & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \alpha_{21} \\ \alpha_{12}\alpha_{11}^{-1} & \alpha_{22} \end{bmatrix} \in \mathrm{Aut}_{pG}(G).$$

Hence it suffices to show that $\alpha \in A_1A_2A_3$ when $\alpha_{11} = 1$. We find further that

$$\begin{bmatrix} 1 & \alpha_{21} \\ \alpha_{12} & \alpha_{22} \end{bmatrix} \begin{bmatrix} 1 & -\alpha_{21} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \alpha_{12} & \alpha_{22} - \alpha_{12}\alpha_{21} \end{bmatrix} \in \mathrm{Aut}_{pG}(G).$$

Hence it suffices to show that $\alpha \in A_1A_2A_3$ when $\alpha_{21} = 0$ and $\alpha_{11} = 1$. We claim that

$$\begin{bmatrix} 1 & 0 \\ \alpha_{12} & \alpha_{22} \end{bmatrix} \in \mathrm{Aut}_{pG}(G) \quad \Longrightarrow \quad \begin{bmatrix} 1 & 0 \\ \alpha_{12} & \alpha_{22} \end{bmatrix} \in \mathrm{Ker}(^-) = A_1.$$

In fact,

$$\begin{bmatrix} 1 & 0 \\ \alpha_{12} & \alpha_{22} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ \alpha_{12}(x) + \alpha_{22}(y) \end{bmatrix}.$$

Here, $\alpha_{12}(x) \in H[p] \subseteq pH = pG$ and $\alpha_{22} \in \mathrm{Aut}_{pH}(H)$, hence

$$\alpha_{22}(y) + pG = y + pG$$

by Proposition 4.5. This says that $\overline{\alpha}\phi(x + y) = \varphi\alpha(x + y) = \varphi(x + y)$, so $\overline{\alpha} = 1_{G/pG}$. $\square$

Remark 4.7. Corresponding to the ascending chain of fully invariant subgroups

$$p^eG = \{0\} \subseteq p^{e-1}G \subseteq \cdots \subseteq p^nG \subseteq p^{n-1}G \subseteq \cdots \subseteq pG \subseteq p^0G = G,$$

there is a descending chain of normal subgroups of $\mathrm{Aut}(G)$ given by

$$\begin{aligned} \mathrm{Aut}(G) = {}&\mathrm{Aut}_{p^eG}(G) \supseteq \mathrm{Aut}_{p^{e-1}G}(G) \supseteq \mathrm{Aut}_{p^{e-2}G}(G) \supseteq \cdots \supseteq \mathrm{Aut}_{p^{n+1}G}(G) \\ &\supseteq \mathrm{Aut}_{p^nG}(G) \supseteq \cdots \supseteq \mathrm{Aut}_{pG}(G) \supseteq \mathrm{Aut}_G(G) = \{1\}. \end{aligned}$$

For every n there is a short exact sequence

$$\mathrm{Aut}_{p^nG}(G) \rightarrowtail \mathrm{Aut}_{p^{n+1}G}(G) \twoheadrightarrow \mathrm{Aut}_{p^{n+1}G}(p^nG).$$

From Proposition 4.6, we obtain the structure of

$$\frac{\mathrm{Aut}_{p^{n+1}G}(G)}{\mathrm{Aut}_{p^nG}(G)} \cong \mathrm{Aut}_{p^{n+1}G}(p^nG)$$

as an iterated semi-direct product of three groups.

With this result the cardinality of $\mathrm{Aut}(G)$ can be obtained by induction.

5. Characteristic and fully invariant subgroups

Recall that a *characteristic* subgroup of a group is one that is mapped onto itself by every automorphism of the group, while a *fully invariant subgroup* is one that is mapped into itself by every endomorphism. Thus fully invariant subgroups are characteristic. We will show that for finite abelian p-groups with $p \geq 3$, the characteristic subgroups are necessarily fully invariant. This is achieved by showing that every endomorphism is a sum of automorphisms.

