

1 Groups

Copyright © 2025 by Gregory G. Smith
Last updated: 2025-09-03

Among the foundational axiomatic systems in mathematics, groups serve as our starting point. Originating in and uniting, the study of numbers, roots, and shapes, this mathematical structure pervades both pure and applied mathematics.

Throughout, the blackboard bold typeface is reserved for special sets of numbers. For instance, $\mathbb{N} := \{0, 1, 2, \dots\}$ denotes the set of nonnegative integers. To ensure that the cardinality of every finite set appears in this set, it must include zero.

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

1.0 Abstract Groups

Although groups involve just a single underlying set and one binary operation, this apparent simplicity belies the rich theory.

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

(*associativity*) For any elements f, g , and h in G , we have

$$(f \star g) \star h = f \star (g \star h).$$

(*identity*) There exists an element e in G such that, for any element g in G , we have $e \star g = g = g \star e$.

(*inverse*) For any element g in G , there exists an element f in G such that $g \star f = e = f \star g$.

A group G is *abelian* or *commutative* if, for any elements f and g in G , we have $f \star g = g \star f$.

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

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

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 a number c is $-c$. $\diamond$

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 case, the identity is $e = 1$, and the inverse of a number c is the reciprocal $c^{-1} = 1/c$. The nonzero quaternions $\mathbb{H}^\times$ form a nonabelian group under multiplication. The nonzero integers do not form a group under multiplication because the only integers with multiplicative inverses are 1 and -1 . $\diamond$

1.0.3 Example. The *circle group* or *1-torus* $\mathbb{T} := \{z \in \mathbb{C} \mid |z| = 1\}$ is an abelian group under multiplication where the identity is $e = 1$. $\diamond$

1.0.4 Example. For any positive integer n , the *n th roots of unity*

$$\mu_n := \{\zeta^k := \exp(2k\pi i/n) \in \mathbb{C} \mid 0 \leq k < n\}$$

form an abelian group under multiplication. The identity is $\zeta^0 = 1$, and the inverse of ζ^k is ζ^{n-k} for all $0 \leq k < n$. $\diamond$

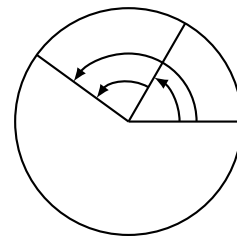


Figure 1.1: Multiplication in the circle group is equivalent to addition of angles

1.0.5 Example. Following [Felix Klein \(1884\)](#), the *Klein 4-group* has four elements: each is an involution (equal to its own inverse), and the product of any two distinct elements among the three nonidentity elements gives the third. All products appear in Figure 1.2. $\diamond$

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

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 itself with the group operation being the composition of functions. The identity element in this group is the identity map $\text{id}_X: X \rightarrow X$. $\diamond$

1.0.8 Lemma (basic properties). *Let G be a group.*

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

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

(inverse properties) *For any elements f and g in G , we have $(g^{-1})^{-1} = g$ and $(f \star g)^{-1} = g^{-1} \star f^{-1}$.*

Proof. The identity property ensures that there exists an element e in G such that $e \star g = e = g \star e$ for any element g in G . If the element e' in G also has this property, then it follows that $e' = e' \star e = e$.

For any element g in G , the inverse property ensures that there exists an element f in G such that $g \star f = e = f \star g$. If the element f' in G also has this property, then we deduce that

$$f' = f' \star e = f' \star (g \star f) = (f' \star g) \star f = e \star f = f.$$

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

1.0.9 Example. Let G be a group and let X be a set. The set of maps from X to G , equipped with the pointwise product, forms the *X -fold direct product* group $G^X = \prod_{x \in X} G$. For any functions $f: X \rightarrow G$ and $g: X \rightarrow G$, the product $fg: X \rightarrow G$ is defined, for all x in X , by $(fg)(x) := f(x) \star g(x)$. The identity in G^X is the constant function defined, for all x in X , by $x \mapsto e$ where e is the identity in G . The inverse of $f: X \rightarrow G$ is defined, for all x in X , by $x \mapsto (f(x))^{-1}$. $\diamond$

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

Figure 1.2: Multiplication table for the Klein 4-group

The identity in the general linear group is the diagonal $(n \times n)$ -matrix

$$I := \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}.$$

We use a [Fraktur](#) typeface to denote special groups. The Fraktur 'S' is $\mathfrak{S}$.

