Rose-Hulman Undergraduate Mathematics Journal

Volume 11
Issue 2

Article 3

On the Fixed Points of Abelian Group Automorphisms

James Checco
St. Olaf College

Rachel Darling
St. Olaf College

Stephen Longfield
St. Olaf College, iphipie@gmail.com

Katherine Wisdom
St. Olaf College

Rose-
Hulman
Undergraduate
Mathematics
Journal

On the Fixed Points of Abelian Group Automorphisms

James Checco[a] Rachel Darling[b] Stephen Longfield[c]
Katherine Wisdom[d]

Volume 11, No. 2, Fall, 2010

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
Email: mathjournal@rose-hulman.edu
http://www.rose-hulman.edu/mathjournal

[a]University of Wisconsin - Madison, jchecco@chem.wisc.edu
[b]St. Olaf College, MN, darling@stolaf.edu
[c]St. Olaf College, MN, iphipie@gmail.com
[d]St. Olaf College, MN, wisdom@stolaf.edu

Rose-Hulman Undergraduate Mathematics Journal
Volume 11, No. 2, Fall, 2010

On the Fixed Points of Abelian Group Automorphisms

James Checco Rachel Darling Stephen Longfield
Katherine Wisdom

Abstract. In this article, we present general properties of fixed-point groups of the automorphisms of finite groups. Specifically, we determine the form of fixed-point groups and partition $\mathrm{Aut}(G)$ according to the number of fixed points possessed by each automorphism. A function θ records the size of each partitioning set; we find properties for θ in general and develop formulae for θ with respect to certain classes of finite abelian groups.

Acknowledgements: The authors did this work under Professor Jill Dietz in the Directed Undergraduate Research course in the fall of 2009, and would like to thank St. Olaf College for supporting this research.

1 Introduction

An automorphism of a group G is an isomorphism whose domain and range are both G (see [3]). Thus, an automorphism of G may be seen as permuting the elements of G in a way that preserves the operation of G. The set of all automorphisms of G under function composition forms a group, called the *automorphism group* of G (denoted $\mathrm{Aut}(G)$) [3].

One may learn more about the structure of both $\mathrm{Aut}(G)$ and G by investigating the fixed points of each automorphism $\alpha \in \mathrm{Aut}(G)$. A *fixed point* of α is an element $g \in G$ for which $\alpha(g) = g$. We begin by introducing the framework through which we will view fixed points. In particular, we shall focus on the function θ that counts the number of automorphisms of G with a given number of fixed points. We then explore how fixed points of G are related to subgroups $H \leq G$ and how the fixed points of two groups A and B are related to those of $A \times B$. This theory is employed to determine formulae for θ for some classes of finite abelian groups. Some of our early results may be found elsewhere in the literature but were included for the sake of completeness.

Note 1 *We assume all groups discussed to be finite and reserve ι as the identity automorphism (which maps each element of G to itself). We denote the identity in a general group G by e.*

2 Background Material

2.1 Fixed-Point Basics

For any group G, the *fixed-point map* $F_G : \mathrm{Aut}(G) \to \mathcal{S}(G)$ is defined by $F_G(\alpha) = \{g \in G : \alpha(g) = g\}$ for each $\alpha \in \mathrm{Aut}(G)$, where $\mathcal{S}(G) = \{H : H \leq G\}$. The set $F_G(\alpha)$ is called the *fixed-point group* of α. The following theorem proves that this map and terminology make sense.

Theorem 1 *For any group G, $F_G(\alpha) \leq G$ for all $\alpha \in \mathrm{Aut}(G)$.*

PROOF: Let $\alpha \in \mathrm{Aut}(G)$ and denote $F = F_G(\alpha)$. Since α is an automorphism, $\alpha(e) = e$, so $e \in F$. Suppose $g, h \in F$. Then $\alpha(g) = g$ and $\alpha(h) = h$, so $\alpha(gh) = \alpha(g)\alpha(h) = gh$ and $\alpha(g^{-1}) = \alpha(g)^{-1} = g^{-1}$. Hence, $gh, g^{-1} \in F$ and $F \leq G$, as desired. ■

Since $F_G(\alpha) \leq G$ for all automorphisms α, it follows by Lagrange's Theorem that the order of $F_G(\alpha)$ divides the order of G. Hence, it is reasonable to collect automorphisms into subsets of $\mathrm{Aut}(G)$ based on how many fixed points each possesses (i.e., based on the order of $F_G(\alpha)$). This motivates the following relation: let $\sim$ be a binary relation defined on $\mathrm{Aut}(G)$ by $\alpha \sim \beta$ if and only if $|F_G(\alpha)| = |F_G(\beta)|$. Because integer equality is an equivalence relation, so is $\sim$. Hence, the equivalence classes induced by $\sim$ partition $\mathrm{Aut}(G)$ and motivate the following definition:

Definition 1 *Let d divide $|G|$. Then the set of d-fixers is $S_d^G = \{\alpha \in \mathrm{Aut}(G) : |F_G(\alpha)| = d\}$ and $\theta(G,d) = |S_d^G|$.*

Note 2 *Where no confusion will result, we denote $F_G(\alpha)$ by $F(\alpha)$, S_d^G by S_d, and $\theta(G,d)$ by $\theta(d)$.*

Note that each automorphism α of G is in some S_d since $|F_G(\alpha)| \mid |G|$. Thus, $\alpha \in S_d$ if and only if $S_d = [\alpha]$, the equivalence class of α under $\sim$. Hence, the collection of nonempty S_d partition $\mathrm{Aut}(G)$ based on the number of fixed points of each automorphism. It follows that $|\mathrm{Aut}(G)| = \sum_{d||G|} \theta(G,d)$.

We conclude with basic facts about fixed-point groups.

Lemma 1 *Let G be a group and $\alpha \in \mathrm{Aut}(G)$. Then we have the following:*

- $F_G(\alpha) = F_G(\alpha^{-1})$
- *$F_G(\alpha) = G$ if and only $\alpha = \iota$, so $S_{|G|} = \{\iota\}$ and $\theta(G,|G|) = 1$*
- *Fix $a \in G$ and let $\sigma_a : g \mapsto aga^{-1}$ for all $g \in G$. Then $F_G(\sigma_a) = C(a)$, the centralizer of a in G.*

Proof: Let G be a group and $\alpha \in \mathrm{Aut}(G)$. If $g \in F_G(\alpha)$, $\alpha(g) = g$, so $\alpha^{-1}(g) = g$ and $g \in F_G(\alpha^{-1})$. Since $(\alpha^{-1})^{-1} = \alpha$, it follows that $F_G(\alpha) = F_G(\alpha^{-1})$. Moreover, $F_G(\alpha) = G$ if and only if α fixes all $g \in G$, so by definition $\alpha = \iota$. Thus, $S_G = \{\iota\}$ and $\theta(G,|G|) = 1$. If σ_a is defined as above, $F_G(\sigma_a) = \{g \in G : aga^{-1} = g\} = \{g \in G : ag = ga\} = C(a)$ by definition. ■

While we shall focus on fixed points, there is one interesting relationship between θ and a related concept, the orbit number. For our purposes, the *orbit* of $g \in G$ is the set of all elements of G to which g is mapped by the automorphisms of G. It turns out that the orbits form a partition of G [3], so the *orbit number* N of G is the number of orbits that partition G.

Theorem 2 *For any group G,*

$$N = \frac{1}{|\mathrm{Aut}(G)|} \sum_{d \mid |G|} \theta(G,d)d \tag{1}$$

Proof: One of Bernside's Lemmas [3] states

$$N = \frac{1}{|\mathrm{Aut}(G)|} \sum_{\alpha \in \mathrm{Aut}(G)} |F_G(\alpha)|$$

Note that for each $d \mid |G|$, there will be $\theta(G,d)$ fixed-point groups of order d, and the result follows. ■

2.2 Coprime Integers

Much of this paper is concerned with counting fixed points and automorphisms, so number theory comes into play. In particular, we shall use the Euler totient function φ, which, for each $n \in \mathbb{N}$, counts the number of positive integers less than and coprime to n. Conveniently, there is a formula for computing φ.

Fact 1 *[1] If $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ is the prime factorization of n (for $p_1, \ldots, p_t$ distinct primes and $k_1, \ldots, k_t \in \mathbb{Z}^+$), then*

$$\varphi(n) = n \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right) \tag{2}$$

Note 3 *We reserve φ for the Euler totient function.*

We also define $\varphi(1) = 1$. Note that if n is itself a prime power p^k, then (2) simplifies to $\varphi(p^k) = p^k - p^{k-1}$. The coprime numbers counted by φ shall play an integral role in our study of fixed points. In particular, we shall exploit the following fact frequently.

Fact 2 *[1] If $\gcd(m, n) = 1$ and if $d \mid (mn)$, there exist unique $d_1 \mid m$ and $d_2 \mid n$ for which $d_1 d_2 = d$. In fact, $d_1 = \gcd(m, d)$ and $d_2 = \gcd(n, d)$.*

2.3 Direct Products

As aforementioned, a question we shall explore is how the fixed points of automorphisms $\alpha \in \mathrm{Aut}(A)$ and $\beta \in \mathrm{Aut}(B)$ relate to those of an automorphism of $A \times B$. To facilitate this discussion, we review this group product.