Proposition 5.1. *Let $p \geq 3$ and G be a finite abelian p-group. Then every endomorphism of G is a sum of automorphisms of G.*

Proof. We use the fact that multiplication by 2 is an automorphism in any p-group with $p > 2$. So 2^{-1} makes sense and $2 \circ 2^{-1} = 1$.

(a) Suppose first that G is elementary, *i.e.*, a vector space over $\mathbb{Z}/p\mathbb{Z}$. Let $U \in \mathrm{End}(G)$. Then $G = \mathrm{Ker}(U) \oplus H$ for some H. For $i \in \{1, 2\}$ define $U_i \in \mathrm{Aut}(G)$ by stipulating that $U_1 = 1$ on $\mathrm{Ker}(U)$ and $U_1 = 2^{-1}U$ on H, while $U_2 = -1$ on $\mathrm{Ker}(U)$ and $U_2 = 2^{-1}U$ on H. Clearly the U_i's are injective and hence automorphisms. For $x \in \mathrm{Ker}(U)$ and $y \in H$, it follows that

$$\begin{aligned}(U_1 + U_2)(x + y) &= U_1(x) + U_2(x) + U_1(y) + U_2(y)\\ &= x - x + 2^{-1}U(y) + 2^{-1}U(y)\\ &= U(y)\\ &= U(x + y).\end{aligned}$$

Thus $U = U_1 + U_2$.

(b) Suppose next that G is homocyclic of exponent p^e. Let $\varphi \in \mathrm{Hom}(G, G/p^{e-1}G)$ be the natural epimorphism. Then we have a short exact sequence

$$\mathrm{Hom}(G/p^{e-1}G, G) \rightarrowtail \mathrm{End}(G) \twoheadrightarrow \mathrm{End}(G[p])$$

with maps $\mathrm{Hom}(G/p^{e-1}G, G) \ni \xi \mapsto \xi\varphi \in \mathrm{End}(G)$ and $\mathrm{End}(G) \to \mathrm{End}(G[p])$ being the restriction map. The restriction map is surjective by Remark 4.2 because $G[p] = p^{e-1}G$. A map $\alpha \in \mathrm{End}(G)$ is the 0-map on $G[p] = p^{e-1}G$ if and only if $\alpha(p^{e-1}G) = 0$ and this is equivalent to the existence of $\xi \in \mathrm{Hom}(G/p^{e-1}G, G)$ such that $\alpha = \xi\varphi$. The exactness of the sequence is now established.

Let $U \in \mathrm{End}(G)$ and let $U[p]$ be its restriction to $G[p]$. By (a) there exist automorphisms U_1 and U_2 of $G[p]$ such that $U[p] = U_1 + U_2$. By Lemma 4.1 there exist automorphisms V_i of G such that $V_i[p] = U_i$. We find that

$$(U - V_1 - V_2)[p] = U[p] - V_1[p] - V_2[p] = 0,$$

and therefore $U = V_1 + V_2 + \xi\varphi$ for some $\xi \in \mathrm{Hom}(G/p^{e-1}G, G)$. Now

$$(V_2 + \xi\varphi)[p] = V_2[p] = U_2$$

is injective on $G[p]$, and therefore $V_2 + \xi\varphi$ is also injective on G and hence an automorphism. Thus U is the sum of the automorphisms V_1 and $V_2 + \xi\varphi$.

(c) In the general case, we identify an endomorphism with a matrix $[u_{ij}]$ as in Theorem 3.2. By (b) every diagonal map u_{ii} is the sum of two automorphisms: $u_{ii} = v_{i1} + v_{i2}$. Our proof consists of a partial but fully convincing example:

$$\begin{aligned}\begin{bmatrix} u_{11} & u_{21} & u_{31}\\ u_{12} & u_{22} & u_{32}\\ u_{13} & u_{23} & u_{33}\end{bmatrix} &= \begin{bmatrix} v_{11} & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix} + \begin{bmatrix} v_{12} & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & -1\end{bmatrix}\\ &\quad + \begin{bmatrix} 1 & 2^{-1}u_{12} & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix} + \begin{bmatrix} -1 & 2^{-1}u_{12} & 0\\ 0 & -1 & 0\\ 0 & 0 & -1\end{bmatrix} + \cdots \quad \square\end{aligned}$$

Corollary 5.2. *In a finite abelian p-group with $p > 2$, the characteristic subgroups are fully invariant.*

In 2-groups there exist characteristic subgroups that are not fully invariant and hence there are endomorphisms that are not sums of automorphisms. A general result to this effect is [Kap69, Theorem 27]. A simple example is the following.