The three defining properties for the group of maps from X to G are inherited from the corresponding properties on the group G .

1.1 Permutations

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

(*arrangement*) A permutation is an arrangement (also known as a total order) of the distinct elements in the set $[n]$.

(*bijection*) A permutation is a bijection from the set $[n]$ to itself.

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

1.1.1 Example. In *one-line notation*, the arrangements $\sigma := 2\ 5\ 4\ 3\ 1$ and $\tau := 5\ 2\ 4\ 1\ 3$ are permutations of the set $[5] := \{1, 2, 3, 4, 5\}$. As bijections, the permutations σ and τ are the functions

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

Composing these permutations, we have two distinct products:

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

which implies that $\sigma \circ \tau = 1\ 5\ 3\ 2\ 4$ and $\tau \circ \sigma = 2\ 3\ 1\ 4\ 5$. Figure 1.3 illustrates the directed graphs for σ , τ , $\sigma \circ \tau$, and $\tau \circ \sigma$. $\diamond$

1.1.2 Remark. Example 1.1.1 shows that, for any integer n greater than 2, the symmetric group $\mathfrak{S}_n$ is nonabelian.

1.1.3 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 finite set $[n]$.

Inductive proof. There is a unique map from the empty set to any set, so there is a unique permutation of the set $[0] = \emptyset$. Since the empty product equals 1, we also have $0! = 1$, which proves the base case. For any nonnegative integer n , assume there are $n!$ permutations of the set $[n]$. In a permutation of the set $[n+1]$, there are $n+1$ choices for the first element. By the induction hypothesis, there are $n!$ arrangements of the remaining n elements. Hence, the total number of permutations is $(n+1)(n!) = (n+1)!$. $\square$

The identity permutation in $\mathfrak{S}_n$ is the arrangement $1\ 2\ 3\ \dots\ n$.

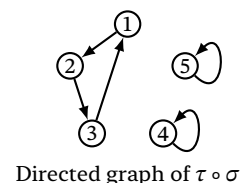
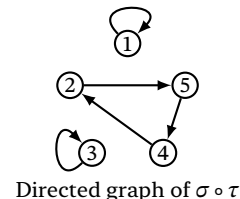
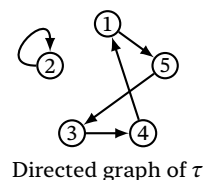
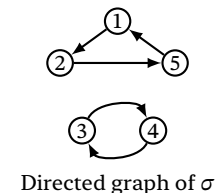


Figure 1.3: Directed graphs of some permutations

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

1.1.4 Definition. Given a sequence $(i_1, i_2, \dots, i_r)$ of distinct elements from the set $[n]$, the **cycle** $\sigma := (i_1 \ i_2 \ \dots \ i_r)$ 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 $j \in [n] \setminus \{i_1, i_2, \dots, i_r\}$. 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. Cycles are **disjoint** if their orbits are disjoint.

1.1.5 Lemma. *Disjoint cycles commute.*

Proof. Consider two disjoint cycles σ and τ in $\mathfrak{S}_n$. It suffices to prove that $(\sigma \circ \tau)(i) = (\tau \circ \sigma)(i)$ for all $i \in [n]$. When i is in the orbit of τ , 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 $(\sigma \circ \tau)(i) = j = (\tau \circ \sigma)(i)$. $\square$

1.1.6 Proposition. *For any nonnegative integer n , every permutation in the symmetric group $\mathfrak{S}_n$ is a product of disjoint 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 $\varpi := \emptyset$

While there exists an $i \in [n]$ not appearing in ϖ do

Find the largest $i \in [n]$ not appearing in ϖ ;

Initialize $r := 0$;

While $\sigma^{r+1}(i) \neq i$ do $r = r + 1$;

Prepend the cycle $(i \ \sigma(i) \ \sigma^2(i) \ \dots \ \sigma^r(i))$ 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. $\square$

1.1.7 Warning. Following the standard conventions for 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 $(2 \ 1)(3 \ 1) = (3 \ 2 \ 1)$.

