1
Group Theory

Last updated: 2020–08–29

As one of the older axiomatic systems and one of more commonly used algebraic structures, we start with an exploration of groups. Although this structure relies on a single underlying set and one binary operation, this apparent simplicity belies the rich theory.

Notation. Throughout, the blackboard bold typeface is reserved for special sets of numbers. For instance, $\mathbb{N} := \{0, 1, 2, 3, \dots\}$ is the set of nonnegative integers. This set includes zero.

Évariste Galois (1846) first employed the word *group* in a sense close to the modern meaning, whereas Arthur Cayley (1854) gave the first axiomatic definition of a group.

1.0 Abstract Groups

1.0.0 Definition. A ***group*** is a nonempty set G together with a binary operation $\star : G \times G \to G$ satisfying the following three properties.

(associativity) For all $f, g, h \in G$, we have $(f \star g) \star h = f \star (g \star h)$.
(identity) There exists $e \in G$ such that $g \star e = e \star g = g$ for all $g \in G$.
(inverse) For each $g \in G$, there exists $f \in G$ such that $g \star f = f \star g = e$.

A group G is ***abelian*** or ***commutative*** if $a \star b = b \star a$ for all $a, b \in G$.

1.0.1 Example. The integers $\mathbb{Z}$, the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, and the quaternions $\mathbb{H}$ are abelian groups under addition where the identity is $e = 0$ and the inverse of the number c is $-c$. ✧

The binary operation in a group is called a *product* and is often denoted by juxtaposition. For abelian groups, the group operation is traditionally denoted by $+$.

1.0.2 Example. The nonzero rational numbers $\mathbb{Q}^\times$, the nonzero real numbers $\mathbb{R}^\times$, and the nonzero complex numbers $\mathbb{C}^\times$ are all abelian groups under multiplication. In each of these groups, the identity is $e = 1$ and the inverse of the nonzero number c is the reciprocal $c^{-1} = 1/c$. The nonzero quaternions $\mathbb{H}^\times$ form a non-abelian group under multiplication. The nonzero integers do not form a group under multiplication because the only integers with a multiplicative inverse are ± 1. ✧

In making a definition, we emphasize the ***definiendum***, that which is being defined, by switching between italic and non-italic fonts and using a bold typeface.

1.0.3 Example. The ***circle*** $S^1 := \{z \in \mathbb{C} : |z| = 1\}$ is an abelian group under multiplication where the identity is $e = 1$. ✧

1.0.4 Example. For any nonnegative integer n, the nth roots of unity

$$\mu_n := \{\zeta^k = e^{2\pi ik/n} \in \mathbb{C} : 0 \leqslant k < n\}$$

form an abelian group under multiplication. The identity is $\zeta^0 = 1$ and the inverse of ζ^k is ζ^{n-k}. ✧

$\star$	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	h	e	a
h	h	g	f	e

Figure 1.1: Multiplication table for the Klein 4-group

1.0.5 Example. The ***Klein* 4*-group*** is a group with four elements. In this group, each element is an involution (equal to its inverse) and the product any two of the three non-identity elements produces the third. All products appear in Figure 1.1. ✧

1.0.6 Example. For any nonnegative integer n, the ***general linear group*** is the set of invertible $(n \times n)$-matrices where the product is matrix multiplication. It is a group because the product of two invertible matrices is again invertible and the inverse of an invertible matrix is invertible. The identity matrix is the identity element in this group. To specify the type of entries in the matrices, we write $\mathrm{GL}(n, \mathbb{Z})$, $\mathrm{GL}(n, \mathbb{Q})$, $\mathrm{GL}(n, \mathbb{R})$, or $\mathrm{GL}(n, \mathbb{C})$ for the general linear groups over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ respectively. ✧

We use a Fraktur typeface to denote special groups. The fraktur 'S' is $\mathfrak{S}$.

