Commutativity in Permutation Groups

Richard Winton, Ph.D. †

Abstract

In the group Sym(S) of permutations on a nonempty set S, fixed points and transient points are defined. Preliminary results on fixed and transient points are developed. Disjoint permutations and disjoint collections of permutations are then defined in terms of transient points. Several commutativity results for disjoint permutations are established.

Introduction

Most relevant texts define the notions of permutations, cycles, and disjoint cycles on a nonempty set. A commutativity result regarding permutations is then presented. However, the degree of generality of this result varies substantially.

For example, some texts define permutations only on finite sets [1, p. 92, Definition 2.15]. Furthermore, the term *disjoint* is defined only for pairs of cycles, but not for permutations in general [1, p. 95]. Thus the corresponding commutativity result is restricted to the observation that disjoint pairs of cycles in S_n commute, where n is a positive integer and S_n is the group of permutations on n elements [1, p. 95].

Other texts extend the definition of permutations to an arbitrary nonempty set S ([2, p. 38],[3, p. 77],[4, p. 18]), but define cycles only for S_n on finite sets, and not for Sym(S) in general ([2, p. 40],[3, p. 80],[4, p. 131]). As before, the term *disjoint* is defined only for pairs of cycles ([2, p. 41],[3, p. 81],[4, p. 131]). Consequently, the commutativity result obtained is restricted as above to the statement that disjoint pairs of cycles in S_n commute ([2, p. 41],[3, p. 82, Theorem 6.2],[4, p. 131, Lemma 3.2.1]).

Still other texts also use the more general definition of a permutation on an arbitrary nonempty set [5, p. 26] while restricting the definition of cycles to finite sets [5, p. 46, Definition 6.1]. However, the term *disjoint* is applied to general permutations rather than being limited to cycles, and is even extended to finite collections of permutations, but is limited to permutations in S_n on a finite set [5, p. 47, Definition 6.2]. Furthermore, the related commutativity result is still restricted to pairs of permutations in finite collections only, and is not extended to include arbitrary collections or even finite collections of permutations as a whole. Thus the commutativity result stated is that disjoint pairs of permutations in S_n commute [5, p. 47].

Finally, some texts define both permutations [6, p. 30] and cycles [6, p. 79] on arbitrary nonempty sets. The term *disjoint* is defined for arbitrary collections of cycles [6, p. 79], but not for arbitrary collections or even pairs of general permutations. Once again, however, the corresponding commutativity result refers only to pairs of cycles, stating that disjoint pairs of cycles in Sym(S) commute [6, p. 79, no. 10].

Each of these sources restricts the term *disjoint* to either pairs of permutations, cycles only, permutations on a finite set, or some combination of these. Consequently the commutativity result produced is limited in one way or another in each case. This paper generalizes these results in all three aspects by extending the term *disjoint* to apply to arbitrary collections of general permutations on any nonempty set. The corresponding result on commutativity is then developed in this more general framework. Throughout this paper it is assumed that S is a nonempty set.

Preliminary Results

We begin with some basic definitions pertinent to all of the following results. The initial definitions of permutations, Sym(S), S_n, cycles, and the identity map on S are standard, and are included here for completeness.

Definition 1: If S is a nonempty set, then a permutation (or symmetry) α on S is a 1-1, onto function $\alpha: S \to S$. 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 n is a positive integer, then a permutation $\alpha \in \text{Sym(S)}$ is a cycle of length n if and only if there is a finite subset $\{a_i\}_{i=1}^{n}$ of S such 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 we write $\alpha = (a_1, a_2, \cdots, a_n)$. The identity map on S is denoted by 1_S.

It is commonly known that Sym(S) endowed with the operation of composition of functions is a group [2, p. 38, Theorem 6.1], called the group of permutations on S. It is also well known that Sym(S) is nonabelian when $|S| \ge 3$ ([1, p. 94, Theorem 2.20],[2, p. 40, Theorem 6.3]). Therefore any nontrivial result on commutativity in permutation groups is significant. In order to achieve the goal of this paper, we need the standard concept of fixed points, along with a contrasting notion of transient points. Thus we have the following definitions.

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

For each $\alpha \in \text{Sym(S)}$, it is clear that $S - F_\alpha = T_\alpha$ and $S - T_\alpha = F_\alpha$. Consequently, if F_α and T_α are nonempty, then $\{F_\alpha, T_\alpha\}$ partitions S. We formally state these facts in the following result.

Corollary 3: Suppose $\alpha \in$Sym(S).

(a) F_α and T_α are set complements of each other relative to S.