Example 5.3. Let $G = \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus \langle a_3 \rangle$ with $\operatorname{ord}(a_i) = p^i$, and let

$$H = \langle x \in G \mid x \notin pG, 0 \neq px \in p^2G \rangle.$$

Then clearly H is characteristic in G. Computations reveal that the generators of H are (without loss of generality) of the form $a_1 + p\alpha a_3$ and $a_1 + p\beta a_2 + p\gamma a_3$, where α, β and γ are relatively prime to p. The projection $a_1 \mapsto a_1$, $a_2 \mapsto 0$ and $a_3 \mapsto 0$ maps H onto $\langle a_1 \rangle$. For $p \geq 3$,

$$2a_1 = (a_1 + (p^2 - 1)pa_3) + (a_1 + pa_3)$$

so $\langle a_1 \rangle \subseteq H$, but for $p = 2$, one finds that $a_1 \notin H$, and therefore H is not fully invariant.

We proceed to describe all fully invariant subgroups of finite abelian p-groups. The basic fully invariant subgroups are p^sG, $G[p^t]$ and their intersections $(p^sG)[p^t]$.

Proposition 5.4. *The fully invariant subgroups of a finite abelian p-group are exactly the subgroups of the form*

$$\sum_{i=1}^{n} (p^{s_i}G)\,[p^{t_i}] \text{ where } s_i \geq 0 \text{ and } t_i > 0.$$

Proof. Let $g \in G$. Then $\operatorname{End}(G)g$ is the smallest fully invariant subgroup containing g. Every fully invariant subgroup H can be written in the form

$$H = \sum \{\operatorname{End}(G)h \mid h \in H\},$$

and therefore it suffices to determine the single generator fully invariant subgroups $\operatorname{End}(G)g$. We utilize again a homocyclic decomposition $G = G_1 \oplus \cdots \oplus G_n$ ($G_i = 0$ allowed) and the corresponding decomposition $g = g_1 + \cdots + g_n$ where $g_i \in G_i$. Each g_i is an endomorphic image of g via projection, hence $\operatorname{End}(G)g \supseteq \sum_i \operatorname{End}(G)g_i$, but also for every $\xi \in \operatorname{End}(G)$ we have

$$\xi(g) = \sum_i \xi(g_i) \in \sum_i \operatorname{End}(G)g_i$$

and we have reduced the problem to finding $\operatorname{End}(G)g_i$ where $g_i \in G_i$.

Let $0 \neq g \in G_i$ $\operatorname{ord}(g) = p^t$. Then $g \in p^{i-t}G_i$ by (3.1) because G_i is homocyclic of exponent p^i. Set $s = i - t$. Clearly $\operatorname{End}(G)g \subseteq (p^sG)[p^t]$. To show the reverse containment, choose $g_0 \in G_i$ such that $g = p^s g_0$. Then $\operatorname{ord}(g_0) = i$. By Lemma 2.1 $\langle g_0 \rangle$ is a direct summand of G_i and hence of G. Therefore, g_0 can be mapped to any element of order $\leq p^i$ by some endomorphism of G. Let $x \in (p^sG)[p^t]$. Then $x = p^s x_0$ and $\operatorname{ord}(x_0) \leq t + s = i$. Hence there is an endomorphism ξ of G such that $\xi(g_0) = x_0$ and therefore

$$\xi(g) = \xi(p^s g_0) = p^s \xi(g_0) = p^s x_0 = x.$$

We have shown that also $(p^sG)[p^t] \subseteq \operatorname{End}(G)g$, which concludes the proof of the equality. □

The description of the fully invariant subgroups can be refined somewhat.

