Fixed Points and Transient Points in Permutation Groups

Richard Winton, Ph.D. †

Abstract

Basic definitions fundamental to the paper are presented. Preliminary material concerning fixed points and transient points in permutation groups is developed. A main theorem is established which provides sufficient conditions for the set of fixed points of a power of a permutation to be contained in the set of fixed points of another power of the same permutation. A result similar to the main theorem is provided for the sets of transient points of powers of a permutation.

Introduction

It is commonly known that the collection Sym(S) of bijections on a nonempty set S is a group with the operation of composition of functions, and is called the group of permutations (or symmetries) on S. It is also well known that Sym(S) is nonabelian whenever $|S| \geq 3$ ([1, p. 94, Theorem 2.20],[2, p. 40, Theorem 6.3],[3, p. 87, no. 30]).

In 2011 results related to commutativity in disjoint permutations were established [6]. The concept of semidisjoint permutations was introduced in 2013, and results related to commutativity in semidisjoint permutations were presented [7]. The notions of fixed points and transient points of a permutation played a crucial role in both of these previous works. Hence the goal of this paper is to establish properties and relationships of fixed points and transient points of permutations in Sym(S). Throughout this paper we assume that S is a nonempty set.

Basic Definitions

We begin with some fundamental definitions and notations which are pertinent to all of the following results. Permutations, Sym(S), S_n, cycles, and the identity map on S are standard concepts ([6, Definition 1],[7, Definition 1]). However, they are included here for completeness.

Definition 1: A permutation (or symmetry) α on a nonempty set S is a bijection α:S$\to$S. The set of all permutations on S is denoted by Sym(S). If S is a finite set of order n, then Sym(S) will be written S_n, and is called the set of permutations on n elements. In this case S can be represented as S = $\{k\}_{k=1}^{n}$. If $\alpha \in$ Sym(S) and n is a positive integer, then α is a cycle of length (or order) n if and only if there is a finite subset $\{a_i\}_{i=1}^{n}$ of S with the property that $\alpha(a_i)$ = a_{i+1} for $1 \le i \le n-1$, $\alpha(a_n) = a_1$, and $\alpha(x) = x$ for each $x \in S - \{a_i\}_{i=1}^{n}$. In this case α is written $\alpha = (a_1, a_2, \cdots, a_n)$. Furthermore, if $\alpha \in \text{Sym}(S)$, m is a positive integer, and n is an integer, then α^m is the result of α operated with itself m times, and $\alpha^{-n} = (\alpha^{-1})^n = (\alpha^n)^{-1}$. Finally, α^0 is the identity map 1_S on S.

The definitions and notations for fixed points and transient points of a permutation on a nonempty set appeared previously in publications related to commutativity in disjoint permutations [6, Definition 2] and semidisjoint permutations [7, Definition 2]. Nevertheless, they are provided here since they are the primary focus of the paper.

Definition 2: Suppose S is a nonempty set, $p, q \in S$, and $\alpha \in \text{Sym}(S)$. Then p is a fixed point of α if and only if $\alpha(p) = p$. In contrast, q is a transient point of α if and only if $\alpha(q) \neq q$. The set of fixed points of α is $F_\alpha = \{x \in S \mid \alpha(x) = x\}$; the set of transient points of α is $T_\alpha = \{x \in S \mid \alpha(x) \neq x\}$.

Preliminary Results

The identity map 1_S on a nonempty set S has a crucial role as the identity element in the group Sym(S). Thus we begin by establishing the sets of fixed points and transient points for this special permutation in Sym(S).

Corollary 3: If S is a nonempty set, then $F_{1_S} = S$ and $T_{1_S} = \emptyset$.

Proof: By the definition of the identity map, we have $1_S(x) = x$ for each $x \in S$. Therefore $x \in F_{1_S}$ for each $x \in S$, and so $S \subseteq F_{1_S}$. However, by Definition 2 we have $F_{1_S} = \{x \in S \mid 1_S(x) = x\} \subseteq S$. Hence $F_{1_S} = S$.

