Dummit & Foote Notes

blanket

Fall 2025

Contents

0 Preliminaries

0.1 Basics

Definition 0.1 ▶ Basic Objects

- The **order** or **cardinality** of a set A will be denoted with $|A|$.
- The **Cartesian product** of two sets A and B is the collection of elements

$$A \times B := \{(a,b) \mid a \in A, b \in B\}$$

- The following are common sets:
  - $\mathbb{Z}$ is the set of integers $\{\ldots,-2,-1,0,1,2,\ldots\}$.
  - $\mathbb{Q}$ is the set of rationals $\{p/q \mid p \in \mathbb{Z}, q \in \mathbb{Z}-\{0\}\}$.
  - $\mathbb{R}$ is the set of real numbers whose decimal expansions cannot be written as a rational.
  - $\mathbb{C}$ is the set of complex numbers $\{a+bi \mid a,b \in \mathbb{R}, i^2=-1\}$.

  Moreover, we denote $\mathbb{Z}^+, \mathbb{Q}^+$, and $\mathbb{R}^+$ to be the positive sets of $\mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$ respectively.

Definition 0.2 ▶ Function Terminology

- A **function** f from A to B is denoted as $f : A \to B$, where the value of f at some $a \in A$ is denoted by $f(a)$.
- The **domain** of f is A, and the **codomain** of f is B. Moreover, we use the notation $f : a \mapsto b$ or $a \mapsto b$ to denote that $f(a) = b$, or that the function is specified on elements.
- The **range** or **image** of f (also known as the **image of** A **under** f is given by

$$f(A) := \{b \in B \mid f(a) = b \text{ for some } a \in A\}$$

- The **preimage** or **inverse image** of some subset C of B is given by

$$f^{-1}(C) := \{a \in A \mid f(a) \in C\}$$

  Moreover, the **fiber of** f **over** b for some $b \in B$ is the preimage of b wherein we may replace C with b above.
- Let $f : A \to B$ and $g : B \to C$ be functions. Then the **composite map** $g \circ f : A \to C$ is given by

$$(g \circ f)(a) := g(f(a))$$

- f is **injective** or an **injection** whenever $a_1 \neq a_2$ implies $f(a_1) \neq f(a_2)$.
- f is **surjective** or a **surjection** if for every $b \in B$ there exists $a \in A$ such that $f(a) = b$, i.e., $f(A) = B$.
- f is **bijective** or a **bijection** when it is both injective and surjective.
- A **left inverse** of f is a function $g : B \to A$ such that $g \circ f : A \to A$ is the identity map on A, i.e., $(g \circ f)(a) = a$ for every $a \in A$.
- A **right inverse** of f is a function $h : B \to A$ such that $f \circ h : B \to B$ is the identity map on B.

Proposition 0.1 ▶ Implication of Function Qualities

Let $f : A \to B$.

1. f is injective if and only if f has a left inverse.
2. f is surjective if and only if f has a right inverse.
3. f is a bijection if and only if there exists $g : B \to A$ such that $f \circ g$ is the identity map on B and $g \circ f$ the identity map on A.
4. If A and B are finite sets where $|A| = |B|$, then $f : A \to B$ is bijective if and only if f is injective if and only if f is surjective.

Proof.

1. ($\Rightarrow$) We first note that A must be nonempty, for otherwise if $A = \varnothing$, then $f : \varnothing \to B$ is vacuously injective. However, no left inverse $g : B \to \varnothing$ of f may exist, since there is no element for $b \in B$ to be mapped to in $\varnothing$ as it contains no elements, by definition. Now suppose f is injective. To construct a left inverse, note that B can be split up into two subsets: $f(A)$ and its complement, $B \backslash f(A)$. If $b \in f(A)$, by definition, there is some $a \in A$ where $f(a) = b$. If $b \notin f(A)$, we may simply choose some element in A to map to. Explicitly, we define a function $g : B \to A$ as follows, fixing some a^*

$$g(b) = \begin{cases} a & a \in A \text{ such that } f(a) = b \\ a^* & b \in B \backslash f(A) \end{cases}$$

This is clearly a left inverse, because for any $a \in A$, we have $f(a) = b$ for some $b \in B$ so that $g(f(a)) = g(b) = a$.

($\Leftarrow$) Suppose now that f has a left inverse g, and let $x, y \in A$ such that $f(x) = f(y)$. Then $g(f(x)) = g(f(y))$. Since g is a left inverse, then $x = y$.

2. ($\Rightarrow$) Suppose f is surjective. Then each fiber of f over every $b \in B$ is nonempty. We may then arbitrarily associate each b with a singular $a_b \in A$ such that $f(a_b) = b$. We may then define a mapping $h : B \to A$ as follows: for any $b \in B$, then $h(b) = a_b$. Then $f(h(b)) = f(a_b) = b$ so that h is a right inverse of f.

   ($\Leftarrow$) Suppose that f has a right inverse h, and let $b \in B$. Then for any $h(b) \in h(B)$, we have $f(h(b)) = b$ so that f is surjective.

3. ($\Rightarrow$) Suppose f is bijective, and let $b \in B$. Since f is surjective, there exists some $a \in A$ such that $f(a) = b$. Moreover, this a is unique because f is injective. Define the function $g : B \to A$ by $g(b) = a$. Then for any $a \in A$, we have $g(f(a)) = g(b) = a$. For any $b \in B$, we have $f(g(b)) = f(a) = b$ so that $g \circ f$ is the identity map on A, and $f \circ g$ is the identity map on B.

   ($\Leftarrow$) Suppose there exists $g : B \to A$ such that $f \circ g$ is the identity map on B, and $g \circ f$ is the identity map on A. Then g is a left inverse and a right inverse of f, hence f is injective and surjective. Then f is bijective, by definition.

4. Suppose f is bijective. It is then injective.

   Suppose f is injective. Then distinct elements of A map to distinct elements of B. Since $|A| = |B|$, then all elements of B are mapped to, hence f is surjective.

   Suppose f is surjective. Then each element of B has at least one element of A that maps to it. Since f is well-defined, then no element of A maps to more than one element in B. Because $|A| = |B|$, then each element in A maps to a distinct element in B, hence f is injective. Then it is bijective, by definition. □

Definition 0.3 ▶ Types of Functions

- In (3) of Proposition 0.1, the map g is unique and is called the **2-sided inverse** of f.
- A **permutation** of a set A is a bijection from A to itself.
- Let $A \subseteq B$ with $f : B \to C$. Then the **restriction** of f to A is denoted by $f|_A$.
- Let $A \subseteq B$ with $g : A \to C$. Let $f : B \to C$ such that $f|_A = g$. Then f is an **extension** of g to B, where f does not need to exist nor be unique.

Definition 0.4 ▶ Relations

Let A be a nonempty set.

- A **binary relation** on a set A is a subset R of $A \times A$, and we write $a \sim b$ when $(a, b) \in R$.
- We say the relation $\sim$ on A is:
  1. **reflexive** if $a \sim a$ for every $a \in A$,
  2. **symmetric** if $a \sim b$ implies $b \sim a$ for every $a, b \in A$,
  3. **transitive** if $a \sim b$ and $b \sim c$ imply $a \sim c$ for all $a, b, c \in A$.
- A relation is an **equivalence relation** when it is reflexive, symmetric, and transitive.
- Let $\sim$ be an equivalence relation on A. Then the **equivalence class** of $a \in A$ is the set $\{x \in A \mid x \sim a\}$. Moreover, the elements of this set are said to be **equivalent** to a. If B is an equivalence class, then any $b \in B$ is a **representative** of B.
- A **partition** of A is some collection $\{A_i \mid i \in I\}$ of nonempty subsets, for some indexing set I, such that
  1. $A = \bigcup_{i \in I} A_i$,
  2. $A_i \cap A_j = \emptyset$ for every $i, j \in I$ where $i \neq j$.

Proposition 0.2 ▶ Fundamental Theorem of Equivalence Relations

Let A be a nonempty set.

1. If $\sim$ is an equivalence relation on A, then the set of equivalence classes of $\sim$ form a partition of A.
2. If $\{A_i \mid i \in I\}$ is a partition of A, then there is an equivalence class relation on A whose equivalence classes are the sets A_i for $i \in I$.

Proof.

1. Let I be an indexing set, put $B = \bigcup_{i \in I} A_i$, and let $\{A_i \mid i \in I\}$ be the set of equivalence classes of $\sim$. Since $A_i \subseteq A$ for each $i \in I$, then $B \subseteq A$. Pick some $a \in A$. Since $\sim$ is reflexive, then $a \sim a$ so that $a \in A_j$ for some $j \in I$. Then $a \in B$ so that $A \subseteq B$, hence $A = B$. To show that these equivalence classes are pairwise disjoint, it suffices to show that they if they are not, then they must be equal. To that end, suppose $A_i \cap A_j$ is not empty for some $i, j \in I$, let a and b be representatives of A_i and A_j respectively, and let $c \in A_i \cap A_j$. By definition, $a \sim c$ and $c \sim b$. By transitivity of $\sim$, we have $a \sim b$. Suppose some $x \in A_i$. Then $x \sim a$ so that $x \sim b$, and $x \in A_j$. Similarly, $y \in A_j$ implies $b \sim y$ so that $a \sim y$, and $y \in A_i$. Then $A_i = A_j$ so that that any two equivalence classes are either distinct or equal.

2. Define a relation on A as follows: $a \sim b$ if and only if $a, b \in A_i$ for some $i \in I$. Clearly, $a \sim a$ so that $\sim$ is reflexive. If $a \sim b$, then $a, b \in A_i$ so that $b, a \in A_i$. Hence, $b \sim a$, and $\sim$ is symmetric. Moreover, if $a \sim b$ and $b \sim c$, then $a, b \in A_i$ and $b, c \in A_j$. Since $A_i \cap A_j$ is nonempty, then $A_i = A_j$, hence $a, c \in A_i$ so that $a \sim c$. Then $\sim$ is transitive, hence it is an equivalence relation. □

0.2 Properties of the Integers

Definition 0.5 ▶ Integer Properties

- **Well Ordering of** $\mathbb{Z}$: If A is a nonempty subset of $\mathbb{Z}^+$, then there exists $m \in A$ such that $m \leq a$ for all $a \in A$. We say m is the **minimal element** of A.
- For $a, b \in \mathbb{Z}$ with $a \neq 0$, then a **divides** b if there is some $c \in \mathbb{Z}$ such that $ac = b$. We write $a \mid b$. Otherwise, if a does not divide b, then we write $a \nmid b$.
- If $a, b \in \mathbb{Z} - \{0\}$, there exists a unique positive integer d called the **greatest common divisor** of a and b where
  1. $d \mid a$ and $d \mid b$ so that d is a common divisor,
  2. If e is another element such that $e \mid a$ and $e \mid b$, then $e \mid d$ so that d is the *greatest* common divisor.

  We denote d as (a, b). Moreover. if $(a, b) = 1$, we say a and b are **relatively prime**.
- If $a, b \in \mathbb{Z} - \{0\}$, there exists a unique positive integer ℓ called the **least common multiple** of a and b where
  1. $a \mid \ell$ and $b \mid \ell$ so that ℓ is a common multiple,
  2. If k is another positive integer such that $a \mid k$ and $b \mid k$, then $\ell \mid k$ so that ℓ is the *least* common multiple.

  Moreover, for any two elements a, b with a greatest common divisor d and least common multiple ℓ, then $ab = d\ell$.

Definition 0.6 ▶ Division and Euclidean Algorithms

- **Division Algorithm**: For $a, b \in \mathbb{Z} - \{0\}$, there exists unique $q, r \in \mathbb{Z}$ such that

$$a = bq + r, 0 \leq r < |b|$$

  where q is the **quotient** and r is the **remainder**.
- **Euclidean Algorithm**: a procedure that produces a greatest common divisor between two integers a and b done by iterating the Division Algorithm. For $a, b \in \mathbb{Z} - \{0\}$, we get a sequence of quotients and remainders:

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

  Note that the sequence of remainders r_i terminates eventually, since they are a decreasing sequence of non-negative integers. We then have that $(a, b) = r_n$.
- A consequence of the Euclidean Algorithm is the $\mathbb{Z}$**-linear combination of** a **and** b. For some $a, b \in \mathbb{Z} - \{0\}$, there exists $x, y \in \mathbb{Z}$ such that

$$(a, b) = ax + by$$

  We can obtain this by recursively solving for r_n in the equations above until we get r_n in terms of a and b again.

Example ▶ Applying the Euclidean Algorithm and Finding the $\mathbb{Z}$-Linear Combination

Let $a = 57970$ and $b = 10353$. Applying the Euclidean Algorithm, we obtain

$$\begin{aligned} 57970 &= (5)10353 + 6205 \\ 10353 &= (1)6205 + 4148 \\ 6205 &= (1)4148 + 2057 \\ 4148 &= (2)2057 + 34 \\ 2057 &= (60)34 + 17 \\ 34 &= (2)17 \end{aligned}$$

so that $(57950, 10353) = 17$. We may then find the $\mathbb{Z}$-linear combination of a and b as follows:

$$\begin{aligned}
17 &= 2057 - (60)34 \\
&= 2057 - 60(4148 - 2(2057)) = -60(4148) + 121(2057) \\
&= -60(4148) + 121(6205 - 4148) = 121(6205) - 181(4148) \\
&= 121(6205) - 181(10353 - 6205) = -181(10353) + 302(6205) \\
&= -181((10353) + 302(57970 - 5(10353)) = 302(57970) - 1691(10353)
\end{aligned}$$

so that $x = 302$ and $y = -1691$. Note that x and y are not unique.

Definition 0.7 ▶ Primality

We say $p \in \mathbb{N}$ is **prime** when $p > 1$ and the only positive divisors of p are p and 1 itself. An integer that is not prime is **composite**. Moreover, if p is prime and $p \mid ab$ for $a, b \in \mathbb{Z}$, then $p \mid a$ or $p \mid b$.

Proof. Let p be some prime, and let $a, b \in \mathbb{Z}$ such that $p \mid ab$. If $p \mid a$, we are done. Suppose now that $p \nmid a$. There must exist some $k \in \mathbb{Z}$ such that $kp = ab$. Since $(p, a) = 1$, then there exist integers $x, y \in \mathbb{Z}$ such that

$$px + ay = 1$$

Multiplying both sides by b, we obtain:

$$bpx + aby = b$$

Recall that $kp = ab$. Then

$$\begin{aligned}
bpx + kpy &= b \\
p(bx + ky) &= b
\end{aligned}$$

hence $p \mid b$. □

Definition 0.8 ▶ Fundamental Theorem of Arithmetic

Any $n \in \mathbb{Z}^+$ can be uniquely factored into a product of primes $p_1, p_2, \ldots, p_s$ with $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathbb{Z}^+$ such that:

$$n = \prod_{i=1}^{s} p_i^{\alpha_i}$$

Proof. We proceed by induction. Since 1 and 2 are divisible by 1 and itself only, the base cases are covered. Let $n \in \mathbb{Z}^+$ be given, and suppose any integer below n can be factored into a product of primes. Then for n itself, we have two cases: if n is prime, we are done. Suppose it is not prime. Then n is composite, and there are $a, b \in \mathbb{Z}^+$ such that $n = ab$, and $a < n$ and $b < n$. By the inductive hypothesis, both a and b can be decomposed into a product of primes, hence n is a product of primes.

To prove uniqueness, let n be a minimal integer with the decomposition above, and suppose there existed another decomposition with primes $q_1, q_2, \ldots, q_t$ and exponents $\beta_1, \beta_2, \ldots, \beta_t$ such that

$$n = \prod_{j=1}^{t} q_j^{\beta_j}$$

Using properties of primes, we see that p_1 divides the product of all q_j. Without loss of generality, we may assume that $p_1 \mid q_1$. Since p_1 and q_1 are both prime, then $p_1 = q_1$. Dividing both products by p_1, we obtain the equality

$$\prod_{i=2}^{s} p_i^{\alpha_i} = \prod_{j=2}^{t} q_j^{\beta_j}$$

which are strictly smaller than n, contradicting its minimality. Hence, n has a unique prime factorization. □

We may also express the greatest common divisor and least common multiple using prime factorization. Let $a, b \in \mathbb{Z}^+$ be represented by the following products:

$$a = \prod_{i=1}^{s} p_i^{\alpha_i}, \quad b = \prod_{i=1}^{s} p_i^{\beta_i}$$

so that a and b utilize the same primes but may have dif and only ifering exponents for primes who are not present in their respective factorizations. Letting $[\cdot,\cdot]$ denote the least common multiple of two integers, we have the following:

$$(a,b) = \prod_{i=1}^{s} p_i^{\min(\alpha_i,\beta_i)}, \quad [a,b] = \prod_{i=1}^{s} p_i^{\max(\alpha_i,\beta_i)}$$

Definition 0.9 ▸ Euler φ-Function

For $n \in \mathbb{N}$, let $\varphi(n)$ be the number of positive integers $a \leq n$ with $(a,n) = 1$. For primes p and powers $a \geq 1$, we have the formula

$$\varphi(p^a) = p^{a-1}(p-1)$$

φ is *multiplicative* in the sense that

$$\varphi(ab) = \varphi(a)\varphi(b) \text{ when } (a,b) = 1$$

We can then obtain a general formula applying φ to some $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ as such:

$$\begin{aligned} \varphi(n) &= \prod_{i=1}^{s} \varphi(p_i^{\alpha_i}) \\ &= \prod_{i=1}^{s} p_i^{\alpha_i - 1}(p_i - 1) \end{aligned}$$

0.3 $\mathbb{Z}/n\mathbb{Z}$: The Integers Modulo n

Definition 0.10 ▸ Modular Congruence and Integers Modulo n

Let $n \in \mathbb{Z}$. Define a relation $\sim$ on $\mathbb{Z}$ by

$$a \sim b \iff n \mid (b-a)$$

Clearly $a \sim a$ since $n \mid 0$. Moreover, if $a \sim b$, then $nk = b - a \implies -nk = a - b$ so that $n \mid (a-b)$, and $b \sim a$. Moreover, if $a \sim b$ and $b \sim c$, then $nk = b - a$ and $n\ell = c - b$ for some $k, \ell \in \mathbb{Z}$. Add those equations to get $n(k+\ell) = c - a$, that $a \sim c$. We conclude that $\sim$ is an equivalence relation, and we write $a \equiv b \bmod n$. For some $k \in \mathbb{Z}$, let the equivalence class of a be denoted as $\overline{a}$, called the **congruence class** or **residue class of** $a \bmod n$. This class consists of the integers dif and only ifering from a by an integer multiple of n, or written out:

$$\overline{a} = \{a + kn : k \in \mathbb{Z}\}$$

The set of equivalence classes under a particular n is called the **integers modulo** n, which partition $\mathbb{Z}$ into n classes: $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. Moreover, we can define both **modular arithmetic**, or operations between any two elements in $\mathbb{Z}/n\mathbb{Z}$ as follows: for any $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, their sum and products are defined as:

$$\overline{a} + \overline{b} := \overline{a+b} \text{ and } \overline{a} \cdot \overline{b} := \overline{ab}$$

Theorem 0.3 ▸ Modular Arithmetic is Well-Defined

The operations of addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ are well-defined. More precisely, if $s_1, s_2 \in \mathbb{Z}$ and $t_1, t_2 \in \mathbb{Z}$ where $\overline{s_1} = \overline{t_1}$ and $\overline{s_2} = \overline{t_2}$, then $\overline{s_1 + s_2} = \overline{t_1 + t_2}$ and $\overline{s_1 s_2} = \overline{t_1 t_2}$.