1.0.7 Example. For any set X, the ***symmetric group*** $\mathfrak{S}_X$ of X is the set of the bijective maps from X to X with the group operation being the composition of functions. The identity element in this group is just the identity map. ✧

1.0.8 Example. Let G be a group and X a nonempty set. The set of maps from X to G equipped with the pointwise product is itself a group. For all functions $f, g : X \to G$, the product $fg : X \to G$ is defined by $(fg)(x) := f(x) \star g(x)$. ✧

1.0.9 Lemma. *Let G be a group.*

(i) *There is a unique element $e \in G$ such that, for all $g \in G$, we have $g \star e = e \star g = e$.*

(ii) *For any element $g \in G$, there exists a unique element $f \in G$ such that $g \star f = f \star g = e$. This* **inverse** *of g is denoted by $g^{-1} := f$.*

(iii) *For all $f, g \in G$, we have $(g^{-1})^{-1} = g$ and $(f \star g)^{-1} = g^{-1} \star f^{-1}$.*

Proof.

(i) The identity axiom ensures that there exists an element $e \in G$ such that $g \star e = e \star g = e$ for all $g \in G$. If $e' \in G$ also has this property, then we have $e' = e' \star e = e$.

(ii) The inverse axiom ensures that there exists an element $f \in G$ such that $g \star f = f \star g = e$. If $f' \in G$ also has this property, then we have $f' = f' \star e = f' \star (g \star f) = (f' \star g) \star f = e \star f = f$.

(iii) Since $g \star g^{-1} = g^{-1} \star g = e$, we see that $g = (g^{-1})^{-1}$. We also have $(g \star f) \star (f^{-1} \star g^{-1}) = g \star (f \star f^{-1}) \star g^{-1} = g \star g^{-1} = e$, which yields $(f^{-1} \star g^{-1}) \star (g \star f) = e$ and $(g \star f)^{-1} = f^{-1} \star g^{-1}$. □

1.1 Permutations

Last updated: 2020–08–30

The most important group is, perhaps, the symmetric group $\mathfrak{S}_n$ of the finite set $[n] := \{1, 2, \dots, n\}$. Elements in this group are called permutations. There are three equivalent ways of thinking about these permutations.

(a) A ***permutation*** is an arrangement of the distinct elements in the set $[n]$. In ***one-line notation***, both $\sigma := 2\ 5\ 4\ 3\ 1$ and $\tau := 5\ 2\ 4\ 1\ 3$ are permutations of the set $[5] := \{1, 2, 3, 4, 5\}$.

(b) A permutation is bijection from the set $[n]$ to itself. From this perspective, the permutations σ and τ are the functions

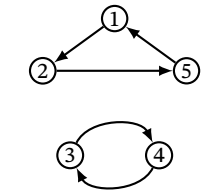
$$\begin{aligned} &\sigma(1) = 2 \quad \sigma(2) = 5 \quad \sigma(3) = 4 \quad \sigma(4) = 3 \quad \sigma(5) = 1\,, \text{ and} \\ &\tau(1) = 5 \quad \tau(2) = 2 \quad \tau(3) = 4 \quad \tau(4) = 1 \quad \tau(5) = 3\,. \end{aligned}$$

This point of view allows one to compose two permutations to obtain a new permutation. For example, we have

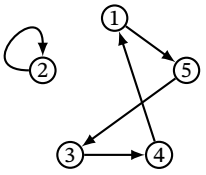
$$\begin{aligned} &(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(5) = 1 \quad (\tau \circ \sigma)(1) = \tau(\sigma(1)) = \tau(2) = 2 \\ &(\sigma \circ \tau)(2) = \sigma(\tau(2)) = \sigma(2) = 5 \quad (\tau \circ \sigma)(2) = \tau(\sigma(2)) = \tau(5) = 3 \\ &(\sigma \circ \tau)(3) = \sigma(\tau(3)) = \sigma(4) = 3 \quad (\tau \circ \sigma)(3) = \tau(\sigma(3)) = \tau(4) = 1 \\ &(\sigma \circ \tau)(4) = \sigma(\tau(4)) = \sigma(1) = 2 \quad (\tau \circ \sigma)(4) = \tau(\sigma(4)) = \tau(3) = 4 \\ &(\sigma \circ \tau)(5) = \sigma(\tau(5)) = \sigma(3) = 4 \quad (\tau \circ \sigma)(5) = \tau(\sigma(5)) = \tau(1) = 5\,, \end{aligned}$$