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

Proof. It suffices to factor cycles. For any positive integer r , we claim that $(i_1 \ i_2 \ \dots \ i_r) = (i_1 \ i_r)(i_1 \ i_{r-1}) \dots (i_1 \ i_2)$. 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

$$(i_1 \ i_r)((i_1 \ i_{r-1})(i_1 \ i_{r-2}) \dots (i_1 \ i_2)) = (i_1 \ i_r)(i_1 \ i_2 \ \dots \ i_{r-1}) \\ = (i_1 \ i_2 \ \dots \ i_r). \quad \square$$

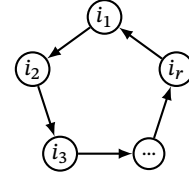


Figure 1.4: Directed graph of the cycle $(i_1 \ i_2 \ \dots \ i_r)$

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.

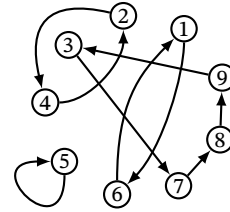


Figure 1.5: The cycle decomposition of the permutation $\sigma := 6 \ 4 \ 7 \ 2 \ 5 \ 1 \ 8 \ 9 \ 3$ is $\sigma = (4 \ 2)(5)(6 \ 1)(9 \ 3 \ 7 \ 8)$

The 24 permutations of the set $[4]$ are

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

1.2 Subgroups

Reductionism postulates that an object can be understood through its subobjects. This basic philosophy permeates mathematics.

1.2.1 Definition. Let G be a group. A subset H of G is a **subgroup** if the restriction of the product on G induces a group structure on H .

1.2.2 Lemma. A nonempty subset H of a group G is a subgroup if and only if, for any elements g and h in H , the product $g h^{-1}$ belongs to H .

Proof. Suppose that H is a group. Since each element in H has an inverse and the product of two elements in H is also an element in H , we deduce that $g h^{-1} \in H$ for any elements g and h in H .

Because associativity is inherited from the group G , the product on G induces a group operation on H if and only if the following three conditions are satisfied:

(closure) For any g and h in H , the product $g h \in G$ belongs to H .

(identity) The identity element e in G belongs to H .

(inverse) For any element h in H , the inverse h^{-1} belongs to H .

Suppose that $g h^{-1} \in H$ for any elements g and h in H . Since the subset H is nonempty, there exists an element h in H , which implies that $e = h h^{-1}$ belongs to H . For any element h in H , we deduce that $h^{-1} = e h^{-1}$ also belongs to H . Finally, for any elements g and h in H , we see that $g h = g (h^{-1})^{-1}$ belongs to H . $\square$

1.2.3 Example. Each inclusion in the chains $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ and $\mu_n \subset \mathbb{T} \subset \mathbb{C}^\times$ defines a subgroup. Although the nonzero rational numbers $\mathbb{Q}^\times$ form a group under multiplication, this subset is not a subgroup of the rational numbers $\mathbb{Q}$. $\diamond$

1.2.4 Example. The *special linear group*

$$\mathrm{SL}(n, \mathbb{R}) := \{A \in \mathrm{GL}(n, \mathbb{R}) \mid \det(A) = 1\}$$

is a subgroup of the general linear group because the determinant of a product is equal to the product of determinants. $\diamond$

1.2.5 Definition. The *centralizer* of a subset X of a group G is the set of elements in G that commute with every element of X ;

$$C_G(X) := \{g \in G \mid gx = xg \text{ for all } x \text{ in } X\}.$$

1.2.6 Proposition. For any subset X of a group G , the centralizer $C_G(X)$ is a subgroup of G .

Proof. An element g in G lies in the centralizer $C_G(X)$ if and only if, for any x in X , we have $gx = xg \Leftrightarrow x = g^{-1}xg \Leftrightarrow x = gxg^{-1}$. For any elements f and g in $C_G(X)$ and any element x in X , we obtain $(fg^{-1})^{-1}x(fg^{-1}) = gf^{-1}xfg^{-1} = gxg^{-1} = x$. Thus, Lemma 1.2.2 shows that $C_G(X)$ is a subgroup of G . $\square$

For any group G , the set G itself is a subgroup of G , and the subset $\{e\}$, consisting of only the identity element, is always a subgroup of G .