(b) If F_α and T_α are nonempty, then $\{F_\alpha, T_\alpha\}$ is a partition of S.

Proof:

(a) It is clear from Definition 2 that $F_\alpha \subseteq$ S and $T_\alpha \subseteq$ S. Furthermore, for each $x \in$S, $x \in F_\alpha$ if and only if $\alpha(x) = x$ if and only if $x \notin T_\alpha$. The result follows.

(b) The result is an immediate consequence of part (a).

Part (a) of Theorem 4 could be stated biconditionally. However, a stronger version of the converse of part (a) exists, and is stated separately in part (b). In this manner, the hypothesis in part (b) assumes only that $\alpha^n(x) \in F_\alpha$ for *some* integer n, rather than for *each* integer n. Consequently the result of the converse of part (a) is obtained using a weaker hypothesis. Parts (a) and (b) are then combined to verify the result in part (c).

Theorem 4: Suppose $\alpha \in$Sym(S) and $x \in$S.

(a) If $x \in F_\alpha$, then $\alpha^n(x) \in F_\alpha$ for each integer n.

(b) Conversely, if $\alpha^n(x) \in F_\alpha$ for some integer n, then $x \in F_\alpha$.

(c) If $\alpha^n(x) \in F_\alpha$ for some integer n, then $\alpha^n(x) \in F_\alpha$ for each integer n.

Proof:

(a) If $x \in F_\alpha$, then $\alpha(x) = x$ by Definition 2. Thus for each integer n, $\alpha^n(x) \in$S and $\alpha[\alpha^n(x)] = \alpha^{n+1}(x) = \alpha^n[\alpha(x)] = \alpha^n(x)$. Hence $\alpha^n(x) \in F_\alpha$ by Definition 2.

(b) If $\alpha^n(x) \in F_\alpha$ for some integer n, then $\alpha[\alpha^n(x)] = \alpha^n(x)$ according to Definition 2. Furthermore $\alpha^{-n} = (\alpha^n)^{-1} \in$Sym(S). Therefore $\alpha(x) = \alpha^{-n+n+1}(x)$ $= \alpha^{-n}[\alpha^{n+1}(x)] = \alpha^{-n}(\alpha[\alpha^n(x)]) = (\alpha^n)^{-1}[\alpha^n(x)] = (\alpha^n)^{-1} \circ \alpha^n(x) = 1_S(x) =$ x. Hence $x \in F_\alpha$ by Definition 2.

(c) If $\alpha^n(x) \in F_\alpha$ for some integer n, then $x \in F_\alpha$ by part (b). Since $x \in F_\alpha$ then $\alpha^n(x) \in F_\alpha$ for each integer n by part (a).

Transient points have properties analogous to those in Theorem 4 for fixed points. In order to establish these properties, we apply Corollary 3 and Theorem 4.

Corollary 5: Suppose $\alpha \in \mathrm{Sym}(S)$ and $x \in S$.

(a) If $x \in T_\alpha$, then $\alpha^n(x) \in T_\alpha$ for each integer n.

(b) Conversely, if $\alpha^n(x) \in T_\alpha$ for some integer n, then $x \in T_\alpha$.

(c) If $\alpha^n(x) \in T_\alpha$ for some integer n, then $\alpha^n(x) \in T_\alpha$ for each integer n.

Proof:
(a) If $x \in T_\alpha$, then $x \notin F_\alpha$ by Corollary 3. Therefore $\alpha^n(x) \notin F_\alpha$ for each integer n by (the contrapositive of) Theorem 4(b). Hence $\alpha^n(x) \in T_\alpha$ for each integer n by Corollary 3.

(b) If $\alpha^n(x) \in T_\alpha$ for some integer n, then $\alpha^n(x) \notin F_\alpha$ by Corollary 3. Thus $x \notin F_\alpha$ by (the contrapositive of) Theorem 4(a). Hence $x \in T_\alpha$ by Corollary 3.

(c) If $\alpha^n(x) \in T_\alpha$ for some integer n, then $x \in T_\alpha$ by part (b). Since $x \in T_\alpha$ then $\alpha^n(x) \in T_\alpha$ for each integer n by part (a).

Analogous special cases of Theorem 4 and Corollary 5 will be useful. More specifically, parts (a) and (b) of Theorem 4 and Corollary 5 are each condensed to a single biconditional statement for the case in which n = 1. Thus we have the following corollary.

Corollary 6: Suppose $\alpha \in \mathrm{Sym}(S)$ and $x \in S$.

(a) Then $x \in F_\alpha$ if and only if $\alpha(x) \in F_\alpha$.