which implies that $\sigma \circ \tau = 1\ 5\ 3\ 2\ 4$ and $\tau \circ \sigma = 2\ 3\ 1\ 4\ 5$.

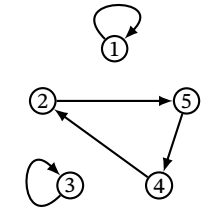
(c) A permutation is a directed graph with vertex set $\{1, 2, \dots, n\}$ such that each vertex is the head of an arrow and the tail of an arrow.



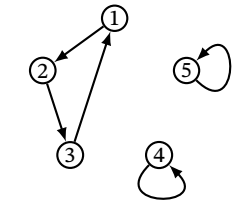
Directed graph of σ



Directed graph of τ



Directed graph of $\sigma \circ \tau$



Directed graph of $\tau \circ \sigma$

Figure 1.2: Directed graphs of various permutations

1.1.1 Proposition. *For any nonnegative integer n, there are*

$$n! := n(n-1)(n-2)\cdots(2)(1) = \prod_{j=1}^{n} j$$

permutations of the set $[n]$.

Inductive Proof. Since there is a unique map from the empty set to any set, there a unique permutation of the set $[0] = \varnothing$. Since the empty product equals 1, we also have $0! = 1$, which establishes the base case. For some nonnegative integer n, assume that there are $n!$ permutations of the set $[n]$. Constructing a permutation of the set $[n+1]$, there are $n+1$ choices for the first element in the arrangement. By the induction hypothesis, there are $n!$ arrangements of the remaining n elements. Hence, the total number of permutations is $(n+1)(n!) = (n+1)!$. □

For each nonnegative integer n, the ***symmetric group*** $\mathfrak{S}_n$ on the set $[n] := \{1, 2, \dots, n\}$ is the set of permutations together with the group operation given by function composition. The identity permutation id is given by the arrangement $1\ 2\ \cdots\ n$.

The 24 permutations of the set [4] are

1 2 3 4	3 4 1 2	2 3 1 4
2 1 3 4	4 3 2 1	3 1 2 4
3 2 1 4	1 4 2 3	2 3 4 1
4 2 3 1	1 4 2 3	3 4 2 1
1 3 2 4	3 2 4 1	3 1 4 2
1 4 3 2	4 2 1 3	4 3 1 2
1 2 4 3	2 4 3 1	2 4 1 3
2 1 4 3	4 1 3 2	4 1 2 3

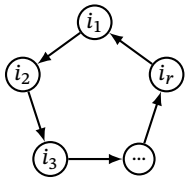


Figure 1.3: Directed graph of a cycle

1.1.2 Definition. Given a sequence $(i_1, i_2, \dots, i_r)$ of distinct elements from the set $[n]$, the ***cycle*** $\sigma := (i_1\ i_2\ \cdots\ i_r)$ is the permutation in $\mathfrak{S}_n$ defined by $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1$, and $\sigma(j) = j$ for all $j \in [n]\backslash\{i_1, i_2, \dots, i_r\}$. The underlying set $\{i_1, i_2, \dots, i_r\}$ is the ***orbit*** of the cycle and the cardinality of the orbit is ***length*** of the cycle. A ***transposition*** is a cycle of length 2. Two cycles are ***disjoint*** if their orbits are disjoint.

Following the standard conventions for composing functions, we multiply permutations from right to left. The two products of the cycles (3 1) and (2 1) are (3 1)(2 1) = (3 1 2) and (2 1)(3 1) = (3 2 1).

