Group Permutations which Preserve Subgroups

Veronica Marth* Greg Oman†

January 27, 2013

Abstract

Let G be a group, and let $f : G \to G$ be a bijection. Say that f *preserves subgroups* (of G) provided that for any subset $X \subseteq G$, X is a subgroup of G if and only if $f[X]$ (the image of X under f) is a subgroup of G. Let $\mathcal{S}(G)$ denote the set of all such functions f. It is easy to show that $\mathcal{S}(G)$ is a group under composition of functions. Further, if $Aut(G)$ is the group of automorphisms of G (again, under composition), then $Aut(G)$ is a subgroup of $\mathcal{S}(G)$. In this note, we study the structure and the size of $\mathcal{S}(G)$, relative to $Aut(G)$, for various groups G. In particular, we show that the disparity in size can be minimal, moderate, or as large as possible (in a sense to be made precise). Finally, we determine all groups G up to isomorphism for which $Aut(G) = \mathcal{S}(G)$.

1 Introduction

Let G and H be groups, and suppose that $f : G \to H$ is a surjective group homomorphism with kernel K. It is well-known (often as "The First Isomorphism Theorem") that the map $\overline{f} : G/K \to H$ defined by $\overline{f}(\overline{g}) := f(g)$ is an isomorphism between G/K and H. Moreover, f induces a one-to-one inclusion-preserving correspondence between the subgroups of G containing K and the subgroups of H via the map $L \mapsto f[L]$ (which is often referred to as "The Correspondence Theorem"). We refer the reader to Corollary 5.7 and Theorem 5.11 of Hungerford [2] for proofs. In the special case where $G = H$ and f is an automorphism (i.e. $K = \{e\}$), The Correspondence Theorem asserts that f induces a permutation of the subgroups of G. In other words, if $X \subseteq G$, then X is a subgroup of G if and only if $f[X] := \{f(x) : x \in X\}$ is a subgroup of G.

In this note, we consider permutations of a group G which have the aforementioned property; that is, we study bijective functions $f : G \to G$ which permute the subgroups of G. Let us say that a bijective map $f : G \to G$ *preserves subgroups* if f has the property that for any subset $X \subseteq G$, X is a subgroup of G if and only if $f[X]$ is a subgroup of G. Let $\mathcal{S}(G)$ denote the set of all functions which preserve the subgroups of G, and let $Aut(G)$ denote the

*(undergraduate) University of Colorado, Colorado Springs
†University of Colorado, Colorado Springs

set of all automorphisms of G. Then both $\mathcal{S}(G)$ and $Aut(G)$ become groups under composition of functions. It follows from the remarks made in the previous paragraph that $Aut(G)$ is a subgroup of $\mathcal{S}(G)$. Thus, in a sense, $\mathcal{S}(G)$ generalizes $Aut(G)$.

Another way of viewing $\mathcal{S}(G)$ is as follows: Let G be a group and let $\mathcal{L}(G)$ denote the set of subgroups of G, partially ordered by set-theoretic inclusion. It is well-known that $(\mathcal{L}(G), \subseteq)$ is a *lattice*. In particular, the least upper bound (join) of subgroups H and K of G is $\langle H, K\rangle$ (the subgroup generated by H and K) and the greatest lower bound (meet) of H and K is $H \cap K$. The set $\mathcal{S}(G)$ is then the set of all permutations f of G which induce a *lattice automorphism* $\overline{f}$ of $\mathcal{L}(G)$ (also called an *autoprojectivity*). In other words, $\mathcal{S}(G)$ consists of all permutations f of G for which the map $\overline{f}$ defined by $\overline{f}(H) := f[H]$ is a permutation of $\mathcal{L}(G)$ with the property (which is inherited automatically by the definition of $\overline{f}$) that for all subgroups H and K of G, $H \subseteq K$ if and only if $\overline{f}(H) \subseteq \overline{f}(K)$. A remark on perspective is now in order. While a lattice theorist may consider maps whose domain is *the set of subgroups* of a given group, we consider maps whose domain is *the group itself*. This difference in perspective will be highlighted in the next section.

The purpose of this paper is to compare $Aut(G)$ and $\mathcal{S}(G)$ for a small class of well-studied groups G. We will showcase a wide range of variance in size and structure between $Aut(G)$ and $\mathcal{S}(G)$. For example, we will show that while $Aut(\mathbb{Z})$ has cardinality 2, $\mathcal{S}(\mathbb{Z})$ has cardinality $2^{\aleph_0}$. On the other hand, there are infinitely many groups G (up to isomorphism) for which $Aut(G)$ and $\mathcal{S}(G)$ coincide. We conclude the paper by determining all such groups.