Proof. Since $\overline{s_1} = \overline{t_1}$ and $\overline{s_2} = \overline{t_2}$, it follows that $s_1 = t_1 + nx$ and $s_2 = t_2 + ny$ for $x, y \in \mathbb{Z}$. Then $s_1 + s_2 = t_1 + t_2 + n(x+y)$. Moreover, we have $s_1 s_2 = (t_1 + nx)(t_2 + ny) = t_1 t_2 + (t_1 y + t_2 x + nxy)n$. □

Example ▶ Calculating Last Digits

Suppose we wanted to calculate the last two digits of 2^{1000}. The last two digits of any number is the remainder when dividing by 100, so the goal is to reduce 2^{1000} to mod100. There are many ways to calculate this, but one such way is when we consider $2^{10} = 1024 \equiv 24 \bmod 100$. Then $2^{20} \equiv 24^2 \bmod 100 = 576 \bmod 100 \equiv 76 \bmod 100$. Then $2^{40} \equiv 76^2 \bmod 100 = 5776 \bmod 100 = 76 \bmod 100$. It looks like multiplying by 2^{20} results in 76 mod 100, and since 1000 is divisible by 20, it follows that $2^{1000} \equiv 76 \bmod 100$.

Definition 0.11 ▶ Primitive Residue Classes Modulo n

Let $\mathbb{Z}/n\mathbb{Z}$ be defined as before. The the **primitive residue classes modulo** n is the subset of $\mathbb{Z}/n\mathbb{Z}$ whose elements contain a multiplicative inverse:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : \exists \overline{c} \in \mathbb{Z}/n\mathbb{Z}, \overline{a} \cdot \overline{c} = \overline{1}\}$$

Proposition 0.4 ▶ Defining $(\mathbb{Z}/n\mathbb{Z})^\times$

The set $(\mathbb{Z}/n\mathbb{Z})^\times \subset \mathbb{Z}/n\mathbb{Z}$ is *precisely* the set of residue classes whose representatives are relatively prime to n, i.e.,

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : (a,n) = 1\}$$

Example ▶ Example of $(\mathbb{Z}/n\mathbb{Z})^\times$ and Calculating Inverses

- For $n = 9$, we have all elements x such that $(x,9) = 1$. It is precisely the set $\{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$. Moreover, the inverses of each of those elements is $\overline{1}, \overline{5}, \overline{7}, \overline{2}, \overline{4}, \overline{8}$ respectively.
- Note that a and n being relatively prime allows the Euclidean Algorithm to produce $x, y \in \mathbb{Z}$ such that $ax + ny = 1$, or $ax \equiv 1 \bmod n$. It follows that $\overline{x}$ would be the multiplicative inverse of $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$.
- Consider $n = 60$ and $a = 17$. Using the Euclidean Algorithm, we obtain

$$\begin{aligned} 60 &= 3(17) + 9 \\ 17 &= 1(9) + 8 \\ 9 &= 1(8) + 1 \end{aligned}$$

so that $(60, 17) = 1$, and $-7(17) + 2(60) = 1$. Then $\overline{-7} = \overline{53}$ is the multiplicative inverse of $\overline{17}$ in $\mathbb{Z}/60\mathbb{Z}$.

1 Introduction to Groups

1.1 Basic Axioms and Examples

Definition 1.1 ▶ Binary Operation

- A **binary operation** $\star$ on a set G is a function $\star : G \times G \to G$. For any $a, b \in G$, then we write $a \star b$ for $\star(a, b)$.
- A binary operation $\star$ on a set G is **associative** on a set G when for al $a, b, c \in G$ we have $a \star (b \star c) = (a \star b) \star c$.
- If $\star$ is a binary operation on a set G, then $a, b \in G$ **commute** if $a \star b = b \star a$. Moreover, $\star$ (or G) is **commutative** if for all $a, b \in G$, then $a \star b = b \star a$.
- If $\star$ is a binary operation on G with $H \subseteq G$, and if $\star|_H$ is a binary operation on H, i.e., if $a \star b \in H$ for all $a, b \in H$, then H is **closed** under H. Moreover, associativity and commutativity on G implies the same on H.

Definition 1.2 ▶ Group Definitions

- A **group** is an ordered pair $(G, \star)$ where G is a set and $\star$ is a binary operation satisfying the axioms:
  1. $\star$ is associative,
  2. there exists $e \in G$, called the **identity**, such that for all $g \in G$, then $g \star e = e \star g = g$,
  3. for every $g \in G$, there exists an element g^{-1}, called the **inverse of** g, such that $g \star g^{-1} = g^{-1} \star g = e$.
- A group $(G, \star)$ is called **abelian**, or **commutative**, if $a \star b = b \star a$ for every $a, b \in G$.
- In addition to referring to G as a group and not the tuple (if $\star$ is clear from the context), we say G is a **finite group** when G itself is a finite set.
- Axiom (2) guarantees non-emptiness of a group.

Example ▶ Binary Operations and Groups

- Common binary operations are:
  - $+$ is commutative on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
  - $\times$ is commutative on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
  - $-$ is non-commutative, since $-(a, b) \neq -(b, a)$.
  - Vector cross products in $\mathbb{R}^3$ is non-commutative and non-associative.
- Common examples of groups include:
  - Any vector space is an additive abelian group.
  - For any $n \in \mathbb{Z}^+$, then $\mathbb{Z}/n\mathbb{Z}$ is an abelian group under $+$ of addition of residue classes. The identity is $\bar{0}$ and the inverse of each $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is $\overline{-a}$.
  - For $n \in \mathbb{Z}^+$, the set $(\mathbb{Z}/n\mathbb{Z})^\times$ is an abelian group under $\times$ of multiplication of residue classes. The identity is $\bar{1}$, and each element has a multiplicative inverse, by definition.
  - Let $(A, \star)$ and $(B, \diamond)$ be groups. Then the **direct product** $A \times B$ is a group whose elements are those from the Cartesian product
    $$A \times B = \{(a, b) : a \in A, b \in B\}$$
    and whose operation is defined componentwise:
    $$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2)$$

Proposition 1.1 ▶ Basic Group Properties

Let G be a group under the operation $\star$. Then:

1. the identity of G is unique,
2. for each $g \in G$, then g^{-1} is uniquely determined,
3. $(g^{-1})^{-1} = g$ for every $g \in G$,
4. $(g_1 \star g_2)^{-1} = g_2^{-1} \star g_1^{-1}$
5. For $g_1, g_2, \ldots, g_n \in G$, then $g_1 \star g_2 \star \cdots \star g_n$ is independent of the bracketing, also known as the **generalized associative law**.

Proof.

1. Let a, b be identities of g. Then $a \star b = a$ and $a \star b = b$.

2. Let h_1, h_2 be inverses of some $g \in G$ with identity e. Then

$$\begin{aligned} h_1 &= h_1 \star e \\ &= h_1 \star (g \star h_2) \\ &= (h_1 \star g) \star h_2 \\ &= e \star h_2 \\ &= h_2 \end{aligned}$$

3. Note that $g^{-1}(g^{-1})^{-1} = e$ and $g^{-1}g = 1$. Since the inverse of an element is uniquely determined, it follows that the inverse of g^{-1} is g.
4. Let $h = (g_1 \star g_2)^{-1}$. Then

$$\begin{aligned} (g_1 \star g_2) \star h &= e \\ g_1^{-1} \star (g_1 \star g_2) \star h &= g_1^{-1} \star e \\ (g_1^{-1} \star g_1) \star (g_2 \star h) &= g_1^{-1} \end{aligned}$$

Note that $g_1^{-1} \star g_1 = e$. Then left multiply by g_2^{-1}:

$$\begin{aligned} g_2^{-1} \star (g_2 \star h) &= g_2^{-1} \star g_1^{-1} \\ h &= g_2^{-1} \star g_1^{-1} \end{aligned}$$

5. The proof will proceed by induction. Note that for $n = 1, 2$, the result is trivial, while $n = 3$ follows from associativity of $\star$ on G. Assume for $k < n$ that a bracketing of any k elements $h_1 \star h_2 \star \cdots \star h_k$ for $h_1, \ldots, h_k \in G$ can be reduced to an expression of the form

$$h_1 \star (h_2 \star (h_3 \star (\cdots \star h_k)) \cdots)$$

Consider an arbitrarily-bracketed expression of $g_1 \star g_2 \star \cdots \star g_n$. Split it into 2 products $(g_1 \star g_2 \star \cdots \star g_k) \star (g_{k+1} \star \cdots \star g_n)$, where each product is also bracketed in any fashion. By the inductive hypothesis, we may arrange these products in the form $g_1 \star (g_2 \star (\cdots \star g_k)) \cdots) \star (g_{k+1} \star (g_{k+2} \star (\cdots \star g_n)) \cdots)$. Applying associativity, we get the result $g_1 \star (g_2 \star (\cdots \star g_k \star (g_{k+1} \star (\cdots \star g_n)) \cdots)$, where the second product had the terms $g_{k+1}, \ldots, g_{n-1}$ arranged in the form above. □

Note ▸

Except when necessary, specified groups $G, H, \ldots$ will be written with the operation $\cdot$, and $a \cdot b$ will be written as ab. Moreover, any parentheses is dropped for products with at least 3 elements due to the generalized associative law. Additionally, the identity of G will be denoted as 1 for $\cdot$, while additive operations $+$ will have identities denoted as 0. Lastly, $x x \cdots x$ with n amount of x will be denoted as x^n, with $x^{-1} x^{-1} \cdots x^{-1}$ (also n amount) will be denoted as x^{-n}, and $x^0 = 1$.

Proposition 1.2 ▸ Cancellation Laws

Let G be a group with $g, h \in G$. Then for any $s, t \in G$, the equations $gs = h$ and $tg = h$ have unique solutions. Moreover, the left and right cancellation laws hold in G:

1. $gs = gt \implies s = t$,
2. $sh = th \implies s = t$.

In particular, if $g \in G$ and $h \in G$ such that $gh = e$ or $hg = e$, then h is necessarily g^{-1}. Moreover, if $gh = g$ or $hg = g$, then h is necessarily e.

Proof. Solve $gs = h$ by left multiplying by g^{-1} to get $s = g^{-1}h$, where s is unique since g^{-1} is unique. If $tg = h$, then $t = hg^{-1}$ is also unique. Lastly, items (1) and (2) are done by left and right multiplying by g^{-1} and h^{-1} respectively. □

Definition 1.3 ▸ Order

Let G be a group with $g \in G$. The **order** of g is the smallest $n \in \mathbb{Z}^+$ such that $g^n = 1$, where n is denoted by $|g|$, and g is said to have order n. Moreover, if no such n exists, then g is said to have **infinite order**.

Example ▸ Examples of Order

- For some $g \in G$ for a group G, then $|g| = 1$ if and only if $g = 1$.
- Under $(S, +)$ where $S = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, then every non-identity element has infinite order.
- In $(\mathbb{R} - \{0\}, \times)$ and $(\mathbb{Q} - \{0\}, \times)$, we have $|-1| = 2$ with other non-identity elements having infinite order.
- Take $\overline{8} \in \mathbb{Z}/12\mathbb{Z}$. Then $\overline{8} + \overline{8} = \overline{16} = \overline{4}$, and $\overline{8} + \overline{8} + \overline{8} = \overline{4} + \overline{8} = \overline{0}$ so that $|\overline{8}| = 3$. Note that powers of an element in an additive group are integer multiples.
- Take $\overline{4} \in (\mathbb{Z}/7\mathbb{Z})^\times$. Then $(\overline{4})^2 = \overline{16} = \overline{2}$, and $(\overline{4})^3 = \overline{64} = \overline{1}$ so that $|\overline{4}| = 3$.

Definition 1.4 ▶ Multiplication/Group Table

Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group with $g_1 = 1$. Then the **multiplication table** is the $n \times n$ matrix whose i, j entry is the product $g_i g_j$.

1.2 Dihedral Groups

Definition 1.5 ▶ Dihedral Group of Order $2n$

For $n \in \mathbb{Z}^+$ and $n \geq 3$, define D_{2n} to be the set of symmetries of a regular n-gon. We define a symmetry to be taking a copy of the n-gon, moving it in any fashion, then placing the copy on the original n-gon to exactly cover it. Each symmetry s places a vertex i to a vertex j of the n-gon, and there is an associated σ that sends i to j.

- As an example, if s was a rotation of $2\pi/n$ radians clockwise about the center of the n-gon, then σ sends i to $i+1$ for $1 \leq i \leq n-1$, and $\sigma(n) = 1$.

We define D_{2n} to now be a group with st for $s, t \in D_{2n}$ to be defined as applying t then s (so we effectively treat symmetries as functions). Moreover, if s, t describe the permutations σ, τ, then st describes the permutation $\sigma \circ \tau$. The identity of D_{2n} is the map 1 that sends each vertex to itself, and the inverse of any $s \in D_{2n}$ is the element s^{-1} that effects σ^{-1} that reverses every rigid motion of s.

We claim that $|D_{2n}| = 2n$. To see this, we observe the following:

- For each vertex i, there exists $s \in D_{2n}$ that sends 1 to i. Adjacency of vertex 2 to 1 makes it end up in vertex $i+1$ or $i-1$, where vertex n is sent to 1 and 1 is sent to 1 so that the vertex labeling is read mod n.
- After this symmetry, we may follow it with a reflection about the line through vertex i and the center of the n-gon. This results in vertex 2 being sent to either vertex $i+1$ or $i-1$ (where $i+1 \to i-1$, and vice versa).
- The rigidity of the symmetries result in the complete determination of the other vertices once the results of vertex 1 and 2 are known. It follows that there are exactly $2n$ symmetries.
- Those symmetries are as follows: n rotations about the center through $2\pi i/n$ radians for $0 \leq i \leq n-1$, and n reflections through the n lines of symmetry (In the reflections, there are two cases: if n is odd, then it goes through a vertex and the midpoint of the opposite side. If n is even, then there are $n/2$ lines of symmetry that cross through 2 opposite vertices, and $n/2$ lines of symmetry that perpendicularly bisect two opposite sides.)

Viewing D_{2n} as an abstract group, we simplify this view as follows: fix a regular n-gon at the origin in the Cartesian plane, and label the vertices consecutively from 1 to n clockwise.

- Define r as the rotation clockwise about the origin through $2\pi/n$ radian.
- Define s as the reflection about the line of symmetry through vertex 1 and the origin.

From this, we may deduce the following:

1. $1, r, r^2, \ldots, r^{n-1}$ are all distinct, and $r^n = 1$ so $|r| = n$.
2. $|s| = 2$.
3. $s \neq r^i$ for any i.
4. $sr^i \neq sr^j$ for all $0 \leq i, j \leq n-1$ with $i \neq j$, so

$$D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$

   i.e., each element is written *uniquely* in the form $s^k r^i$ for $k \in \{0, 1\}$ and $0 \leq i \leq n-1$.
5. $rs = sr^{-1}$. [First work out what permutation s effects on $\{1, 2, \ldots, n\}$ and then work out separately what each side in this equation does to vertices 1 and 2.] This shows in particular that r and s do not commute so that D_{2n} is non-abelian.
6. $r^i s = sr^{-i}$ for all $0 \leq i \leq n$. [Proceed by induction on i and use the fact that $r^{i+1}s = r(r^i)s$ together with the preceeding calculation.] This indicates how to commute s with powers of r.

The following is a proof of each assertion:

Proof.

1. Note that r^n is a 2π rotation, so it is the same as the identity map. Then $|r| \leq n$. Suppose $r^i = r^j$ for $i \neq j$ and $0 \leq i < j \leq n-i$. Then $r^{j-i} = 1$, which is false, since a rotation by $2\pi(j-i)/n$ radians is not returning each vertex to itself since $n \nmid (j-i)$. In particular, the rotation $2\pi m/n$ is an identity rotation when $n \mid m$, which is not true here since $i, j < n$. Then n is the smallest integer such that $r^n = 1$, hence $|r| = n$.
2. Recall that s is a reflection, and so 2 reflections must send a reflected vertex back to its position so that $s^2 = 1$, and $|s| \leq 2$. Moreover, since applying s guarantees a vertex moving to a position it was not originally in, then $|s| \neq 1$.
3. Since a rotation preserves the orientation of the vertices (in particular, it maintains the clockwise manner to which we have constructed the n-gon), and a reflection reverses this to a counter-clockwise manner, then no amount of rotations can equal a reflection.
4. If (4) was true, left multiply by s to obtain $r^i = r^j$. Since $i \neq j$, this contradicts the earlier assertion of (1). Hence any element of D_{2n} is the form of $s^k r^i$.
5. On the set $\{1, 2, \ldots, n\}$, we may figure out how s effects on this set by considering two cases:
   - If n is odd, then $s(1) = 1$, and $s(i) = n+2-i$.
   - If n is even, then $s(1) = 1$ and $s(n/2+1) = n/2+1$. For other i, then $s(i) = n+2-i$.

   Moreover, for r, we have $r(n) = 1$ and $r(i) = i+1$ for $1 \leq i \leq n-1$. Then rs sends 1 to 2 and 2 to 1, and sr^{-1} sends 1 to 2 and 2 to 1.
6. The case for $i = 1$ is true by (5). Suppose it is true for $i \in \mathbb{Z}^+$. Then for $i+1$, we have $r^{i+1}s = r(r^i s) = r(sr^{-i}) = (sr^{-1})r^{-i} = sr^{-(i+1)}$, and the result follows by induction. □

Generators and Relations

Definition 1.6 ▶ Generators and Generating

Let G be a group with a subset S such that every $g, g^{-1} \in G$ can be written as a (finite) product of elements of S. Then S is a set of **generators** of G, denoted by $G = \langle S \rangle$, and we say S **generates** G or that G is **generated by** S. We can see by (4) above that $D_{2n} = \langle r, s \rangle$.