Given two sets A and B, we may create a new set $A \times B$, the Cartesian product of A and B, defined by $A \times B = \{(a, b) : a \in A, b \in B\}$. If in fact A and B are groups, we may use their structure to define such a structure on $A \times B$. The most natural way to do this is componentwise: $(a, b)(a', b') = (aa', bb')$ for all $a, a' \in A$ and $b, b' \in B$. If this structure is imposed on $A \times B$, we call $A \times B$ the *direct product* of A and B, a group with identity (e_A, e_B) and inverses $(a, b)^{-1} = (a^{-1}, b^{-1})$.

3 General Theory of Fixed Points

In this section, we investigate the properties of fixed points of groups which are related to each other. Many of the ideas explored here play major roles in our later study of specific classes of groups.

3.1 Isomorphic Groups

As may be suspected, fixed points are preserved under isomorphism.

Theorem 3 *If $G \cong H$, then $\mathrm{Aut}(G) \cong \mathrm{Aut}(H)$ and $\theta(G,d) = \theta(H,d)$ for all $d \mid |G|$.*

Proof: Let G, H be finite groups and $\sigma : G \to H$ be an isomorphism. Define $f : \mathrm{Aut}(G) \to \mathrm{Aut}(H)$ by $f(\alpha) = \sigma\alpha\sigma^{-1}$ for all $\alpha \in \mathrm{Aut}(G)$. Since α and σ are isomorphisms, then $\sigma\alpha\sigma^{-1} : H \to H$ is an isomorphism and hence an automorphism. Similarly, f is onto, for if $\beta \in \mathrm{Aut}(H)$, then $\sigma^{-1}\beta\sigma : G \to G$ is an automorphism, and $f(\sigma^{-1}\beta\sigma) = \beta$. Additionally, suppose $f(\alpha) = f(\alpha')$ for some $\alpha, \alpha' \in \mathrm{Aut}(G)$. Then $\sigma\alpha\sigma^{-1} = \sigma\alpha'\sigma^{-1}$, so $\alpha = \alpha'$ since σ is bijective. Finally, let $\alpha, \alpha' \in \mathrm{Aut}(G)$. Then $f(\alpha\alpha') = \sigma\alpha\alpha'\sigma^{-1} = \sigma\alpha\sigma^{-1}\sigma\alpha'\sigma^{-1} = f(\alpha)f(\alpha')$, so f is a homomorphism. Therefore, $\mathrm{Aut}(G) \cong \mathrm{Aut}(H)$.

Let $d \mid |G|$ and $\alpha \in \mathrm{Aut}(G)$. We show now that $F_G(\alpha) \cong F_H(f(\alpha))$. Consider $\sigma|_{F_G(\alpha)} = \bar{\sigma} : F_G(\alpha) \to F_H(f(\alpha))$. Now, $\bar{\sigma}$ is well-defined, for if $g \in F_G(\alpha)$, then $f(\alpha)(\sigma(g)) = (\sigma\alpha\sigma^{-1}\sigma)(g) = (\sigma\alpha)(g) = \sigma(g)$, so $\sigma(g) \in F_H(f(\alpha))$. Moreover, $\bar{\sigma}$ is a one-to-one homomorphism, so it remains to show that $\bar{\sigma}$ is onto. If $\sigma(g) \in F_H(f(\alpha))$, then $f(\alpha)(\sigma(g)) = (\sigma\alpha\sigma^{-1}\sigma)(g) = \sigma(\alpha(g)) = \sigma(g)$, so since σ is one-to-one, $\alpha(g) = g$, and $g \in F_G(\alpha)$. Therefore, $\bar{\sigma}$ is an isomorphism. Since σ is bijective, $\alpha \in S_d^G$ if and only if $f(\alpha) \in S_d^H$, and since f is bijective, $\theta(G,d) = \theta(H,d)$, as desired. ■

We make note of a few facts present in the above proof:

Corollary 1 *If σ, f are as defined in the proof of Theorem 3, then $F_G(\alpha) \cong F_H(f(\alpha))$ for all $\alpha \in \mathrm{Aut}(G)$ and $f(S_d^G) = S_d^H$.*

While the converse of Theorem 3 need not be true, there is a partial converse:

Theorem 4 *If for two groups G_1 and G_2, $\theta(G_1,d) = \theta(G_2,d)$ for all $d \in \mathbb{Z}$, then $|G_1| = |G_2|$ and $|\mathrm{Aut}(G_1)| = |\mathrm{Aut}(G_2)|$, but it need not be that $G_1 \cong G_2$.*

Proof: Suppose that for two groups G_1 and G_2, $\theta(G_1,d) = \theta(G_2,d)$ for all $d \in \mathbb{Z}$, and assume $|G_1| > |G_2|$. Then $\theta(G_1, |G_1|) = 1$ but $\theta(G_2, |G_1|) = 0$, a contradiction, so $|G_1| = |G_2|$. Moreover, $|\mathrm{Aut}(G_1)| = \sum_{d \mid |G_1|} \theta(G_1,d) = \sum_{d \mid |G_2|} \theta(G_2,d) = |\mathrm{Aut}(G_2)|$. However, as the reader can verify, for the groups $\mathbb{Z}_2 \times \mathbb{Z}_4$ and D_8, $\theta(\mathbb{Z}_2 \times \mathbb{Z}_4, d) = \theta(D_8, d)$ for each divisor d of 8 (and, in fact, their automorphism groups are isomorphic), yet $\mathbb{Z}_2 \times \mathbb{Z}_4 \ncong D_8$. ■

3.2 Subgroups and Fixed Points

It is natural to ask whether the fixed points of automorphisms of a subgroup H of G are related to the fixed points of the automorphisms of G. However, any answer to this question is complicated by the fact that the automorphism groups of G and H need not be related. Instead, more can be said about how the subgroup H and the fixed points of automorphisms of G interact.

Definition 2 *A subgroup $H \leq G$ is characteristic in G (and we write $H \blacktriangleleft G$) if $\alpha(H) = H$ for all $\alpha \in \mathrm{Aut}(G)$.*

Clearly, if $H \blacktriangleleft G$, then $H \lhd G$. Moreover, any automorphism of G restricts to an automorphism of $H \blacktriangleleft G$.

We shall consider two ways of viewing the relationship between a subgroup H of G and the fixed points of $\alpha \in \mathrm{Aut}(G)$. The first method examines all automorphisms which fix *at least* the elements of a subset X of G. That is, define, for each $X \subseteq G$, the set $X_F = \{\alpha \in \mathrm{Aut}(G) : X \subseteq F_G(\alpha)\}$. This view is advantageous in that for each $X \subseteq G$, $X_F \leq \mathrm{Aut}(G)$.

Lemma 2 *For any $X \subseteq G$, $X_F \leq \mathrm{Aut}(G)$. In fact, if $X \subseteq X' \subseteq G$, then $X'_F \leq X_F$. Moreover, for any subsets $X, X' \subseteq G$, $(X \cup X')_F = X_F \cap X'_F$.*

PROOF: Let $X \subseteq G$. Since ι fixes all of G pointwise, ι fixes X pointwise so $X \subseteq F_G(\iota)$ and $\iota \in X_F$. Let $\alpha, \beta \in X_F$ and $x \in X$. Then $(\alpha\beta)(x) = \alpha(\beta(x)) = \alpha(x) = x$, so $\alpha\beta \in X_F$, and $\alpha^{-1}(x) = \alpha^{-1}(\alpha(x)) = x$, so $\alpha^{-1} \in X_F$. Thus, $X_F \leq \mathrm{Aut}(G)$.

If $X \subseteq X' \subseteq G$ and $\alpha \in X'_F$, then $F_G(\alpha) \supseteq X' \supseteq X$, so $\alpha \in X_F$, and $X'_F \leq X_F$. If X, X' are any subsets of G, and $\alpha \in (X \cup X')_F$, then $F(\alpha) \supseteq X \cup X'$ so $F(\alpha) \supseteq X, X'$ and $\alpha \in X_F \cap X'_F$. Conversely, if $\alpha \in X_F \cap X'_F$, then $F(\alpha)$ fixes every element of X and of X', so it fixes every element of $X \cup X'$ and $\alpha \in (X \cup X')_F$. ■

If we assume X to be a subgroup of G, X_F gains additional structure.

Lemma 3 *If $H \blacktriangleleft G$, then $H_F \lhd \mathrm{Aut}(G)$. Moreover, if $H, K \leq G$ and $H \cong K$, then $H_F \cong K_F$.*

PROOF: Suppose $H \blacktriangleleft G$. By Lemma 2, $H_F \leq \mathrm{Aut}(G)$. Let $\alpha \in \mathrm{Aut}(G)$, $\beta \in H_F$, and $h \in H$. Then $(\alpha\beta\alpha^{-1})(h) = \alpha(\beta(\alpha^{-1}(h))) = \alpha(\alpha^{-1}(h)) = h$ since $H \blacktriangleleft G$. Thus, $\alpha\beta\alpha^{-1} \in H_F$, and $H_F \lhd \mathrm{Aut}(G)$.