We close the introduction by commenting on notation. For $m \in \mathbb{Z}$, we denote the cyclic subgroup of $\mathbb{Z}$ generated by m by $m\mathbb{Z}$. Now let n be a positive integer. The symmetric group on n elements (that is, the group of permutations of a set of n elements) will be denoted, as usual, by S_n. We let $\mathbb{Z}/n\mathbb{Z}$ denote the cyclic group of order n. The multiplicative group of units of $\mathbb{Z}/n\mathbb{Z}$ will be denoted by $(\mathbb{Z}/n\mathbb{Z})^*$. Finally, if G is a group, then (as above) $\mathcal{L}(G)$ will denote the lattice of subgroups of G, ordered by inclusion. Finally, the set of all nonnegative integers will be denoted by $\mathbb{Z}^{\geq 0}$ (we prefer this notation to $\mathbb{N}$ as not all authors include 0 as a member of $\mathbb{N}$).

2 $\mathbb{Z}/p^n\mathbb{Z}$

We begin our comparison of $Aut(G)$ and $\mathcal{S}(G)$ by analyzing the cyclic groups $\mathbb{Z}/p^n\mathbb{Z}$, where p is a prime and n is a positive integer. From a lattice-theoretic point of view, such groups are particularly simple. In fact, they are precisely the nontrivial finite groups whose subgroup lattices are linearly ordered (see Lotto [3] for a proof of this fact). Lagrange's Theorem implies that every subgroup of $\mathbb{Z}/p^n\mathbb{Z}$ has order p^i for some i satisfying $0 \leq i \leq n$. Moreover, for each i with $0 \leq i \leq n$, $\mathbb{Z}/p^n\mathbb{Z}$ has a *unique* (cyclic) subgroup of order p^i. To wit, $\langle \overline{p^{n-i}} \rangle$ has order p^i. Uniqueness follows immediately from the fact that the subgroups of $\mathbb{Z}/p^n\mathbb{Z}$ are linearly ordered.

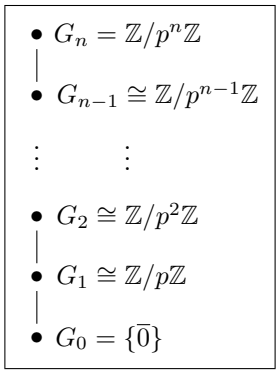

Figure 1. *The subgroup lattice of* $\mathbb{Z}/p^n\mathbb{Z}$

It is easy to see that the only *lattice automorphism* of $\mathbb{Z}/p^n\mathbb{Z}$ is the identity map (that is, the only bijection $f : \mathcal{L}(\mathbb{Z}/p^n\mathbb{Z}) \to \mathcal{L}(\mathbb{Z}/p^n\mathbb{Z})$ which preserves inclusion is the identity function). However, the structure of $Aut(\mathbb{Z}/p^n\mathbb{Z})$ and, more generally, of $\mathcal{S}(\mathbb{Z}/p^n\mathbb{Z})$, is much more interesting.

Theorem 1. *Let p be a prime, and let n be a positive integer. Then*
(*a*) $Aut(\mathbb{Z}/p^n\mathbb{Z}) \cong (\mathbb{Z}/p^n\mathbb{Z})^*$, *and*
(*b*) $\mathcal{S}(\mathbb{Z}/p^n\mathbb{Z}) \cong S_{p-1} \times S_{p^2-p} \times S_{p^3-p^2} \times \cdots \times S_{p^{n-1}-p^{n-2}} \times S_{p^n-p^{n-1}}$.

Proof. We assume that p is a prime and that n is a positive integer.

(a): This assertion is well-known; we refer the reader to p. 301 of [2].

(b): Let $f \in \mathcal{S}(\mathbb{Z}/p^n\mathbb{Z})$ be arbitrary. Recall that for each i with $0 \leq i \leq n$, G_i (notation as in Figure 1) is the *unique* subgroup of $\mathbb{Z}/p^n\mathbb{Z}$ of order p^i. It follows that $f[G_i] = G_i$ for each i. When $i = 0$, this implies that $f(\overline{0}) = \overline{0}$. Now fix an i with $1 \leq i \leq n$. Since $f[G_{i-1}] = G_{i-1}$, $f[G_i] = G_i$, $G_{i-1} \subseteq G_i$, and since f is one-to-one, we deduce that $f[G_i - G_{i-1}] = G_i - G_{i-1}$. Thus f permutes $G_i - G_{i-1}$. Conversely, if $g : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ satisfies $f(\overline{0}) = \overline{0}$ and permutes $G_i - G_{i-1}$ for each i, $1 \leq i \leq n$, then it is readily checked that $g \in \mathcal{S}(\mathbb{Z}/p^n\mathbb{Z})$.