Definition 1.7 ▶ Relation

For a group G with a set of generators S, we define **relations** to be a set of equations that the generators satisfy. In D_{2n}, the relations are: $r^n = 1, s^2 = 1$, and $rs = sr^{-1}$. We also see that any other relation between the groups are derived from these primary 3.

Definition 1.8 ▶ Presentation

Let G be a group with a set of generators S satisfying a set of relations R_i, where each R_i is an equation using elements from $S \cup \{1\}$. Then the collection of generators and relations form a **presentation** of G and write

$$G = \langle S \mid R_1, R_2, \ldots, R_m \rangle$$

We may then describe D_{2n} as the following:

$$D_{2n} := \langle r, s \mid r^n = 1, s^2 = 1, rs = sr^{-1} \rangle \tag{1.1}$$

Example ▶ Subtleties in Group Presentations

- One must caution that, in an arbitrary representation of a group, it may be difficult to tell when two elements of a group are equal when using the generators given. Consequently, the order of the presented group may be difficult to determine. For example, one can show that $\langle x_1, y_1 \mid x_1^2 = y_1^2 = (x_1 y_1)^2 = 1 \rangle$ is a presentation of a group with order 4, while $\langle x_2, y_2 \mid x_2^3 = y_2^3 = (x_2 y_2)^3 = 1 \rangle$ is a presentation of an infinite group.
- Another caution is that collapsing of the relations may occur, even in simple presentations, because the relations are intertwined in an unobvious way. This creates difficulty in ascertaining a lower bound of the group order. For example, take a mimic of D_{2n} specified as such:

$$X_{2n} := \langle x, y \mid x^n = y^2 = 1, xy = yx^2 \rangle \tag{1.2}$$

  The relation $xy = yx^2$ describes how to commute y and x such that every element in X_{2n} can be written in the form $y^k x^i$. From $x^n = y^2 = 1$, we may suppose that $0 \leq i \leq n-1$ and $k \in \{0, 1\}$ so that we deduce X_{2n} is

of order $2n$. However, using the fact that $x = xy^2$ because $y^2 = 1$, we may use the commutative relation to deduce:

$$x = xy^2 = (xy)y = (yx^2)y = (yx)(xy) = (yx)(yx^2) = y(xy)x^2 = y(yx^2)x^2 = x^4$$

Then $x^3 = 1$ in X_{2n} so that it has order of at most 6 for any n.

- Consider the next presentation as such:

$$Y = \langle u, v \mid u^4 = v^3 = 1, uv = v^2u^2 \rangle \tag{1.3}$$

While it may be tempting to guess that $|Y| = 12$, this actually degrades to the trivial group of order 1, where $u = v = 1$.

1.3 Symmetric Groups

Definition 1.9 ▶ Symmetric Group

Let Ω be a nonempty set and S_Ω be the set of all bijections from Ω to itself. Then $(S_\Omega, \circ)$ is the **symmetric group on the set** Ω with $\circ$ representing function composition. Moreover, recognize that the elements of S_Ω are permutations of the elements of Ω rather than the elements of Ω itself.

- If $\sigma, \tau \in S_\Omega$, then $\sigma \circ \tau$ remains a bijection from Ω to Ω so that $\circ$ is a binary operation on S_Ω.
- The identity of S_Ω is 1, where $1(x) = x$ for $x \in \Omega$.
- $\circ$ is associative, in general.
- For any $\sigma \in S_\Omega$, we have the associated inverse $\sigma^{-1} \in S_\Omega$, where $\sigma^{-1} \circ \sigma = 1$ and $\sigma \circ \sigma^{-1} = 1$. More explicitly, if $\sigma(a) = b$, then $\sigma^{-1}(b) = a$ for every $a, b \in \Omega$.

In the case where $\Omega = \{1, 2, \ldots, n\}$, we denote it as S_n instead, or the **symmetric group of degree** n. Moreover, we claim that $|S_n| = n!$.

Proof. From Proposition 0.1, the permutations of $\{1, 2, \ldots, n\}$ are the injective functions of this set to itself since it is finite. To count the number of injective functions, proceed as such: For any $\sigma \in S_n$, then $\sigma(1)$ has n choices. Then $\sigma(2)$ has $n-1$ choices, since $\sigma(2) \neq \sigma(1)$ because σ is injective. Going on this vein until $\sigma(n)$ is left, we have $n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 = n!$ injections. □

Definition 1.10 ▶ Cycle Terminology

- A **cycle** is a string of integers that represents the elements of S_n which cyclically permute these integers and fixes all other integers. For example, the cycle $(a_1 a_2 \ldots a_m)$ is the permutation that sends $a_i \to a_{i+1}$ for $1 \leq i \leq m-1$ and then sends $a_m \to a_1$.
- To generalize, for any $\sigma \in S_n$, then the numbers 1 to n are arranged and grouped into k cycles of the form

$$(a_1 a_2 \ldots a_{m_1})(a_{m_1+1} a_{m_1+2} \ldots a_{m_2}) \ldots (a_{m_{k-1}+1} a_{m_{k-1}+2} \ldots a_{m_k})$$

To read this, pick some x between 1 to n and find x in the above expression. If x is not on the right end of one of the k cycles, then $\sigma(x)$ is the integer immediately to the right of x. If x is at the right end, then $\sigma(x)$ is the integer at the left end, i.e., if $x = a_{m_i}$, then $\sigma(x) = a_{m_{i-1}+1}$, where $m_0 = 0$.

- The product of all the k cycles is called the **cycle decomposition** of σ.
- If a cycle contains t integers, then we call that a t**-cycle**.
- Two cycles that contain no elements in common are called **disjoint**.

Definition 1.11 ▶ Cycle Decomposition Algorithm

1. To start a new cycle, pick the smallest element of $\{1, 2, , \ldots, n\}$ that has not appeared in a previous cycle, call it a. If the process is beginning, then start with $a = 1$.
2. From the given description of σ, find $\sigma(a)$ and call it b. If $b = a$, then close the current cycle with a right parenthesis without writing b and return to step 1. If $b \neq a$, then write b next to a in the ongoing cycle.
3. Find $\sigma(b)$ and call it c. If $c = a$, close the cycle with a right parenthesis and return to step 1. Otherwise, write c next to b. Using c as b in step 2, repeat step 3 until the cycle ends.
4. Remove all cycles of length 1.

Example ▸ Cycle Decomposition of $\sigma \in S_{13}$

Let $n = 13$ and define $\sigma \in S_{13}$ as

$$\sigma(1)=12,\quad \sigma(2)=13,\quad \sigma(3)=3,\quad \sigma(4)=1,\quad \sigma(5)=11,\quad \sigma(6)=9,\quad \sigma(7)=5,$$
$$\sigma(8)=10,\quad \sigma(9)=6,\quad \sigma(10)=4,\quad \sigma(11)=7,\quad \sigma(12)=8,\quad \sigma(13)=2$$

- Starting the cycle, begin with $a = 1$. Since $\sigma(1) = 12 \neq 1$, then $\sigma(12) = 8, \sigma(8) = 10, \sigma(10) = 4$, and $\sigma(4) = 1$. The first cycle is then (1 12 8 10 4).
- The next smallest number is 2, so $\sigma(2) = 13$ and $\sigma(13) = 2$. Then the second cycle is (2 13).
- The next smallest number is 3, so $\sigma(3) = 3$, and the third cycle is (3).
- The next smallest is 5, so $\sigma(5) = 11, \sigma(11) = 7$, and $\sigma(7) = 5$. Then the fourth cycle is (5 11 7).
- The next smallest is 6, so $\sigma(6) = 9$ and $\sigma(9) = 6$. Then the fifth cycle is (6 9).
- Remove the single cycle (3).

Following this, we have $\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$.

Definition 1.12 ▸ Additional Properties of Cycles

- If $\sigma \in S_n$ that permutes $\{1, 2, \ldots, n\}$, then $\sigma \in S_m$ for $m > n$ permutes the elements $\{1, 2, \ldots, n\}$ the same way as $\sigma \in S_n$ with the additional permutation that $\sigma(x) = x$ for $n < x \leq m$.
- For $\sigma \in S_n$, then σ^{-1} is found by reversing the orders of the numbers in each of the cycles in σ.
- To compute products of cycles, follow each of the elements in succession in each permutation. Moreover, for $\sigma, \tau \in S_n$, we calculate $\sigma \circ \tau$ by sending the integers through τ first as in function composition.
- It is easy to show that S_n is a non-abelian group for all $n \geq 3$.
- Because each cycle permutes only the integers involved in the cycle, and disjoint cycles permute numbers that lie in disjoint sets by definition (otherwise, they wouldn't be disjoint as they share integers), then it follows that disjoint cycles commute.
- For an arbitrary cycle $(a_1\ a_2 \ldots a_m)$, recall that this cycle permutes the elements $\{a_1, a_2, \ldots, a_m\}$ cyclically. Hence, it follows that the cycle is equal to any representation that preserves the order in which the integers are represented. Explicitly, this means that

$$(a_1\ a_2 \ldots a_m) = (a_2\ a_3 \ldots a_m\ a_1) = (a_3\ a_4 \ldots a_m\ a_1\ a_2) = \cdots = (a_m\ a_1\ a_2 \ldots a_{m-1})$$

- The cycle decomposition of any permutation is actually the *unique* way of expressing a permutation as a product of disjoint cycles, up to rearrangement of the cycles. It follows that reducing an arbitrary product of cycles to a product of disjoint cycles allows the determination of whether or not two permutations are the same.
- Lastly, the exercises will show that the order of a permutation is the lcm of the lengths of the cycles in the cycle decomposition.

1.4 Matrix Groups

Definition 1.13 ▸ Field

- A **field** is a set F with two binary operations $+$ andd $\cdot$ on F such that $(F, +)$ is an abelian group (with identity 0) and $(F - \{0\}, \cdot)$ is an abelian group with the distributive law:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \text{ for all } a, b, c \in F$$

- Denote $F^\times = F - \{0\}$.

For prime p, denote $\mathbb{Z}/p\mathbb{Z}$ as $\mathbb{F}_p$.

Definition 1.14 ▸ General Linear Group of Degree n

For $n \in \mathbb{Z}^+$, denote $\mathrm{GL}_n(F)$ as the set of all $n \times n$ matrices with entries from F and nonzero determinant, which is calculated with the same formula when $F = \mathbb{R}$.

- For $A, B \in \mathrm{GL}_n(F)$, denote AB as their product whose calculation is the same when $F = \mathbb{R}$. Since $\det(A) \neq 0$ and $\det(B) \neq 0$, then $\det(A)\det(B) = \det(AB) \neq 0$ so that $AB \in \mathrm{GL}_n(F)$. Hence, matrix multiplication is closed.
- Matrix multiplication is associative, in general.
- A matrix A has nonzero determinant if and only if A^{-1} exists whose calculation is the same when $F = \mathbb{R}$. Then for each $A \in \mathrm{GL}_n(F)$ there exists $A^{-1} \in \mathrm{GL}_n(F)$ such that $AA^{-1} = A^{-1}A = I$, where I denotes the $n \times n$ identity matrix.

Then $\mathrm{GL}_n(F)$ is a group under matrix multiplication and is called the **general linear group of degree** n. Moreover, there are two additional facts that are known:
1. For a field F with $|F|<\infty$, then $|F|=p^m$ for prime p and $m\in\mathbb{Z}^+$.
2. If $|F|=q<\infty$, then

$$|\mathrm{GL}_n(F)|=\prod_{i=1}^{n}(q^n-q^{i-1})$$

1.5 The Quaternion Group

Definition 1.15 ▶ Quaternion Group

The **quaternion group**, denoted as Q_8, is defined as

$$Q_8:=\{1,-1,i,-i,j,-j,k,-k\}$$

with product $\cdot$ as follows:

$$1\cdot a=a\cdot 1=a,\quad \text{for all } a\in Q_8$$
$$(-1)\cdot(-1)=1,\quad (-1)\cdot a=a\cdot(-1)=-a,\quad \text{for all } a\in Q_8$$
$$i\cdot i=j\cdot j=k\cdot k=-1$$
$$i\cdot j=k,\quad j\cdot i=-k$$
$$j\cdot k=i,\quad k\cdot j=-i$$
$$k\cdot i=j,\quad i\cdot k=-j$$

- The associative law can be proven by multiplying every 3-tuple of numbers, but that is 512 potential combinations (since $|Q_8|=8$), so a more sophisticated method will be associating Q_8 with matrices wherein matrix multiplication is associative.
- The identity element of Q_8 is 1.
- Q_8 is clearly closed under the definition of the defined product.
- The inverse of -1 is itself, and the inverse of i,j,k is $-i,-j,-k$ respectively.
- Q_8 is non-abelian.

1.6 Homomorphisms and Isomorphisms

Definition 1.16 ▶ Homomorphism

Let $(G,\star)$ and $(H,\diamond)$ be groups. Then a map $\varphi:G\to H$ such that

$$\varphi(x\star y)=\varphi(x)\diamond\varphi(y),\quad \text{for all } x,y\in G$$

is called a **homomorphism**. Moreover, if the operations of G and H are not explicitly rewritten, the above becomes $\varphi(xy)=\varphi(x)\varphi(y)$.

Definition 1.17 ▶ Isomorphism

Let $\varphi:G\to H$ be a bijective homomorphism. Then it is an **isomorphism** and G and H are said to be **isomorphic** or of the same **isomorphism type**, written as $G\cong H$, if
1. φ is a homomorphism, and
2. φ is a bijection.

In some sense, $G\cong H$ implies that G and H are the same group but written dif and only iferently. Moreover, any properties deduced about G using group axioms only will also hold in H.

Example ▶ Examples of Homomorphism and Isomorphisms

- For any group G, then $G\cong G$. A potential isomorphism is the identity map $\varphi:G\to G$ defined as $\varphi(g)=g$ for all $g\in G$. Clearly, for $g,h\in G$, then $\varphi(gh)=gh=\varphi(g)\varphi(h)$. Moreover, the identity map is trivially a bijection, so it indeed is an isomorphism. More generally, suppose $\mathscr{G}$ is a collection of groups $G_1,G_2,\ldots$. Then $\cong$ is an equivalence relation on $\mathscr{G}$:

Proof. As shown above, $\cong$ is reflexive. Suppose now that $G \cong H$ for some $G, H \in \mathscr{G}$. Then there exists an isomorphism $\varphi : G \to H$. Since φ is bijective, then $\varphi^{-1} : H \to G$ exists and is also bijective. Moreover, for any $h_1, h_2 \in H$, there exists corresponding $g_1, g_2 \in G$ such that $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$. Then

$$\varphi^{-1}(h_1 h_2) = \varphi^{-1}(\varphi(g_1)\varphi(g_2)) = \varphi^{-1}(\varphi(g_1 g_2)) = g_1 g_2 = \varphi^{-1}(h_1)\varphi^{-1}(h_2)$$

so that φ^{-1} is an isomorphism, and $H \cong G$. Then $\cong$ is symmetric.
Suppose now $G, H, K \in \mathscr{G}$ such that $G \cong H$ and $H \cong K$ with isomorphisms $\varphi : G \to H$ and $\psi : H \to K$. Consider the mapping $\psi \circ \varphi$, which is bijective since a composition of bijective mappings is bijective (To see this, let $f : A \to B$ and $g : B \to C$ be bijective mappings, and consider $g \circ f$. Suppose $f(a_1) = f(a_2)$ for $a_1, a_2 \in A$. Then $g(f(a_1)) = g(f(a_2))$ implies that $f(a_1) = f(a_2)$, since g is injective. Then $a_1 = a_2$, since f is injective so that $g \circ f$ is injective. Now suppose $c \in C$. Since g is surjective, there exists $b \in B$ such that $g(b) = c$. Moreover, there exists $a \in A$ such that $f(a) = b$ because f is surjective. Then $g(f(a)) = g(b) = c$ so that $g \circ f$ is surjective, hence it is bijective.)
Suppose $g_1, g_2 \in G$. Then

$$\psi(\varphi(g_1 g_2)) = \psi(\varphi(g_1)\varphi(g_2)) = \psi(\varphi(g_1))\psi(\varphi(g_2))$$

so that $\psi \circ \varphi$ is a homomorphism, hence it is an isomorphism. Then $G \cong K$, and $\cong$ is transitive on $\mathscr{G}$. It follows that $\cong$ is an equivalence relation on $\mathscr{G}$. □

Moreover, we say that the equivalence classes of $\cong$ on $\mathscr{G}$ are **isomorphism classes**.

- The exponential mapping $\exp : R \to \mathbb{R}^+$ defined as $\exp(x) = e^x$ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \times)$. Since exp is a bijection (because it has the inverse ln), and it is a homomorphism because $\exp(x+y) = e^{x+y} = e^x e^y = \exp(x)\exp(y)$, then it is an isomorphism.
- Isomorphism type of symmetric groups depends on the cardinality of the underlying set being permuted, i.e., if Δ and Ω are nonempty sets. then S_Δ and S_Ω are isomorphic if and only if $|\Delta| = |\Omega|$.

Proof. Suppose $S_\Delta \cong S_\Omega$. For simplicity's sake, the proof will only show the finite case, while the infinite case will be handled later. Because an isomorphism is a bijection, it follows that $|S_\Delta| = |S_\Omega|$. Since we assumed finiteness of Δ and Ω, i.e., $|\Delta| = m$ and $|\Omega| = n$, then $|S_\Delta| = m! = n! = |S_\Omega|$. Then $|\Delta| = m = n = |\Omega|$.
Suppose now that $|\Delta| = |\Omega|$. While the exact details will be done below in the exercises, the intuition for this is as follows. Since there must be a bijection from $\theta : \Delta \to \Omega$, then we may associate each element $x \in \Delta$ to $\theta(x) \in \Omega$. A map $\varphi : S_\Delta \to S_\Omega$ must associate $\sigma \in S_\Delta$ to $\varphi(\sigma) \in S_\Omega$, where $\varphi(\sigma)$ must move the elements of Ω in the same fashion that σ moves elements in Δ. More explicitly, if $\sigma(a) = b$ for $a, b \in \Delta$, then $\varphi(\sigma)(\theta(a)) = \theta(b)$. □

Definition 1.18 ▶ Properties of Isomorphisms

Let $\varphi : G \to H$ be an isomorphism. Then the following is true:

1. $|G| = |H|$,
2. G is abelian if and only if H is abelian, and
3. for every $g \in G$, then $|g| = |\varphi(g)|$.