Consequently, $T_{1_S} = S - F_{1_S}$ [6, Corollary 3] $= S - S = \emptyset$.

Clearly if $\alpha \in \text{Sym}(S)$ and $x, y \in S$, then $\alpha(x) = y$ if and only if $\alpha^{-1}(y) = x$. Based on this simple observation, we now formally establish the fact that each permutation on S has the same set of fixed points as its inverse.

Lemma 4: If $\alpha \in \text{Sym}(S)$, then $F_\alpha = F_{\alpha^{-1}}$.

Proof: From the basic property of an inverse function that $\alpha(x) = y$ if and only if $\alpha^{-1}(y) = x$, we have $x \in F_\alpha$ if and only if $\alpha(x) = x$ if and only if $\alpha^{-1}(x) = x$ if and only if $x \in F_{\alpha^{-1}}$. Therefore $F_\alpha = F_{\alpha^{-1}}$.

Alternatively, if $x \in F_\alpha$, then $\alpha(x) = x$. Therefore $\alpha^{-1}(x) = \alpha^{-1}[\alpha(x)] = \alpha^{-1}\alpha(x) = 1_S(x) = x$. Thus $x \in F_{\alpha^{-1}}$, and so $F_\alpha \subseteq F_{\alpha^{-1}}$. Conversely, note that $(\alpha^{-1})^{-1} = \alpha$. Then by the above argument, $F_{\alpha^{-1}} \subseteq F_{(\alpha^{-1})^{-1}} = F_\alpha$. Hence we have $F_\alpha = F_{\alpha^{-1}}$.

As a third argument, since $\alpha^{-1} \in \mathrm{Sym}(S)$, then α^{-1} is a well defined, 1-1 function. Therefore $x \in F_\alpha$ if and only if $\alpha(x) = x$ if and only if $\alpha^{-1}[\alpha(x)] = \alpha^{-1}(x)$ if and only if $\alpha^{-1}\alpha(x) = \alpha^{-1}(x)$ if and only if $1_S(x) = \alpha^{-1}(x)$ if and only if $x = \alpha^{-1}(x)$ if and only if $x \in F_{\alpha^{-1}}$. Consequently $F_\alpha = F_{\alpha^{-1}}$.

In 2011 it was proven that for each permutation α on a nonempty set S, F_α and T_α are set complements relative to S [6, Corollary 3]. This fact is useful in producing a result for transient points analogous to the one in Lemma 4 for fixed points. More specifically, we now show that each permutation on S has the same transient points as its inverse.

Corollary 5: If $\alpha \in \mathrm{Sym}(S)$, then $T_\alpha = T_{\alpha^{-1}}$.

Proof: If $\alpha \in \mathrm{Sym}(S)$, then $T_\alpha = S - F_\alpha$ [6, Corollary 3] = $S - F_{\alpha^{-1}}$ (by Lemma 4) = $T_{\alpha^{-1}}$ [6, Corollary 3].

Lemma 4 can be substantially generalized with a simple observation. More precisely, if α is a permutation on S and n is an integer, then α^{-n} is the inverse of α^n according to Definition 1. Hence we have the following result.

Theorem 6: If $\alpha \in \mathrm{Sym}(S)$, then $F_{\alpha^n} = F_{\alpha^{-n}}$ for each integer n.

Proof: Since $\alpha \in \mathrm{Sym}(S)$, then $\alpha^n \in \mathrm{Sym}(S)$ and $(\alpha^n)^{-1} = \alpha^{-n}$ by Definition 1. Thus by Lemma 4, $F_{\alpha^n} = F_{(\alpha^n)^{-1}} = F_{\alpha^{-n}}$.

Similar to the relationship between Lemma 4 and Corollary 5, we can immediately establish a result for transient points analogous to the one for fixed points in Theorem 6. Therefore we present the following corollary.