Now define the map $\varphi : \mathcal{S}(\mathbb{Z}/p^n\mathbb{Z}) \to S_{p-1} \times S_{p^2-p} \times S_{p^3-p^2} \times \cdots \times S_{p^n-p^{n-1}}$ by $\varphi(f) : (f|G_1 - G_0, f|G_2 - G_1, f|G_3 - G_2, \ldots, f|G_n - G_{n-1})$. One verifies easily that φ is a group isomorphism. This completes the proof. □

Corollary 1. *Let p be a prime and n be a positive integer. Then:*
(*a*) $|Aut(\mathbb{Z}/p^n\mathbb{Z})| = \varphi(p^n) = p^n - p^{n-1}$, *where φ is the Euler phi function (totient function).*
(*b*) $|\mathcal{S}(\mathbb{Z}/p^n\mathbb{Z})| = \prod_{i=1}^{n}(p^i - p^{i-1})!$.
(*c*) $\lim_{n\to\infty} \frac{|Aut(\mathbb{Z}/p^n\mathbb{Z})|}{|\mathcal{S}(\mathbb{Z}/p^n\mathbb{Z})|} = 0$.
(*d*) *If $G \cong \mathbb{Z}/n\mathbb{Z}$ for $n = 1, 2, 3,$ or 4, then $Aut(G) = \mathcal{S}(G)$.*

Proof. Assertion (a) is well-known (see Herstein [1], p. 31) and (b) is immediately implied by Theorem 1. Claim (c) follows easily from (a) and (b), and (d)

is deduced from the fact (which is easily checked using (a) and (b)) that if either $p = 2, 3$, and $n = 1$, or if $p = 2$ and $n = 2$, then $|Aut(\mathbb{Z}/p^n\mathbb{Z})| = |\mathcal{S}(\mathbb{Z}/p^n\mathbb{Z})|$. Recall from the Introduction that $Aut(G) \subseteq \mathcal{S}(G)$ for every group G. Since $|Aut(\mathbb{Z}/p^n\mathbb{Z})| = |\mathcal{S}(\mathbb{Z}/p^n\mathbb{Z})|$ for the above values of p and n, we conclude that $Aut(\mathbb{Z}/p^n\mathbb{Z}) = \mathcal{S}(\mathbb{Z}/p^n\mathbb{Z})$ □

3 $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

In the previous section, we computed the orders of $Aut(G)$ and $\mathcal{S}(G)$ where G is a nontrivial finite group for which any two subgroups of G compare with respect to $\subseteq$. In this section, we study the groups $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Whereas any two subgroups of $\mathbb{Z}/p^n\mathbb{Z}$ compare under $\subseteq$, if H and K are subgroups of $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, then $H \subsetneq K$ if and only if either $H = \{0\}$ or $K = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Thus there is a sort of dichotomy between the subgroup lattice of $\mathbb{Z}/p^n\mathbb{Z}$ and the subgroup lattice of $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ in the sense that $\mathbb{Z}/p^n\mathbb{Z}$ has a maximum of containment relations whereas $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ has a minimum. We investigate this dichotomy relative to the orders of $Aut(G)$ and $\mathcal{S}(G)$. We begin with the following (well-known) lemma, which will enable us to completely determine the structure of the subgroup lattice of $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Lemma 1. *Let p be a prime. There are exactly $p+1$ subgroups of $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ of order p.*

Proof. Let $G_1, G_2, \ldots, G_k$ be the subgroups of $G := \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ of order p, and let $0 := (\overline{0}, \overline{0})$ be the identity of G. Every non-identity element of G has order p, whence belongs to G_i for some i. We deduce that

$$G = (G_1 - \{0\}) \cup (G_2 - \{0\}) \cup \cdots \cup (G_k - \{0\}) \cup \{0\} \tag{1}$$

Moreoever, any two distinct subgroups of G of order p intersect trivially (that is, their intersection is $\{0\}$). It follows that the sets on the right side of the equals sign in (1) above are pairwise-disjoint. Taking the cardinality of both sides of the equation, we get:

$$p^2 = k(p-1) + 1 \tag{2}$$

Solving for k yields $k = p + 1$. □

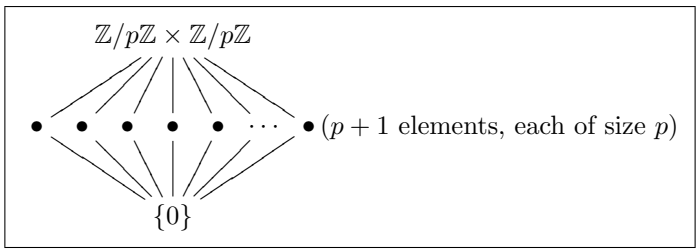

Figure 2. *The subgroup lattice of* $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

With this information in hand, we determine the sizes of $Aut(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})$ and $\mathcal{S}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})$.

Theorem 2. *Let p be a prime, let n be a positive integer, and set $G := \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Then:*
(a) $|Aut(G)| = p(p+1)(p-1)^2$*, and*
(b) $|\mathcal{S}(G)| = (p+1)!((p-1)!)^{p+1}$.

Proof. We let p, n, and G be as defined above.