Proved later in the exercises, one may exhibit a property in G not present in H to determine that $G \ncong H$.

Example ▶ Non-Isomorphic Groups

- S_3 is not isomorphic to $\mathbb{Z}/6\mathbb{Z}$ since the former is not abelian while the latter is.
- $(\mathbb{R}-\{0\}, \times$ and $(\mathbb{R}, +)$ are not isomorphic since $-1 \in (\mathbb{R}-\{0\}, \times)$ has order 2, while there are no elements of order 2 in $(\mathbb{R}, +)$.

Definition 1.19 ▶ Homomorphisms of Group Presentations

Let G be a finite group with order n with some presentation and generators $S = \{s_1, s_2, \ldots, s_m\}$. Let H be another group with elements $\{r_1, r_2, \ldots, r_m\}$.

- If a relation satisfied in G by the s_i is also satisfied in H when s_i replaces r_i, then there exist a unique homomorphism $\varphi : G \to H$ that maps s_i to r_i.
- If $H = \langle r_1, r_2, \ldots, r_m \rangle$, then φ is necessarily surjective, since any element in H is a combination of r_i whose preimage is s_i.
- If $|G| = |H|$, then $G \cong H$ if φ is a surjective map since it would be necessarily injective.

Example ▶ Showing Isomorphism Via Group Presentations

- Let D_{2n} have its usual representation. Let H be a group with $a, b \in H$ such that $a^n = 1, b^2 = 1$, and $ba = a^{-1}b$. There exists a homomorphism from D_{2n} to H that maps a to r and b to s. Let $k \in \mathbb{Z}$ such that $k \mid n$ and $k \geq 3$, and define $D_{2k} = \langle r_1, s_1 \mid r_1^k = s_1^2 = 1, s_1 r_1 = r_1^{-1} s_1 \rangle$. Define the map

$$\varphi : D_{2n} \to D_{2k} \quad \text{by} \quad \varphi(r) = r_1, \varphi(s) = s_1$$

  Putting $n = km$ for $m \in \mathbb{Z}$, then $r_1^n = (r_1^k)^m = 1$. Then all relations in D_{2n} are satisfied by r_1, s_1 in D_{2k} so that φ extends to a homomorphism form D_{2n} to D_{2k}. Moreover, φ is surjective since $\{r_1, s_1\}$ generates D_{2k} but is not an isomorphism when $k < n$.
- Consider D_6 and S_3. Set $a = (1\ 2\ 3)$ and $b = (1\ 2)$ so that $a^3 = b^2 = 1$, and $ba = (1\ 2)(1\ 2\ 3) = (1\ 3) = (1\ 2\ 3)(1\ 2) = ab^{-1}$. Then there is a homomorphism $\varphi : D_6 \to S_3$ defined by $\varphi(r) = a$ and $\varphi(s) = b$. Since $(1\ 2\ 3)^2 = (1\ 3\ 2), (1\ 2\ 3)(1\ 2) = (1\ 3)$, and $(1\ 2\ 3)^2(1\ 2) = (2\ 3)$, then S_3 is indeed generated by a and b so that φ is a surjective homomorphism. Lastly, φ is an isomorphism since $|D_6| = |S_3|$.

1.7 Group Actions

Definition 1.20 ▶ Group Action

A **group action** of a group G on a set A is a map from $G \times A$ to A, written as $g \cdot a$, for all $g \in G$ and $a \in A$ satisfying the following properties:

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G, a \in A$, and
2. $1 \cdot a = a$, for all $a \in A$.

We may say that G is a group acting on a set A, and we usually write $g \cdot a$ as ga. For property (1), g_1 acting on $g_2 \cdot a$ makes sense, since $g_2 \cdot a \in A$. Moreover, $g_1 g_2 \in G$, so we may have that element act on $a \in A$.

Definition 1.21 ▶ Permutation Representation

Let G act on a set A. For fixed $g \in G$, define the map σ_g as:

$$\sigma_g : A \to A$$
$$\sigma_g(a) = g \cdot a$$

Moreover, there are two important facts:

1. For each fixed $g \in G$, then σ_g is a **permutation** of A, and
2. The map $\varphi : G \to S_A$ defined by $\varphi(g) = \sigma_g$ is a homomorphism.

Proof.

1. Let σ_g be defined as above. Then $\sigma_{g^{-1}}$ is its 2-sided inverse. For any $a \in A$, then

$$\begin{aligned}(\sigma_{g^{-1}} \circ \sigma_g)(a) &= \sigma_{g^{-1}}(\sigma_g(a)) \\ &= \sigma_{g^{-1}}(g \cdot a) \\ &= g^{-1} \cdot (g \cdot a) \\ &= (g^{-1} g) \cdot a \\ &= 1 \cdot a = a\end{aligned}$$

   So that $\sigma_{g^{-1}} \circ \sigma_g$ is the identity map on A. Interchange g and g^{-1} in the above to show that $\sigma_g \circ \sigma_{g^{-1}}$ is also the identity map on A so that σ_g has a 2-sided inverse. Hence, σ_g is a permutation of A.
2. Let φ be defined as above. Note that $\sigma_g \in S_A$ by above, because S_A consists of the set of permutations on A. Then for any $a \in A$ and $g, h \in G$, we have

$$\begin{aligned}\varphi(gh)(a) &= \sigma_{gh}(a) \\ &= (gh) \cdot a \\ &= g \cdot (h \cdot a) \\ &= \sigma_g(\sigma_h(a)) \\ &= (\varphi(g) \circ \varphi(h))(a)\end{aligned}$$

   Then φ is a homomorphism. □

We may additionally see that if given the homomorphism $\varphi : G \to S_A$, then a map $G \times A \to A$ defined by

$$g \cdot a = \varphi(g)(a) \quad \text{for all } g \in G \text{ and } a \in A$$

would satisfy the properties of a group action of G on A.

Definition 1.22 ▶ Group Action Types

1. Let G be a group with A a nonempty set. Suppose $ga = a$ for all $g \in G$ and $a \in A$. Then the group action properties clearly follow, and we call this the **trivial action**. Moreover, we say that G **acts trivially** on A. The *same* permutations are induced by *distinct* elements of G, i.e., the identity permutation. Moreover, the associated permutation representation $\varphi : G \to S_A$ satisfies that $\varphi(g)(a) = ga = a$, so that $\varphi = 1$, or the trivial homomorphism.
2. A group action G on a set A is **faithful** if distinct elements $g, h \in G$ induces distinct permutations, i.e., if $g \neq h$, then for any $a \in A$ we have that $g \cdot a \neq h \cdot a$, or that the associated permutation homomorphism is injective. Moreover, a faithful action is when the associated permutation representation is injective. For example, the trivial action on groups with $|G| > 1$, then the kernel $\{g \in G \mid gb = b \text{ for every } b \in B\}$ is equal to G, so it is *not faithful*.
3. Let G be a group with $A = G$, and define the map from $G \times A$ to A by $g \cdot a = ga$, where $a \in A, g \in G$. We then get a group action of G on itself, where each $g \in G$ permutes the elements of G by **left multiplication**. If G has an additive operation, we then write $g \cdot a = g + a$, called the **left translation**. Known as the **left regular action** of G on itself, we may check that the group action properties hold:
   For $g, h \in G$ and for any $a \in A$, then $g \cdot (h \cdot a) = g \cdot (ha) = g(ha) = (gh)a = (gh) \cdot a$. Moreover, $1 \cdot a = 1a = a$. Lastly, consider the homomorphism $\varphi : G \to S_G$ defined by $\varphi(g) = \sigma_g$. Then for any $a \in G$, we have $\varphi(g)(a) = \sigma_g(a) = g \cdot a = ga$. Supposing that $\varphi(g) = \varphi(h)$ for some $g, h \in G$, then $ga = ha$ implies $g = h$ so that φ is injective, hence the left regular action is faithful.

Example ▶ Group Actions

1. For a vector space V over a field F, the two properties of group actions that the group $F^\times$ acts on the set V are satisfied by the vector space axioms. For example, when $V = \mathbb{R}^n$ and $F = \mathbb{R}$, then the map

   $$x(r_1, r_2, \ldots, r_n) = (xr_1, xr_2, \ldots, xr_n)$$

   is a group action. For any $x, y \in \mathbb{R}$, then

   $$x(y(r_1, \ldots, r_n)) = x(yr_1, \ldots, yr_n) = (xyr_1, \ldots, xyr_n) = (xy)(r_1, \ldots, r_n)$$

   and $1(r_1, \ldots, r_n) = (r_1, \ldots, r_n)$. Note that $\varphi : \mathbb{R}^\times \to S_{\mathbb{R}^n}$ is injective, because if $\varphi(x) = \varphi(y)$, then for any $(r_1, \ldots, r_n) \in \mathbb{R}^n$, we have $\varphi(x)(r_1, \ldots, r_n) = \varphi(y)(r_1, \ldots, r_n)$, or $(xr_1, \ldots, xr_n) = (yr_1, \ldots, yr_n)$. Picking any nonzero r_i, we see that $xr_i = yr_i$ implies $x = y$. Then the multiplicative action of a field on a vector space is faithful.
2. For a nonempty set A, then let S_A act on A by $\sigma \cdot a = \sigma(a)$ for every $\sigma \in S_A, a \in A$. Clearly, for $\sigma, \tau \in S_A$, then $\sigma \cdot (\tau \cdot a) = \sigma \cdot (\tau(a)) = \sigma(\tau(a)) = (\sigma \circ \tau)(a) = (\sigma \circ \tau) \cdot a$. Moreover, $1 \cdot a = 1(a) = a$. The associated homomorphism is $\varphi : S_A \to S_A$ defined by $\varphi(\tau) = \sigma_\tau$. Since $\sigma_\tau : A \to A$ is defined as the permutation on A such that $\sigma_\tau(a) = \tau \cdot a = \tau(a)$, it follows that $\varphi(\tau)(a) = \tau(a)$, or that $\varphi(\tau) = \tau$. Then φ is the identity map on A, which has a trivial kernel so that it is actually an isomorphism (since A, thus S_A, are finite).
3. Fix the vertices of a regular n-gon. Then every element $\alpha \in D_{2n}$ is associated with a permutation σ_α of the set $\{1, 2, \ldots, n\}$, which shall be referred to as A. For example, $r \in D_{2n}$ is associated with $\sigma_r : A \to A$ where $\sigma_r(a) = a + 1$, and $\sigma_r(n) = 1$. The mapping from $D_{2n} \times A$ to A defined by $\cdot(\alpha, i) \to \sigma_\alpha(i)$ is indeed a group action: for any $\alpha, \beta \in D_{2n}$, then $\cdot(\alpha, \cdot(\beta, i)) = \cdot(\alpha, \sigma_\beta(i)) = \sigma_\alpha(\sigma_\beta(i)) = (\sigma_\alpha \circ \sigma_\beta)(i) = \cdot(\alpha \circ \beta, i)$. Moreover, $\cdot(1, i) = \sigma_1(i) = 1(i) = i$. This action is faithful, since all elements of D_{2n} are distinct.
   One thing to note is that for $n = 3$, then $D_6 \cong S_3$ because $|D_6| = |S_3|$ and the associated homomorphism is injective. It is not true, however, that $D_{2n} \cong S_n$ for $n \geq 4$, which is easy to see by considering orders.

2 Subgroups

2.1 Definitions and Examples

Definition 2.1 ▶ Subgroup

Let G be a group. Then $H \subseteq G$ is a **subgroup** if H is nonempty and H is closed under products and inverses, i.e., if $x, y \in H$, then $xy, x^{-1} \in H$. Moreover, we write $H \leq G$ if H is a subgroup of G, and $H < G$ if H is a *proper subset* of G.

- Equations in H may also be viewed as equations in G so that cancellation laws hold in H and imply that $1_G = 1_H$.

Proposition 2.1 ▶ The Subgroup Criterion

Let G be a group with $H \subseteq G$. Then $H \leq G$ if and only if

1. $H \neq \emptyset$, and
2. for all $g, h \in H$, then $gh^{-1} \in H$.

Moreover, if H is finite, then we only check that $H \neq \emptyset$ and is closed under the group operation of G.

Proof. Suppose H is a subgroup. Then (1) and (2) follow immediately, since $1 \in H$ and $h^{-1} \in H$ for any $h \in H$ since H is closed under inverses. Moreover, H is closed under multiplication.

Now suppose H satisfies (1) and (2). By (1), there exists $h \in H$. Setting $g = h$ and $h = h$ in (2), then $hh^{-1} = 1 \in H$ so that H contains the identity. Set $1 = g$ and $h = h$ so that $1h^{-1} = h^{-1} \in H$ so that H is closed under inverses. Finally, set $g = g$ and $h^{-1} = h$ so that $g(h^{-1})^{-1} = gh \in H$, hence H is closed under multiplication so that H is a subgroup of G.

Now suppose H is finite and is closed under multiplication. Pick $h \in H$. By finiteness, then there are finitely many distinct elements $x, x^2, \ldots$. We may deduce that $x^r = x^s$ for $r, s \in \mathbb{Z}$ such that $s > r$. Then $x^{s-r} = 1$ so that any $x^n \in H$ is of some finite order. Then $x^{s-r-1} = x^{-1}$ so that H is closed under inverses. □

Example ▶ Subgroup Examples

1. $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Q} \leq \mathbb{R}$ with the operation of addition.
2. A group G has always has two subgroups, $H = G$ and $H = \{1\}$. Moreover, the latter is referred to as the **trivial subgroup** and will henceforth be denoted by 1.
3. Let $G = D_{2n}$ and $H = \{1, r, \ldots, r^{n-1}\}$ be the set of all rotations in G. Then $H \leq G$.
4. The set of even integers is a subgroup of $\mathbb{Z}$ under addition.
5. The relation of being a subgroup is transitive: Suppose $H \leq G$ and $K \leq H$. Then $K \leq G$.
6. Examples of subsets that are not subgroups:
   - $(\mathbb{Q} - \{0\}, \times)$ is not a subgroup of $(\mathbb{R}, +)$ since $\times$ is not the restriction of the operation of $+$ on $\mathbb{R}$, even though $\mathbb{Q} - \{0\} \subseteq \mathbb{R} - \{0\}$.
   - $(\mathbb{Z}^+, +)$ is not a subgroup of $(\mathbb{Z}, +)$ since $0 \notin \mathbb{Z}^+$ and for any $x \in \mathbb{Z}^+$, then $-x \in \mathbb{Z}$ but $-x \notin \mathbb{Z}^+$.
   - D_6 is not a subgroup of D_8 since $D_6 \not\subseteq D_8$.

We now prove that the above examples are indeed subgroups using the above proposition:

Proof.

1. Clearly $\mathbb{Z} \neq \emptyset$. Pick $m, n \in \mathbb{Z}$. Then $m - n \in \mathbb{Z}$ so that $\mathbb{Z} \leq \mathbb{R}$. A similar proof follows to show $\mathbb{Q} \leq \mathbb{R}$.
2. Trivial to show.
3. Note that $1 \in H$. Suppose $r^i, r^j \in H$. Consider r^k, where $k = (i - j) \bmod n$. Then $0 \leq k < n$ so that $r^i r^{-j} \in H$, hence $H \leq D_{2n}$.
4. Let $\mathbb{E} = \{2n \mid n \in \mathbb{Z}\}$ denote the set of even integers. Clearly $0 \in \mathbb{E}$ so that it is nonempty. Pick $x, y \in \mathbb{E}$, where $x = 2a$ and $y = 2b$ for $a, b \in \mathbb{Z}$. Then $x - y = 2(a - b)$. Since $a - b \in \mathbb{Z}$, then $x - y \in \mathbb{E}$ so that $\mathbb{E} \leq \mathbb{Z}$.
5. Pick $a, b \in K$. Then $ab^{-1} \in H \leq G$ so that $ab^{-1} \in G$. Then $K \leq G$. □

2.2 Centralizers and Normalizers, Stabilizers and Kernels

Definition 2.2 ▶ Centralizer

Let G be a group with nonempty $A \subseteq G$. Define the subset of G:

$$C_G(A) := \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$$

This set is called the **centralizer** of A in G. Moreover, the above implies that $ga = ag$ so that $C_G(A)$ is the set of elements of G that commute with every element of A. Lastly, $C_G(A) \leq G$.

Proof. Since $1a1^{-1} = a$, then $1 \in C_G(A)$ so that it is nonempty. Suppose $x, y \in C_G(A)$, and consider xy^{-1}. Then

$$\begin{aligned}(xy^{-1})a(xy^{-1})^{-1} &= (xy^{-1})a(yx^{-1}) \\ &= x(y^{-1}ay)x^{-1} \\ &= xax^{-1} = a\end{aligned}$$

where $y^{-1}ay = a$ because $yay^{-1} = a$. Then $xy^{-1} \in C_G(A)$, hence $C_G(A) \leq G$. □

Note that if G was abelian, then $C_G(A) = G$ for any $A \subseteq G$.

Definition 2.3 ▶ Center

Let G be a group. Define the **center** of G to be the set

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

Moreover, $Z(G) \leq G$.

Proof. Since 1 commutes with all elements of G, then $1 \in Z(G)$ so that it is nonempty. Suppose $x, y \in Z(G)$. Then for any $g \in G$, we have

$$xy^{-1}gyx^{-1}g^{-1} = xy^{-1}ygg^{-1}x^{-1} = 1 \implies xy^{-1}g = gxy^{-1}$$

Then $xy^{-1} \in Z(G)$, hence $Z(G) \leq G$. □

Definition 2.4 ▶ gAg^{-1} and Normalizer

For group G and nonempty $A \subseteq G$, define the set

$$gAg^{-1} := \{gag^{-1} \mid a \in A\}$$

and the **normalizer** of A in G as

$$N_G(A) := \{g \in G \mid gAg^{-1} = A\}$$

Also, $N_G(A) \leq G$ as follows.

Proof. Note that $1A1^{-1} = A$, so $1 \in N_G(A)$. For $g, h \in N_G(A)$, then

$$\begin{aligned}(gh^{-1})A(gh^{-1})^{-1} &= (gh^{-1})A(hg^{-1}) \\ &= g(h^{-1}Ah)g^{-1} \\ &= gAg^{-1} = A\end{aligned}$$

where $h^{-1}Ah = A$ because $A = hAh^{-1}$. Then $gh^{-1} \in N_G(A)$ so that $N_G(A) \leq G$. □

Finally, if $g \in C_G(A)$, then $gag^{-1} = a$ for all $a \in A$ implies that $ga = ag$, hence $C_G(A) \leq N_G(A)$.

