COMPUTATIONAL MATHEMATICS
TOPIC 33A - PERMUTATION GROUPS

PAUL L. BAILEY

ABSTRACT. We state the pertinent definitions and immediate results regarding permutation groups.

1. Permutations and Cycles

Let X be a set. A *permutation* of X is a bijective function $\alpha : X \to X$. Set

$$\mathrm{Sym}(X) = \{\alpha : X \to X \mid \alpha \text{ is bijective } \}.$$

The composition of bijective functions is bijective, and the composition of functions from X to X is also a function from X to X. Thus we see that $\mathrm{Sym}(X)$ is closed under the operation of composition. We know that composition of functions is associative. The identity function on X is acts as an identity for composition, and the inverse of a bijective function from X to X is also a bijective function from X to X. Thus $\mathrm{Sym}(X)$ is a group under the operation of composition, which we call the *symmetry group* of X.

It is conventional to use multiplicative notation to indicate composition in $\mathrm{Sym}(X)$. Thus if $\alpha, \beta \in \mathrm{Sym}(X)$, we write $\alpha\beta$ to mean $\alpha \circ \beta$. We will denote the identity function by ϵ, and the inverse of α is α^{-1}, so that $\alpha\alpha^{-1} = \alpha^{-1}\alpha = \epsilon$. Let n be a positive integer. The n^{th} power of α is α^n; this means α composed with itself n times. We set $\alpha^0 = \epsilon$, and $\alpha^{-n} = (\alpha^{-1})^n$.

The *order* of α is the smallest positive integer n such that $\alpha^n = \epsilon$. If there is not such n, then we say α has infinite order. If X is finite, however, it is clear that α has finite order.

Let $X = \{1, 2, \ldots, n\}$, and set

$$S_n = \mathrm{Sym}(X).$$

That is, S_n is the set of permutations of 1 through n. We will use these groups as a convenient vehicle for examples of the concepts which follow, but we should keep in mind that $\mathrm{Sym}(X)$ is a more general concept (in particular, when X is infinite), and most of what follows applies in general.

The size of S_n is the number of permutation of n things; this is

$$|S_n| = n!.$$

Date: Friday, February 8, 2019.

One way to specify a member of S_n is as a $2 \times n$ array, where the top row consists of the number 1 through n, in order, and the bottom row is the destinations of these numbers. For example, let $\phi, \psi \in S_5$ be given by

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \text{ and } \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}.$$

Then $\phi(1) = 2$, $\phi(2) = 3$, and $\phi(3) = 1$. Also, $\psi(2) = 5$, so $\psi\phi(1) = \psi(2) = 5$. Compute that

$$\phi^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix} \text{ and } \psi^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix};$$

thus, $\psi^2 = \epsilon$. Also,

$$\psi\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}, \text{ and } \phi\psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix}.$$

As we see from this example, composition permutations is not necessarily commutative. We will continue to use these permutations as examples.

Let $y \in X$. The *orbit* of y under α is

$$\mathrm{orb}_\alpha(y) = \{x \in X \mid x = \alpha^n \text{ for some } n \in \mathbb{Z}\}.$$

The set of orbits of α form a partition of X; that is, each element in X is in exactly one orbit. An orbit is *trivial* if it contains exactly one element.

In our example:

$$\mathrm{orb}_\phi(1) = \{1, 2, 3\}, \mathrm{orb}_\phi(4) = \{4, 5\}, \mathrm{orb}_\psi(4) = \{4\}.$$

We see that the orbit of 4 under ψ is trivial.

We say that y is a *fixed point* of α if $\alpha(y) = y$. Thus, the orbit of y under α is trivial if and only if y is a fixed point of α. The *fixed set* of α is

$$\mathrm{fix}(\alpha) = \{x \in X \mid \alpha(x) = x\}.$$

The *support* of α is

$$\mathrm{supp}(\alpha) = \{x \in X \mid \alpha(x) \neq x\}.$$

Thus $\mathrm{supp}(\alpha) = X \setminus \mathrm{fix}(\alpha)$.

The only fixed point of ψ is 4, so the fixed set of ψ is $\{4\}$. The fixed set of ϕ is empty.

