Part II. Permutations, Cosets, and Direct Products

Section II.8. Groups of Permutations

Note. In this section, we introduce groups which consist of functions acting on sets of elements. In particular, we consider how a set of n elements can be permuted around. Recall that a *permutation* of a set on n elements is a way to arrange the n elements. The number of ways to arrange (or *order*) n elements from a set of size n is $n! = n(n-1)(n-2)\cdots(3)(2)(1)$.

Note. A fundamental result of this section is that every group is related to a group of permutations (see Theorem 8.16, Cayley's Theorem, for details). So there is something very fundamental about groups of permutations.

Note. We use lower case Greek letters to represent permutations. First, by definition, we have:

Definition 8.3. A *permutation* of a set A is a function $\varphi : A \to A$ that is both one-to-one and onto.

Lemma. If σ and τ are permutations on set A, then the composite function $\sigma \circ \tau$ (defined as $A \xrightarrow{\tau} A \xrightarrow{\sigma} A$) is a permutation on A. Normally we drop the composition symbol $\circ$ and write $\sigma \circ \tau = \sigma\tau$. Notice that we must read this from right to left since $\sigma\tau$ is permutation τ first, followed by permutation σ.

Note. Since we can compose permutations on a given set A, then permutation composition (called *permutation multiplication*) is a binary operation on the set S of all permutations of set A. As we'll see, this binary structure is, in fact, a group.

Note. The standard notation for a permutation on a finite set is to write the elements of the set as the first row of a matrix and the corresponding images of the elements as the second row.

Example. Suppose $A = \{1, 2, 3, 4, 5, 6\}$ and

$$\begin{array}{ll} \sigma(1) = 3 & \tau(1) = 2 \\ \sigma(2) = 1 & \tau(2) = 4 \\ \sigma(3) = 4 & \tau(3) = 1 \\ \sigma(4) = 5 & \tau(4) = 3 \\ \sigma(5) = 6 & \tau(5) = 6 \\ \sigma(6) = 2 & \tau(6) = 5 \end{array}$$

then we represent σ and τ as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix} \text{ and } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}.$$

To take the permutation product $\sigma\tau$, we take each element a of set A, first use τ to find the image of a under τ, say $a' = \tau(a)$, and then find the image of a' under

σ. So

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$$

implies

$$(\sigma\tau)(1) = \sigma(\tau(1)) = \sigma(2) = 1$$

$$(\sigma\tau)(2) = \sigma(\tau(2)) = \sigma(4) = 5$$

$$(\sigma\tau)(3) = \sigma(\tau(3)) = \sigma(1) = 3$$

$$(\sigma\tau)(4) = \sigma(\tau(4)) = \sigma(3) = 4$$

$$(\sigma\tau)(5) = \sigma(\tau(5)) = \sigma(6) = 2$$

$$(\sigma\tau)(6) = \sigma(\tau(6)) = \sigma(5) = 6,$$

so

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 4 & 2 & 6 \end{pmatrix}.$$

Exercise 8.2. For σ and τ as above, find $\tau^2\sigma$.

Solution 1. We can find τ^2:

$$\tau^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 5 & 6 \end{pmatrix},$$

and then $\tau^2\sigma$:

$$\tau^2\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 5 & 6 & 3 \end{pmatrix}.$$

Solution 2. We can write out the three permutations and simply follow the elements (from right to left):

$$\tau^2\sigma = \tau\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 5 & 6 & 3 \end{pmatrix}$$

Theorem 8.5. Let A be a nonempty set, and let S_A be the collection of all permutations of A. Then S_A is a group under permutation multiplication.

Note. The text warns (page 78) that some other books write permutations in left-to-right order, so that "$\sigma\mu$" would mean first permutation σ, then followed by permutation μ (which is backwards from Fraleigh's notation).

Note. At the stage (we are more than 1/3 of the way through the material of Introduction to Modern Algebra 1), you are probably wondering what all this group stuff has to do with what you have previously thought of as "algebra"! In the quest for an algebraic formula that would give all the roots of an nth degree polynomial (basically, a "quadratic equation" but not just for a degree 2 polynomial, but for an nth degree polynomial). Algebraic formulae for 1st degree (easy), 2nd degree (the quadratic equation), 3rd degree (hard) and 4th degree (hard) polynomials are known. An interesting history of the least two results is given in *Unknown Quantity: A Real and Imaginary History of Algebra*, by John Derbyshire, Plume Publishing,

2007. While looking for a general formula, Joseph-Louis Lagrange (1736–1813) and others considered how an algebraic formula would relate to permutations of the roots of a polynomial. This lead to set A being the set of roots and S_A the "group" of permutations of the roots. The "standard notation" of a permutation is due to Augustin-Louis Cauchy (1789–1857). (See the *Historical Notes* on pages 38, 39, and 77.) Amazingly, it was shown using permutation groups that there is not an algebraic formula for the roots of a polynomial of degree n when $n \geq 5$. This was shown by Niels Henrik Abel (1802–1829), a Norwegian mathematician. Our term "abelian" for a group in which commutivity holds is in commemoration of Abel. The precise conditions under which a polynomial equation can be solved algebraically (i.e., "in terms of radicals") was given in 1831 by Evariste Galois (1811–1832). (Notice how young he was!) We'll encounter Galois again in Section III.13 when we discuss normal subgroups. Also, notice that the title of Section X.53 is Galois Theory.