(b) Furthermore, $x \in T_\alpha$ if and only if $\alpha(x) \in T_\alpha$.

Proof:
(a) If $x \in F_\alpha$, then $\alpha(x) \in F_\alpha$ by Theorem 4(a) with n = 1. Conversely, if $\alpha(x) \in F_\alpha$, then $x \in F_\alpha$ by Theorem 4(b) with n = 1.

(b) If $x \in T_\alpha$, then $\alpha(x) \in T_\alpha$ by Corollary 5(a) with n = 1. Conversely, if $\alpha(x) \in T_\alpha$, then $x \in T_\alpha$ by Corollary 5(b) with n = 1.

Alternatively, $x \in T_\alpha$ if and only if $x \notin F_\alpha$ (by Corollary 3) if and only if $\alpha(x) \notin F_\alpha$ (by part (a)) if and only if $\alpha(x) \in T_\alpha$ (by Corollary 3).

We now present the definitions of disjoint permutations, disjoint cycles, and disjoint collections of permutations in Definition 7. These concepts are defined in terms of transient points, and are crucial to obtaining the main results on commutativity.

Definition 7: Suppose $\alpha,\beta \in \mathrm{Sym}(S)$. Then α and β are disjoint if and only if $T_\alpha \cap T_\beta = \varnothing$. In particular, if $\alpha = (a_1, \cdots, a_k)$ and $\beta = (b_1, \cdots, b_m)$ are cycles in Sym(S), then α and β are disjoint if and only if $a_i \neq b_j$ for each i and j such that $1 \le i \le k$ and $1 \le j \le m$. A collection C of permutations in Sym(S) is disjoint if and only if α and β are disjoint for each $\alpha,\beta \in C$ such that $\alpha \neq \beta$.

The last part of Definition 7 raises the question of whether or not a permutation can be disjoint with itself. That is, if S is a nonempty set and $\alpha \in \mathrm{Sym}(S)$, are α and α disjoint? We resolve this issue with the following corollary.

Corollary 8: Suppose $\alpha \in \mathrm{Sym}(S)$. Then α is disjoint with itself (that is, α and α are disjoint) if and only if $\alpha = 1_S$.

Proof: Since $1_S(x) = x$ for each $x \in S$ then $F_{1_S} = S$ by Definition 2, so $T_{1_S} = \varnothing$ by Corollary 3. Therefore $T_{1_S} \cap T_{1_S} = \varnothing$, so that 1_S is disjoint with itself according to Definition 7. However, if $\alpha \neq 1_S$ then there exists $x \in S$ such that $\alpha(x) \neq x$. Thus $x \in T_\alpha$ by Definition 2, so that $T_\alpha \neq \varnothing$. Consequently $T_\alpha \cap T_\alpha = T_\alpha \neq \varnothing$, and so α is not disjoint with itself.

Main Results

The most common commutativity result for permutations found in literature states that disjoint pairs of cycles in S_n commute ([2, p. 41],[3, p. 82, Theorem 6.2],[4, p. 131, Lemma 3.2.1]). The following theorem generalizes this statement in two ways. The result for disjoint cycles is extended to disjoint permutations in general. Furthermore, the restriction to permutations in S_n on a finite set containing n elements is generalized to permutations in Sym(S) on an arbitrary nonempty set S.

Theorem 9: Suppose $\alpha,\beta \in \mathrm{Sym}(S)$. If α and β are disjoint, then $\alpha\beta = \beta\alpha$.

Proof: If α and β are disjoint permutations in Sym(S), then $T_\alpha \cap T_\beta = \varnothing$ by Definition 7. Furthermore, for each $x \in S$, either $x \in T_\alpha$, $x \in T_\beta$, or $x \in S-(T_\alpha \cup T_\beta)$. However, $S-(T_\alpha \cup T_\beta) = (S-T_\alpha) \cap (S-T_\beta) = F_\alpha \cap F_\beta$ by Corollary 3.

If $x \in T_\alpha$ then $\alpha(x) \in T_\alpha$ by Corollary 5(a) (or Corollary 6(b)). Then $x, \alpha(x) \notin T_\beta$ since $T_\alpha \cap T_\beta = \varnothing$. Therefore $x, \alpha(x) \in F_\beta$ by Corollary 3, so that $\beta(x) = x$ and $\beta[\alpha(x)] = \alpha(x)$ by Definition 2. Thus $\alpha\beta(x) = \alpha[\beta(x)] = \alpha(x) = \beta[\alpha(x)] = \beta\alpha(x)$. Similarly, if $x \in T_\beta$ then $\alpha\beta(x) = \beta\alpha(x)$. Finally, if $x \in F_\alpha \cap F_\beta$, then $\alpha(x) = x$ and $\beta(x) = x$ by Definition 2. Therefore $\alpha\beta(x) = \alpha[\beta(x)] = \alpha(x) = x = \beta(x) = \beta[\alpha(x)] = \beta\alpha(x)$.