We say that two permutations α and β are *disjoint* if their supports are disjoint; that is, if

$$\mathrm{supp}(\alpha) \cap \mathrm{supp}(\beta) = \varnothing.$$

For example, let

$$\phi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \text{ and } \phi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}.$$

Then $\mathrm{supp}(\phi_1) = \{1, 2, 3\}$ and $\mathrm{supp}(\phi_2) = \{4, 5\}$, so these permutation have disjoint support. Note that $\phi = \phi_2\phi_1 = \phi_1\phi_2$.

Proposition 1. *Disjoint permutations commute.*

Proof. Let $\alpha, \beta \in \mathrm{Sym}(X)$ be disjoint. Let $x \in X$. Then $x \in \mathrm{fix}(\alpha)$ or $x \in \mathrm{fix}(\beta)$, for otherwise, x would be the support of both. Without loss of generality, let us assume that x is fixed by α. That is, $\alpha(x) = x$.

We claim that $\beta(x)$ is fixed by α. To see this, suppose not; since $\beta(x)$ cannot be moved by both α and β, we must have that $\beta(x)$ is fixed by β, so $\beta^2(x) = \beta(x)$. Apply β^{-1} to both sides to see that $\beta(x) = x$, so x is fixed by β. Then $\alpha(\beta(x)) = \alpha(x) = x$. That is, α sends $\beta(x)$ to $x = \beta(x)$, so indeed, α fixes $\beta(x)$.

Thus $\alpha(\beta(x)) = \beta(x)$. This shows that $\alpha\beta(x) = \beta\alpha(x)$ for all $x \in X$, whence $\alpha\beta = \beta\alpha$. □

A *cycle* is a permutation with exactly one nontrivial orbit; it "cycles" the points in the orbit, and fixes everything else. The *length* of a cycle is the size of its support.

For example, ϕ_1 and ϕ_2 are cycles.

Proposition 2. *Every permutation of a finite set is a product of disjoint cycles.*

Proof. Let α be a permutation of a finite set X. The orbits of α are disjoint sets. For each such orbit O, define a function $\alpha_O : X \to X$ by

$$\alpha_O = \begin{cases} \alpha(x) & \text{if } x \in O; \\ x & \text{if } x \notin O. \end{cases}$$

Clearly α_O is bijective. If $\{O_1, \ldots, O_r\}$ is the set of orbits of α, then

$$\alpha = \prod_{i=1}^{r} \alpha_{O_i}.$$

Since the cycles are disjoint, the order of composition does not matter. □

This leads us to our second way of writing elements of S_n, called *cycle notation*. A cycle of length r is denoted by an ordered n-tuple $\alpha = (a_1, a_2, \ldots, a_r)$, which indicates that $\alpha(a_1) = a_2$, $\alpha(a_2) = a_3$, and so forth, until $\alpha(a_r) = a_1$:

$$\alpha(a_i) = \begin{cases} a_{i+1} & \text{if } i < r\ ; \\ a_1 & \text{if } i = r. \end{cases}$$

This compact notation is more convenient. It is also common to write the tuple without the commas; we use a special font to make this easier. Composition of cycles is indicated by juxtaposition. Ordered tuples of length one are *trivial*, and represent the identity permutation. These are generally not written.

For example, the some of the previous permutations we have seen, written in this notation, are

$$\begin{aligned} \phi_1 &= \texttt{(1 2 3)} = \texttt{(1 2 3)} \\ \phi_2 &= \texttt{(4 5)} \\ \phi &= \texttt{(1 2 3)(4 5)} \\ \psi &= \texttt{(1 3)(2 5)} \\ \psi\phi &= \texttt{(1 5 4 2)} \\ \phi\psi &= \texttt{(2 4 5 3)} \end{aligned}$$

Note that there is more than one way to write a cycle: `(1 3 5)` = `(3 5 1)` = `(5 1 3)`. In general, we prefer to write the cycles with the least element of the support farthest to the left. Also since disjoint cycles commute, `(1 2 3)(4 5)` = `(4 5)(1 2 3)`. Here, we prefer to write the disjoint cycles in increasing order of their least element. Thus, the *standard form* of a permutation, written in disjoint cycle notation, is

- Do not write trivial cycles. Write the identity as ϵ.
- Write each cycle starting with the least element of its support;
- Write the cycles, from left to right, in the order of the least element of its support.

There is a unique standard form for any given permutation in S_n. Note, however, that the n is not indicated in the notation. Unless otherwise indicated, we assume that a given permutation is a permutation of 1 through n, where n is the largest number in its support.