Definition 8.6. Let A be the finite set $\{1, 2, \ldots, n\}$. The group of all permutations of A is the *symmetric group on n letters*, denoted S_n.

Note. A simple counting argument shows that $|S_n| = n! = n(n-1)(n-2)\cdots(3)(2)(1)$: In counting the permutations, notice that there are n choices for what 1 is mapped to (namely, $1, 2, 3, \ldots, n-1$, or n). Then there are $n-1$ choices for what 2 is mapped to (namely, all of $1, 2, \ldots, n-1, n$ except for what 1 was mapped to). There are then $n-2$ choices for what 3 is mapped to, and so forth. We multiply together the number of choices for each case and $n!$ results.

Example 8.7. The symmetric group on 3 letters S_3 has the following elements, where $A = \{1, 2, 3\}$:

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

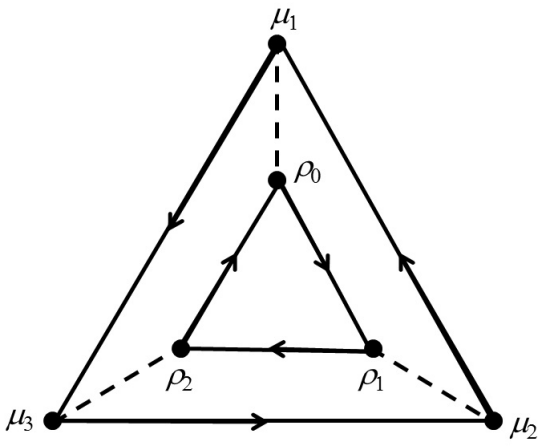
$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

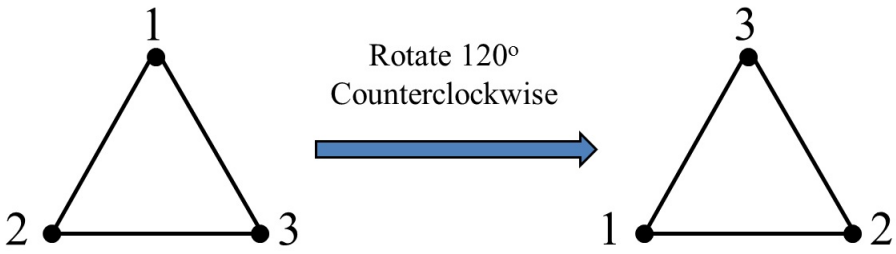
The multiplication table for S_3 is then:

	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Notice that S_3 is nonabelian: $\rho_2\mu_1 = \mu_3 \neq \mu_2 = \mu_1\rho_2$. In fact, order 6 (as we will see) is the smallest possible order of a nonabelian group. Also notice that S_3 is generated by $\{\rho_1, \mu_1\}$. If we represent ρ_1 with $\longrightarrow$ and μ_1 with - - - - (notice that $\mu_1^2 = \rho_0 =$ identity), then the Cayley digraph for S_3 is:



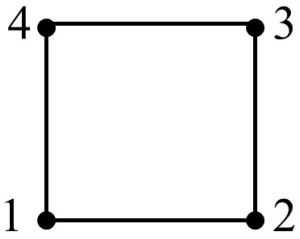
Example. The *dihedral group* D_3 is the group of all symmetries of an equilateral triangle. That is, we have an element of D_3 if we have a particular way to pick up a rigid equilateral triangle, rotate or flip it around, and place it back down so that it lies over its original position. For example, we might pick up the triangle, rotate it 120° counterclockwise and place it back down:



There are six such ways to manipulate the triangle. In fact, $D_3 \cong S_3$. In the table above, ρ_0, ρ_1, ρ_2 represent rotations of the triangle, and μ_1, μ_2, μ_3 represent mirror images of the triangle (which fixes one number/vertex and interchanges the other two).

Note. In general, the nth *dihedral group* D_n is the group of symmetries of a regular n-gon. Exercise 8.44 has you give a geometric argument (as opposed to a "proof") that D_n actually is a group. In fact, $|D_n| = 2n$.

Example 8.10. The dihedral group D_4 has 8 elements and is sometimes called the *octic group*. Since n is even, there is an additional symmetry from that of the triangle. A square can be rotated, a mirror image can be taken, and it can be diagonally flipped:



These three procedures inspire the following notation:

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

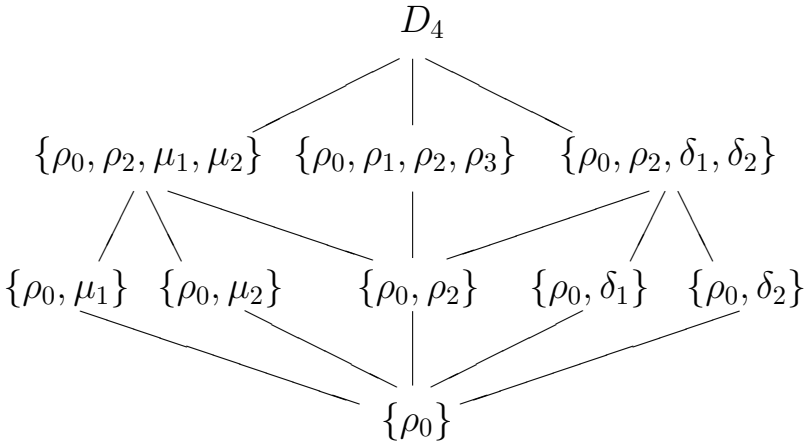
$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \quad \delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

Notice that D_4 is a subgroup of S_4 ($D_4 < S_4$). It is fairly intuitive that a (nonzero) rotation followed by a mirror image or diagonal flip is not the same as the mirror

image or diagonal flip followed by a (nonzero) rotation. That is, D_4 is not an abelian group. This is confirmed as well by considering the multiplication table

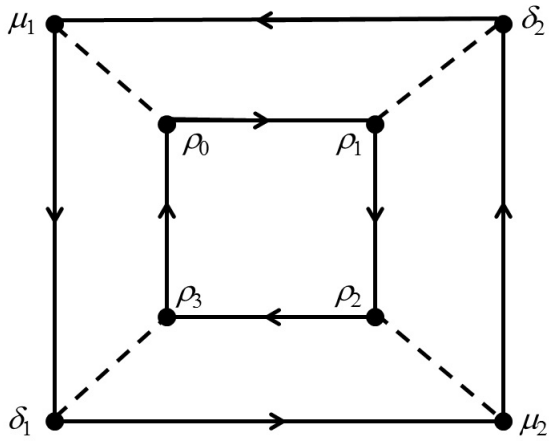
	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	δ_1	δ_2	μ_1	μ_2
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	δ_2	μ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	δ_1	μ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	μ_1	δ_2	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	μ_2	δ_1	μ_1	ρ_3	ρ_1	ρ_2	ρ_0

The subgroup diagram is:



Fraleigh goes a little nerdy here and refers to this group as "simply beautiful" and (twice) as having "lovely symmetries" (page 81)!

Note. We also have that D_4 is generated by a set consisting of two elements $\{\rho_1, \mu_1\}$, say. (Can you guess why these groups are called dihedral groups?) This really means that all of the symmetries of a square result from a sequence of rotations and mirror images (or also, for example, rotations and diagonal flips). With ρ_1 represented as $\longrightarrow$ and μ_1 as - - - (notice $\mu_1^2 = \rho_0$ =identity), we get the Cayley digraph:



Example. Use the Cayley digraph to write the mirror image μ_2 as a product of elements of $\{\rho_1, \mu_1\}$.

Solution. We need either (1) a path from ρ_1 to μ_2, or (2) a path from μ_1 to μ_2 in the above Cayley digraph. We can use, for example, (1) $\rho_1\rho_1\mu_1$ and (2) $\mu_1\rho_1\rho_1$. Other solutions are $\rho_1\mu_1\rho_1\rho_1\rho_1$, $\mu_1\rho_1\rho_1\mu_1\mu_1$, and $\rho_i\rho_1\rho_1\rho_1\mu_1\rho_1$. Notice that it is impossible to write μ_2 purely in terms of ρ_1's or purely in terms of μ_1's. Of course, D_4 does not have a single generator, or else it would be a cyclic group and then would be (by Theorem 6.1) abelian.

Note. You'll notice that in the table for any group, each row and each column represents a permutation of the elements of the group. This is circumstantial evidence that there is a deep connection between permutation groups and groups in general. Of course, not every group *is* a permutation group (for example, finite permutation groups are of orders $n!$ for $n \in \mathbb{N}$, and there exist groups of different orders—take $\mathbb{Z}_n$ where n is not the factorial of some other natural number). The big result in this direction is Cayley's Theorem and states that every group is isomorphic to a group of permutations (a finite "group of permutations" must be a subgroup of S_G for some finite set G). Before we prove Cayley's Theorem, we need a preliminary result and another definition.

Definition 8.14. Let $f : A \to B$ for sets A and B. Let $H \subset A$. The *image of set* H under f is $\{f(h) \mid h \in H\}$, denoted $f[H]$.

Lemma 8.15. Let G and G' be groups and let $\varphi : G \to G'$ be a one-to-one function such that $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$. Then $\varphi[G]$ is a subgroup of G' and φ is an isomorphism of G with $\varphi[G]$.

Theorem 8.16. Cayley's Theorem. Every group is isomorphic to a group of permutations.

Note. Don't confuse "group of permutations" with the "permutation group" (i.e., the group of ALL permutations on a set) in the statement of Cayley's Theorem.

Note. The map φ defined in the proof of Cayley's Theorem is called the *left regular representation* of G for all $x \in G$, $\varphi(x) = \lambda_x$ where $\lambda_x(g) = xg$ for all $g \in G$. Notice that the x in the definition of λ_x is multiplied on the left. A similar definition can be made using multiplication on the right and the *right regular representation* of G.

Revised 7/6/2023