Corollary 7: If $\alpha \in \mathrm{Sym}(S)$, then $T_{\alpha^n} = T_{\alpha^{-n}}$ for each integer n.

Proof: If n is an integer, then $T_{\alpha^n} = S - F_{\alpha^n}$ [6, Corollary 3] = $S - F_{\alpha^{-n}}$ (by Theorem 6) = $T_{\alpha^{-n}}$ [6, Corollary 3].

Alternatively, an approach similar to the proof of Theorem 6 can be employed. That is, $T_{\alpha^n} = T_{(\alpha^n)^{-1}}$ (by Corollary 5) = $T_{\alpha^{-n}}$ by Definition 1.

The following result reveals a relationship between the set of fixed points of a permutation α on a nonempty set S and the set of fixed points of powers of α. In particular, if α is a permutation on S, then any fixed point of α is also a fixed point of any power of α.

Theorem 8: If $\alpha \in \mathrm{Sym}(S)$, then $F_\alpha \subseteq F_{\alpha^n}$ for each integer n.

Proof: Suppose $x \in F_\alpha = \{x \in S \mid \alpha(x) = x\}$ by Definition 2. Then $x \in S = F_{1_S}$ (by Corollary 3) = F_{α^0} by Definition 1. Furthermore, $x \in F_\alpha = F_{\alpha^1}$ by the hypothesis.

If k is a nonnegative integer and $x \in F_{\alpha^k}$, then $\alpha^k(x) = x$. Therefore $\alpha^{k+1}(x) = \alpha[\alpha^k(x)] = \alpha(x) = x$ since $x \in F_\alpha$, and so $x \in F_{\alpha^{k+1}}$. Thus by induction, $x \in F_{\alpha^n}$ for each integer $n \geq 0$. Consequently, $x \in F_{\alpha^{-n}}$ for each integer $n \geq 0$ since $F_{\alpha^n} = F_{\alpha^{-n}}$ by Theorem 6.

Hence if $x \in F_\alpha$ then $x \in F_{\alpha^n}$ for each integer n, and so $F_\alpha \subseteq F_{\alpha^n}$.

We now present another fact about transient points corresponding to a similar one for fixed points. That is, an inclusion relationship also exists between the transient points of α and the transient points of any power of α. However, in the case of transient points the set theoretic relationship between the set of transient points of a permutation α on S and the set of transient points of powers of α is reversed relative to the relationship for fixed points established in Theorem 8.

Corollary 9: If $\alpha \in \mathrm{Sym}(S)$, then $T_{\alpha^n} \subseteq T_\alpha$ for each integer n.

Proof: If $\alpha \in \mathrm{Sym}(S)$ and n is an integer, then $F_\alpha \subseteq F_{\alpha^n}$ by Theorem 8. Therefore $T_{\alpha^n} = S - F_{\alpha^n}$ [6, Corollary 3] $\subseteq S - F_\alpha = T_\alpha$ [6, Corollary 3].

We complete the preliminary results with a lemma which will be useful for the main theorem and corollary to follow. Lemma 10 establishes the crucial fact that if α is a permutation on a nonempty set S, $x \in S$, m is a nonzero integer, $\alpha^m(x) = x$, n is an integer, and r is the least residue of n modulo $|m|$, then $\alpha^n(x) = \alpha^r(x)$.

Lemma 10: Suppose $\alpha \in \mathrm{Sym}(S)$, m is a nonzero integer, n is an integer, and $x \in F_{\alpha^m}$. Then $\alpha^n(x) = \alpha^{n(\mathrm{mod}|m|)}(x)$.

Proof: Suppose that $m > 0$.