Corollary 5.5. *Let H be a fully invariant subgroup of G. Fix a decomposition $G = G_1 \oplus \cdots \oplus G_e$, where G_i is 0 or homocyclic of exponent p^i for $i = 1, \dots, e$. Then H has a description*

$$H = G[p^t] + (H \cap pG) = (G_1 \oplus \cdots \oplus G_t) \oplus (H \cap pG \cap G_t^*)$$

with $G_t^* = G_{t+1} \oplus \cdots \oplus G_e$, where $t = 0$ is allowed and means that

$$H = H \cap pG \cap G_t^* = H \cap pG.$$

Proof. Beginning with $H = \sum_{i=1}^{n} (p^{s_i} G)\,[p^{t_i}]$, we get

$$H = \sum \{(p^{s_i} G)[p^{t_i}] \mid s_i = 0\} + \sum \{(p^{s_i} G)[p^{t_i}] \mid s_i > 0\},$$

where $\{(p^{s_i} G)[p^{t_i}] \mid s_i = 0\} = G[p^t]$ for $t := \max\{t_i \mid s_i = 0\}$ and

$$\sum \{(p^{s_i} G)[p^{t_i}] \mid s_i > 0\} \subseteq H \cap pG.$$

Using that

$$G[p^t] = G_1 \oplus \cdots \oplus G_t \oplus pG_{t+1} \oplus \cdots \oplus p^{e-t} G_e,$$

this shows that

$$H = G[p^t] + (H \cap pG) = (G_1 \oplus \cdots G_t) + (H \cap pG).$$

Note that $H \cap pG$ is a fully invariant subgroup of G. Hence intersecting

$$G = (G_1 \oplus \cdots \oplus G_t) \oplus G_t^*$$

with $H \cap pG$, we get

$$H \cap pG = ((G_1 \oplus \cdots \oplus G_t) \cap (H \cap pG)) \oplus (H \cap pG \cap G_t^*).$$

Substituting in $H = (G_1 \oplus \cdots \oplus G_t) + (H \cap pG)$ we obtain the desired decomposition

$$H = (G_1 \oplus \cdots \oplus G_t) \oplus (H \cap pG \cap G_t^*). \qquad \square$$

6. Normal subgroups of $\mathrm{Aut}(G)$

The normal structure of $\mathrm{Aut}(G)$ has been a topic of interest since Shoda. We will study a connection between characteristic subgroups of G and normal subgroups of $\mathrm{Aut}(G)$.

Definition 6.1. Let $H \leq G$. Set

$$\mathrm{Aut}_H(G) := \{\alpha \in \mathrm{Aut}(G) \mid \forall\, x \in H : \alpha(x) = x\}.$$

Let N be a subgroup of $\mathrm{Aut}(G)$. Define $\mathrm{Fx}(N) := \{x \in G \mid N(x) = x\}$.

Lemma 6.2. *The following statements hold true.*

(1) *If H is a characteristic subgroup of G, then $\mathrm{Aut}_H(G)$ is normal in $\mathrm{Aut}(G)$.*

(2) *If N is normal in $\mathrm{Aut}(G)$, then $\mathrm{Fx}(N)$ is a characteristic subgroup of G.*

(3) *If H_1, H_2 are characteristic subgroups of G and $H_1 \leq H_2$, then*

$$\mathrm{Aut}_{H_2}(G) \subseteq \mathrm{Aut}_{H_1}(G).$$

(4) *If* N_1, N_2 *are normal subgroups of* $\mathrm{Aut}(G)$ *and* $N_1 \subseteq N_2$, *then*

$$\mathrm{Fx}(N_2) \subseteq \mathrm{Fx}(N_1).$$

(5) *Let* H *be a characteristic subgroup of* G *and let* N *be a normal subgroup of* $\mathrm{Aut}(G)$. *Then*

$$H \subseteq \mathrm{Fx}(\mathrm{Aut}_H(G)), \quad N \subseteq \mathrm{Aut}_{\mathrm{Fx}(N)} G.$$

(6) $\mathrm{Aut}_{\mathrm{Fx}(\mathrm{Aut}_H(G))}(G) = H$ *and* $\mathrm{Fx}(\mathrm{Aut}_{\mathrm{Fx}(N)}(G)) = N$.