(a): An automorphism f of G is completely determined by its action on $(\overline{1}, \overline{0})$ and $(\overline{0}, \overline{1})$. The map f can send $(\overline{1}, \overline{0})$ to any nonzero element of G. Thus there are $p^2 - 1$ ways to choose $f((\overline{1}, \overline{0}))$. Once $f((\overline{1}, \overline{0}))$ has been chosen, $f((\overline{0}, \overline{1}))$ can be chosen to be any element not in the subgroup generated by $f((\overline{1}, \overline{0}))$. Hence there are $p^2 - p$ was to choose $f((\overline{0}, \overline{1}))$. It follows that $|Aut(G)| = (p^2-1)(p^2-p) = p(p+1)(p-1)^2$.

(b): Let $G_1, G_2, \ldots, G_{p+1}$ be the subgroups of G of order p. Any element $f \in \mathcal{S}(G)$ must map 0 to 0 and induce a permutation of the set $\{G_1 - \{0\}, G_2 - \{0\}, \ldots, G_{p+1} - \{0\}\}$ (and conversely, any map with these properties is an element of $\mathcal{S}(G)$). Fix an arbitrary $f^* \in S_{p+1}$. For $1 \leq j \leq p+1$, there are exactly $(p-1)!$ bijections between $G_j - \{0\}$ and $G_{f^*(j)} - \{0\}$. Thus there are $((p-1)!)^{p+1}$ permutations of G which map 0 to 0 and induce a bijection between $G_i - \{0\}$ and $G_{f^*(i)} - \{0\}$ for each i, $1 \leq i \leq p+1$. Since $|S_{p+1}| = (p+1)!$, (b) follows. □

The following corollary is immediate.

Corollary 2. [1] $\lim_{p\to\infty} \frac{|Aut(\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z})|}{|\mathcal{S}(\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z})|} = 0$.

Remark 1 Corollary 1 and Corollary 2 state that $\lim_{n\to\infty} \frac{|Aut(\mathbb{Z}/p^n\mathbb{Z})|}{|\mathcal{S}(\mathbb{Z}/p^n\mathbb{Z})|} = 0$ and $\lim_{p\to\infty} \frac{|Aut(\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z})|}{|\mathcal{S}(\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z})|} = 0$. One might surmise that, more generally, $\lim_{|G|\to\infty} \frac{|Aut(G)|}{|\mathcal{S}(G)|} = 0$, where G denotes a finite group. However, it follows from the results in the final section that $\lim_{|G|\to\infty} \frac{|Aut(G)|}{|\mathcal{S}(G)|}$ does not exist.

Remark 2 Invoking the Sylow Theorems, it is possible to determine $|\mathcal{S}(G)|$ for any group G of cardinality pq, where p and q are prime. However, we will not present such a calculation in this note.

[1] In this limit, we let p approach infinity *through the primes*.

4 $\mathbb{Z}$

In this section, we analyze the groups $Aut(\mathbb{Z})$ and $\mathcal{S}(\mathbb{Z})$. Our reasons for considering the group $(\mathbb{Z}, +)$ are threefold. First, it allows to present a study of an infinite group. Second, the disparity in size between $Aut(\mathbb{Z})$ and $\mathcal{S}(\mathbb{Z})$ is as large as possible (in a sense to be made precise shortly). Lastly, both $Aut(\mathbb{Z})$ and $\mathcal{S}(\mathbb{Z})$ have particularly elegant characterizations. We begin by describing $\mathcal{S}(\mathbb{Z})$.

Theorem 3. *Let $f : \mathbb{Z} \to \mathbb{Z}$. Then $f \in \mathcal{S}(\mathbb{Z})$ if and only if the following hold:*
(a) f is an odd function (that is, $f(-m) = -f(m)$ for every $m \in \mathbb{Z}$), and
(b) $|f|$ is an automorphism of $(\mathbb{Z}^{\geq 0}, \cdot)$ (that is, if one restricts the domain of $|f|$ to $\mathbb{Z}^{\geq 0}$, then $|f|$ is bijective and satisfies $|f|(xy) = |f|(x) \cdot |f|(y)$ for all $x, y \in \mathbb{Z}^{\geq 0}$).

Proof. Let $f : \mathbb{Z} \to \mathbb{Z}$ be a function. We assume first that $f \in \mathcal{S}(\mathbb{Z})$. Thus for every subset $X \subseteq \mathbb{Z}$, X is a subgroup of $\mathbb{Z}$ if and only if $f[X]$ is a subgroup of $\mathbb{Z}$. Let $a, b \in \mathbb{Z}$ be arbitrary. We claim:

$$\text{If } f[a\mathbb{Z}] = b\mathbb{Z}, \text{ then } f(a) = b \text{ or } f(-a) = b. \tag{3}$$

To see this, assume that $f[a\mathbb{Z}] = b\mathbb{Z}$. Suppose first that $a = 0$. Since f maps subgroups to subgroups, we see that $f(0) = 0$. Since $f[a\mathbb{Z}] = b\mathbb{Z}$, clearly $b = 0$, and we are done in this case. Thus we assume that $a \neq 0$. Since $f[a\mathbb{Z}] = b\mathbb{Z}$, there exists some $m \in \mathbb{Z}$ such that $f(am) = b$. It follows that f maps $(am)\mathbb{Z}$ onto a subgroup of $\mathbb{Z}$ containing b. Hence

$$b\mathbb{Z} \subseteq f[(am)\mathbb{Z}] \subseteq f[a\mathbb{Z}] = b\mathbb{Z}. \tag{4}$$

We deduce that $f[(am)\mathbb{Z}] = f[a\mathbb{Z}]$. Since f is one-to-one, it follows that $(am)\mathbb{Z} = a\mathbb{Z}$. Since $a \neq 0$, we conclude that $m = \pm 1$. Recalling above that $f(am) = b$, (3) is established.