Since m is a positive integer and n is an integer, then by the Division Algorithm there exist integers q and r such that $0 \le r \le m-1$ and $n = mq + r$. Then r is a least residue modulo m and $n \equiv r \pmod{m}$, so that $r = n \ (\mathrm{mod}\ m)$. Furthermore, since $x \in F_{\alpha^m}$ then $x \in F_{(\alpha^m)^q} = F_{\alpha^{mq}}$ by Theorem 8. Therefore $x \in F_{\alpha^{-mq}}$ by Theorem 6, and so $\alpha^{-mq}(x) = x$. Thus $\alpha^{n(\mathrm{mod}|m|)}(x) = \alpha^{n(\mathrm{mod}\,m)}(x)$ (since $m > 0$) $= \alpha^r(x) = \alpha^{n-mq}(x) = \alpha^n[\alpha^{-mq}(x)] = \alpha^n(x)$.

For an alternate proof, note that $(\alpha^m)^0(x) = \alpha^0(x) = 1_S(x) = x$. Furthermore, since $x \in F_{\alpha^m}$, then $(\alpha^m)^1(x) = \alpha^m(x) = x$.

Now suppose that k is an integer, $k \ge 0$, and $(\alpha^m)^k(x) = x$. Then $(\alpha^m)^{k+1}(x) = \alpha^{mk+m}(x) = \alpha^m\alpha^{mk}(x) = \alpha^m[(\alpha^m)^k(x)] = \alpha^m(x)$ (by the induction hypothesis) $= x$ since $x \in F_{\alpha^m}$. Thus by induction $(\alpha^m)^k(x) = x$ for each $k \ge 0$.

If k is an integer and $k < 0$, then $-k > 0$. Furthermore, since $x \in F_{\alpha^m}$, then $x \in F_{\alpha^{-m}}$ as well by Theorem 6. Therefore $(\alpha^m)^k(x) = \alpha^{mk}(x) = \alpha^{(-m)(-k)}(x) = (\alpha^{-m})^{-k}(x) = x$ by the argument above for $k \ge 0$ since $-k > 0$ and $x \in F_{\alpha^{-m}}$.

Consequently $(\alpha^m)^k(x) = x$ for each integer k. Thus if n is an integer, then by the Division Algorithm there exist integers q and r such that $0 \le r \le m-1$ and $n = mq + r$. Therefore r is a least residue modulo m and $n \equiv r \pmod{m}$, so that $r = n \ (\mathrm{mod}\ m)$. Hence $\alpha^n(x) = \alpha^{mq+r}(x) = \alpha^r[(\alpha^m)^q(x)] = \alpha^r(x)$ (by the induction argument above) $= \alpha^{n(\mathrm{mod}\,m)}(x) = \alpha^{n(\mathrm{mod}|m|)}(x)$ since $m > 0$.

On the other hand, suppose that $m < 0$, so that $-m > 0$. Furthermore, since $x \in F_{\alpha^m}$ then $x \in F_{\alpha^{-m}}$ by Theorem 6. Then by the argument above for $m > 0$, $\alpha^n(x) = \alpha^{n(\mathrm{mod}|-m|)}(x) = \alpha^{n(\mathrm{mod}|m|)}(x)$.

Thus if α is a permutation on a nonempty set S, m is a nonzero integer, and $x \in F_{\alpha^m}$, then there are only a finite number of distinct values in the collection $\{\alpha^n(x) \mid n \text{ is an integer}\}$, namely $\{\alpha^n(x)\}_{n=0}^{|m|-1}$.

Main Results

The following main theorem generalizes Theorem 8. More specifically, Theorem 8 is a special case of Theorem 11 for $m = 1$. Furthermore, a relationship similar to the one between Theorem 8 and Theorem 11 also exists between Corollary 9 and Corollary 12. That is, Corollary 9 is a special case of Corollary 12 for $m = 1$.

Several pairs of corresponding relationships between fixed points and transient points were validated in Lemma 4 and Corollary 5, Theorem 6 and Corollary 7, and Theorem 8 and Corollary 9. Theorem 11 establishes sufficient conditions on integers m and n to guarantee that $F_{\alpha^m} \subseteq F_{\alpha^n}$. Similar to the results referenced above, Corollary 12 provides the corresponding relationship for transient points.