(7) *Let* H_1 *and* H_2 *be characteristic subgroups of* G. *Then*

$$\mathrm{Aut}_{H_1+H_2}(G) = \mathrm{Aut}_{H_1}(G) \cap \mathrm{Aut}_{H_2}(G).$$

Proof. (1) Let $\alpha \in \mathrm{Aut}_H(G)$, $\beta \in \mathrm{Aut}(G)$, and $x \in H$. Then

$$(\beta^{-1}\alpha\beta)x = \beta^{-1}\alpha(\beta x) = \beta^{-1}(\beta x) = x.$$

Thus $\mathrm{Aut}_H(G)$ is normal in $\mathrm{Aut}(G)$.

(2) Let N be a normal subgroup of $\mathrm{Aut}(G)$, $\alpha \in N$, $x \in \mathrm{Fx}(N)$, and $\beta \in \mathrm{Aut}(G)$. Then $\alpha(\beta x) = \beta(\beta^{-1}\alpha\beta)(x) = \beta(x)$.

The verifications of (3) through (7) are routine consequences of the definitions. □

Example 6.3. Assume that G is p-elementary, *i.e.*, a direct sum of cyclic subgroups of order p. Then G can be considered to be a $\mathbb{Z}/p\mathbb{Z}$-vector space and $\mathrm{Aut}(G)$ acts transitively on the subset of non-zero elements. Hence there are only two characteristic subgroups, namely $\{0\}$ and G, but there are more than two normal subgroups of $\mathrm{Aut}(G)$, for example the center of $\mathrm{Aut}(G)$. The assignment $H \mapsto \mathrm{Aut}_H(G)$ on characteristic subgroups of G to normal subgroups of $\mathrm{Aut}(G)$ is injective in this case.

Example 6.3 shows that the map $N \mapsto \mathrm{Fx}(N)$ on normal subgroups of $\mathrm{Aut}(G)$ is not injective and the map $H \mapsto \mathrm{Aut}_H(G)$ on characteristic subgroups is not surjective. However, we will show that the assignment $H \mapsto \mathrm{Aut}_H(G)$ is injective.

Proposition 6.4. *Let* $p > 2$ *and let* G *be a finite abelian* p*-group. Then the assignment on characteristic subgroups* H, $H \mapsto \mathrm{Aut}_H(G)$ *is injective.*

Proof. (a) Note that "characteristic" coincides with "fully invariant" because $p > 2$. Also, given two fully invariant subgroups H and H' with $\mathrm{Aut}_H(G) = \mathrm{Aut}_{H'}(G)$, we have

$$\mathrm{Aut}_H(G) = \mathrm{Aut}_H(G) \cap \mathrm{Aut}_{H'}(G) = \mathrm{Aut}_{H+H'}(G).$$

If we can show that $H = H + H'$, then it follows that $H' \subseteq H$ and by symmetry $H = H'$. Therefore it suffices to show that $\mathrm{Aut}_H(G) \neq \mathrm{Aut}_{H'}(G)$ for fully invariant subgroups $H' < H$. Hence assume that H' and H are characteristic subgroups with $H' < H$. We claim that $\mathrm{Aut}_H(G) \neq \mathrm{Aut}_{H'}(G)$.

(b) By Example 6.3 the claim is true for an elementary p-group. We therefore can proceed by induction on the order of G.

(c) Choose a decomposition $G = G_1 \oplus \cdots \oplus G_e$ where G_i is 0 or homocyclic of exponent p^i. This decomposition will be fixed for the rest of the proof. Suppose that

$H' \subseteq H$ are characteristic subgroups of G. Then, by Corollary 5.5,

$$H' = (G_1 \oplus \cdots G_m) \oplus (H' \cap pG \cap G_m^*)$$

and

$$H = (G_1 \oplus \cdots G_n) \oplus (H \cap pG \cap G_n^*).$$

Case I: $m < n$, $G_n \neq 0$, and $n \geq 2$. In this case there is a non-zero homomorphism $\xi : G_n \twoheadrightarrow G_n/pG_n \to pG_n$ and therefore a non-identity automorphism $1 + \xi$ of G_n that leaves pG_n element-wise invariant. Let $\alpha \in \operatorname{Aut}(G)$ be the identity on $G_1 \oplus \cdots \oplus G_{n-1} \oplus G_n^*$ and equal $1 + \xi$ on G_n. Then α fixes pG element-wise and therefore H', but it moves elements of $G_n \subseteq H$.