Example ▶ Examples of Centralizers, Centers, and Normalizers

- If G is abelian, then every element of G commutes with every other element, hence $Z(G) = G$. Moreover, for any $A \subseteq G$ with any $a \in A$, then $gag^{-1} = agg^{-1} = a$ for any $g \in G$, hence $C_G(A) = N_G(A) = G$.
- Consider $G = D_8$ and $A = \{1, r, r^2, r^3\}$, the subgroup of rotations of D_8. We compute $C_G(A), N_G(A)$, and $Z(G)$.
  Since rotations commute with each other, it follows that $A \leq C_G(A)$. Moreover, $sr \neq rs$ so that $s \notin C_G(A)$. Lastly, $sr^i \notin C_G(A)$, for otherwise $r^i sr^i = s \in C_G(A)$, which is a contradiction. Hence, $C_G(A) = A$.
  Since $C_G(A) \leq N_G(A)$ (it follows because if $g \in C_G(A)$, then $gag^{-1} = a$ for every $a \in A$ so that $gAg^{-1} = A$, hence $g \in N_G(A)$, and $C_G(A) \leq G$), then $A \leq N_G(A)$. Consider $s \in G$. Then

  $$sAs^{-1} = \{s1s^{-1}, srs^{-1}, sr^2s^{-1}, sr^3s^{-1}\}\{1, r^3, r^2, r\} = A$$

  so that $s \in N_G(A)$. Since $\langle r, s\rangle = D_8$, and $r, s \in N_G(A)$, then $G \leq N_G(A)$ so that $N_G(A) = G$.
  Observe that if $g \in Z(G)$, then $ga = ag$ for every $a \in G$ so that $gag^{-1} = a$, hence $g \in C_G(A)$. Then $Z(G) \leq C_G(A)$. In calculating $C_G(A)$, we saw that $sr \neq rs$ and $sr^3 \neq r^3s$ so that $r, r^3 \notin Z(G)$. Hence, $Z(G) = \{1, r^2\}$ only.

- Let $G = S_3$ and $A = \{1, (1\ 2)\}$. Recall that $(1\ 2)$ and $(1\ 3)$ generate S from Section 1.4, Exercise 20, and inspection leads to $A \leq C_G(A)$. Since $(1\ 3) \notin C_G(A)$, then no other element of S_3 lies in $C_G(A)$, hence $C_G(A) = A$. Moreover, note that $\sigma \in N_G(A)$ if and only if
$$\{\sigma 1\sigma^{-1}, \sigma(1\ 2)\sigma^{-1}\} = \{1, (1\ 2)\}$$
This equality occurs when $\sigma(1\ 2)\sigma^{-1} = (1\ 2)$, or when $\sigma \in C_G(A)$. Since the only nonidentity element of $C_G(A)$ is $(1\ 2)$, then $N_G(A) = A$. Lastly, $Z(G) = \{1\}$ because $Z(G) \leq C_G(A)$, and $(1\ 2) \notin Z(G)$ since $(1\ 2)(1\ 3) \neq (1\ 3)(1\ 2)$.

Stabilizers and Kernels of Group Actions

Definition 2.5 ▶ Stabilizer

Let G act on a set S with some fixed $s \in S$. Then the **stabilizer** of s in G is defined as

$$G_s := \{g \in G \mid g \cdot s = s\}$$

Note that $G_s \leq G$:

Proof. Since $1 \cdot s = s$ by definition, then $1 \in G_s$. Suppose $g, h \in G_s$. Then

$$(gh) \cdot s = g \cdot (h \cdot s) = g \cdot s = s$$

so that $gh \in G_s$. Moreover,

$$s = 1 \cdot s = (g^{-1}g) \cdot s = g^{-1} \cdot (g \cdot s) = g^{-1}s$$

so that $g^{-1} \in G_s$. It follows that $G_s \leq G$. □

One may generalize the proof above to show that $\ker(\cdot) \leq G$. Note that $\ker(\cdot)$ references every $s \in S$ so that $G_s \leq \ker(\cdot)$ since G_s refers to just one $s \in S$.

Example ▶ Examples of Stabilizers

- Let $G = D_8$ with $A = \{1, 2, 3, 4\}$ being the vertices of a square. Since no rotation except the identity preserves vertex location, then $G_i = \{1, s_i\}$ for every $i \in A$, where s_i refers to the reflection about the line from vertex i to the center. Moreover, $\ker(\cdot) = 1$ only, since no other element in D_8 fixes all vertices.
- Let $G = D_8$ again with $A = \{\{1, 3\}, \{2, 4\}\}$ be the set of opposite vertices of a square. Then the kernel of this action is $\{1, r^2, s, sr^2\}$ by Section 7, Exercise 12. Since $G_a \leq \ker(\cdot)$ for all $a \in A$, and all elements in the kernel fix all pairs of vertices of a square (order doesn't matter), then $G_a = \ker(\cdot)$ for all $a \in A$.

Definition 2.6 ▶ Connecting Centralizers, Normalizers, Kernels, and Stabilizers

Let G be a group with $S = \mathscr{P}(G)$ being the set of subsets of G. Let G act on S by *conjugation*, i.e., for each $g \in G$ and $B \subseteq G$, define the map

$$g : B \to gBg^{-1} \text{ where } gBg^{-1} = \{gbg^{-1} \mid b \in B\}$$

By definition, if $g \cdot B = B$ or $gBg^{-1} = B$ for some $B \in S$, then $G_B = N_G(B)$ which shows that $N_G(B) \leq G$.

Let $N_G(A)$ act on A by conjugation, i.e., for every $g \in N_G(A)$ and $a \in A$, then

$$g : a \mapsto gag^{-1}$$

Clearly, this is an action since $A \subseteq G$ so that g maps A to A. Moreover, note that $\ker(\cdot)$ consists of elements $g \in G$ such that $g \cdot a = gag^{-1} = a$ which is precisely the set $C_G(A)$. Then $C_G(A) \leq N_G(A) \leq G$ so that $C_G(A) \leq G$.

Let G act on G by conjugation. Similar to above, the kernel of this action is the set of $g \in G$ such that for all $a \in A$, then $gag^{-1} = a$ or that $ga = ag$, which is $Z(G)$ so that $Z(G) = G$.

2.3 Cyclic Groups and Cyclic Subgroups

Definition 2.7 ▶ Cyclic, Generators and Generated

We say a group H is **cyclic** if H is generated by a single element, i.e., there exists $h \in H$ such that $H = \{h^n \mid n \in \mathbb{Z}\}$.

- If the operation of H is additive, we may write $H = \{nh \mid n \in \mathbb{Z}\}$.
- We write $H = \langle h \rangle$ and say that H is **generated** by h, and h is a **generator** of H.
- A cyclic group may have more than one generator: if $H = \langle h \rangle$, then $H = \langle h^{-1} \rangle$ because $(h^{-1})^n = h^{-n}$ and the fact that $n \in \mathbb{Z}$ so that
$$\{x^n \mid n \in \mathbb{Z}\} = \{(x^{-1})^n \mid n \in z\}$$
- Note that elements of $\langle h \rangle$ are powers of h, not integers.
- Not all powers of h are distinct.
- Cyclic groups are always abelian, by Section 1.1, Exercise 19.

Example ▶ Cyclic Group Examples

- Let $G = D_{2n}$ for $n \geq 3$ and let $H = \langle r \rangle$ be the subgroup of all rotations. The distinct elements of H are $1, r, \ldots, r^{n-1}$ which are the distinct powers of r. It follows that $|H| = |r| = n$. In general, any power of r such as r^a can be written as r^b for some $0 \leq b < n$. By the Division Algorithm, we have for $0 \leq b < n$ that $a = nq + b$. It then follows
$$r^a = r^{nq+b} = (r^n)^q r^b = 1^q r^b = r^b$$
Since D_{2n} itself is not abelian, then it is not cyclic.
- Let $H = (\mathbb{Z}, +)$. Then $H = \langle 1 \rangle$ where 1 represents the actual integer 1 as $\mathbb{Z}$ has identity element 0, and every $h \in H$ has the form $h = n \cdot 1$ for some $n \in \mathbb{Z}$. Since every multiple of 1 is distinct and we take all positive, negative, and zero multiples, then $|H| = |1| = \infty$. Moreover, $h = (-n) \cdot (-1)$ for any $n \in \mathbb{Z}$ so that $H = \langle -1 \rangle$ as well.

Proposition 2.2 ▶ Elements of Cyclic Groups

Let $H = \langle h \rangle$. Then $|H| = |h|$. More specifically,

1. If $|H| = n < \infty$, then $h^n = 1$ and $1, h, h^2, \ldots, h^{n-1}$ are all the distinct elements of H, and
2. if $|H| = \infty$, then $h^n \neq 1$ for all $n \neq 0$ and $h^a \neq h^b$ for any $a, b \in \mathbb{Z}$ where $a \neq b$.

Proof.

1. Put $|h| = n$. If the aforementioned elements were not all distinct, then $h^x = h^y$ for some $0 \leq x < y < n$ so that $h^{y-x} = 1$, contradicting that $|h| = n$. Then $|H| \geq n$. Suppose $h^k \in H$ for any $k \in \mathbb{Z}$. By the Division Algorithm, there exists $q \in \mathbb{Z}$ and $0 \leq r < n$ such that $k = nq + r$. Then
$$h^k = h^{nq+r} = (h^n)^q h^r = 1^q h^r = h^r$$
Since $0 \leq r < n$, then h^r is one of the elements mentioned. Hence, $H = \{1, h, h^2, \ldots, h^{n-1}\}$.
2. If $|h| = \infty$ and $h^a = h^b$ for some $a, b \in \mathbb{Z}$, then $h^{b-a} = 1$, contradicting that $|h| = \infty$. Since distinct powers of h are distinct elements in H, then $|H| = \infty$. □

Proposition 2.3 ▶ Divisibility of Orders

Let G be a group with $g \in G$ and $m, n \in \mathbb{Z}$. If $g^m = g^n = 1$, then $g^d = 1$ where $d = (m, n)$. In particular, if $g^m = 1$ for $m \in \mathbb{Z}$, then $|g|$ divides m.

Proof. By the Euclidean Algorithm, there exists $s, t \in \mathbb{Z}$ such that $ms + nt = d$. Then
$$g^d = g^{ms+nt} = (g^m)^s (g^n)^t = 1^s 1^t = 1$$
Suppose $g^m = 1$ and let $|g| = n$. Certainly $n \mid m$ if $m = 0$, so assume $m \neq 0$. Moreover, $n < \infty$ since it is some nonzero power of g. Put $d = (m, n)$ so that $g^d = 1$ by the preceding proof. Since $0 < d \leq n$ and n is the smallest power that gives the identity, then $d = n$ so that $n \mid m$. □

Theorem 2.4 ▶ Cyclic Groups of Same Order are Isomorphic

Any two cyclic groups of the same order are isomorphic.

1. If $n \in \mathbb{Z}^+$ and $\langle x \rangle$ and $\langle y \rangle$ are cyclic groups of order n, then
$$\varphi : \langle x \rangle \to \langle y \rangle \quad \text{given by} \quad x^k \mapsto y^k$$
is well defined and an isomorphism.
2. If $\langle x \rangle$ is an infinite cyclic group, then the map
$$\varphi : \mathbb{Z} \to \langle x \rangle \quad \text{given by} \quad k \mapsto x^k$$
is also well defined and an isomorphism.

Proof.
1. Suppose $x^a = x^b$ for $a, b \in \mathbb{Z}$. Then $x^{b-a} = 1$ so that $n \mid b-a$. Then $nt = b-a$, or $b = nt + a$ for some $t \in \mathbb{Z}$. We then have
$$\varphi(x^b) = \varphi(x^{nt+a}) = y^{nt+a} = (y^n)^t y^a = y^a = \varphi(x^a)$$
so that φ is well defined. Moreover,
$$\varphi(x^a x^b) = \varphi(x^{a+b}) = y^{a+b} = y^a y^b = \varphi(x^a)\varphi(x^b)$$
so that φ is a homomorphism. Finally, $y^k = \varphi(x^k)$ for some $y^k \in \langle y \rangle$ so that φ is surjective. Since $\langle x \rangle$ and $\langle y \rangle$ are both finite, this implies injectivity, hence bijectivity. Then φ is an isomorphism.
2. Note that φ will be well-defined, since there is no ambiguity in the representation of elements in $\mathbb{Z}$. Moreover, Proposition 2.2 says that $x^a \neq x^b$ for distinct $a, b \in \mathbb{Z}$ so that φ is injective. Since cyclic groups take on every integer power of the generator, φ is necessarily surjective. Using similar reasoning as in (1), φ is a homomorphism, hence it is an isomorphism. Then $Z \cong \langle x \rangle$. □

Definition 2.8 ▶ Cyclic Group of Order n

For each $n \in \mathbb{Z}^+$, denote Z_n as the cyclic group of order n, written multiplicatively. We note that Z_n is the *unique* cyclic group of order n, and $Z_n \cong \mathbb{Z}/n\mathbb{Z}$. If additive notation proves to be advantageous, then we may use $\mathbb{Z}/n\mathbb{Z}$ instead of Z_n. Moreover, $\langle x \rangle$ will usually be used as the infinite cyclic group, while $\mathbb{Z}$ will be used to represent the infinite cyclic group additively.

Proposition 2.5 ▶ Orders of Elements in a Cyclic Group

Let G be a group with $g \in G$ and $a \in \mathbb{Z} - \{0\}$.
1. If $|g| = \infty$, then $|g^a| = \infty$.
2. If $|g| = n < \infty$, then $|g^a| = \dfrac{n}{(n,a)}$.
3. If $|g| = n < \infty$ and $a \mid n$, then $|x^a| = \dfrac{n}{a}$.

Proof.
1. Suppose $|g| = \infty$ but $|g^a| = m < \infty$. Then
$$g^{-am} = (g^{am})^{-1} = 1^{-1} = 1 = (g^a)^m = g^{am}$$
Since neither a nor m is 0, then one of am or $-am$ is positive, hence a positive power of g is 1, contradicting that $|g| = \infty$. Then the result follows.
2. Let $d = (n,a)$ and put $n = dx$ and $a = dy$ for $x \in \mathbb{Z}^+$ and $y \in \mathbb{Z}$. Since $d = (n,a)$, then $(x,y) = 1$. (To see why, suppose $(x,y) = e > 1$. Then $x = es$ and $y = et$ for $s, t \in \mathbb{Z}$ so that $n = des$ and $a = det$. Then $(n,a) = de > d$ since $e > 1$, contradicting the definition of d.) Observe that
$$(g^a)^x = g^{ax} = g^{dxy} = g^{ny} = (g^n)^y = 1^y = 1$$
Let $|g^a| = m$. Using Proposition 2.3 on $\langle g^a \rangle$, we see that $m \mid x$. Then
$$g^{am} = (g^a)^m = 1$$
so by applying Proposition 2.3 on $\langle g \rangle$, then $n \mid am$, or that $dx \mid dym$. Then $x \mid ym$. Since $(x,y) = 1$, then $x \mid m$. It follows that $x = m$.

3. Referring to item (2), we see that if $a \mid n$, then $(n,a) = a$. □

Proposition 2.6 ▶ Cyclic Group Generator Properties

Let $H = \langle h \rangle$.

1. If $|h| = \infty$, then $H = \langle h^a \rangle$ if and only if $a = \pm 1$.
2. If $|h| = n < \infty$, then $H = \langle h^a \rangle$ if and only if $(a,n) = 1$. In particular, the number of generators of H is $\varphi(n)$, where φ denotes Euler's φ-function.

Proof.

1. Suppose $H = \langle h^a \rangle$. In particular, $h \in H$ so that $h = h^{ak}$ for some $k \in \mathbb{Z}$. Then $a = k = 1$ or $a = k = -1$ so that $a = \pm 1$. If $a = 1$, the case is clear. If $a = -1$ instead, then Definition 2.7 asserts that h^{-1} generates H as well.
2. If $|h| = n$, then Proposition 2.2 says that $\langle h^a \rangle$ has order $|h^a|$. This generates H if and only if $|h^a| = |h|$. Using Proposition 2.5, then
$$|h^a| = |h| \iff \frac{n}{(a,n)} = n \iff (a,n) = 1$$
This is precisely the number of generators of H. □

Theorem 2.7 ▶ Fundamental Theorem of Cyclic Groups

Let $H = \langle h \rangle$ be a cyclic group.

1. Every subgroup of H is cyclic. More precisely, if $K \leq H$ then either $K = \{1\}$ or $K = \langle h^d \rangle$, where d is the smallest positive integer such that $h^d \in K$.
2. If $|H| = \infty$, then for any $a, b \in \mathbb{Z}^+$ where $a \neq b$, then $\langle h^a \rangle \neq \langle h^b \rangle$. Moreover, for every $k \in \mathbb{Z}$, then $\langle h^k \rangle = \langle h^{|k|} \rangle$, where $|k|$ is the absolute value of k. It follows that nontrivial subgroups of H correspond bijectively with $\mathbb{Z}^+$.
3. If $|H| = n < \infty$, then for every positive integer x such that $x \mid n$, there is a unique subgroup of H with order x which is the subgroup $\langle h^d \rangle$, where $d = n/x$. Moreover, for every $k \in \mathbb{Z}$, then $\langle h^k \rangle = \langle h^{(n,k)} \rangle$ so that subgroups of H correspond bijectively with all positive divisors of n.

Proof.

1. Suppose $K \leq H$. If $K = \{1\}$, we are done, so suppose it is not. Then there exists x such that $h^x \in K$. If $x > 0$, then $h^{-x} = (h^x)^{-1} \in K$ as $K \leq H$. Define the set
$$\mathscr{P} = \{y \mid y \in \mathbb{Z}^+, h^y \in K\}$$
Since $\mathscr{P}$ is a nonempty set of positive integers, then there exists a minimal element d by the Well Ordering Principle. Clearly, $\langle h^d \rangle \leq K$ since $h^d \in K$. Moreover, since $K \leq H$, then every element in K is of the form h^x for some $x \in \mathbb{Z}$. Using the Division Algorithm:
$$x = nd + r, \quad 0 \leq r < d$$
Then $h^r = h^{x-nd} = h^x (h^d)^{-n} \in K$. By minimality of d, then $r = 0$ so that $h^a = h^{nd} \in \langle h^d \rangle$ so that $K \leq \langle h^d \rangle$, and we are done.
2. Suppose $\langle h^a \rangle = \langle h^b \rangle$. Then $h^b = h^{am}$ and $h^a = h^{bn}$ for some $m, n \in \mathbb{Z}$. Then $b = am = bnm = 1$, or $b(1 - mn) = 0$. Since $b \neq 0$, then $1 - mn = 0$. This occurs when $m = n = 1$ (we disregard -1, for otherwise $m = n = -1$ implies that $b = -a$, contradicting that $a, b \in \mathbb{Z}^+$). This contradicts that a and b are distinct, hence $\langle h^a \rangle \neq \langle h^b \rangle$.