We now establish (a). Let $a \in \mathbb{Z}$ be arbitrary. We must show that $f(-a) = -f(a)$. If $a = 0$, then (since $f(0) = 0$) the result is patent. So assume that $a \neq 0$. As above, since f preserves subgroups, $f[a\mathbb{Z}] = b\mathbb{Z}$ for some $b \in \mathbb{Z}$. By (3), either $f(a) = b$ or $f(-a) = b$. Suppose first that $f(a) = b$. Note that $(-b)\mathbb{Z} = b\mathbb{Z}$. Thus $f[a\mathbb{Z}] = (-b)\mathbb{Z}$. We deduce from (3) again that $f(a) = -b$ or $f(-a) = -b$. Since $f(a) = b$, $a \neq 0$, $f(0) = 0$, and f is one-to-one, we see that $f(a) = -b$ is impossible. Thus $f(-a) = -b = -f(a)$. The case where $f(-a) = b$ is proved analogously, and is omitted.

As for (b), we first show that $|f|$ is one-to-one on $\mathbb{Z}^{\geq 0}$. Thus assume that $|f|(x) = |f|(y)$ and that $x, y \geq 0$. We will show that $x = y$. Since $|f|(x) = |f|(y)$, it follows by definition of $|f|$ that $|f(x)| = |f(y)|$. We deduce that $f(x) = \pm f(y)$. Suppose first that $f(x) = f(y)$. Since f is injective, we see that $x = y$, as required. Now suppose that $f(x) = -f(y)$. Recall from (a) that f is odd. Thus $f(x) = -f(y) = f(-y)$ As f is injective, we obtain $x = -y$. But since $x \geq 0$ and $y \geq 0$, it follows that $x = y = 0$. We have shown that $|f|$ is injective on $\mathbb{Z}^{\geq 0}$. We now show that $|f|$ (with restricted domain $\mathbb{Z}^{\geq 0}$) is onto $\mathbb{Z}^{\geq 0}$. Indeed,

let $n \geq 0$ be arbitrary. Since f is surjective, there exists some $x \in \mathbb{Z}$ such that $f(x) = n$. If $x \geq 0$, we are done. So suppose that $x < 0$. Then $-x > 0$ and since f is odd, $f(-x) = -f(x) = -n$. We conclude that $|f|(-x) = n$, and $|f|$ is onto.

We now work toward showing that $|f|$ preserves multiplication in $\mathbb{Z}^{\geq 0}$. To do this, we note the following simple but important observation (noted in the introduction):

(*) For any subgroups H and K of $\mathbb{Z}$, $H \subseteq K$ if and only if $f[H] \subseteq f[K]$.

We use (*) to establish the following:

$$\text{For any prime } p, f[p\mathbb{Z}] = q\mathbb{Z} \text{ for some prime } q. \tag{5}$$

To wit, let p be a prime. Then $p\mathbb{Z}$ is a maximal subgroup of $\mathbb{Z}$. By (*), we conclude that $f[p\mathbb{Z}]$ is a maximal subgroup of $\mathbb{Z}$, whence $f[p\mathbb{Z}] = q\mathbb{Z}$ for some prime q. We now prove:

$$\text{If } p \text{ and } q \text{ are primes and } f[p\mathbb{Z}] = q\mathbb{Z}, \text{ then for all } n > 0, f[p^n\mathbb{Z}] = q^n\mathbb{Z}. \tag{6}$$

To prove (6), we assume that $f[p\mathbb{Z}] = q\mathbb{Z}$ for some primes p and q and we let $n > 0$ be arbitrary. Note trivially that