Case II: $m < n = 1$, $G_1 \neq 0$. In this case $G = G_1 \oplus G_1^*$ and $pG = pG_1^* \subseteq pG$. As $p > 2$, there is an automorphism of G that is not the identity on G_1, but restricts to the identity on G_1^*. Since $H' \subseteq pG$, this automorphism fixes H' but not H.

Case III: $n = m$ and $G_n \neq 0$. In this case, necessarily

$$(H' \cap pG \cap G_n^*) \neq (H \cap pG \cap G_n^*)$$

and these are characteristic subgroups of G_n^*. The case is easily settled by induction.

Case IV: $n = m = 0$. In this case $H', H \subseteq pG$ and since the restriction map $\operatorname{Aut}(G) \to \operatorname{Aut}(pG)$ is surjective, the claim follows by induction. □

7. Endomorphisms and automorphisms as integral matrices

We conclude with a short characterization of the numerical description of endomorphisms and automorphisms of finite abelian groups.

Let $G = \langle g_1 \rangle \oplus \cdots \oplus \langle g_r \rangle$ be a finite abelian group,

$$\operatorname{ord}(g_i) = p^{e_i}, \quad 1 \leq e_1 \leq e_2 \leq \cdots \leq e_r.$$

In the following we will need the following diagonal matrix:

$$D := \operatorname{diag}(p^{e_1}, \ldots, p^{e_r}) := \begin{bmatrix} p^{e_1} & 0 & \cdots & 0 \\ 0 & p^{e_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & p^{e_r} \end{bmatrix}.$$

The group G is the epimorphic image of a free abelian group of column vectors $\mathbb{Z}^{\downharpoonleft} := \{[m_1, \ldots, m_r]^{\mathrm{tr}} \mid m_i \in \mathbb{Z}\}$ with basis $\{c_i \mid 1 \leq i \leq r\}$, where c_i is the column vector with 1 in position i and 0 elsewhere, that is

$$\frac{\mathbb{Z}^{\downharpoonleft}}{D\,\mathbb{Z}^{\downharpoonleft}} \cong G \quad \text{induced by} \quad c_i \mapsto g_i. \tag{7.1}$$

By $\mathbb{M}_r(\mathbb{Z})$ we denote the ring of all $r \times r$ integral matrices. A matrix $U \in \mathbb{M}_r(\mathbb{Z})$ induces an endomorphism of $\mathbb{Z}^{\downharpoonleft}$ by left multiplication.

Lemma 7.1. *A matrix $U \in \mathbb{M}_r(\mathbb{Z})$ induces an endomorphism of the quotient $\frac{\mathbb{Z}^{\downharpoonleft}}{D\,\mathbb{Z}^{\downharpoonleft}}$ if and only if there exists $V \in \mathbb{M}_r(\mathbb{Z})$ such that $UD = DV$.*

Proof. Clearly U induces an endomorphism of the quotient $\frac{\mathbb{Z}^{\downharpoonleft}}{D\,\mathbb{Z}^{\downharpoonleft}}$ if and only if $UD\,\mathbb{Z}^{\downharpoonleft} \subseteq D\,\mathbb{Z}^{\downharpoonleft}$. The columns V_{*j} of the matrix V are obtained from the equations

$$UDc_j = DV_{*j}. \qquad \square$$

By means of the isomorphism (7.1), the endomorphisms of G can also be described by matrices. As in linear algebra, the action of a matrix U on G is realized via matrix multiplication on coordinate vectors of the elements of G with respect to a given basis of G.