Now let $H, K \leq G$ and suppose $\sigma : H \to K$ is an isomorphism. Define $f : H_F \to K_F$ by $f(\beta) = \sigma\beta\sigma^{-1}$ for all $\beta \in H_F$. To see that f is well-defined, let $\beta \in H_F$ and $k \in K$. Then $(\sigma\beta\sigma^{-1})(k) = \sigma(\beta(\sigma^{-1}(k))) = \sigma(\sigma^{-1}(k)) = k$, so $\sigma\beta\sigma^{-1} \in K_F$. Similarly, to see that f is onto, let $\gamma \in K_F$ and $h \in H$. Then $(\sigma^{-1}\gamma\sigma)(h) = \sigma^{-1}(\gamma(\sigma(h))) = \sigma^{-1}(\sigma(h)) = h$ so $\sigma^{-1}\gamma\sigma \in H_F$ and $f(\sigma^{-1}\gamma\sigma) = \gamma$. Next, suppose $f(\beta) = f(\beta')$ for some $\beta, \beta' \in H_F$. Then $\sigma\beta\sigma^{-1} = \sigma\beta'\sigma^{-1}$ so $\beta = \beta'$ and f is one-to-one. Finally, for any $\beta, \beta' \in H_F$, we have $f(\beta\beta') = \sigma\beta\beta'\sigma^{-1} = \sigma\beta\sigma^{-1}\sigma\beta'\sigma^{-1} = f(\beta)f(\beta')$, so $H_F \cong K_F$, as desired. ■

While viewing the fixed points in terms of X_F provides group structure, it does not easily permit counting fixed points, for $X \cap X' = \emptyset$ need not imply that $X_F \cap X'_F = \emptyset$. A second view, however, more readily lends itself to counting fixed points relative to subgroups. In this view, we examine all automorphisms of G which fix *exactly* the elements of $H \leq G$. More formally, for any $H \leq G$, the *set of H-fixers* is $F_G^{-1}(H) = \{\alpha \in \mathrm{Aut}(G) : F_G(\alpha) = H\}$.

As the notation suggests, this set is the preimage of H under the map F_G. Of course, $F_G^{-1}(H) \subseteq H_F$ for any $H \leq G$.

While $F_G^{-1}(H)$ need not be a group, the concept does lend itself to counting automorphisms in that it affords another partition of $\mathrm{Aut}(G)$. Define the binary relation $\approx$ on $\mathrm{Aut}(G)$ by $\alpha \approx \beta$ if and only if $F_G(\alpha) = F_G(\beta)$ (i.e., $\alpha, \beta \in F_G^{-1}(H)$ for some H). It is clear that this is an equivalence relation, and the partition induced by $\approx$ is finer than that induced by $\sim$ (for if $\alpha \approx \beta$, then $\alpha \sim \beta$). Hence, for each $d \mid |G|$, S_d is itself partitioned by $\approx$. Therefore, to determine $\theta(G, d)$, first count, for each $H \leq G$ of order d, the number of automorphisms whose fixed-point group is H (i.e., find $|F_G^{-1}(H)|$), and then add these counts together. That is,

$$\theta(G, d) = \sum_{H \leq G, |H| = d} |F_G^{-1}(H)| \tag{3}$$

This technique, combined with the following lemma, provides a powerful counting tool to calculate θ-values, as we shall illustrate in our study of elementary abelian groups.

Theorem 5 *Let $H \leq G$ and $\alpha \in \mathrm{Aut}(G)$. Then $|F_G^{-1}(H)| = |F_G^{-1}(\alpha(H))|$ and $F_G(\alpha) \cap H \cong F_G(\alpha) \cap \alpha(H)$.*

Proof: Let $H \leq G$ and $\alpha \in \mathrm{Aut}(G)$. Since the map $\alpha|_H : H \to \alpha(H)$ is an isomorphism, $H \cong \alpha(H)$. Now, define $\tau : F_G^{-1}(H) \to F_G^{-1}(\alpha(H))$ by $\tau(\beta) = \alpha\beta\alpha^{-1}$ for all $\beta \in F_G^{-1}(H)$. We show that τ is a bijection. To see that τ is well-defined, let $\beta \in F_G^{-1}(H)$ and $\alpha(h) \in \alpha(H)$. Now, $\alpha\beta\alpha^{-1} \in \mathrm{Aut}(G)$ since $\beta, \alpha \in \mathrm{Aut}(G)$. Moreover $(\alpha\beta\alpha^{-1})(\alpha(h)) = \alpha(\beta(h)) = \alpha(h)$, so $\alpha(h) \in F_G(\alpha\beta\alpha^{-1})$. Suppose that $(\alpha\beta\alpha^{-1})(g) = g$ for some $g \in G$. Then $\alpha(\beta(\alpha^{-1}(g))) = \alpha(\alpha^{-1}(g))$ so as α is one-to-one, $\beta(\alpha^{-1}(g)) = \alpha^{-1}(g)$. Thus, $\alpha^{-1}(g) \in F_G(\beta) = H$ so $g \in \alpha(H)$, and $\alpha\beta\alpha^{-1} \in F_G^{-1}(\alpha(H))$.

Let $\gamma \in F_G^{-1}(\alpha(H))$. Then $\alpha^{-1}\gamma\alpha \in \mathrm{Aut}(G)$ since $\alpha, \gamma \in \mathrm{Aut}(G)$. Additionally, for all $h \in H$, $(\alpha^{-1}\gamma\alpha)(h) = \alpha^{-1}(\gamma(\alpha(h))) = \alpha^{-1}(\alpha(h)) = h$, so h is fixed by $\alpha^{-1}\gamma\alpha$. Suppose $(\alpha^{-1}\gamma\alpha)(g) = g$ for some $g \in G$. Then $\alpha^{-1}(\gamma(\alpha(g))) = \alpha^{-1}(\alpha(g))$ so as α^{-1} is one-to-one, $\gamma(\alpha(g)) = \alpha(g)$. Hence, $\alpha(g)$ is fixed by γ, so $\alpha(g) \in F_G(\gamma) = \alpha(H)$ and $g \in H$ since α is one-to-one. Therefore, $\alpha^{-1}\gamma\alpha \in F_G^{-1}(H)$, and $\tau(\alpha^{-1}\gamma\alpha) = \gamma$, so τ is onto.

Finally, suppose $\tau(\beta) = \tau(\beta')$ for some $\beta, \beta' \in F_G^{-1}(H)$. Then $\alpha\beta\alpha^{-1} = \alpha\beta'\alpha^{-1}$, so $\beta = \beta'$, and τ is one-to-one. Therefore, τ is a bijection and $|F_G^{-1}(H)| = |F_G^{-1}(\alpha(H))|$. The final claim is easily shown by $F_G(\alpha) \cap H \cong \alpha(F_G(\alpha) \cap H) = \alpha(F_G(\alpha)) \cap \alpha(H) = F_G(\alpha) \cap \alpha(H)$ since α is one-to-one and since $F_G(\alpha)$ is invariant under α. ■

3.3 Direct Products and Fixed Points

Another natural question about fixed points involves the extent to which the fixed points of automorphisms of $A \times B$ are related to those of A and of B. We shall see that this relationship is strong indeed.

Theorem 6 *For any groups A, B, $\mathrm{Aut}(A) \times \mathrm{Aut}(B) \leq \mathrm{Aut}(A \times B)$.*

PROOF: Let $\alpha \in \mathrm{Aut}(A)$ and $\beta \in \mathrm{Aut}(B)$; we consider the map (α, β) naturally defined by $(\alpha, \beta)(a, b) = (\alpha(a), \beta(b))$ for all $(a, b) \in A \times B$. Let $(a, b), (a', b') \in A \times B$. Then $(\alpha, \beta)[(a, b)(a', b')] = (\alpha(aa'), \beta(bb')) = (\alpha(a)\alpha(a'), \beta(b)\beta(b')) = (\alpha(a), \beta(b))(\alpha(a'), \beta(b')) = (\alpha, \beta)[(a, b)](\alpha, \beta)[(a', b')]$, so (α, β) is a homomorphism. If $(a', b') \in A \times B$, there are $a \in A$ and $b \in B$ such that $\alpha(a) = a'$ and $\beta(b) = b'$, so $(\alpha, \beta)[(a, b)] = (a', b')$, and (α, β) is onto. Moreover, suppose $(\alpha, \beta)[(a, b)] = (\alpha, \beta)[(a', b')]$ for some $(a, b), (a', b') \in A \times B$. It follows that $\alpha(a) = \alpha(a')$ and $\beta(b) = \beta(b')$, so $a = a'$, $b = b'$, and $(a, b) = (a', b')$. Thus, (α, β) is an automorphism of $A \times B$. ■

This link between the automorphisms of the two factors A and B and those of $A \times B$ implies a connection between their fixed points.

Lemma 4 *For any groups A, B and any $\alpha \in \mathrm{Aut}(A)$ and $\beta \in \mathrm{Aut}(B)$, $F_{A\times B}((\alpha, \beta)) = F_A(\alpha) \times F_B(\beta)$.*

PROOF: Let $\alpha \in \mathrm{Aut}(A)$ and $\beta \in \mathrm{Aut}(B)$. Suppose $(a, b) \in F_{A\times B}((\alpha, \beta))$. Then $(\alpha, \beta)[(a, b)] = (\alpha(a), \beta(b)) = (a, b)$, so $\alpha(a) = a$, $\beta(b) = b$, and $(a, b) \in F_A(\alpha) \times F_B(\beta)$. Conversely, suppose $(a', b') \in F_A(\alpha) \times F_B(\beta)$. Then $\alpha(a') = a'$ and $\beta(b') = b'$, so $(\alpha, \beta)[(a', b')] = (\alpha(a'), \beta(b')) = (a', b')$, and $(a', b') \in F_{A\times B}((\alpha, \beta))$. ■

Since the fixed-point group of (α, β) is simply the direct product of the fixed-point groups of α and β, we may begin to relate the θ-values of $A \times B$ to those of A and of B.