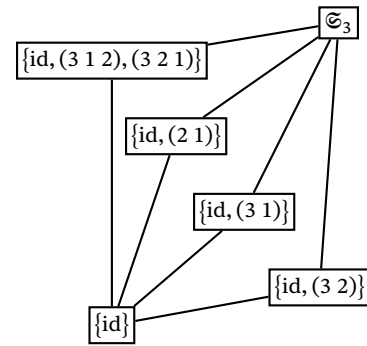


Figure 1.6: Hasse diagram of all subgroups in $\mathfrak{S}_3$

1.2.7 Definition. The *centre* of a group G is the centralizer of the group itself: $Z(G) := C_G(G) = \{g \in G \mid fg = gf \text{ for all } f \in G\}$.

A group G is abelian if and only if it is equal to its centre: $Z(G) = G$.

1.2.8 Lemma. Let X be a set. For any family $\{H_x \mid x \in X\}$ of subgroups in a group G , the intersection $H := \bigcap_{x \in X} H_x$ is also a subgroup of G .

Proof. Since $e \in H_x$ for all $x \in X$, it follows that $H \neq \emptyset$. Consider elements f and g in H . The definition of intersection implies that $f \in H_x$ and $g \in H_x$ for all $x \in X$. Since H_x is a subgroup of G , we see that $fg^{-1} \in H_x$ for all $x \in X$. We deduce that $fg^{-1} \in H$ and Lemma 1.2.2 shows that H is a subgroup of G . $\square$

1.2.9 Definition. The subgroup $\langle X \rangle$ *generated* by a subset X of a group G is the intersection of all subgroups in G that contain X . The group G is *finitely generated* if there exists a finite subset X such that $G = \langle X \rangle$, and the group G is *cyclic* if there exists an element g in G such that $G = \langle g \rangle := \langle \{g\} \rangle$.

The group μ_n of n th roots of unity is cyclic, generated by $\zeta := \exp(2\pi i/n)$. Corollary 1.1.8 establishes that the symmetric group $\mathfrak{S}_n$ is generated by the $\binom{n}{2}$ transpositions.

1.2.10 Definition. The *order* $|G|$ of a group G is the cardinality of its underlying set.

Proposition 1.1.3 proves that $\mathfrak{S}_n$ has order $n!$. The group μ_n has order n and the Klein 4-group has order 4.

1.2.11 Lemma. Fix an element g in a group G and consider $H := \langle g \rangle$.

(infinite order) The cyclic subgroup H has infinite order if and only if, for any positive integer n , we have $g^n \neq e$.

(finite order) When the subgroup H has finite order, its order $|H|$ is the smallest positive integer m such that $g^m = e$.

(divisibility) There exists a positive integer k such that $g^k = e$ if and only if the order $|H|$ divides k .

Proof. Suppose that $g^n \neq e$ for any positive integer n . If there were positive integers r and s such that $r < s$ and $g^r = g^s$, then we would have $g^{s-r} = e$ contradicting our supposition. We deduce that $|\{g^n \mid n \in \mathbb{N}\}| = |\mathbb{N}|$, so H has infinite order. Conversely, suppose that there is a positive integer n such that $g^n = e$. For any positive integer s , there are nonnegative integers q and r such that $s = qn + r$ and $0 \leq r < n$. It follows that $g^s = g^{qn+r} = (g^n)^q g^r = g^r$. Thus, we deduce that $H \subseteq \{e, g, g^2, \dots, g^{n-1}\}$, so H has finite order.

Suppose that the cyclic subgroup H has finite order. Let m be the minimum positive integer such that $g^m = e$. If there were integers r and s such that $0 \leq r < s \leq m-1$ and $g^r = g^s$, then we would have $g^{s-r} = e$ contradicting our choice of m . Hence, we must have $H = \{e, g, \dots, g^{m-1}\}$ and $|H| = m$.

Suppose that $g^k = e$ and set $m := |H|$. There exists nonnegative integers q and r such that $k = qm + r$ and $0 \leq r < m$. Since we have $e = g^k = g^{qm+r} = (g^m)^q g^r = g^r$, the finite order condition implies that $r = 0$, so $k = qm$ and the order $|H|$ divides k . $\square$

The *order* of an element g in a group G is, by definition, the cardinality of the subgroup it generates and equals the smallest positive integer m such that $g^m = e$.