   Moreover, $k = |k|$ for $k \geq 0$ so the reuslt follows. If $k < 0$, note that $k = -|k|$ so that
$$\langle h^k \rangle = \langle h^{-|k|} \rangle = \langle (h^{|k|})^{-1} \rangle$$
Hence, $\langle h^k \rangle = \langle h^{|k|} \rangle$ for all $k \in \mathbb{Z}$.
3. Suppose $|H| = n$ and consider x such that $x \mid n$. Put $d = n/x$ so that Proposition 2.5 asserts that $\langle x^d \rangle$ is a subgroup of H with order x. For uniqueness, let K be another subgroup with order x. Then part (1) asserts that $K = \langle h^b \rangle$, where $b \in \mathbb{Z}^+$ is the smallest positive integer where $h^b \in K$. Proposition 2.5 asserts that
$$\frac{n}{d} = x = |K| = |h^b| = \frac{n}{(n,b)}$$
so that $d = (n,b)$. Then $d \mid b$ so that $h^b \in \langle h^d \rangle$, hence $\langle h^b \rangle \leq \langle h^d \rangle$. Because $|\langle h^d \rangle| = x = |K|$, then $K = \langle h^d \rangle$. □

Example ▸ Finding Subgroups

1. Using Proposition 2.6 and Theorem 2.7, we may list the subgroups of $\mathbb{Z}/n\mathbb{Z}$ for any n. For example, the subgroups of $\mathbb{Z}/12\mathbb{Z}$ are:
   - $\mathbb{Z}/12\mathbb{Z} = \langle\bar{1}\rangle = \langle\bar{5}\rangle = \langle\bar{7}\rangle = \langle\overline{11}\rangle$ with order 12,
   - $\langle\bar{2}\rangle = \langle\overline{10}\rangle$ with order 6,
   - $\langle\bar{3}\rangle = \langle\bar{9}\rangle$ with order 4
   - $\langle\bar{4}\rangle = \langle\bar{8}\rangle$ with order 3
   - $\langle\bar{6}\rangle$ with order 2,
   - $\langle\bar{0}\rangle$ with order 1.

   Moreover, the inclusions for any a, b where $1 \le a, b, \le 12$ is given as follows:

$$\langle\bar{a}\rangle \le \langle\bar{b}\rangle \iff (b,12) \mid (a,12)$$

2. Some subgroups we may form are $C_G(\langle x\rangle)$ and $N_G(\langle x\rangle)$ for some group G with $x \in G$. Moreover, note that an element $g \in G$ commutes with x if and only if g commutes with all powers of x. To see this, note that if g commutes with all powers of x, then it commutes with the 1st power. For the other direction, we proceed by induction: if $gx = xg$, then suppose it is true for $gx^n = x^n g$ for some $n \in \mathbb{Z}^+$. Then

$$gx^{n+1} = gx^n x = x^n gx = x^n xg = x^{n+1} g$$

   so that the result follows by induction. For $n = 0$, the result is clear, and for any negative x, note that g commuting with x implies commuting with x^{-1}. It follows that

$$C_G(\langle x\rangle) = C_G(x)$$

   Moreover, note that $\langle x\rangle \le N_G(\langle x\rangle)$ but equality does not need to hold.

2.4 Subgroups Generated by Subsets of a Group

Proposition 2.8 ▸ Intersection of Subgroups is a Subgroup

Let $\mathscr{A}$ be a nonempty collection of subgroups of G. Then the intersection of all members of $\mathscr{A}$ is a subgroup of G.

Proof. Put

$$K = \bigcap_{H \in \mathscr{A}} H$$

Since $H \le G$ for each $H \in \mathscr{A}$, then $1 \in H$ so that $1 \in K$. Moreover, for $g, h \in K$, then $g, h \in H$ for every $H \in \mathscr{A}$. Then $gh^{-1} \in H$ for each $H \in \mathscr{A}$ so $gh^{-1} \in K$, hence $K \le G$. □

Definition 2.9 ▸ Subgroup of G Generated by A

Let A be a subset of a group G. Then the **subgroup of G generated by A** is defined as

$$\langle A\rangle := \bigcap_{\substack{A \subseteq H \\ H \le G}} H$$

i.e., $\langle A\rangle$ is the intersection of all subgroups of G that contain A. Moreover, $\langle A\rangle \le G$ by applying Proposition 2.8 on $\mathscr{A} = \{H \le G \mid A \subseteq H\}$. Lastly, $\langle A\rangle$ is the *unique minimal* element of $\mathscr{A}$ that satisfies this: $\langle A\rangle$ is a subgroup of G that contains A so $\langle A\rangle \in \mathscr{A}$, and any element of $\mathscr{A}$ must contain the intersection of all elements in $\mathscr{A}$, or contain $\langle A\rangle$.

Lastly, if A is the finite set $\{a_1, a_2, \ldots, a_n\}$, then we write $\langle a_1, a_2, \ldots, a_n\rangle$ for the group generated by said elements. If A, B are subsets of G, then we write $\langle A, B\rangle$ rather than $\langle A \cup B\rangle$.

Definition 2.10 ▸ Closure, Words

Let A be a subset of a group G. Then the **closure** of A under the group operation of G is the set

$$\bar{A} := \{a_1^{\varepsilon_1} a_2^{\varepsilon_2} \ldots a_n^{\varepsilon_n} \mid n \in \mathbb{Z}^+ \cup \{0\}, a_i \in A, \varepsilon_i = \pm 1 \text{ for each } i\}$$

where $\overline{A} = \{1\}$ if A is empty. The elements of $\overline{A}$ are known as **words** and consist of all finite products of elements in A and inverses of elements in A. Moreover, each a_i need not be distinct (so that $a^2 = aa$ in $\overline{A}$), and $\overline{A}$ need not be a finite or countable set.

Proposition 2.9 ▶ $\overline{A} = \langle A \rangle$

Let G be a group with $A \subseteq G$. Then $\overline{A} = \langle A \rangle$.

Proof. We begin by showing $\overline{A} \leq G$. By definition, $\overline{A}$ is never empty. Suppose $a, , b \in \overline{A}$ with $a = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n}$ and $b = b_1^{\delta_1} b_2^{\delta_2} \dots b_m^{\delta_m}$. Then

$$ab^{-1} = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n} b_m^{-\delta_m} b_{m-1}^{-\delta_{m-1}} \dots b_1^{-\delta_1}$$

It follows that ab^{-1} is a word so that $\overline{A} \leq G$.

Since any $a \in A$ is written as a^1, then any associated product of this form is also in $\langle A \rangle$ so that $\langle A \rangle \subseteq \overline{A}$. Conversely, $\langle A \rangle$ is a group that contains A and thus must contain elements of the form $a_1^{\varepsilon_1} a_2^{\varepsilon_2} \dots a_n^{\varepsilon_n}$ so that $\overline{A} \subseteq \langle A \rangle$. □

Note ▶ A Discussion on $\overline{A}$

- We now use $\langle A \rangle$ in place of $\overline{A}$. Noting that products such as $a \cdot a \cdot a$ can be simplified to a^3, we redefine $\langle A \rangle$ as such:
$$\langle A \rangle = \{a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n} \mid \text{for each } i,\ a_i \in A, \alpha_i \in \mathbb{Z}, a_i \neq a_{i+1}, n \in \mathbb{Z}^+\}$$
- Suppose G is abelian. Then we may commute the a_i together to obtain the above form but removing the necessity that $a_i \neq a_{i+1}$. Moreover, if each a_i has finite order d_i for every i, then the number of distinct products $a_1^{\alpha_i} a_2^{\alpha_2} \dots a_k^{\alpha_k}$ for $\alpha_i \in \mathbb{Z}$ is at most $d_1 d_2 \dots d_k$, hence
$$|\langle A \rangle| \leq d_1 d_2 \dots d_k$$
A situation to note is that it may occur that $a^\alpha b^\beta = a^\gamma b^\delta$ even though $a^\alpha \neq a^\gamma$ and $b^\beta \neq b^\delta$.
- Non-abelian groups prove to have much harder structures to deduce, as seen in the examples below. In general, it is impractical and difficult to analyze the subgroup generated by random subsets of a group, but we may choose specific subsets such as $C_G(x)$ or $N_G(x)$ to get some upper bound on the generated subgroup.

Example ▶ Generators of Non-Abelian Groups

- Let $G = D_8$ with $a = s, b = rs$, and let $A = \{a, b\}$. Since $r \in \langle a, b \rangle$ because $ba = r$, then $A = G$. However, $|D_8| = 8$ but $|a| = |b| = 2$ so that there are elements in D_8 that are not of the form $a^\alpha b^\beta$ for $\alpha, \beta \in \mathbb{Z}$. This shows that, unlike the examination on abelian (including cyclic) groups, we cannot obtain an upper bound on the order of a non-abelian group.
- Consider $S_n = \langle (1\ 2), (1\ 2\ 3 \dots n) \rangle$. Then $(1\ 2)$ has order 2, while $(1\ 2\ 3 \dots n)$ has order n, but $|S_n| = n!$.
- Let $G = \mathrm{GL}_2(\mathbb{R})$. Consider the matrices
$$a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 2 \\ 1/2 & 0 \end{pmatrix}$$
Observe that $|a| = |b| = 2$, but $|ab|$ is infinite. Then $\langle a, b \rangle$ is an infinite subgroup of $\mathrm{GL}_2(\mathbb{R})$ that is generated by two elements of order 2.

2.5 The Lattice of Subgroups of a Group

Definition 2.11 ▶ Subgroup Lattice

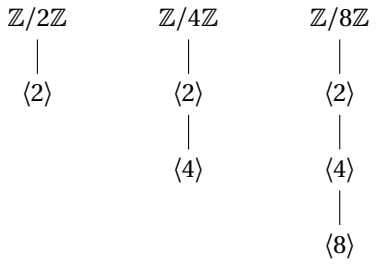
- In a given group with relationships between its subgroups, we may draw what's known as a **subgroup lattice**, which depicts containment of the subgroups. We may construct it as follows:
  1. Let G be a finite group. The bottom of the graph consists of only the trivial subgroup 1, and the top of the graph consists of G.
  2. Put subgroups of larger order higher on the graph.
  3. For subgroups H and K, we draw a line from H to K if $H \leq K$ *and* there are no other subgroups proper subgroups. Note that there may be many paths from H to K if H is contained in other subgroups, or if K contains other subgroups.
  4. The initial positioning of the subgroups may be chosen a priori to produce a "nicer" picture.

- For any two subgroups H and K in the subgroup lattice, there is a unique smallest subgroup $\langle H, K\rangle$, called the **join** of H and K, that contains both H and K. We may ensure that a path is drawn from H and K to $\langle H, K\rangle$ as follows: if we draw a path from H and K to another subgroup L, but we find another subgroup L_1 such that $L_1 \leq L$, draw a path from H and K to L_1 instead and check if $L_1 = \langle H, K\rangle$.
- The process of drawing subgroup lattices cannot be done for infinite groups.
- Isomorphic groups have the same lattices, and nonisomorphic groups may have the same lattices which could prove useful in determining properties that are held between the two.

Example ▸ Subgroup Lattices Drawn Out

Note that the following examples should only be taken as fact, with proofs of the subgroup lattices for *non-cyclic* groups being seen later in the text.

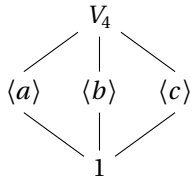
1. For $Z_n \cong \mathbb{Z}/n\mathbb{Z}$, Theorem 2.7 says that the subgroups of Z_n is the lattice of divisors of n. Specific examples are:



2. The **Klein 4-group (Vierergruppe)**, V_4, is the group of order 4 with each nonidentity element order 2

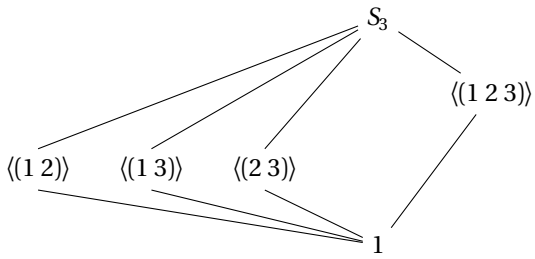
·	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

and lattice

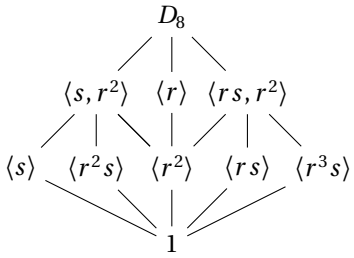


Note that V_4 is abelian that is not isomorphic to Z_4 since it does not contain elements of order 3.

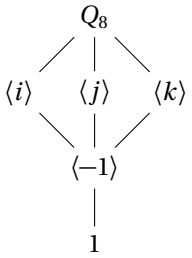
3. S_3 is the lattice:



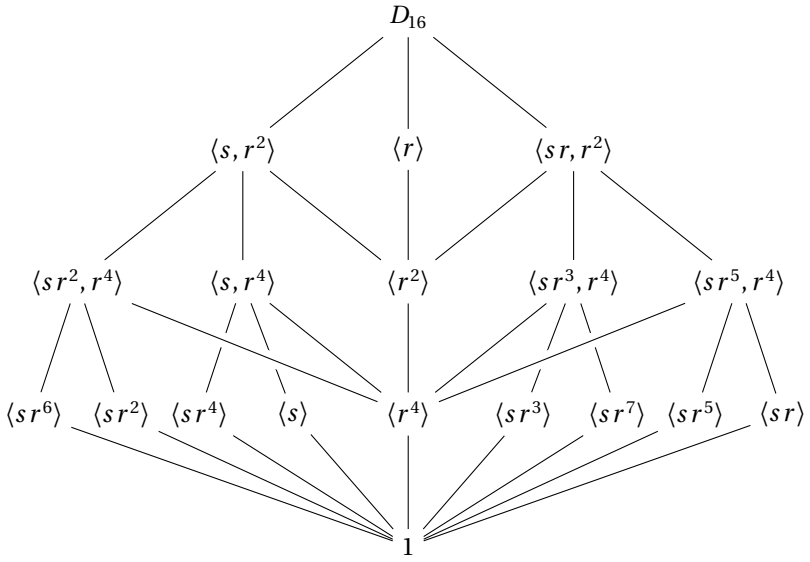
4. D_8 is the lattice:



5. Q_8 is the lattice:

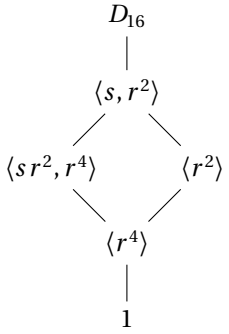


6. D_{16} has a lattice that is not a planar graph, or is a graph drawn on a plane without lines crossing. A way of drawing it is



Note ► Sublattices and Computing Centralizers and Normalizers

- For any given proof or problem, we are often interested only in a portion of its subgroup lattice. We may then construct a *sublattice* of the subgroup lattice, which involves only relevant joins and intersections for the groups. For example, we may discuss only the relationship between the subgroups $\langle sr^2, r^4\rangle$ and $\langle r^2\rangle$ of D_{16}, in which case we may draw the sublattice



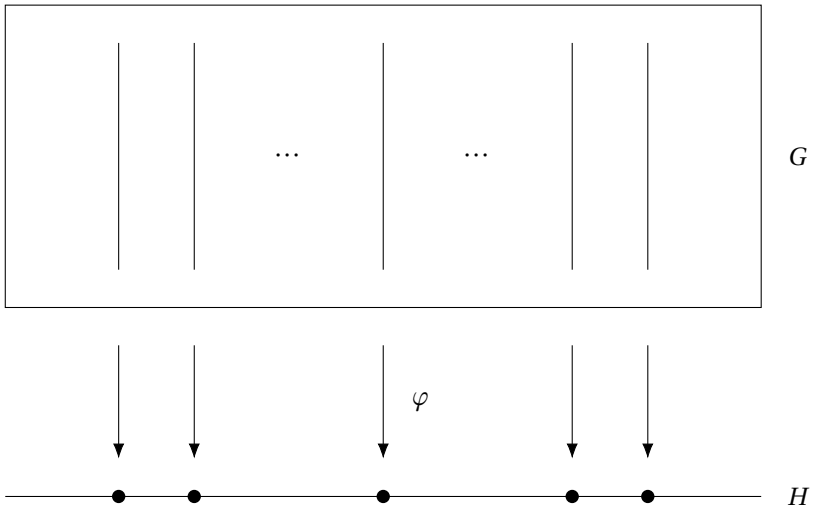
- When we have access to the subgroup lattice of a group, we can compute normalizers and centralizers. In D_8, we see that $C_{D_8}(s) = \langle s, r^2\rangle$ because we know that $r^2 \in C_{D_8}(s)$ so that $\langle s, r^2\rangle \leq C_{D_8}(s)$. Since no other subgroups that contain $\langle s, r^2\rangle$ except itself and D_8, and $r \notin C_{D_8}(s)$ so that $C_{D_8}(s) \neq D_8$, it must be that $C_{D_8}(s) = \langle s, r^2\rangle$.