Lemma 5 *Let A, B be groups, $d_A \mid |A|$, and $d_B \mid |B|$. Then $S^A_{d_A} \times S^B_{d_B} \subseteq S^{A\times B}_{d_A d_B}$ and $\theta(A, d_A)\theta(B, d_B) \leq \theta(A \times B, d_A d_B)$.*

PROOF: If $(\alpha, \beta) \in S^A_{d_A} \times S^B_{d_B}$, then $|F_A(\alpha)| = d_A$ and $|F_B(\beta)| = d_B$. Thus, $|F_{A\times B}((\alpha, \beta))| = |F_A(\alpha) \times F_B(\beta)| = d_A d_B$, so $(\alpha, \beta) \in S^{A\times B}_{d_A d_B}$. Then $\theta(A, d_A)\theta(B, d_B) = |S^A_{d_A} \times S^B_{d_B}| \leq |S^{A\times B}_{d_A d_B}| = \theta(A \times B, d_A d_B)$. ■

Combining the theory of fixed points for subgroups and direct products demonstrates some fairly intuitive results.

Lemma 6 *If $X \subseteq A$ and $Y \subseteq B$, then $X_F \times Y_F = (X \times Y)_F$. Moreover, if $H \leq A$ and $K \leq B$, then $F_A^{-1}(H) \times F_B^{-1}(K) \subseteq F^{-1}_{A\times B}(H \times K)$.*

PROOF: Suppose $(\alpha, \beta) \in X_F \times Y_F$. Then for all $x \in X$ and $y \in Y$, $\alpha(x) = x$ and $\beta(y) = y$, so $(\alpha, \beta)[(x, y)] = (x, y)$. Thus, $(\alpha, \beta) \in (X \times Y)_F$ by definition. Conversely, let $(\alpha, \beta) \in (X \times Y)_F$. Then for all $(x, y) \in X \times Y$, $(\alpha, \beta)[(x, y)] = (\alpha(x), \beta(y)) = (x, y)$, so $\alpha(x) = x$ and $\beta(y) = y$. Hence, $\alpha \in X_F$ and $\beta \in Y_F$, so $(\alpha, \beta) \in X_F \times Y_F$.

Let $(\alpha, \beta) \in F_A^{-1}(H) \times F_B^{-1}(K)$ and $(h, k) \in H \times K$. Then $(\alpha, \beta)[(h, k)] = (\alpha(h), \beta(k)) = (h, k)$. If $(\alpha, \beta)[(a, b)] = (a, b)$ for any $(a, b) \in A \times B$, it follows that $\alpha(a) = a$ and $\beta(b) = b$, so that $a \in H$ and $b \in K$. Thus, $(\alpha, \beta) \in F^{-1}_{A\times B}(H \times K)$, as desired. ■

The relationship between the automorphisms of $A \times B$ and those of A and B is strengthened if we require that $|A|$ and $|B|$ be coprime. This assumption enhances our ability to describe $A \times B$, per the following lemma.

Lemma 7 *Suppose* $\gcd(|A|, |B|) = 1$. *Then for all* $(a, b) \in A \times B$, $|(a, b)| = |a||b|$, *and* $A' := A \times \{e\}, B' := \{e\} \times B \blacktriangleleft A \times B$.

Proof: For any $a \in A$ and $b \in B$, $\gcd(|a|, |b|) = 1$, so $|(a, b)| = \text{lcm}(|a|, |b|) = |a||b|$. We prove the second statement for A'; the proof for B' is similar. Let $\sigma \in \text{Aut}(A \times B)$ and $(a, e) \in A'$. Then $\sigma(a, e) = (a', b')$ for some $a' \in A, b' \in B$. But $|(a', b')| = |a'||b'| = |(a, e)| = |a|$, so since $\gcd(|a|, |b'|) = 1$, $|a'| = |a|$ and $|b'| = 1$. Thus, $b' = e$, and $(a', b') \in A'$. So, $\sigma(A') \subseteq A'$ and $A' \blacktriangleleft A \times B$. ■

To facilitate the discussion below, we consider $A, B \leq A \times B$ by associating $a \leftrightarrow (a, e)$ and $b \leftrightarrow (e, b)$ for all $a \in A$ and $b \in B$. With this, we may replace A' and B' with A and B (respectively) and write $A, B \blacktriangleleft A \times B$. By Lemma 7, any automorphism of $A \times B$ restricted to either A or B is itself an automorphism.

Theorem 7 *If* A, B *are groups for which* $\gcd(|A|, |B|) = 1$, $\text{Aut}(A) \times \text{Aut}(B) = \text{Aut}(A \times B)$.

Proof: By Theorem 6, it suffices to show that $\text{Aut}(A \times B) \subseteq \text{Aut}(A) \times \text{Aut}(B)$. Let $\sigma \in \text{Aut}(A \times B)$ and define $\alpha_\sigma = \sigma|_A$ and $\beta_\sigma = \sigma|_B$. By Lemma 7, $\alpha_\sigma \in \text{Aut}(A)$ and $\beta_\sigma \in \text{Aut}(B)$. Let $(a, b) \in A \times B$. It follows that $(\alpha_\sigma, \beta_\sigma)(a, b) = (\alpha_\sigma(a), \beta_\sigma(b)) = \sigma(a, b)$. Therefore, $\sigma = (\alpha_\sigma, \beta_\sigma)$, and these α_σ, β_σ are uniquely determined by (and uniquely determine) σ. ■

The equality of the automorphism group of $A \times B$ and $\text{Aut}(A) \times \text{Aut}(B)$ provides in turn stronger relationships between the fixed points of $A \times B$ and those of A and B. The following corollary is quite powerful, for it allows us to compute the θ-values of $A \times B$ using the θ-values of A and B when $\gcd(|A|, |B|) = 1$. This fact shall be employed extensively in our investigation of cyclic and abelian groups.

Theorem 8 *Let* A, B *be groups for which* $\gcd(|A|, |B|) = 1$. *Then for all* $d_A \mid |A|$ *and* $d_B \mid |B|$, $S^{A\times B}_{d_A d_B} = S^A_{d_A} \times S^B_{d_B}$ *and* $\theta(A \times B, d_A d_B) = \theta(A, d_A)\theta(B, d_B)$.

Proof: Let A, B be groups for which $\gcd(|A|, |B|) = 1$, let $d_A \mid |A|$, and let $d_B \mid |B|$. By Lemma 5, it remains to show that $S^{A\times B}_{d_A d_B} \subseteq S^A_{d_A} \times S^B_{d_B}$. Suppose $(\alpha, \beta) \in S^{A\times B}_{d_A d_B}$. Then by Lemma 4, $|F_{A\times B}((\alpha, \beta))| = |F_A(\alpha) \times F_B(\beta)| = |F_A(\alpha)||F_B(\beta)| = d_A d_B$, so by Fact 2, $|F_A(\alpha)| = d_A$ and $|F_B(\beta)| = d_B$. Hence, $\alpha \in S^A_{d_A}$ and $\beta \in S^B_{d_B}$, so $(\alpha, \beta) \in S^A_{d_A} \times S^B_{d_B}$ and $S^{A\times B}_{d_A d_B} = S^A_{d_A} \times S^B_{d_B}$. It follows that $\theta(A \times B, d_A d_B) = |S^{A\times B}_{d_A d_B}| = |S^A_{d_A} \times S^B_{d_B}| = \theta(A, d_A)\theta(B, d_B)$. ■

The assumption that the orders of A and B are coprime also strengthens the results regarding direct products and subgroups.

Lemma 8 *If* $\gcd(|A|,|B|)=1$ *and if* $H \leq A$ *and* $K \leq B$, *then* $F^{-1}_{A\times B}(H\times K) = F^{-1}_A(H)\times F^{-1}_B(K)$.

PROOF: By Lemma 6, it remains to show that $F^{-1}_{A\times B}(H\times K) \subseteq F^{-1}_A(H)\times F^{-1}_B(K)$. Let $(\alpha,\beta)\in F^{-1}_{A\times B}(H\times K)$. Since for all $h\in H$ and all $k\in K$, $(\alpha,\beta)[(h,k)]=(h,k)$, it follows that $\alpha(h)=h$ and $\beta(k)=k$. If $\alpha(a)=a$ for some $a\in A$, then $(\alpha,\beta)[(a,e)]=(a,e)$, so $a\in H$, and if $\beta(b)=b$ for some $b\in B$, then $(\alpha,\beta)[(e,b)]=(e,b)$, so $b\in K$. Therefore, $\alpha\in F^{-1}_A(H)$ and $\beta\in F^{-1}_B(K)$, so $(\alpha,\beta)\in F^{-1}_A(H)\times F^{-1}_B(K)$, as desired. ■

4 Cyclic Groups

Through the remainder of this paper, we determine formulae for θ for a few classes of finite abelian groups. In this section, we consider the finite cyclic groups, presented as the additive groups $\mathbb{Z}_n$, and determine how to calculate their θ-values. We first find the fixed-point groups and then use this information to compute the θ-values.