$$p^n\mathbb{Z} \subseteq p\mathbb{Z}. \tag{7}$$

Now suppose that p' is any prime such that $p^n\mathbb{Z} \subseteq p'\mathbb{Z}$. Then since $p'|p^n$ and p, p' are prime, we deduce that $p' = p$. We conclude that $p^n\mathbb{Z}$ is contained in a *unique* maximal subgroup of $\mathbb{Z}$ (namely $p\mathbb{Z}$). Invoking (*) above, we deduce that $f[p^n\mathbb{Z}]$ is contained in a unique maximal subgroup of $\mathbb{Z}$. But then $f[p^n\mathbb{Z}] = p_1^m\mathbb{Z}$ for some prime prime p_1 and positive integer m. Note that there are exactly $n+1$ subgroups of $\mathbb{Z}$ which contain $p^n\mathbb{Z}$ and exactly $m+1$ subgroups of $\mathbb{Z}$ which contain $p_1^m\mathbb{Z}$. We invoke (*) yet again to conclude that $n+1 = m+1$, and thus $n = m$. So we now have $f[p^n\mathbb{Z}] = p_1^n\mathbb{Z}$. It remains to show that $p_1 = q$. Recall from (7) above that $p^n\mathbb{Z} \subseteq p\mathbb{Z}$. Applying f, we obtain $p_1^n\mathbb{Z} = f[p^n\mathbb{Z}] \subseteq f[p\mathbb{Z}] = q\mathbb{Z}$. Thus $p_1^n\mathbb{Z} \subseteq q\mathbb{Z}$. This implies that $q|p_1^n$. Since p_1 and q are prime, it follows that $p_1 = q$, as required.

Finally, we are able to show that $|f|$ preserves multiplication in $\mathbb{Z}^{\geq 0}$. As $f(0) = 0$, also $|f|(0) = 0$. Since $f[\mathbb{Z}] = \mathbb{Z}$, it follows from (3) that $f(1) = 1$ or $f(-1) = 1$. In any case, since f is odd, we infer that $|f|(1) = 1$. Now let $n > 1$ with prime factorization $n = p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$. It suffices to show that $|f|(n) = (|f|(p_1))^{m_1}(|f|(p_2))^{m_2}\cdots(|f|(p_k))^{m_k}$. For each i, (by (5)) $f[p_i\mathbb{Z}] = q_i\mathbb{Z}$ for some prime q_i. Now simply observe that $f[n\mathbb{Z}] = f[p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}\mathbb{Z}] = f[p_1^{m_1}\mathbb{Z}\cap p_2^{m_2}\mathbb{Z}\cap\cdots\cap p_k^{m_k}\mathbb{Z}] = f[p_1^{m_1}\mathbb{Z}]\cap f[p_2^{m_2}\mathbb{Z}]\cap\cdots\cap f[p_k^{m_k}\mathbb{Z}] = $ (by (6)) $q_1^{m_1}\mathbb{Z}\cap q_2^{m_2}\mathbb{Z}\cdots\cap q_k^{m_k}\mathbb{Z} = q_1^{m_1}q_2^{m_2}\cdots q_k^{m_k}\mathbb{Z}$. Since $f[p_i\mathbb{Z}] = q_i\mathbb{Z}$ and f is odd, we conclude from (3) that $|f|(p_i) = q_i$. Analogously, since $f[n\mathbb{Z}] = q_1^{m_1}q_2^{m_2}\cdots q_k^{m_k}\mathbb{Z}$,

we deduce that $|f|(n) = q_1^{m_1} q_2^{m_2} \cdots q_k^{m_k} = (|f|(p_1))^{m_1} (|f|(p_2))^{m_2} \cdots (|f|(p_k))^{m_k}$. This completes the proof of the first implication.

Conversely, suppose that $f : \mathbb{Z} \to \mathbb{Z}$ satisfies (a) and (b). We will show that $f \in \mathcal{S}(\mathbb{Z})$. We first record the following useful observation:

$$|f|(x) = |f|(|x|) \text{ for all } x \in \mathbb{Z}. \tag{8}$$

To verify (8), we let $x \in \mathbb{Z}$ be arbitrary. Note that $|f|(-x) = |f(-x)| = |-f(x)| = |f(x)| = |f|(x)$. Thus $|f|(x) = |f|(|x|)$, and (8) is established. We use this observation to prove that f is injective. So suppose that $f(x) = f(y)$. Then (8) yields $|f|(|x|) = |f|(|y|)$. Since $|f|$ is an automorphism of $(\mathbb{Z}^{\geq 0}, \cdot)$, we deduce that $|x| = |y|$. Thus $x = \pm y$. If $x = y$, we have what we want. Thus suppose that $x = -y$. Then $f(y) = f(x) = f(-y) = -f(y)$. We conclude that $2f(y) = 0$, and thus $f(y) = 0$. But then $|f|(y) = 0$. Since $|f|$ is an automorphism of $(\mathbb{Z}^{\geq 0}, \cdot)$, we see that $y = 0$. Thus $x = y = 0$ and f is injective. To show that f is onto, let $m \in \mathbb{Z}$ be arbitrary. Since $|f|$ is an automorphism of $(\mathbb{Z}^{\geq 0}, \cdot)$, there is some $n \geq 0$ such that $|f|(n) = |m|$. Thus $f(n) = \pm m$. Since f is odd, we deduce that either $f(n) = m$ or $f(-n) = m$, and f is onto. Lastly, we must show that f preserves subgroups. Toward this end, let $a \geq 0$. We claim that $f[a\mathbb{Z}] = f(a)\mathbb{Z}$. We first show that $f[a\mathbb{Z}] \subseteq f(a)\mathbb{Z}$. Let $m \in \mathbb{Z}$ be arbitrary. Then (by (8)) $|f(am)| = |f|(a|m|) =$ (since $|f|$ is an automorphism of $(\mathbb{Z}^{\geq 0}, \cdot)$) $|f|(a)|f|(|m|) = |f(a)f(|m|)|$. Thus $f(am) = \pm f(a)f(|m|)$. In any case, $f(am) \in f(a)\mathbb{Z}$, and $f[a\mathbb{Z}] \subseteq f(a)\mathbb{Z}$. Analogously, one proves that $f(a)\mathbb{Z} \subseteq f[a\mathbb{Z}]$. Finally, we suppose that $X \subseteq \mathbb{Z}$ and that $f[X] = b\mathbb{Z}$ for some $b \geq 0$. We must show that X is a subgroup of $\mathbb{Z}$. We first claim that f^{-1} is odd. To wit, let $x \in \mathbb{Z}$ be arbitrary. Then since f is odd, we see that $-x = f(f^{-1}(-x)) = f(-f^{-1}(x))$. As f is one-to-one, we deduce that $f^{-1}(-x) = -f^{-1}(x)$ and f^{-1} is odd. It is now straightforward to show that $|f|^{-1} = |f^{-1}|$ on $\mathbb{Z}^{\geq 0}$ (of course, $|f|$ is *not* one-to-one on $\mathbb{Z}$, but it *is* one-to-one on $\mathbb{Z}^{\geq 0}$, whence has an inverse on $\mathbb{Z}^{\geq 0}$). We conclude that f^{-1} satisfies conditions (a) and (b). Recall again that $f[X] = b\mathbb{Z}$. Applying f^{-1}, we conclude that $X = f^{-1}[b\mathbb{Z}]$. But since f^{-1} satisfies (a) and (b), it follows (by what we just proved above) that $f^{-1}[b\mathbb{Z}] = f^{-1}(b)\mathbb{Z}$, and hence X is a subgroup of $\mathbb{Z}$. This completes the proof. □

We finish this section with a corollary. Before stating the corollary, a few remarks are in order. First, every group G of order greater than 2 (finite or not) possesses a non-identity automorphism (this is a very well-known result). We give a quick sketch of the argument. Let G be a group with $|G| > 2$. If G is nonabelian, choose any $a \in G$ not in the center. Then the *inner automorphism* $f_a : G \to G$ given by $f_a(x) := axa^{-1}$ is not the identity map. Now suppose that G is abelian (we switch to additive notation). If there exists an element of G of order greater than 2, then the map $f : G \to G$ defined by $f(g) := -g$ is a nonidentity automorphism of G. Lastly, assume that $2G = \{0\}$, and let β be a basis for G as a vector space over $\mathbb{Z}/2\mathbb{Z}$. Choose a nonidentity permutation $f : \beta \to \beta$. Then f extends by linearity (as a vector space over $\mathbb{Z}/2\mathbb{Z}$) to a

non-identity vector space (hence additive) automorphism of G. We now present our corollary.

Corollary 3. *$|Aut(\mathbb{Z})| = 2$ (whence $Aut(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$) and $|\mathcal{S}(\mathbb{Z})| = 2^{\aleph_0}$. Thus $Aut(\mathbb{Z})$ is as small as possible and $\mathcal{S}(\mathbb{Z})$ is as large as possible.*

Proof. It is easy to show that the only automorphisms of $\mathbb{Z}$ are $x \mapsto x$ and $x \mapsto -x$. This establishes the first assertion (and so by the comments preceding this corollary, $Aut(\mathbb{Z})$ is as small as possible). As for the second, let $\mathcal{P}$ be the set of primes, and let $S \subseteq \mathcal{P}$, $|S| > 1$. Let $f : \mathcal{P} \to \mathcal{P}$ be a function which permutes S and which moves every element of S, yet fixes every element of $\mathcal{P} - S$. Then one may extend f to a function $\overline{f}$ on $\mathbb{Z}^{\geq 0}$ by defining $\overline{f}(0) = 0$, $\overline{f}(1) = 1$, and for primes $p_1, p_2, \ldots, p_k$, $\overline{f}(p_1 p_2 \cdots p_k) := f(p_1)f(p_2)\cdots f(p_k)$. Now extend $\overline{f}$ to $\mathbb{Z}$ by setting $\overline{f}(-n) = -\overline{f}(n)$. One verifies at once that $\overline{f} \in \mathcal{S}(\mathbb{Z})$ and that distinct subsets (of size larger than 1) of the primes give rise to distinct such functions. This shows that $|\mathcal{S}(\mathbb{Z})| \geq 2^{\aleph_0}$. But since there are exactly $2^{\aleph_0}$ functions $f : \mathbb{Z} \to \mathbb{Z}$, we see that $|\mathcal{S}(\mathbb{Z})| = 2^{\aleph_0}$, and thus $\mathcal{S}(\mathbb{Z})$ is as large as possible. □

5 Which Groups G Satisfy $Aut(G) = \mathcal{S}(G)$?

In the previous three sections, we studied groups which showcase the disparity in size which can occur between $Aut(G)$ and $\mathcal{S}(G)$. In this section, we change gears and determine all groups G (up to isomorphism) for which this disparity is nonexistent. Said another way, we find all groups G for which $Aut(G) = \mathcal{S}(G)$. These are the groups G for which every permutation of G which permutes the subgroups of G is necessarily an automorphism of G.