Consequently $\alpha\beta(x) = \beta\alpha(x)$ for each $x \in S$. Hence $\alpha\beta = \beta\alpha$.

In the proof of Theorem 9, DeMorgan's Laws and Corollary 3 were used to show that $S-(T_\alpha \cup T_\beta) = F_\alpha \cap F_\beta$. A similar application of these two results provides a slightly different perspective on the result of Theorem 9. More specifically, the same commutativity result established in Theorem 9 can be obtained by a relationship between the sets of fixed points of permutations rather than their respective sets of transient points.

Corollary 10: Suppose $\alpha, \beta \in Sym(S)$. If $F_\alpha \cup F_\beta = S$, then $\alpha\beta = \beta\alpha$.

Proof: Note that $F_\alpha \cup F_\beta = S$ if and only if $S-(F_\alpha \cup F_\beta) = \varnothing$ if and only if $(S-F_\alpha) \cap (S-F_\beta) = \varnothing$ if and only if $T_\alpha \cap T_\beta = \varnothing$ (by Corollary 3) if and only if α and β are disjoint (by Definition 7). Thus if $F_\alpha \cup F_\beta = S$, then α and β are disjoint. Hence $\alpha\beta = \beta\alpha$ by Theorem 9.

Theorem 9 extended the common commutativity result for pairs of cycles in S_n on a finite set to the same result for pairs of general permutations in Sym(S) on an arbitrary nonempty set. We now generalize the third aspect of this result for disjoint *pairs* of permutations in Sym(S) by extending it to include disjoint *collections* of permutations in Sym(S).

Corollary 11: If C is a disjoint collection in Sym(S), then $\alpha\beta = \beta\alpha$ for each $\alpha, \beta \in C$.

Proof: Suppose C is a disjoint collection in Sym(S) and $\alpha, \beta \in C$. Therefore either $\alpha = \beta$ or α and β are disjoint by Definition 7. If $\alpha = \beta$, then clearly $\alpha\beta = \beta\alpha$. Otherwise α and β are disjoint, and so $\alpha\beta = \beta\alpha$ by Theorem 9.

Concluding Remarks

It should be noted that the converse of Theorem 9 is not true. That is, if $\alpha, \beta \in Sym(S)$ and $\alpha\beta = \beta\alpha$, then it is not necessarily true that α and β are disjoint.

For a simple example, suppose that $|S| > 1$ and $\alpha \neq 1_S$. Clearly α (like any permutation) commutes with itself. However, α is not disjoint with itself by Corollary 8.

Furthermore, the converse of Theorem 9 is false even in the case of distinct permutations on a finite set. For example, suppose $S = \{1,2,3,4\}$,

$\alpha,\beta \in S_4$, $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$, and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$. Therefore $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = \beta\alpha$. However, $T_\alpha = \{1,2\}$ and $T_\beta = \{1,2,3,4\}$. Therefore $T_\alpha \cap T_\beta = \{1,2\} \neq \varnothing$, so that α and β are not disjoint by Definition 7.

Counterexamples also exist with permutations on infinite sets. Suppose **R** is the set of real numbers, n is an odd integer, and $n \geq 3$. Define $\alpha(x) = x^n$ and $\beta(x) = \sqrt[n]{x}$ for each $x \in \mathbf{R}$. Therefore $\alpha,\beta \in \mathrm{Sym}(\mathbf{R})$ and $\alpha\beta(x) = x = \beta\alpha(x)$ for each $x \in \mathbf{R}$, so that $\alpha\beta = \beta\alpha$. However, $F_\alpha = F_\beta = \{0,1,-1\}$, so that $T_\alpha = T_\beta = \mathbf{R} - \{0,1,-1\}$ by Corollary 3. Hence $T_\alpha \cap T_\beta = \mathbf{R} - \{0,1,-1\} \neq \varnothing$, and so α and β are not disjoint according to Definition 7.

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

References

1. Burton, David M., *Abstract Algebra*, Wm. C. Brown Publishers, Dubuqua, 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. Shapiro, Louis, *Introduction to Abstract Algebra*, McGraw-Hill Book Company, New York, 1975.