The finite cyclic groups have a particularly straightforward automorphism group. Since $\mathbb{Z}_n$ is generated by 1, any automorphism of $\mathbb{Z}_n$ must map 1 to another generator of $\mathbb{Z}_n$, namely another element of $\mathbb{Z}_n$ that is coprime to n. Since these are exactly the elements in U_n (the group of units modulo n), we have the following result.

Theorem 9 *For any cyclic group* $\mathbb{Z}_n$, $\mathrm{Aut}(\mathbb{Z}_n)\cong U_n$, *so* $|\mathrm{Aut}(\mathbb{Z}_n)|=\varphi(n)$. *Specifically, we may write* $\mathrm{Aut}(\mathbb{Z}_n)=\{\alpha_r : 1\mapsto r \mid r\in U_n\}$.

PROOF: Define $f:\mathrm{Aut}(\mathbb{Z}_n)\to U_n$ by $f(\alpha)=\alpha(1)$ for all $\alpha\in\mathrm{Aut}(\mathbb{Z}_n)$. For any $\alpha\in\mathrm{Aut}(\mathbb{Z}_n)$, $|1|=n=|\alpha(1)|$, so $\gcd(\alpha(1),n)=1$ and $f(\alpha)=\alpha(1)\in U_n$. Conversely, if $r\in U_n$, define the homomorphism $\alpha_r : 1\mapsto r$. Then $\mathbb{Z}_n=\langle r\rangle$, so α_r is onto and hence (as $\mathbb{Z}_n$ is finite) one-to-one. Thus, α_r is an automorphism and $f(\alpha_r)=r$ (so f is onto). If $f(\alpha)=f(\beta)$ for some $\alpha,\beta\in\mathrm{Aut}(\mathbb{Z}_n)$, then $\alpha(1)=\beta(1)$. So, $\alpha=\beta$, and f is one-to-one. Finally, $f(\alpha\beta)=(\alpha\beta)(1)=\alpha(\beta(1))=\alpha(1)\beta(1)=f(\alpha)f(\beta)$. Hence, we may write $\mathrm{Aut}(\mathbb{Z}_n)=\{\alpha_r : 1\mapsto r \mid r\in U_n\}$ and $|\mathrm{Aut}(\mathbb{Z}_n)|=\varphi(n)$. ■

Note 4 *When discussing cyclic groups,* α_r *is reserved as* $\alpha_r : 1\mapsto r$, *for* $r\in U_n$.

Now that we know the form of each automorphism of $\mathbb{Z}_n$, we can determine the fixed-point groups.

Theorem 10 *Let* $\alpha_r\in\mathrm{Aut}(\mathbb{Z}_n)$. *Then* $F(\alpha_r)=\langle n/d_r\rangle$ *where* $d_r=\gcd(r-1,n)$. *So,* $|F(\alpha_r)|=d_r$.

PROOF: Let $\alpha_r\in\mathrm{Aut}(\mathbb{Z}_n)$ and $d_r=\gcd(r-1,n)$. If $r=1$, α_1 is the identity map, so $F(\alpha_1)=\mathbb{Z}_n=\langle n/d_r\rangle$. Suppose $r\neq 1$. Then $m\in F(\alpha_r)$ if and only if $mr\equiv m \pmod n$, which occurs if and only if $m\equiv 0 \pmod{n/d_r}$. This is equivalent to $m\in\langle n/d_r\rangle$, so it follows that $F(\alpha_r)=\langle n/d_r\rangle$, as desired. ■

Example 1 *The automorphism group of* $\mathbb{Z}_9$ *is isomorphic to* $U_9 = \{1, 2, 4, 5, 7, 8\}$*, so the automorphisms are* $\alpha_1, \alpha_2, \alpha_4, \alpha_5, \alpha_7, \alpha_8$*. The automorphism* α_4 *sends* $1 \mapsto 4$*,* $2 \mapsto 8$*,* $3 \mapsto 3$*,* $4 \mapsto 7$*,* $5 \mapsto 2$*,* $6 \mapsto 6$*,* $7 \mapsto 1$*, and* $8 \mapsto 5$*, so the fixed-point group is* $F(\alpha_4) = \{0, 3, 6\} = \langle 3 \rangle$*. Indeed,* $\gcd(4-1, 9) = 3$*, so by Theorem 10,* $F(\alpha_4) = \langle 9/3 \rangle = \langle 3 \rangle$*. In a similar manner, we find* $F(\iota) = \mathbb{Z}_9$*,* $F(\alpha_2) = F(\alpha_5) = F(\alpha_8) = \{0\}$*, and* $F(\alpha_4) = F(\alpha_7) = \langle 3 \rangle$*.*

Now that we know the fixed point sets of the automorphisms of $\mathbb{Z}_n$, we may classify the automorphisms according to the number of fixed points each has. That is, we compute the θ-values for cyclic groups. However, by Theorem 8 and the following well-known result, it suffices to consider cyclic p-groups (a finite *p-group* is one of prime power order).

Fact 3 *[3] Let* $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ *be the prime factorization of* n*, where the primes* p_i *are distinct and* $k_i \in \mathbb{Z}^+$ *for all* $1 \leq i \leq t$*. Then* $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_t^{k_t}}$*.*

As such, we now explicitly compute the θ-values for groups of the form $\mathbb{Z}_{p^k}$, for p a prime.

Theorem 11 *Let* p *be a prime and* $k \in \mathbb{Z}^+$*. For any* $0 \leq l \leq k$*:*

$$\theta(\mathbb{Z}_{p^k}, p^l) = \begin{cases} p^k - 2p^{k-1} \text{ for } l = 0 \\ \varphi(p^{k-l}) \text{ otherwise} \end{cases} \tag{4}$$

Proof: Let p be prime and $k \in \mathbb{Z}^+$. Any divisor of p^k is of the form p^l, where $0 \leq l \leq k$. If $k = l$, then $p^k = p^l$ and $\theta(p^l) = 1$. We now show that for all $0 < l < k$, $S_{p^l} = \{\alpha_{p^l x+1} : x \in U_{p^{k-l}}\}$. Let $x \in U_{p^{k-l}}$ and $d = \gcd(p^l x, p^k)$. Since $\gcd(x, p^{k-l}) = 1$, it must be that $\gcd(x, p^k) = 1$, so $\gcd(x, d) = 1$. Since $d \mid (p^l x)$, it follows that $d \mid p^l$, but as $p^l \mid d$, we have $d = p^l$. Let $\gcd(p^l x + 1, p^k) = d'$. If $p \mid d'$, then $p \mid 1$, a contradiction, so $d' = 1$. Hence, $p^l x + 1 \in U_{p^k}$ and $\alpha_{p^l x+1} \in \mathrm{Aut}(\mathbb{Z}_n)$. Moreover, by Theorem 10, $|F(\alpha_{p^l x+1})| = \gcd(p^l x, p^k) = p^l$, so $\alpha_{p^l x+1} \in S_{p^l}$.

Conversely, suppose $\alpha_r \in S_{p^l}$. Then $\gcd(r-1, p^k) = p^l$. This gives $\gcd((r-1)/p^l, p^{k-l}) = 1$, so $(r-1)/p^l \in U_{p^{k-l}}$ and $r = p^l((r-1)/p^l) + 1$, as desired. Finally, we must show that $|S_{p^l}| = \varphi(p^{k-l})$. Suppose $p^l x_1 + 1 \equiv p^l x_2 + 1 \pmod{p^k}$ for some $x_1, x_2 \in U_{p^{k-l}}$. Then $p^l x_1 \equiv p^l x_2 \pmod{p^k}$, but since (without loss of generality) $x_1, x_2 < p^{k-l}$, it follows that $p^l x_1, p^l x_2 < p^k$ so $p^l x_1 = p^l x_2$ and $x_1 = x_2$. Hence, $|U_{p^{k-l}}| = |S_{p^l}| = \varphi(p^{k-l})$. So, $\theta(p^l) = \varphi(p^{k-l}) = p^{k-l} - p^{k-l-1}$.

Finally, all automorphisms (of which there are $\varphi(p^k)$ total) for which we have not yet

accounted must be in S_1. Thus,

$$\begin{aligned}\theta(\mathbb{Z}_{p^k},1) &= \varphi(p^k) - \sum_{l=1}^{k}\theta(\mathbb{Z}_{p^k},p^l)\\ &= p^k - p^{k-1} - 1 - \sum_{l=1}^{k-1}(p^{k-l} - p^{k-l-1})\\ &= p^k - p^{k-1} - 1 - \sum_{l=1}^{k-1}(p^{k-l}) + \sum_{l=1}^{k-1}(p^{k-l-1})\\ &= p^k - p^{k-1} - 1 - \sum_{l=1}^{k-1}(p^{k-l}) + \sum_{L=2}^{k}(p^{k-L}) \text{ (where } L = l+1)\\ &= p^k - p^{k-1} - 1 - p^{k-1} + 1 = p^k - 2p^{k-1}\end{aligned}$$

as desired. ■

Example 2 *Returning again to $\mathbb{Z}_9$, from Example 1, we see that there are three automorphisms which fix only one point, two automorphisms which fix three points, and one which fixes all nine points, so $\theta(1) = 3$, $\theta(3) = 2$, and $\theta(9) = 1$. Indeed, by Theorem 11, $\theta(1) = 9 - 6 = 3$, $\theta(3) = 3 - 1 = 2$, and $\theta(9) = 1$.*

As aforementioned, we now exploit Fact 3 and Theorem 8 to compute θ for general finite cyclic groups.