1.3 Automorphism Groups

Why would any sensible person introduce the abstract concept of a group? In practice, groups arise as the symmetries of an object.

1.3.1 Definition. A *morphism* is a structure-preserving map from one object to another having the same mathematical structure. We write $\varphi: X \rightarrow Y$ for a morphism φ with *source* X and *target* Y . The composition $\psi \circ \varphi$ of the morphisms φ and ψ is defined when the target of φ is the source of ψ . Composition satisfies two axioms.

(*associativity*) For any triple $\theta: W \rightarrow X$, $\varphi: X \rightarrow Y$, and $\psi: Y \rightarrow Z$ of morphisms, we have $\psi \circ (\varphi \circ \theta) = (\psi \circ \varphi) \circ \theta$.

(*identity*) For every object X , there is an *identity morphism* $\text{id}_X: X \rightarrow X$ such that, for any morphism $\varphi: X \rightarrow Y$, we have $\text{id}_Y \circ \varphi = \varphi = \varphi \circ \text{id}_X$.

1.3.2 Example. A morphism of sets is an arbitrary map. For vector spaces, it is a linear map; for topological spaces, it is a continuous map; and for differentiable manifolds, it is a differentiable map. $\diamond$

1.3.3 Definition. A morphism $\varphi: X \rightarrow Y$ is an *isomorphism* if there exists a morphism $\psi: Y \rightarrow X$ such that $\psi \circ \varphi = \text{id}_X$ and $\varphi \circ \psi = \text{id}_Y$. An *automorphism* is an isomorphism whose source and target are identical objects.

1.3.4 Example. An isomorphism of sets is a bijective map. For vector spaces, it is an invertible linear map; for topological spaces, it is a homeomorphism (also known as a bicontinuous function); and for differentiable manifolds, it is a diffeomorphism (the function and its inverse are continuously differentiable). $\diamond$

As follows immediately from the definitions, the automorphisms of a given mathematical object form a group.

1.3.5 Definition. The *automorphism group* $\text{Aut}(X)$ of an object X is the group of all automorphisms of X .

1.3.6 Example. The automorphism group of a set X is precisely the symmetric group $\mathfrak{S}_X$. $\diamond$

1.3.7 Example. For any positive integer n , the *dihedral group* D_n is the automorphism group of a regular polygon with n edges. The group D_n has order $2n$ because a regular polygon with n edges has $2n$ different automorphisms, consisting of n rotational symmetries and n reflection symmetries. $\diamond$

1.3.8 Example. The *orthogonal group*, which is defined to be

$$\text{O}(n, \mathbb{R}) := \{A \in \text{GL}(n, \mathbb{R}) \mid A^T A = I\},$$

The opening question rephrases a query by [Vladimir I. Arnold \(1998\)](#).

Definition 1.3.1 foreshadows our discussion of categories; compare with Definition 11.4.1

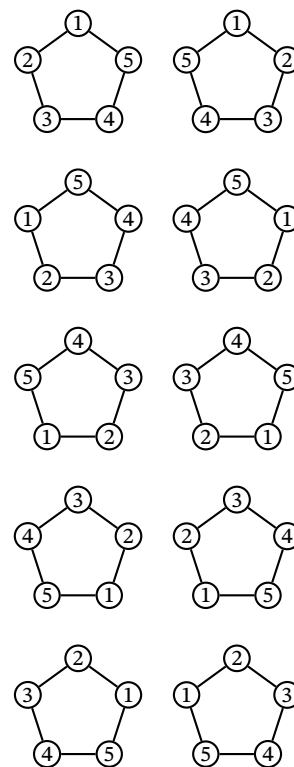


Figure 1.7: An illustration of the 10 elements in the dihedral group D_5

consists of the distance-preserving linear maps on the Euclidean space $\mathbb{R}^n$ because $\|A\mathbf{v}\|^2 = (A\mathbf{v})^T(A\mathbf{v}) = \mathbf{v}^T A^T A \mathbf{v} = \mathbf{v}^T \mathbf{v} = \|\mathbf{v}\|^2$. Thus, the orthogonal group $O(n, \mathbb{R})$ is the automorphism group of the normed vector space $\mathbb{R}^n$. $\diamond$

To justify the group axioms, we demonstrate that every group is the automorphism group of some mathematical object. To reduce the mathematical prerequisites, we employ certain directed graphs.