One sees that the inverse of a cycle is obtained by reversing the order of its components:

$$\texttt{(1 3 5 2 7 4)}^{-1} = \texttt{(4 7 2 5 3 1)} = \texttt{(1 4 7 2 5 3)}.$$

If we wish to multiply (compose) permutations written in cycles notation, we need to "merge" them to place them in standard form. That is, we need to resolve overlaps between the cycles, are rewrite the product as a composition of *disjoint* cycles.

Example 1. Consider the permutation $\alpha =$ `(2 8 3)(7 8)(2 5 6 3)(1 6)`. Plug in 1 on the right, and follow it through each permutation, from right to left. You will get 2. Then, plug in 2, and see where it goes. Continue this until you get back to 1.

- $1 \to$ `(1 6)` $\mapsto 6 \to$ `(2 5 6 3)` $\mapsto 3 \to$ `(7 8)` $\mapsto 3 \to$ `(2 8 3)` $\mapsto 2$, so 1 goes to 2
- $2 \to$ `(1 6)` $\mapsto 2 \to$ `(2 5 6 3)` $\mapsto 5 \to$ `(7 8)` $\mapsto 5 \to$ `(2 8 3)` $\mapsto 5$, so 2 goes to 5
- $5 \to$ `(1 6)` $\mapsto 5 \to$ `(2 5 6 3)` $\mapsto 6 \to$ `(7 8)` $\mapsto 6 \to$ `(2 8 3)` $\mapsto 6$, so 5 goes to 6
- $6 \to$ `(1 6)` $\mapsto 1 \to$ `(2 5 6 3)` $\mapsto 1 \to$ `(7 8)` $\mapsto 1 \to$ `(2 8 3)` $\mapsto 1$, so 6 goes to 1

Thus, one of the disjoint cycles of the product is `(1 2 5 6)`. However, we have not completed the support of α. So, we find the smallest integer in the support of α which is not in `(1 2 5 6)`. This is three. So, we start with three to find the next disjoint cycle.

- $3 \to$ `(1 6)` $\mapsto 3 \to$ `(2 5 6 3)` $\mapsto 2 \to$ `(7 8)` $\mapsto 2 \to$ `(2 8 3)` $\mapsto 8$, so 3 goes to 8
- $8 \to$ `(1 6)` $\mapsto 8 \to$ `(2 5 6 3)` $\mapsto 8 \to$ `(7 8)` $\mapsto 7 \to$ `(2 8 3)` $\mapsto 7$, so 8 goes to 7
- $7 \to$ `(1 6)` $\mapsto 7 \to$ `(2 5 6 3)` $\mapsto 7 \to$ `(7 8)` $\mapsto 8 \to$ `(2 8 3)` $\mapsto 3$, so 7 goes to 3

Thus, the next cycle is `(3 8 7)`. This completes the support of α, so we may rewrite α as

$$\alpha = \texttt{(1 2 5 6)(3 8 7)}.$$

The *shape* of a permutation is the list of the lengths of the disjoint cycles, sorted in increasing order. The order of the permutation is the least common multiple of the numbers in the shape.

- shape `(1 2)(3 4 5)(6 7)` $= [2, 2, 3]$, with order 6
- shape `(1 2 3 4)(5 6 7)(8 9)(10 11 12)` $= [2, 3, 3, 4]$, with order 12

2. Examples of Permutation Groups

2.1. **Dihedral Groups.** A dihedral group represents the rigid motions of a regular n-gon; that is, if P is a regular polygon with n sides, the dihedral group on n vertices is the set of all isometries $P \to P$. Such a function is completely determined by where it maps the vertices of the polygon; if we enumerate the vertices 1 through n, each isometry is represented by the corresponding member of S_n which permutes the vertices in the manner of the isometry.

There are exactly $2n$ permutations of the vertices which come from isometries; these can be viewed as n rotations (including the identity) of one side, and then n rotations following a reflection. We establish some standard notation to describe dihedral groups.

Let $\rho, \tau \in S_n$ be given by

$$\rho = (1 \quad 2 \quad \dots \quad n) \quad \text{and} \quad \tau = \begin{cases} (2 \quad n)(3 \quad n-1)\dots(\frac{n+1}{2} \quad \frac{n+3}{2}) & \text{if } n \text{ is odd;} \\ (2 \quad n)(3 \quad n-1)\dots(\frac{n}{2} \quad \frac{n}{2}+2) & \text{if } n \text{ is even.} \end{cases}$$

Set

$$D_n = \{\epsilon, \rho, \rho^2, \dots, \rho^{n-1}, \tau, \tau\rho, \tau\rho^2, \dots, \tau\rho^{n-1}\} \subset S_n.$$

Then D_n is a subgroup of S_n, called the *dihedral subgroup*. The proof that this is a subgroup follows from the identity $\tau\rho = \rho^{n-1}\tau$. The dihedral group is generated by ρ and τ; it is the smallest subgroup of S_n which contains ρ and τ.