Theorem 12 *Let $n = p_1^{k_1}, p_2^{k_2}\cdots p_t^{k_t}$ be the unique prime factorization of n and let $d \mid n$, i.e. $d = p_1^{l_1}p_2^{l_2}\cdots p_t^{l_t}$ with $0 \le l_i \le k_i$ for all $1 \le i \le t$. Then*

$$\theta(\mathbb{Z}_n, d) = \prod_{i=1}^{t}\theta(\mathbb{Z}_{p_i^{k_i}}, p_i^{l_i}) = \varphi(n/d)\prod_{l_i=0}\theta(\mathbb{Z}_{p_i^{k_i}},1) \tag{5}$$

PROOF: By Fact 3, $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}}\times\cdots\times\mathbb{Z}_{p_t^{k_t}}$, so by Theorems 3 and 8, since $\gcd(|\mathbb{Z}_{p_i^{k_i}}|, |\mathbb{Z}_{p_j^{k_j}}|) = 1$ for all $i \ne j$, the first equality holds. If we collect all $l_i \ne 0$, we have

$$\prod_{l_i\ne 0}\theta(\mathbb{Z}_{p_i^{k_i}}, p_i^{l_i}) = \prod_{l_i\ne 0}\varphi(p_i^{k_i-l_i}) = \varphi\left(\prod_{l_i\ne 0}(p_i^{k_i-l_i})\right) = \varphi(n/d)$$

since φ is multiplicative [1]. Hence, the second equality holds. ■

Example 3 *Since $\mathbb{Z}_{18} \cong \mathbb{Z}_2 \times \mathbb{Z}_9$, we have for instance $\theta(\mathbb{Z}_{18}, 2) = \theta(\mathbb{Z}_2, 2)\theta(\mathbb{Z}_9, 1) = (1)(3) = 3$, $\theta(\mathbb{Z}_{18}, 3) = \theta(\mathbb{Z}_2, 1)\theta(\mathbb{Z}_9, 3) = (0)(2) = 0$, and $\theta(\mathbb{Z}_{18}, 6) = \theta(\mathbb{Z}_2, 2)\theta(\mathbb{Z}_9, 3) = (1)(2) = 2$.*

To underscore the relationship between $\theta(\mathbb{Z}_n)$ and φ, the following corollary is worthy of note.

Corollary 2 *Let $d \mid n$. If for all $p \mid n$, $p \mid d$, then $\theta(\mathbb{Z}_n, d) = \varphi(n/d)$.*

5 Elementary Abelian Groups

We now turn to more complicated finite abelian groups. All finite abelian groups can be expressed as the direct product of cyclic groups of prime power order [3]. However, by Theorem 8, it suffices to consider finite abelian p-groups (i.e., groups of the form $\mathbb{Z}_{p^{k_1}} \times \mathbb{Z}_{p^{k_2}} \times \cdots \times \mathbb{Z}_{p^{k_t}}$ for prime p), for, as we shall explain in detail later, the values of θ for any other abelian group can be computed by multiplying the θ-values of the relevant p-groups.

Thus, we begin by examining elementary abelian p-groups, of the form $\mathbb{Z}_p^n = \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ for some prime p (note that, as with cyclic groups, we consider these groups additively). These groups are a convenient starting point for many reasons: $\mathbb{Z}_p^n$ may be viewed as a vector space over $\mathbb{Z}_p$, any subgroup of order p^k is isomorphic to $\mathbb{Z}_p^k$, and all nonidentity elements of $\mathbb{Z}_p^n$ are of order p. As such, we shall view $\mathbb{Z}_p^n$ both as a group and as a vector space over $\mathbb{Z}_p$ and let e_i denote the ith standard basis vector of $\mathbb{Z}_p^n$.

The group of automorphisms of $\mathbb{Z}_p^n$ is isomorphic to $GL_n(\mathbb{Z}_p)$, the group of $n \times n$ matrices whose entries are in $\mathbb{Z}_p$ and which are invertible (i.e., their determinant is nonzero modulo p) [2]. These automorphisms, however, are difficult to analyze on an individual basis, so we take a more indirect route to compute θ for $\mathbb{Z}_p^n$. Specifically, for each subgroup H of $\mathbb{Z}_p^n$, we count the number of automorphisms of $\mathbb{Z}_p^n$ whose fixed-point group is exactly H (i.e., $|F^{-1}(H)|$). As discussed above, for each $d \mid p^n$, we can then compute $\theta(\mathbb{Z}_p^n, d)$ by adding $|F^{-1}(H)|$ over all subgroups H of $\mathbb{Z}_p^n$ of order d. The key to this approach lies the following lemmas, which show that it suffices to consider, for each divisor d of p^n, one representative subgroup of order d, greatly simplifying our task.

Lemma 9 *If $H, K \leq \mathbb{Z}_p^n$ and $|H| = |K|$, then there is an automorphism $\alpha \in \mathrm{Aut}(\mathbb{Z}_p^n)$ such that $\alpha(H) = K$.*

Proof: Since $H, K \leq \mathbb{Z}_p^n$ and $|H| = |K|$, $H \cong \mathbb{Z}_p^k \cong K$ for some $0 \leq k \leq n$. If $|H| = |K| = 1$, then $H = K = \{\vec{0}\}$, and any automorphism satisfies $\alpha(H) = K$. Otherwise, view H and K as vector spaces over $\mathbb{Z}_p$ and let $\mathcal{B}_H = \{a_1, \ldots, a_k\}$ and $\mathcal{B}_K = \{b_1, \ldots, b_k\}$ be bases for H and K, respectively. There are $M_H, M_K \in GL_n(\mathbb{Z}_p)$ for which column i of M_H is a_i and column i of M_K is b_i for all $1 \leq i \leq k$. It follows that $M_H e_i = a_i$ and $M_K e_i = b_i$ for all $1 \leq i \leq k$. Define α_H and α_K to be the automorphisms corresponding to M_H and M_K, respectively, so $\alpha_H(e_i) = a_i$ and $\alpha_K(e_i) = b_i$ for all $1 \leq i \leq k$. Then the automorphism $\alpha_K \alpha_H^{-1}$ satisfies $(\alpha_K \alpha_H^{-1})(a_i) = b_i$ for all $1 \leq i \leq k$. It follows that $(\alpha_K \alpha_H^{-1})(H) \subseteq K$, but since α is bijective and $|H| = |K|$, $(\alpha_K \alpha_H^{-1})(H) = K$, as desired. ■

Corollary 3 *If $H, K \leq \mathbb{Z}_p^n$ and $|H| = |K|$, then $|F^{-1}(H)| = |F^{-1}(K)|$.*

Proof: Since $H, K \leq \mathbb{Z}_p^n$ and $|H| = |K|$, $H \cong \mathbb{Z}_p^k \cong K$ for some $0 \leq k \leq n$. Then there is an automorphism $\alpha \in \mathrm{Aut}(\mathbb{Z}_p^n)$ for which $\alpha(H) = K$ by Lemma 9. By Theorem 5, $|F^{-1}(H)| = |F^{-1}(K)|$, as desired. ■

Suppose that for each $1 \leq k \leq n$, we may find the number of automorphisms whose fixed-point group is H_k (i.e., $|F^{-1}(H_k)|$) where $H_k \cong \mathbb{Z}_p^k$. By Corollary 3, any other subgroup K of $\mathbb{Z}_p^n$ of order p^k would satisfy $|F^{-1}(K)| = |F^{-1}(H_k)|$. Thus, if there are N_k subgroups of $\mathbb{Z}_p^n$ of order p^k, it follows that $\theta(\mathbb{Z}_p^n, p^k) = N_k \cdot |F^{-1}(H_k)|$. Because we seek these θ-values, we begin by computing N_k.

Lemma 10 *For each $1 \leq k \leq n$, the number of subgroups of order p^k is*

$$N_k = \prod_{i=0}^{k-1} \frac{(p^n - p^i)}{(p^k - p^i)} \tag{6}$$

and $N_0 = 1$.

PROOF: Let n be given. Of course, the only subgroup of order $p^0 = 1$ is the trivial subgroup, so $N_0 = 1$. Now let $1 \leq k \leq n$ be given, define $\mathbf{B}_n(k)$ as the collection of all ordered sets of k linearly independent vectors from $\mathbb{Z}_p^n$, let $\mathcal{S}_n(k) = \{H \leq \mathbb{Z}_p^n : H \cong \mathbb{Z}_p^k\}$, and consider the map $f : \mathbf{B}_n(k) \to \mathcal{S}_n(k)$ defined by $f(\{v_1, \ldots, v_k\}) = \text{span}\{v_1, \ldots, v_k\}$. Since the span of k linearly independent vectors is of dimension k, f maps $\mathbf{B}_n(k)$ into $\mathcal{S}_n(k)$, and since every subspace $\mathbb{Z}_p^k$ has a basis of size k, the map f is onto. In fact, each subspace will have an equal number of possible bases. Specifically, given a subspace $H \cong \mathbb{Z}_p^k$, to form a basis of H, we may choose linearly independent vectors one by one, as follows. For the first basis vector b_1, we may select any nonzero vector in H, so there are $p^k - 1$ choices for b_1. Since the second vector b_2 must be linearly independent from b_1, we may choose any vector in H not in $\text{span}\{b_1\}$ (which contains the p scalar multiples of b_1), so there are $p^k - p$ options for b_2. Similarly, the third basis vector b_3 may be chosen to be any vector in H not in $\text{span}\{b_1, b_2\}$ (which contains the p^2 linearly combinations of b_1 and b_2), so there are $p^k - p^2$ options for b_3. We proceed in this manner until we have $p^k - p^{k-1}$ choices for the last basis vector. To obtain the total number of ordered bases possible, we multiply together the number of choices for each of the vectors in the basis, so there are $\prod_{i=0}^{k-1}(p^k - p^i)$ possible ordered bases for H.