Theorem 4. *Let G be a group. Then $Aut(G) = \mathcal{S}(G)$ if and only if either G is cyclic of order at most 4 or G is an elementary abelian 2-group (that is, $g + g = 0$ for all $g \in G$).*

Proof. Let G be a group for which $Aut(G) = \mathcal{S}(G)$. We claim that every $g \in G$ has order at most 4. Thus suppose that $g \in G$ and $|g| > 3$. It suffices to show that $|g| = 4$. Define $f : G \to G$ by $f(g) := g^{-1}$, $f(g^{-1}) := g$, and $f(x) := x$ for $x \notin \{g, g^{-1}\}$. One checks easily that $f \in \mathcal{S}(G)$ and thus f is an automorphism of G. Since g has order greater than 3, we see that $g^2 \neq g$ and $g^2 \neq g^{-1}$. So by definition of f, we get $f(g^2) = g^2$. On the other hand, f is an automorphism. Thus $f(g^2) = f(g)f(g) = g^{-2}$. We deduce that $g^2 = g^{-2}$, and so $g^4 = e$. Suppose now that $g \in G$ and $|g| > 2$. We claim that $G = \langle g \rangle$. To see this, suppose by way of contradiction that there exists $h \in G - \langle g \rangle$. Again, we define $f : G \to G$ by $f(g) := g^{-1}$, $f(g^{-1}) := g$, and $f(x) := x$ for $x \notin \{g, -g\}$. Then as above, $f \in \mathcal{S}(G)$. It follows that $f \in Aut(G)$. Since $h \notin \langle g \rangle$, we see that $gh \neq g$ and $gh \neq g^{-1}$. Thus $f(gh) = gh$. On the other hand, $f(gh) = f(g)f(h) = g^{-1}h$. We conclude that $g = g^{-1}$, and hence $g^2 = e$. But this contradicts $|g| > 2$, and hence $G = \langle g \rangle$. We have shown that either every nonidentity element of G has

order 2 (hence G is abelian) or G is cyclic of order at most 4. This proves the first implication.

Suppose now that G is cyclic of order at most 4. Then it follows from Corollary 1 that $Aut(G) = \mathcal{S}(G)$. Finally, assume that G is an elementary abelian 2-group. We must prove that $Aut(G) = \mathcal{S}(G)$. Let $f \in \mathcal{S}(G)$ be arbitrary. We will show that f is an automorphism of G (we switch to additive notation). Toward this end, let $g, h \in G$ be arbitrary. We must establish that $f(g + h) = f(g) + f(h)$. If either $g = 0$ or $h = 0$, the result is patent since $f(0) = 0$. Further, if $g = h$, then the result also follows from the facts that $f(0) = 0$ and $2x = 0$ for all $x \in G$. So we may assume that $0, g$, and h are all distinct. $H := \{0, g, h, g + h\}$ is a subgroup of G. Since f preserves subgroups, $f[H] = \{f(0), f(g), f(h), f(g + h)\}$ is also a subgroup of G. Again, recall that $f(0) = 0$, whence $f[H] = \{0, f(g), f(h), f(g+h)\}$. Consider $f(g)+f(h) \in f[H]$. If $f(g) + f(h) = 0$, then $f(g) = -f(h) = f(h)$. Since f is injective, $g = h$, a contradiction. If $f(g) + f(h) = f(g)$, then $f(h) = 0$. Since $f(0) = 0$ and f is injective, $h = 0$, another contradiction. Analogously, $f(g) + f(h) \neq f(h)$. We conclude that $f(g + h) = f(g) + f(h)$, as required. This shows that f is an automorphism of G, and completes the proof. □

References

[1] Herstein, I.N., "Topics in Algebra", Blaisdell, Waltham, 1964.

[2] Hungerford, T., "Algebra", Springer, New York, 1974.

[3] Lotto, B., *Stacked groups,* American Mathematical Monthly, Vol. 114, No. 9, pp 811-812, 2007.

About the authors:

Veronica Marth

Veronica is finishing up her B.A. in mathematics (with a physics minor) at The University of Colorado, Colorado Springs (UCCS). She plans to pursue a Ph.D. in mathematics, specializing in either algebra or probability.

University of Colorado, Colorado Springs, Colorado, 80918.
marth31415@hotmail.com

Greg Oman

Greg is an assistant professor of mathematics at UCCS. He specializes in ring theory, logic, universal algebra, and consistently wussing out when invited on skiing trips.

University of Colorado, Colorado Springs, Colorado, 80918.
goman@uccs.edu