3 Quotient Groups and Homomorphisms

3.1 Definitions and Examples

Note ▸ Set of Fibers as a Group

- To study a group G, we will introduce the idea of a quotient group of G, which is essentially a "smaller" group from G that we may use to study G itself.
- The studying of this quotient group is equivalent to studying the homomorphisms of G. Recall that for a homomorphism $\varphi : G \to H$, the *fibers* of φ are the sets of elements of G that project to a set of elements in H. We may present this pictorially as follows:



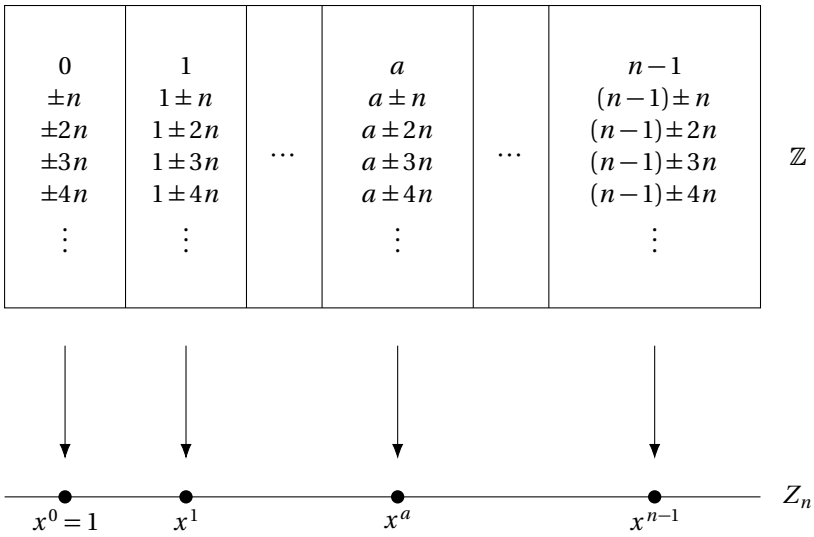
- Two elements on the horizontal line in H provides a natural idea of making the set of fibers into a group: Let F_a be the fiber above a and F_b be the fiber above b, then F_{ab} is the fiber above the product ab so that $F_a F_b = F_{ab}$. Moreover, the identity of this group is $F_1 = \ker(\varphi)$, associativity follows because of associativity in H, i.e., $(F_a F_b)F_c = F_{ab}F_c = F_{(ab)c} = F_{a(bc)} = F_a F_{bc} = F_a(F_b F_c)$. Lastly, the inverse of F_a is simply $F_{a^{-1}}$. In general, the group G has now been partitioned into pieces, and these pieces have formed into a quotient group.

Example ▸ Example of Partitioning $\mathbb{Z}$ Into Z_n

Define $\varphi : \mathbb{Z} \to Z_n$ by $\varphi(a) = x^a$. Since $\varphi(m+n) = x^{m+n} = x^m x^n = \varphi(m)\varphi(n)$, then φ is a group homomorphism. Moreover, φ is surjective. Then the fiber of φ over x^a is the set

$$\varphi^{-1}(x^a) = \{m \in \mathbb{Z} \mid x^m = x^a\} = \{m \in \mathbb{Z} \mid x^{m-a} = 1\} = \{m \in \mathbb{Z} \mid n \text{ divides } m-a\} = \{m \in \mathbb{Z} \mid m \equiv a \bmod n\} = \overline{a}$$

the fibers of φ are precisely the residue classes modulo n. Then the above picture becomes



In Z_n, we have $x^a x^b = x^{a+b}$ with corresponding fibers $\overline{a}$, $\overline{b}$, and $\overline{a+b}$, hence the corresponding group operation for the set of fibers is $\overline{a}\cdot\overline{b} = \overline{a+b}$, which is isomorphic to the group $\mathbb{Z}/n\mathbb{Z} \cong \text{im}(Z_n)$. The identity is the multiples of n in $\mathbb{Z}$, or $n\mathbb{Z}$. The remaining fibers are the translates $a + n\mathbb{Z}$.

Definition 3.1 ▶ Kernel

Let $\varphi : G \to H$ be a homomorphism. Then the **kernel** of φ is the set

$$\ker(\varphi) := \{g \in G \mid \varphi(g) = 1\}$$

where 1 is the identity of H.

Proposition 3.1 ▶ Homomorphism Properties

1. $\varphi(1_G) = 1_H$, where 1_G and 1_H are the identities of G and H, respectively.
2. $\varphi(g^{-1}) = \varphi(g)^{-1}$ for every $g \in G$.
3. $\varphi(g^n) = \varphi(g)^n$ for every $n \in \mathbb{Z}$.
4. $\ker(\varphi) \leq G$.
5. $\text{im}(\varphi) \leq H$.

Proof.

1. $\varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G)\varphi(1_G)$. By cancellation, $1_H = \varphi(1_G)$.
2. $1_H = \varphi(1_G) = \varphi(g g^{-1}) = \varphi(g)\varphi(g^{-1})$ for all $g \in G$. Then $\varphi(g)^{-1} = \varphi(g^{-1})$.
3. This is true for $n = 0$, by part (1). It holds true for $n = 1$. Suppose it is true for any $n \in \mathbb{Z}^+$. Then

$$\varphi(g^{n+1}) = \varphi(g^n g) = \varphi(g^n)\varphi(g) = \varphi(g)^n \varphi(g) = \varphi(g)^{n+1}$$

so the result for positive integers holds true by induction. Moreover, for any $n < 0$, then

$$\varphi(g^m) = \varphi((g^{-1})^{-m}) = (\varphi(g)^{-1})^{-m} = \varphi(g)^m$$

so it holds true for all $n \in \mathbb{Z}$.

4. Since $\varphi(1_G) = 1_H$, then $\ker(\varphi)$ is nonempty. Suppose $x, y \in \ker(\varphi)$. Then $\varphi(x y^{-1}) = \varphi(x)\varphi(y^{-1}) = 1_H 1_H^{-1} = 1_H$ so that $x y^{-1} \in \ker(\varphi)$. Then $\ker(\varphi) \leq G$.
5. Note that $\varphi(1_G) = 1_H$ so that $1_H \in \text{im}(\varphi)$. Suppose $x, y \in \text{im}(\varphi)$. Then there exists $g, h \in G$ such that $\varphi(g) = x$ and $\varphi(h) = y$. Then $x y^{-1} = \varphi(g)\varphi(h^{-1}) = \varphi(g h^{-1})$. Since $g h^{-1} \in G$, then $x y^{-1} \in \text{im}(\varphi)$, hence $\text{im}(\varphi) \leq H$. □

Definition 3.2 ▶ Quotient Group

- Let $\varphi : G \to H$ be a homomorphism with kernel K. Then the **quotient group**, or **factor group**, G/K (read as G *modulo* K or G *mod* K) is the group whose elements are the fibers of φ with group operation defined above: if X is the fiber above a and Y is the fiber of b, then the product XY is defined as the fiber above the product ab.

- This defines K to be a single element in G/K with the other elements of G/K being translates of K. Then G/K is collapsing the group G by K

Proposition 3.2 ▶ Defining Homomorphism Sets

Let $\varphi : G \to H$ be a homomorphism of groups with kernel K. Let $X \in G/K$ be the fiber above a, or $X = \varphi^{-1}(a)$. Then

1. For any $x \in X$, $X = \{xk \mid k \in K\}$.
2. For any $x \in X$, $X = \{kx \mid k \in K\}$.

Proof.

1. Let $x \in X$ so that $\varphi(x) = a$. Let
$$xK = \{xk \mid k \in K\}$$
For any $k \in K$, then
$$\varphi(xk) = \varphi(x)\varphi(k) = \varphi(x) = a$$
so that $xk \in X$, hence $xK \subseteq X$. Now suppose $y \in X$, and put $k = x^{-1}y$. Then
$$\varphi(k) = \varphi(x^{-1})\varphi(y) = \varphi(x)^{-1}\varphi(y) = a^{-1}a = 1$$
so that $k \in \ker(\varphi)$. Since $k = x^{-1}y$, then $y = xk \in xK$ so that $X \leq xK$.
2. The proof follows similarly as (1), where we define
$$Kx = \{kx \mid k \in K\}$$
Showing $Kx \subseteq X$ is similar, and if we set $k = yx^{-1}$, then $k \in \ker(\varphi)$ so that $kx = y \in X$, hence $X \subseteq Kx$. □

Definition 3.3 ▶ Left and Right Cosets

- Let $N \leq G$ and $g \in G$. Then
$$gN = \{gn \mid n \in N\} \text{ and } Ng = \{ng \mid n \in N\}$$
are called the **left coset** and **right coset** of N in G respectively. Moreover, any element of a coset is a **representative** of that coset.
- If N is the kernel of a homomorphism and h is a representative for the coset gN (or Ng), then $hN = gN$ (or $Nh = Ng$). This become for any subgroup N.
- In additive groups G, we write $g + N$ and $N + g$ for left and right cosets respectively. We may see that the left coset gN is the left translate of N by g in G.
- Proposition 3.2 shows that the fibers of a homomorphisms are the left/right cosets of the kernel, i.e., the elements of the quotient group G/K are the left cosets gK for $g \in G$.

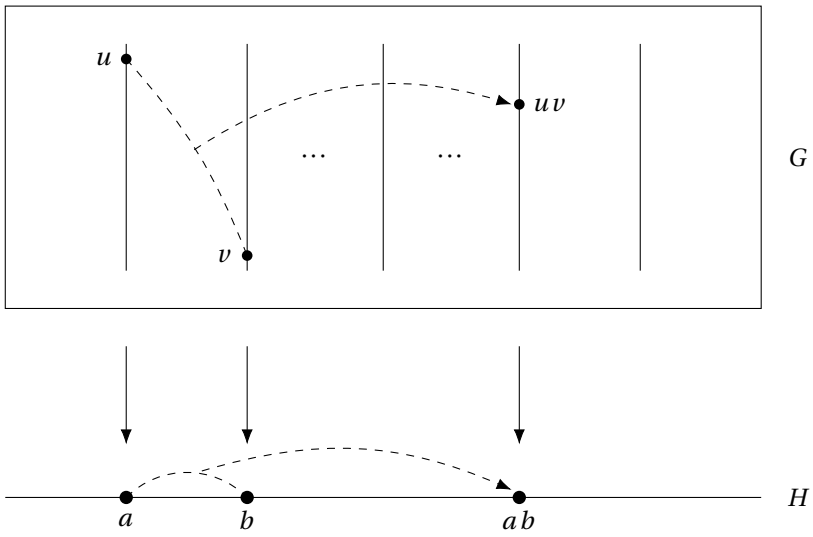
Theorem 3.3 ▶ Coset Multiplication

Let G be a group with K a group homomorphism from G to another group. The set of left cosets of K in G defined with the operation
$$uK \circ vK = (uv)K$$
forms a group, G/K. In particular, this operation is well defined in that if $u' \in uK$ and $v' \in vK$, then $u'v' \in uvK$, and $u'v'K = uvK$. Moreover, this is also analogously defined for right cosets.

Proof. Let $X, Y \in G/K$ and let $Z = XY \in G/K$ so that X, Y, and Z are left cosets of K. Since K is the kernel of a group homomorphism, then $X = \varphi^{-1}(a)$ and $Y = \varphi^{-1}(b)$ for $a, b \in H$. Moreover, $Z = \varphi^{-1}(ab)$ by definition. Let $x \in X$ and $y \in Y$ so that $\varphi(x) = a$ and $\varphi(y) = b$. Then $X = xK$ and $Y = yK$. Then
$$\varphi(u)\varphi(v) = \varphi(uv) = ab \iff uv \in \varphi^{-1}(ab) \iff uv \in Z$$
Then Z is the left coset uvK. An exercise below will show that every $z \in Z$ is written as xy for $x \in X$ and $y \in Y$. Then $XY = Z$, and by Proposition 3.2, it follows that $xK = Kx$ and $yK = Ky$ for every $x, y \in G$. □

Note ▶ Additional Coset Notes

- By the preceding theorem, multiplication is independent of the particular representatives chosen. A coset uK containing u will usually be denoted with $\overline{u}$, and a quotient group G/K will be denoted as $\overline{G}$, and the product of two elements $\overline{u}$ and $\overline{v}$ is the coset containing uv, or $\overline{uv}$.
- The following is a pictorial representation of coset multiplication:



Example ▸ Quotient Group Examples

- The homomorphism $\varphi : \mathbb{Z} \to Z_n$ has fibers $a + n\mathbb{Z}$ of the kernel $n\mathbb{Z}$. By Theorem 3.3, the set of cosets forms a group under addition of representatives, which is $\mathbb{Z}/n\mathbb{Z}$.
- If $\varphi : G \to H$ is an isomorphism, then $K = 1$ as φ is injective, and the fibers of φ are singleton subsets. It follows easily that $G/1 \cong G$ with the isomorphism $\psi : G/1 \to G$ given by $\psi(g1) = g$.
- The *trivial homomorphism* is $\varphi : G \to 1$ with $\ker(\varphi) = G$ so that $G/G \cong Z_1 = \{1\}$.
- Let $G = \mathbb{R}^2$ and $H = \mathbb{R}$. Define $\varphi : \mathbb{R}^2 \to \mathbb{R}$ by $\varphi((x,y)) = x$ so that φ is a projection onto the x-axis. This is clearly a homomorphism, as

$$\varphi((x,y)+(a,b)) = \varphi((x+a, y+b)) = x + a = \varphi(x,y) + \varphi(a,b)$$

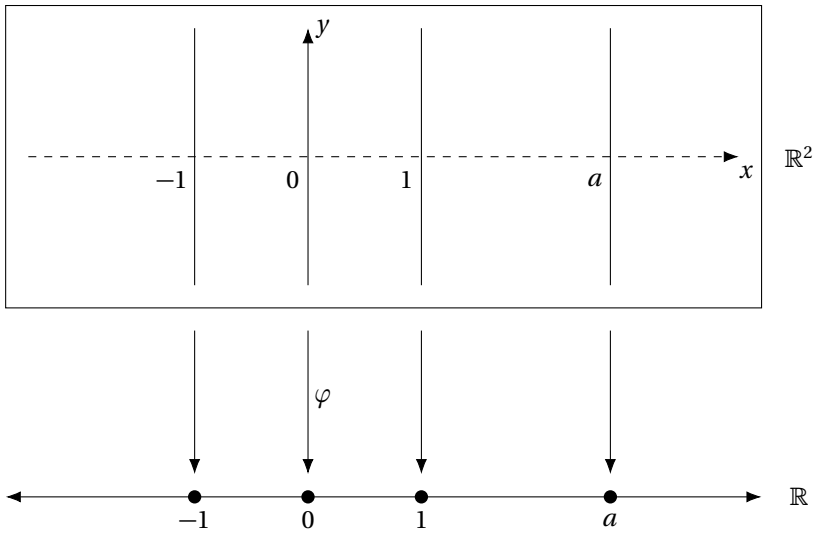
Moreover,

$$\ker(\varphi) = \{(x,y) \mid \varphi((x,y)) = 0\} = \{(x,y) \mid x = 0\}$$

which is just the y-axis. Then the cosets in $\overline{\mathbb{R}^2}$ are the elements $\overline{(a,0)}$ that represent

$$(a,0) + y\text{-axis}$$

or left/right translates of the y-axis by some real number a (hence the vertical line $x = a$). Note that the choice of representatives is not important, as any y-coordinate can be chosen without abandon. The group operation in $\overline{\mathbb{R}^2}$ is described as follows: in the perspective of the mapping φ, then we can sum the lines $x = a$ and $x = b$ to obtain $x = a + b$, or if we add the coset representatives of the vertical line containing (a,y) and the vertical line containing (b,y'), then we get the vertical line containing $(a+b, y+y')$. A diagram below describes this pictorially:



- Define $\varphi : Q_8 \to V_4$ by

$$\varphi(\pm 1) = 1, \quad \varphi(\pm i) = a, \quad \varphi(\pm j) = b, \quad \varphi(\pm k) = c$$

To see that φ is a homomorphism, note the following:

$$\begin{aligned} \varphi(ij) = \varphi(k) = c = ab = \varphi(i)\varphi(j) \\ \varphi(ik) = \varphi(j) = b = ac = \varphi(i)\varphi(k) \\ \varphi(jk) = \varphi(i) = a = bc = \varphi(j)\varphi(k) \end{aligned}$$

In each of these, we may note that we may swap the placements of the a, b, c in the 3rd equality in each line as V_4 is abelian to get the corresponding negative Q_8 element. φ is surjective, and $\ker(\varphi) = \{\pm 1\}$. We think of φ as an absolute value function, which collapses similar terms to just one value. The fibers of φ are $F_1 = \{\pm 1\}, F_a = \{\pm i\}, F_b = \{\pm j\}$, and $F_c = \{\pm k\}$, which subsequently collapse to $1, a, b$, and c respectively in $Q_8/\langle -1\rangle$. Moreover, note that the fibers are exactly equivalent to the cosets of $\ker(\varphi)$ (for example, $F_a = i\ker(\varphi) = \{i, -i\}$.

Proposition 3.4 ▶ Set of Cosets Partition Group and Equivalency of Two Cosets

Let N be a subgroup of a group G. Then the set of left cosets of N in G form a partition of G. Moreover, for every $g, h \in G$, then $gN = hN$ if and only if $h^{-1}g \in N$. In particular, $gN = hN$ if and only if g and h are representatives of the same coset.

Proof. Since $N \leq G$, then $1 \in N$ so that $g \in gN$ for every $g \in G$. Then

$$G = \bigcup_{g \in G} gN$$

If $gN \cap hN$ is empty, then we are done. If it not, we then have some $k \in gN \cap hN$. Then $k = gn = hn'$ for some $n, n' \in N$. Then $g = kn^{-1} = hn'n^{-1}$, where we note that $n'n^{-1} \in N$ because $N \leq G$. Then for any $gn_0 \in gN$ for some $n_0 \in N$, we have $gn_0 = hn'n^{-1}n_0 \in hN$ so that $gN \subseteq hN$. A similar argument shows that $hN \subseteq gN$ so that they are equal, hence cosets are either distinct or are equal.

From the preceding argument, we see that $gN = hN$ if and only if $g \in hN$ if and only if $g = hn$ for $n \in N$ if and only if $h^{-1}g \in N$. Moreover, $h \in gN$ implies that h is a representative of gN so that $hN = gN$ if and only if g and h represent the same coset. □

Proposition 3.5 ▶ Coset Multiplication Part 2

Let G be a group with $N \leq G$.

1. The operation on the set of left cosets of N in G described by

$$gN \cdot hN = (gh)N$$

is well defined if and only if $xnx^{-1} \in N$ for every $x \in G$ and $n \in N$.

2. If the above operation is well defined, then the set of left cosets of N in G forms a group. In particular, the identity of this group is the coset $1N = N$ and the inverse of gN is $(gN)^{-1} = g^{-1}N$.