Now we find $|\mathbf{B}_n(k)|$ in an argument similar to that above. In constructing an arbitrary element of $\mathbf{B}_n(k)$, we have $p^n - 1$ choices for the first vector, $p^n - p$ choices for the second vector, and so on, up to $p^n - p^{k-1}$ choices for the last vector. Thus, there are $\prod_{i=0}^{k-1}(p^n - p^i)$ elements of $\mathbf{B}_n(k)$. Hence, since f is onto and each element of $\mathcal{S}_n(k)$ is the span of an equal number of bases, we have

$$N_k = |\mathcal{S}_n(k)| = \frac{\prod_{i=0}^{k-1}(p^n - p^i)}{\prod_{i=0}^{k-1}(p^k - p^i)} = \prod_{i=0}^{k-1} \frac{(p^n - p^i)}{(p^k - p^i)}$$

as desired. ■

Example 4 *In $\mathbb{Z}_3^3$, any nontrivial subgroup is isomorphic to one of $\mathbb{Z}_3$, $\mathbb{Z}_3^2$, or $\mathbb{Z}_3^3$. Using Lemma 10, the number of subgroups isomorphic to $\mathbb{Z}_3$ is $N_1 = (3^3-1)\ /\ (3^1-1) = 13$, the number of subgroups isomorphic to $\mathbb{Z}_3^2$ is $N_2 = (3^3-1)(3^3-3)\ /\ (3^2-1)(3^2-3) = 13$, and the number of subgroups isomorphic to $\mathbb{Z}_3^3$ is $N_3 = (3^3-1)(3^3-3)(3^3-3^2)\ /\ (3^3-1)(3^3-3)(3^3-3^2) = 1$.*

It remains to find, for each $1 \leq k \leq n$, $|F^{-1}(H)|$ for some representative $H \cong \mathbb{Z}_p^k$. For each $1 \leq k \leq n$, the "simplest" subspace isomorphic to $\mathbb{Z}_p^k$ (for our purposes) is $\langle e_1, e_2, \ldots, e_k\rangle$. Thus, we shall compute $|F^{-1}(\langle e_1, \ldots, e_k\rangle)|$, the number of automorphisms which fix *exactly* $\langle e_1, \ldots, e_k\rangle$. To do this, we count the number of automorphisms which fix *at least* $\langle e_1, \ldots, e_k\rangle$ and then subtract off the automorphisms which fix additional vectors.

Lemma 11 *For each $1 \leq k \leq n-1$, the number of automorphisms of $\mathbb{Z}_p^n$ which fix at least $\langle e_1, \ldots, e_k\rangle$ is $|\langle e_1, \ldots, e_k\rangle_F| = \prod_{i=k}^{n-1}(p^n - p^i)$. Also, $|\langle e_1, \ldots, e_n\rangle_F| = 1$.*

Proof: First, note that since $\langle e_1, \ldots, e_n\rangle = \mathbb{Z}_p^n$, the only automorphism to fix at least $\mathbb{Z}_p^n$ is ι, so it must be that $|\langle e_1, \ldots, e_n\rangle_F| = 1$. Now, let $1 \leq k \leq n-1$, let $\alpha \in \mathrm{Aut}(G)$, and consider M_α, the corresponding matrix in $GL_n(\mathbb{Z}_p)$. For any $1 \leq i \leq n$, M_α fixes e_i if and only if the ith column of M_α is e_i. Suppose M_α fixes $e_1, \ldots, e_k$ (and hence all of $\langle e_1, \ldots, e_k\rangle$). The first k columns of M_α are then $e_1, e_2, \ldots, e_k$, so we have freedom to choose the remaining $n-k$ columns of M_α (so long as M_α remains invertible). Proceeding as in Lemma 10, then, there are $p^n - p^k$ choices for the $(k+1)$th column, $p^n - p^{k+1}$ choices for the $(k+2)$th column, and so on, up to $p^n - p^{n-1}$ choices for the last column. Thus, in total there are $\prod_{i=k}^{n-1}(p^n - p^i)$ invertible matrices (i.e., automorphisms) which fix at least $\langle e_1, \ldots, e_k\rangle$. ■

Example 5 *In $\mathbb{Z}_3^3$, Lemma 11 tells us that the number of automorphisms which fix at least $\langle e_1\rangle$ is $(3^3-3^1)(3^3-3^2) = 432$. Similarly, the number of automorphisms which fix at least $\langle e_1, e_2\rangle$ is $(3^3-3^2) = 18$.*

We desire to subtract from the result of Lemma 11 the number of subgroups which fix not only $\langle e_1, \ldots, e_k\rangle$, but also other vectors in $\mathbb{Z}_p^n$. To do this, we need to know how many subgroups are of the form $\langle e_1, \ldots, e_k, a_1, \ldots, a_l\rangle$, where $\{e_1, \ldots, e_k, a_1, \ldots, a_l\}$ is a minimal generating set, $1 \leq k \leq n-1$, and $1 \leq l \leq n-k$.

Lemma 12 *The number of subgroups of $\mathbb{Z}_p^n$ of the form $\langle e_1, \ldots, e_k, a_1, \ldots, a_l\rangle$ for any $1 \leq k \leq n-1$ and any $1 \leq l \leq n-k$ is*

$$\sigma_n(k,l) = \prod_{i=0}^{l-1} \frac{(p^n - p^{k+i})}{(p^{k+l} - p^{k+i})} \tag{7}$$

PROOF: This proof mimics that of Lemma 10 above. Fix k and l, define $\mathbf{B}_n(k,l)$ as the collection of all ordered sets of $k+l$ linearly independent vectors containing $e_1,\ldots,e_k$, and define $\mathcal{S}_n(k,l)$ as the the collection of all subgroups of $\mathbb{Z}_p^n$ of the form $\langle e_1,\ldots,e_k,a_1,\ldots,a_l\rangle$, where $\{e_1,\ldots,e_k,a_1,\ldots,a_l\}$ is a minimal generating set. Consider the map $f:\mathbf{B}_n(k,l)\to\mathcal{S}_n(k,l)$ defined by $f(\{e_1,\ldots,e_k,a_1,\ldots,a_l\})=\text{span}\{e_1,\ldots,e_k,a_1,\ldots,a_l\}$. Each element of $\mathbf{B}_n(k,l)$ generates a subspace in $\mathcal{S}_n(k,l)$, so f maps $\mathbf{B}_n(k,l)$ into $\mathcal{S}_n(k,l)$, and each subspace in $\mathcal{S}_n(k,l)$ has a basis in $\mathbf{B}_n(k,l)$, so f is onto. For a given subspace H of the specified form, a basis of the given form must contain $e_1,\ldots,e_k$, but we may freely choose the remaining vectors $a_1,a_2,\ldots,a_l$ from those in H. There are $p^{k+l}-p^k$ choices for a_1, $p^{k+l}-p^{k+1}$ choices for a_2, and so on, up to $p^{k+l}-p^{k+l-1}$ choices for a_l. Hence, there are $\prod_{i=0}^{l-1}(p^{k+l}-p^{k+i})$ possible ordered bases of the given form for H.

The size of $\mathbf{B}_n(k,l)$ may be determined in a similar way. We construct any given element of $\mathbf{B}_n(k,l)$ by starting with $e_1,\ldots,e_k$ and choosing the remaining vectors $a_1,a_2,\ldots,a_l$. There are p^n-p^k choices for a_1, p^n-p^{k+1} choices for a_2, and so on, until there are p^n-p^{k+l-1} choices for a_l. Hence, there are $\prod_{i=0}^{l-1}(p^n-p^{k+i})$ ordered bases in $\mathbf{B}_n(k,l)$. Thus, the number of subgroups is

$$\sigma_n(k,l)=|\mathcal{S}_n(k,l)|=\frac{\prod_{i=0}^{l-1}(p^n-p^{k+i})}{\prod_{i=0}^{l-1}(p^{k+l}-p^{k+i})}=\prod_{i=0}^{l-1}\frac{(p^n-p^{k+i})}{(p^{k+l}-p^{k+i})}$$

as desired. ■

Example 6 *Continuing to work in $\mathbb{Z}_3^3$, we apply Lemma 14 to find that the number of subgroups of the form $\langle e_1,a_1\rangle$ is $\sigma_3(1,1)=(3^3-3)\ /\ (3^2-3)=4$. The number of subgroups of the form $\langle e_1,a_1,a_2\rangle$ is $\sigma_3(1,2)=(3^3-3)(3^3-3^2)\ /\ (3^3-3)(3^3-2)=1$ and the number of subgroups of the form $\langle e_1,e_2,a_1\rangle$ is $\sigma_3(2,1)=(3^3-3)\ /\ (3^3-3)=1$.*

We are now in a position to find the number of automorphisms whose fixed-point group is exactly $\langle e_1,\ldots,e_k\rangle$ (i.e., $|F^{-1}(\langle e_1,\ldots,e_k\rangle)|$. Since we know that $|F^{-1}(\langle e_1,\ldots,e_n\rangle)|=1$ (as only ι fixes the whole group), we use the above lemmas to compute $|F^{-1}(\langle e_1,\ldots,e_k\rangle)|$ recursively for each $1\le k\le n$.