1.3.9 Definition. An automorphism of an edge-coloured directed graph is a permutation σ of its vertex set such that an ordered pair of vertices (u, v) is an arrow from u to v coloured c if and only if the ordered pair $(\sigma(u), \sigma(v))$ is an arrow from $\sigma(u)$ to $\sigma(v)$ coloured c .

1.3.10 Theorem. Every group is the automorphism group of some edge-coloured directed graph.

Proof. Let G be a group. The *Cayley diagram* Γ of this group is the edge-coloured directed graph constructed as follows:

- (vertices) The vertex set $V(\Gamma)$ is the underlying set of the group G .
- (colours) Each arrow is assigned a colour from the set $G \setminus \{e\}$.
- (arrows) For any v in $V(\Gamma)$ and any c in $G \setminus \{e\}$, the ordered pair (v, vc) forms an arrow from v to vc that is coloured c .

By design, the colour of an arrow (v, vc) in Γ can be reconstructed from the appropriate product of its tail and head: $v^{-1}(vc) = c$. We claim that the group G is the automorphism group $\text{Aut}(\Gamma)$.

We first show that each element in the group G determines an automorphism of the Cayley diagram Γ . For any element g in G , consider the map $\lambda_g: V(\Gamma) \rightarrow V(\Gamma)$ defined by $\lambda_g(v) := gv$. The associativity property of the group G implies that, for any elements g and h in G , we have $\lambda_g \circ \lambda_h = \lambda_{gh}$. Since $\lambda_g \circ \lambda_{g^{-1}} = \lambda_e = \text{id}_{V(\Gamma)}$ and $\lambda_{g^{-1}} \circ \lambda_g = \lambda_e = \text{id}_{V(\Gamma)}$, the map λ_g is a permutation of the set $V(\Gamma)$. Since each element in G has an inverse, it follows that the ordered pair (v, vc) is an arrow in Γ coloured c if and only if the ordered pair $\lambda_g(v, vc) = (gv, gvc)$ is an arrow in Γ coloured c .

For the other direction, suppose that σ is an automorphism of the Cayley diagram Γ . For all c in $G \setminus \{e\}$, the ordered pair (e, c) is an arrow in Γ coloured c if and only if the ordered pair $(\sigma(e), \sigma(c))$ is an arrow in Γ coloured c . Hence, we deduce that $(\sigma(e))^{-1}\sigma(c) = c$ or $\sigma(c) = \sigma(e)c$, so we conclude that $\sigma = \lambda_{\sigma(e)}$. $\square$

1.3.11 Remark. There are many other universality results proving that all groups arise as the automorphism groups of some specific mathematical structure including graphs, trivalent graphs, lattices, fields, topological spaces, and commutative rings.

The dihedral group D_n is a finite subgroup of $O(2, \mathbb{R})$.

Robert Wertheimer Frucht (1939) proves that every finite group is isomorphic to the automorphism group of some finite graph. Johannes de Groot (1959) and Gert Sabidussi (1960) independently show that any group can be realized as the automorphisms of an infinite graph.

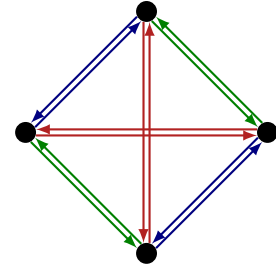


Figure 1.8: The Cayley diagram of the Klein 4-group

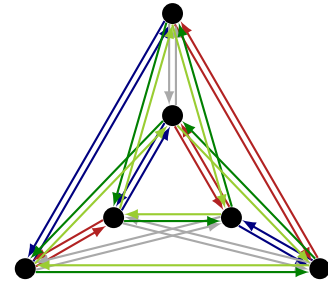


Figure 1.9: The Cayley diagram of the symmetric group $\mathfrak{S}_3$

In *geometric group theory*, one identifies the colour classes of c and c^{-1} to convert the directed graph into a graph. This graph is endowed with the structure of a metric space.