Theorem 7.2. *Let $G = \langle g_1 \rangle \oplus \cdots \oplus \langle g_r \rangle$ be a finite p-group.*

(1) *A matrix*

$$U = \begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1r} \\ u_{21} & u_{22} & \cdots & u_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ u_{r1} & u_{r2} & \cdots & u_{rr} \end{bmatrix} \in \mathbb{M}_r(\mathbb{Z})$$

induces an endomorphism of G given by

$$\begin{aligned} U(m_1g_1 + m_2g_2 + \cdots + m_rg_r) = (&u_{11}m_1 + u_{12}m_2 + \cdots + u_{1r}m_r)g_1 \\ &+ (u_{21}m_1 + u_{22}m_2 + \cdots + u_{2r}m_r)g_2 + \cdots \\ &+ (u_{r1}m_1 + u_{r2}m_2 + \cdots + u_{rr}m_r)g_r, \end{aligned}$$

if and only if there exists $V \in \mathbb{M}_r(\mathbb{Z})$ such that $UD = DV$.

(2) *Let $U \in \mathrm{End}(G)$. Then $U \in \mathrm{Aut}(G)$ if and only if $\gcd(p, \det U) = 1$.*

Proof. (1) This part follows from the isomorphism (7.1) and Lemma 7.1.

(2) By $U[p]$ we mean the matrix that is obtained from U by viewing the entries as elements of $\mathbb{Z}/p\mathbb{Z}$. Note that $U[p]$ is the linear transformation obtained by restricting U to $G[p]$. Also we will use that U is injective on G if and only if $U[p]$ is injective on $G[p]$.

Suppose first that $U \in \mathrm{Aut}(G)$. Then $U[p]$ is an invertible linear transformation on $G[p]$, hence has non-zero determinant which means that $\gcd(p, \det U) = 1$.

Conversely, suppose that $\gcd(p, \det U) = 1$. Then $\det(U[p]) \neq 0$ which means that $U[p]$ is an invertible linear transformation, hence injective. It follows that U is also surjective and hence invertible. $\square$

8. Remarks on the literature

There is a large literature concerning endomorphisms and automorphisms of abelian groups, mostly for infinite groups where many difficult questions arise. Perhaps the oldest paper on automorphisms is [Ran07]. Ranum treats automorphisms as matrices and so does Shoda ([Sho28], [Sho30]) who also studies chains of normal subgroups and determines the quotients similar to Remark 4.7. These results were generalized to infinite p-groups in [Fuc60] and [Mad66]. In particular, Fuchs proves a general version of Proposition 4.3. The recent paper [HR07] and the older [GG60] also approach the automorphism group of a finite abelian group via integral matrices. The compact characterization (Lemma 7.1) of those matrices that induce endomorphisms can be found in Jacobson [Jac74, Theorem 3.15]. The book [Spe45], [Spe56] contains a good description of the automorphism group of a finite abelian group that is similar to ours. The description of the fully invariant subgroups as in Proposition 5.4 is studied in detail by Shiffman [Shi40] for infinite abelian p-groups G without elements of infinite height, *i.e.*, it is assumed that $\bigcap_{n\in\mathbb{N}} p^n G = 0$. Another generalization to algebraically compact groups is in [Mad70].

A different approach to fully invariant and characteristic subgroups in terms of Ulm sequences was introduced by Kaplansky ([Kap52], [Kap54], [Kap69]), which led to a large number of papers concerned with associated questions. These papers have little impact on finite abelian groups.

The question of whether endomorphisms are sums of (two) automorphisms is treated in [Cas68], [Fre68], and [Fre69]. W. Liebert [Lie67] determined which abstract rings can be realized as endomorphism rings of a finite abelian p-group and obtains such characterizations for more general classes of groups (see, for example, [Lie68], [Lie83]). While the endomorphism rings of abelian p-groups are very special, the endomorphism rings of torsion-free abelian groups can be very general. The most admired and influential result in this direction is due to A.L.S. Corner [Cor63] with the revealing title "Every countable reduced torsion-free ring is an endomorphism ring". Baer-Kaplansky type theorems are theorems that say that groups with isomorphic endomorphism rings or automorphism groups are themselves isomorphic ([Bae43], [Kap52], [Lep60]).

REFERENCES

[Bae43] R. Baer, *Automorphism rings of primary abelian operator groups,* Ann. of Math. (2) **44** (1943), 192–227.