Lemma 13 *For each $1\le k\le n-1$, in $\mathbb{Z}_p^n$,*

$$|F^{-1}(\langle e_1,\ldots,e_k\rangle)|=|\langle e_1,\ldots,e_k\rangle_F|-\sum_{l=1}^{n-k}(\sigma_n(k,l)\cdot|F^{-1}(\langle e_1,\ldots,e_{k+l}\rangle)|) \tag{8}$$

Also, $|F^{-1}(\langle e_1,\ldots,e_n\rangle)|=1$.

PROOF: Per the above discussion, $|F^{-1}(\langle e_1, \ldots, e_n \rangle)| = 1$. Now let $1 \leq k \leq n-1$. By definition, $|\langle e_1, \ldots, e_k \rangle_F|$ is the number of automorphisms which fix at least $\langle e_1, \ldots, e_k \rangle$. For each $1 \leq l \leq n-k$, $|F^{-1}(\langle e_1, \ldots, e_{k+l} \rangle)|$ is the number of automorphisms whose fixed-point group is exactly $\langle e_1, \ldots, e_{k+l} \rangle$. By Corollary 3, this count is equal to the number of automorphisms which fix any subgroup isomorphic to $\mathbb{Z}_p^{k+l}$, and there are $\sigma_n(k,l)$ such subgroups containing $e_1, \ldots, e_k$. So, $\sigma_n(k,l) \cdot |F^{-1}(\langle e_1, \ldots, e_{k+l} \rangle)|$ is the number of automorphisms which fix at least $e_1, \ldots, e_k$ and whose fixed-point group is of order p^{k+l}. Since we wish to subtract such automorphisms for each $1 \leq l \leq n-k$ from our initial count $|\langle e_1, \ldots, e_k \rangle_F|$, we obtain the desired formula. ■

Example 7 *From our previous examples, in* $\mathbb{Z}_3^3$, $|F^{-1}(\langle e_1, e_2 \rangle)| = |\langle e_1, e_2 \rangle_F| - \sum_{l=1}^{1}(\sigma_3(2,l) \cdot |F^{-1}(\langle e_1, \ldots, e_{2+l} \rangle)|) = 18 - (1 \cdot 1) = 17$. *Similarly,* $|F^{-1}(\langle e_1 \rangle)| = |\langle e_1 \rangle_F| - \sum_{l=1}^{2}(\sigma_3(1,l) \cdot |F^{-1}(\langle e_1, \ldots, e_{1+l} \rangle)|) = 432 - (4 \cdot 17 + 1 \cdot 1) = 363$.

Now that we know the values of N_k and $|F^{-1}(\langle e_1, \ldots, e_k \rangle)|$ for each $1 \leq k \leq n$, we are able to compute $\theta(\mathbb{Z}_p^n, p^k)$, as we shall do below. However, we must also find $\theta(\mathbb{Z}_p^n, 1)$, which requires the order of the automorphism group of $\mathbb{Z}_p^n$.

Theorem 13 *For any* $n \in \mathbb{N}$ *and prime* p, $|GL_n(\mathbb{Z}_p)| = \prod_{i=0}^{n-1}(p^n - p^i)$.

PROOF: Consider $\mathbb{Z}_p^n$ as a vector space over $\mathbb{Z}_p$, so that $\dim(\mathbb{Z}_p^n) = n$, and consider any ordered basis $\mathcal{B} = \{b_1, b_2, \ldots, b_n\}$. There are $p^n - 1$ choices for b_1, $p^n - p$ choices for b_2, and so on, up to $p^n - p^{n-1}$ choices for b_n. The number of possible ordered bases is then $\prod_{i=1}^{n}(p^n - p^{i-1})$. Let $M \in M_n(\mathbb{Z}_p)$ (the set of $n \times n$ matrices with entries from $\mathbb{Z}_p$). By the invertible matrix theorem, the columns of M form a basis for $\mathbb{Z}_p^n$ if and only if M is invertible. That is, the elements of $GL_n(\mathbb{Z}_p)$ are exactly those matrices whose columns form a basis for $\mathbb{Z}_p^n$ over $\mathbb{Z}_p$. Hence, $|GL_n(\mathbb{Z}_p)| = \prod_{i=0}^{n-1}(p^n - p^i)$, as desired. ■

Example 8 *In* $\mathbb{Z}_3^3$, $|GL_3(\mathbb{Z}_3)| = (3^3 - 3^0)(3^3 - 3^1)(3^3 - 3^2) = 11,232$.

Finally, we have all the tools necessary to compute the θ-values of $\mathbb{Z}_p^n$.

Theorem 14 *For any* $n \in \mathbb{N}$ *and prime* p,

$$\theta(\mathbb{Z}_p^n, p^k) = \begin{cases} |GL_n(\mathbb{Z}_p)| - \sum_{k=1}^{n}\theta(\mathbb{Z}_p^n, p^k) & \text{if } k = 0 \\ |F^{-1}(\langle e_1, \ldots, e_k \rangle)| \cdot N_k & \text{if } 1 \leq k \leq n \end{cases} \tag{9}$$

PROOF: Let $1 \leq k \leq n$ be given. Then $|F^{-1}(\langle e_1, \ldots, e_k \rangle)|$ gives the number of automorphisms which fix exactly any given subgroup of $\mathbb{Z}_p^n$ of order p^k, and there are N_k such subgroups. So, θ is as specified above. To obtain $\theta(\mathbb{Z}_p^n, 1)$, we simply subtract from the total number of automorphisms (namely, $|GL_n(\mathbb{Z}_p)|$) the number of automorphisms which fix more elements than the identity. ■

Example 9 *Continuing in* $\mathbb{Z}_3^3$, $\theta(\mathbb{Z}_3^3, 3^1) = 363 \cdot 13 = 4,719$. *Similarly,* $\theta(\mathbb{Z}_3^3, 3^2) = 17 \cdot 13 = 221$, $\theta(\mathbb{Z}_3^3, 3^3) = 1$ *(for only the identity fixes the whole group), and* $\theta(\mathbb{Z}_3^3, 3^0) = 11,232 - (4,719 + 221 + 1) = 6,291$.

As aforementioned, we may use Theorems 8 and 14 to compute θ values for groups of the form $\mathbb{Z}_{p_1}^{n_1} \times \mathbb{Z}_{p_2}^{n_2} \times \cdots \times \mathbb{Z}_{p^t}^{n_t}$ for distinct primes $p_1, \ldots, p_t$, per the below corollary.

Corollary 4 *If* $p_1, \ldots, p_t$ *are distinct primes,* $n_1, \ldots, n_t \in \mathbb{N}$, *and* $0 \leq m_i \leq n_i$ *for each* i, *then*

$$\theta(\mathbb{Z}_{p_1}^{n_1} \times \cdots \times \mathbb{Z}_{p^t}^{n_t}, p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}) = \prod_{i=1}^{t} \theta(\mathbb{Z}_{p_i}^{n_i}, p_i^{m_i}) \tag{10}$$

6 Conclusion

We have investigated the general properties of fixed points and determined θ-formulae for cyclic groups and elementary abelian groups. Moreover, we have proposed (but have not proved) the following θ-formula for groups of the form $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ (for p a prime):

Conjecture 1 *For* $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ *where* p *is any prime:*

$$\theta(\mathbb{Z}_p \times \mathbb{Z}_{p^2}, d) = \begin{cases} p^3(p-2)^2 \text{ for } d = 1 \\ p(2p^3 - 4p^2 + 1) \text{ for } d = p \\ p^3 - p - 1 \text{ for } d = p^2 \\ 1 \text{ for } d = p^3 \end{cases} \tag{11}$$

In this paper, we lay out two strategies for computing θ. The first is straightforward: find the general form of the fixed-point groups and count the automorphisms according to how many fixed points each has. The second approach is more indirect. Here, for each subgroup H of G, we count the number of automorphisms whose fixed-point group is H (often, this can be done by counting the number of automorphisms which fix at least H pointwise and then subtracting those which fix more than H). It follows then that for any $d \mid |G|$, $\theta(G, d)$ is the sum of these counts over all subgroups of order d. These approaches can potentially be applied to find θ-values for more classes of groups, such more general finite abelian groups (it is worth noting that in working toward a solution to general finite abelian groups, by Theorem 8, it suffices to consider finite abelian p-groups).

References

[1] D. Burton. *Elementary Number Theory* (5th ed.). New York: McGraw-Hill (2001).

[2] C.J Hillar and D.L. Rhea. *Automorphisms of Finite Abelian Groups*. Amer. Math. Monthly, **114** (2007), no. 10, 917–923.

[3] W.K. Nicholson. *Introduction to Abstract Algebra* (3rd ed.). Hoboken, NJ: John Wiley and Sons, Inc. (2007).

[4] Y. Yeh. *On Prime Power Abelian Groups*. Bull. Amer. Math. Soc., **54** (1948), 323-327.