For example,

$$D_5 = \{\epsilon,$$
$$\texttt{(1 2 3 4 5)}, \texttt{(1 3 5 2 4)}, \texttt{(1 4 2 5 3)}, \texttt{(1 5 4 3 2)},$$
$$\texttt{(2 5)(3 4)}, \texttt{(1 3)(4 5)}, \texttt{(1 5)(2 4)}, \texttt{(1 2)(3 5)}, \texttt{(1 4)(2 3)}\}.$$

2.2. **Alternating Groups.** A *transposition* is a two-cycle. Every permutation may be written as a product of transpositions, in multiple ways. For example,

$$\texttt{(1 2 3 4 5)} = \texttt{(1 5)(1 4)(1 3)(1 2)} = \texttt{(2 3)(1 4)(4 5)(1 3)}.$$

Although the manner of doing this is not unique, the number of transpositions is always either even or odd. A cycle of odd length requires an even number of transpositions, and a cycle of even length requires an odd number of transpositions.

A permutation $\alpha \in S_n$ is called *even* if it can be written as a product of an even number of transpositions; otherwise it is called *odd*. Exactly half of the permutations in S_n are even.

The product of even permutations is even, and the product of odd permutations is even. The product of one odd and one even permutation is an odd permutation.

Set

$$A_n = \{\alpha \in S_n \mid \alpha \text{ is even}\}.$$

Then A_n is a subgroup of S_n, called the *alternating subgroup*.

For example,

$$A_4 = \{\epsilon,$$
$$\texttt{(1 2 3)}, \texttt{(1 3 2)}, \texttt{(1 2 4)}, \texttt{(1 4 2)},$$
$$\texttt{(1 3 4)}, \texttt{(1 4 3)}, \texttt{(2 3 4)}, \texttt{(2 4 3)},$$
$$\texttt{(1 2)(3 4)}, \texttt{(1 3)(2 4)}, \texttt{(1 4)(2 3)}\}.$$

Let H be a subgroup of S_n. Then either H consists of even permutations or exactly half of the permutations in H are even. Thus either $H \subset A_n$, in which case $H \cap A_n = H$, or $H \cap A_n$ is exactly half of H. We outline the proof. Suppose that H is not contained in A_n and let $K = H \cap A_n$; we want to show that $|H| = 2|K|$. Let $\alpha \in H$ be an odd permutation. Set $\alpha K = \{\alpha\kappa \mid \kappa \in K\}$. Then $K \cup \alpha K = H$, $K \cap \alpha K = \varnothing$, and $|K| = |\alpha K|$.

2.3. **Generalized Klein Groups.** If G is a group, H is a subgroup of G, and K is a subgroup of H, then K is a subgroup of G.

If G is a group, and H and K are subgroups of G, then their intersection $H \cap K$ is a subgroup of G.

Set $K_n = D_n \cap A_n$. Then K_n is a subgroup of S_n, and either $K_n = D_n$ or K_n is exactly half of D_n. Let us examine the relationship between n and the structure of the group K_n.

Problem 1. Let $H \leq S_n$. Show that either $H \leq A_n$ or $|H| = 2|H \cap A_n|$.

Problem 2. Let $n = 4$.

(a) Compute ρ and τ in this case.
(b) Show that K_4 is a noncyclic abelian subgroup of S_4.

Problem 3. Let $n = 5$.

(a) Compute ρ and τ in this case.
(b) Show that $K_5 = D_5$.

Problem 4. Let $n = 7$.

(a) Compute ρ and τ in this case.
(b) Show that K_7 is a cyclic subgroup of S_7.

Problem 5. Try to generalize the previous problems: what can you say about K_n in the following cases?

(a) $n \equiv 0 \pmod 2$
(b) $n \equiv 1 \pmod 4$
(c) $n \equiv 2 \pmod 4$
(d) $n \equiv 3 \pmod 4$

Department of Mathematics and CSci, BASIS Scottsdale
Email address: paul.bailey@basised.com