Proof.
1. Suppose the operation is well defined, and let $g \in G$ and $n \in N$. Then $g^{-1}N = ng^{-1}N$. Since $1 \in N$, then $ng^{-1}1 \in ng^{-1}N$ so that $ng^{-1} = g^{-1}n'$ for some $n' \in N$. Then $gng^{-1} \in N$.
   If $gng^{-1} \in N$ instead for every $g \in G$ and $n \in N$, suppose $g, g' \in gN$ and $h, h' \in hN$. Then
$$g' = gn, \quad h' = hn' \quad \text{for } n, n' \in N$$
   Then
$$g'h' = (gn)(hn') = g(hh^{-1})nhn' = gh(h^{-1}n(h^{-1})^{-1})n'$$
   where we note that $h^{-1}n(h^{-1})^{-1} \in N$ by assumption. Then $g'h' \in ghN$ so that $g'h'N \cap ghN$ is nonempty. By Proposition 3.4, then $g'h'N = ghN$.
2. If the operation is indeed well defined, then the group axioms hold easily due to G being a group. In particular, associativity holds as follows for any $g, h, k \in G$
$$gN(hNkN) = gN(hkN) = g(hk)N = (gh)kN = (ghN)kN = (gNhN)kN$$
   The identity in G/N is $1N$, and if $gNxN = 1N$ for $x \in G$, it follows that $gx = 1$ implies $x = g^{-1}$ so that $(gN)^{-1} = g^{-1}N$. □

Definition 3.4 ▶ Conjugate, Normal

Let G be a group with $g \in G$ and $N \leq G$.
- The element gng^{-1} is the **conjugate** of $n \in N$ by g.
- The set $gNg^{-1} = \{gng^{-1} \mid n \in N\}$ is the **conjugate** of N by g. Moreover, we say g **normalizes** N if $gNg^{-1} = N$.
- N is called **normal** if every $g \in G$ normalizes N, or $gNg^{-1} = N$ for every $g \in G$. Moreover, we write $N \trianglelefteq G$.

Theorem 3.6 ▶ Normal Subgroup Results

Let G be a group with $N \leq G$. Then the following are equivalent:
1. $N \trianglelefteq G$,
2. $N_G(N) = G$,
3. $gN = Ng$ for every $g \in G$,
4. the operation on left cosets of N in G described in Proposition 3.5 makes the set of left cosets into a group,
5. $gNg^{-1} \subseteq N$ for every $g \in G$.

Proof. (1) $\iff$ (2): $N \trianglelefteq G$ if and only if $gNg^{-1} = N$ for every $g \in G$ if and only if $N_G(N) = G$.
(2) $\implies$ (3): Since $N_G(N) = G$, then $gNg^{-1} = N$ for every $g \in G$. In particular, $gng^{-1} = n'$ for $n, n' \in N$ so that $gn = n'g$, or $gN = Ng$.
(3) $\implies$ (4): Since $gN = Ng$ for every $g \in G$, then $gn = n'g$ for some $n, n' \in N$, or that $gng^{-1} \in N$ for every $g \in G$. By Proposition 3.5, the implication follows.
(4) $\implies$ (5): The coset being formed into a group implies the operation is well defined, or that $gng^{-1} \in N$ for every $g \in G$. Then $gNg^{-1} \subseteq N$.
(5) $\implies$ (1): If $gNg^{-1} \subseteq N$ for every $g \in G$, then $g^{-1}Ng \subseteq N$ in particular. Let $n \in N$. Then for some $g \in G$, we have that $gng^{-1} \in N$. Then $n = g(g^{-1}ng)g^{-1} \in gNg^{-1}$ so that $N \subseteq gNg^{-1}$, hence $N \trianglelefteq G$. □

Note ▶ Calculating a Normal Subgroup
- A good goal is to minimize the computations necessary to determine if $N \trianglelefteq G$. Particularly, we minimize the calculations of all conjugates gng^{-1} for some $n \in N$ and $g \in G$.
- In a later exercise, it will suffice to note that the elements of N normalize N itself since $N \leq G$. Moreover, if N is found to have a set of generators, then we may only check the generators, since the conjugate of a product is the product of its conjugates, and the conjugate of the inverse is the inverse of a conjugate.
- If a set of generators for G is also known, then we may only check that these generators normalize N, so in particular, knowing both sets of generators for G and N reduces the calculations considerably.
- Some examples show that directly showing $N_G(N) = G$ proves that $N \trianglelefteq G$ without computing all conjugates.

Proposition 3.7 ▶ Subgroup is Normal If and Only If Kernel

Let G be a group with $N \leq G$. Then $N \trianglelefteq G$ if and only if $\ker(\varphi) = N$ for some homomorphism φ.

Proof. Suppose $N \trianglelefteq G$. Define the mapping $\pi : G \to G/N$ given by

$$\pi(g) = gN, \quad \text{for every } g \in G$$

Then π is a homomorphism, because

$$\pi(gh) = (gh)N = gNhN = \pi(g)\pi(h)$$

Then

$$\ker(\pi) = \{g \in G \mid \pi(g) = 1N = N\} = \{g \in G \mid gN = N\} = \{g \in G \mid g \in N\} = N$$

so that N is the kernel of a homomorphism. Conversely, if N is the kernel instead, then Proposition 3.2 says that the left and right cosets of N with both being the fibers of the homomorphism. Then Theorem 3.6 implies that $N \trianglelefteq G$. □

Definition 3.5 ▶ Natural Projection

Let $N \trianglelefteq G$. The homomorphism $\pi : G \to G/N$ defined by $\pi(g) = gN$ is the **natural projection** of G onto G/N. Moreover, if $\overline{H} \leq G/N$, then the **complete preimage** of $\overline{G}$ in G is $\pi^{-1}(\overline{H})$.

Note ▶ A Word on Normal Subgroups and Quotient Groups

- We first note that the complete preimage of a subgroup of G/N is a subgroup of G that contains N since they are the elements that map $\overline{1} \mapsto \overline{H}$.
- A criterion that determines a subgroup N of G is the kernel of a homomorphism is when

  $$N_G(N) = G$$

  Then the normalizer of a subgroup N of G determines "how close" N is to being a normal subgroup of G, hence the choice of name. We note that being normal depends on the relation of N to G rather than depending on the structure of N itself, i.e., it may be true that $N \trianglelefteq G$ but $N \ntrianglelefteq H$ for some $H \supseteq G$.
- The kernel of a homomorphism is a normal subgroup N of G, and the quotient G/N is naturally isomorphic to $\text{im}(\varphi(G))$. Conversely, for $N \trianglelefteq G$, then we are equipped with G/N and $\pi : G \to G/N$ where $\ker(\pi) = N$ (the natural projection). It follows that when discussing homomorphic images of G is equivalent to discussing quotient groups of G and producing normal subgroups.
- Lastly, we emphasize that elements of a quotient group are subsets of G.

Example ▶ Normal Subgroups and Associated Quotients

Let G be a group.

- It is easy to show that $1 \trianglelefteq G$ and $G \trianglelefteq G$, and $G/1 \cong G$ and $G/G \cong 1$.
- If G is abelian, then any $N \leq G$ is normal because for every $g \in G$ and $n \in N$, then

  $$gng^{-1} = gg^{-1}n = n \in N$$

  It must be that G is abelian, not just N being abelian.
- If $G = \mathbb{Z}$, then every subgroup of N is cyclic:

  $$N = \langle n \rangle = \langle -n \rangle = n\mathbb{Z}, \quad \text{for some } n \in \mathbb{Z}$$

  so that $G/N = \mathbb{Z}/n\mathbb{Z}$ is a cyclic group with generator $\overline{1} = 1 + n\mathbb{Z}$. We also note that $\mathbb{Z} = \langle 1 \rangle$.
- Suppose $G = Z_k$, let $Z_k = \langle x \rangle$, and let $N \leq G$. Then $N = \langle x^d \rangle$ by Proposition 2.6, where d is the smallest power such that $x^d \in N$. Then

  $$G/N = \{gN \mid g \in G\} = \{x^\alpha N \mid \alpha \in \mathbb{Z}\}$$

  By a following exercise that will show $x^\alpha N = (xN)^\alpha$, then $G/N = \langle xN \rangle$ so that the quotient group G/N is cyclic with xN as a generator. A following exercise will also show that $x^d \in N$ implies that $|xN| = d$. Moroever, Proposition 2.5 shows that $d = |G|/|N|$. This discussion shows that *quotient groups of a cyclic group are cyclic*, and if $G = \langle g \rangle$, then $G/N = \langle \overline{g} \rangle$, where $\overline{g} = gN$. If G is finite in addition to being cyclic with $N \leq G$, then $|G/N| = |G|/|N|$.

- Suppose $N \leq Z(G)$. Then $N \trianglelefteq G$, since $gng^{-1} = n \in N$ for every $g \in G$ and $n \in N$. In particular, $Z(G) \trianglelefteq G$. Recall that $\langle -1 \rangle \subseteq Q_8$ was seen to be the kernel of a homomorphism, but because $\langle -1 \rangle = Z(Q_8)$, then we have another fashion of arguing for its normality in Q_8.
- Let $G = D_8$, and note that $Z(D_8) = \langle r^2 \rangle$. Then for every $x \in D_8$, the coset $x\langle r^2 \rangle = \{x, xr^2\}$. Since D_8 has 8 elements and $x\langle r^2 \rangle$ has 2, there are 4 cosets consisting of two elements each in the quotient group:

$$D_8/\langle r^2 \rangle = \{\overline{1}, \overline{r}, \overline{s}, \overline{rs}\}$$

We then have that $D_8/\langle r^2 \rangle \cong Z_4$ or V_4. However, we note the following:

$$(\overline{r})^2 = r^2\langle r^2 \rangle = 1\langle r^2 \rangle = \overline{1}$$
$$(\overline{s})^2 = s^2\langle r^2 \rangle = 1\langle r^2 \rangle = \overline{1}$$
$$(\overline{rs})^2 = (rs)^2\langle r^2 \rangle = 1\langle r^2 \rangle = \overline{1}$$

so that every nonidentity element in the quotient group has order 2. Since no element has order 4, then $D_8/\langle r^2 \rangle$ is not cyclic, hence $D_8/\langle r^2 \rangle \cong V_4$.

3.2 More on Cosets and Lagrange's Theorem

Theorem 3.8 ▶ Lagrange's Theorem

Let G be a finite group and let $H \leq G$. Then the order of H divides the order of G, and the number of distinct left cosets of H in G is given by $|G|/|H|$.

Proof. Let $|H| = n$ and let the number of left cosets of H in G be k. By Proposition 3.4, the set of left cosets of H in G partition G. The mapping from $H \to gH$ defined by $h \mapsto gh$ is clearly a surjection, and is injective, since $gh_1 = gh_2$ implies $h_1 = h_2$ for $gh_1, gh_2 \in gH$. It follows that $|gH| = |H| = n$. Since G is partitioned into k disjoint subsets each with cardinality n, it follows that $|G| = kn$ so that $k = |G|/|H|$. □

Definition 3.6 ▶ Index

Let G be a (possibly infinite) group with $H \leq G$. Then the number of left cosets of H in G is called the **index** of H in G, denoted by $[G : H]$.

- If G is finite, then $[G : H] = |G|/|H|$ by Theorem 3.8.
- If G is infinite, then $[G : H]$ may be finite or infinite. For example, $\{0\} \leq \mathbb{Z}$ has infinite index, while $\langle n \rangle \leq \mathbb{Z}$ has index n.

Corollary 3.9 ▶ Order of Element Divides Group Order

Let G be a finite group and let $g \in G$. Then the order of g divides the order of G. In particular, $g^{|G|} = 1$.

Proof. Proposition 2.2 shows that $|g| = |\langle x \rangle|$. Then the first part follows by using Lagrange's Theorem on $H = \langle g \rangle$. Since $|G|$ is a multiple of $|g|$, the second part follows. □

Corollary 3.10 ▶ Prime Order Implies Cyclic

Let G be a group with prime order p. Then G is cyclic, and $G \cong Z_p$.

Proof. Let $g \in G$ be a nonidentity element. Then $|\langle g \rangle| > 1$, and $|\langle g \rangle| \mid p$ by Corollary 3.9, hence $|\langle g \rangle| = p$. It follows that $\langle g \rangle = G$, so that G is cyclic. It follows that $G \cong Z_p$ by Theorem 2.4. □

Example ▶ Normal Subgroup of S_3

Let $H = \langle (1\ 2\ 3) \rangle$ and $G = S_3$ so that $H \leq G$. Note that $H \leq N_G(H) \leq G$. Since $|H| = 3$ and $|G| = 6$, then $N_G(H)$ must either be 3 or 6. Observe that

$$(1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3\ 2) = (1\ 2\ 3)^{-1}$$

so that $(1\ 2) \in N_G(H)$, hence $N_G(H) \neq H$ so that $N_G(H) = G$. It follows that $H \trianglelefteq G$.

Example ▶ Subgroups of Index 2 are Normal

Let G be a group with $H \leq G$ such that $|G : H| = 2$. Pick $g \in G - H$ so that the two left cosets of H in G are $1H$ and gH. Since $1H = H$ and the cosets partition G, it must be that $gH = G - H$. A similar argument shows that

$Hg = G - H$ so that $gH = Hg$. Then Theorem 3.6 shows that $H \trianglelefteq G$. By definition of index, then $|G/H| = 2$, and $G/H \cong Z_2$.

We note this result is not because we may choose the same coset representatives 1 and g for both the left and right cosets of H, but through a pigeon-hole principle: because $1H = H = H1$, then the index assumption shows the remaining elements to be the remaining coset, either left or right.

Note ▸ Transitivity of Normality

It is not generally true that if $N \trianglelefteq H$ and $H \trianglelefteq G$ then $N \trianglelefteq G$. For example, $\langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8$, but $\langle s \rangle$ is not normal in D_8 because $rsr^{-1} = sr^2 \notin \langle s \rangle$.

Example ▸ Non-Normal Subgroup

Let $H = \langle (1\,2) \rangle \leq S_3$. Since H has prime index 3, then Lagrange's Theorem shows that $N_{S_3}(H)$ are either H or S_3. Since $(1\,3)(1\,2)(1\,3) = (2\,3) \notin H$, then $N_{S_3}(H) = H$, hence H is not a normal subgroup of S_3.

Another way to argue this is to consider the left and right cosets of H in S_3. For example, $(1\,3)H = \{(1\,3), (1\,2\,3)\}$, while $H(1\,3) = \{(1\,3), (1\,3\,2)\}$. Since $(1\,3)H$ is the unique left coset containing $(1\,3)$, then $(1\,3)H$ cannot be a left coset.

Yet another way to see this is to observe that the multiplication of two cosets is not well-defined. For example, consider $1H$ and $(1\,3)H$. Observe that $1H = (1\,2)H$, yet $1(1\,3) \neq (1\,2)(1\,3) = (1\,3\,2) \notin H$ so that they are not elements of the same left coset. This shows that the cosets of a subgroup form a group *only* when the subgroup is normal.

Example ▸ Generalization of Previous Example

Let $G = S_n$ for $n \in \mathbb{Z}^+$, and fix $i \in \{1, 2, \ldots, n\}$. The stabilizer of i is the set $G_i = \{\sigma \in G \mid \sigma(i) = i\}$. Now suppose $\tau \in G$ such that $\tau(i) = j$. Then $\tau\sigma(i) = j$ for all $\sigma \in G_i$. Moreover, if $\mu \in G$ such that $\mu(i) = j$, then $\tau^{-1}\mu(i) = i$ so that $\tau^{-1}\mu \in G_i$, hence $\mu \in \tau G_i$. Then the left coset $\tau G_i = \{\mu \in G \mid \mu(i) = j\}$ comprises of the permutations in S_n that send i to j.

It is clear that distinct left cosets have no elements in common, for otherwise if $\tau G_i = \pi G_i$ for $\tau, \pi \in G$ such that $\tau(i) = j$ and $\pi(i) = k$, then there would be some permutation $\mu \in \tau G_i$ such that $\mu(i) = k$ and $\mu(i) = j$, hence μ would not be well-defined. The number of distinct left cosets is precisely the number of images that i may be sent to, namely n. It follows that $|G : G_i| = n$.

Note that elements of the left coset τG_i are permutations that begin with σ and end with τ so that $i \mapsto j$. It follows that elements of the right coset $G_i\tau$ are permutations that begin with τ and end with σ so that $k \mapsto j$. Hence, if $k = \tau^{-1}(i)$, then $\tau(k) = i$, and $G_i\tau = \{\lambda \in G \mid \lambda(k) = i\}$. For $n > 2$ and $\tau \in G$, then $\tau G_i \neq G_i\tau$ in general, since there exists permutations that take i to j but do not take k to i. Hence, G_i is not a normal subgroup.

Note ▸ Converse of Lagrange's Theorem

- Observe that the full converse of Lagrange's Theorem is not true, i.e., if G is a finite group with n dividing $|G|$, then G need not have a subgroup of order n. Consider A to be the group of symmetries of a regular tetrahedron, where $|A| = 12$. If A had a subgroup H of order 6, then $|A : H| = 2$ so that $H \trianglelefteq A$, and $A/H \cong Z_2$. It follows that the square of every element in A/H is the identity, hence for every $g \in A$, then $(gH)^2 = 1H$ or that $g^2 \in H$. In particular, if $g \in A$ such that $|g| = 3$, then $g^3H = gH = H$ so that $g \in H$, hence H contains all elements of order 3. However, there are 8 elements of order 3 in A, which are the 120° rotations about a line from a vertex to the center of the opposing face.
- Some partial converses to Lagrange's Theorem exists, namely that the full converse is true for finite *abelian* groups. There are other theorems that guarantee the existence of subgroups of certain orders, such as Cauchy's Theorem and Sylow's Theorems.

Theorem 3.11 ▸ Cauchy's Theorem

Let G be a finite group with p dividing $|G|$. Then G has an element of order p.

Theorem 3.12 ▸ Sylow

Let G be a finite group of order $p^\alpha m$, where p is a prime with $p \nmid m$. Then G has a subgroup of order p^α.

Definition 3.7 ▸ Product of Subgroups

Let H and K be subgroups of a group G. Then their **product** is the set

$$HK = \{hk \mid h \in H,\ k \in K\}$$

Proposition 3.13 ▸ Order of Subgroup Product

Let H and K be finite subgroups of a group G. Then

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Proof. Note that HK is a union of left cosets of K, namely

$$HK = \bigcup_{h \in H} hK$$

Since each coset of K has $|K|$ elements, we need to find the number of *distinct* left cosets of the form hK for $h \in H$. Observe that $h_1K = h_2K$ if and only if $h_2^{-1}h_1 \in K$ for $h_1, h_2 \in H$. Then $h_2^{-1}h_1 \in H \cap K$ if and only if $h_1(H \cap K) = h_2(H \cap K)$. Then the number of distinct left cosets of K in HK is equal to the number of distinct left cosets of $H \cap K$ in H, which is given by Lagrange's Theorem as $|H|/|H \cap K|$. Since each distinct cosets of K contain $|K|$ elements, then the formula follows. □