1.1.3 Lemma. *Disjoint cycles commute.*

Proof. Consider two disjoint cycles $\sigma, \tau \in \mathfrak{S}_n$. It suffices to prove that $\sigma \circ \tau(i) = \tau \circ \sigma(i)$ for all $i \in [n]$. Without loss of generality, suppose that i is in the orbit of τ, so we have $\tau(i) = j \neq i$. Since τ is injective, j is also in the orbit of τ. Because σ and τ are disjoint, $\sigma(i) = i$ and $\sigma(j) = j$. It follows that $\sigma \circ \tau(i) = j = \tau \circ \sigma(i)$. □

To eliminate the ambiguity in a cycle decomposition, one typically begins each cycle with its largest element and lists the cycles in increasing order by their first element. Cycles of length 1 are often omitted.

1.1.4 Proposition. *For any nonnegative integer n, every permutation in the symmetric group $\mathfrak{S}_n$ may be expressed as a disjoint union of cycles.*

Proof. We describe an algorithm that factors a permutation into a product of disjoint cycles.

Input: a permutation σ of the finite set $[n]$
Output: a factorization ϖ of σ into a product of disjoint cycles
Initialize $\varpi := \varnothing$
While there exists an $i \in [n]$ not appearing in ϖ do
    Find the largest $i \in [n]$ not appearing in ϖ;
    Initialize $r := 1$;
    While $\sigma^{r+1}(i) \neq i$ do $r = r + 1$;
    Prepend the cycle $(i\ \sigma(i)\ \sigma^2(i)\ \cdots\ \sigma^r(i))$ to ϖ;
Return ϖ

By design, each element in $[n]$ appears in a unique cycle of ϖ. The inner while loop must terminate because every vertex is the head of unique arrow and there are only finitely many vertices. □

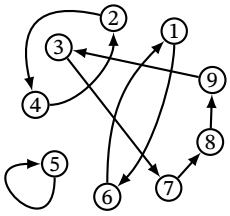


Figure 1.4: The cycle decomposition of $\sigma := 6\ 4\ 7\ 2\ 5\ 1\ 8\ 9\ 3 \in \mathfrak{S}_9$ is $\sigma = (4\ 2)(5)(6\ 1)(9\ 3\ 7\ 8)$

The 24 permutations of the set [4] are

(1)(2)(3)(4)	(3 1)(4 2)	(4)(3 1 2)
(2 1)(3)(4)	(3 2)(4 1)	(4)(3 2 1)
(2)(3 1)(4)	(1)(4 2 3)	(4 1 2 3)
(2)(3)(4 1)	(1)(4 3 2)	(4 1 3 2)
(1)(3 2)(4)	(2)(4 1 3)	(4 2 1 3)
(1)(3)(4 2)	(2)(4 3 1)	(4 2 3 1)
(1)(2)(4 3)	(3)(4 1 2)	(4 3 1 2)
(2 1)(4 3)	(3)(4 2 1)	(4 3 2 1)

1.1.5 Corollary. *For any nonnegative integer n, every permutation in the symmetric group $\mathfrak{S}_n$ is a product transpositions.*

Proof. It suffices to factor cycles. For all positive integers r, we claim that that $(i_1\ i_2\ \cdots\ i_r) = (i_1\ i_r)(i_1\ i_{r-1})\cdots(i_1\ i_2)$. We proceed by induction on r. Since the empty product is the identity, the base case $r = 1$ holds. Assuming the formula holds for $r - 1$, we have

$$\begin{aligned}(i_1\ i_r)\big((i_1\ i_r)(i_1\ i_{r-2})\cdots(i_1\ i_2)\big) &= (i_1\ i_r)(i_1\ i_2\ \cdots\ i_{r-1}) \\ &= (i_1\ i_2\ \cdots\ i_r)\,.\end{aligned}$$

□