Theorem 11: Suppose S is a nonempty set, $\alpha \in Sym(S)$, and m and n are integers. If $m \mid n$ then $F_{\alpha^m} \subseteq F_{\alpha^n}$.

Proof: Suppose that $\alpha \in Sym(S)$, m and n are integers, and $m \mid n$.

Case 1: Suppose $n = 0$. Therefore $\alpha^n = \alpha^0 = 1_S$, so that $F_{\alpha^n} = F_{1_S} = S$ by Corollary 3. Thus $F_{\alpha^m} = \{x \in S \mid \alpha^m(x) = x\}$ (by Definition 2) $\subseteq S = F_{\alpha^n}$.

Case 2: Suppose $n > 0$. Since $m \mid n$ then $m \neq 0$.

If $m > 0$ then $n \equiv 0 \pmod{m}$ since $m \mid n$, and so $n(\mathrm{mod}\ m) = 0$. Thus if $x \in F_{\alpha^m}$, then by Lemma 10 $\alpha^n(x) = \alpha^0(x) = 1_S(x)$ (by Definition 1) $= x$. Therefore $x \in F_{\alpha^n}$, and so $F_{\alpha^m} \subseteq F_{\alpha^n}$.

If $m < 0$ then $-m > 0$ and $(-m) \mid n$ as well. Therefore $F_{\alpha^{-m}} \subseteq F_{\alpha^n}$ by the argument above for $m > 0$. Since $F_{\alpha^m} = F_{\alpha^{-m}}$ by Theorem 6, then $F_{\alpha^m} \subseteq F_{\alpha^n}$.

Case 3: Suppose $n < 0$. Similar to Case 2, since $m \mid n$ then $m \neq 0$. Furthermore, $-n > 0$ and $m \mid (-n)$ as well. Therefore $F_{\alpha^m} \subseteq F_{\alpha^{-n}}$ by Case 2 above. However, since $F_{\alpha^n} = F_{\alpha^{-n}}$ by Theorem 6, then $F_{\alpha^m} \subseteq F_{\alpha^n}$.

Hence in all possible cases, if $m \mid n$ then $F_{\alpha^m} \subseteq F_{\alpha^n}$.

We conclude with a result for transient points analogous to that of Theorem 11 for fixed points. Comparing the relationship between F_α and F_{α^n} in Theorem 8 with the relationship between T_α and T_{α^n} in Corollary 9, it is not surprising that the set containment relationship between T_{α^m} and T_{α^n} in Corollary 12 is reversed relative to that of F_{α^m} and F_{α^n} in Theorem 11.

Corollary 12: Suppose S is a nonempty set, $\alpha \in \text{Sym}(S)$, and m and n are integers. If $m \mid n$, then $T_{\alpha^n} \subseteq T_{\alpha^m}$.

Proof: Suppose that $\alpha \in \text{Sym}(S)$ and m and n are integers. If $m \mid n$ then $F_{\alpha^m} \subseteq F_{\alpha^n}$ by Theorem 11. Therefore $T_{\alpha^n} = S - F_{\alpha^n}$ [6, Corollary 3] $\subseteq S - F_{\alpha^m} = T_{\alpha^m}$ [6, Corollary 3].

Concluding Remarks

If $\alpha \in \text{Sym}(S)$ and n is an integer, then clearly $1 \mid n$. Thus $F_\alpha = F_{\alpha^1} \subseteq F_{\alpha^n}$ by Theorem 11, thereby establishing Theorem 8 as the special case for m = 1 in Theorem 11. Furthermore, since $1 \mid n$ then $T_{\alpha^n} \subseteq T_{\alpha^1} = T_\alpha$ by Corollary 12, establishing Corollary 9 as the special case for m = 1 in Corollary 12.