[Cas68] F. Castagna, *Sums of automorphisms of a primary abelian group,* Pacific J. Math. **27** (1968), 463–473.

[Cor63] A.L.S. Corner, *Every countable reduced torsion-free ring is an endomorphism ring,* Proc. London Math. Soc. (3) **13** (1963), 687–710.

[Fre68] H. Freedman, *On endomorphisms of primary abelian groups,* J. London Math. Soc. **43** (1968), 305–307.

[Fre69] H. Freedman, *On endomorphisms of primary abelian groups, II,* J. London Math. Soc. (2) **1** (1969), 630–632.

[Fuc60] L. Fuchs, *On the automorphism group of abelian p-groups,* Publ. Math. Debrecen **7** (1960), 122–129.

[GG60] M. Golasiński and D.L. Gonçalves, *On automorphisms of finite abelian p-groups,* Math. Slovaca **58** (2008), no. 4, 405–412.

[HR07] C.J. Hillar and D.L. Rhea, *Automorphisms of finite abelian groups,* Amer. Math. Monthly **114** (2007), 51–62.

[Jac74] N. Jacobson, *Basic Algebra I*, W. H. Freeman & Co., San Francisco, Calif., 1974, xvi+472 pp.

[Kap52] I. Kaplansky, *Some results on abelian groups,* Proc. Nat. Acad. Sci. U. S. A. **38** (1952), 538–540.

[Kap54] I. Kaplansky, *Infinite abelian groups*, University of Michigan Press, Ann Arbor, 1954, v+91 pp.

[Kap69] I. Kaplansky, *Infinite abelian groups*, revised edition, The University of Michigan Press, Ann Arbor, Mich., 1969, vii+95 pp.

[Lep60] H. Leptin, *Abelsche p-Gruppen und ihre Automorphismengruppen,* Math. Z **73** (1960), 235–253.

[Lie67] W. Liebert, *Charakterisierung der Endomorphismenringe endlicher abelscher Gruppen,* Arch. Math. (Basel) **18** (1967), 128–135.

[Lie68] W. Liebert, *Endomorphism rings of abelian p-groups,* 1968, Studies on Abelian Groups (Symposium, Montpellier, 1967), pp. 239–258, Springer, Berlin.

[Lie83] W. Liebert, *Endomorphism rings of abelian p-groups,* Abelian group theory (Honolulu, Hawaii, 1983), 384–399, Lectures Notes in Math., 1006, Springer, Berlin, 1983.

[Mad66] A. Mader, *On the normal structure of the automorphism group and the ideal structure of the endomorphism ring of abelian p-groups,* Publ. Math. Debrecen **13** (1966), 123–137.

[Mad70] A. Mader, *The fully invariant subgroups of algebraically compact groups,* Publ. Math. Debrecen **17** (1970), 299–306.

[Ran07] A. Ranum, *The group of classes of congruent matrices with application to the group of isomorphisms of any abelian group,* Trans. Amer. Math. Soc. **8** (1907), no. 1, 71–91.

[Shi40] M. Shiffman, *The ring of automorphisms of an abelian group,* Duke Math. J. **6** (1940), 579–597.

[Sho28] K. Shoda, *Über die Automorphismen einer endlichen Abelschen Gruppe,* Math. Ann. **100** (1928), no. 1, 674–686.

[Sho30] K. Shoda, *Über den Automorphismenring bzw. die Automorphismengruppe einer endlichen Abelschen Gruppe,* Proc. Imp. Acad. **6** (1930), no. 1, 9–11.

[Spe45] A. Speiser, *Die Theorie der Gruppen von endlicher Ordnung,* Dover Publications, New York, N.Y., 1945, x+262 pp.

[Spe56] A. Speiser, *Die Theorie der Gruppen von endlicher Ordnung,* Birkhäuser Verlag, Basel und Stuttgart, 1956, xi+271 pp.

A. Mader, 2565 McCarthy Mall, Dept. of Math., U. of Hawaii, Honolulu, HI 96822, USA.
adolf@math.hawaii.edu