Note that the converses of Theorem 11 and Corollary 12 are false. For example, suppose S is a nonempty set, $|S| \geq 2$, $x, y \in S$, and $x \neq y$. Then $\alpha = (x,y)$ is a transposition in Sym(S). Therefore $T_{\alpha^0} = T_{1_S} = \varnothing$ and $F_{\alpha^0} = F_{1_S} = S$ by Corollary 3, while $T_{\alpha^1} = T_\alpha = \{x,y\}$ and $F_{\alpha^1} = F_\alpha = S - \{x,y\}$ [6, Corollary 3]. Furthermore, since α is a cycle of length two then $|\alpha| = 2$ ([4, p. 133, Lemma 3.2.3],[5, p. 46]). Thus for each integer n, $\alpha^n = \alpha^{n \pmod 2}$. Hence $F_{\alpha^3} = F_{\alpha^1} = S - \{x,y\}$, $T_{\alpha^3} = T_{\alpha^1} = \{x,y\}$, $F_{\alpha^4} = F_{\alpha^0} = S$, and $T_{\alpha^4} = T_{\alpha^0} = \varnothing$. Consequently $F_{\alpha^3} \subseteq F_{\alpha^4}$ and $T_{\alpha^4} \subseteq T_{\alpha^3}$, but $3 \nmid 4$.

It might be conjectured that Theorem 11 and Corollary 12 could be generalized. For example, if m and n are integers and $1 \leq m \leq n$, is it necessarily true that $F_{\alpha^m} \subseteq F_{\alpha^n}$ (or equivalently that $T_{\alpha^n} \subseteq T_{\alpha^m}$ [6, Corollary 3])? More generally, if m and n are integers and $1 \leq |m| \leq |n|$, is it necessarily true that $F_{\alpha^m} \subseteq F_{\alpha^n}$ or $T_{\alpha^n} \subseteq T_{\alpha^m}$?

Note, however, that a counterexample for the case for fixed points will immediately refute the case for transient points as well [6, Corollary 3]. Furthermore, a counterexample for the case of $1 \leq m \leq n$ will also serve as a counterexample for the case of $1 \leq |m| \leq |n|$.

To this end, consider the transposition $\alpha = (x,y)$ on S defined above. Since $\alpha^n = \alpha^{n \pmod 2}$ for each integer n, then $F_{\alpha^2} = F_{\alpha^0} = S$, $T_{\alpha^2} = T_{\alpha^0} = \varnothing$, $F_{\alpha^3} = F_{\alpha^1} = S - \{x,y\}$, and $T_{\alpha^3} = T_{\alpha^1} = \{x,y\}$. Thus $1 \leq 2 \leq 3$, but $F_{\alpha^2} \not\subseteq F_{\alpha^3}$ and $T_{\alpha^3} \not\subseteq T_{\alpha^2}$.

† *Richard Winton*, *Ph.D.*, Tarleton State University, Texas, USA

References

1. Burton, David M., *Abstract Algebra*, Wm. C. Brown Publishers, Dubuque, Iowa, 1988.
2. Durbin, John R., *Modern Algebra: An Introduction*, 3rd edition, John Wiley & Sons, New York, 1992.
3. Gallian, Joseph A., *Contemporary Abstract Algebra*, D. C. Heath and Company, Lexington, Massachusetts, 1986.
4. Herstein, I. N., *Abstract Algebra*, Macmillan Publishing Company, New York, 1986.
5. Hungerford, Thomas W., *Algebra*, Springer-Verlag, New York, 1974.
6. Winton, Richard, *Commutativity in Permutation Groups*, Journal of Mathematical Sciences and Mathematics Education, Vol. 6, No. 2, (2011) pp. 1-7.
7. Winton, Richard, *Semidisjoint Permutations*, Journal of Mathematical Sciences and Mathematics Education, Vol. 8, No. 1, (2013) pp. 1-11.